

RETO 10

**Escaneo,
estudio y análisis
de redes WIFI del entorno con Acrylic**

Pablo Ramiro Foronda

Marianela Estévez Bosso

Ignacio García García

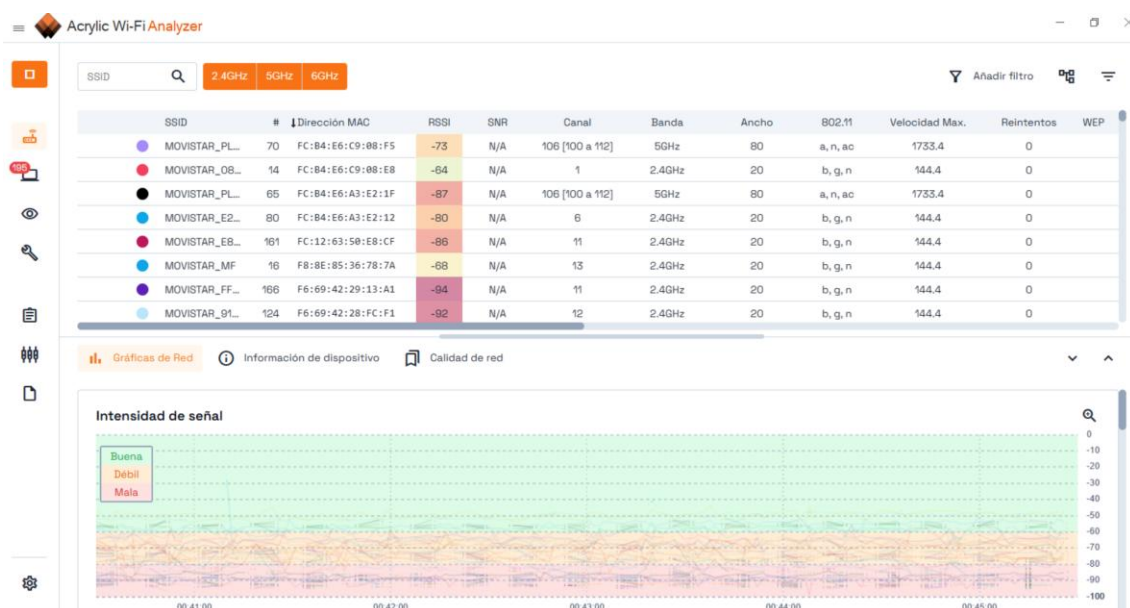
Guillermo Rojo Martín

En esta documentación se procede a realizar un informe acerca del comportamiento y características de redes WIFI mediante el uso de Acrylic Wi-Fi Analyzer, software de pago desarrollado para la recogida de datos en tiempo real de redes inalámbricas, entre otras cosas.

Este análisis se da en un entorno residencial, por lo que se da por entendido que la mayoría de estas redes, por no decir en su totalidad, son de uso doméstico.

El informe se enfocará en puntos tales como la seguridad y protocolos usados por dichas redes, la intensidad de señal que tienen y el canal.

1. Intensidad de la señal



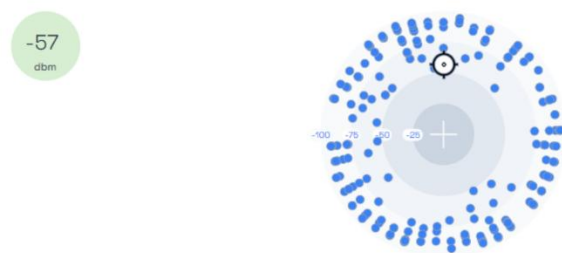
La intensidad de señal se mide en dBm (decibelios miliwatt) con valor negativo. Se dividen en tres áreas siendo estas coloreadas y representando cada una un intervalo.

De -100 a -80 dBm se entiende que la red tiene mala señal, no sería la más apta para conectarse.

De -80 a -60 la red es débil, y por último de -60 a 0 decimos que la red tiene buena señal y sería muy apta para conectarse. Mayoritariamente las redes se sitúan en la parte baja, por lo que se entiende que no estamos en un sitio óptimo para conectarnos a placer, ya sea por una

gran distancia a los routers o la existencia de obstáculos físicos o intangibles que no dejan captar la señal mejor (paredes, interferencias...).

Radar de dispositivo ⓘ



La red a la que estamos conectados es próxima a nuestra posición y tiene buena señal.

2. Análisis de seguridad

Acrylic Wi-Fi Analyzer

SSID

2.4GHz

5GHz

6GHz

Añadir filtro

Ancho	802.11	Velocidad Max.	Reintentos	WEP	WPA	WPA2	WPA3	WPS	Fabricante	Data	Management	Enviados
80	a, n, ac	1733.4	0			PSK-CCMP		1.0	ASKEY COM...	0	143	143
20	b, g, n	144.4	0			PSK-CCMP		1.0	ASKEY COM...	0	511	511
80	a, n, ac	1733.4	0			PSK-CCMP		1.0	ASKEY COM...	0	91	91
20	b, g, n	144.4	0			PSK-CCMP		1.0	ASKEY COM...	0	130	130
20	b, g, n	144.4	0		PSK-(TKL...			1.0	Comtrend ...	0	182	182
20	b, g, n	144.4	0			PSK-CCMP			ASKEY COM...	0	7	7
80	a, n, ac, ax	2268	0			PSK-CCMP			ASKEY COM...	0	22	22
20	b, g, n, ax	540	0			PSK-CCMP		1.0	ASKEY COM...	0	18	18
80	a, n, ac, ax	2268	0			PSK-CCMP		1.0	ASKEY COM...	0	96	96
80	a, n, ac	1733.4	0			PSK-CCMP		1.0		0	153	153
80	a, n, ac	1733.4	0			PSK-CCMP		1.0		0	105	105
20	b, g, n	144.4	0			PSK-CCMP		1.0	MitraStar T...	0	40	40
80	a, n, ac	866.7	0			PSK-CCMP				0	46	46
40	b, g, n	300	0			PSK-CCMP				0	1	1
80	a, n, ac	866.7	0			PSK-CCMP				0	13	13
40	b, g, n	300	0			PSK-CCMP				0	2	2
80	a, n, ac	1733.4	0			PSK-CCMP			zte corpor...	0	4	4

Gráficas de Red

Información de dispositivo

Calidad de red

Se presta especial atención a las columnas subrayadas.

802.11 es el estándar WIFI que soporta cada red. Se trata de un conjunto de normas creada en 1997 por IEEE que cuenta con varias revisiones. Hoy en día algunas versiones trabajan con tanto con 2,4GHZ como con 5GHz.

En la imagen cada fila representa una red, teniendo cada una ligera variación en sus características, aunque con gran parecido en general.

En lo referente a la columna 802.11, se ven letras tales como a, b, n, ax... Esto representa las versiones del estándar soportados, con diferentes bandas (2.4, 5 o 6) y velocidades máximas teóricas distintas (Mbps).

Sin embargo, los mecanismos de seguridad aquí son optativos, para ver verdad la seguridad de estas redes, miramos las columnas del medio. Estas representan distintos protocolos usados como mecanismo de cifrado.

WEP (Wired Equivalent Privacy) prácticamente no se usa por ser obsoleta, aunque cabe destacar que las pocas redes con WEP tenían dos métodos de autenticación: SharedKey (hay que conocer una clave compartida para entrar), y Open (no hace falta clave para conectarse), además de menos segura que el resto.

WPA tampoco es común ya.

WPA2 es la más frecuente y prácticamente todas las redes la usan porque es segura. Cabe mencionar que tanto WPA como WPA2 usan PSK-CCMP (Pre-Shared Key-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) que es un método de cifrado fuerte basado en AES.

Se puede observar que WPA3 tampoco es un tipo de mecanismo que se acepte ampliamente, al menos para redes de uso común y “de hogar”.

Por último, se puede apreciar que un número moderado de redes tienen WPS activada (1,0). Esto reduce la seguridad efectiva, pues esto supone una vulnerabilidad y un punto por el que un ataque de fuerza bruta puede llevarse a cabo.

Con Acrylic podemos ver también el envío y recibimiento de paquetes.

WPS	Fabricante	Data	Management	Enviados	Recibidos	Primera vez	Última vez
1.0	ASKEY COM...	0	460	460	0	23:42:36	01:02:01
1.0	ASKEY COM...	0	1561	1561	0	23:42:23	01:02:06
1.0	ASKEY COM...	0	356	356	0	23:42:36	01:02:01
1.0	ASKEY COM...	0	623	623	0	23:42:59	01:02:05
1.0	ASKEY COM...	0	20	20	0	00:07:38	00:48:50
1.0	Comtrend ...	0	638	638	0	23:42:23	01:02:06
	ASKEY COM...	0	4	4	0	00:11:29	00:18:07
	ASKEY COM...	0	29	29	0	23:45:53	01:01:57
	ASKEY COM...	0	40	40	0	23:42:42	00:30:03
	ASKEY COM...	0	14	14	0	00:24:57	00:45:16
1.0	ASKEY COM...	0	49	49	0	23:53:14	01:01:47
1.0	ASKEY COM...	0	15	15	0	00:17:20	01:01:33
1.0	ASKEY COM...	0	254	254	0	23:42:32	01:01:33
1.0		0	503	503	0	23:42:32	01:02:01
1.0		0	392	392	0	23:42:32	01:02:01
	MitraStar T...	0	13	13	0	00:11:20	00:37:13
1.0		0	3	3	0	00:42:28	00:48:50

La mayoría de tráfico de paquetes enviados por parte de las redes era de gestión, lo que quiere decir que no se registró tráfico de usuario activo (o transferencia de datos activa) durante el escaneo.

Esto puede deberse a la hora en que se realiza el análisis (cerca de la 1 de la mañana).

3. Canales

Por último, veremos rápidamente los canales usados por las redes. Aunque es verdad que la frecuencia de por si no determina la seguridad de una red, si podemos destacar por ejemplo el hecho de que una red en 5 GHz tiene menor alcance, lo que se podría traducir a menor exposición hacia afuera y un incremento en la dificultad en caso de que alguien quiera atacar o interceptar la señal. Además, las redes 5 GHz se asocian a routers mas recientes que ya no usarán cifrados de tipo débil como WEP



4. Conclusión

En conclusión, gracias al análisis se han podido observar diferentes comportamientos en un conjunto de redes domésticas.

Se ve una aceptación generalizada la WPA2 con cifrado CCMP, que es bueno porque indica un cifrado fuerte. Sin embargo, se ha detectado un punto débil que varias de estas redes compartían, la activación del protocolo WPS, que deja a nuestra red con posibilidad de ser atacado.

En promedio 1 de cada 10 redes no usaba WPA2 si no alguna de las otras 3 y 6 de cada 10 presentaban vulnerabilidad al tener WPS activado.