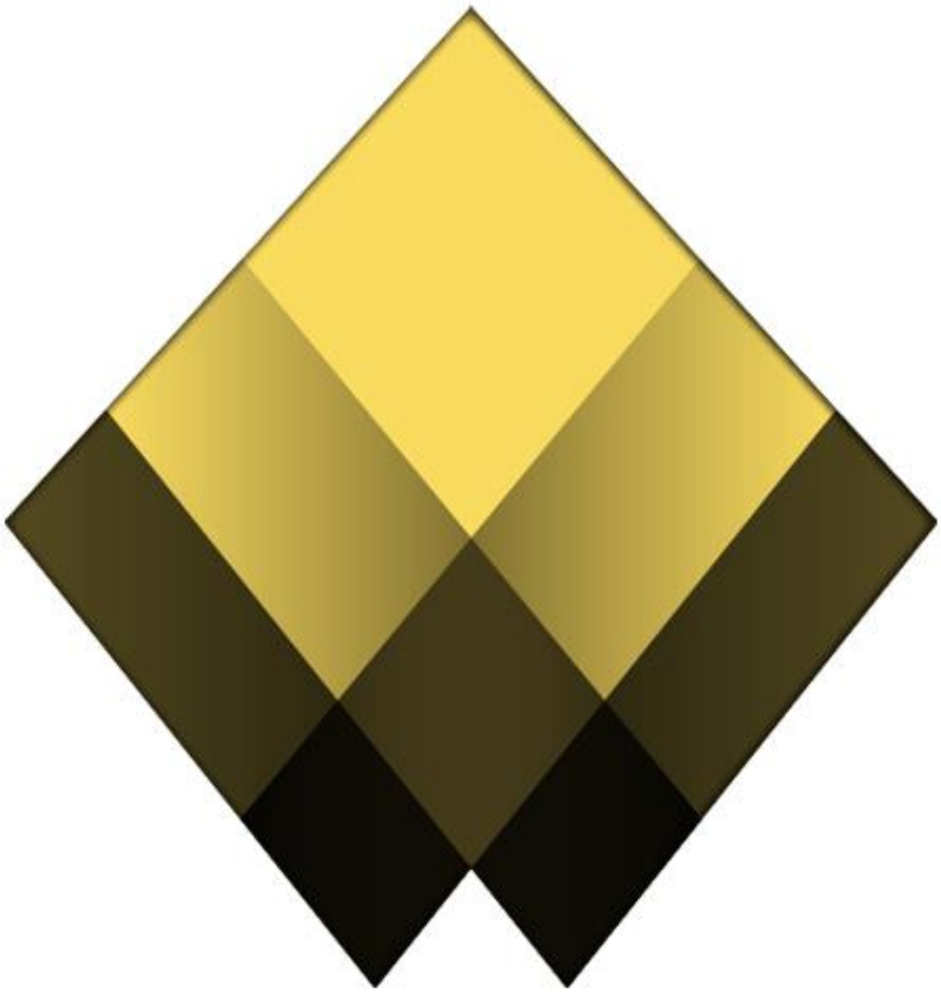


PROFESSIONAL
ACRYLIC
WiFi

Quick Help

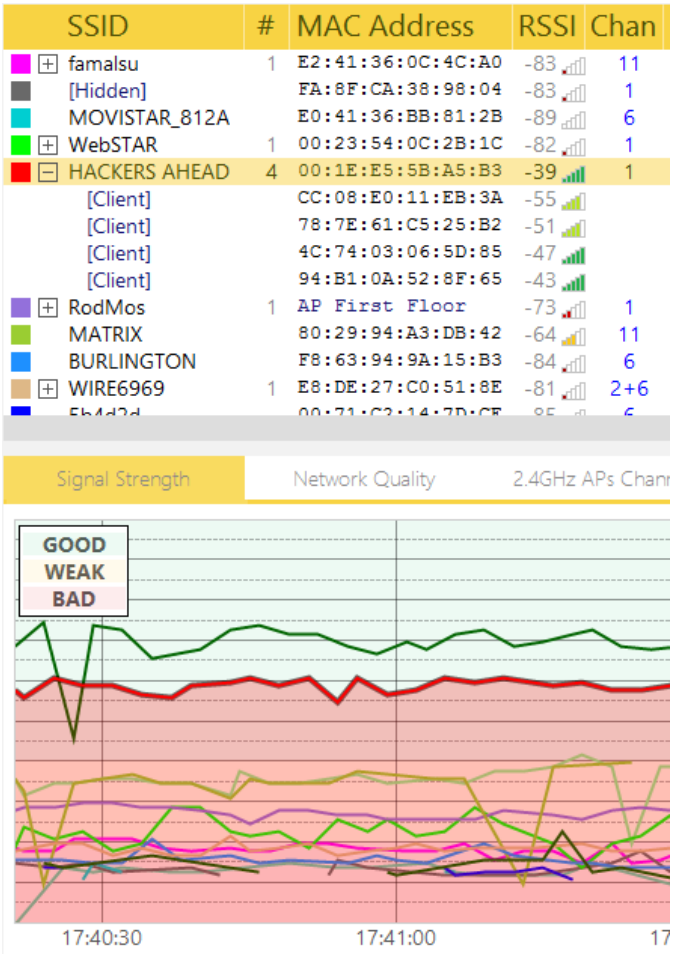
25/04/2016

support@acrylicwifi.com
www.acrylicwifi.com

Contenido

Puntos de acceso

Esta sección es el panel central de la aplicación dónde se mostrará una vista general de los dispositivos WiFi detectados.



Los puntos de acceso y los dispositivos conectados se muestran de manera jerárquica.

Cada dispositivo se representa en una fila dentro de la tabla, incluyendo información sobre el en cada columna, como intensidad de señal, ratio señal-ruido, dirección MAC, opciones de seguridad, etc. Esta ventana es de gran ayuda se quiere obtener información sobre el estado de los dispositivos WiFi de un vistazo.

Es posible pulsar en los cuadrados de colores para cambiar la selección de puntos de acceso, lo que modificará lo que se muestra en las pestañas debajo de esta.

Haciendo clic sobre el icono **'+'** el árbol se expandirá mostrando todos los dispositivos conectados al puntos de acceso seleccionado.

Columna	¿Qué información proporciona?
SSID	Significa: 'Service Set Identifier'. En otras palabras: el nombre de la red. Una red puede ocultar su nombre, lo que llevará a que en el software se muestra este campo con el texto [Hidden]. Este texto es configurable en

Columna	¿Qué información proporciona?
	la ventana de *Preferences* que se muestra pulsando la opción *Configure* en el menú principal. Sin embargo, incluso cuando una red no está publicando su nombre, en algunos casos en modo monitor este nombre puede ser obtenido inspeccionando y analizando el tráfico WiFi de los dispositivos que se conectan a esa red. En caso de que esto sea posible, Acrylic mostrará este nombre en color rojo, lo que significa que es una red oculta y que el nombre ha sido inferido por el software.
#	Esta columna muestra el número de dispositivos que hay conectados a esa red. Si se muestra vacío significa que ningún dispositivos ha sido detectado como conectado a la red. Cuando un *Scan* se lleva a cabo en modo Normal, este campo se ocultará automáticamente. Esto se debe a que en este modo, Acrylic WiFi solo puede recoger información sobre puntos de acceso, no de dispositivos cliente.
Mac Address	(**M**edia **A**ccess **C**ontrol **Address**) Identificador único asignado a las interfaces de red y utilizado como dirección de red. Este campo puede mostrar un nombre en lugar de los bytes de la dirección en caso de que la dirección MAC haya sido previamente inventariada.
RSSI	(**R**eceived **S**ignal **S**trength **I**ndication) Valor, medido en dBm, que indica la intensidad de la señal WiFi recibida, usualmente en el rango de 0 a -100. Cuanto más alto es el valor de esta propiedad, mejor es la intensidad de señal.
SNR	(**S**ignal-to-**N**oise **R**atio) Ratio medido en dB que se utiliza para comparar la señal recibida y el ruido de fondo. Cuanto más alto es el valor de esta propiedad, mejor es la calidad de la comunicación. Este campo se ocultará automáticamente cuando se lleve a cabo un *Scan* en modo *Monitor*. Esto se debe a que esta información no puede ser obtenida cuando se captura tráfico WiFi en este modo (a no ser que se utilice un dispositivo Airpcap).
Chan	Canal en el que la red está operando. Se puede mostrar como una suma de dos valores (como: '1+5'), lo que indica que la red está operando en ambos canales (primario y secundario).
Width	Anchura de canal medida en Mhz. Los valores posibles son 20, 40, 80 y 160.
802.11	Representa los estándares de comunicación que soportan los puntos de acceso que publican esta red. Los posibles valores son una combinación de a,b,g,n,ac.
Max rate	La tasa máxima de transferencia que soporta el punto de acceso en esta red, medida en Mb/s.

Columna	¿Qué información proporciona?
Retries	Porcentaje de paquetes que han tenido que ser retransmitidos debido a errores de transmisión. Entre paréntesis se muestra el número total de paquetes retransmitidos.
WEP	Tipo de seguridad WEP del punto de acceso. Si se muestra vacío significa que la red no soporta WEP. Los posibles valores son 'SharedKey' y 'Open'.
WPA	Tipo de seguridad WPA del punto de acceso. Si se muestra vacío significa que la red no soporta WPA. Los posibles valores son 'PSK' and 'MGT'.
WPA2	Tipo de seguridad WPA2 del punto de acceso. Si se muestra vacío significa que la red no soporta WPA2. Los posibles valores son 'PSK' and 'MGT'.
WPS	Muestra la versión soportada por el punto de acceso de WPS. Si se muestra vacío significa que la red no soporta WPS. Si la autenticación WPS está habilitada se muestra en verde. En caso contrario se muestra en rojo.
Password	Algunos puntos de acceso que son proporcionados por ISPs incluyen contraseñas por defecto conocidas. La sección de *Scripting* contiene scripts que identifican esos puntos de acceso y revelan la contraseña por defecto. Dependiendo del modelo, pueden ser reveladas una o varias contraseñas. En todo caso, es posible utilizar el módulo de conectividad para probar un conjunto de contraseñas contra el punto de acceso. Por favor, tenga en cuenta que solo las contraseñas por defecto serán reveladas, por lo que el usuario debería cambiarlas por seguridad.
WPS PIN	Algunos puntos de acceso que son proporcionados por ISPs incluyen Pin WPS por defecto de fábrica. La sección de *Scripting* contiene scripts que identifican esos puntos de acceso y revelan el Pin WPS. Dependiendo del modelo, pueden ser revelados uno o varios Pin WPS.
Vendor	El nombre del fabricante de la interfaz de red que está siendo utilizada por el dispositivo.
Data	Número de paquetes *Data* que han sido enviados por el dispositivo.
Mgt	Número de paquetes *Management* que han sido enviados por el dispositivo.
First	Hora a la que el dispositivo ha sido detectado por primera vez.
Last	Hora a la que el dispositivo ha sido detectado por última vez.
Type	Tipo de red. Los posibles valores son 'Infrastructure' and 'Ad-hoc'. Este campo solo tiene sentido con puntos de acceso
Latitude	Cuando se monitoriza con GPS, la latitud se actualiza a la posición donde el dispositivo ha sido detectado por última vez.
Longitude	Cuando se monitoriza con GPS, la longitud se actualiza a la posición donde el dispositivo ha sido detectado por última vez.

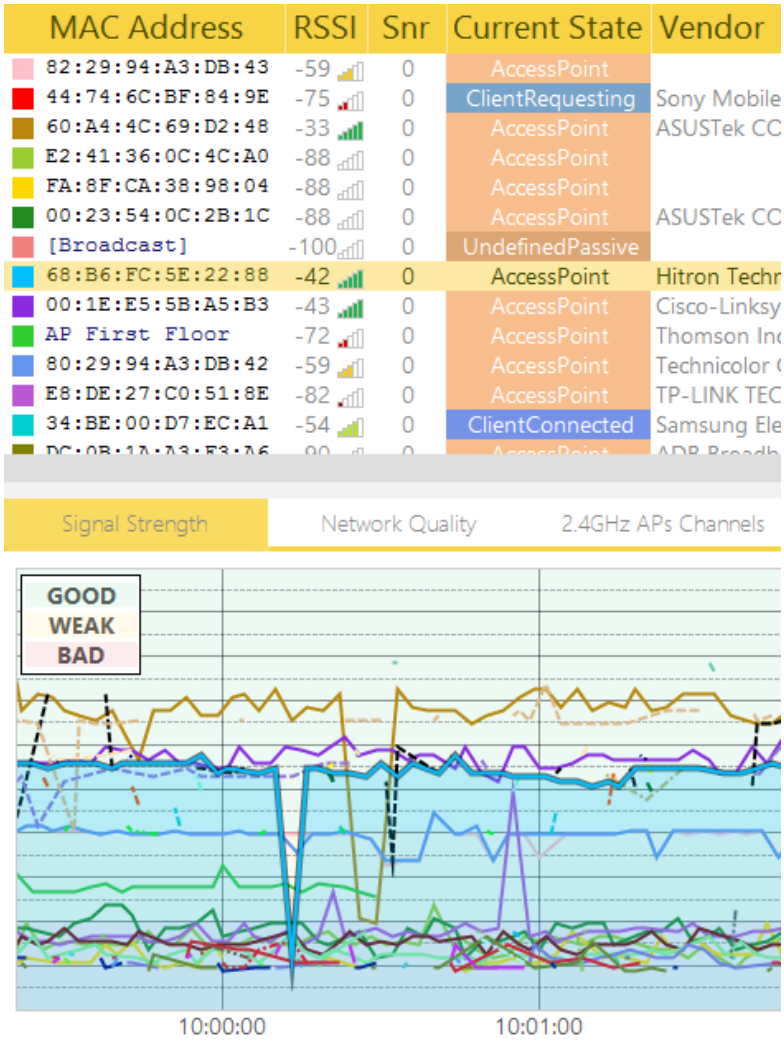
Opciones adicionales

Pulsando con el botón derecho del ratón sobre la ventana *Puntos de acceso*, se mostrará un menú contextual que permite llevar a cabo acciones sobre los puntos de acceso o dispositivos.

Stations

La sección de *Stations* muestra cada dispositivo con sus capacidades WiFi.

Normalmente, un dispositivo se denomina **STATION** o **STA**.



Todos los dispositivos Wireless envían paquetes Wireless al aire cuando se encienden. Los puntos de acceso anuncian que pueden proporcionar una determinada red, los dispositivos como teléfonos móviles, tabletas u ordenadores portátiles envían paquetes preguntando si hay dispositivos en los alrededores.

Cada dispositivo tiene un identificador único conocido como dirección MAC. Acrylic WiFi Professional obtiene información relacionada con cada uno y proporciona métricas de transmisión como las que se muestran en siguiente tabla:

Columna	¿Qué información proporciona?
Mac Address	(Media Access Control Address) Identificador único asignado a las interfaces de red y utilizado como dirección de red.

<table>
<tr><th>Columna</th><th>¿Qué información proporciona?</th></tr>
<tr><td></td><td>Este campo puede mostrar un nombre en lugar de los bytes de la dirección en caso de que la dirección MAC haya sido previamente inventariada.</td></tr>
<tr><td>RSSI</td><td>(Received Signal Strength Indication) Valor, medido en dBm, que indica la intensidad de la señal WiFi recibida, usualmente en el rango de 0 a -100. Cuanto más alto es el valor de esta propiedad, mejor es la intensidad de señal.</td></tr>
<tr><td>SNR</td><td>(Signal-to-Noise Ratio) Ratio medido en dB que se utiliza para comparar la señal recibida y el ruido de fondo. Cuanto más alto es el valor de esta propiedad, mejor es la calidad de la comunicación.

Este campo se ocultará automáticamente cuando se lleve a cabo un Scan en modo Monitor. Esto se debe a que esta información no puede ser obtenida cuando se captura tráfico WiFi en este modo (a no ser que se utilice un dispositivo Airpcap).</td></tr>
<tr><td>Current State</td><td>Nomenclatura interna que Acrylic WiFi Professional utilizar para clasificar cada dispositivo atendiendo a su comportamiento.</td></tr>
<tr><td></td><td>
<table>
<tr><th>Estado</th><th>Descripción</th></tr>
<tr><td>AccessPoint</td><td>El dispositivo actúa como un punto de acceso</td></tr>
<tr><td>ClientRequesting</td><td>El dispositivo está solicitando redes. Es el comportamiento normal de smartphones, ordenadores portátiles, tabletas, etc…</td></tr>
<tr><td>ClientConnected</td><td>Es un dispositivo conectado a otro dispositivo WiFi.</td></tr>
<tr><td>UndefinedActive</td><td>El dispositivo envía paquetes pero no se ha obtenido suficiente información para inferir su tipo.</td></tr>
<tr><td>UndefinedPassive</td><td>El dispositivo es receptor de paquetes WiFi pero no se ha obtenido suficiente información para inferir su tipo.</td></tr>
<tr><td>WDS</td><td>El dispositivo se comporta como un WDS, Sistema de Distribución Wireless.</td></tr>
<tr><td>Unknown</td><td>No se ha obtenido suficiente información para inferir su comportamiento.</td></tr>
</table>
</td></tr>
<tr><td>Vendor</td><td>El nombre del fabricante de la interfaz de red que está siendo utilizada por el dispositivo.</td></tr>
<tr><td>WPS Info</td><td>Indica si el dispositivo soporta WPS y la cantidad de información que proporciona.</td></tr>
<tr><td>Retries</td><td>Porcentaje de paquetes que han tenido que ser retransmitidos debido a errores de transmisión. Entre paréntesis se muestra el número total de paquetes retransmitidos.</td></tr>
<tr><td>Attempts</td><td>Intentos de conexión a otro dispositivo WiFi realizados por este dispositivo.</td></tr>
<tr><td># Sent</td><td>Cantidad de paquetes cuyo origen es este dispositivo.</td></tr>
</table>

Columna	¿Qué información proporciona?
# Received	Cantidad de paquetes cuyo destino es este dispositivo
# BSSID	Cantidad de paquetes en los que este dispositivo actúa de intermediario.
First	Hora a la que el dispositivo ha sido detectado por primera vez.
Last	Hora a la que el dispositivo ha sido detectado por última vez.
Data	Número de paquetes *Data* que han sido enviados por el dispositivo.
Mgt	Número de paquetes *Management* que han sido enviados por el dispositivo.

Opciones adicionales

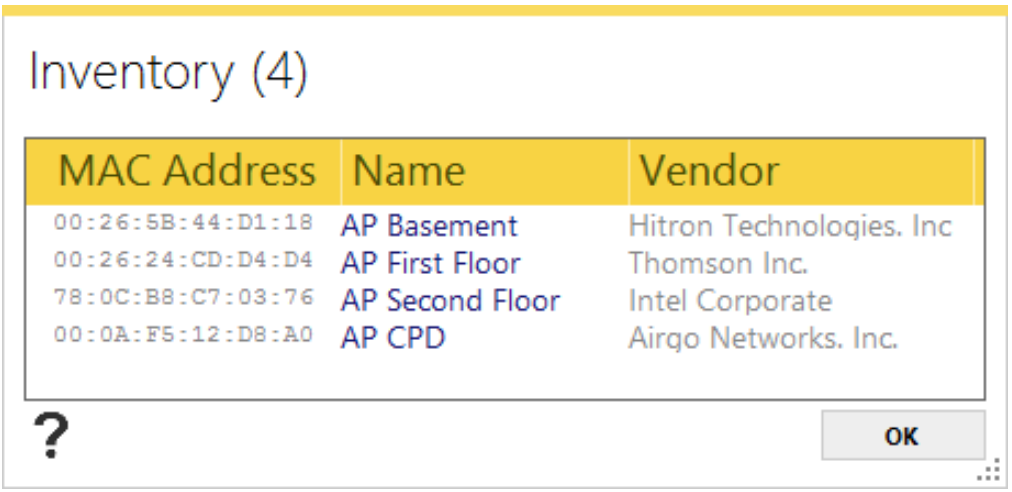
Es posible interactuar con los dispositivos que se muestran en esta sección a través del menú contextual de botón derecho.

En este menú contextual es posible interactuar con las *Stations* y realizar tareas como generar informes en formato HTML, TXT o CSV, enviar un tweet en el que se visualice la información o copiar datos al portapapeles.

Inventario

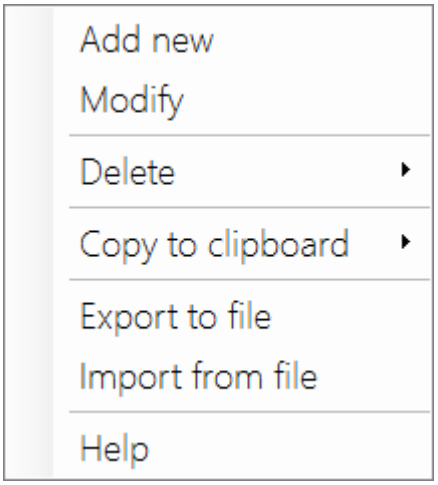
En esta sección se muestran todos los dispositivos que han sido inventariados

Cuando un dispositivo es inventariado, se le asigna un nombre común a su dirección MAC, de tal manera que cada vez que se muestre dicho dispositivo en Acrylic WiFi lo hará con el nombre asignado en lugar que con la dirección MAC.



Columna	¿Qué información proporciona?
Mac Address	(Media Access Control Address) Identificador único asignado a las interfaces de red y utilizado como dirección de red.
Name	Nombre común asignado al dispositivo. Este nombre se mostrará en Acrylic WiFi en lugar de la dirección MAC.
Vendor	Nombre del fabricante del dispositivo. No editable: Se obtiene automáticamente en base a la dirección MAC.

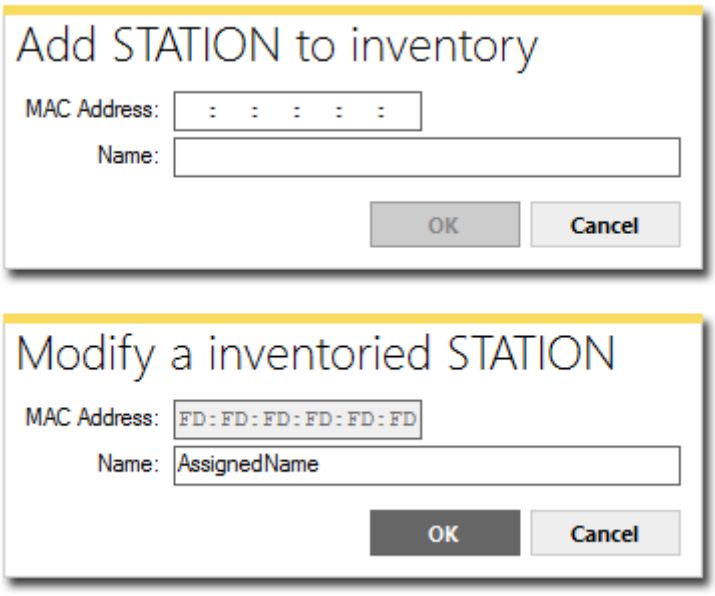
Menú de botón derecho del ratón



Menú contextual solo disponible al pulsar el botón derecho el ratón sobre la ventana de inventario.

Elemento	Función
Add new	Añade una nueva entrada al inventario
Modify	Permite modificar la información del elemento inventariado
Delete	Elimina un elemento inventariado
Copy to clipboard	Copia la información sobre elementos inventariados al portapapeles
Export to file	Permite exportar el contenido del inventario a un fichero .csv
Import from file	Permite importar el contenido del inventario desde un fichero .csv

Añadir o modificar elementos del inventario



La ventana para añadir o modificar entradas del inventario permite la introducción de datos del dispositivo.

En caso de modificarlos, estos campos serán rellenados con la información actual que va a ser editada.

Visor de paquetes

Filtros

Los filtros pueden aplicarse sobre los paquetes recibidos para realizar un análisis específico. Estos filtros pueden añadirse desde la caja de texto de filtros o, directamente, desde el árbol de paquetes (Botón derecho sobre la vista de árbol para utilizar el nodo como filtro). Cuando se introduce texto en la caja de texto de filtros se llevará a cabo una comprobación de sintaxis en tiempo real. Si la sintaxis es correcta la caja de texto se mostrará con el fondo verde. En otro caso, se mostrará con el fondo rojo.

Ejemplos de filtros

Filtro	Resultado
`ieee80211.management.beacon.exists`	Muestra todos los paquetes que contienen un campo *beacon*
`ieee80211.management.sa == 00:20:1F:1A:03:F1`	Muestra todos los paquetes con la dirección de origen especificada
`ieee80211.management.sequencecontrol > 0x3400`	Muestra todos los paquetes con una secuencia de control mayor que 0x3400

Sintaxis

Las especificaciones de paquete en el protocolo 802.11 han sido encapsuladas en una estructura de árbol. Es posible acceder a esta estructura a través de nombres de campo separados por puntos (“.”). La estructura del protocolo se muestra al seleccionar un nodo de paquete en el “*Packet tree view*”.

Hay dos nodos raíz para acceder a la información de paquete:

Nodo raíz	Descripción
`ieee80211`	Este es el nodo raíz por defecto. Todos los paquetes 208.11 comienzan con este nodo, lo que permite acceder a todo el protocolo a través de sus campos. Es posible comprobar esto haciendo clic sobre un paquete y observando la representación del *Packet Tree View*. Estos son ejemplos de campos a los que se llegó a través del nodo raíz: • `ieee80211.management` • `ieee80211.control` • `ieee80211.data`

Nodo raíz	Descripción
`RadioTapHeader`	Este nodo raíz permite acceder a datos adicionales procesados para cada paquete por el *driver* del adaptador de red. Estos datos no forman parte del paquete transmitido, pero proporcionan información extra sobre él, tales como el canal en el que se recibió, la intensidad de señal, etc. Ejemplo de uso: RadioTap.AntennaSignal > -50 <--- Paquetes que han sido recibidos con un nivel de señal mayor que -50dBm
`ies`	Este es un nodo especial, ya que permite acceder directamente a los *information elements* de cada paquete, si están disponibles. De esta manera, es posible establecer un filtro sobre un *information element* para cualquier tipo de paquete. De otra manera, sería necesario establecer todas las rutas posibles al IES para cada tipo de paquete. Ejemplo: `ies.ssid.ssid` <--- Afecta a beacons y probes.

Operadores válidos

Operador	Descripción
==	Operador de igualdad. Puede usarse con campos numéricos y de texto.
!=	Operador de desigualdad. Puede usarse con campos numéricos y de texto.
<	Menor que
>	Mayor que
<=	Menor o igual que
>=	Mayor o igual que
%	Módulo
+	Suma
-	Resta
*	Producto
/	División
and	**AND** lógico Ejemplo: (ies.ssid.ssid == 'HACKERS_AHEAD') **and** (ieee80211.management.sequencecontrol > 0x3400)
or	**OR** lógico Ejemplo: (ies.ssid.ssid == 'HACKERS_AHEAD') **or** (ieee80211.management.sequencecontrol > 0x3400)

Tipos

Tipo	Descripción
Number	Los valores numéricos pueden ser expresados como decimal o hexadecimal (comenzando con **0x**).

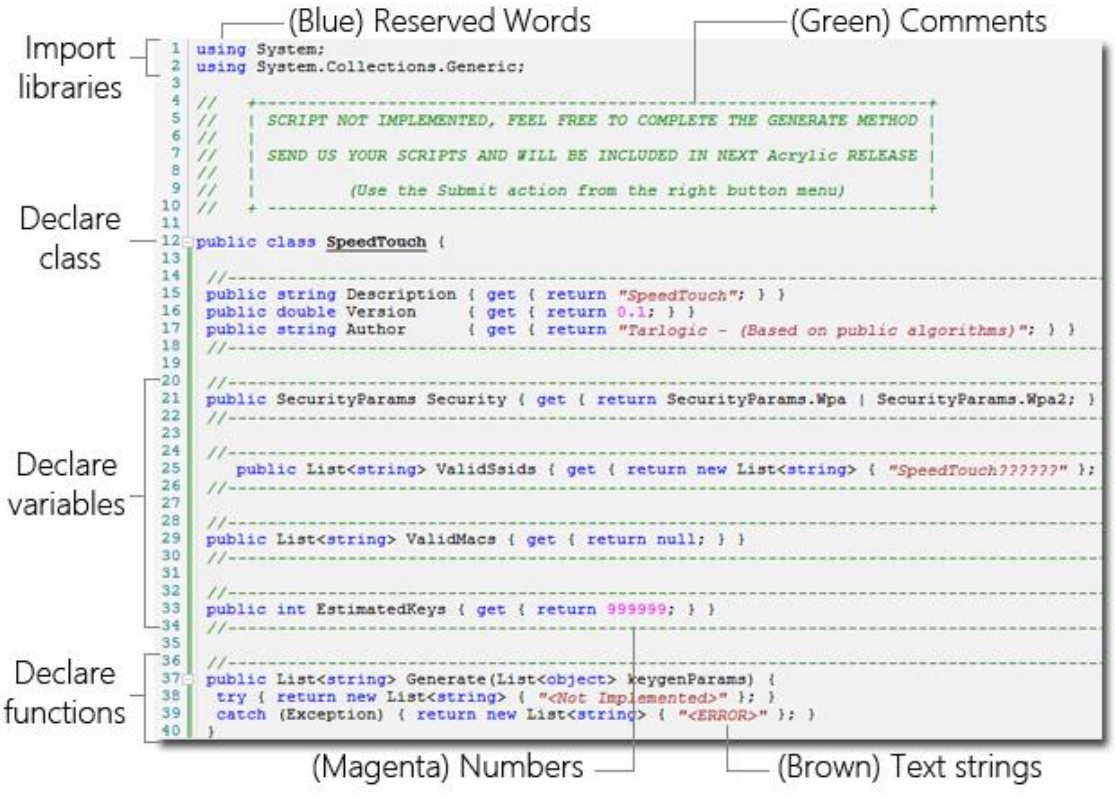
Tipo	Descripción
	Ejemplos: Decimal: `ieee80211.management.sequencecontrol > 13312` Hexadecimal: `ieee80211.management.sequencecontrol > 0x3400`
Text	El texto debe ser expresado entre comillas simples (') Ejemplo: • `ies.ssid.ssid == '#FBI Surveillance Van #1'`
Bytes	Las secuencias de bytes se pueden expresar concatenando bytes hexadecimales con dos puntos (:). Ejemplos: • `ieee80211.management.sa == 60:A4:4C:69:D2:48` • `ieee80211.management.beacon.fixed == 85:71:83:07:00:00:00:00:64:00`

Scripts

Editor de scripts

Desde esta sección es posible crear y modificar scripts, y probarlos contra ciertos SSIDs / MACs para validar que funcionan correctamente.

Los scripts están programados en C#.



El editor tiene resaltado de sintaxis como ayuda al desarrollo.

Los scripts pueden desarrollarse en otros IDEs (por ejemplo, Visual Studio) y ser incluidos en Acrylic WiFi

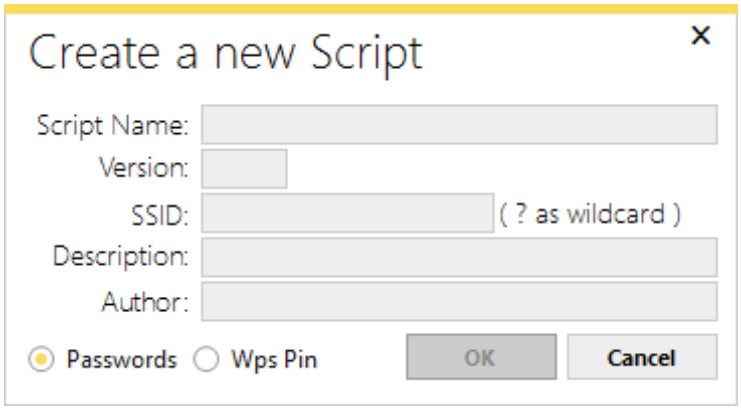
Acrylic también cuenta con una plantilla, a la que se accede escogiendo la opción *New script* en las opciones de la parte derecha del editor.

Los scripts de Acrylic WiFi deben tener siempre una clase principal, cuyo nombre es igual que el del fichero. Esta clase debe contar con las siguientes propiedades:

```
// Script description
public string Description { get { return "DESCRIPTION"; } }
// Script Version.
public double Version { get { return VERSION; } }
// Script Author
public string Author { get { return "AUTHOR"; } }
// Valid SSID's
public List<string> ValidSsids { get { return new List<string>{ "SSIDS" };}}
// Valid MAC's
public List<string> ValidMacs { get { return null; } }
// Estimated keys
public int EstimatedKeys { get { return 1; } }
// SSID Security type
public SecurityParams Security { get { return SecurityParams.Wpa |
SecurityParams.Wpa2; } }
```

Además, la clase principal debe tener una función de nombre *Generate* que será llamada cuando sea necesaria una contraseña.

```
public List string Generate(List<object> keygenParams);
```

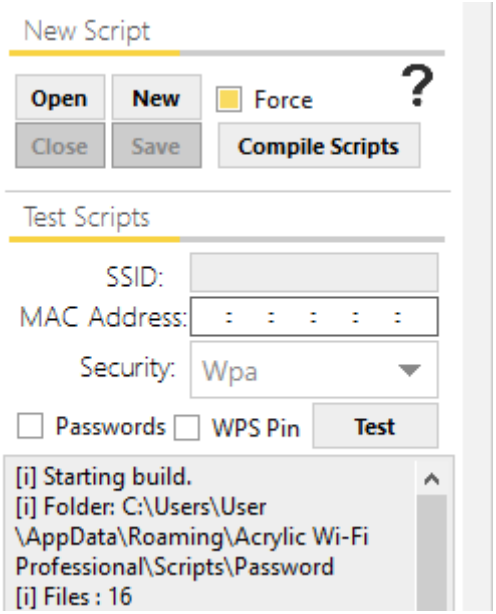


Para simplificar la creación de scripts, cuando se crea uno nuevo se muestra un Wizard en el que se solicitan los detalles principales para, a continuación, generar una plantilla de script, lista para introducir código en la función *Generate*.

También es posible interactuar con el editor de scripts a través del menú contextual accesible pulsando el botón derecho sobre el editor.

Opciones del editor

Además de las típicas opciones de un editor de texto, la sección de New Script tiene un botón que compilará todos los scripts para comprobar si existen errores de implementación. El proceso de compilación puede seguirse desde la consola de depuración.



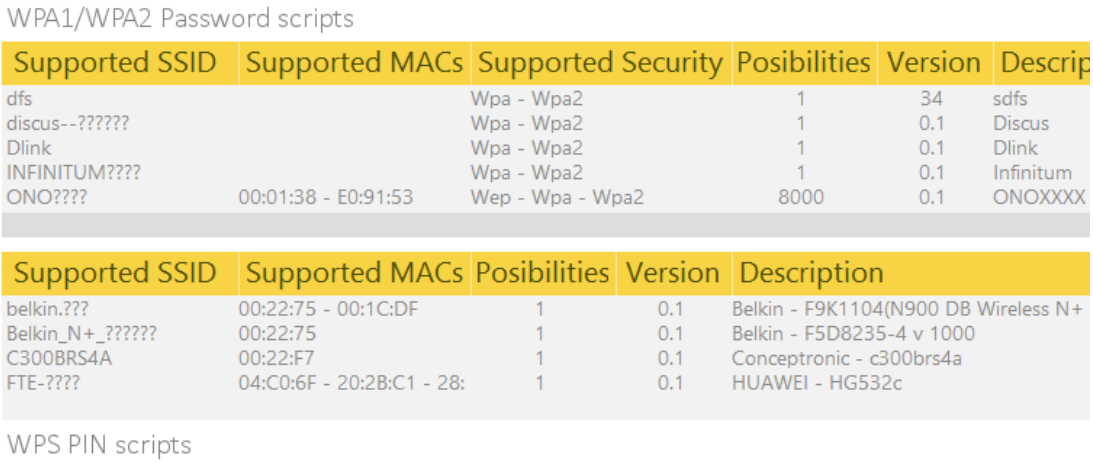
En la sección de prueba de scripts es posible especificar con que parámetros se van a probar dichos scripts para validar que están funcionando correctamente. Los campos referidos a los puntos de acceso, SSID, MAC y el tipo de protección que implementa, deben rellenarse para ejecutar la prueba. Es necesario especificar si se están probando contraseñas o Pin WPS. Por último, es necesario hacer clic en el botón *Test* para comenzar una nueva prueba.

Lista de scripts

En esta sección se muestra la lista de los scripts disponibles.

Los scripts utilizan una serie de algoritmos para generar contraseñas utilizadas en rúters WiFi comerciales.

Estos scripts se dividen en dos bloques diferentes, el primero, en la parte superior, para aquellos que generan contraseñas para WPA1 y WPA2, y el segundo, en la parte inferior, para aquellos que generan Pins para WPS.



Column	¿Qué información proporciona?
Supported SSID	SSIDs que coinciden con los criterios especificados en el script. '?' se usa como comodín de un carácter.
Supported MACs	Dirección MAC que coincide con los criterios especificados en el script.
Supported Security	Solo es necesario para scripts de WPA1 y WPA2, y especifica qué tipo de protección soporta el script.
Possibilities	Número de contraseñas posibles generadas por el script.
Version	Versión del script (Informativo)
Description	Descripción del script (Informativo)
Author	Autor del script (Informativo)
Filename	Nombre de fichero del script (Informativo)

También es posible interactuar con los scripts de la lista a través del menú contextual accesible al pulsar el botón derecho sobre uno de los scripts.