# Immunity SILICA User Guide

## Table of Contents

## Overview

SILICA is a wireless security vulnerability assessment and penetration tool. It simplifies the task of scanning your wireless networks and WiFi-enabled devices as it integrates a large number of WiFi specific attacks with a user friendly graphical interface.

Unlike traditional scanners that merely identify possible vulnerabilities, SILICA determines the true risk of a particular access point. SILICA does this by unobtrusively leveraging vulnerabilities and determining what assets behind the vulnerable access point can be compromised.

Additionally while traditional scanners can enumerate the vulnerabilities of a particular target, they cannot evaluate whether a mitigating control is in place on the target or in the surrounding environment. With SILICA's unique methodology it can report on whether a vulnerability can be successfully exploited.

Highly automated, SILICA has a one-button interface for many of the actions that a security professional will want to take during an assessment.

SILICA also implements threat detection modules that can passively scan for malicious attacks or unintentional vulnerabilities.

SILICA gathers and consolidates all information from its modules with a polished user interface designed to support a large amount of information without performance loss.

SILICA includes a large number of modules and individual exploits. In this manual, the main modules and exploits are documented, but there are other information sources that may also be referenced:

- SILICA demo videos: https://vimeo.com/album/3385057
- SILICA release notes: https://www.immunityinc.com/products/silica/releases.html
- SILICA support email silica@immunityinc.com

This user guide is available online in two formats:

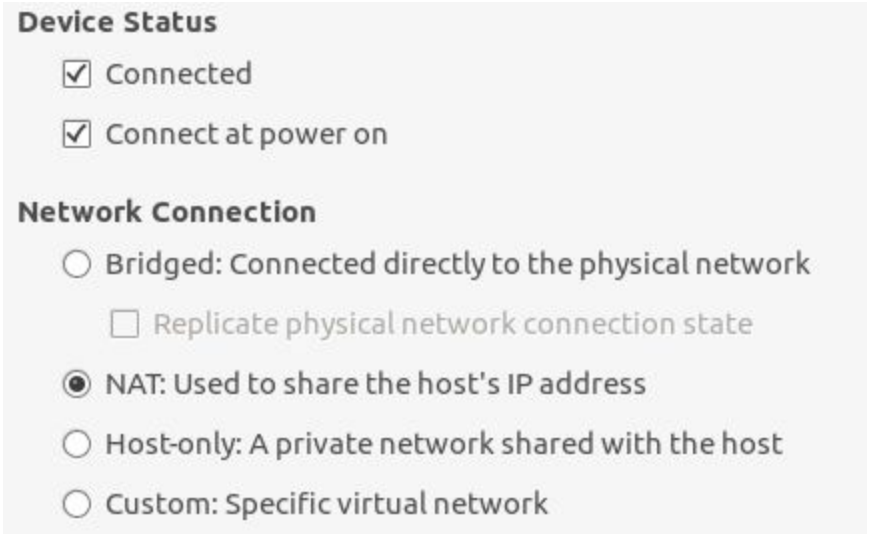
- https://www.immunityinc.com/products/silica/documentation.pdf
- https://www.immunityinc.com/products/silica/documentation.html

## Installation

SILICA runs inside a virtual machine. Each SILICA user will receive an email with their credentials and instructions on how to activate SILICA.

Notes:

- VMWare Workstation, VMWare Player or VMWare Fusion are required.
- SILICA comes with two wireless cards, however only one is required for regular SILICA use and activation. The additional wireless card is only required to perform the KRACK attack.
- For activation SILICA requires an Internet connection. Make sure you are online and the SILICA main Wireless card is plugged when you activate your account.
- Unless explicitly stated in the release notes, the virtual machine does not change for each SILICA release, so it is not necessary to download the virtual machine again to obtain the last version. Updates can be deployed by clicking the **UPDATE** button on the SILICA interface.
- **Troubleshooting:** By default, the virtual machine has a virtual interface set in bridge mode. On some networks, for example on networks with whitelisted MAC addresses or guest networks with captive portals, this would result in no Internet connection, and thus in SILICA not activating. The virtual interface mode can be changed to NAT in VMWare's **VM** > **Settings** submenu to resolve this issue.




*Virtual network interface mode to be used if bridge mode does not work.*

## Getting Started

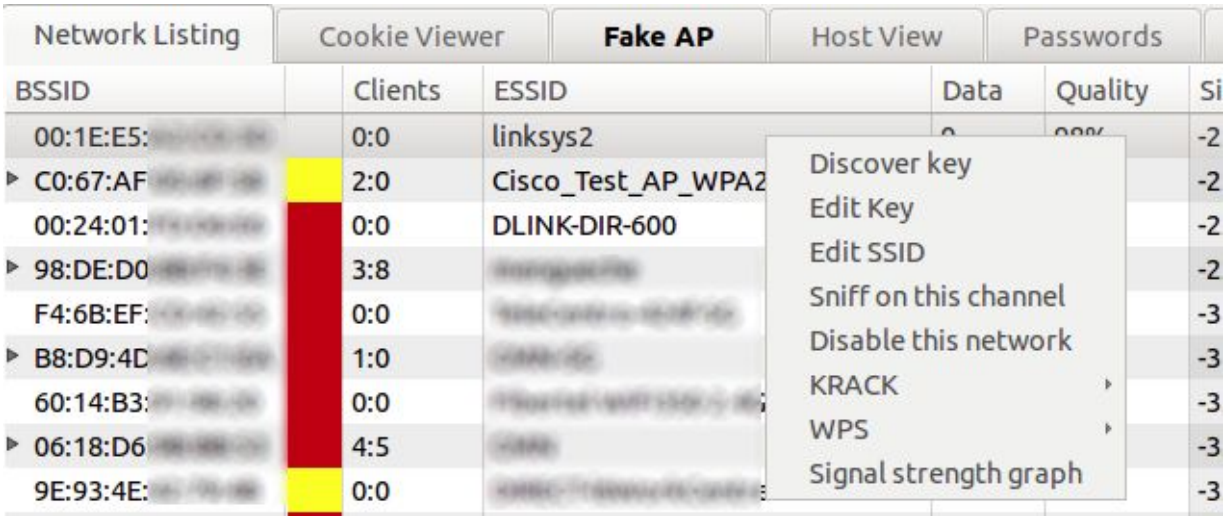
This chapter has a brief overview of the SILICA user interface and how to interact with it.

As soon as SILICA starts, it begins scanning for wireless devices by hopping through all the wireless channels. Detected access points are listed under the **Network Listing** tab.

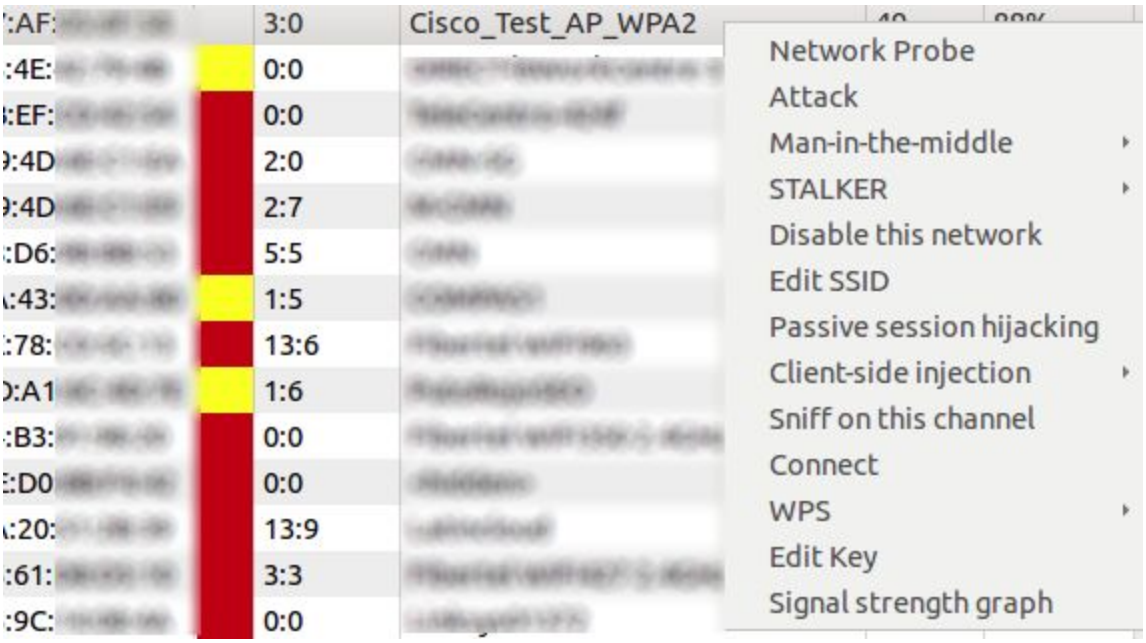
There are 4 top buttons that can be accessed from any tab. There are additional buttons on the bottom bar that are specific to the current tab.


*The **SCAN** button can be used to control whether to scan for wireless networks and devices.*

For each network entry, right-clicking shows a submenu with the available actions.




*The **Discover key** and **WPS** menu options launch the WEP/WPA attack and WPS attacks to try to obtain the preshared key for the WLAN.*




*When an access points pre-shared key is set in SILICA, a different set of modules options are available.*

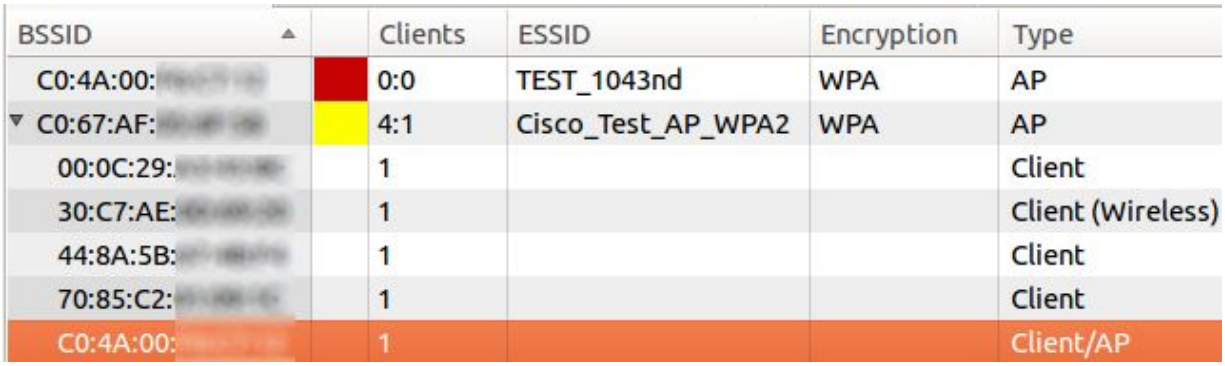
After a module is started, the **Log** tab will be updated to show its progress. A module can be stopped at any moment by clicking the **STOP** button.

## Network Listing Tab

Each row in the **Network Listing** Tab represents a Basic Service Set (BSS). A BSS can be formed by either infrastructure mode redistribution points, or by peer-to-peer ad hoc topology devices. The **Type** values for BSSs are “AP”, or “Ad-Hoc”. In this manual, we will refer to them as Access Points (AP) as that is the most common network architecture.

Each AP has a set of clients that can be seen by clicking the **Expand** button or by expanding the row entry. A client can be either a wired host connected to the network, or a wireless station. The **Type** values for clients are: “Client”, “Client(Wireless)”, or “Client/AP”.

- ***Client*** describes a device that is either a wired client, or a wireless station outside the detection range.
- ***Client(Wireless)*** describes a wireless station of the access point.
- ***Client/AP*** describes a MAC address that was both detected as joined to an access point and announced as an access point itself.



| BSSID | | Clients | ESSID | Encryption | Type |
|---|---|---|---|---|---|
| C0:4A:00: | | 0:0 | TEST_1043nd | WPA | AP |
| ▼ C0:67:AF: | | 4:1 | Cisco_Test_AP_WPA2 | WPA | AP |
| 00:0C:29: | | 1 | | | Client |
| 30:C7:AE: | | 1 | | | Client (Wireless) |
| 44:8A:5B: | | 1 | | | Client |
| 70:85:C2: | | 1 | | | Client |
| C0:4A:00: | | 1 | | | Client/AP |

*There are Two APs in this listing. The C0:4A:00... AP is also a client of the Cisco AP. The Cisco AP has 4 wired clients and only one wireless client.*

The network listing tab fields are:

| Field | Meaning |
|---|---|
| **BSSID** | BSSID of the AP. For clients, the MAC address of the device. |
| (Color code) | A measure of how interesting each AP is from a practical attacker point of view. The scale is red/yellow/green, with green being the most |

| | |
|---|---|
| | interesting.<br>The rules that SILICA follows are:<br><br>● Green: SILICA has the encryption key or it's vulnerable to the Pixie Dust attack.<br>● Yellow: WPS is available<br>● Red: SSID is hidden or signal less than 20%<br><br>Depending on the AP traffic colors may change. |
| **Clients** | Number of Wireless**:** Number of wired clients. |
| **ESSID** | The Service Set Identifier (SSID) for the network. This field may be hidden for some access points.<br>If a hidden SSID is revealed by sniffing a probe response or association request/response, the background of the cell will be in dark gray. |
| **Data** | Number of data packets sniffed. |
| **Quality** | A value in the 0-100 range derived from the Signal field |
| **Signal** | Signal-to-noise ratio of packets received from the access point as reported by the wireless card. |
| **Channel** | Wireless channel of the WLAN. |
| **Encryption** | Encryption type of the WLAN. (None, WPA, and WEP) |
| **Cipher** | Supported ciphers of the WLAN. (None, AES/CCMP, TKIP, WEP-40, and WEP-104) |
| **Type** | Type of entry. (AP, Ad-hoc, Client, Client(Wireless), and Client/AP) |
| **Auth** | Authentication types supported by the AP. (None, PSK, WPS, and 802.1X) |
| **Recovered Key** | Pre-shared key for the AP (None, the key, "Handshake captured", and "EAP")<br>Captured WPA handshake will be shown with an orange background |

| | |
|---|---|
| **WPS PIN** | WPS PIN recovered by a WPS attack. |
| **Last Seen** | Last time a packet from this AP was sniffed. Entry color will change to a lighter gray as time passes without this value being updated. |
| **Vendor** | Vendor of the AP derived from the BSSID's UI. |
| **Extended** | Extended information available for some CISCO APs |
| **WPS Info** | Additional AP information obtained from the WPS modules. |

The available module actions are:

| Menu option | Action |
|---|---|
| **Discover key** | Launch WEP or WPA attack. |
| **Edit key** | Set encryption key manually. |
| **Sniff on this channel** | Launch Wireshark sniffing in the channel of this AP. |
| **Disable this network** | Launch denial of service attack against stations connected to this AP, so they are disconnected from it. |
| **WPS** | WPS attack or information retrieval modules. |
| **Network Probe/Attack** | Connects to the WLAN and uses a reduced version of the CANVAS network exploitation platform to probe or attack the network. |
| **Man-in-the-middle** | Connects to the WLAN and uses ARP spoofing to establish a MITM network position. |
| **Client-side injection** | Connects to the WLAN and performs packet injection attacks. |
| **KRACK** | Performs a key reinstallation attack combined with an ssl-stripping and spoofing attack. |
| **Kr00k Attack** | Attacks a vulnerability on Broadcom chipsets that allows decrypting WPA traffic. |

| | |
|---|---|
| **Signal strength graph** | Plots a real-time graph of signal strength. |
| **Passive session hijacking** | Tries to capture HTTP cookies from stations connected to the WLAN. |
| **Deauthenticate this client** | This menu option is available only for stations. It will send deauthentication packets only to the selected station. |

## WEP/WPA Cracking Attacks

As long as SILICA is running, a background WPA handshake sniffer module will be storing the last captured WPA handshake for every AP to the file system in the */su/Reports/WPA_HANDSHAKES* folder. These handshake files, stored in .pcap format, can be used by external tools for cracking, or can be used from the **Key Recovery** tab.

Active or passive key recovery attacks can be launched from the **Discover Key** submenu on the **Network Listing** tab. When this option is selected for a WEP WLAN, an active WEP key recovery attack using ARP injection is launched. When this option is selected for a WPA WLAN, if a handshake was not yet captured, an active deauth attack will be launched until a handshake is obtained. Once the handshake is captured, offline dictionary cracking is started to recover the key. SILICA includes a one million wordlist dictionary. SILICA also supports WPA/WPA2 brute-forcing using PMKID data. This allows SILICA to attack some access points even when no stations (clients) are present.

## Key Reinstallation Attack (KRACK)

KRACK is a man-in-the-middle attack between a target access point and the target devices that try to connect to the network. When a vulnerable device tries to connect, SILICA will intercept the packets and replay them in a way that will cause the device to install an zeroed-out encryption key. SILICA will then proceed with ssl-stripping and ssl-spoofing attacks against the target device. The module supported targets are wpa_supplicant 2.4 and 2.5, and was tested on a stock Ubuntu 16.04.1 target.

To make the KRACK attack work, SILICA requires two wireless cards, as the fake access point needs to be on a different channel than the real Access Point. If SILICA is not able to initialize the second interface when starting the KRACK attack, an error message (in red in the log window) is displayed and the module stops.

For the attack to be successful, these conditions should hold:

- The target should be vulnerable to the zero-key attack (wpa_supplicant 2.4 and 2.5)
- The signal from SILICA's card should be stronger than the real AP from the target's point of view.
- The target should try to reconnect to the network (SILICA will not try to force the target to reconnect).

Video resource: https://vimeo.com/album/3385057/video/251369829

## Kr00k Attack

The Kr00k Attack exploits a vulnerability in some very common Broadcom chipsets that cause a

device to send zero-key encrypted data packets for a short period of time after a deauthentic ation packet is received. This module will send deauthentication packets to trigger the vulnerability, decrypt the packets, and display them on a wireshark window. The module supports attacking a single device, or all devices connected to an access point. The module uses an heuristic based on the timing and throughput of data packets from the target to be more effective. The heuristic parameters can be adjusted from the Preferences Panel. Note: Some Broadcom chipsets support a non-standard modulation scheme that the SILICA card does not support. It is possible that this module does not work when the target is connected to an Access Point that has some Broadcom chipsets and they are using this modulation scheme. This module was tested on a Raspberry Pi 3 target.

## EAP Relay Attack

When trying to connect to a network using 802.1X authentication, SILICA will launch an MSCHAP Relay Attack if the credentials are unknown. This attack will allow SILICA to join the network after a man-in-the-middle attack on a legitimate client device trying to join the network. Only the PEAP with MSCHAPv2 authentication protocol is supported for this attack.

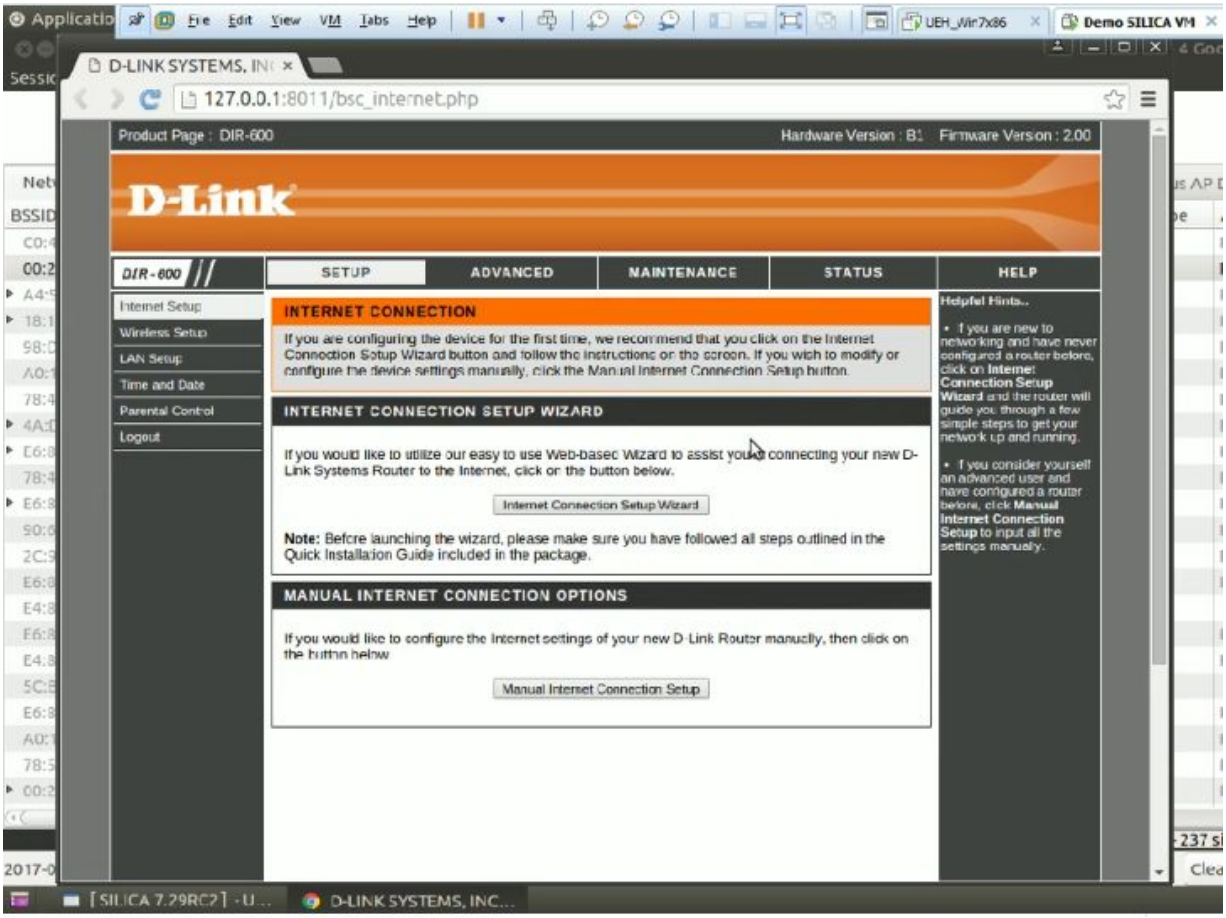
## Signal strength graphs

Real time signal-to-noise ratio graphs are available for both access points and stations. These can be used to better position your wireless card, or to try and find the location of a wireless device (a directional antenna could be of help in that case).


*Higher dots represent stronger signal. A color code is also used but not very visible here.*

## Attack Modules

A reduced version of the CANVAS network exploitation platform (https://www.immunityinc.com/products/canvas/index.html) to probe and attack the target WLAN is included with SILICA. In addition to a number of remote code execution exploits, authentication bypass exploits that try to access the administrative interface of the target access points are included as well.




*An access point administrative interface accessed using an authentication bypass exploit.*

## Post Exploitation Modules

After a remote code execution exploit is successful, post exploitation modules are run to gather information from the target:

- Screengrab: take a screenshot in the target host
- Get password hashes
- Get stored WiFi keys
- Get device information for Android devices
- Get system information

Results from these modules are stored in the Reports folder on the */su/Reports/default/<ip>* path, and also added to the **Attack Tree** tab.

## WPS Attacks

SILICA includes three WPS attack:

- WPS brute-forcing

- WPS default PINs by MAC address
- Offline brute-forcing (also known as Pixie Dust)

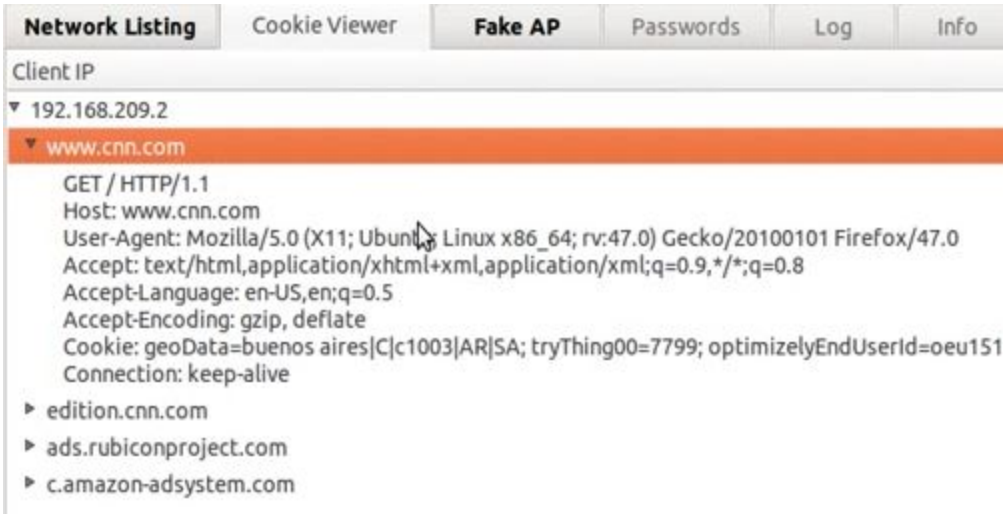
WPS brute-forcing is selected from the **WPS** > **Get WPS PIN (full bruteforce)** submenu. It will iterate over up to 11000 PINs. When successful, the WPS PIN and WPA shared key for the target are obtained. SILICA supports resuming an interrupted bruteforce attack against a target. NOTE: Many access points do not handle large numbers of WPS authentication events well, either as a protection or as a result of bugs, so in those cases this attack will most likely fail.

WPS default PINs are tested by either **WPS** > **Get WPS PIN (full bruteforce)** or **WPS** > **Get WPS PIN (try only default pins)**. Certains access points are known to have PINs that can be derived from their BSSID, and SILICA will try these first.

Offline WPS PIN brute-forcing, also known as the Pixie Dust attack, is also attempted with any WPS attack. If successful, this attack will be very quick (less than one minute) as it does not need to try multiple PINs against the access point.

Video resource: https://vimeo.com/album/3385057/video/130883860

## Cookie Viewer Tab




*Cookie captured from a request to [http://www.cnn.com](http://www.cnn.com) from the 192.168.209.2 IP*

In this tab, captured HTTP requests will be added from different attack modules. HTTP requests that do not use cookies will not be stored. The **Send this request** submenu launches the ACCOMPLICE plugin for the request. ACCOMPLICE is a chrome plugin that uses the captured cookies to hijack the user's session.

## Fake AP Tab

While scanning, SILICA will sniff for probe requests to populate this table. Each row represents an SSID probed for by a wireless device. Custom SSIDs can also be manually added by filling the text box next to the "**Become custom AP**" button and clicking the button. By right-clicking a row, a variety of Fake AP attack modules can be launched using the row's ESSID and Channel as a parameter.

When running a Fake AP module, SILICA will accept connections from wireless devices trying to connect to the spoofed SSID. Network traffic from the devices (stations) will be monitored for cookies and credentials, and these are stored in the **Cookie Viewer**, **Attack Tree** and **Passwords** tabs.

| Menu option | Action |
|---|---|
| **Edit Encryption** | Sets encryption method and parameters of the Fake AP. When radius authentication mode is set, stations probably will not connect to the Fake AP, but challenge/responses will be logged for offline cracking in the **Passwords** and **Attack Tree** tabs. |
| **Edit Channel** | Set channel of the Fake AP. |
| **Become this network with client-side injection** | Starts the Fake AP. Inject exploits in the HTTP traffic of stations that connect to the Fake AP. |
| **Become this network with ssl-stripping and self-signed certificates** | Starts the Fake AP. Performs man-in-the-middle attacks between stations and the websites that they connect to in order to remove or spoof SSL connections. |
| **Become this network with service impersonation** | Starts the Fake AP. Creates fake services for popular internet services in order to capture credentials. Also launches the SMB proxy attack. |

The column meanings are the same as in **Network Listing** except for these:

| Field | Meaning |
|---|---|
| (Color code) | Common open WiFi SSIDs (guest, free, etc) are shown in green. Older probes or with lower signal strength are shown in red. |
| **Hostname** | Hostname from stations connected to the Fake AP. |
| **IP** | IP assigned to each station by the Fake AP. |
| **Count** | Number of sniffed probes for each station. |

Additional settings are available for the FakeAP:

| Menu option | Action |
|---|---|
| **Karma Mode** | Instead of impersonating one SSID, the FakeAP will respond to all probe requests, trying to get as many stations as possible to connect. |
| **Check for internet connectivity** | Check that SILICA can connect to the Internet before starting the Fake AP. |
| **Enable Transparent HTTP Proxy** | Intercepts HTTP and HTTPs connections. |
| **Filter SSIDs and MACs in karma mode** | Instead of responding to all probe requests, implement custom filters to limit which devices and SSIDs to target. |
| **Fake Captive Portal** | Redirect HTTP traffic from stations when they first connect to a fake captive portal that will accept any credential and log it to the **Passwords** and **Attack Tree** tabs. |

## Client-side Injection Attack

The client-side injection module is active when the Fake Ap is started by the **Become this network with client-side injection** submenu. HTTP traffic from stations is intercepted and a hidden iframe HTML tag inserted into the HTTP responses to the target browser. From this hidden iframe, a number of remote code execution client-side exploits are deployed. If any exploit is successful, the post-exploitation modules are run on the target.

## SSL Stripping and Spoofing attack

The SSL stripping and spoofing attack is active when the Fake AP is started by the **Become this network with ssl-stripping and self-signed certificates** submenu. HTTP traffic is intercepted and HTTP responses are modified on the fly to change any *https://* links to *http://*, as to prevent the victim browser from using TLS.

HTTP headers in HTTP responses are modified to make HTTP cookies expire in order to force the targets to re-authenticate. As in any Fake AP attack, HTTP requests are inspected for credentials (user names, passwords, tokens, etc).

The spoofed SSL certificate attack is implemented by intercepting traffic to the 443 (HTTP/SSL) port. Self-signed SSL certificates are used to intercept the traffic. If the target browser and the user accept the spoofed certificate, this module will forward requests and responses to the real server in order to inspect the HTTP traffic. Any captured cookies and credentials are logged to the corresponding tab.

Video resource: https://vimeo.com/122117823

## Service Impersonation Attack

This module is started with the **Become this network with service impersonation** submenu. This module works by intercepting part of the network traffic from the stations. DNS requests are inspected, and if they match certain predefined domain names or patterns, spoofed DNS responses with the SILICA IP are sent as responses. A number of fake service modules are run: DNS, POP, POPS, SMTP, SMTPS, IMAP, IMAPS, VPN, HTTP, and HTTPS. Fake HTTP and HTTPS for popular sites are included. Any credential sent to the fake services are stored in the **Passwords** tab.

This module also includes a spoofing vulnerability and two remote code execution exploits for Microsoft Windows. See release notes for details:
http://www.immunityinc.com/products/silica/release7.40.html (CVE-2020-0601)
https://www.immunityinc.com/products/silica/release7.22.html (MS15-011)
https://www.immunityinc.com/products/silica/release7.35.html (CVE-2017-11906)

This module also intercepts all SMB traffic using an unique SMB Proxy module. SMB requests for ".exe" files will be answered with a backdoor to achieve code execution. This works as long as mandatory SMB signing is not enabled on the target.

Video resource: https://vimeo.com/album/3385057/video/136964755

This module may be useful when SILICA does not have an Internet connection, as this is the only Fake AP attack that does not require one.

## Karma Attack

Instead of impersonating only one SSID, the FakeAP will respond to all probe requests , trying to get as many stations as possible to connect. This option is selected with the **Karma Mode (reply to all probes)** checkbox. This option is available for Fake AP with open or radius authentication.

The karma mode also invokes the attack known as "mana": build a per-mac view of the proximate network list, and respond to broadcast probes with direct responses for each proximate network list. This allows SILICA to attract more client devices than the standard karma attack.

When the karma option is set, another option is available: **Filter SSIDs and MACs in karma**, used to fine control what SSIDs and devices are targeted.

Video resource: https://vimeo.com/155393829


*Karma filter settings dialog. With these settings, any SSID except "Production_WLAN" will be spoofed, and any station except the two specified MACs will be able to connect.*

## Neighborhood Graph Visualization

This option gives a visualization of the related networks, Access Points, SSIDs, and client devices graph for a given wireless device. This graph can be useful, for example, for looking for rogue access points, or for figuring out how to attack an access point by attacking its stations.

## Fake Captive Portal Attack

When this option is set, HTTP traffic from each station is redirected to a fake sign-in page until the user introduces any credentials. Captured credentials are added to the **Passwords** tab. This option is available for Fake APs using the service impersonation module.

Video resource: https://vimeo.com/198045435


*Fake Captive Portal login page*

## Executable Replacement Attack

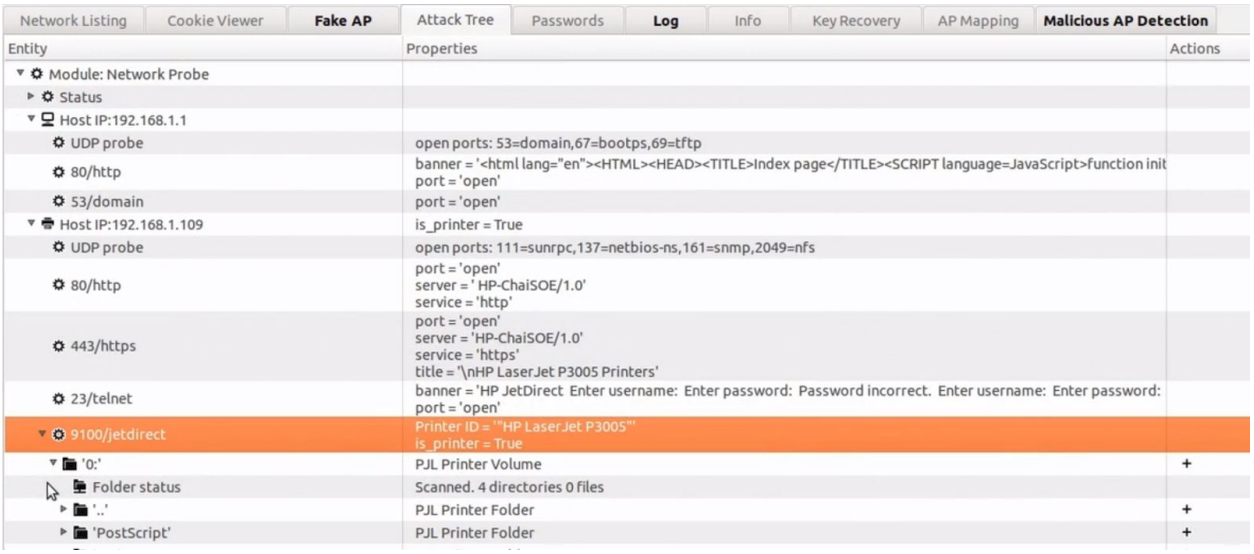
When the Fake AP is started with the **Enable Transparent HTTP Proxy** option set, requests from stations to files with an executable extension done over HTTP will be intercepted and the responses replaced with backdoors. This attack works for Windows, Linux and OSX targets.

## Apple EAP-success attack (CVE-2019-6203)

There is a vulnerability in same Apple devices that allows an attacker to create fake access points that successfully spoof real access points for those devices by sending EAP-success messages that the Apple devices accept even before validating credentials. SILICA will try to exploit the vulnerability when creating a FakeAP with 802.1X encryption.

## Attack Tree Tab

The attack tree shows scan and attack results in a centralized manner, grouped by network, attack type, and target. Entries are shown in a tree format. The first level are the network entries, the second level the attack type, the third level the target devices, and individual results are stored in further levels in a hierarchical manner. Entries can be folded or expanded to collapse the tree visualization. Some entries allow for additional actions to be performed by right-clicking on them. This is signaled by an icon on the **Actions** column.



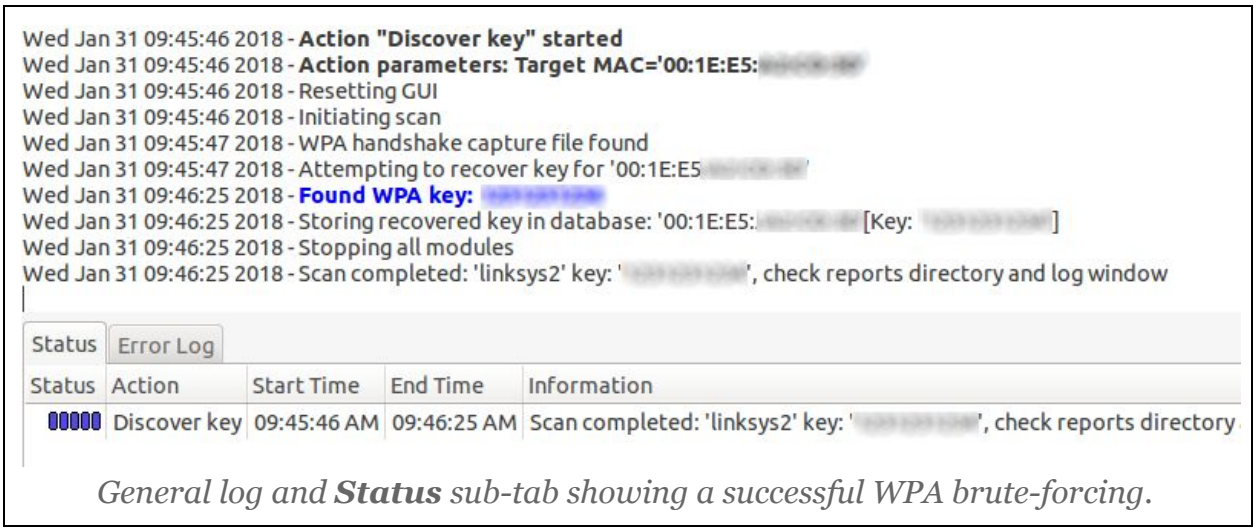

### Printer exploitation

When SILICA finds a network printer, it will add the PJL file system to the Attack Tree. By expanding the PJL entries, you can explore directories, download files, and exploit path traversal vulnerabilities in the printer's file system. This is done on demand and in real time, so SILICA should be connected to the printer's network for this feature to work.

## Log Tab

The general log can be seen in the Log tab. Information from all modules are added here. Successful attacks results are shown in blue. Error information is shown in the **Error Log** sub-tab.

The **Status** sub-tab has an overview of each module that was launched. When an action entry is clicked, the log is scrolled to the time the module was started, where action parameters for the module can be seen.




*General log and **Status** sub-tab showing a successful WPA brute-forcing.*

## Key Recovery Tab

This tab allows the user to launch offline brute forcing key recovery attacks.

| Control | Action |
|---|---|
| **Load wordlist file Button** | Selects the wordlist (also known as dictionary) used for the key recovery module. |
| **Load WPA Capture file Button** | Loads WPA handshake in .pcap format used for key recovery attack. |
| **Load PCL Capture file Button** | Loads VPN or WPA capture file in .pcl (SILICA Pickle) format used for key recovery attack. |
| **Recover Key Button** | Starts brute forcing key recovery module. |
| **Wordlist Generator Tab** | This tab can be used to generate custom wordlists with the specified parameters. |

# AP Mapping Tab

The AP Mapping feature is used to create wireless site surveys. This can be useful to detect rogue (unauthorized) access points. By combining spatial information with signal-to-noise data provided by the wireless card, SILICA unique algorithms are able to create high-resolution site survey mappings.

## Performing a site survey

Although it is not required, it is recommended to obtain a facility diagram and load it before starting the survey.

A capture path is the basic unit of a site survey. There is no limit on the number of capture paths that can be included in a site survey. A capture path is a continuous session of wireless signal capture combined with spatial information provided by the operator. When capturing a path, the capture channel can be set to a fixed value, or it can hop. If hopping, the survey session time should be longer as the quantity of information needed to survey several channels at once is larger.

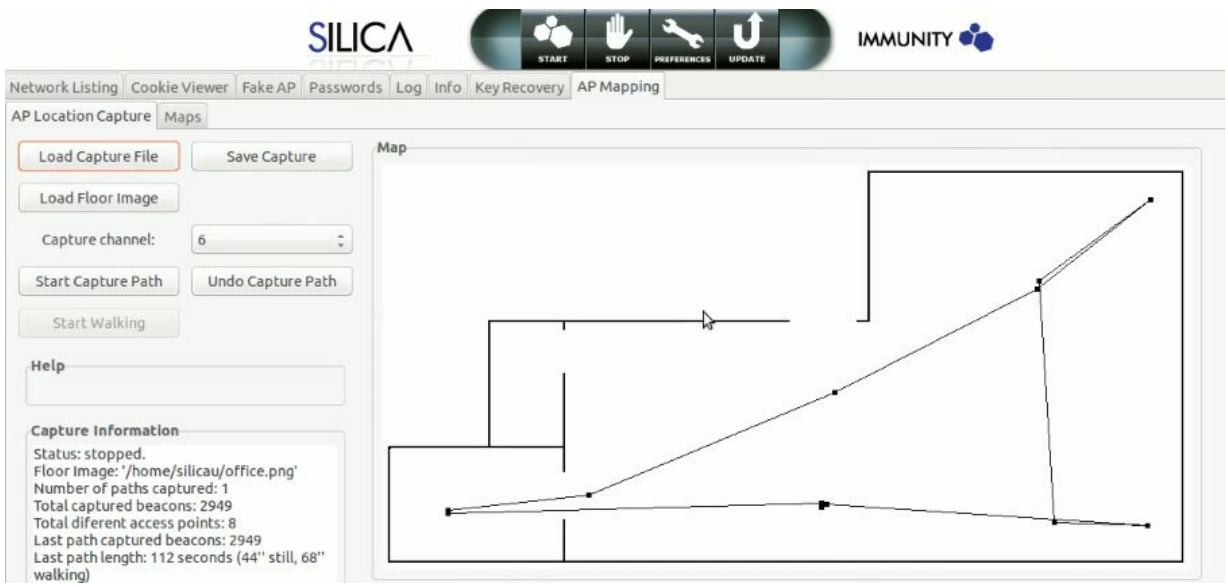
To obtain spatial information, the operator is asked to point to their location in the map, and to press specific buttons when walking, changing directions, or stopping. Walking when doing a capture path is not required, a capture path can consist of just the data captured during a period of time in a fixed position. To obtain a good result, a site survey should cover a certain portion of the map, especially along the facility perimeter.

Visualization maps are updated after every capture path recording. The captured data visualization can be used to validate that enough data is being captured. After the site survey is completed, the locations of known AP should match the position shown on the heatmap or zone visualization.

Video resource: https://vimeo.com/157178038

| Control | Action |
|---|---|
| **Load Capture File** | Loads a site survey from the file system. |
| **Save Capture** | Saves current site survey to file system. |
| **Load Floor Image** | Loads facility diagram. Supported image formats are: PNG, BMP, and TIFF. |
| **Capture channel** | Sets wireless channel used for capturing. A site survey using multiple channels needs to be proportionally longer to archive the same level of detail. |
| **Start Capture Path** | Start a capture path. Multiple capture paths |

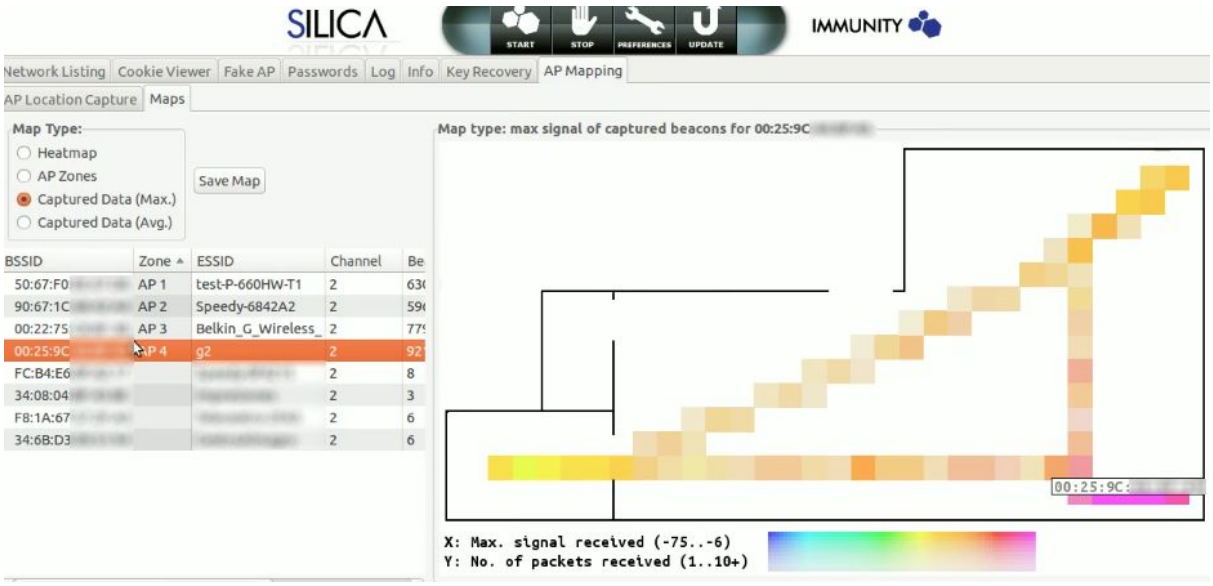
| | |
|---|---|
| | can be performed in the same site survey. The operator should follow the instructions shown in the Help box to provide the spatial information. The operator is first asked to click on the current position on the map after clicking this button. |
| **Stop Capture Path** | Finalizes capture path. |
| **Undo Capture Path** | Discards last recorded capture path from site survey. |
| **Start Walking** | With this button the operator informs SILICA that they are leaving the stationary position and that they can start moving in a linear path at a constant speed. The operator can click on the map each time they change velocity (direction or speed). A zero velocity is valid so they can click on the map when stopping instead of pressing the **Stop Walking** button. |
| **Stop Walking** | With this button the operator informs SILICA that they stopped moving. After clicking this button, SILICA will ask the operator to mark their current location on the map. |



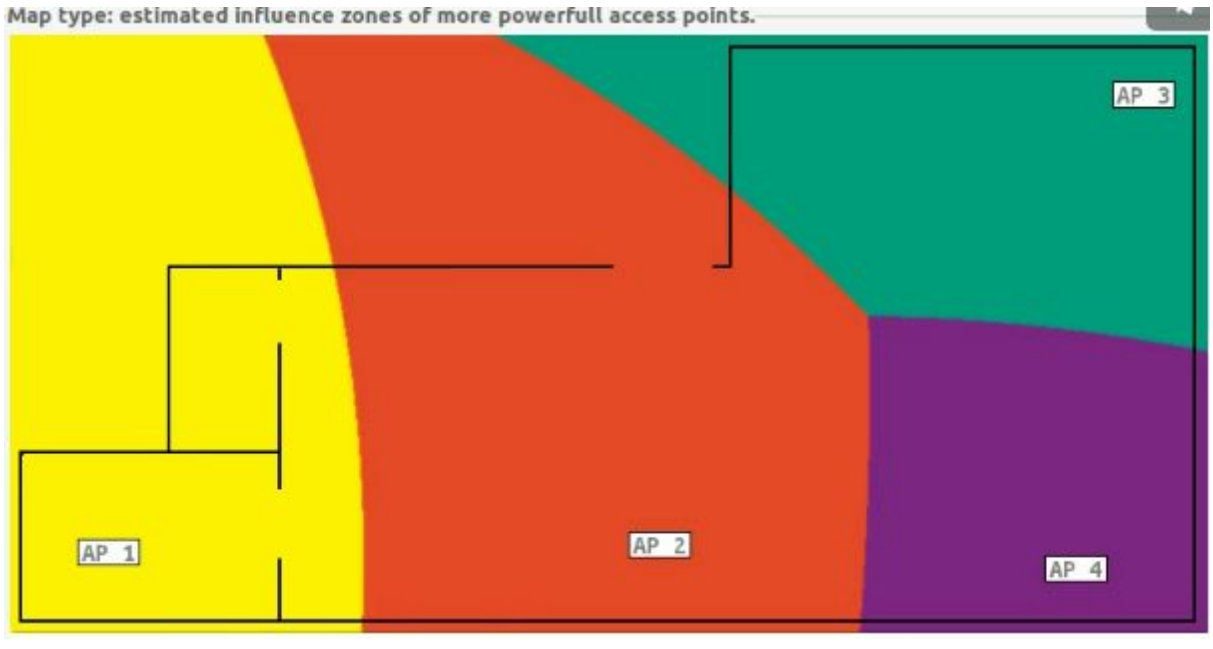

*Site survey with one capture path.*

## Site survey visualizations

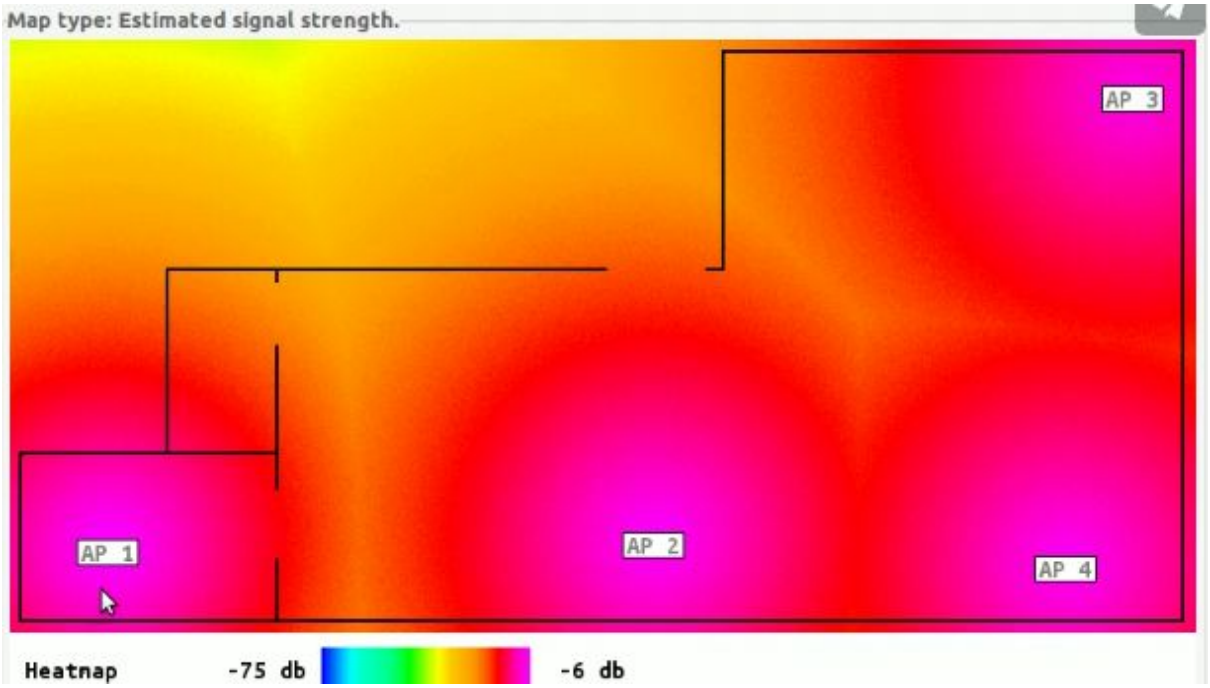
There are different visualization maps used to show site survey results.




*Captured Data (Max.) Visualization*




*AP Zones Visualization*

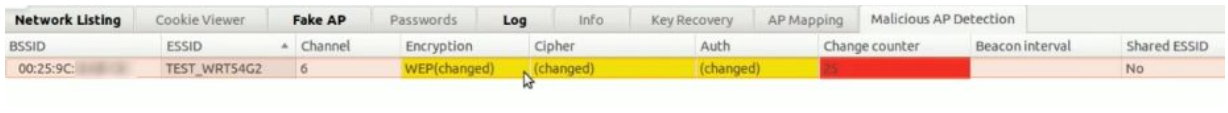



*Heatmap Visualization*

| Map type | Interpretation |
|---|---|
| **Heatmap** | Based on the estimated signal power of the access point that is most powerful in each location. It is also available for individual access points. Can be useful to locate rogue access points. |
| **AP Zones** | Based on the estimated zones of influence of the access points. We call the zone of influence the area where the signal from one access point is more powerful than from any other one. |
| **Captured Data** | The color coding of this visualization shows both the signal power and the number of captured beacons captured in each location for a given AP. This can be useful to validate that enough data was captured to generate an accurate site survey, and also to detect spatial location errors made when performing the site survey. |

## Malicious AP Detection Tab

SILICA analyzes captured beacons and probe responses looking for possible malicious access points. Any access point possibly spoofing a valid SSID will be added to this tab with the reason that the AP is suspicious. There is one entry for each unique BSSID/Channel pair.




*Suspicious access point showing a high number of changes.*

The color code is yellow for suspicious but probably benign configuration changes. Red is for known malicious or highly unexpected conditions.

There is one submenu, **Sniff beacons and probe responses for this BSSID**, that will launch Wireshark with a specific filter for inspecting the relevant packets.

There is an **Info** text box with additional information for each entry.

| Field | Meaning |
|---|---|
| **Change counter** | Number of changes detected on the AP configuration. High values could mean that an evil twin AP is present in the same channel sharing the same BSSID . |
| **Beacon interval** | APs regularly emit beacons. In case an irregular beacon interval is found, this may mean that an evil twin AP is present sharing the same BSSID. |
| **Shared ESSID** | Shared ESSID are common. More than one Access Point can have the same SSID when they are part of the same Extended Basic Service Set (ESS). |
| **Channel** | Same APs emit beacons in more than one channel, but multiple channels could also be a sign of a twin AP. |
| **ESSID** | Multiple changes in the ESSID are found in probe responses during a karma attack. |
| **BSSID** | SILICA will passively sniff for encrypted WPA traffic and try to decrypt it using an all-zero |

| | |
|---|---|
| | key. If the decryption succeeds, this is sign of an active KRACK or kr00k Attack, and the BSSID of decrypted packets will be shown in red. |

## Main Menu Options

| Menu option | Action |
|---|---|
| **Session** > **Open** | Loads session from file system. A session consists of all data displayed in SILICA tabs with certain exceptions like the **Log** tab information. The loaded information is merged into the current session. That means listed existing content is not purged before loading a session file. |
| **Session > Save** | Saves session to file system. Warning: in case an existing file is selected, it will be overwritten without prompting for confirmation. In addition to the session file, another file with the same name plus a .csv extension is written. This file can be loaded in a spreadsheet for exporting information. |
| **Filters** > **Open BSSIDs whitelist** | Loads a list of BSSIDs from a filter. Once a filter is loaded, only Access Points who are in the whitelist are shown in the Network Listing tab. The format of the file is a plain-text newline separated list of MAC addresses. |
| **Filters** > **Open BSSIDs blacklist** | Loads a list of BSSIDs from a filter. Once a filter is loaded, only Access Points who are not in the blacklist are shown in the Network Listing tabs. The format of the file is a plain-text newline separated list of MAC addresses. |
| **Filters** > **Reset MAC filter** | Disables active BSSIDs whitelist or blacklist. |
| **Filters** > **Open domain list** | Loads a newline separated domain filter list from the file system. Once a domain is loaded, only credentials directed to domains included in the filter are logged to the **Passwords** tab. Note that this filter will discard credentials without a domain field. |
| **Filters** > **Reset domain filter** | Disable domain filter list. |

## Preferences Dialog

The list of valid channels depends on the regulatory region setting for the wireless card. This setting can be changed from the **CARD** sub-tab.

The **Reports** sub-tab allows to choose which post-exploitation modules are run after an exploit obtains remote code execution on a target.

A custom channel hop list can be defined in the **Wireless** sub-tab. This list can be selected later via the bottom right button of the **Network Listing** sub-tab.

A static network configuration can be set in the **IP** sub-tab. This configuration is used instead of DHCP when joining a WLAN.

The WPS Start and End PIN can be set in the **WPS** sub-tab to limit the WPS bruteforce range.