Wi-Fi Scanning and Capturing: Day 1

As part of our deep dive, we'll engage in interactive, hands-on labs to learn about the key features of WiFi Explorer and Airtool, helping you build the skills to assess, analyze, and troubleshoot Wi-Fi networks.

For the best learning experience, please follow the instructor's directions and avoid starting labs early. Keeping pace as a group makes the session more effective for everyone.

Conventions

Unless specified otherwise, "WiFi Explorer" refers to either WiFi Explorer Pro 3 or WiFi Explorer Pro for Windows. The full name—WiFi Explorer Pro 3 or WiFi Explorer Pro for Windows—will be explicitly stated when a particular version is required. “Airtool” refers to Airtool 2.

Materials

If you haven't already, click the link below to download the ZIP file containing the necessary files for each lab. Save it locally, then extract the contents to access the materials as you progress through the labs.

https://www.intuitibits.com/downloads/resources/intuitibits-wlpc-phx-2026.zip

Hands-On Labs - Day 1

- Lab #1: Local Data Acquisition
- Lab #2: Data Acquisition Using Remote Sensors
- Lab #3: Data Import from Capture Files
- Lab #4: Data Import from Apple’s AirPort Utility
- Lab #5: Data Import from Analiti
- Lab #6: Built-in Columns
- Lab #7: Annotations
- Lab #8: Custom Columns

Lab #1 – Local Data Acquisition

In this lab, you will learn to scan for nearby wireless networks using your laptop's built-in Wi-Fi adapter while getting familiar with WiFi Explorer's user interface. You will also learn about some additional mechanisms to discover networks in the 6 GHz band.

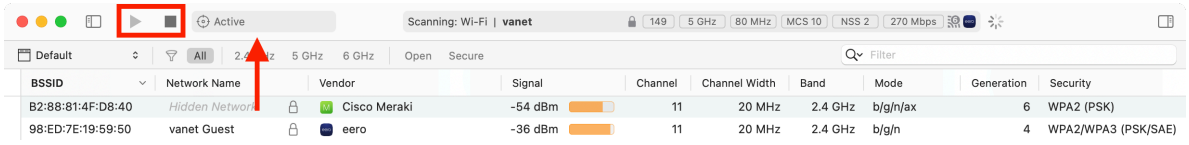
Wi-Fi networks can be discovered using **active** or **passive** scanning. WiFi Explorer Pro 3 supports both modes, while WiFi Explorer Pro for Windows is limited to *active scan mode*.

Scan for Networks Using Active Mode

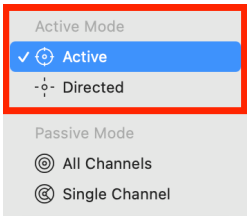
A client device typically uses active scanning to discover wireless networks quickly by broadcasting probe requests to all nearby APs. Any AP that receives a probe request responds with network information in a probe response. The client sequentially sends probe requests across all supported channels to discover nearby Wi-Fi networks.

To scan for networks using active mode in **WiFi Explorer Pro 3**:

1. Open WiFi Explorer Pro 3.
2. By default, WiFi Explorer Pro 3 automatically starts scanning for Wi-Fi networks using the built-in adapter in *Active* scan mode.
3. The *Play* and *Stop* buttons in the toolbar let you manually start and stop a scan, while the *scan mode selector* (indicated by the arrow in the screenshot below) provides a list of available scan modes. Switching to a different scan mode automatically starts a new scan.

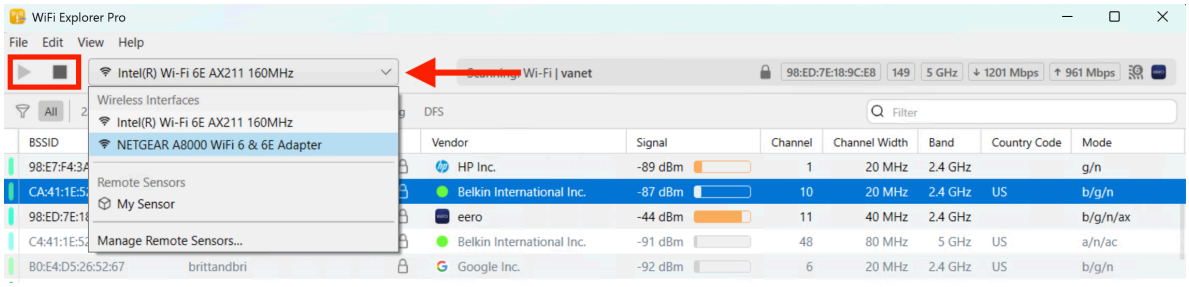


In WiFi Explorer Pro 3, there are two types of *active* scan modes: *Active* (default) and *Directed*. In *Active* mode, ***null*** *probe requests* are sent to discover all nearby networks. In *Directed* mode, ***directed*** *probe requests* are sent to discover only nearby networks matching a specific SSID.

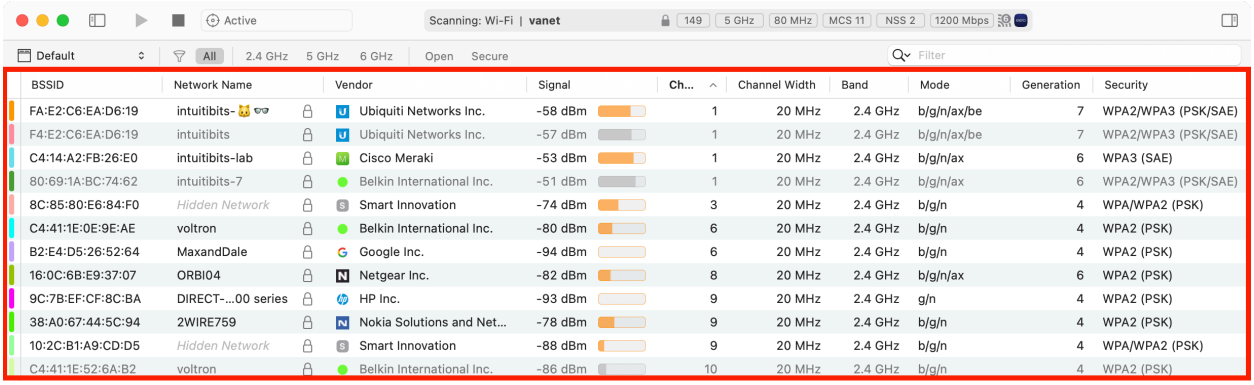


To scan for networks using active mode in **WiFi Explorer Pro for Windows**:

1. Open WiFi Explorer Pro for Windows.
2. WiFi Explorer Pro for Windows automatically starts scanning for Wi-Fi networks using the first available Wi-Fi adapter.
3. The *Play* and *Stop* buttons in the toolbar let you manually start and stop a scan, while the *scan mode selector* provides a list of available adapters. Switching to a different adapter automatically starts a new scan.



Scan results are continuously added to or updated in the networks table as WiFi Explorer periodically scans until manually stopped.



Scan for Networks Using Passive Mode

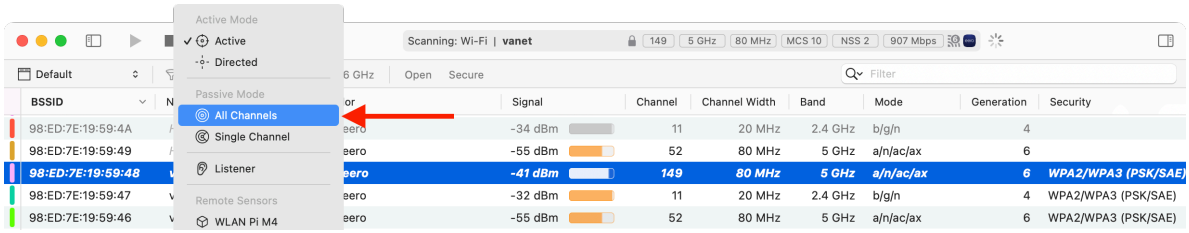
A client can also discover nearby Wi-Fi networks by passively listening for beacon frames broadcast by nearby APs. During passive scanning, WiFi Explorer Pro 3 switches the built-in Wi-Fi adapter from *managed* to *monitor mode* and captures beacon frames sequentially across all supported channels.

Scanning for networks using passive mode is not available on **WiFi Explorer Pro for Windows**.

Monitor mode *is a special mode for Wi-Fi adapters that allows them to capture all wireless traffic on a channel, regardless of whether the packets are addressed to the adapter. Unlike managed mode, where a Wi-Fi adapter connects to a specific network and only processes packets intended for it, monitor mode enables passive network analysis by capturing beacon frames, probe requests, and other management and control frames. All Mac models come with a built-in Wi-Fi adapter that supports monitor mode.*

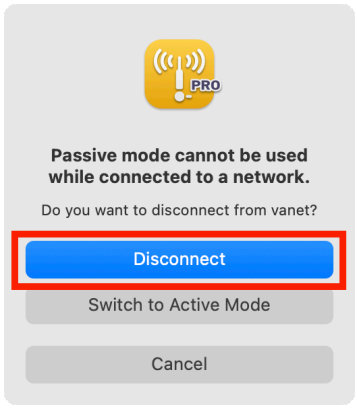
To scan for networks using passive mode in **WiFi Explorer Pro 3**:

1. Open WiFi Explorer Pro 3.
2. Click the *scan mode selector* in WiFi Explorer Pro 3's toolbar to reveal other scan modes, and select *All Channels*.

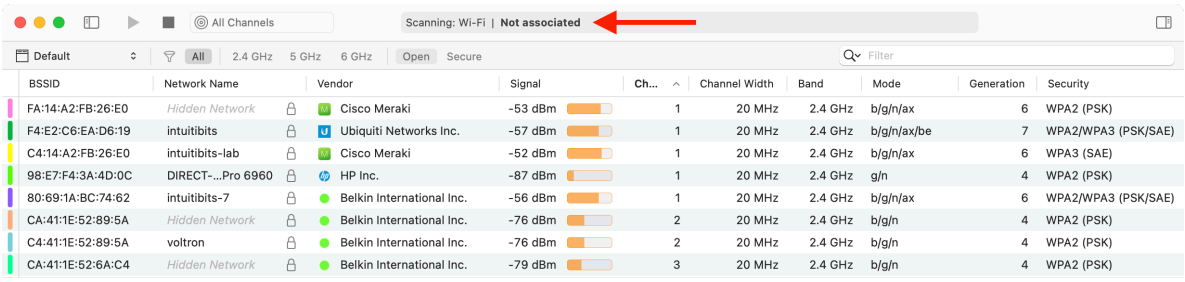


Passive scan mode is unavailable on Apple silicon Macs with an M1 chip.

3. Click *Disconnect* to continue.



4. WiFi Explorer Pro 3 disconnects from the network and switches the adapter to monitor mode, capturing beacons on each supported channel. As the scan progresses, results are continuously added to the networks table.



BSSID	Network Name	Vendor	Signal	Ch...	Channel Width	Band	Mode	Generation	Security
FA:14:A2:FB:26:E0	*Hidden Network*	Cisco Meraki	-53 dBm	1	20 MHz	2.4 GHz	b/g/n/ax	6	WPA2 (PSK)
F4:E2:C6:EA:D6:19	intuitibits	Ubiquiti Networks Inc.	-57 dBm	1	20 MHz	2.4 GHz	b/g/n/ax/be	7	WPA2/WPA3 (PSK/SAE)
C4:14:A2:FB:26:E0	intuitibits-lab	Cisco Meraki	-52 dBm	1	20 MHz	2.4 GHz	b/g/n/ax	6	WPA3 (SAE)
98:E7:F4:3A:4D:0C	DIRECT-...Pro 6960	HP Inc.	-87 dBm	1	20 MHz	2.4 GHz	g/n	4	WPA2 (PSK)
80:69:1A:BC:74:62	intuitibits-7	Belkin International Inc.	-56 dBm	1	20 MHz	2.4 GHz	b/g/n/ax	6	WPA2/WPA3 (PSK/SAE)
CA:41:1E:52:89:5A	*Hidden Network*	Belkin International Inc.	-76 dBm	2	20 MHz	2.4 GHz	b/g/n	4	WPA2 (PSK)
C4:41:1E:52:89:5A	voltron	Belkin International Inc.	-76 dBm	2	20 MHz	2.4 GHz	b/g/n	4	WPA2 (PSK)
CA:41:1E:52:6A:C4	*Hidden Network*	Belkin International Inc.	-79 dBm	3	20 MHz	2.4 GHz	b/g/n	4	WPA2 (PSK)

5. Stop the scan to return the adapter to managed mode. MacOS will attempt to reconnect to the network the Mac was connected to before the scan started, though you may need to rejoin manually in some cases.

6 GHz Discovery

The discovery of Wi-Fi networks on the 6 GHz band presents unique challenges due to the number of channels available. Several options are available to allow clients to discover 6 GHz BSSIDs. Two of the most often used are:

- Preferred Scanning Channels (PSC) (**in-band**)
- Reduced Neighbor Reports (**out-of-band**)

Preferred Scanning Channels (PSC)

Preferred Scanning Channels is a subset of 20 MHz channels prioritized within the 6 GHz WiFi band. In the US, PSC reduces the number of channels scanned on the 6 GHz band from 59 to 13. The list of PSCs is: 5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, and 229.

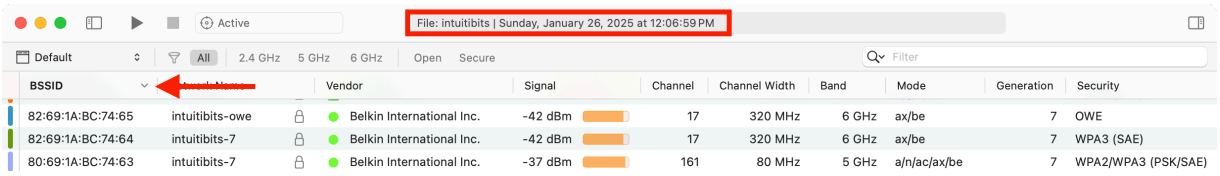
Reduced Neighbor Reports

Reduced Neighbor Reports are additional information elements added to beacon or probe response frames on the 2.4 and 5 GHz bands, indicating that an AP also supports one or more SSIDs on the 6 GHz channel. RNRs provide an out-of-band discovery mechanism for WLANs on the 6 GHz band.

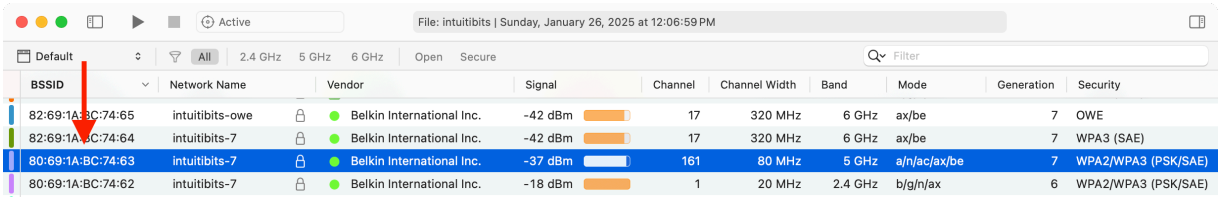
As an exercise, let's inspect RNRs in WiFi Explorer:

1. Launch WiFi Explorer.
2. Go to the *File* menu and select *Open*.
3. Navigate to the folder where you saved the deep dive supporting files, then choose the capture file **intuitibits.pcapng**.
4. Click *Open* to load the file.

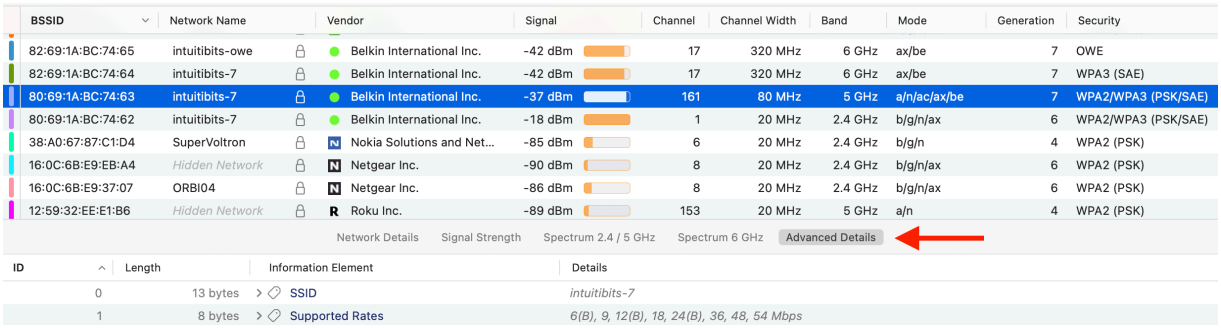
5. Click on the BSSID column's title to sort the results by BSSID and make it easier to find specific networks.



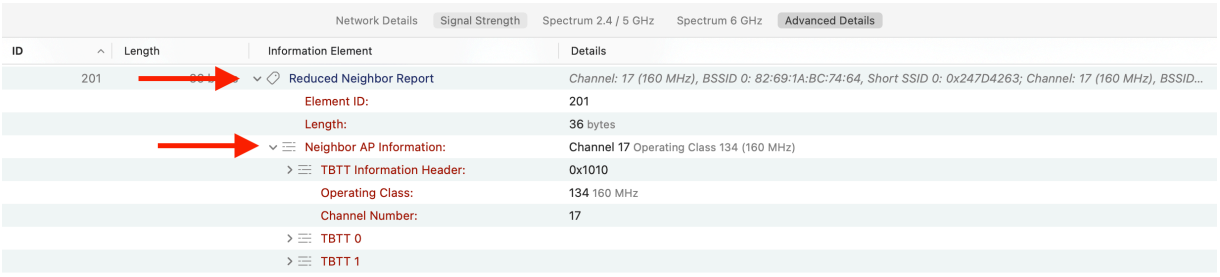
6. Select the network with BSSID **80:69:1A:BC:74:63**, and network name (SSID) *intuitibits-7*.



7. Navigate to the *Advanced Details* view.



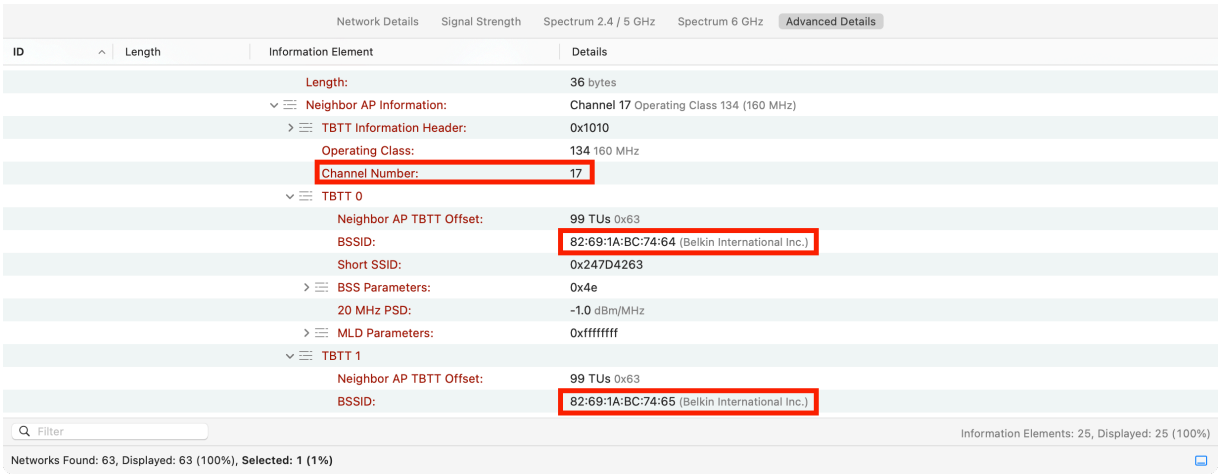
8. Expand the *Reduced Neighbor Report* information element and then the *Neighbor AP Information* field by clicking on the snap-open (**>**) control.



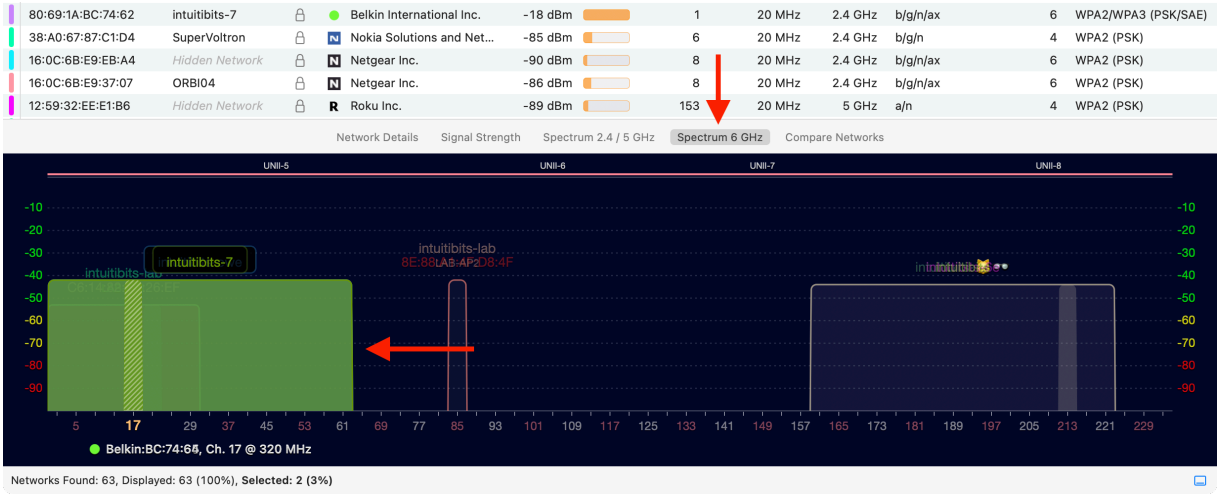
9. Expand the *TBTT 0* and *TBTT 1* fields.

As you can see, there are two BSSIDs on channel 17 (6 GHz):

- 82:69:1A:BC:74:64
- 82:69:1A:BC:74:65



These two BSSIDs on channel 17 are shown in the *Spectrum 6 GHz* view. Also, note that channel 17 (6 GHz) is not a PSC.



Conclusion

In this lab, you learned how to scan for nearby wireless networks using your laptop's built-in Wi-Fi adapter while becoming familiar with WiFi Explorer's user interface. You also explored additional in- and out-of-band mechanisms for discovering networks in the 6 GHz band, such as *Preferred Scanning Channels* and *Reduced Neighbor Reports*.

References

For detailed insights on scanning for nearby wireless networks using the built-in adapter in your laptop, see *Chapter 2: WLAN Scanning Theory* and *Chapter 3: Local Data Acquisition* in *WiFi Explorer Pro 3: The Definitive User Guide*.

< End of Lab >

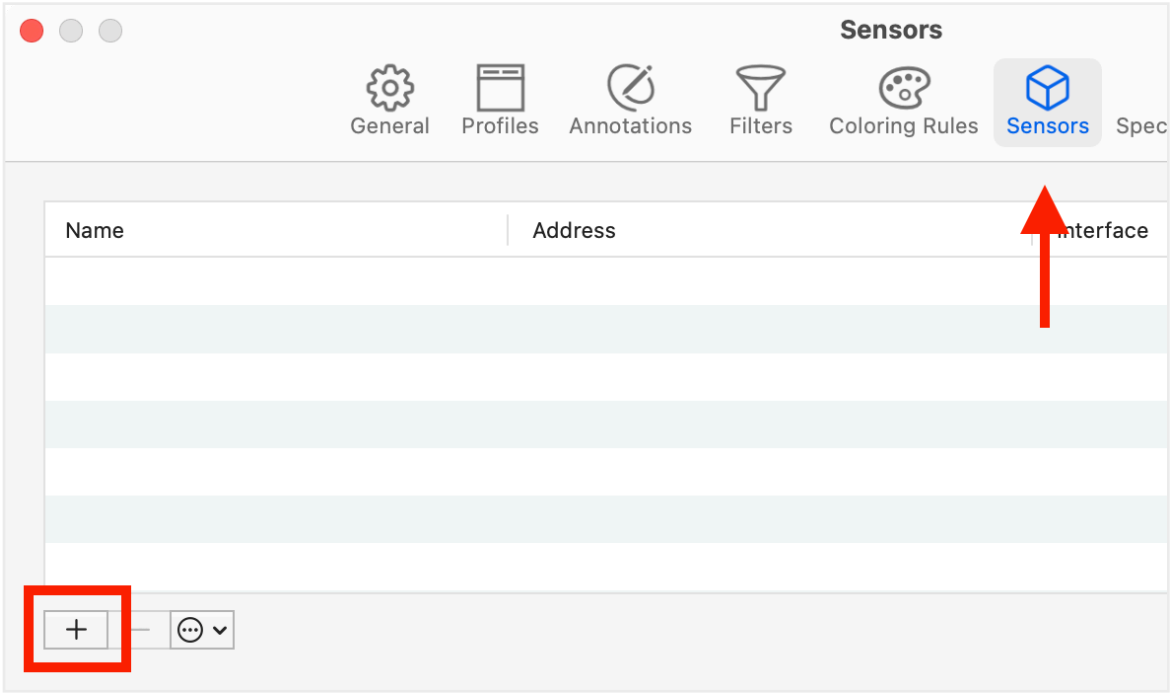
Lab #2 – Data Acquisition using Remote Sensors

In this lab, you will learn how WiFi Explorer uses remote sensors to scan for Wi-Fi networks. A remote sensor is a dedicated hardware device deployed for external or remote data collection, such as a WLAN Pi, a Raspberry Pi, or any existing Linux-based computer with wireless scanning capabilities. You will also learn how to run diagnostics on a sensor for troubleshooting purposes if needed.

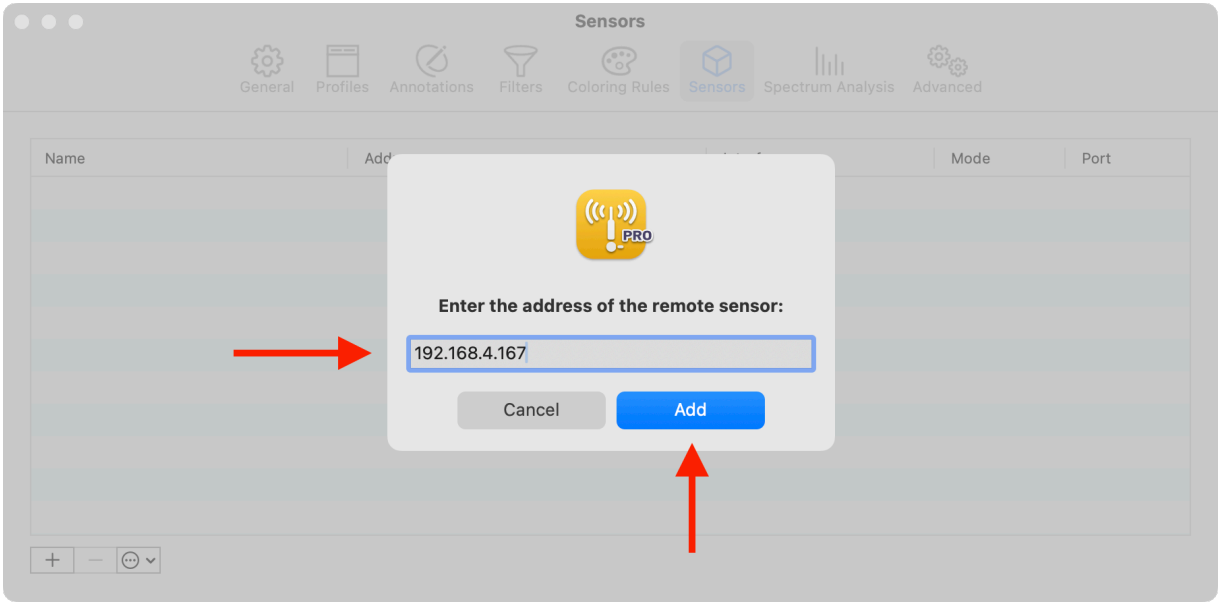
Add a New Remote Sensor

Before using a remote sensor, you must add it to the list of sensors in WiFi Explorer. Follow the steps below to add a new sensor:

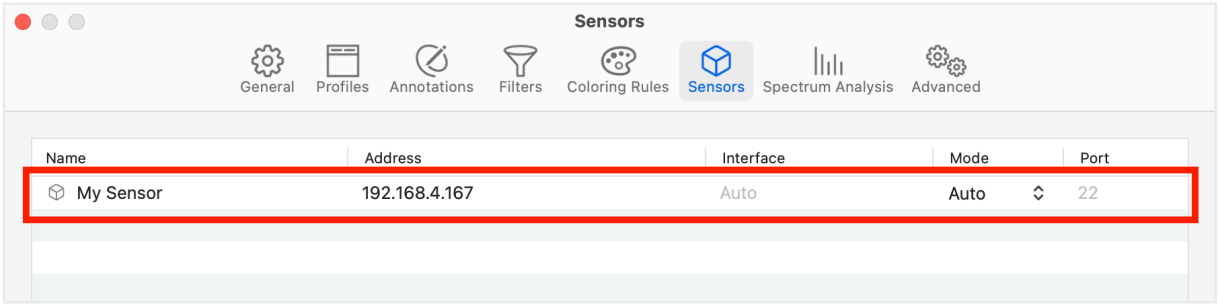
1. *Mac users*: open WiFi Explorer Pro 3, then go to *WiFi Explorer Pro 3* > *Settings* in the menu bar.
   Windows users: open WiFi Explorer Pro, then navigate to *File* > *Settings* in the menu.
2. In the *Settings* panel, go to the *Sensors* tab.



3. Click the "+" button to add a new sensor.
4. Enter the sensor's IP address and click *Add*.



5. Rename the sensor **My Sensor**, then press *Return (Enter* on Windows*)*.



Configure the Remote Sensor

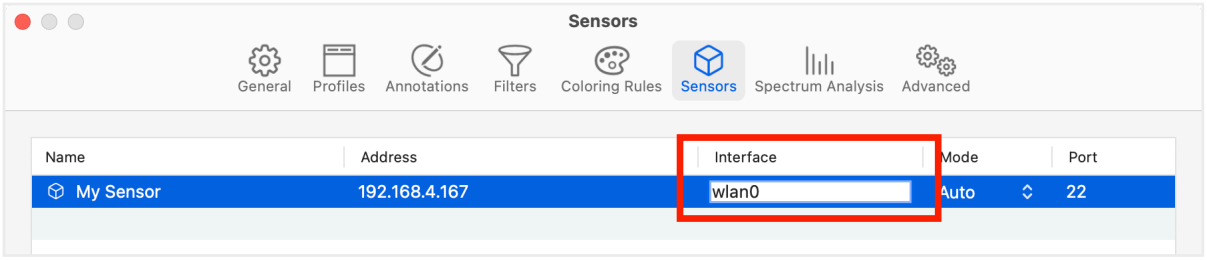
You may choose the WLAN interface and scan mode when scanning using a remote sensor. The "Interface" is set to *Auto* by default. When set to **Auto**, WiFi Explorer will choose the first available remote sensor's WLAN interface. The (Scan) "Mode" is also set to **Auto** by default. Other options are **Active** or **Passive**. When set to *Auto*, WiFi Explorer will use active scan mode if available. Otherwise, it will use passive mode.

As an exercise, we will configure the sensor's interface to be **wlan0** and the scan mode to be **Active**.

Configure the WLAN interface

Follow the steps below to configure the interface to be *wlan0*:

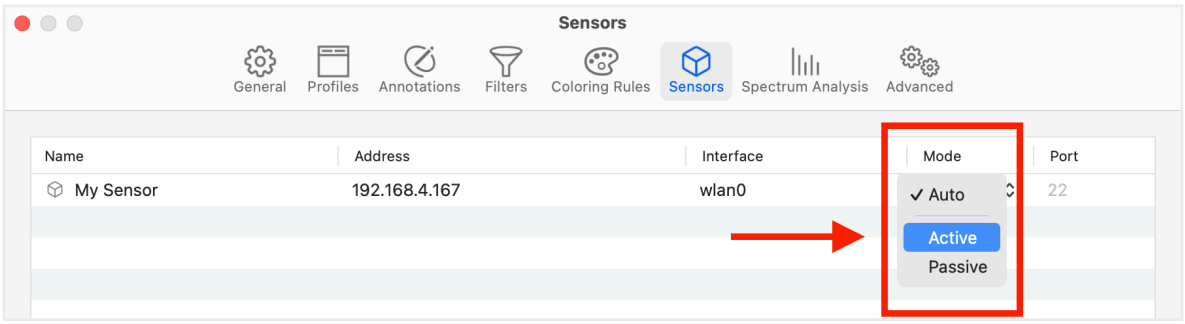
1. In the *Settings* panel, go to the *Sensors* tab and select the **My Sensor** sensor.
2. Double-click the field under the "Interface" column.
3. Enter **wlan0** as the interface, then press *Return* (*Enter* on Windows).



Configure the scan mode

Follow the steps below to use active scan mode:

1. In the *Settings* panel, go to the *Sensors* tab and select the **My Sensor** sensor.
2. Click the field under the "Mode" column and choose **Active** mode.

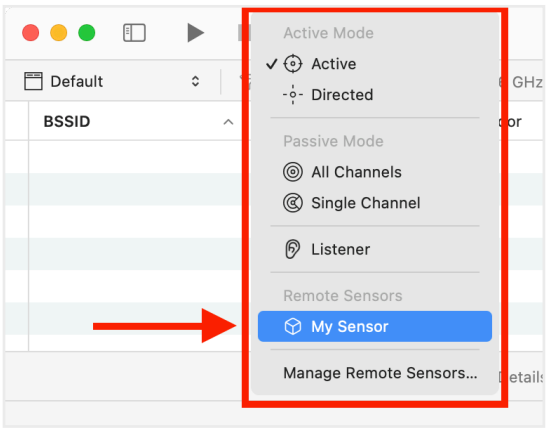


3. Close the *Settings* panel.

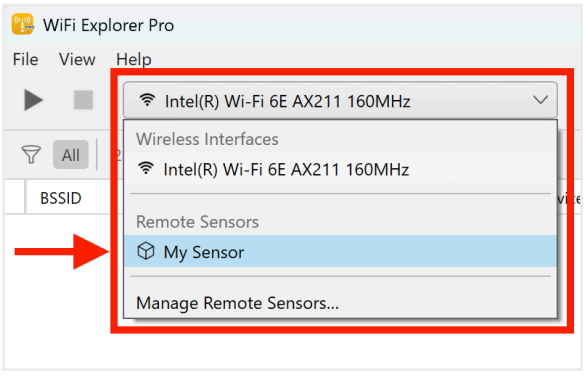
Use the Remote Sensor

Once added and configured, you can select the remote sensor for Wi-Fi scanning. Follow the steps below to start scanning using the **My Sensor** sensor:

1. In WiFi Explorer's toolbar, click the *Scan Mode* selector and choose the new remote sensor from the dropdown list, as shown in the screenshots for each platform below.

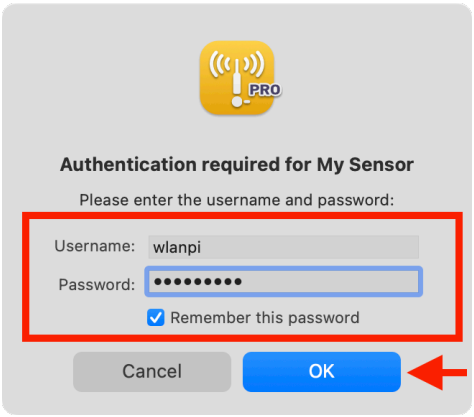


WiFi Explorer Pro 3



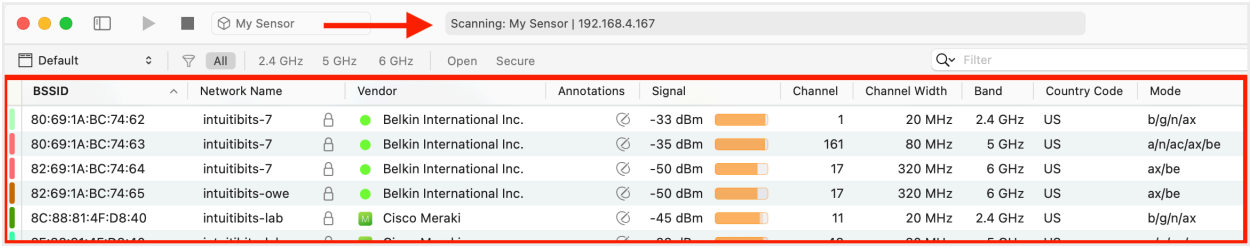
WiFi Explorer Pro for Windows

2. WiFi Explorer will connect to the sensor. If an error occurs, verify the sensor's IP address and try again.
3. When prompted, enter the sensor's username and password and click **OK**.



Select **Remember this password** to prevent being prompted each time you use the sensor.

4. After a few seconds, WiFi Explorer will display the scan results just as it does when performing local Wi-Fi network scans.



Remote Scans using Passive Mode

We previously configured the sensor to use active scan mode. Active scan mode uses *scandump,* a custom utility that enables active scanning on Linux-based devices in a way that produces all the necessary information required by WiFi Explorer, including pseudo-headers and information elements.

Remote sensors equipped with wireless adapters that support *Monitor* mode can also operate in passive scan mode. In passive scan mode, data is collected by listening to beacons on each supported Wi-Fi channel.

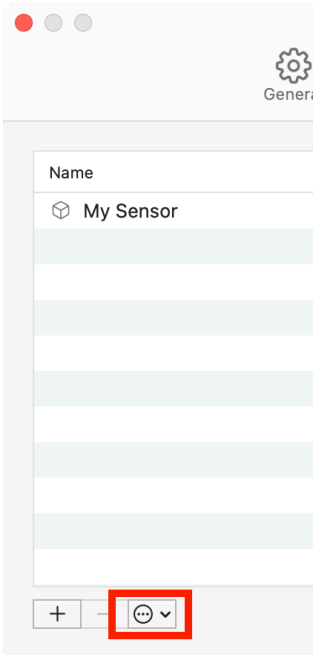
Let's change the sensor's configuration to use passive scan mode:

1. *Mac users*: open WiFi Explorer Pro 3, then go to *WiFi Explorer Pro 3* > *Settings* in the menu bar.
   Windows users: open WiFi Explorer Pro, then navigate to *File* > *Settings* in the menu.
2. In the *Settings* panel, go to the *Sensors* tab and select the **My Sensor** sensor.
3. Click the field under the "Mode" column, choose **Passive** mode, and close the *Settings* panel.
4. If the sensor is already scanning, WiFi Explorer will automatically restart the scan using passive mode. Otherwise, click the *Play* button in the toolbar to begin scanning.

Do you observe any differences?

Troubleshooting a Remote Sensor

If you experience issues when using a remote sensor, WiFi Explorer has diagnostic capabilities to help you identify the problem.

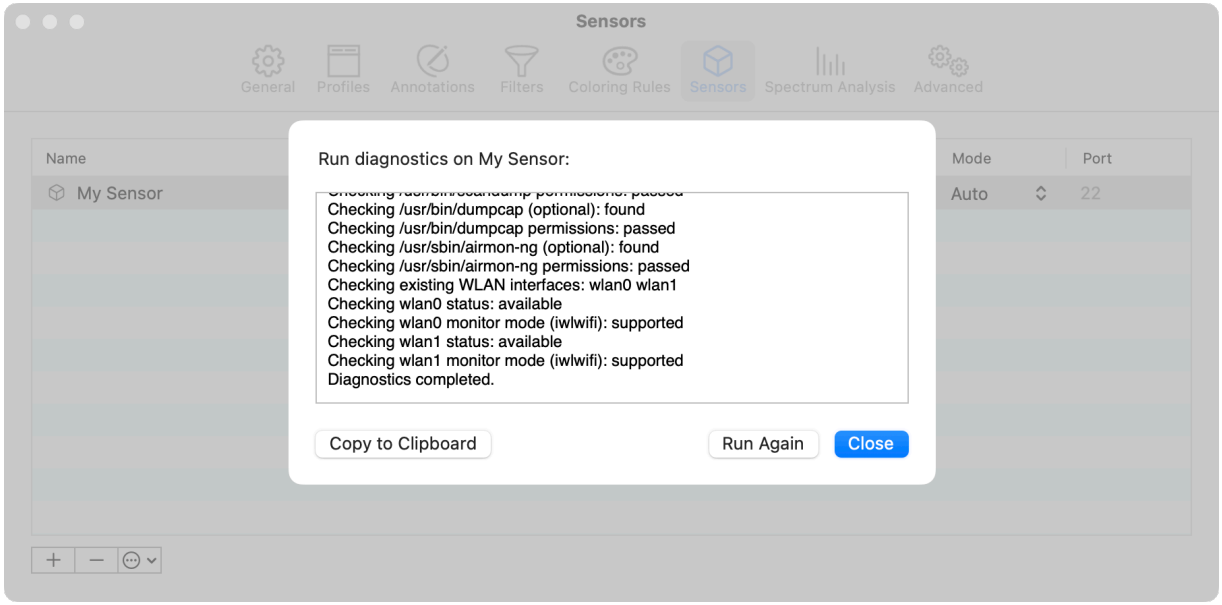


Follow the steps below to run diagnostics for the **My Sensor** sensor:

1. *Mac users*: open WiFi Explorer Pro 3, then go to *WiFi Explorer Pro 3* > *Settings* in the menu bar.
   Windows users: open WiFi Explorer Pro, then navigate to *File* > *Settings* in the menu.
2. In the *Settings* panel, go to the *Sensors* tab and select the

My Sensor sensor.

3. Click the *More* (three-dots) button at the bottom of the sensors list.
4. Choose *Run Diagnostics*.
5. WiFi Explorer will execute a series of tests to check network connectivity, availability of several software packages, and suitable Wi-Fi adapters.



6. Use the provided information to troubleshoot the issue, or click "Copy to Clipboard" to copy the output and email it to support@intuitibits.com for further assistance.

Conclusion

In this lab, you learned how WiFi Explorer uses remote sensors for Wi-Fi scanning. Remote sensors are Linux-based devices with wireless scanning capabilities for external or remote data acquisition. You also learned how to add, configure, and utilize a remote sensor with WiFi Explorer.

References

For detailed insights on remote sensors, see *Chapter 4: Data Acquisition Using Sensors* in *WiFi Explorer Pro 3: The Definitive User Guide*.

< End of Lab >

Lab #3 – Data Import from Capture Files

In this lab, you will learn to import scan data from a packet capture file containing Wi-Fi frames.

WiFi Explorer can import and decode capture files generated by various protocol analysis tools and capture utilities, including network devices (such as access points) and mobile device apps.

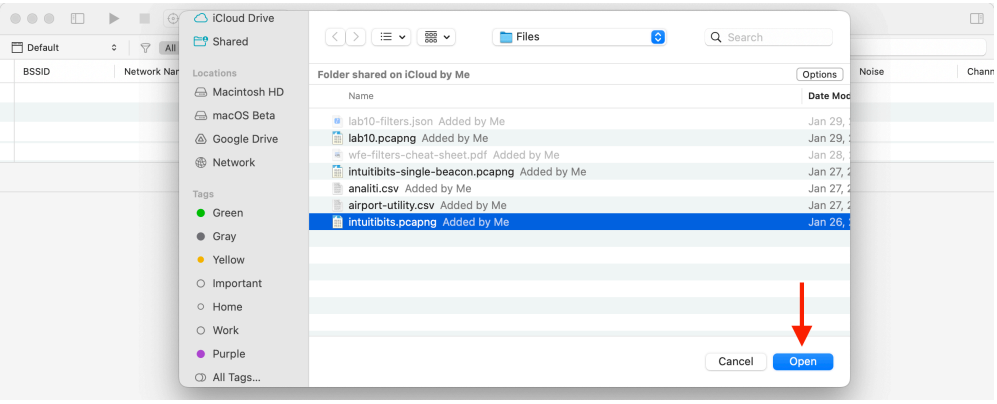
Capture files may include all frame types (management, control, and data frames). However, the networks table will be populated only with data decoded from beacons and probe response frames.

Import Scan Data from PCAP File

There are two types of PCAP files: PCAP and PcapNG. PcapNG is an evolution of the legacy PCAP format that includes several improvements, such as multiple interface support and metadata (capture application name, comments, etc.), extensible format, and higher resolution timestamps. WiFi Explorer can import both PCAP and PcapNG files.

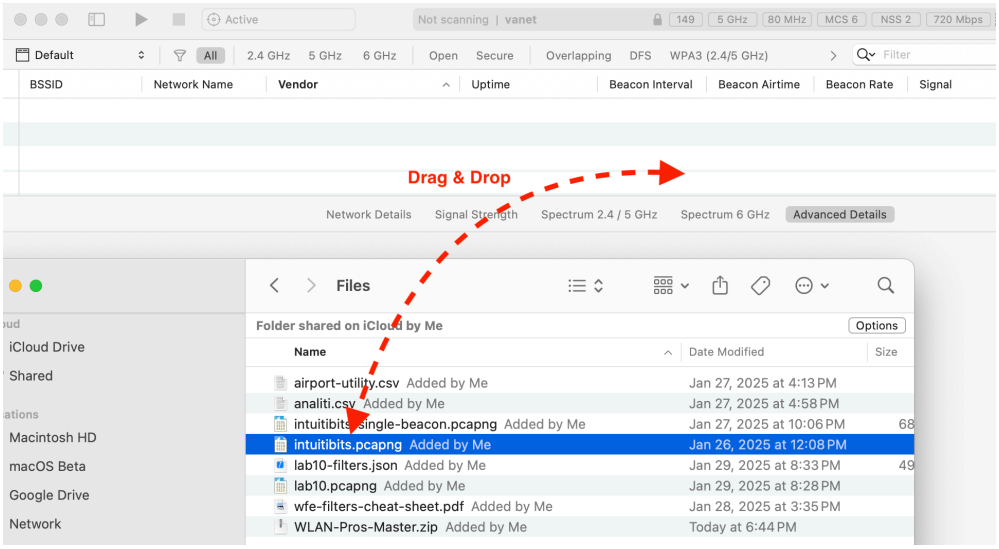
As an exercise, follow the steps below to import scan data from a capture file named **intuitibits.pcapng**:

1. Launch WiFi Explorer.
2. Go to the *File* menu and select *Open*.
3. Navigate to the folder where you saved the deep dive supporting files, then choose the capture file **intuitibits.pcapng**.
4. Click *Open* to load the file.

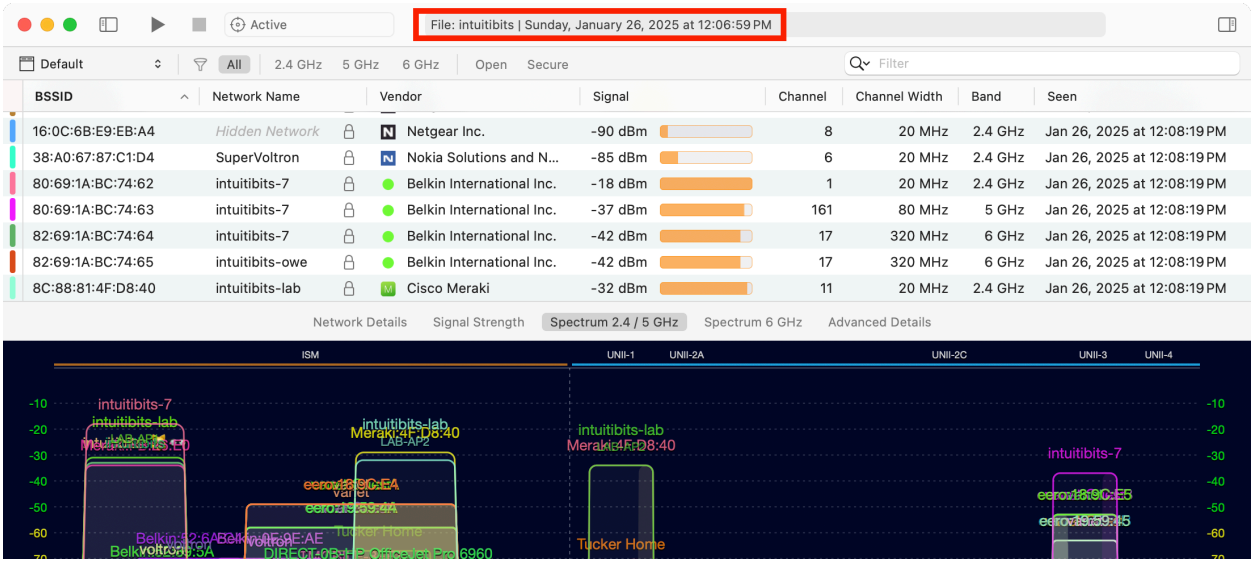


Alternatively:

1. Launch WiFi Explorer.
2. Open *Finder* (Mac) or *File Explorer* (Windows).
3. Navigate to the folder where you saved the deep dive supporting files, then select the capture file **intuitibits.pcapng**.
4. Drag & drop the file into WiFi Explorer's main window.



The screenshot below shows scan data decoded from the beacon and probe response frames found in the file **intuitibits.pcapng**.



Note that scan results are displayed for networks on multiple channels. Many capture utilities allow you to scan on a single channel only.

The capture file **intuitibits.pcapng** was generated using the *Capture on All Channels (2.4, 5, and 6 GHz)* option in *Airtool 2*. This feature enables *Airtool 2* to capture traffic using Mac's built-in Wi-Fi adapter across all supported channels by actively hopping between them.

Review Scan Data from a PCAP File

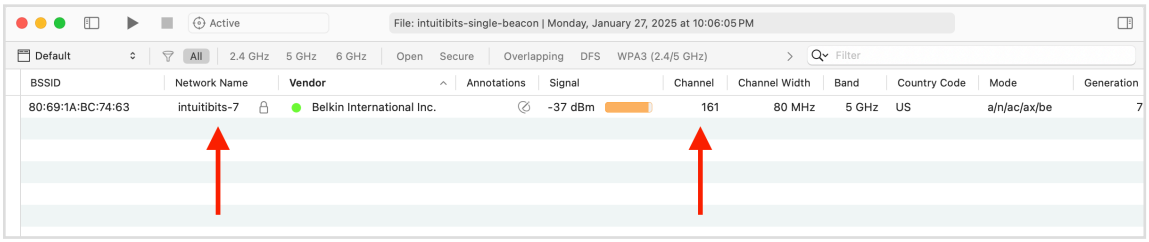
When WiFi Explorer imports a PCAP file, it extracts details from the pseudo-header (e.g., Radiotap), the beacon or probe response frame header, and the information elements within those frames.

As an exercise, let's compare the details of a network side by side in WiFi Explorer and Wireshark.

First, open the file **intuitibits-single-beacon.pcapng** in WiFi Explorer:

1. Launch WiFi Explorer.
2. Go to the *File* menu and select *Open*.
3. Navigate to the folder where you saved the deep dive supporting files, then choose the capture file **intuitibits-single-beacon.pcapng**.
4. Click *Open* to load the file.

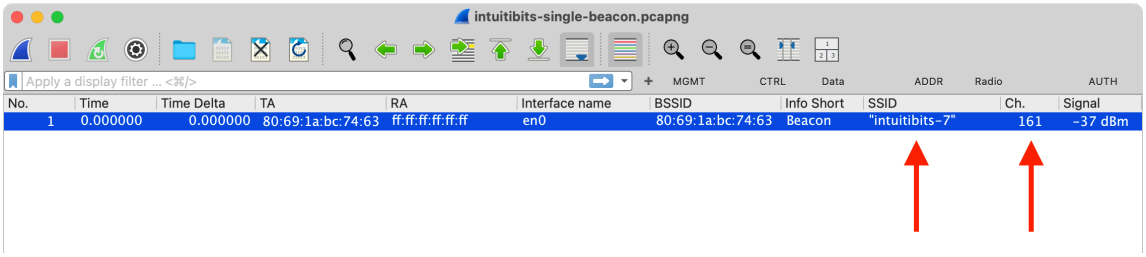
This file includes a single beacon from a Wi-Fi 7 network on channel 161 (5 GHz) with network name (SSID) *intuitibits-7*.



Second, open the same file in Wireshark:

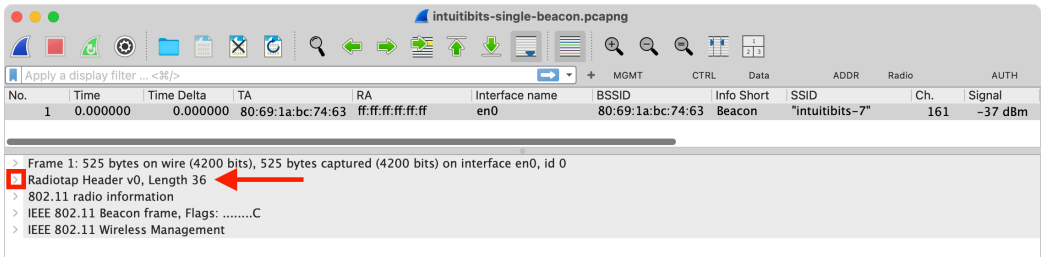
1. Launch Wireshark.
2. Go to the *File* menu and select *Open*.
3. Navigate to the folder where you saved the deep dive supporting files, then choose the capture file **intuitibits-single-beacon.pcapng**.

4. Click *Open* to load the file.

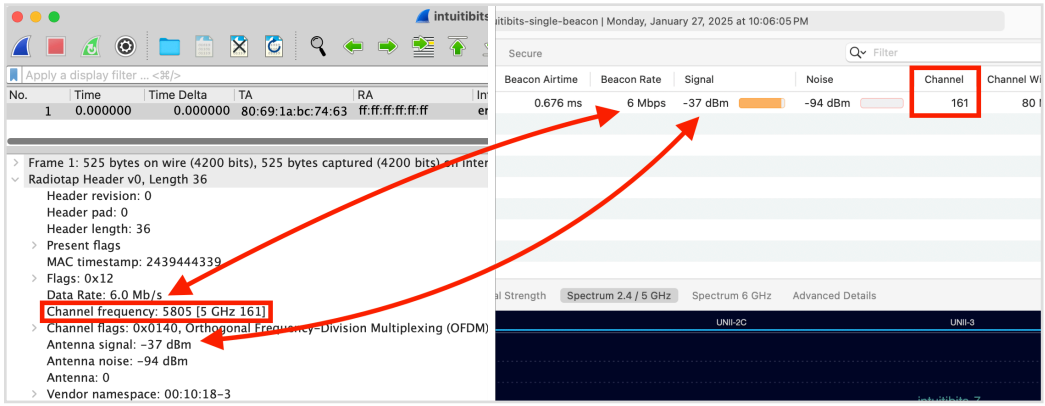


Third, follow the steps below to enable additional columns in WiFi Explorer and compare the details of the *intuitibits-7* network with those in Wireshark:

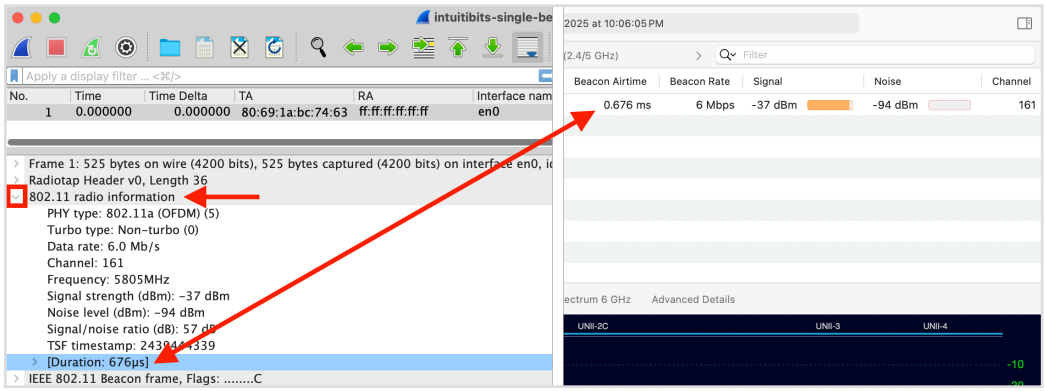
1. In WiFi Explorer, right-click anywhere on the networks table header and select the column *Beacon Rate*. Then repeat for the columns *Beacon Interval*, *Beacon Airtime,* and *Uptime*.
2. In Wireshark, select the frame and expand the *Radiotap Header* section by clicking the **>** button next to it.



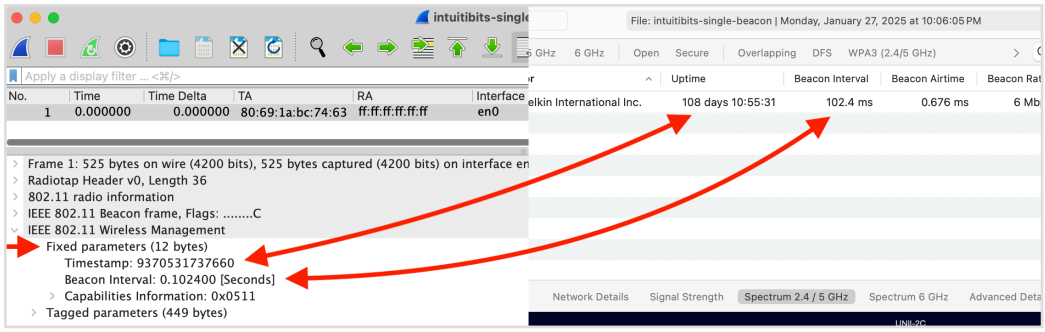
3. Compare the *Data Rate*, *Channel frequency*, and *Antenna signal* fields in the Radiotap header in Wireshark with the *Beacon Rate*, *Channel*, and *Signal* columns in WiFi Explorer, respectively.



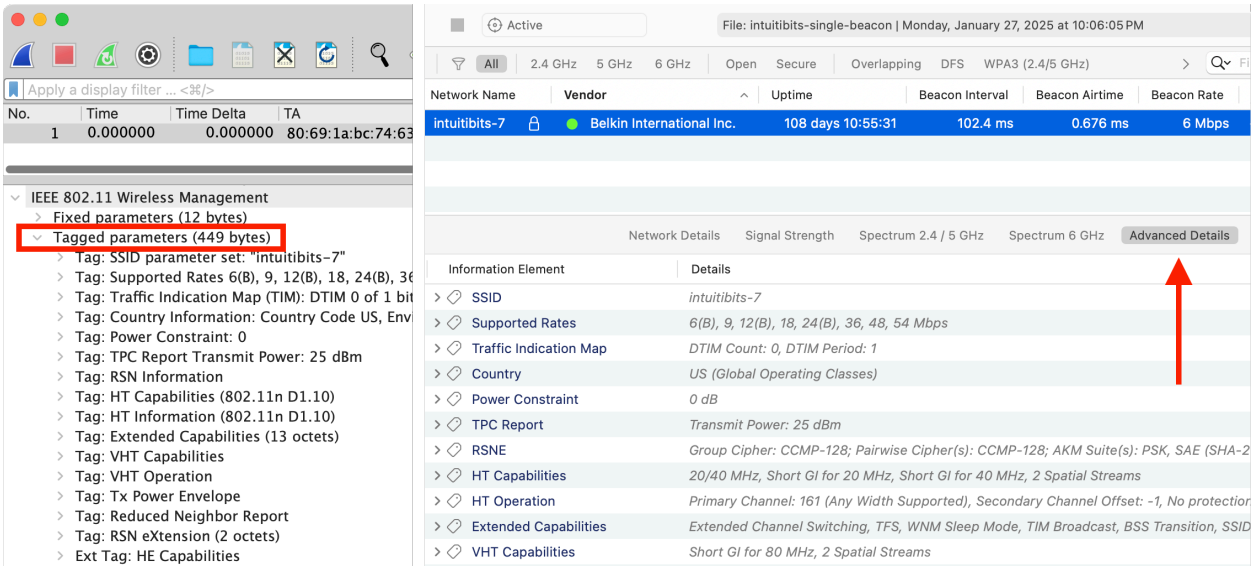
4. Expand the 802.11 radio information section in Wireshark and compare Wireshark's *Duration* field with WiFi Explorer's *Beacon Airtime* column. Note that the value of Wireshark's *Duration* field is in microseconds, while the value of the *Beacon Airtime* column is in milliseconds.



5. In Wireshark, expand the *IEEE 802.11 Wireless Management* section and then the *Fixed Parameters* section. WiFi Explorer uses the *Timestamp* field to estimate the access point's uptime. Also, compare the *Beacon Interval* field in Wireshark with the *Beacon Interval* column in WiFi Explorer. Note that the value of Wireshark's *Beacon Interval* field is in seconds, while the value of the *Beacon Interval* column is in milliseconds.



6. Finally, expand the *IEEE 802.11 Wireless Management* section.
7. Then, expand the *Tagged Parameters* section to view the beacon's information element data. In WiFi Explorer, you can quickly access the same information by selecting the network and navigating to the *Advanced Details* tab, as shown in the screenshot below.



Conclusion

In this lab, you learned how to import scan data from capture files. Additionally, you gained an understanding of the various fields in the Radiotap header and beacon fields that WiFi Explorer uses to extract network data.

Notes

- The data in the Radiotap header and the 802.11 radio information section in Wireshark are not transmitted with the frame. The adapter's driver provides the Radiotap header during the capture, while Wireshark generates the 802.11 radio information from various sources, including the Radiotap header.
- The Radiotap header is only available when capturing Wi-Fi traffic in *Monitor* mode. *Monitor* mode is a special mode for wireless network adapters to capture all wireless traffic on a specific channel, regardless of whether the traffic is addressed to the device itself.

References

For detailed insights on importing scan data from PCAP files, see *Chapter 5: Data Import from External Systems* in *WiFi Explorer Pro 3: The Definitive User Guide*.

< End of Lab >

Lab #4 – Data Import from Apple's AirPort Utility

In this lab, you will learn to import scan results from Apple's AirPort Utility, a legacy app initially designed to manage Apple's AirtPort base stations. Although the AirPort hardware was discontinued years ago, the app remains available for free on Apple's App Store. It includes a Wi-Fi scanning feature, and its network data can be exported in CSV format to be imported and displayed in WiFi Explorer.

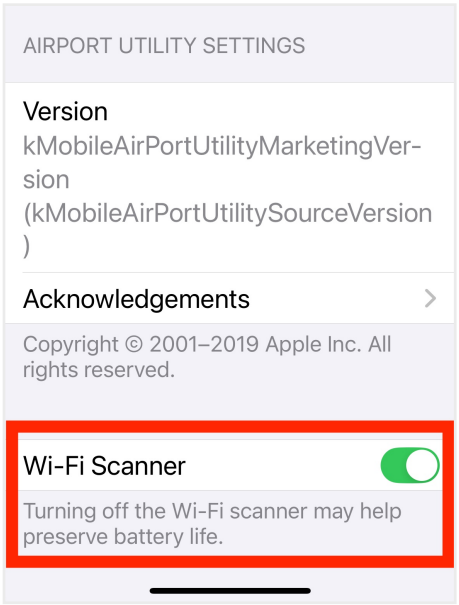
Import CSV Data from AirPort Utility (iOS)

If you don't have an iPhone or can't install AirPort Utility, go to *File > Open* in WiFi Explorer to open the provided sample file **airport-utility.csv**, then proceed to the **Review Scan Data from AirPort Utility** section later in this lab.

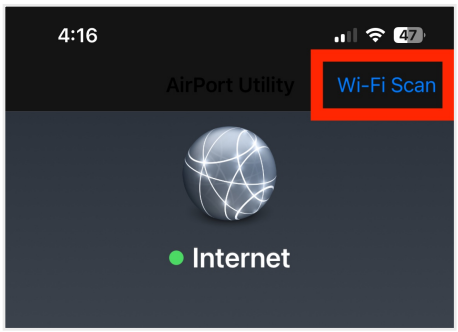
Configure AirPort Utility for Wi-Fi Scanning

(Skip if you have already installed and configured AirPort Utility for Wi-Fi scanning)
AirPort Utility doesn't expose the Wi-Fi scanning option by default, so enabling scanning for nearby networks requires the following configuration steps:

1. Download and install AirPort Utility from Apple's App Store.
2. Go to *Settings* on your iPhone, choose *Apps,* and scroll down to *AirPort Utility*.
3. Select *AirPort Utility* and enable the *Wi-Fi Scanner* option.



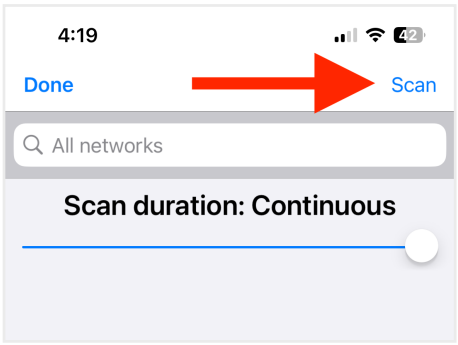
4. Open AirPort Utility and confirm that the *Wi-Fi Scan* option is now available. If the *Wi-Fi Scan* option doesn't appear, force quit the app and reopen it.

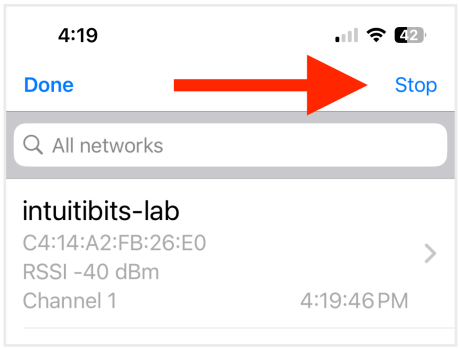


Import Scan Data from AirPort Utility

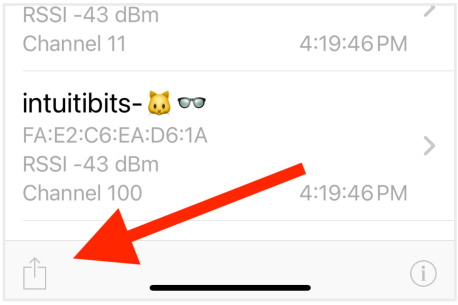
Follow the steps below to import scan data from AirPort Utility into WiFi Explorer:

1. Open AirPort Utility and tap the *Wi-Fi Scan* button.
2. Then, tap the *Scan* option within the scanning page and let it run for 30 seconds, then hit the *Stop* option.

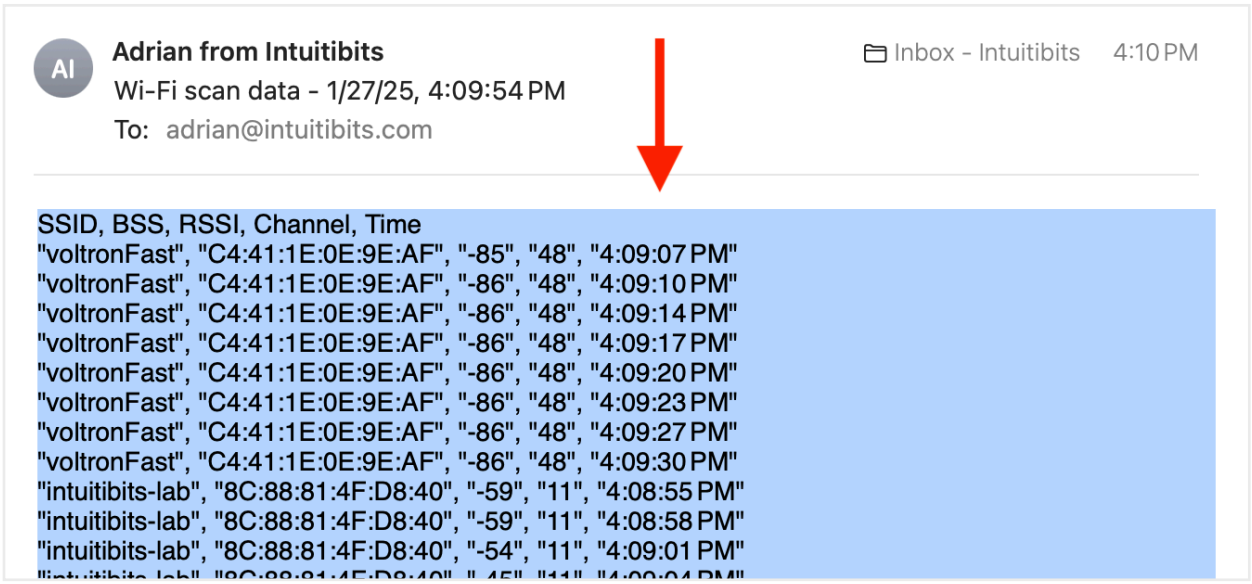




3. Once the scanner has stopped, email the results to yourself using the *Share* option in the bottom-left corner of the scanning page.



4. Open the email on the WiFi Explorer computer, select all the text in the email, and then copy it.



5. Switch to WiFi Explorer and click anywhere in the main window to make it the active window.
6. Paste the scan results using *Command+V (Control+V* on Windows*)*.

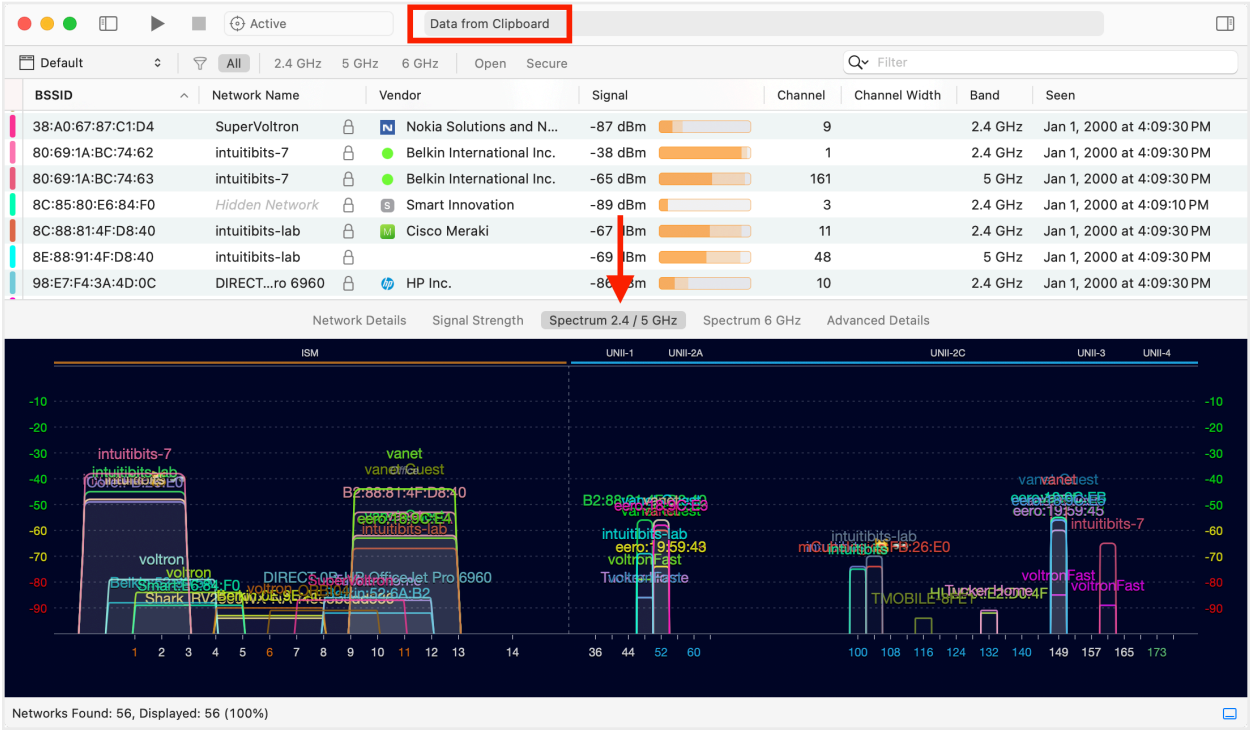
Alternatively, if you're using WiFi Explorer Pro 3, you may also import the scan results generated by AirPort Utility in two different ways:

- Using AirDrop:
    1. In AirPort Utility, tap the *Share* button and use *AirDrop* to transfer the results to your Mac.
    2. On your Mac, open *Finder*, locate the text file transferred via *AirDrop,* and drag it into WiFi Explorer.

- Using Apple's Universal Clipboard (Continuity / Handoff):
    1. In AirPort Utility, tap the *Share* button and choose *Copy*.
    2. Switch to WiFi Explorer and click anywhere in the main window to make it the active window.
    3. Paste the scan results using *Command+V*.

Review Scan Data from AirPort Utility

The screenshot below shows an example of scan results from AirPort Utility displayed in WiFi Explorer with the *Spectrum 2.4 / 5 GHz* view selected.



Note that values for the *Channel Width* and other columns are missing, as the data available from AirPort Utility is limited to SSID, BSSID, RSSI, channel, and timestamp. Other columns like *Vendor* and *Band* are derived from the BSSID and channel.

Although the fields available are limited, WiFi Explorer can still provide a valuable snapshot of the environment where the scan data was collected. The *Spectrum 2.4/5 GHz* is particularly helpful for quickly evaluating how channels are distributed or assigned across the different Wi-Fi networks in the area.

Conclusion

In this lab, you learned to import scan data from Apple's AirPort Utility (iOS) in CSV format to generate a valuable snapshot of the environment where the scan data was collected.

References

For detailed insights on importing data from CSV files, see *Chapter 5*: *Data Import from External Systems* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Notes

- CSV data does not include all the values usually available from information elements found in beacon and probe response frames. Therefore, it is recommended that scan data be collected in PCAP format when possible.
- When importing CSV data from AirPort Utility, the data displayed in the *Seen*, *Last Seen,* and *First Seen* columns defaults to 2000/01/01 as data details are missing from the CSV file. However, the times shown for each field are correct.

< End of Lab >

Lab #5 – Data Import from Analiti

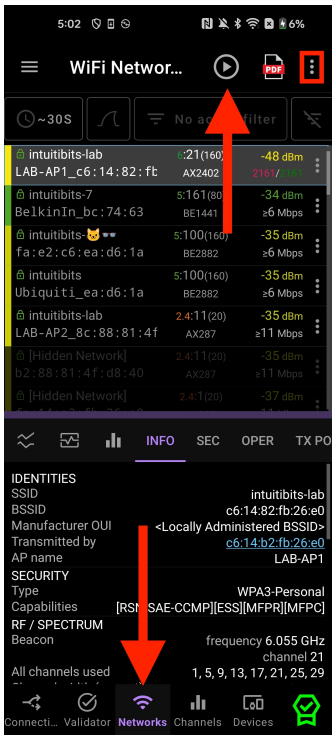
In this lab, you will learn to import scan data from Analiti, an Android app available on the Google Play Store that supports several Wi-Fi test utilities. It can scan for Wi-Fi networks and export results as a CSV file. WiFi Explorer can decode Analiti CSV data, allowing you to review the scan results.

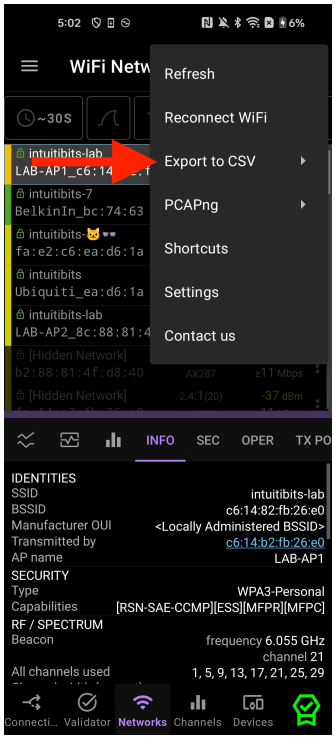
Import CSV Data from Analiti (Android)

If you don't have an Android phone or can't install Analiti, go to *File* > *Open* in WiFi Explorer to open the provided sample file **analiti.csv**, then proceed to the **Review Scan Data from Analiti** section later in this lab.

Follow the steps below to import scan data from Analiti into WiFi Explorer:

1. Download and install Analiti from the Google Play Store.
2. Open Analiti, select the *Networks* tab.
3. Tap the *Play* button to start scanning for Wi-Fi networks.
4. Let it run for 30 seconds, then tap the *Pause* button to stop it.
5. Use the three-dot option selector at the top right of the display to reveal the options available, then tap the *Export to CSV* option.

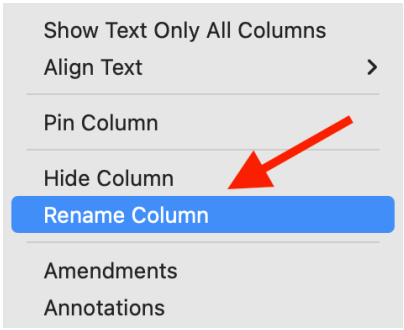


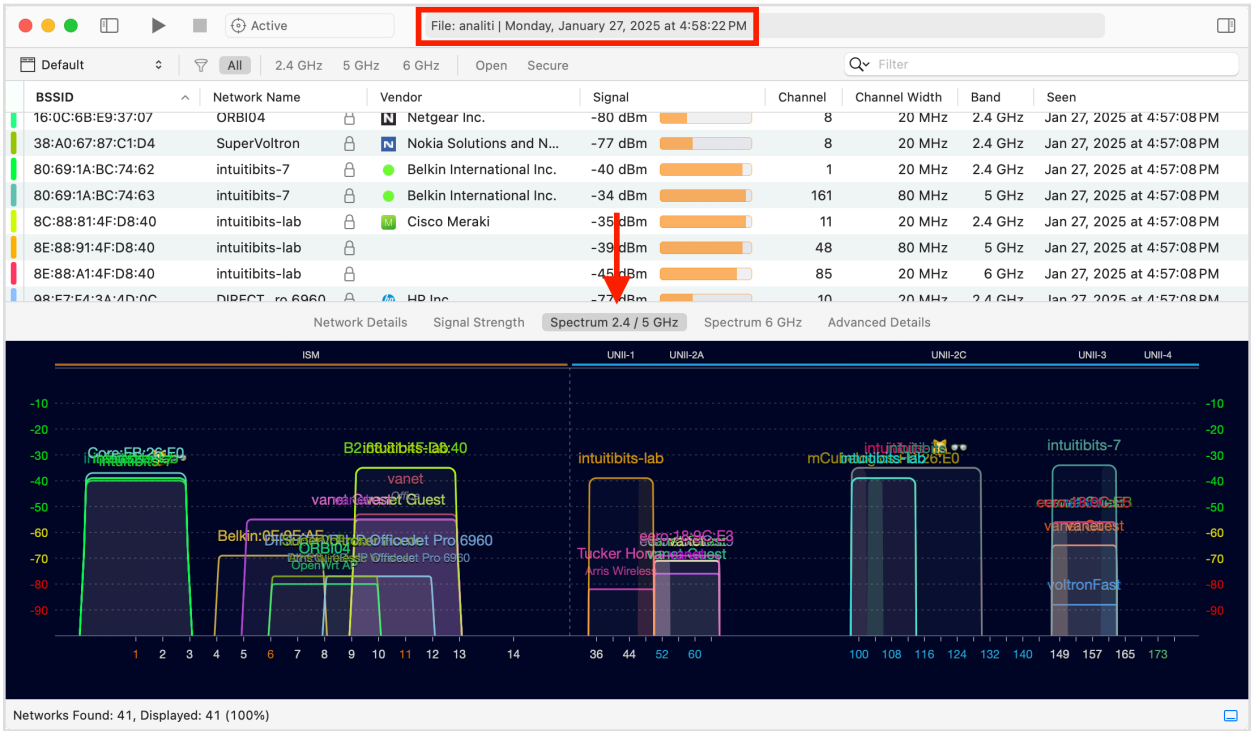


6. Choose *Share file* and email the results to yourself.
7. Launch WiFi Explorer.
8. Open the email on the computer running WiFi Explorer, then drag the attached text file directly into the app. Alternatively, save the attachment to your computer, then open it in WiFi Explorer by selecting *File* > *Open* and choosing the saved file.

Review Scan Data from Analiti

The screenshot below shows an example of scan results from Analiti displayed in WiFi Explorer with the *Spectrum 2.4 / 5 GHz* view selected.





You may notice that the values in the *Country Code, Mode, Generation,* and other columns are missing. This is because the data available in CSV format from Analiti is limited to specific fields only. Other columns, like *Vendor*, are derived from the BSSID.

Although the fields available are limited, WiFi Explorer can still provide a valuable snapshot of the environment where the scan data was collected. The *Spectrum 2.4/5 GHz* and *Spectrum 6 GHz* tabs are particularly helpful for quickly evaluating how channels are distributed or assigned across the different Wi-Fi networks in the area.

Conclusion

In this lab, you learned to import scan data from Analiti (Android) in CSV format to generate a valuable snapshot of the environment where the scan data was collected.

References

For detailed insights on importing data from CSV files, see *Chapter 5*: *Data Import from External Systems* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Notes

- CSV data does not include all the values usually available from information elements found in beacon and probe response frames. Therefore, it is recommended that scan data be collected in PCAP format when possible.

< End of Lab >

Lab #6 – Built-in Columns

In this lab, you will learn about WiFi Explorer's built-in columns, which display key network details, derived data, or data not found on information elements. You will also learn about the different options to manage columns.

Built-in Columns

WiFi Explorer's built-in columns are categorized into four groups: *Basic*, *Standard*, *Expert*, and *Legacy*. *Basic* columns include common metrics found in most Wi-Fi scanners, while *Standard* and *Expert* columns offer advanced network details. Legacy columns, introduced in the earliest versions of WiFi Explorer, are retained for compatibility.

Basic	Standard	Expert	Legacy
• **BSSID** • Band • Channel • Channel Width • Generation • Max Rate • Mode • Network Name (SSID) • Security • Seen • Signal (RSSI) • Vendor	• Annotations • Basic Rates • Beacon Interval • Center Frequency • Channel Utilization • Country Code • AP Name • First Seen • Last Seen • Min Rate • Noise* • SNR* • Stations • Streams • Type	• Amendments • Beacon Airtime • Beacon Mode • Beacon Rate • Clients* • Count* • IE Count • IE Total Length • Max Basic Rate • Min Basic Rate • Uptime • Wide Channel	• Fast Transition* • Protected Mode* • WPS*

* *Not available on WiFi Explorer Pro for Windows.*

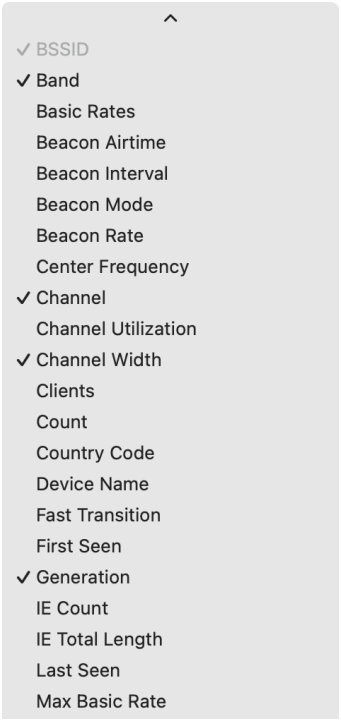
A description of each column can be found in *Chapter 11: Data Visualization: Columns & Profiles* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Manage Built-in Columns

Columns may be shown or hidden, pinned or unpinned, and renamed as required to suit the requirements of a particular scenario.

Show or Hide a Column

Not all columns are visible in the table and may be shown or hidden as needed.



Follow these steps to show or hide a column:

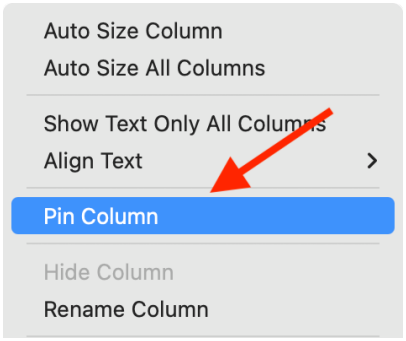
1. Open WiFi Explorer.
2. Right-click on the networks table's header to reveal the list of built-in columns (*columns with a check mark are currently visible in the table*).
3. Select the column you want to hide or show.

To hide a column, you may also right-click on the column title and select the "Hide column" option.

As an exercise, use the steps above to show the *Amendments*, *AP Name*, *Channel Utilization*, and *Stations* columns.

Pin a Column

Column pinning allows columns to be fixed to the left edge of the networks table so that the column remains visible when scrolling horizontally.

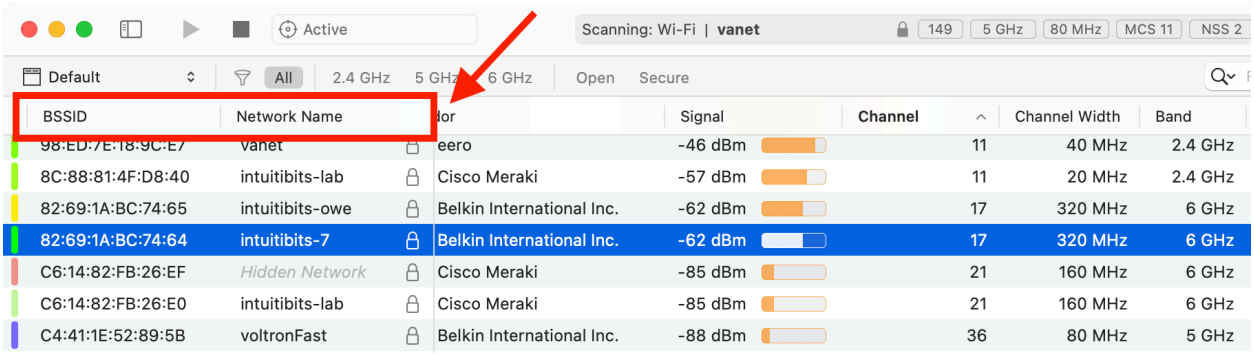


Follow the steps below to pin or unpin a column:

1. Open WiFi Explorer.
2. Right-click the title of the column you want to pin or unpin to display a contextual menu with column-specific options.
3. Select **Pin Column** or **Unpin Column** to pin or unpin that column.

As an exercise, **use the steps above to pin** the *BSSID* and *Network Name* columns and notice how they remain fixed to the left edge of the table as you scroll

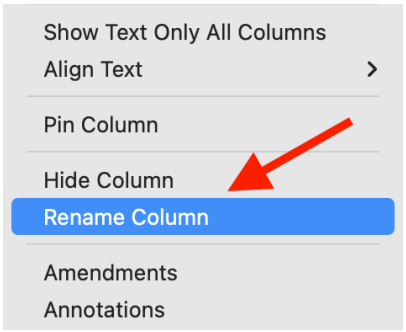
horizontally to view other columns.



Rename a Column

You can rename a column to make it more descriptive or concise.

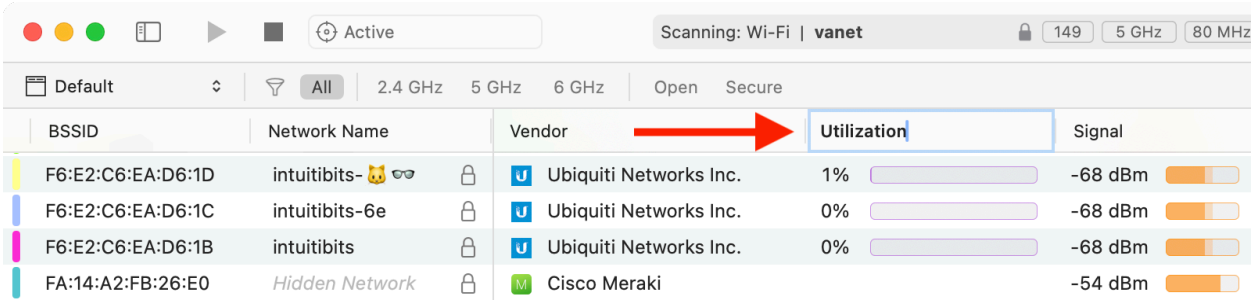
Follow the steps below to rename a column:



1. Launch WiFi Explorer.
2. Right-click the title of the column you want to rename to display a contextual menu with column-specific options.
3. Select **Rename Column**.
4. Type a new name in the column title, then press *Enter (Return* on Windows*)*.

You may also rename a column by double-clicking the column title in the networks table and entering a new column name.

As an exercise, **use the steps above to rename** the *Channel Utilization* column to *Utilization*. If this column is not visible, right-click the table header to reveal the list of available columns and select it to make it visible.



The column's name can be restored to its original value by deleting the custom name and leaving it blank.

Sort, Rearrange, and Resize Columns

Columns can also be sorted, moved, and resized.

- *Sorting*: Click a column title to sort it in ascending order. Click it again to sort in descending order.
- *Moving*: Click and hold a column title to move the column to a different position in the table.
- *Resizing*: Drag the vertical divider between columns to adjust their width. You can also right-click a column title and select **Auto Size Column** or **Auto Size All Columns** to resize the column to fit the content automatically.

Conclusion

In this lab, you learned about WiFi Explorer's built-in columns and how to manage them, including renaming and pinning, to improve navigation and facilitate the identification of key network details in scan results.

References

For detailed insights on built-in columns, including their description and whether or not they are supported in active and passive scan mode, see *Chapter 11: Data Visualization: Columns & Profiles* in *WiFi Explorer Pro 3: The Definitive User Guide*.

< End of Lab >

Lab #7 – Annotations

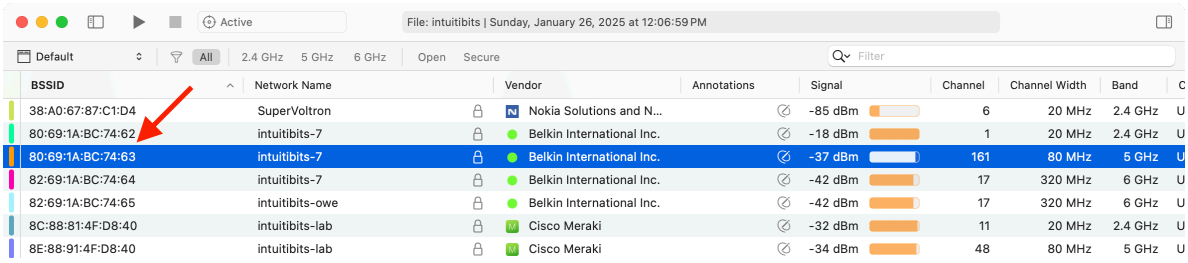
In this lab, you will learn to use annotations. Annotations are custom labels that can be manually assigned to specific BSSIDs. They can be used, for example, to indicate the location of an access point (e.g., "Main Office") or to manually group several BSSIDs that share a common characteristic.

Simple Annotations

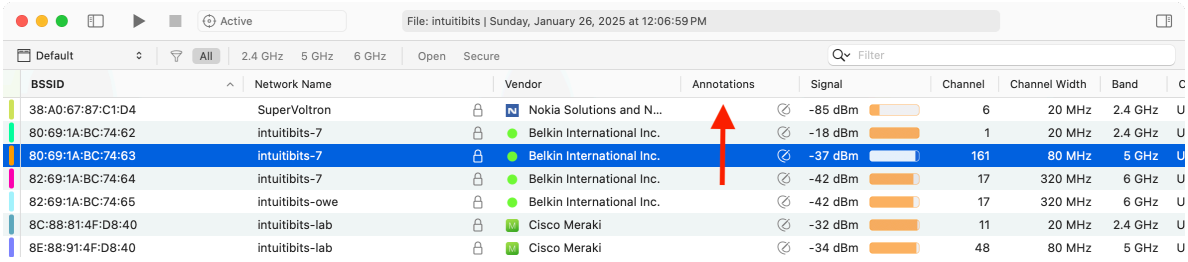
The easiest way to apply an annotation to a BSSID is to double-click in the *Annotations* column of the chosen BSSID and enter the desired text.

As an exercise, let's add annotations to a BSSID by using the *Annotations* column:

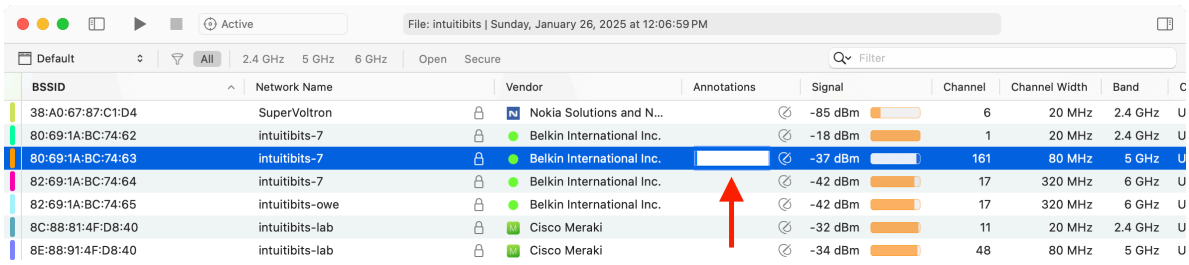
5. Launch WiFi Explorer and go to *File* > *Open* to open the provided capture file **intuitibits.pcapng**.
6. Select the network with BSSID **80:69:1A:BC:74:63**, and network name (SSID) *intuitibits-7*.



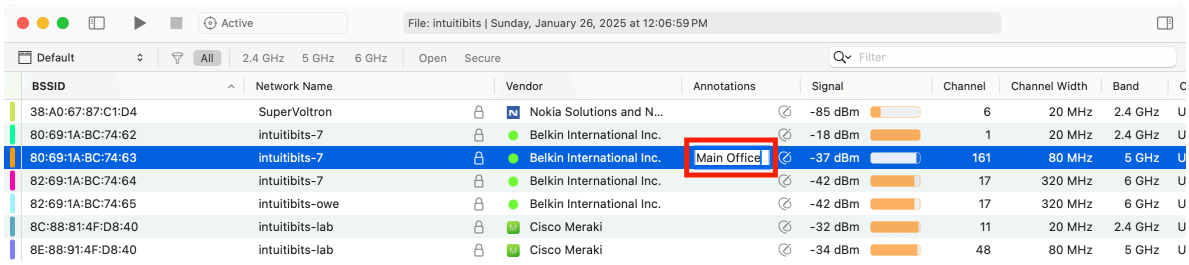
7. Find the *Annotations* column in the networks table. If it's not visible, right-click the table header to reveal the list of available columns and select the **Annotations** column to enable it.



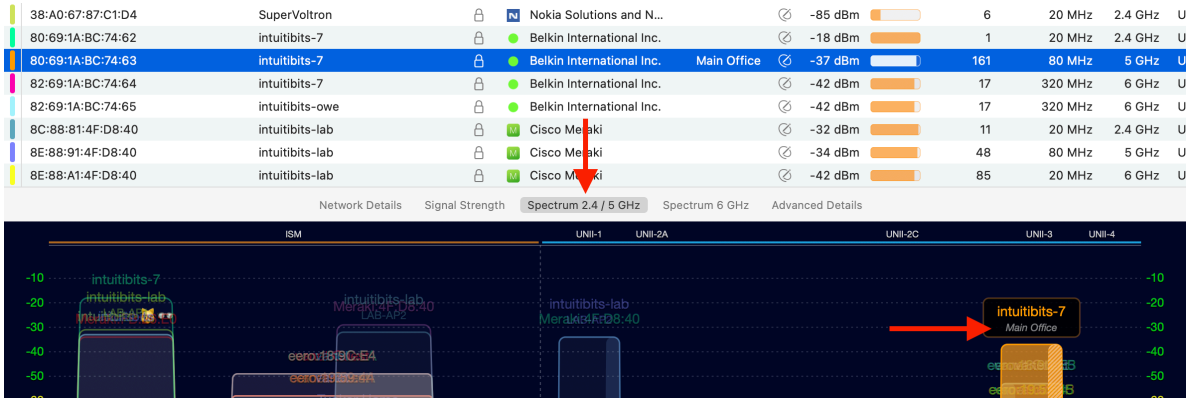
8. Double-click the field in the *Annotations* column for the selected BSSID.



9. Type **Main Office**, then press *Enter (Return* on Windows*)*.



10. The selected BSSID is now labeled **Main Office**.



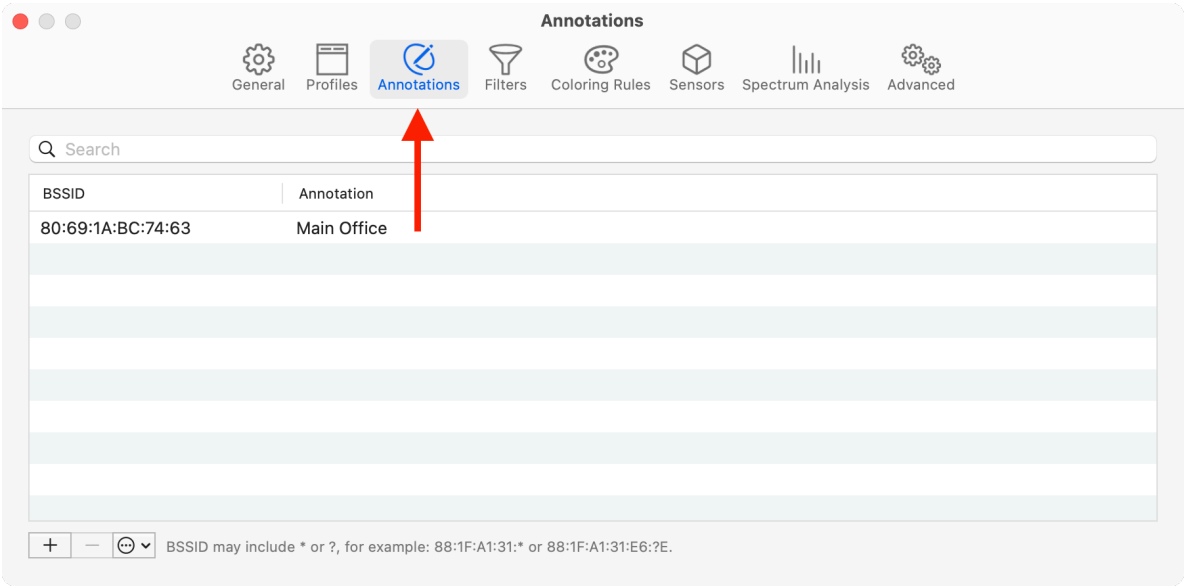
Advanced Annotations

You can annotate BSSIDs through the *Annotations* tab in the *Settings* panel, enabling you to assign labels to specific or multiple BSSIDs. This tab also lets you quickly search, edit, and remove annotations.

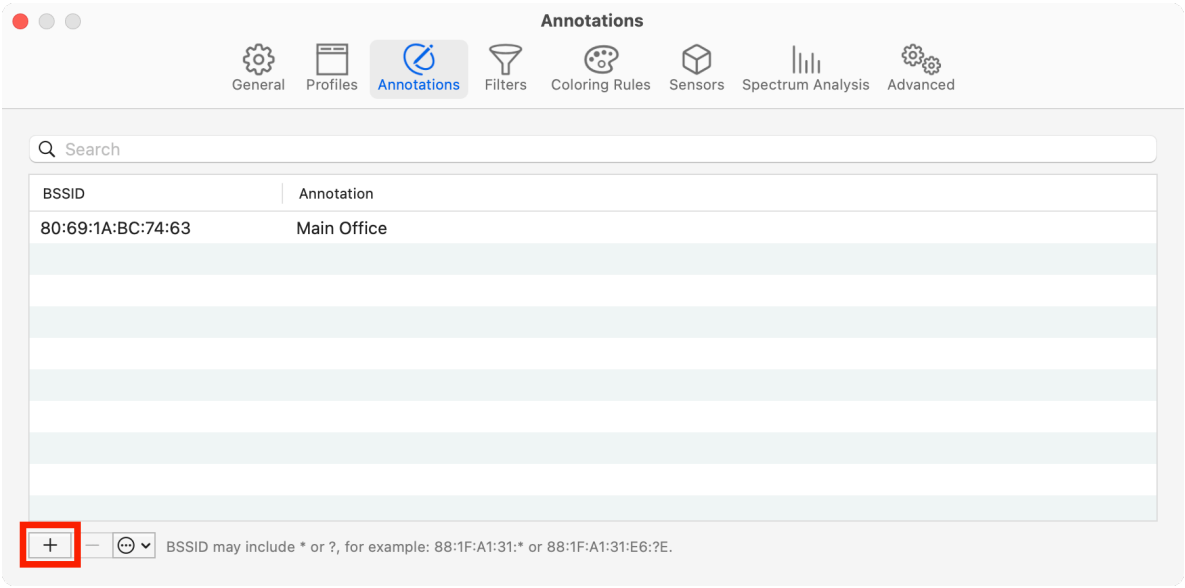
As an exercise, let's add annotations to a BSSID by using the *Annotations* settings:

1. Launch WiFi Explorer and go to *File* > *Open* to open the provided capture file **intuitibits.pcapng**.
2. Mac users: Go to *WiFi Explorer Pro 3* > *Settings* in the menu bar.
   Windows users: *Navigate to File* > *Settings* in the menu.

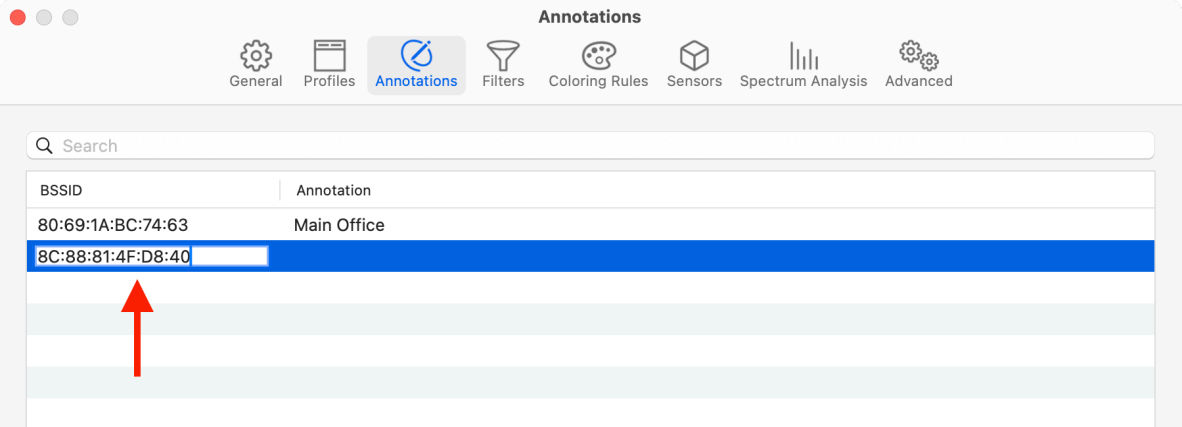
3. In the *Settings* panel, go to the *Annotations* tab.



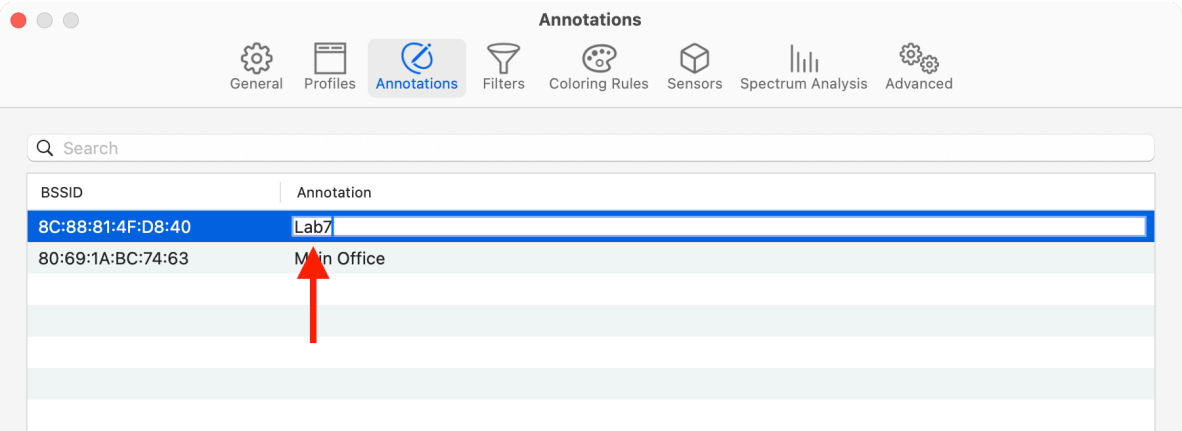
4. Click the "+" button to add a new annotation.



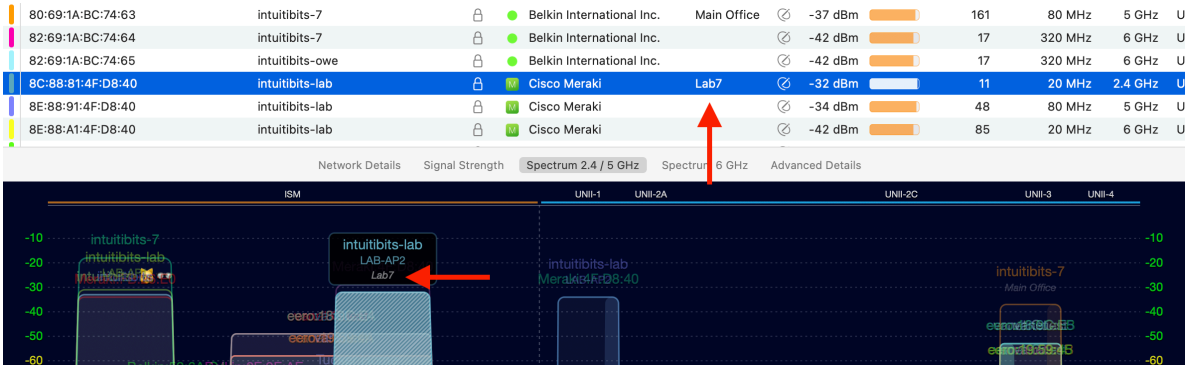
5. Type **8C:88:81:4F:D8:40** in the *BSSID* field, then press *Enter* (*Return* on Windows).



6. Double-click the *Annotation* field, enter **Lab7**, and press *Enter* (*Return* on Windows).



7. Close the settings panel and return to the main window. The BSSID **8C:88:81:4F:D8:40** is now labeled **Lab7**.

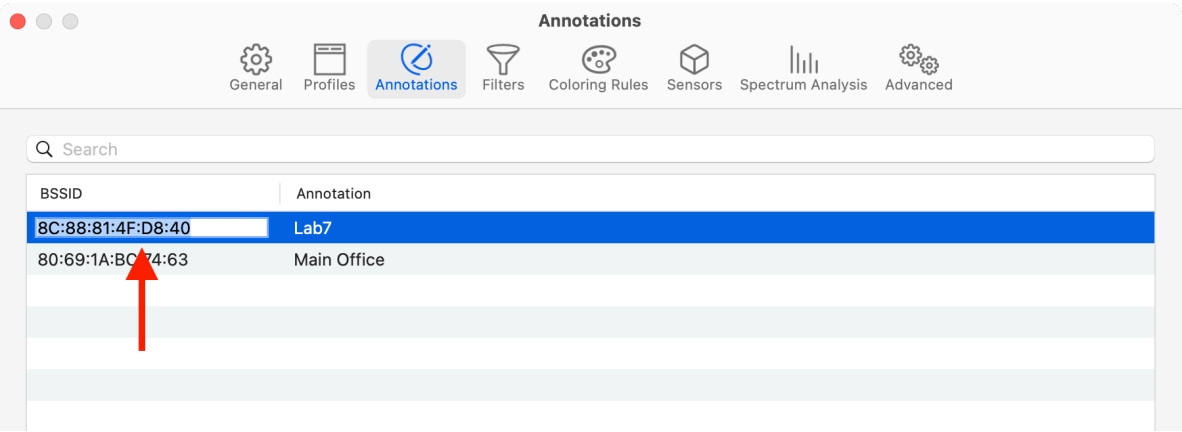


Groups of BSSIDs may be identified using a wildcard address-matching format:

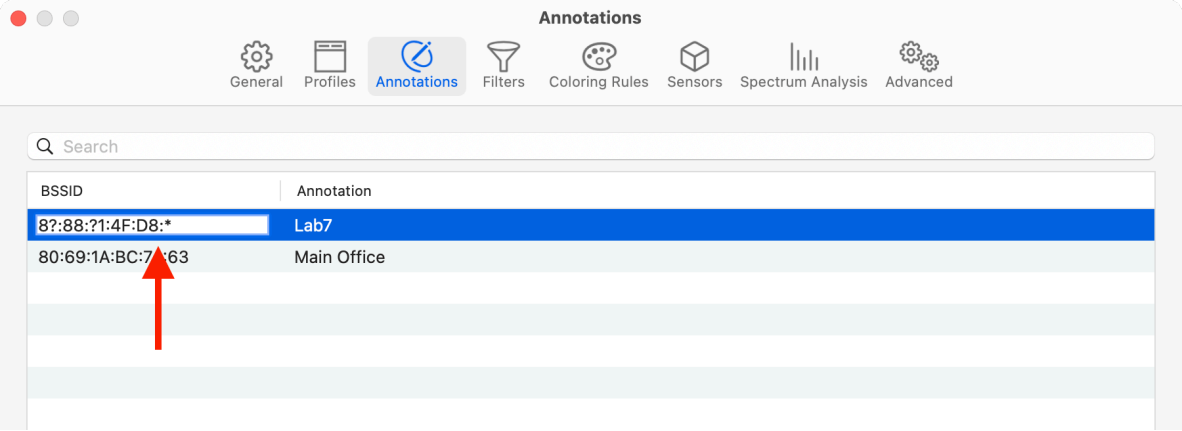
- **?** to match a single character
- ***** to match multiple characters

As an exercise, let's modify the **Lab7** annotation we just added so that it will match all BSSIDs from the same AP:

5. Mac users: Go to *WiFi Explorer Pro 3* > *Settings* in the menu bar.
   Windows users: *Navigate to File* > *Settings* in the menu.
6. In the *Settings* panel, go to the *Annotations* tab.
7. Double-click the *BSSID* field for the **Lab7** annotation.

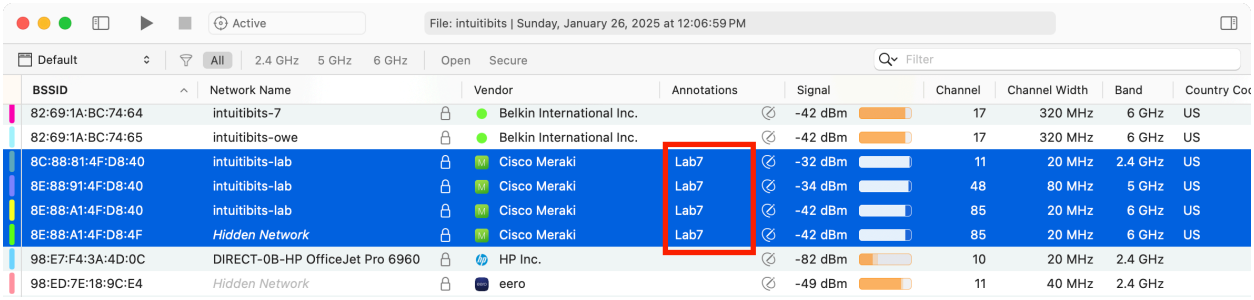


8. Edit the BSSID and change it to **8?:88:?1:4F:D8:***, then press *Enter* (*Return* on Windows)



9. Close the settings panel and return to the main window.
10. The following BSSIDs are now labeled **Lab7**:
    - 8C:88:81:4F:D8:40

- 8E:88:91:4F:D8:40
- 8E:88:A1:4F:D8:40
- 8E:88:A1:4F:D8:4F

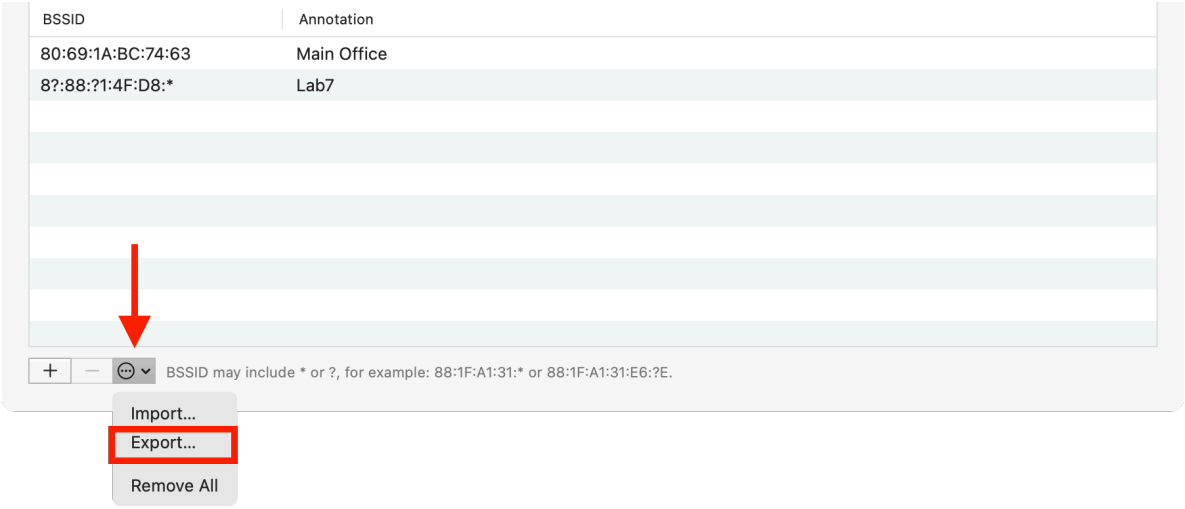


Export and Import Annotations

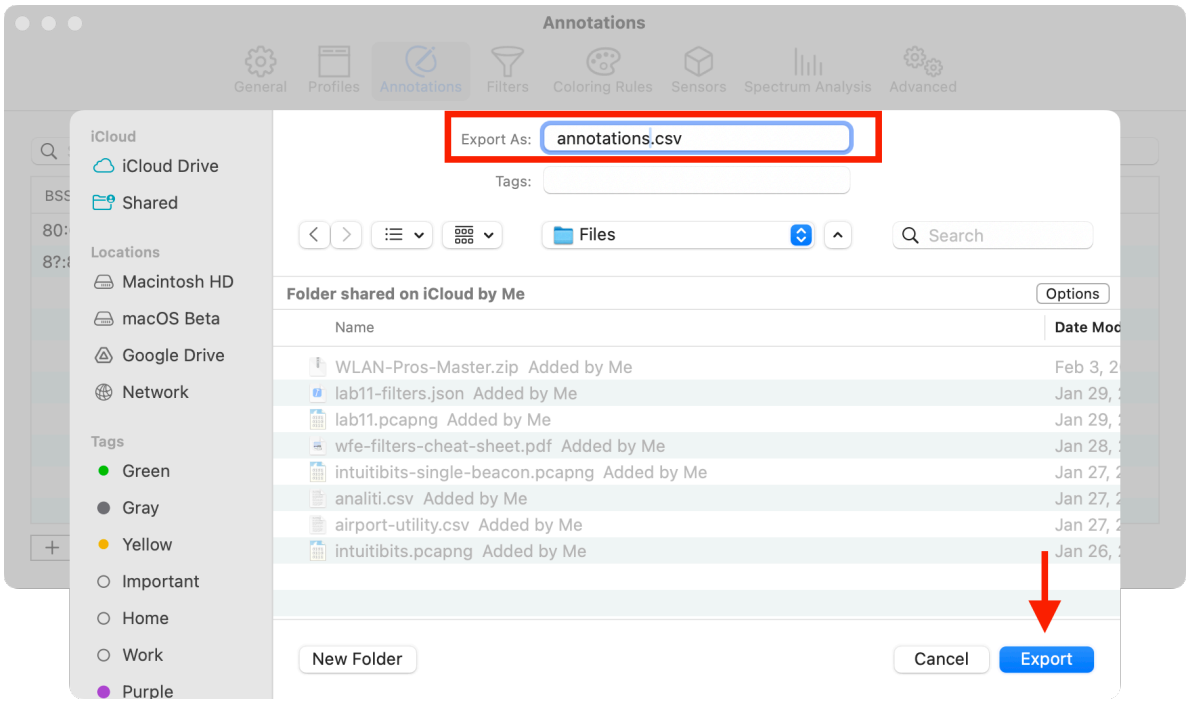
You can export annotations for backup, modification, or sharing with other WiFi Explorer users. Annotations are exported in CSV format.

Follow these steps to export the annotations created in this lab:

1. Mac users: Go to *WiFi Explorer Pro 3* > *Settings* in the menu bar.
   Windows users: *Navigate to File* > *Settings* in the menu.
2. In the *Settings* panel, go to the *Annotations* tab.
3. Click the *More* button and choose **Export**.



4. Enter a desired file name, for example, **annotations.csv**, then choose a location to save the file and click **Export** (**Save** on Windows).



The screenshot below shows the contents of the exported file when opened in a text editor:

When creating or editing an annotations file, ensure that **annotations are enclosed in quotation marks** if they contain spaces or commas.

Importing annotations follows a similar process: Create a CSV file with the desired annotations and use the **Import** option to add them to WiFi Explorer. Typically, annotation files to be imported are generated from a dataset of BSSIDs, with labels manually or automatically assigned.

Conclusion

In this lab, you learned how to use annotations to assign persistent labels to one or more BSSIDs. Specifically, you learned to apply annotations in two ways: directly through the *Annotations* column or via the *Annotations* tab in the *Settings* panel.

References

For detailed insights on using annotations, see *Chapter 12: Data Visualization: Scan Results Organization, Coloring Rules, Data Enhancements & Hidden Gems* in *WiFi Explorer Pro 3: The Definitive User Guide*.

< End of Lab >

Lab #8 – Custom Columns

In this lab, you will learn how to create and use custom columns to explore specific technical details for each network. You can create custom columns from over 850 information element fields.

Let's assume a scenario of conducting a security audit for a Wi-Fi network to understand why custom columns should be used. We want to verify the *Group Cipher Suite* used by the network. As the *Group Cipher Suite* is not one of WiFi Explorer's predefined columns, we must create a custom column.

In WiFi Explorer Pro 3, there are three different ways to create a custom column, while there are two in WiFi Explorer Pro for Windows. In this lab, we'll practice creating a custom column using the two common mechanisms available on both platforms.

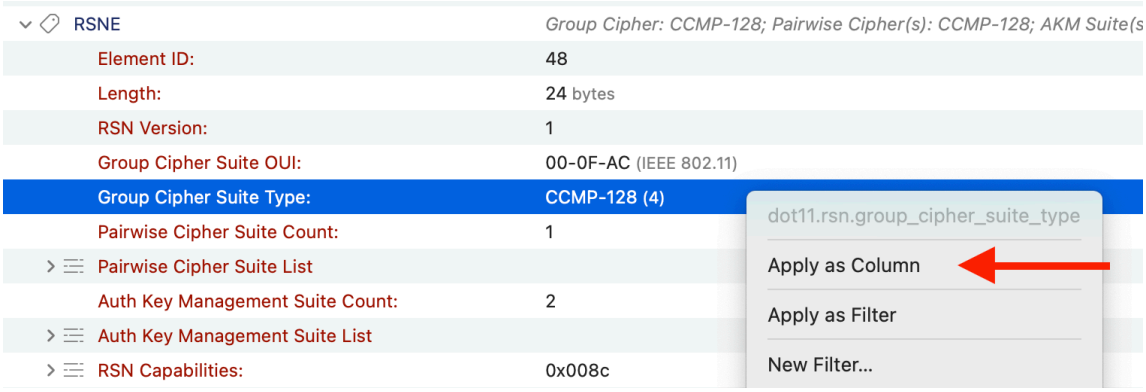
Create a Custom Column

As part of the security audit, we will add the Group Cipher Suite Type column and the Auth Key Management Suite Type column. Each column will be added using one of the two available mechanisms in WiFi Explorer Pro 3 / WiFi Explorer Pro for Windows.

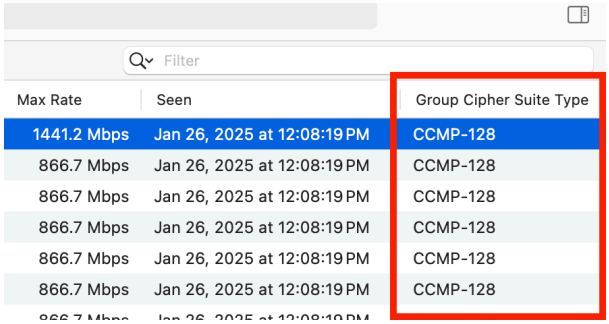
Create the Group Cipher Suite Type Column

To create the custom column *Group Cipher Suite Type* using the *Apply as Column* method, follow the steps below:

1. Launch WiFi Explorer and go to *File* > *Open* to open the provided capture file **intuitibits.pcapng**.
2. Select the network with BSSID **80:69:1A:BC:74:63**, and name (SSID) *intuitibits-7*.
3. Navigate to the *Advanced Details* view and look for the *RSNE information element*.
4. Expand the RSNE information element and select the field *Group Cipher Suite Type*.
5. Right-click and select the **Apply as Column** option from the contextual menu.



A new column titled "Group Cipher Suite Type" will be added to the far right of the networks table. Like any other column, it can be rearranged and moved to a different location in the table as needed.

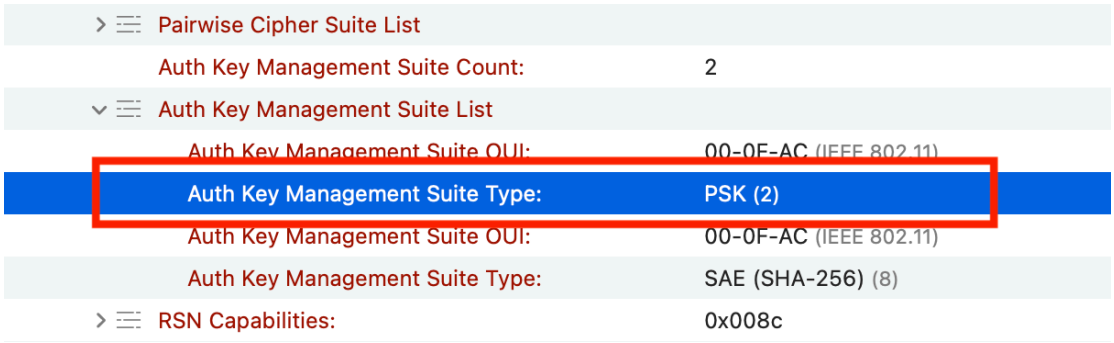


Note that the value of this column is populated only for the networks that advertise an RSNE information element.

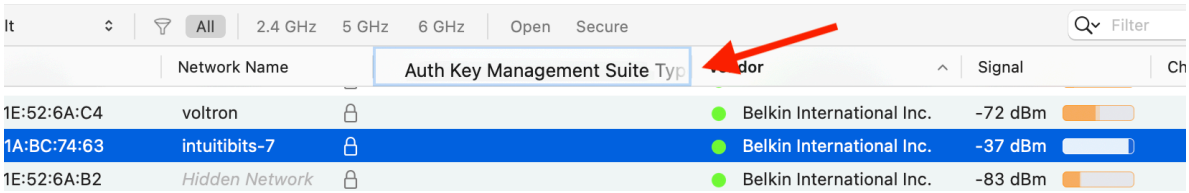
Create the Auth Key Management Suite Type Column

To create the custom column *Auth Key Management Suite Type* using the drag & drop method, follow the steps below:

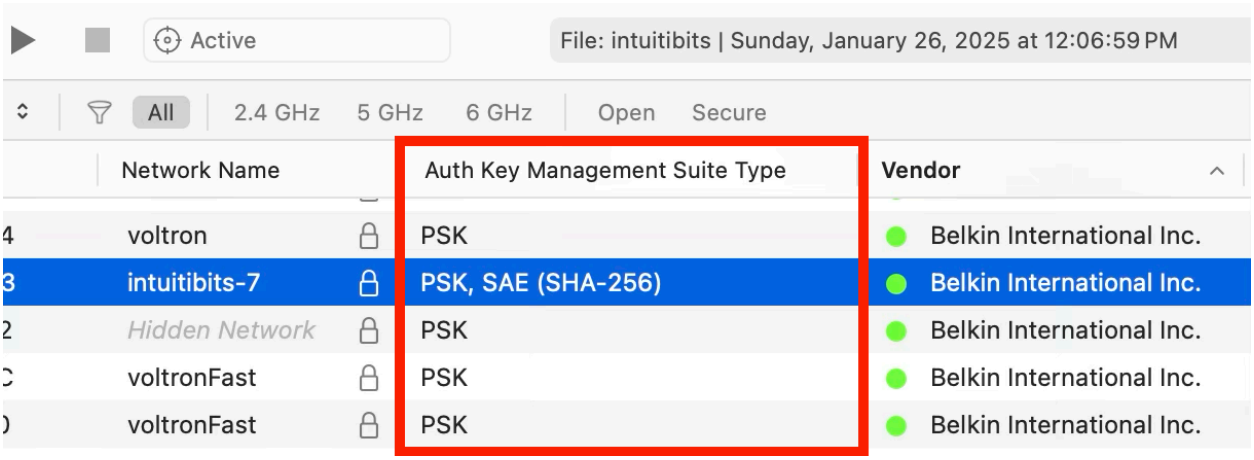
1. Using the same scan results from the file **intuitibits.pcapng**, ensure the network with BSSID **80:69:1A:BC:74:63**, and name (SSID) *intuitibits-7,* is selected.
2. Navigate to the *Advanced Details* view and look for the *RSNE information element*.
3. Expand the *RSNE* information element.
4. Expand the *Auth Key Management Suite List* field and select the first *Auth Key Management Suite Type* field.



5. Click to drag the field and drop it over the networks table's header in the desired position.



6. The networks table will now have a new column titled "Auth Key Management Suite Type" at the position where you dropped it.
7. Resize the column's header to display the entire title if needed.



What do you observe about the values populated for this column?

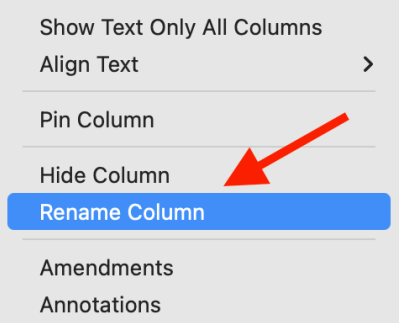
If the *Auth Key Management Suite Type* field appears multiple times within the *Auth Key Management Suite List*, the values for each network are combined into a comma-separated list and displayed in the table under the *Auth Key Management Suite Type* custom column.

Rename a Custom Column

By default, a custom column's title matches the name of the information element field. However, some titles may be too long or not descriptive enough. You can rename a custom column to make it clearer and more concise.

Follow these steps to rename the *Auth Key Management Suite Type* custom column to *AKM:*

1. Locate the *Auth Key Management Suite Type* column in the networks table.
2. Right-click the column's title to display a contextual menu with column-specific options.
3. Select **Rename Column**.
4. Type *AKM* in the column's title, then press *Return* (*Enter* on Windows).

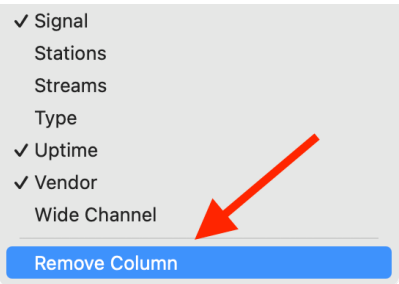


Remove a Custom Column

If a custom column is no longer needed, you can permanently remove it.

Follow these steps to remove the *Group Cipher Suite Type* column:

1. Locate the *Group Cipher Suite Type* column in the networks table.
2. Right-click the column's title to display a contextual menu with column-specific options.
3. Scroll to the bottom of the options in the contextual menu and select **Remove Column**.
4. Click **Remove** when prompted for confirmation.



Conclusion

In this lab, you learned how to create and utilize custom columns to analyze specific technical details for each network. Custom columns allow you to display information in a table that isn't available through the predefined columns.

References

For detailed insights on custom columns, see *Chapter 11: Data Visualization: Columns & Profiles* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Notes

- If an information element field is found multiple times within multiple instances of the information element in the beacon, values will also be combined into a comma-separated list and displayed in the table under the custom column corresponding to that field. This includes information elements included inside a Multiple BSSID element, for example.
- Only custom columns can be removed; predefined columns cannot be deleted.

< End of Lab >