Wi-Fi Scanning and Capturing: Day 2

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 2

- Lab #9: Basic Filtering
- Lab #10: Advanced Filtering using Network Attributes
- Lab #11: Advanced Filtering using IE Fields
- Lab #12: Custom Display Filters
- Lab #13: Built-in Wi-Fi Captures
- Lab #14: Remote Sensor Captures
- Lab #15: Multi-Source Captures
- Lab #16: Capture Workflow Settings

Lab #9 – Basic Filtering

In this lab, you will learn how to use basic filter expressions to build display filters. By narrowing scan results to specific networks of interest, you can make diagnosing and troubleshooting specific Wi-Fi networks and environments easier.

To filter the scan results, you may use *arbitrary strings* in addition to three types of filter expressions:

- Keyword-based filter expressions
- Network attribute-based filter expressions
- Information element field-based filter expressions

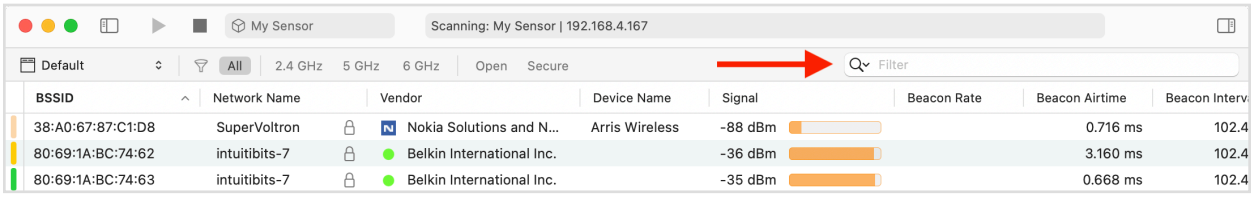
This lab's hands-on exercises will explore basic filter expressions created from **arbitrary strings** and **keyword-based filters**.

A filter expressions cheat sheet accompanies this lab. Keep it accessible as you work through the exercises.

Keyword-based Filter Expressions

Various filter keywords may be entered into WiFi Explorer's filter field to filter the networks displayed in the table. You may also enter arbitrary strings for matching text in various columns, including the *BSSID, Name (SSID), AP Name, Annotations, and Country Code* columns.

The location of the filter field is shown in the screenshot below.

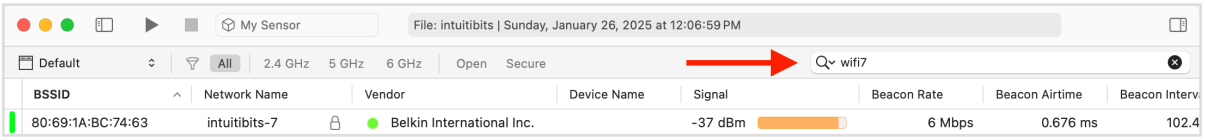


The general steps to filter scan results using keywords or arbitrary strings are:

1. Enter a keyword or arbitrary string in the filter field.
2. Scan results will update automatically as you type.

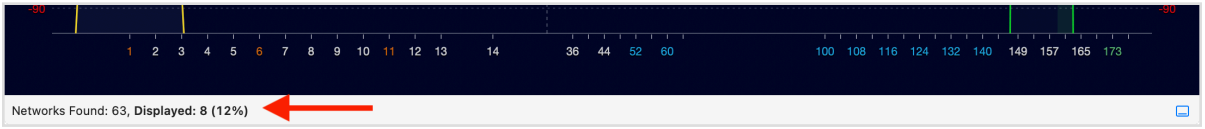
As an exercise, let's practice some filter expressions following these steps:

1. Launch WiFi Explorer and open the file **intuitibits.pcapng**.
2. Enter the filter expressions from the table below, one at a time, in the filter field, as shown in this screenshot:



Arbitrary strings and keywords are CASE INSENSITIVE.

3. Then, verify that the number of displayed networks in the table matches those indicated at the bottom of the WiFi Explorer window after applying the filter.



	Filter Expression	Displayed Networks
1	wifi7	8
2	D8:40	5
3	intuitibits	14
4	8	4
5	11be	8
6	wpa3	22
7	11v	51
8	40mhz	9
9	hidden	21
10	>=-72	41

Arbitrary strings may not always yield the expected results. When you use an arbitrary string, WiFi Explorer applies heuristics to interpret your intent. For example, entering a number that matches a known Wi-Fi channel will filter by channel, while a string containing a colon (":") will be treated as a BSSID filter.

However, in some cases, the string may be interpreted differently than intended. When this occurs, use advanced filtering with network attribute-based or information element field-based expressions for more precise results.

Conclusion

In this lab, you learned how to use arbitrary strings and keyword-based filter expressions to narrow scan results to specific networks of interest.

References

For detailed insights on keyword-based filter expressions, see *Chapter 10: Data Visualization: Filter Expressions and Display Filters* in *WiFi Explorer Pro 3: The Definitive User Guide*.

< End of Lab >

Lab #10 – Advanced Filtering using Network Attributes

In this lab, you will learn to create advanced and precise display filters using network attribute-based expressions, enabling you to refine scan results and focus on specific networks of interest.

A filter expressions cheat sheet accompanies this lab. Keep it accessible as you work through the exercises.

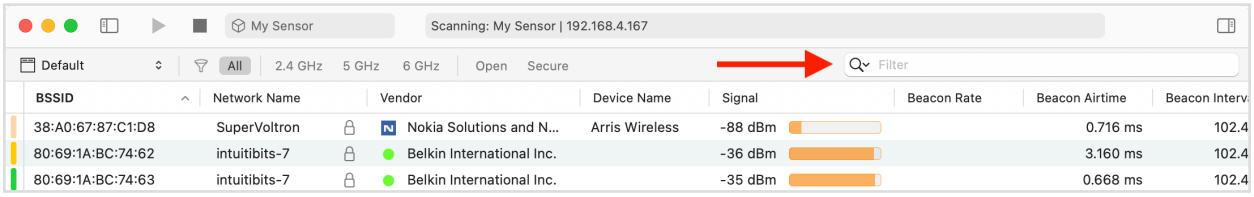
Network Attribute-based Filter Expressions

Scan results may be filtered using network attributes. These attributes map to WiFi Explorer pre-defined columns and are identified with the prefix **dot11.net**. For example, to show networks with a minimum basic rate of 11 Mbps or higher, the filter expression **dot11.net.min_basic_rate >= 11** may be applied.

For a complete list of network attributes, please refer to the cheat sheet's *Filter by Network Attribute* section.

There's no need to memorize every network attribute—WiFi Explorer's auto-complete feature makes it easy to construct filter expressions. Type **dot11.net** in the filter field, and a list of network attributes will appear. Continue typing to narrow down the list further.

The following screenshot shows the location of the filter field.



The general steps to filter scan results using network attribute-based filters are:

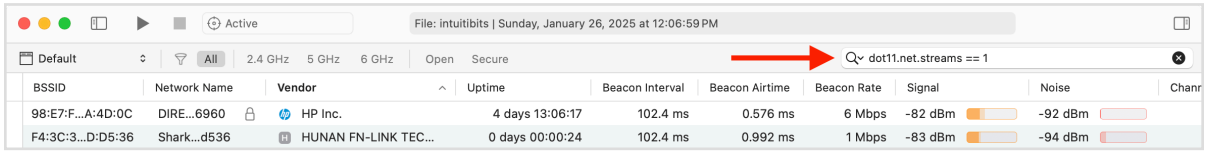
1. Enter *dot11.net* in the filter field, then continue typing to construct the expression based on the desired network attribute or choose an attribute from the list using the auto-complete feature.
2. Complete the filter expression by selecting an appropriate comparison operator (refer to the table below) and specifying the desired filter value.

Operator	Description	Value Type
==	Equal	Number, Text
!=	Not equal	Number, Text
~~	Contains	Text
!~	Does not contain	Text
>	Greater than	Number
>=	Greater than or equal	Number
<	Less than	Number
<=	Less than or equal	Number

Comparison Operators

As an exercise, let's practice some filter expressions following these steps:

1. Launch WiFi Explorer and open the file **intuitibits.pcapng**.
2. Enter the network attribute-based filter expressions from the table below, one at a time, in the filter field, as shown in this screenshot:



The values used with network attribute-based filters are CASE INSENSITIVE.

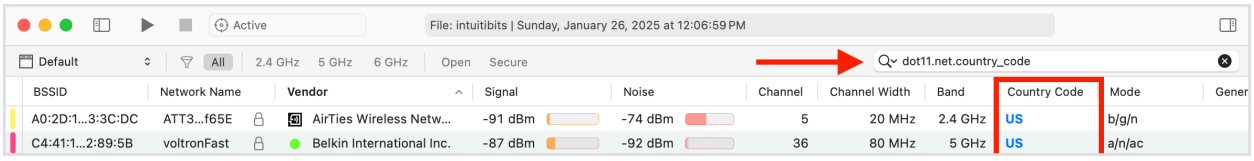
3. Then, verify that the number of displayed networks in the table matches those indicated at the bottom of the WiFi Explorer window after applying the filter.

	Filter Expression	Displayed Networks
1	dot11.net.streams == 1	3
2	dot11.net.vendor == Meraki	0

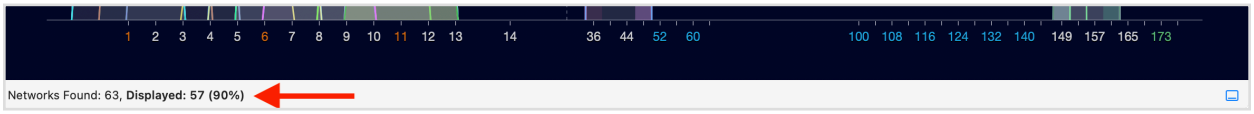
	Filter Expression	Displayed Networks
3	dot11.net.vendor ~~ Meraki	10
4	dot11.net.ssid == "vanet Guest"	4
5	dot11.net.mode ~~ ax	35
6	dot11.net.mode !~ ax	28
7	dot11.net.security ~~ wpa2/wpa3	13
8	dot11.net.beacon_mode == Nontransmitted	3
9	dot11.net.channel_util >= 20	3
10	dot11.net.device_name	8

If no comparison operator is used and the filter expression contains only the network attribute identifier, WiFi Explorer will filter scan results to include only networks with a non-empty value for that attribute.

For example, enter the filter expression **dot11.net.country_code** and verify that all the networks displayed advertise a country code.



In this case, only 57 out of 63 networks in the scan results found in the file *intuitibits.pcapng* include a country code.

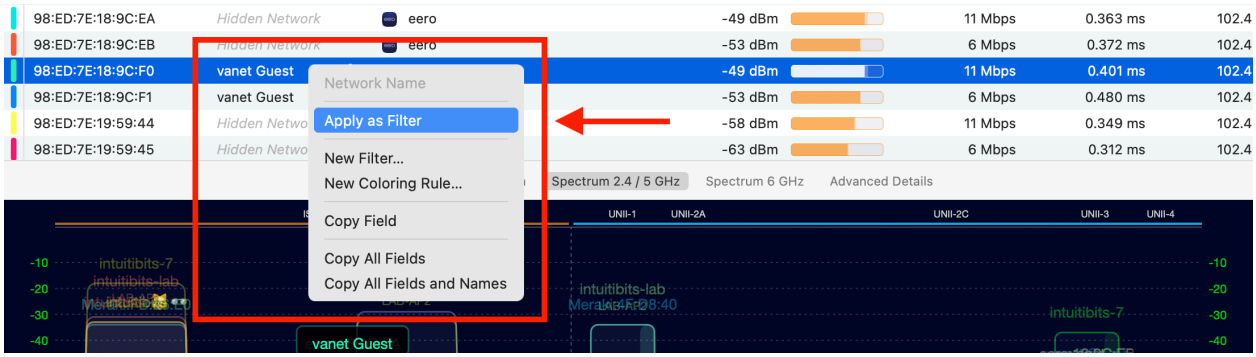


Quick Network Attribute-based Filter Expressions

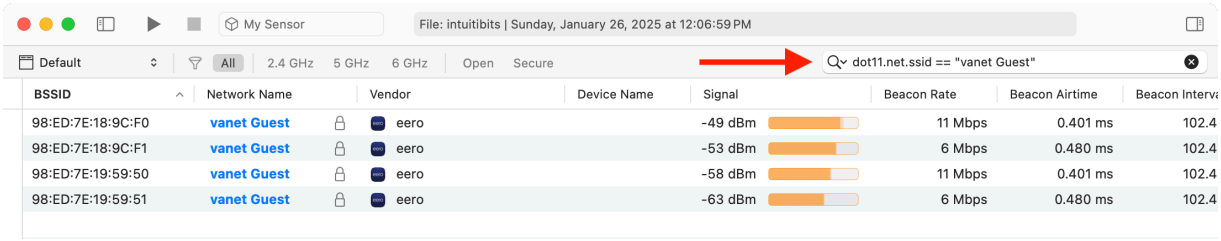
Another quick method for creating network attribute-based filter expressions is leveraging WiFi Explorer's pre-defined columns in the networks table. You can quickly generate a display filter directly from a field within these columns.

Follow these steps to create a network attribute-based filter using a field from a pre-defined column:

1. Launch WiFi Explorer and open the file **intuitibits.pcapng**.
2. Select any network with the name “vanet Guest.”
3. Right-click the value “vanet Guest.” and choose **Apply as Filter**.



4. The filter field will be populated with the expression **dot11.net.ssid == “vanet Guest”** and immediately applied to narrow the scan results.



Operating System Differences

In WiFi Explorer Pro for Windows, the **Apply as Filter and Negate** option appears under **Apply as Filter** when you right-click on a field within a pre-defined column. As the name suggests, this creates a negated filter expression, for example, **dot11.net.ssid != “vanet Guest”**

On Mac, holding the Option key changes **Apply as Filter** to **Apply as Filter and Negate**.

Conclusion

In this lab, you learned how to use network attribute-based filter expressions to narrow scan results to specific networks of interest.

References

For detailed insights on network attribute-based filter expressions, see *Chapter 10: Data Visualization: Filter Expressions and Display Filters* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Notes

- Quotation marks must be used when comparing values that contain spaces. For example, **dot11.net.ssid == "Guest Network"**
- Units (MHz, GHz, dBm, etc.) are optional when comparing numerical values. For example, the filter **dot11.net.snr > 15** is equivalent to **dot11.net.snr > 15dB**

< End of Lab >

Lab #11 – Advanced Filtering using IE Fields

In this lab, you will learn to create advanced and precise display filters using field-based expressions. This will enable you to refine scan results by focusing on specific information element fields.

A filter expressions cheat sheet accompanies this lab. Keep it accessible as you work through the exercises.

Information Element Field-based Filter Expressions

Scan results may be filtered using information element fields. These fields map to specific identifiers that begin with the prefix **dot11**. For example, to show the networks that advertise a transmit power level in their *Transmit Power Control* information element greater than or equal to 23 dBm, the filter expression **dot11.tpc_report.transmit_power >= 23** may be applied.

While you can manually enter filter expressions in the filter field, remembering the exact identifiers for specific fields can be challenging—especially with over 850 information element fields available. A more efficient approach is to inspect the fields within a network of interest, select the relevant field, and use it to construct a filter expression that refines the scan results based on that field.

The general steps to filter scan results using information element field-based filters are:

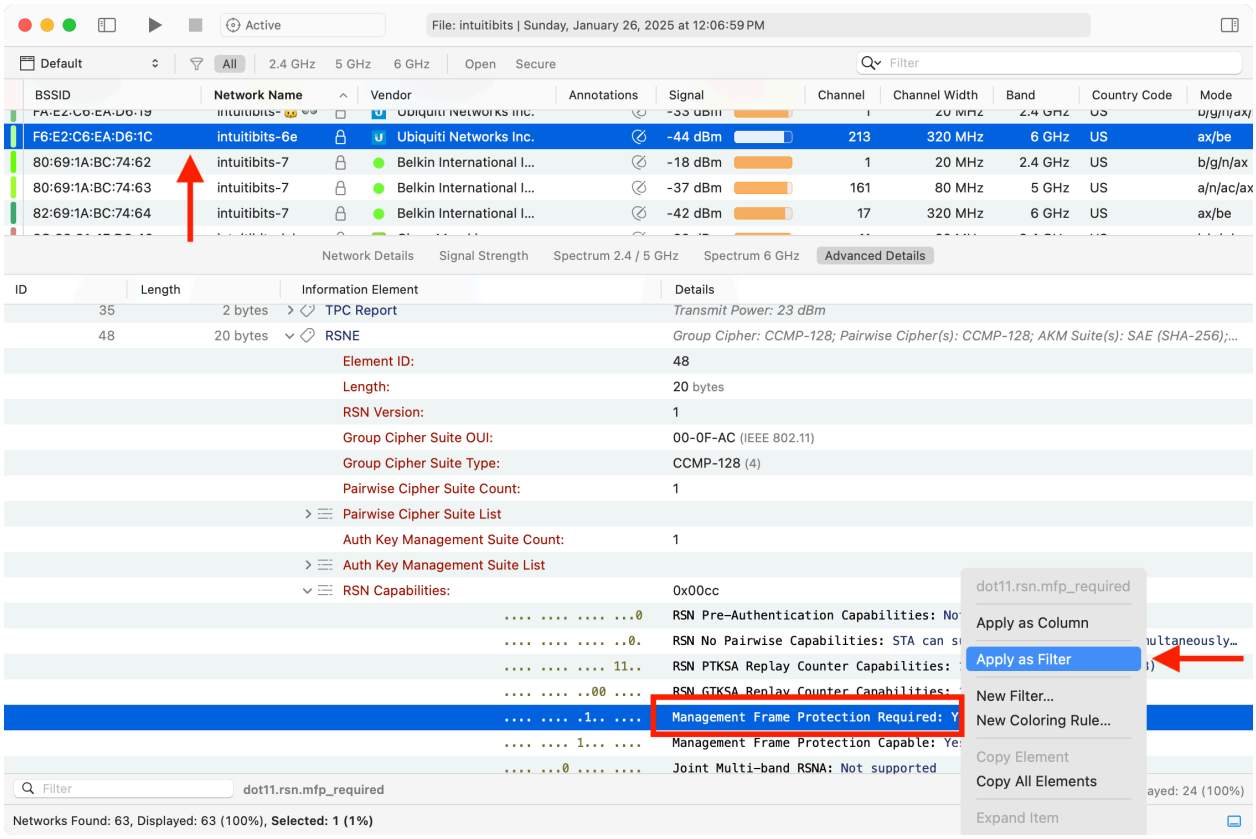
1. Select a network from the scan results.
2. Navigate to the *Advanced Details* tab.
3. Expand the relevant information element.
4. Right-click the desired field and choose **Apply as Filter**.

As an exercise, launch WiFi Explorer and open the file **intuitibits.pcapng**, then follow the steps below to display only the networks that require *Management Frame Protection*.

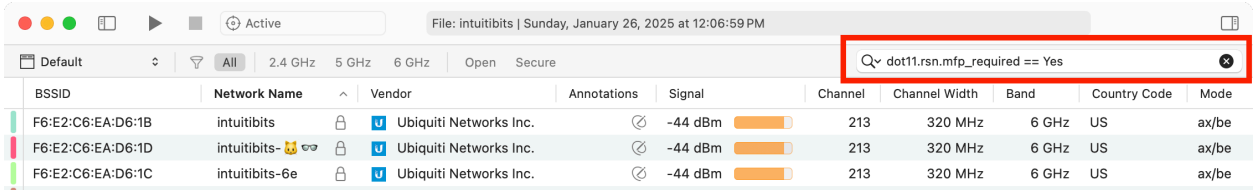
If WiFi Explorer is already running, ensure no filters are being applied.

1. Select the network with BSSID **F6:E2:C6:EA:D6:1C** and name (SSID) **intuitibits-6e**.
2. Navigate to the *Advanced Details* tab.

3. Expand the *RSNE* information element.
4. Expand the *RSN Capabilities* field.
5. Right-click the *Management Frame Protection Required* field and choose **Apply as Filter**.



6. The filter field will be populated with the expression **dot11.rsn.mfp_required == Yes** and immediately applied to narrow the scan results.



Operating System Differences

In WiFi Explorer Pro for Windows, the **Apply as Filter and Negate** option appears under **Apply as Filter** when you right-click on an information element field. As the name suggests, this creates a negated filter expression, for example, **dot11.rsn.mfp_capable != yes**

On Mac, holding the Option key changes **Apply as Filter** to **Apply as Filter and Negate**.

Conclusion

In this lab, you learned how to use field-based filter expressions to narrow scan results by focusing on specific information element field values.

References

For detailed insights on information element field-based filter expressions, see *Chapter 10: Data Visualization: Filter Expressions and Display Filters* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Notes

- Quotation marks must be used when comparing values that contain spaces. For example, **dot11.ext.he_oper.6ghz_oper_info.control.regulatory_info == "Standard Power AP"**
- Units (MHz, GHz, dBm, etc.) are optional when comparing numerical values. For example, the filter **dot11.tpc_report.transmit_power >= 23** is equivalent to **dot11.tpc_report.transmit_power >= 23dBm**

< End of Lab >

Lab #12 – Custom Display Filters

In this lab, you will learn how to create custom display filters to quickly narrow the networks shown in the networks table to those relevant to a specific scenario. You will also explore combining filter expressions for greater precision.

Custom filters are perfect for saving frequently used filters, especially when they involve complex expressions to target specific networks. They also simplify applying complex filters, eliminating the need for manual re-entry each time.

A filter expressions cheat sheet accompanies this lab. Keep it accessible as you work through the exercises.

Custom Filters

Custom filters can be created by accessing the *Filters* panel in the WiFi Explorer's *Settings* window. Once created, these filters are added as buttons above the networks table, allowing you to apply filter expressions with a single click.

When creating custom filters, you'll often need to combine multiple filter expressions for greater precision. Logical operators can achieve this.

Logical Operators

Filter expressions can be combined using the **OR** or **AND** logical operators to create even more powerful expressions. For example, to filter networks to show only 2.4 GHz networks with a name (SSID) containing the string *School*, use the filter **24ghz AND School**. To display only networks on channels 1, 6, or 11, use the filter **1 OR 6 OR 11**.

Logical operators are CASE-SENSITIVE.

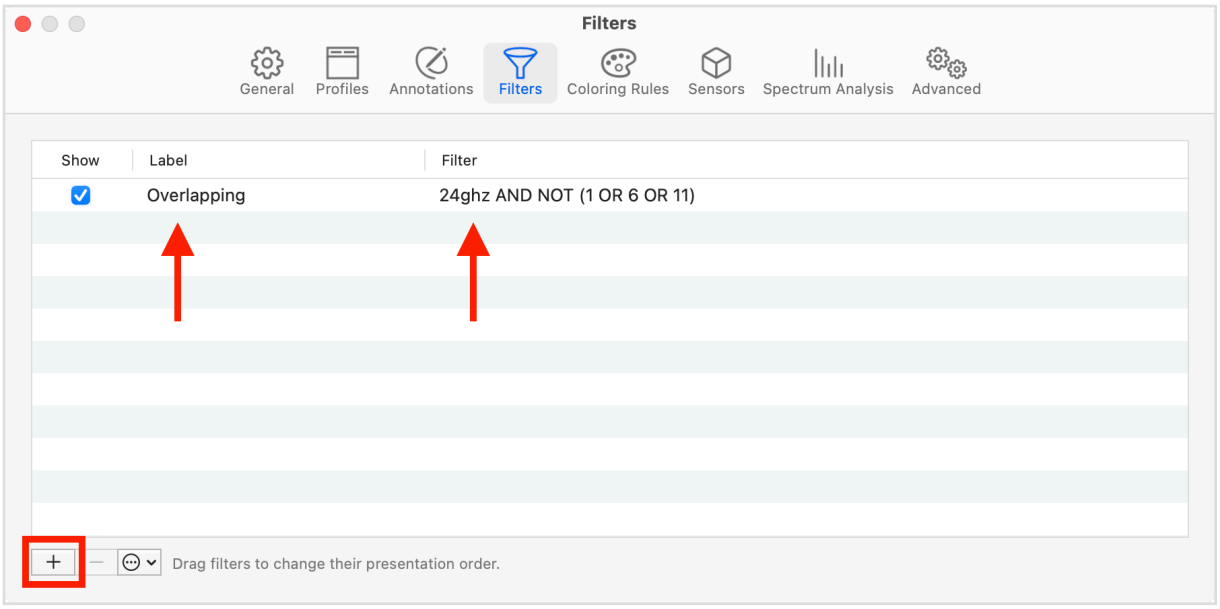
Parenthesis may be used to group filter expressions and change the order of evaluation of the **OR** and **AND** operators. For example, the filter **(24GHz AND 40MHz) OR (5GHz AND 160MHz)** will show 2.4 GHz networks using a 40 MHz channel width or 5 GHz networks using a 160 MHz channel width.

You can also negate filters by using the **NOT** operator. For example, to list all networks that do not have the word *School* as part of their names, enter **NOT School**.

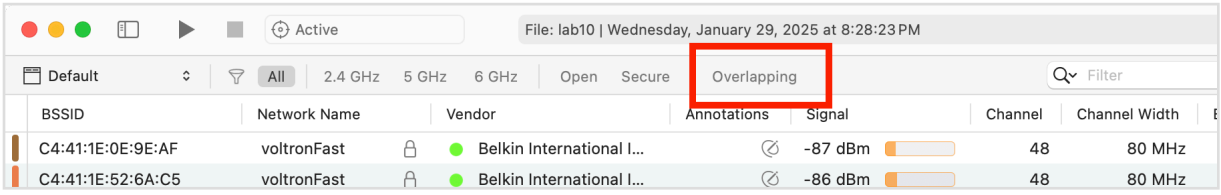
Add a New Custom Display Filter

As an exercise, follow the steps below to create a custom display filter that shows networks using overlapping channels in the 2.4 GHz band.

1. Launch WiFi Explorer and open the file **lab12.pcapng**.
2. *Mac users*: go to *WiFi Explorer Pro 3* > *Settings* in the menu bar, then click *Filters*.
   Windows users: navigate to *File* > *Settings* in the menu, then click *Filters*.
3. Click the **+** button at the bottom of the list to add a new filter.
4. Double-click the *Label* field, type **Overlapping**, then press *Return (Enter* on Windows*)*.
5. Double-click the *Filter* field, type the filter expression **24ghz AND NOT (1 OR 6 OR 11)**, then press Return (*Enter* on Windows*)*.



6. Close the *Settings* window.
7. A new button titled **Overlapping** now appears above the networks table.
8. Apply the custom filter by clicking the **Overlapping** button (only 9 out of 64 networks will be displayed).



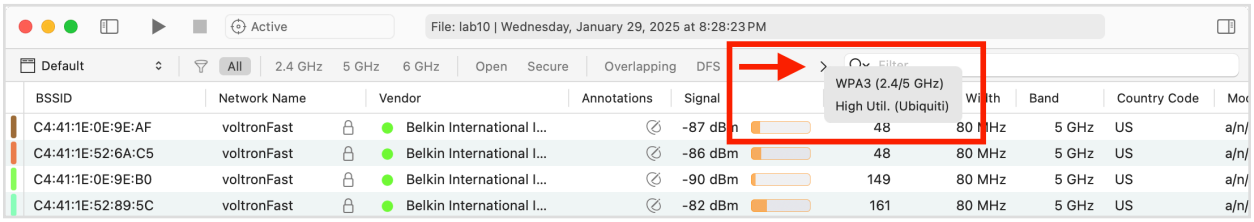
Now, practice adding the custom filters below:

1. Create a new custom filter with the label and filter expression as specified in the table.
2. Verify that, after applying each filter, the number of displayed networks matches the count shown in the table's *Display Networks* column.
3. Check for missing spaces or typos in the filter expression if the custom filter is not working as expected.

	Label	Filter	Displayed Networks
1	DFS	5GHz AND (dot11.net.channel >= 52 AND dot11.net.channel <= 144)	12
2	WPA3 (2.4/5 GHz)	wpa3 AND (24ghz OR 5ghz) AND NOT wpa2	4
3	High Util. (Ubiquiti)	dot11.net.vendor ~~ Ubiquiti AND dot11.net.channel_util >= 20	2

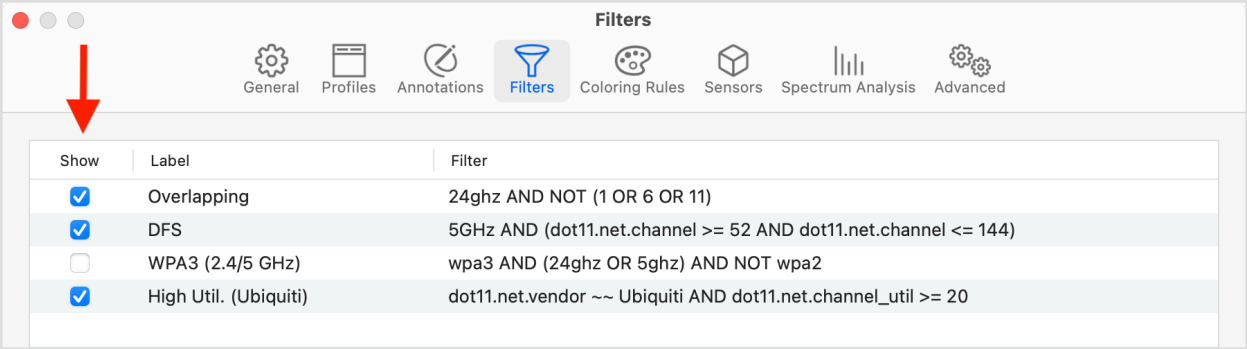
Clicking an active custom filter will deselect it.

If no space is available in the custom filters area, additional filters will appear as a list, which can be accessed by clicking the **>** control next to the filter field.



You can reorder custom filters by rearranging the entries in the list under *Settings* > *Filters* using drag & drop.

You can disable (without removing) a custom filter by unchecking the **Show** field in *Settings* > *Filters*.



Conclusion

In this lab, you learned how to create custom display filters to quickly limit the networks shown in the networks table to those relevant to a particular scenario. You also learned how to use logical operators to combine filter expressions for more precise filters.

References

For detailed insights on information element field-based filter expressions, see *Chapter 10: Data Visualization: Filter Expressions and Display Filters* in *WiFi Explorer Pro 3: The Definitive User Guide*.

Notes

- Quotation marks must be used when comparing values that contain spaces. For example, **dot11.ext.he_oper.6ghz_oper_info.control.regulatory_info == “Standard Power AP"**
- Units (MHz, GHz, dBm, etc.) are optional when comparing numerical values. For example, the filter **dot11.tpc_report.transmit_power >= 23** is equivalent to **dot11.tpc_report.transmit_power >= 23dBm**

< End of Lab >

Lab #13 – Built-in Wi-Fi Captures

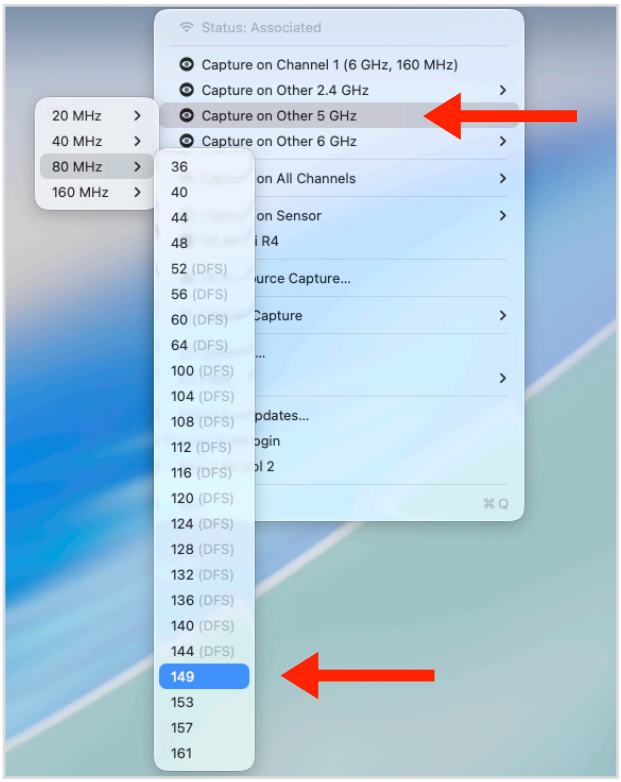
In this lab, you will learn how to capture Wi-Fi traffic using the built-in Wi-Fi adapter on your Mac. Because the adapter already supports monitor mode, capturing traffic is straightforward and requires no additional hardware. The captured frames can then be analyzed in your preferred protocol analyzer, such as Wireshark.

Using monitor mode disconnects the Wi-Fi interface from the network. Airtool will try to reconnect once the capture ends, but you may need to reconnect manually.

Capture on a Single Channel

Single-channel captures can be done by choosing *Capture on* from the *Airtool* menu.

If you want to do a capture using a specific channel and channel width, you must select the desired channel and channel width combination from the *Capture on Other 2.4 GHz*, *Capture on Other 5 GHz*, or *Capture on Other 6 GHz* options in the Airtool 2 menu.

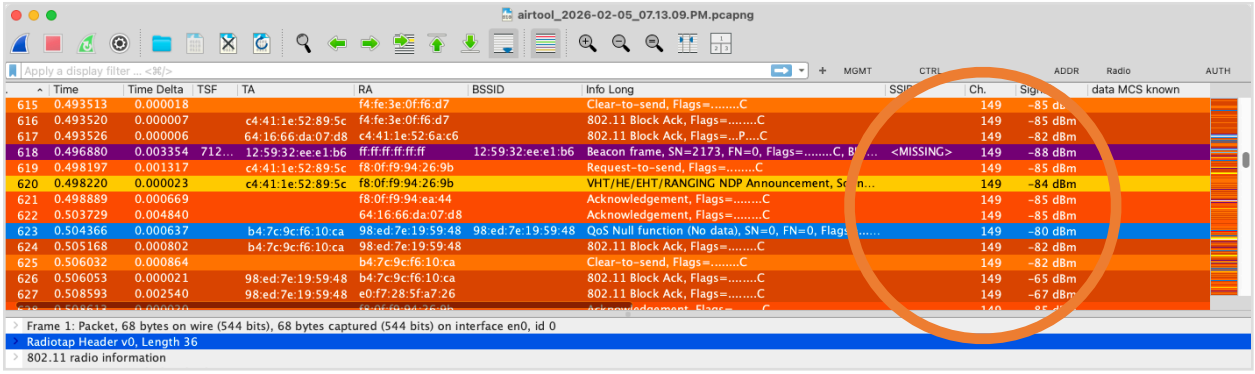


Follow the steps below to capture on channel 149 (5 GHz) and 80 MHz:

1. Click on the Airtool icon to open the menu.
2. Choose *Capture on Other 5 GHz > 80 MHz > 149*.

3. After a few seconds, stop the capture.

4. If configured, Airtool will automatically open Wireshark and display the captured frames.
5. Confirm that the frames were captured on channel 149 (5 GHz).



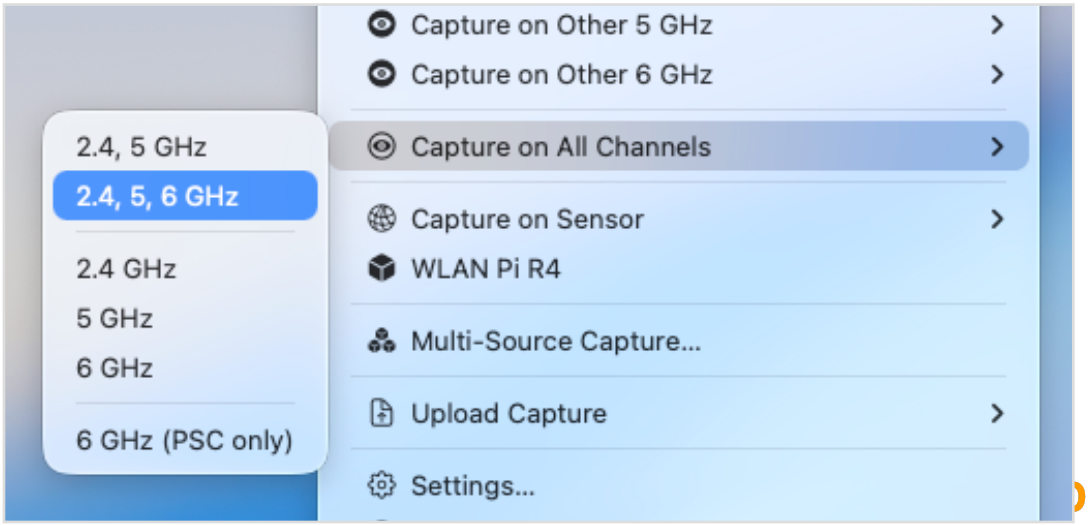
Capture on Multiple Channels

Multiple, non-simultaneous channel captures can be performed by selecting *Capture on All Channels,* then choosing the desired band) from the Airtool menu.

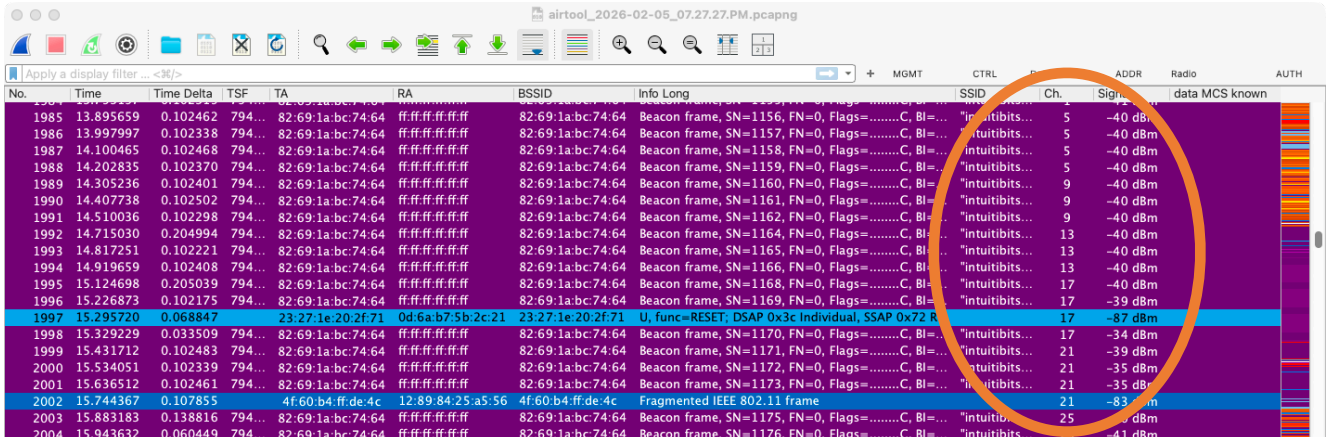
When performing a multi-channel capture, Airtool iterates (hops) over the selected channels with a dwell time of 250 ms. The dwell time is the amount of time Airtool will listen on a channel before switching to the next channel. The channel dwell time can be changed by going to *Settings* > *Advanced*. The minimum dwell time is 100 ms.

Follow the steps below to capture on all bands:

1. Click on the Airtool icon to open the menu.
2. Choose *Capture on All Channels* > *2.4, 5, and 6 GHz*.



3. After a few seconds, stop the capture.
4. If configured, Airtool will automatically open Wireshark and display the captured frames.
5. Confirm that the frames were captured on multiple channels.



Conclusion

In this lab, you captured Wi-Fi traffic using your Mac's built-in Wi-Fi adapter and analyzed the results in a protocol analyzer such as Wireshark. By using the adapter's native monitor mode support, you were able to perform captures without additional hardware.

< End of Lab >

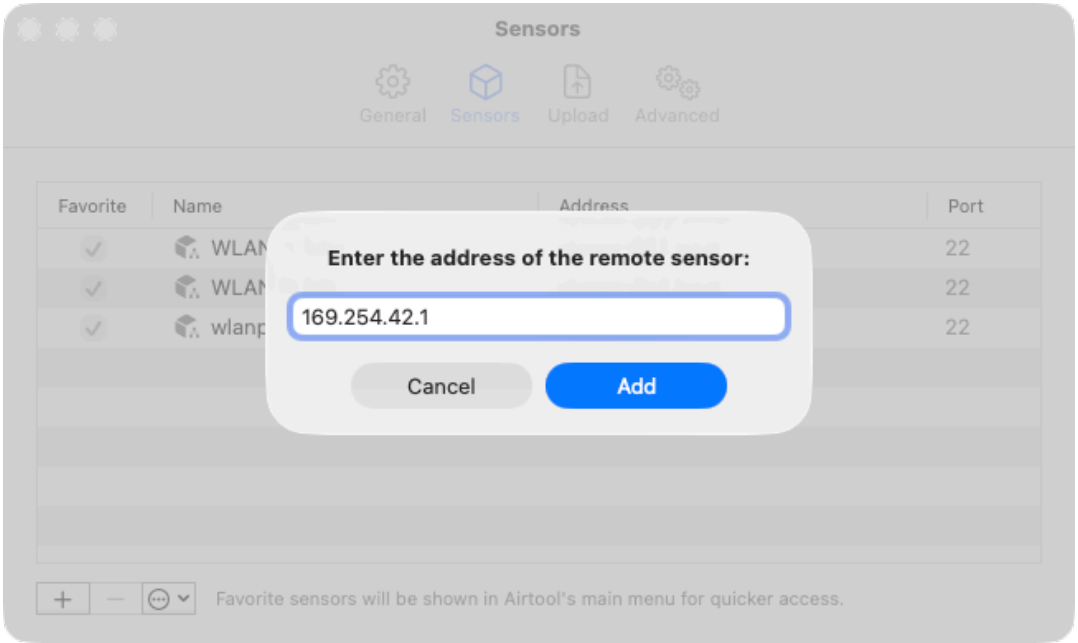
Lab #14 – Remote Sensor Captures

In this lab, you will learn how to capture Wi-Fi traffic using a remote sensor. As covered in a previous lab, a remote sensor is a dedicated hardware device used for external or remote data collection, such as a WLAN Pi, a Raspberry Pi, or any Linux-based system with wireless scanning capabilities.

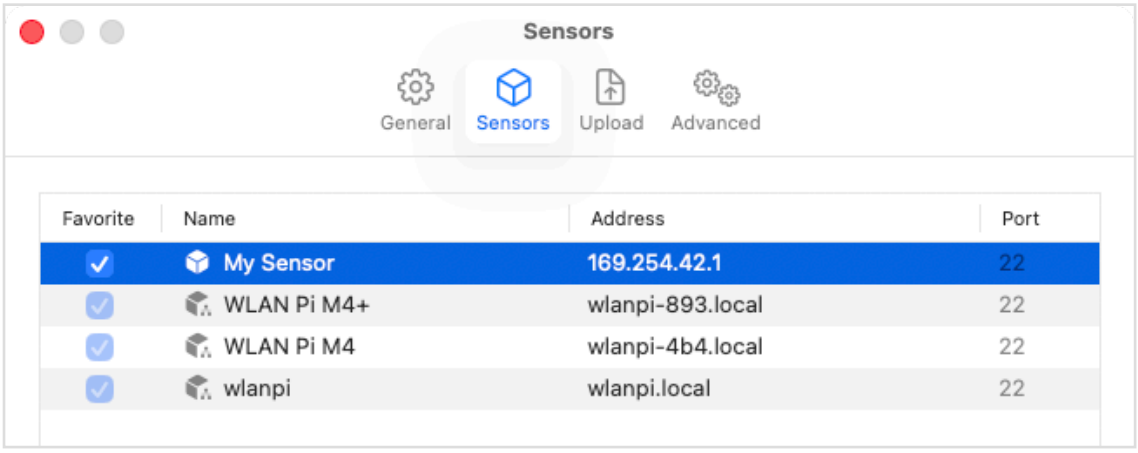
Add a New Remote Sensor

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

1. Click on the Airtool icon to open the menu.
2. Select *Settings* > *Sensors*.
3. Click the "+" button to add a new sensor.
4. Enter the sensor's IP address and click *Add*.



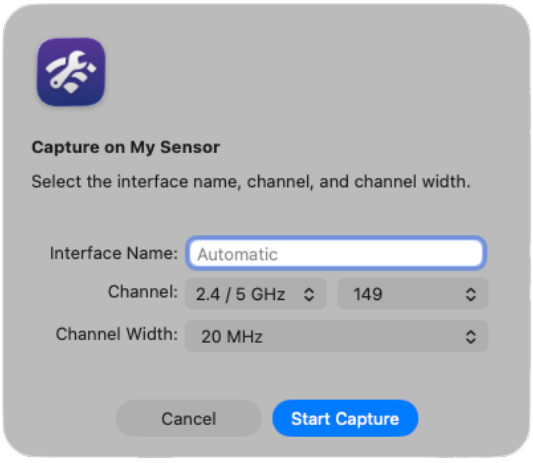
5. Rename the sensor **My Sensor**, then press *Return*.



Use the Remote Sensor

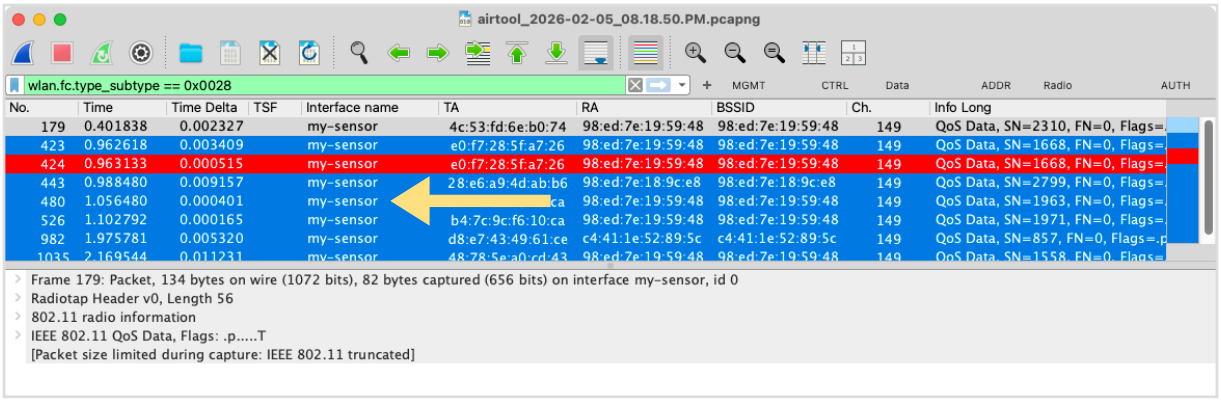
Once added, you can select the remote sensor for capturing. Follow the steps below to start a capture using the sensor:

1. Click on the Airtool icon to open the menu.
2. Choose **My Sensor**.
3. A prompt will appear where you can specify the interface, channel, and channel width.



4. If no interface is specified, Airtool uses the first available interface, which is typically the right choice since most sensors have only one. If the sensor has multiple interfaces, you may need to specify the interface name explicitly, for example, **wlan1**.
5. Select the channel and channel width, and click *Start Capture*.

6. After a few seconds, stop the capture.
7. Open the capture and inspect the **Interface name** column, which should indicate the name of the sensor that was used for capturing.



8. Note that when enabled, frame slicing also applies to remote captures. In fact, the same capture settings, including frame slicing and capture limits, are applied consistently across all capture sources.

Conclusion

In this lab, you learned how to capture Wi-Fi traffic using a remote sensor and how Airtool integrates with external devices to extend capture capabilities beyond the local machine. By using a dedicated sensor, you can perform captures in locations or environments that would otherwise be difficult or impractical to reach, while maintaining the same capture behavior and analysis workflows.

< End of Lab >

Lab #15 – Multi-Source Captures

In this lab, you will learn how to use Airtool 2 to capture Wi-Fi traffic across multiple channels at the same time using multiple sensors and adapters. You'll see how multi-source captures work, how frames from different sensors are merged into a single capture file, and why time synchronization is critical for accurate analysis.

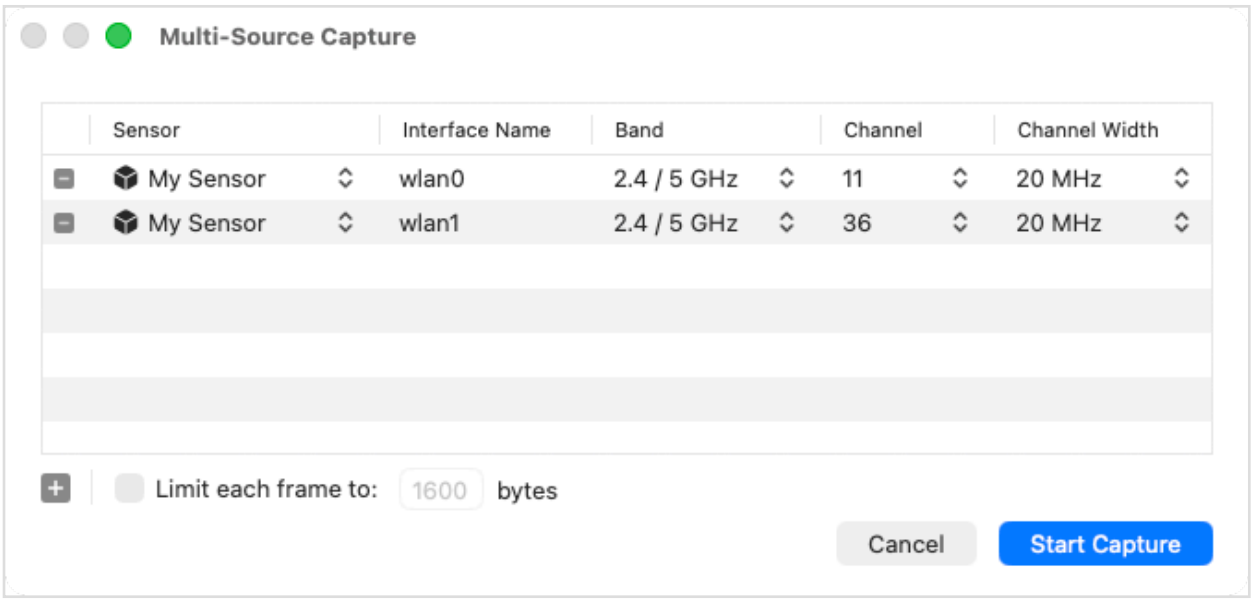
For this lab, you need either one sensor with two Wi-Fi adapters or two sensors with one adapter each. If this setup isn't available, you may skip this lab and complete it later in your own lab environment.

One Sensor, Multiple Adapters

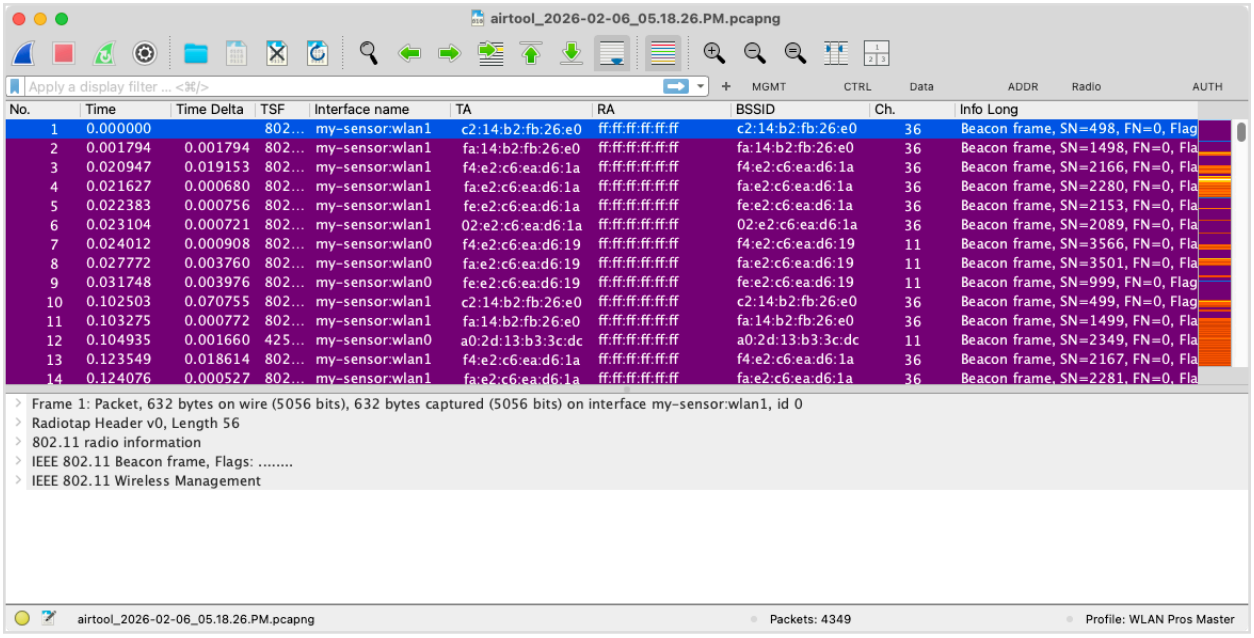
You can capture Wi-Fi traffic on multiple channels simultaneously using a single sensor that supports more than one Wi-Fi adapter. Airtool combines traffic from all adapters into a single capture file.

Follow the steps below to capture on channels 11 (2.4 GHz) and 36 (5 GHz) simultaneously using the **My Sensor** sensor with two Wi-Fi adapters:

1. Ensure your sensor has two Wi-Fi adapters connected.
2. Click on the Airtool icon to open the menu and choose the **Multi-Source Capture**.
3. Click the "+" button to add a second entry and select **My Sensor** for both entries.
4. For the first entry, enter **wlan0** as the interface name and select channel 11 (2.4 GHz).
5. For the second entry, enter **wlan1** as the interface name and select channel 36 (5 Ghz).



6. Click **Start Capture**, wait a few seconds, then stop the capture.
7. Open the capture in Wireshark and confirm that traffic was captured on both channels.



Multiple Sensors, Multiple Adapters

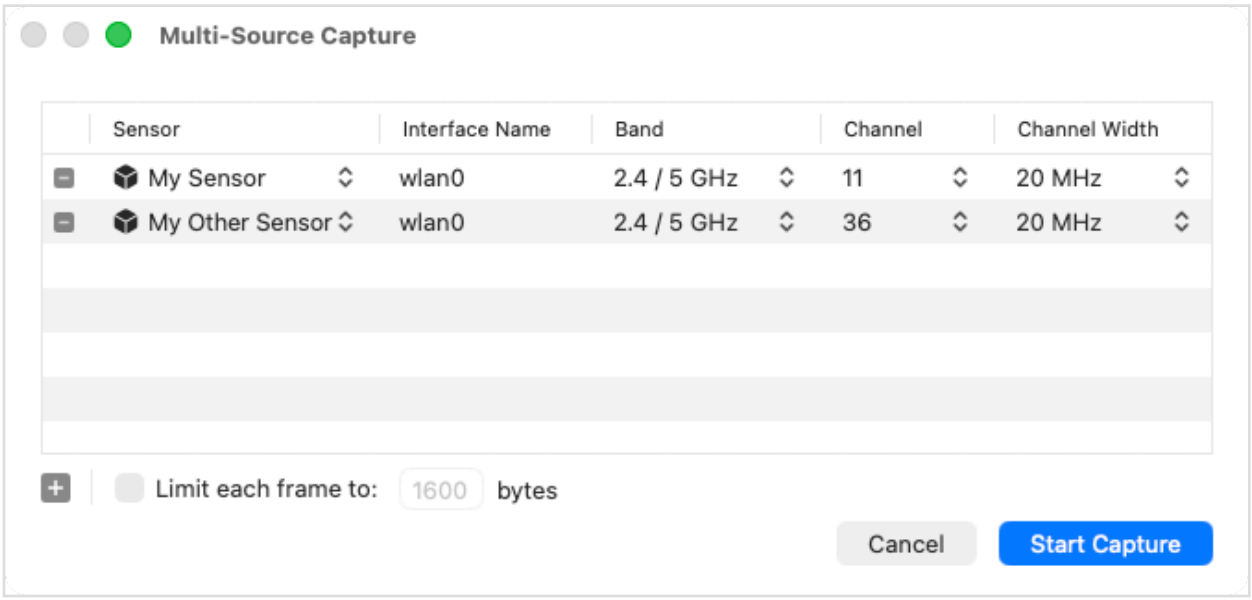
You can also capture Wi-Fi traffic across many channels at the same time by using multiple sensors, each with one or more Wi-Fi adapters. Airtool combines traffic from all sensors and adapters into a single capture file.

This section requires two sensors. If you don't have a second sensor available, you can skip this section and complete it later when one is available.

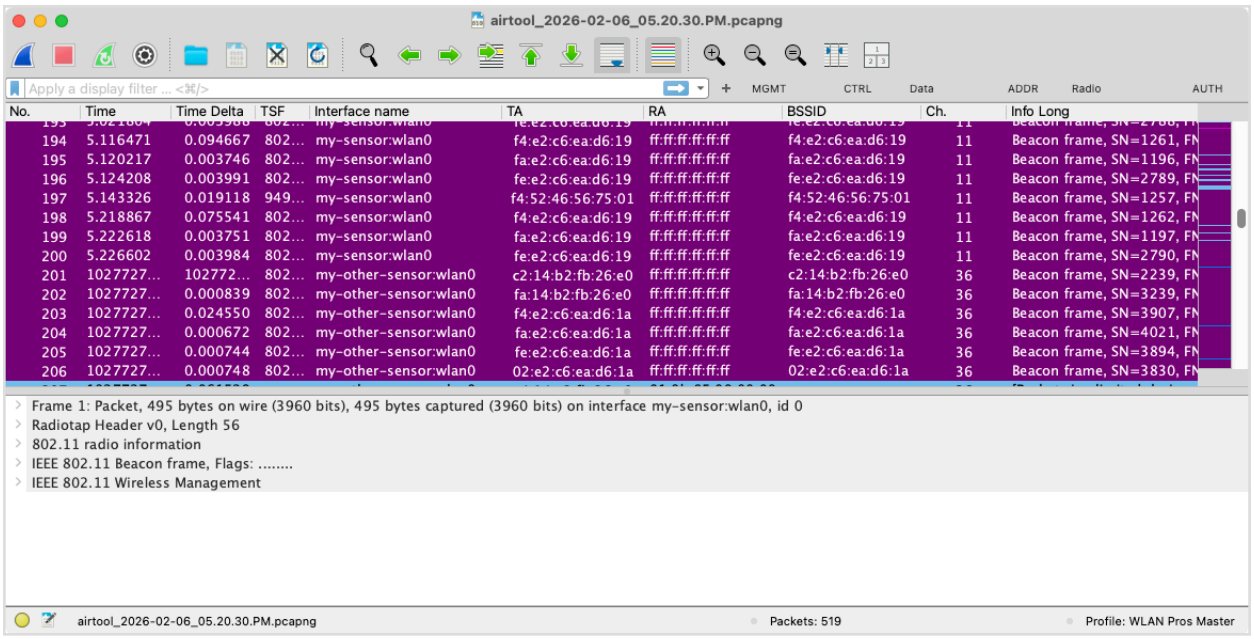
When capturing from multiple sensors, accurate time synchronization is required. Airtool 2 merges frames based on timestamps, so **all sensors must share a common time reference using NTP or another time synchronization mechanism**. Unsynchronized sensors can result in out-of-order frames and unreliable analysis.

Follow the steps below to capture on channels 11 (2.4 GHz) and 36 (5 GHz) simultaneously using two sensors, each with one Wi-Fi adapter:

1. Click on the Airtool icon to open the menu and choose **Multi-Source Capture**.
2. Click the "+" button to add a second entry if needed. If more than two entries are present, click the "–" button to remove the extras.
3. For the first entry, select the first sensor, enter **wlan0** as the interface name (or leave it blank), and select channel 11 (2.4 GHz).
4. For the second entry, select the second sensor, enter **wlan0** as the interface name (or leave it blank), and select channel 36 (5 Ghz).



5. Click **Start Capture**, wait a few seconds, then stop the capture.
6. Open the capture in Wireshark and confirm that traffic was captured on both channels. You can also use the **Interface Name** column to see which sensor and interface captured each frame.



Conclusion

In this lab, you learned how to capture Wi-Fi traffic on multiple channels at the same time using Airtool 2. You practiced configuring multi-source captures with both multiple adapters on a single sensor and multiple sensors working together, and you saw how Airtool 2 merges all captured frames into a single file for analysis. You also learned why time synchronization matters and how to verify capture sources and channels in Wireshark.

< End of Lab >

Lab #16 – Capture Workflow Settings

In this lab, you will learn how to configure capture limits and file rotation to control how capture files are created and managed, how to enable frame slicing to reduce capture size while preserving protocol headers, and how to use live captures with Wireshark to analyze traffic in real time as the capture is in progress.

Capture Limits and File Rotation

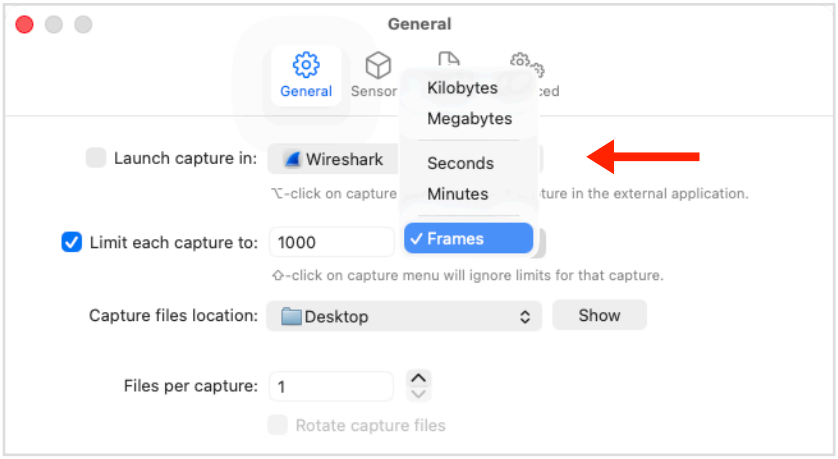
Capture limits and file rotation control how long a capture runs and how capture files are created and managed. Capture limits let you automatically stop a capture based on time or file size, helping prevent unintentionally large captures. When file rotation is enabled, captures are split into multiple files based on the configured size or time limits, rather than being saved as a single large file. This makes captures easier to open, analyze, share, and archive. Together, these settings help keep captures predictable and manageable, especially during long or unattended capture sessions.

Capture Limits

Capture limits allow you to automatically stop a capture based on time (seconds or minutes), file size (kilobytes or megabytes), or number of frames.

Follow the steps below to set a limit of 1000 frames for all captures:

1. Click on the Airtool icon to open the menu.
2. Select *Settings* > *General,* then enable the **Limit each capture to** option.
3. Enter 1000 and select *Frames* as the unit.



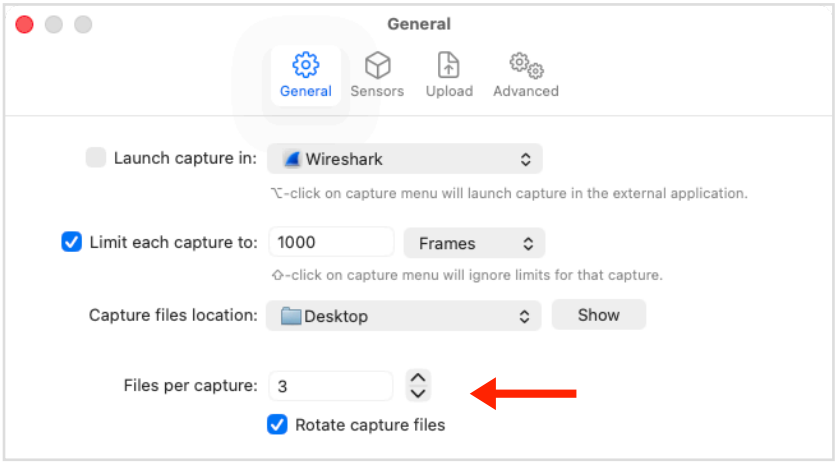
4. Start a capture. The capture will automatically stop after 1000 frames have been captured.
5. Open the capture in Wireshark and verify that it contains exactly 1000 frames.

Files per Capture and Rotation

The Files per Capture and File Rotation settings work together to control how many capture files are created and what happens when that limit is reached. Captures are split into multiple files based on the configured time or size limits, up to the specified number of files. If file rotation is disabled, the capture stops once that number of files is reached. When file rotation is enabled, the capture continues by rotating out the oldest files as new ones are created. Together, these settings help manage disk usage and keep capture files at a manageable size during longer or unattended capture sessions.

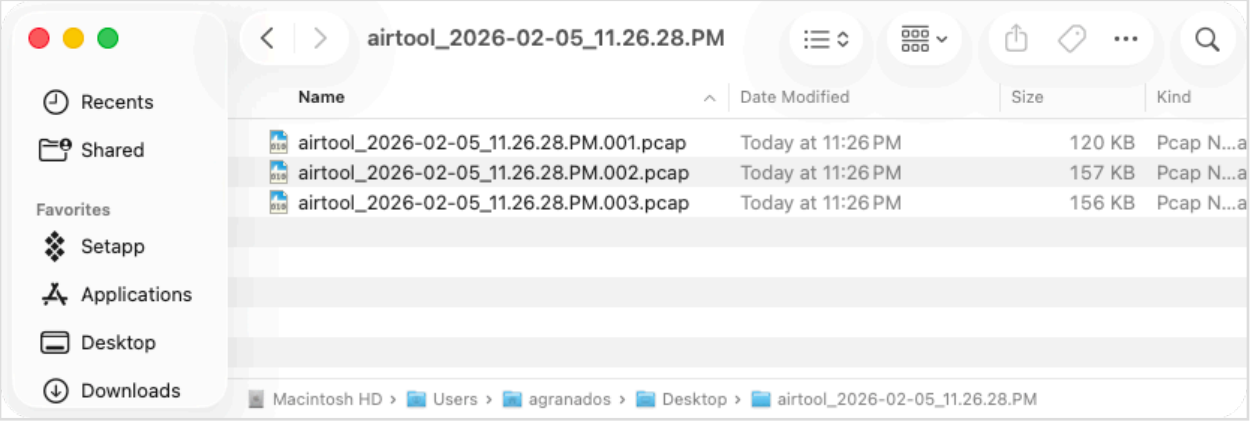
Follow the steps below to enable file rotation with a maximum of three files per capture:

1. Click on the Airtool icon to open the menu.
2. Select *Settings* > *General*.
3. Increase the number of files per capture to three.



4. Enable the **Rotate capture files** option.

5. Start a capture. A new file is created for every 1000 frames captured. Once the maximum number of capture files is reached, the oldest file is replaced.
6. After a few seconds, stop the capture.
7. The capture files are stored in a dedicated folder that contains only the files from that capture session, with each file numbered sequentially.



Frame Slicing

Frame slicing is a capture technique in which only part of each frame is recorded rather than the entire frame. In Wi-Fi captures, the most useful information for analysis resides in the frame headers: addresses, frame type and subtype, sequence numbers, QoS fields, and security-related headers. The payload, which carries user data, is often large and, in most networks, encrypted, so capturing it rarely adds value.

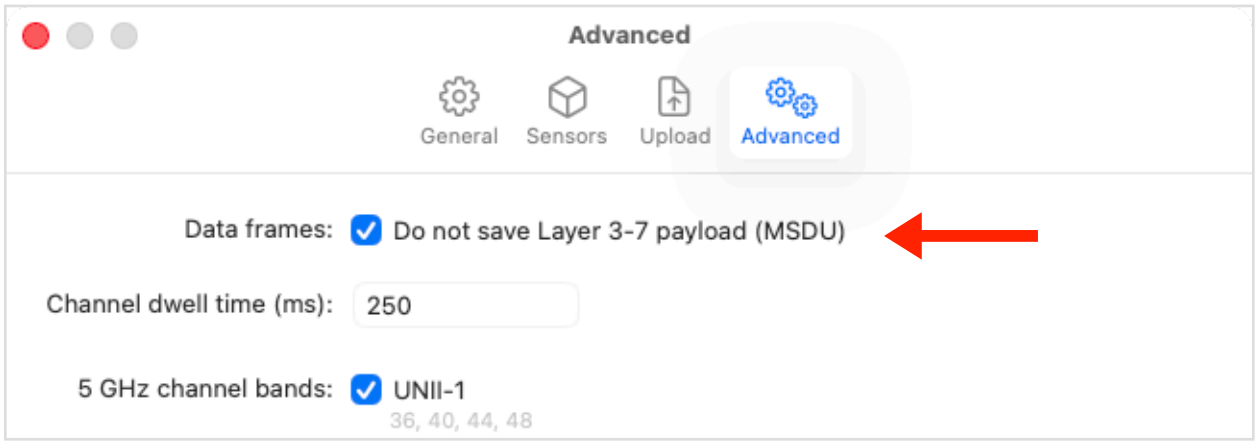
Traditional frame slicing typically works by truncating frames at a fixed byte length. This reduces file size, but it can be imprecise because 802.11 header sizes vary by frame type and enabled features. A fixed slice may cut off important header fields in some frames or include unnecessary data in others.

Airtool takes a different approach. Instead of slicing at a fixed size, it preserves the full set of headers for each frame and discards only the payload. This ensures that all protocol-level information is retained, regardless of how large or complex the headers are, while still keeping capture files compact.

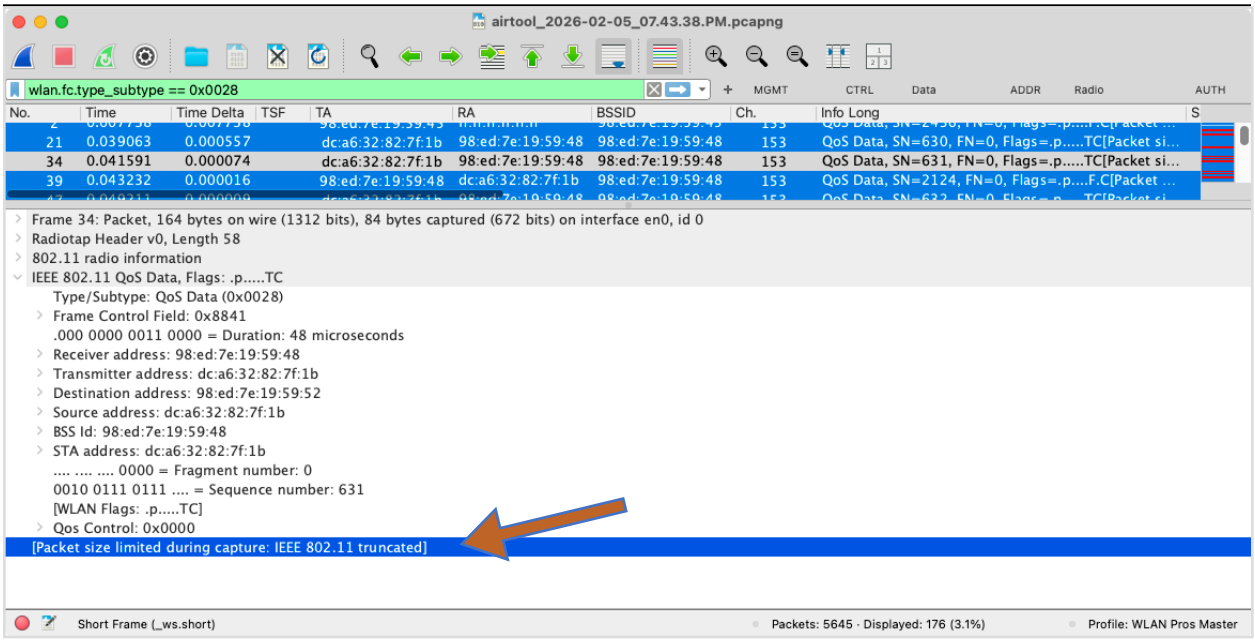
The result is smaller, more efficient capture files that load faster, are easier to share, and remain fully usable for protocol analysis without risking the loss of critical header information.

Follow the steps below to enable frame slicing:

1. Click on the Airtool icon to open the menu.
2. Select *Settings > Advanced.*
3. Enable **Do not save Layer 3-7 payload (MSDU)** to turn on frame slicing.



4. Close Settings and go back to the Airtool menu.
5. Choose *Capture on Channel <channel> (<band>, <width>)* to start a capture on the currently active channel.
6. After a few seconds, stop the capture.
7. Open the capture and confirm frame slicing is in use by inspecting the data frames. You can use the filter **wlan.fc.type_subtype == 0x0028** to display data frames only.



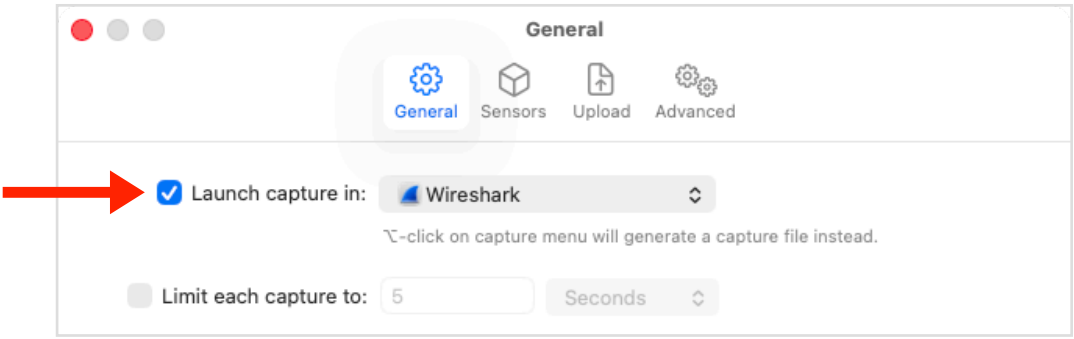
Live Captures using Wireshark

When live captures are enabled, Airtool automatically launches Wireshark and streams frames to it in real time as the capture runs. This allows you to verify capture settings, observe traffic patterns immediately, and adjust channels or filters without waiting for the capture to finish.

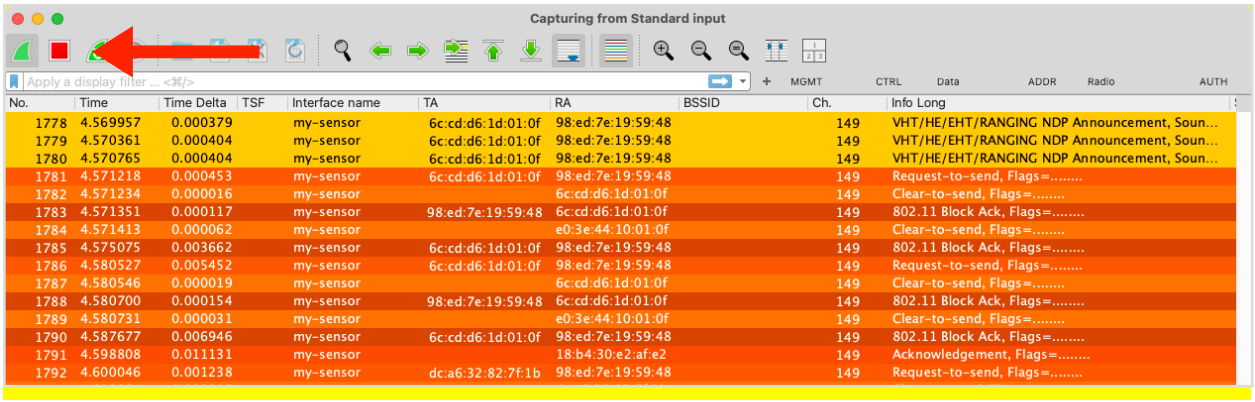
Live captures can be enabled for all captures in *Settings*, or on a per-capture basis by holding the **Option** key when selecting any capture option, including remote sensors.

Follow the steps below to enable live captures for all captures:

1. Click on the Airtool icon to open the menu.
2. Select *Settings* > *General*.
3. Enable **Launch capture in: Wireshark** and turn on live captures.



4. Start another capture using the remote sensor. Wireshark will open automatically and display the capture in real time.
5. After a few seconds, stop the capture by clicking the **Stop** button in Wireshark.



Note that when using live captures, Airtool does not generate a capture file. You can choose to save the capture from Wireshark or discard it.

Conclusion

In this lab, you learned how to control how captures are recorded, stored, and analyzed by configuring capture limits, file rotation, and frame slicing, and by using live captures with Wireshark. Together, these settings help keep captures manageable, reduce unnecessary data, and make it easier to analyze traffic as it is captured, whether you are troubleshooting interactively or running longer capture sessions.

< End of Lab >