MetaGeek App User Guide

support.metageek.com/hc/en-us/articles/16676518627735-MetaGeek-App-User-Guide

Logo

An Introduction to MetaGeek App (formerly Chanalyzer 6)

MetaGeek App was formerly released as Chanalyzer 6. As spectrum analysis capabilities were added to the Wi-fi troubleshooting tool, it became clear that the best channel analysis includes both Wi-Fi traffic and Spectrum Analyzer data.

MetaGeek App adds an incredible amount of visibility into Wi-Fi client behavior (or misbehavior) on wireless networks. It is no longer limited to spectrum data.

Most Wi-Fi performance issues are related to RF signal and Wi-Fi congestion. MetaGeek App is a fantastic tool to understand channel congestion as it sees all Wi-Fi traffic.

Getting Started

MetaGeek App requires at least one packet capture adapter. MetaGeek recommends using 3. The network adapters that MetaGeek App can leverage are standard, off-the-shelf USB Wi-Fi adapters, but they use a special packet capture driver to perform full packet capture.

To capture from a spectrum analyzer, plug in a supported adapter.

Supported Adapters

MetaGeek App supports several standard, off-the-shelf Wi-Fi adapters. You can bring your own adapter(s), or purchase adapters from MetaGeek or a MetaGeek Partner.

- MetaGeek App Supported Packet Network Capture Adapters
- Spectrum Analyzer WiPry Clarity
- Spectrum Analyzer Wi-Spy Lucid
- Spectrum Analyzer Wi-Spy DBx

Setting up MetaGeek App

Directory for Temporary Capture Files

MetaGeek App saves live capture data to a temporary file. This directory can be changed in the preferences. The preference window will also display the percentage of available space on the hard drive.

Network Requirements

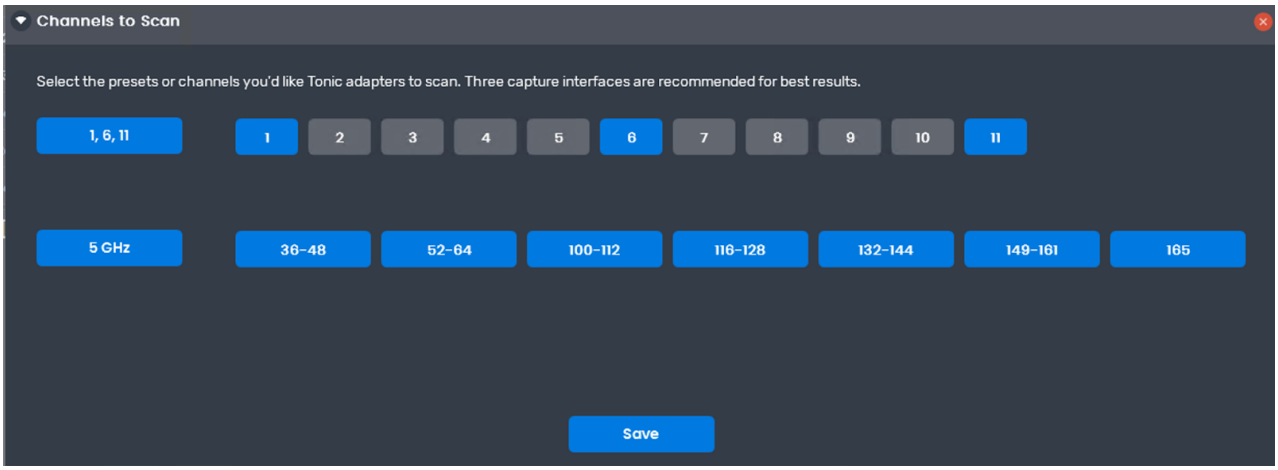
The values in the preferences are intended to allow users to define what thresholds are appropriate for their organization. The thresholds determine what will show up as an event in the capture navigation or at what point a bar graph will change from green to red.

Some of the values will require a persistent level in which the average exceeds the threshold for 15 seconds.

Channel Selection

The Channels to Scan allows the user to exclude channels from the list that the USB NIC cards scan. It is recommended to match the channels used by the organization. For example, if your organization has a 5 GHz SSID that you are troubleshooting, click on any blue boxes in the 2.4 GHz section to update.

The large buttons on the left hand side will toggle between custom presets and all channel or band enabled.



Clicking “Save” will start a new capture.

Capture Operations

It is possible to leave MetaGeek App recording with a computer set to not idle. The software will store the captures in the temporary directory and then create a new file every hour. The software will display a prompt to save or discard the capture. If the prompt is not responded to in 5 minutes it will save the file and continue with the next capture.

By default MetaGeek App automatically stores captures in a temporary .pcap directory. As the user captures, it writes the data to a .pcapng

Your First Capture

To begin, connect one to three supported packet capture adapters, and launch MetaGeek App. As MetaGeek App launches, it will swap out the packet capture adapter's default driver for the special packet capture driver.

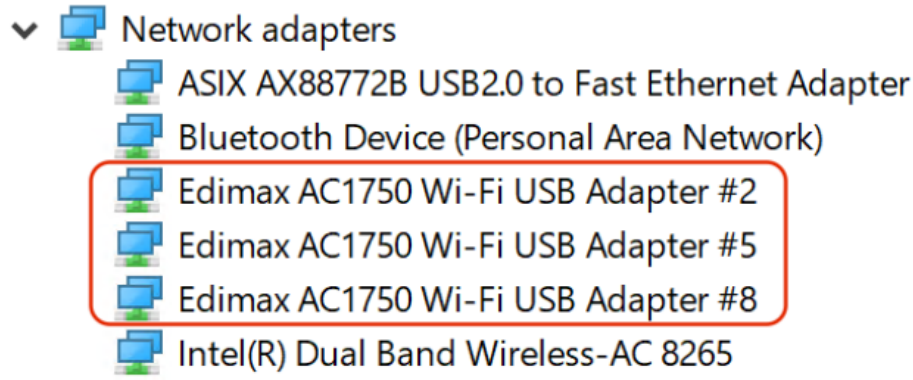
Note: While MetaGeek App does support hot plugging and hot unplugged packet capture adapters, hot plugging adapters can sometimes cause unexpected results. This is especially true when mixing adapter models. As a result, we generally recommend connecting all desired adapters before launching MetaGeek App.

A Wi-Spy can be connected to provide spectrum analysis data of the 2.4, 5, and 6* GHz bands (*requires Lucid).

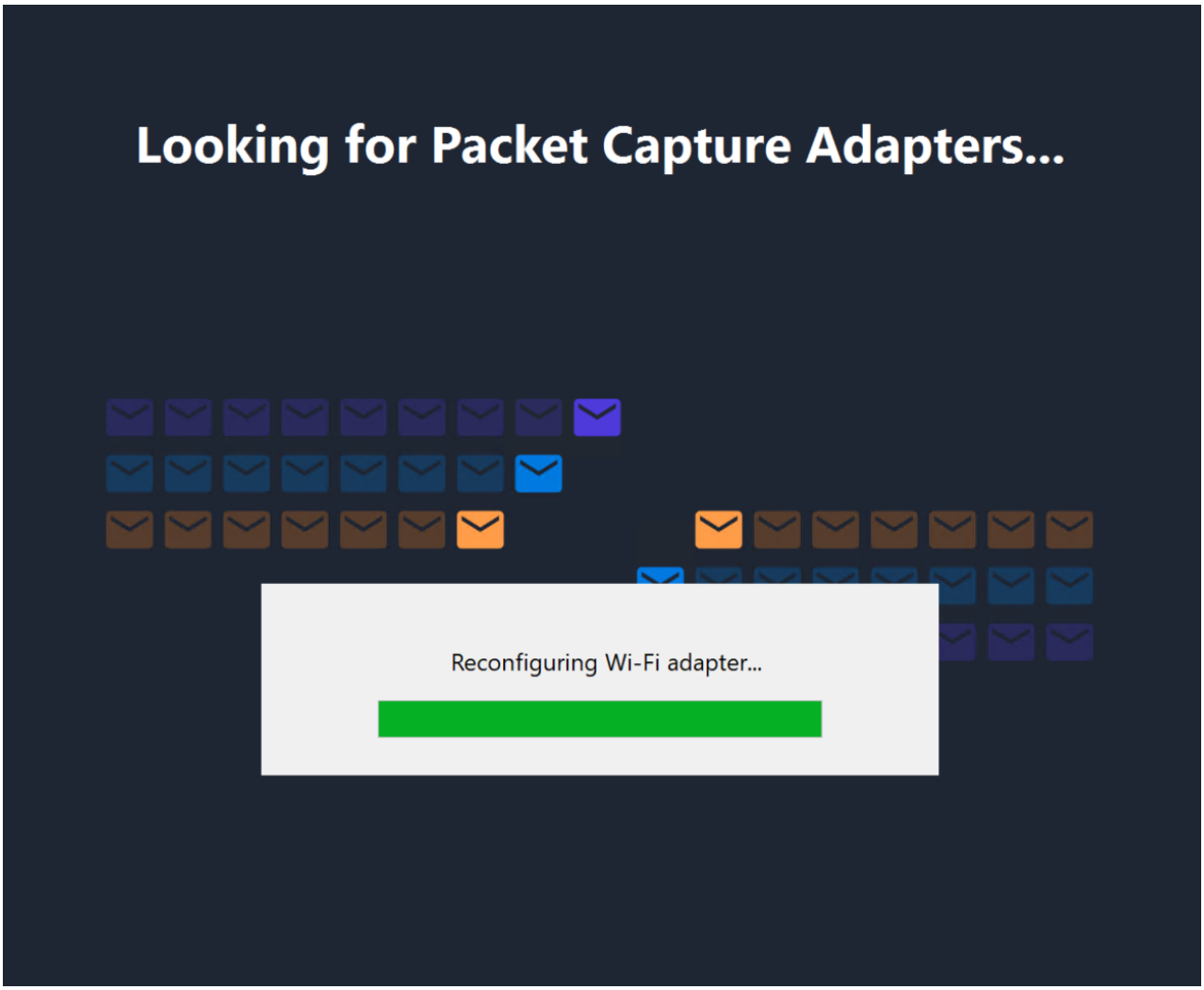
Driver Installation

To perform packet capture functions, MetaGeek App installs a special packet capture driver for each supported adapter. This process happens automatically when MetaGeek App launches, and is why MetaGeek App requires Administrator privileges.

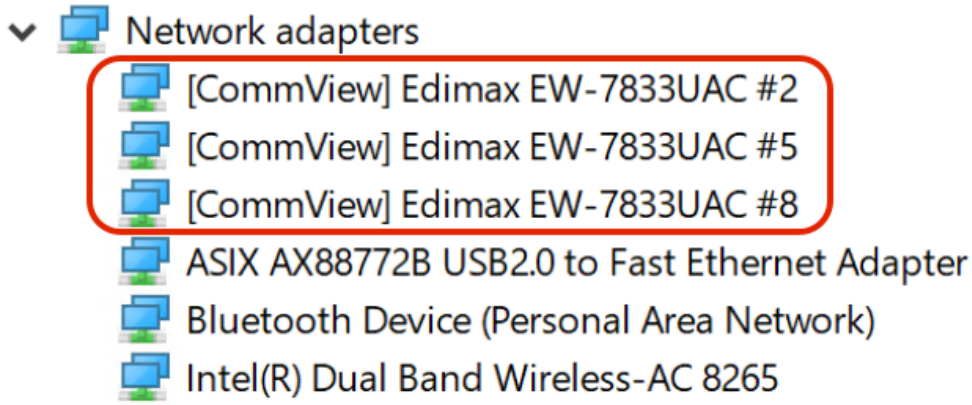
Before MetaGeek App launches, supported packet capture adapters will either have no driver installed, or a standard driver.



While MetaGeek App launches, a "Reconfiguring Wi-Fi adapter..." progress will appear while the special packet capture drivers are installed.



For the rest of the user session, Windows Device Manager will show that the special packet capture driver has been installed.



When the user session concludes and MetaGeek App is closed, it will uninstall the special packet capture drivers, and reinstall the standard driver (if available).

Troubleshooting Packet Capture Adapters

If you experience issues where supported packet capture drivers aren't detected, or MetaGeek App is stuck at "Looking for Packet Capture Adapters...", consult the packet capture adapter troubleshooting guide.

Packet Capture Adapter Troubleshooting Guide

Navigation

Basic Layout

- Navigation Breadcrumbs
- Status Pane
- Navigation Table
- Visualization Pane
- Details Pane
- Time Graphs Pane

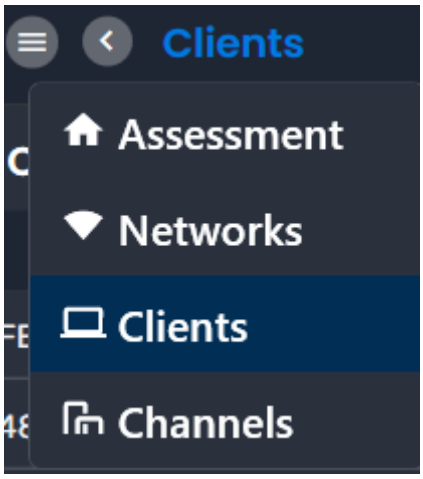
Navigation Menu

At the top level, MetaGeek App has four views. Some of the views are dependent on what adapters are plugged in.

- **Assessment** provides a snapshot of the current thresholds , events and nearby devices to help the user drill down to a network, BSSID, or a client .
- **Networks** shows a list of all of the networks, or ESSIDs, that have been observed. This will aggregate radios broadcasting the same network name. To see radios double click on the network name.
- **Clients** shows all of the client devices that have been observed
- **Channels** lists Wi-Fi channels, and details about them

From the Networks View, the user can enter the Navigation Breadcrumbs, and drill down through:

- Networks View
- ESSID View
- BSSID View
- Client View



Status Pane

The Status Pane shows how many packet capture adapters are connected, if a spectrum analyzer is connected, and how much system memory MetaGeek App is consuming.

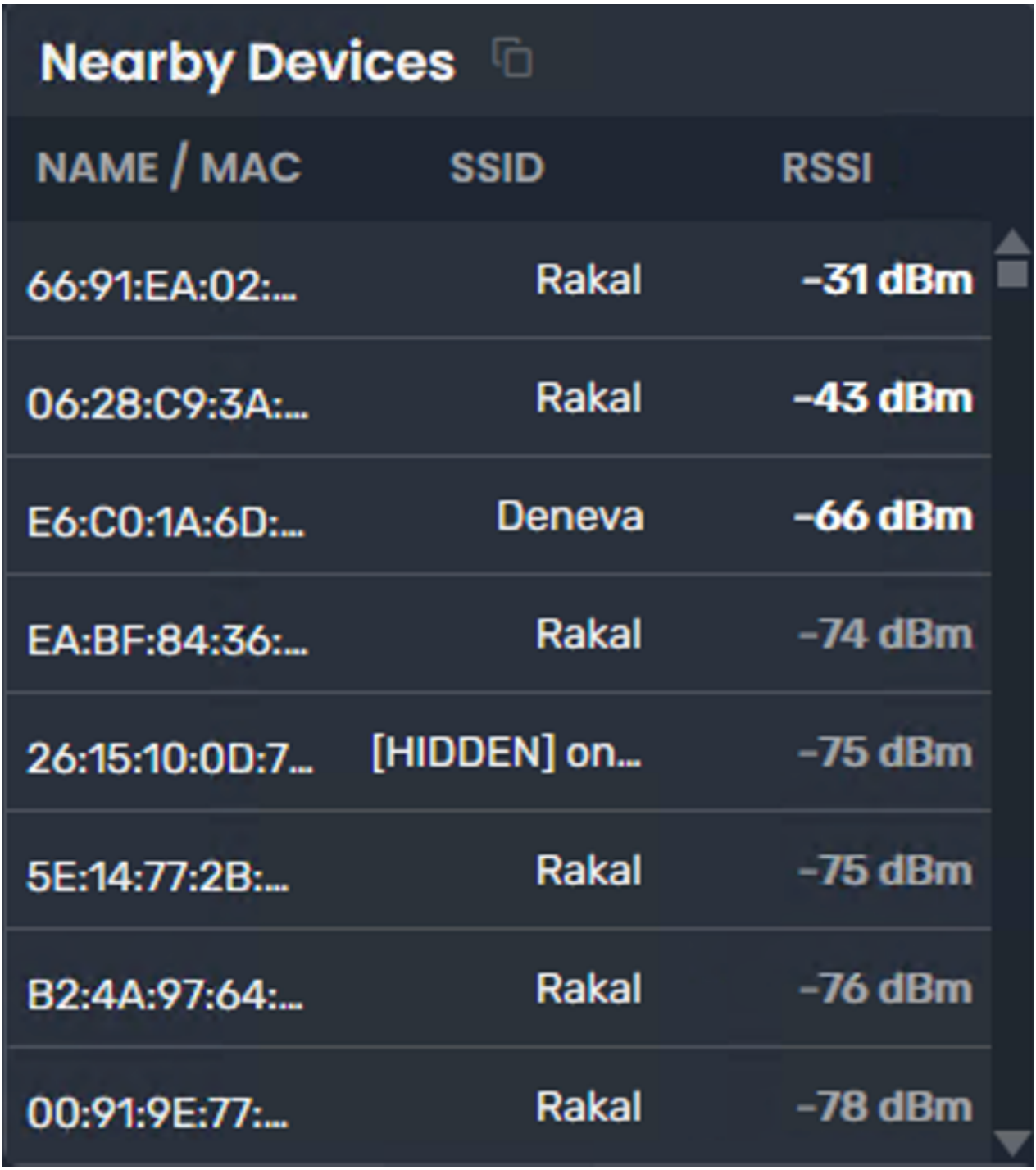
Each packet capture adapter receives a unique color (indicated by the dot), which is used to identify that adapter's influence elsewhere in MetaGeek App.

Assessment Page

Nearby Devices

Sometimes a device will be connected to the wrong network. This table is sorted by device received signal strength. The devices nearest to the MetaGeek App capture interfaces will be near the top.

This table is intended to help find the device to follow and troubleshoot.



Clicking on a MAC address will open the client details page. Clicking on the SSID will open up the BSSID that the client is associated with.

Thresholds

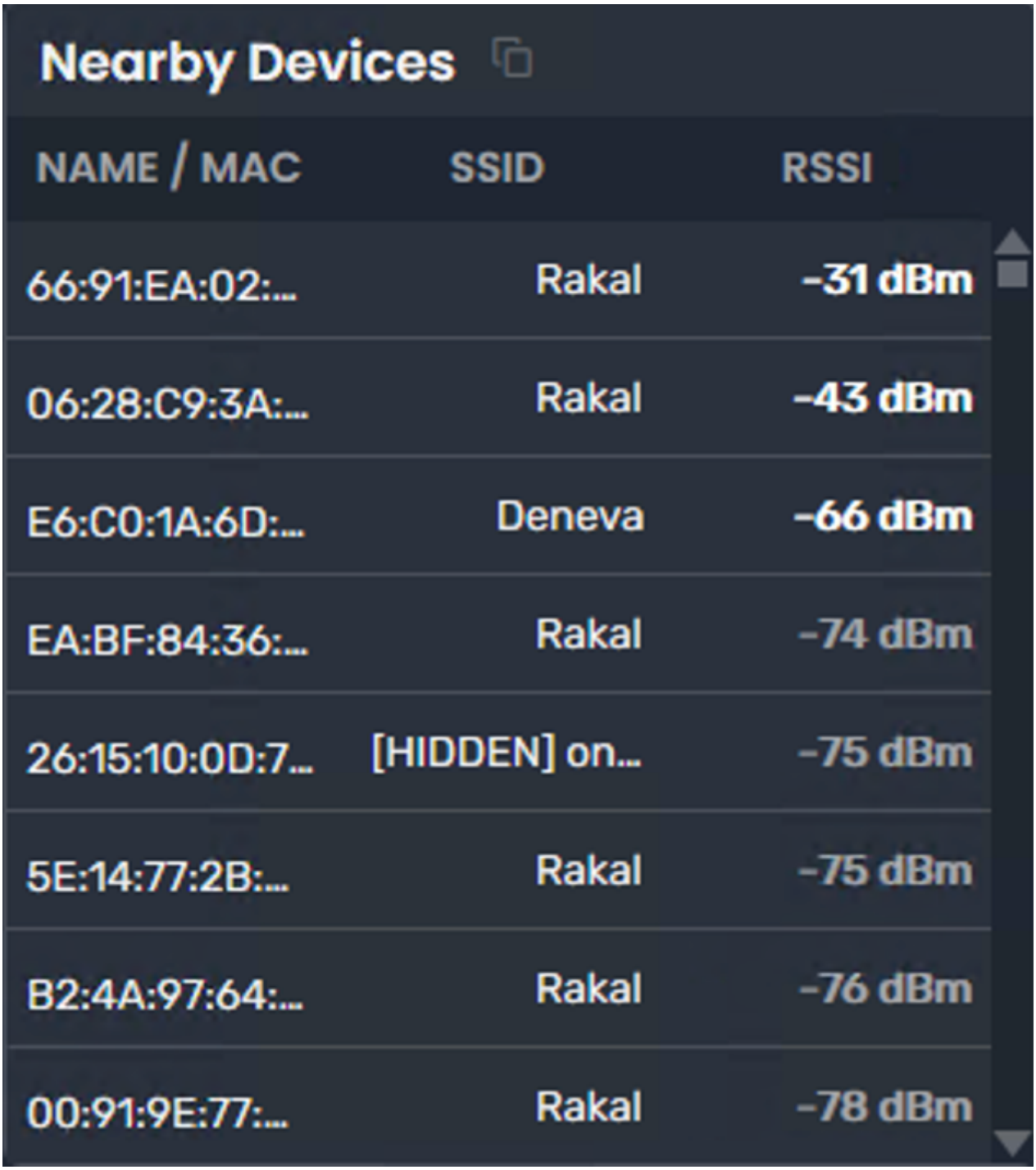
When a network is selected, the tool will use the selection to update all of the panes in the Assessment Page View.

This graph is a measurement of the BSSID with the strongest signal strength, client count of the BSSID, and the airtime of the channel it is on. If another BSSID becomes the strongest RSSI, MetaGeek App will start graphing it when it is 5 dB higher.

If a previously selected network is detected in a capture, it will automatically be selected in the thresholds pane.

To change the network selected, click the refresh button and select the next network.

Clients per Channel



Clients per Channel is a visual representation of how many client devices per channel. At the top is the total clients on a channel. Any 2.4 GHz channels will be purple, while 5 GHz will be colored green. If you see a purple bar graph in the top, this may be justification for an investigation.

Underneath is a measurement of the peak airtime, which is intended to help understand the “burstiness” of the devices on a channel. In the time span selected, the top quartile of airtime measurements were above the percentage displayed.

For example, if Peak Airtime is at 15%, it means that the channel was busier than 15% in a quarter of the measurements MetaGeek App took.This measurement will match the top part of the box and whisker plots on the network page.

Client Statistics

The client statistics graph highlights the capabilities and performance of client devices seen by MetaGeek App. Purple slices indicate 2.4 GHz. Green represents 5 GHz. These pie charts will change if a network is selected in the thresholds.

The Band pie chart shows the band that a client device is currently connected on.

The Retry pie chart graphs the retry percentage for all client devices.

Events

Events displayed on the Assessment Page will be related to the network selected in the Thresholds pane.

The events that will appear on the assessment page will all be related to the network selected, or the channels that the network uses.

AP/BSSID Related Events

MetaGeek App intends to minimize the amount of alerts and noise generated by its event detection. There are two primary components to this. ESSID and BSSID Signal Strength.

The user must select an ESSID in the threshold for Events to appear in the Event history. If an ESSID matches the previously selected ESSID, it will auto-populate using it.

MetaGeek App is always calculating the signal strength all BSSIDs sharing the same network name. MetaGeek App will generate events for the top 5 BSSIDs

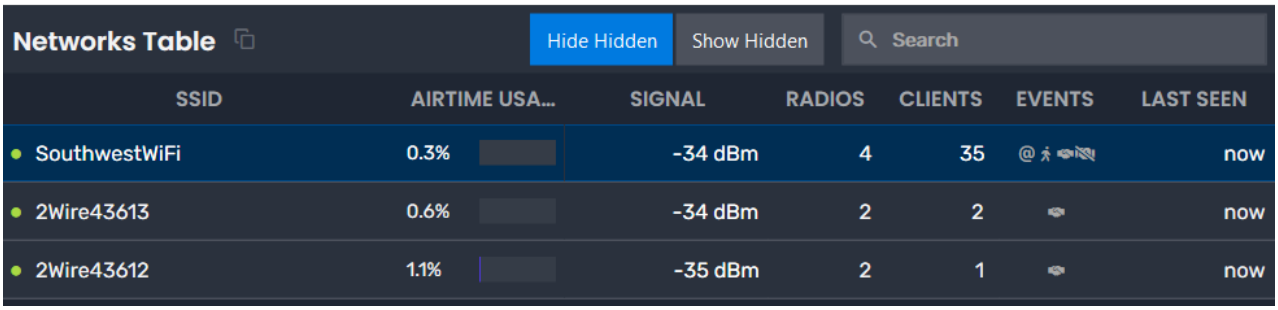
Event Details

Event Name	Icon	Type	Metrics
Inadequate Signal Strength Coverage		Network	ESSID signal strength drops below network requirement value for 5 seconds. This is only triggered for the top 5 strongest BSSIDs that share the selected ESSID.

Channel Airtime Exceeds Threshold		Channel	Average Channel Airtime exceeds threshold value set in network spreferences for over 15 second period of time. Identify APs affected. This is only triggered for the top 5 strongest BSSIDs that share the selected ESSID.
Excessive AP Retries		BSSID	Channel Airtime for BSSID exceeds 5%, and all retries for all traffic exceed the threshold. This is only triggered for the top 5 strongest BSSIDs that share the selected ESSID.
High Channel Overlap		Network	APs with same SSID that are on the same channel above threshold set in network preferences. This is only triggered for the top 5 strongest BSSIDs that share the selected ESSID.
Clients roaming to 2.4 GHz		Network	Clients associated to ESSID and were previously detected on 5 GHz, but are now on 2.4 GHz. Event can only only occur every 5 minutes. Devices will be aggregated to the most recent event with this title.
Excessive Probe Requests		Network	When Channel Airtime is above 10% and probe responses make up more than 30% of that total airtime.
Successful8021X		Client	When the application detects a new BSSID, EAP Data frames followed by data frames.
Failed8021X		Network	When the application sees a failed response code, or is unable to detect data frames after an authentication attempt.
FailedConnection		Network	
Successful Connection		Client	A client has successfully connected to an open network.

Networks View

Networks is a list of all of the ESSIDs captured by the Wi-Fi interfaces in use by MetaGeek App. If the user has selected to scan a limited range of channels, the networks table may not display all networks in the environment in the same way that inSSIDer does.



Airtime Usage Definition

The worst/highest airtime of all BSSIDs, value and graph match.

Clients View

The Clients View shows any clients within range of your adapter, including clients that are unassociated or associated to a neighboring network. Clicking on a client will drill down into more details (see Client View below).

Client	MAC address or the Alias provided by the user.
Network	The name of the network the client is currently associated
Events	Events or changes MetaGeek App detected for the client MAC address
Signal	The received signal strength. This is how loud the network interface card heard the client device transmit. Based on proximity to the client, this is most likely different from how loud the client hears the Access Point.
SNR	The Signal To Noise Ratio reported by a client device to the Access Point. This is the best indicator of a client device's health. The higher the number the better. As a general rule anything below 15 is poor.
Retry	The percentage of frames that have a flag indicating that it is a retransmission.
Channel	The channel the client device was last seen on.
Channel Airtime	The percentage of the airtime the client device has consumed in the time frame.
PHY Type	The 802.11 standard currently used by the BSSID.
Percentage of BSSID	The percentage of the BSSID traffic associated with the client.
Capabilities	Currently identifies 802.11 k, v and r from the association frame.
Last Seen	The last time MetaGeek App received a frame sent by the client device.

Channels View

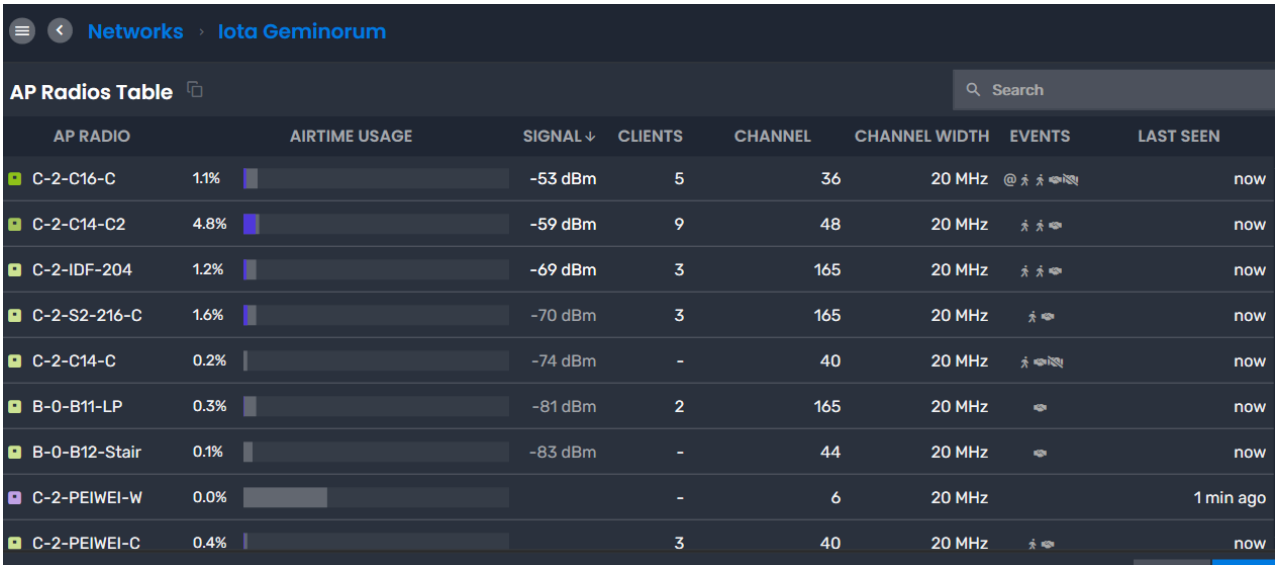
The Channels View will display all relevant information for each channel in the 2.4, 5 and 6 GHz bands. This is helpful for understanding which channels are at capacity, or which channels are the most clear. To sweep 6 GHz spectrum with the WiPry Clarity or Wi-Spy Lucid, see this article here.

Channel	Wi-Fi channel
Spectrum Utilization	Only available with a Wi-Spy attached. How often RF activity is occurring on the channel, or how often the channel is being "Utilized"
Airtime Usage	Current Airtime utilization taken up by Wi-Fi devices (dark purple) compared to total available airtime on the channel (gray)
Highest Utilization	Indicates which ESSID is taking up the most airtime on that channel

Legacy Present	Indicates whether an 802.11b device is present on the channel

Network View (ESSID)

The first "drilldown" from the Networks view by clicking on a network name (ESSID). This view will display the radios or BSSIDs underneath the selected ESSID. This view is helpful to understand client distribution per radio.



Airtime Usage	Airtime of BSSID traffic. Bar chart graph is BSSID (purple) and other networks on same channel (gray).

Network Radios View (BSSID)

The second "drilldown" from the Networks view by clicking on a radio or BSSID. This view will display a table of all clients connected to the radio, an Airtime Usage treepie, and AP Radio Details.

Airtime Usage	Value is of client radio's airtime per channel. Bar chart is the percentage of traffic within BSSID. client percentage (purple) other clients on bssid (gray).
Channel Airtime	There are two types of air time. Airtime that comes from the BSSID that is transmitting and all the clients . The next type of air time is traffic that is on the same channel but comes from other BSSIDs. If the traffic comes from another radio that is broadcasting the same network name or ESSID MetaGeek App will describe it as an extended network. The neighbor network is a network that does not broadcast the same ESSID but is transmitting on the same channel as the BSSID in view.

AP Radio Details Pane

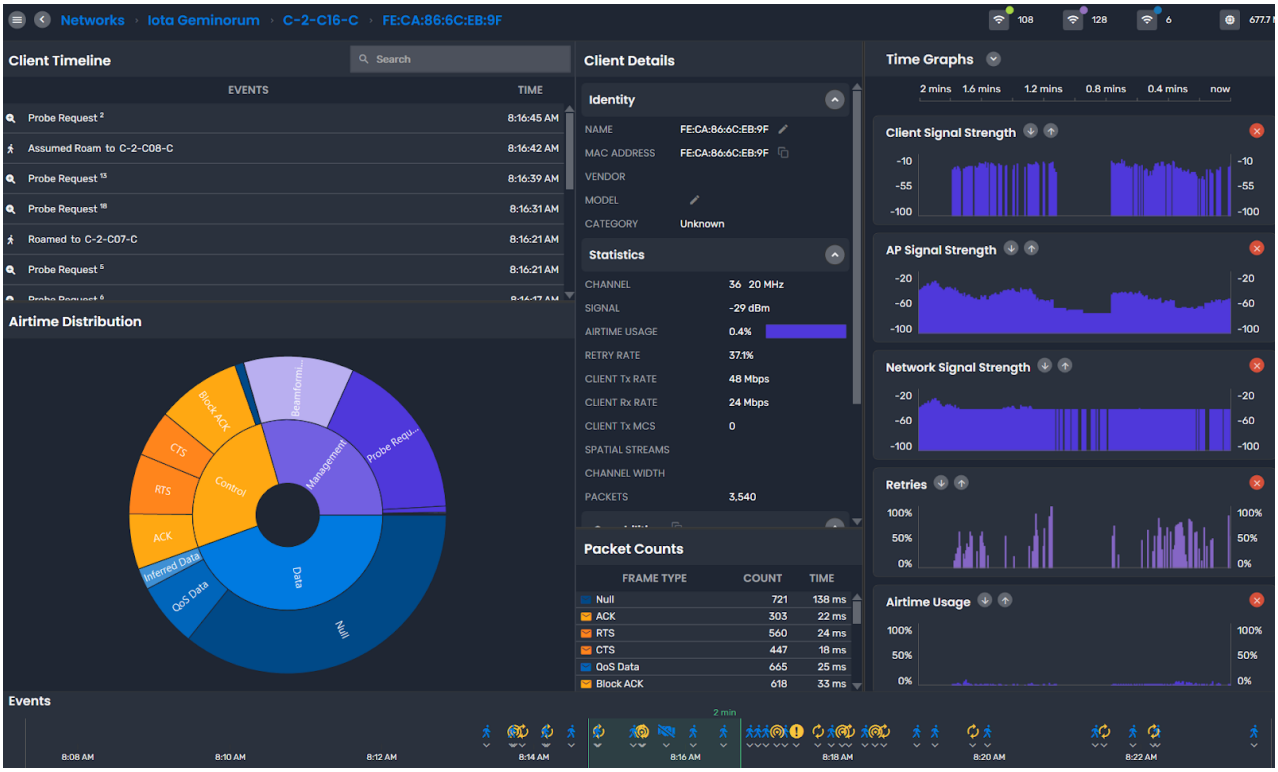
In the AP Radio Details Pane, you can find live information about the client.

IDENTITY	
SSID	The network name that the BSSID is broadcasting
Access Point	The device name being broadcasted by the AP, or AP alias. Click the pencil icon to alias the radio.
MAC Address	MAC address of the radio
Vendor	AP vendor
Model	Model of AP - select the pencil icon to enter / edit AP model
STATS	
Signal	Current signal strength of radio in dBm
Airtime Usage	Current Airtime utilization the radio is taking up (darker purple) compared to total utilization the AP is taking up (light grey)
Channel Airtime	How much airtime all networks are taking up compared to the total airtime available on the channel
Spectrum Utilization	Only available with a Wi-Spy attached. How often RF activity is occurring on the channel, or how often the channel is being "Utilized".
Clients	Number of clients picked up by the adapter
CONFIG	
Channel	Current channel of the radio and its channel width
Security	The security protocol that the access is configured to support
Basic Rates	Shows min supported data rates (slower data rates fly farther, but cause more channel utilization)
Country	Country config currently being used
CAPABILITIES	
PHY Types	Phy type
Generation	Wi-Fi Alliance generation designation
Max Data Rate	Maximum supported data rate
Spatial Streams	How many spatial streams AP is able to utilize

Max MCS Index	Max MCS index number
Additional	Displays other AP capabilities, such as 802.11v transition

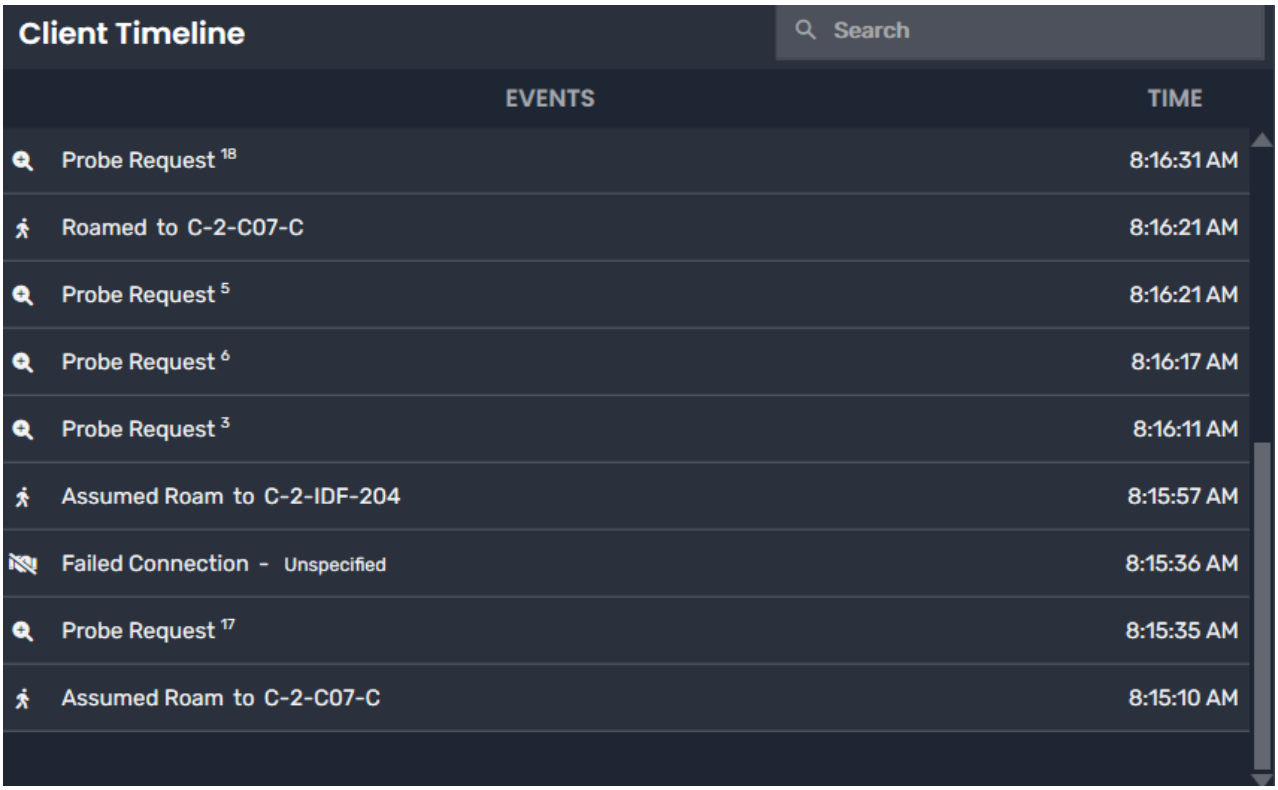
Client Details View

The Client View is the furthest extent of "drilldown" in MetaGeek App. It contains details about recent Packet Events that the client has experienced, as well as details about the client status, identity, and capabilities.



Events Pane

Events



MetaGeek App captures Wi-fi traffic in real time and its intelligent engine is able to quickly decipher events that occur on the wireless network in real time.

Some events will be based on a single frame type that MetaGeek App received. Other events will be based on a series of frames that MetaGeek App received and determined a more meaningful event such as a failed authentication attempt

MetaGeek App is also capable of capturing and recognizing when a device has roamed from one radio to another. MetaGeek App may not always see the reassociation frames that were sent between the client and the access point. MetaGeek App may not always see the reassociation frames that were sent between the client and the access point but when it sees a data frame on a new radio it must assume that a Roam was successful. In such a case, MetaGeek App will identify the event as an assumed roam.

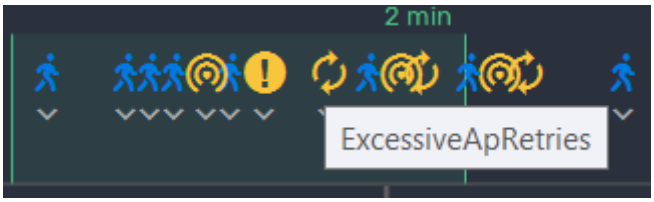
Event Types

Assumed Successful WPA 2/3		Client-Detail	This is the initial discovery of a device on a WPA2 or WPA3 network.
Assumed Successful Connection		Client	This is the initial discovery of a device on an open network.
Assumed Roam		Client	The application detected a new BSSID but did not see the reassociation or authentication frames.

Roam		Client	The application saw any management frames related to a roam followed by a data frame
Neighbor Report		Client-Detail	The client requested a neighbor report in an action frame.
Probe Request		Client	The application caught the client device probing.
Successful WPA 2/3		Client	The application detected some of the authentication sequence followed by a data frame.

Infrastructure Events on the Client Details Pane

MetaGeek App will display AP related events on the client details pane if the client was associated to the access point when the event was detected. These will show up in the time frame, but when clicked on, they will navigate the user back to the access point.

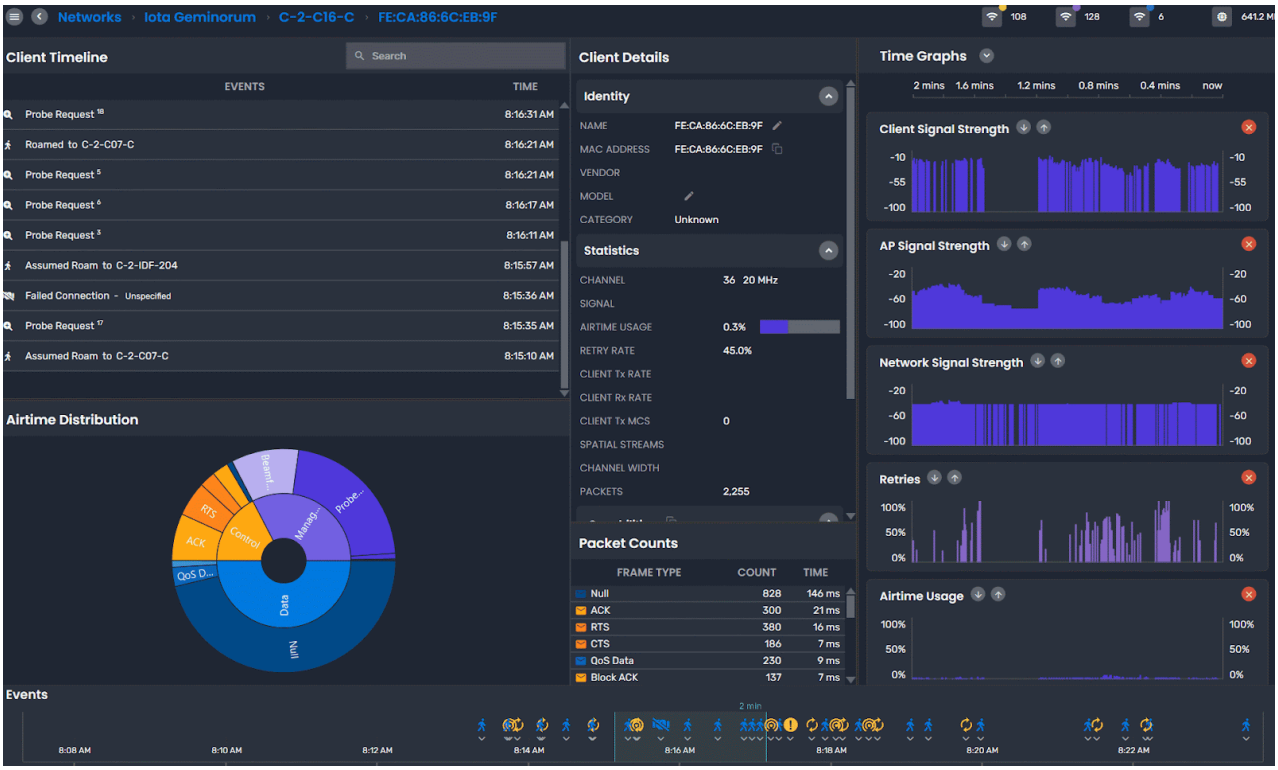


Selecting an Event

When a Packet Event is observed, Click on the Packet Event to open the Packet Flow Pane.

Time Frame Selection and Events

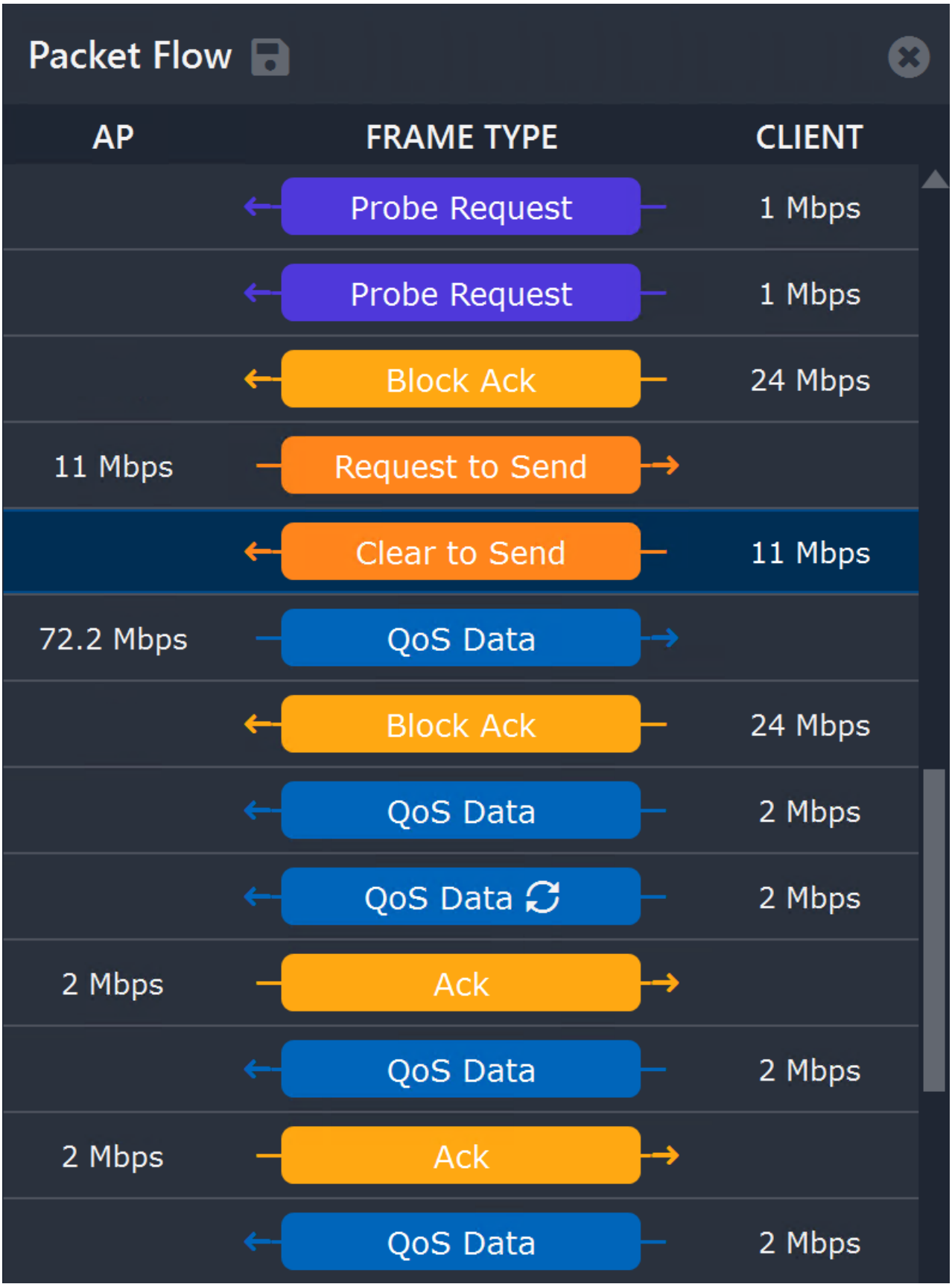
Events will be displayed based on the time frame selected. The time frame navigation at the bottom of the application can be moved to events for the client. Not all events will appear as an icon in the time frame navigation, such as probe requests and neighbor reports.



Packet Flow

Packet Flow shows a list of packets between the access point and client that were captured during or immediately following the Packet Event.

- The **AP column**, when populated, shows what data rate the access point transmitted the frame at.
- The **Frame Type** column shows what kind of 802.11 frame was transmitted. The arrow direction shows who the transmitter was, and who the receiver was.
- The **Client column**, when populated, shows what data rate the client transmitted the frame at.

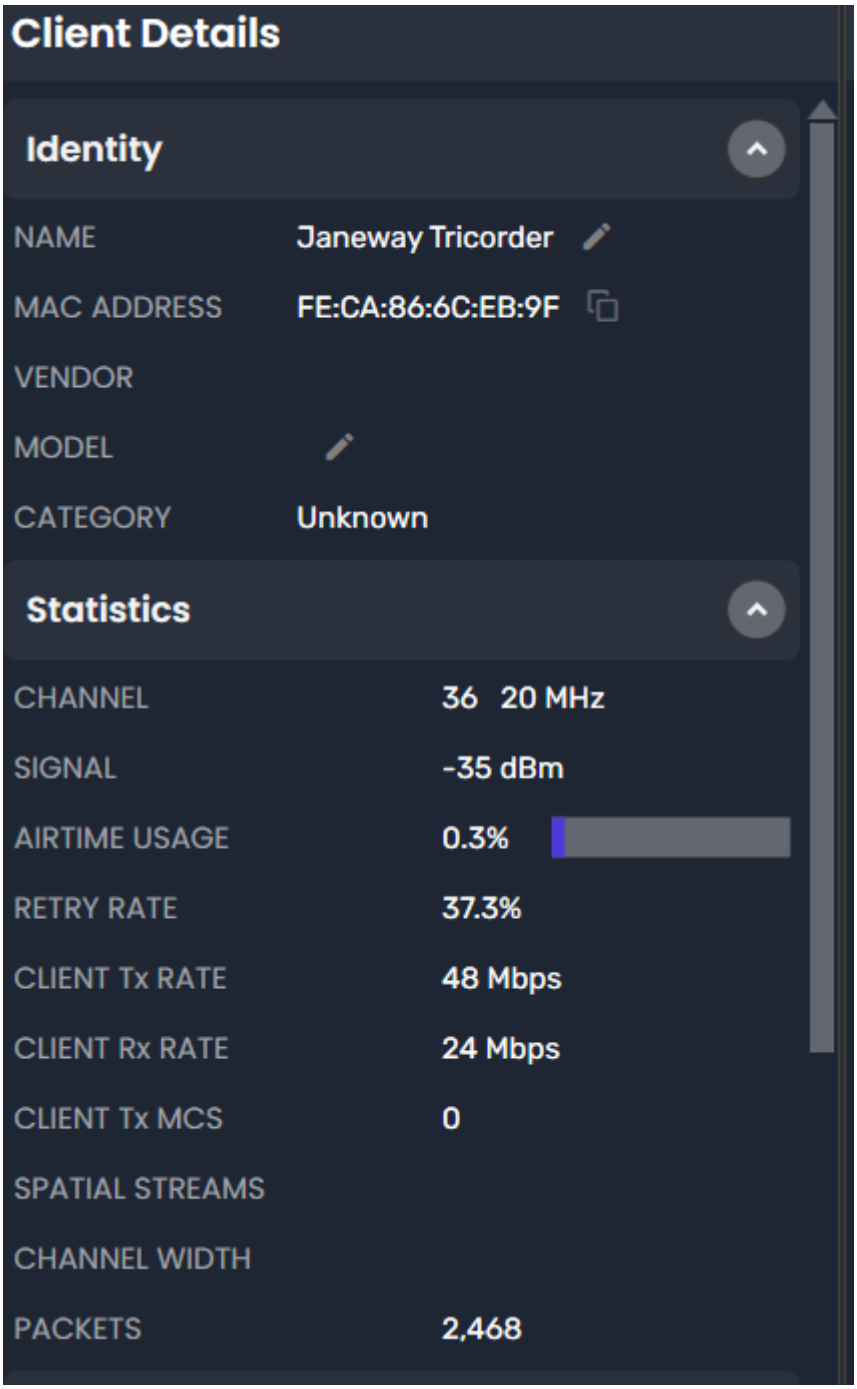


Air Time Distribution

The Multi-Layer Pie Chart (or "treepie") shows how the client traffic was distributed between management, control and data frames.

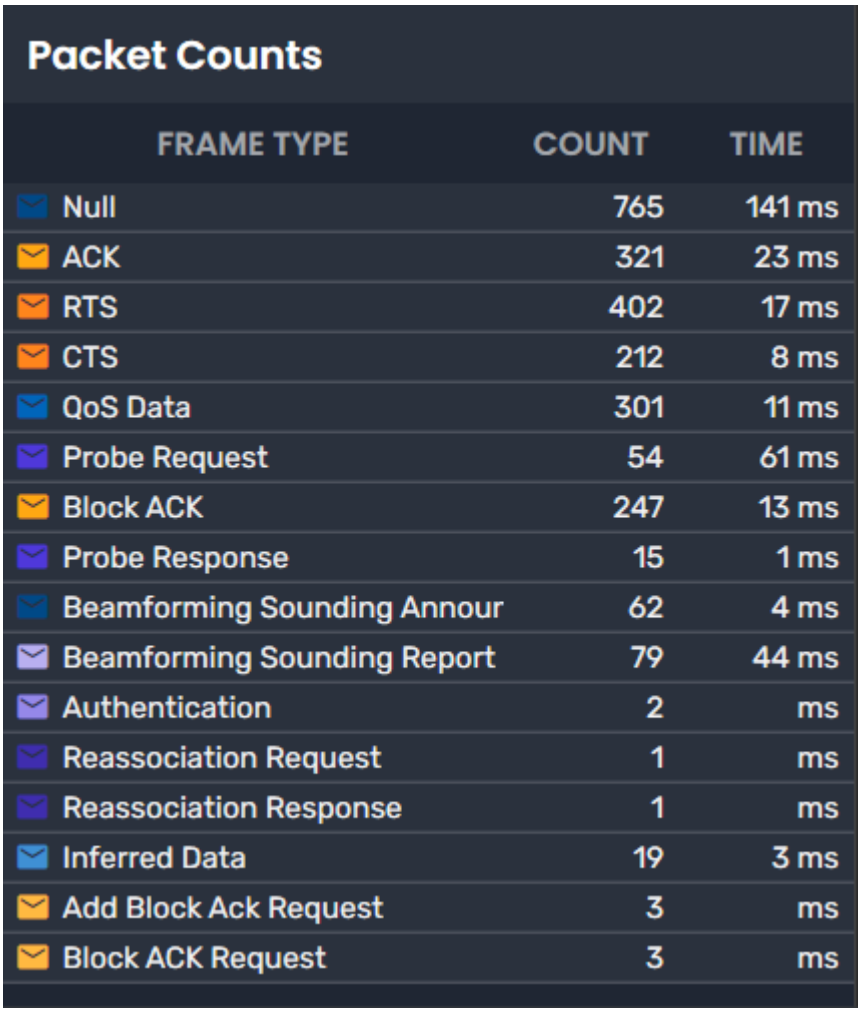
Client Details Pane

In the Client Details Pane, you can find static details and live information about the client.



Packet Counts Pane

The Packet Counts Pane shows how many packets have been captured in the conversation between the access point (or multiple access points, if the client has roamed) within the selected timespan.



Packet Counts

FRAME TYPE	COUNT	TIME
Null	765	141 ms
ACK	321	23 ms
RTS	402	17 ms
CTS	212	8 ms
QoS Data	301	11 ms
Probe Request	54	61 ms
Block ACK	247	13 ms
Probe Response	15	1 ms
Beamforming Sounding Annour	62	4 ms
Beamforming Sounding Report	79	44 ms
Authentication	2	ms
Reassociation Request	1	ms
Reassociation Response	1	ms
Inferred Data	19	3 ms
Add Block Ack Request	3	ms
Block ACK Request	3	ms

Inferred Data Frames

In some cases, the packet capture adapter(s) might not demodulate some or all of the data frames transmitted by the access point or client device. Missed data frames can be caused by:

- Poor signal strength from the capture adapter's perspective
- AP and client with more spatial streams than the capture adapter
- AP and client newer phy type than the capture adapter

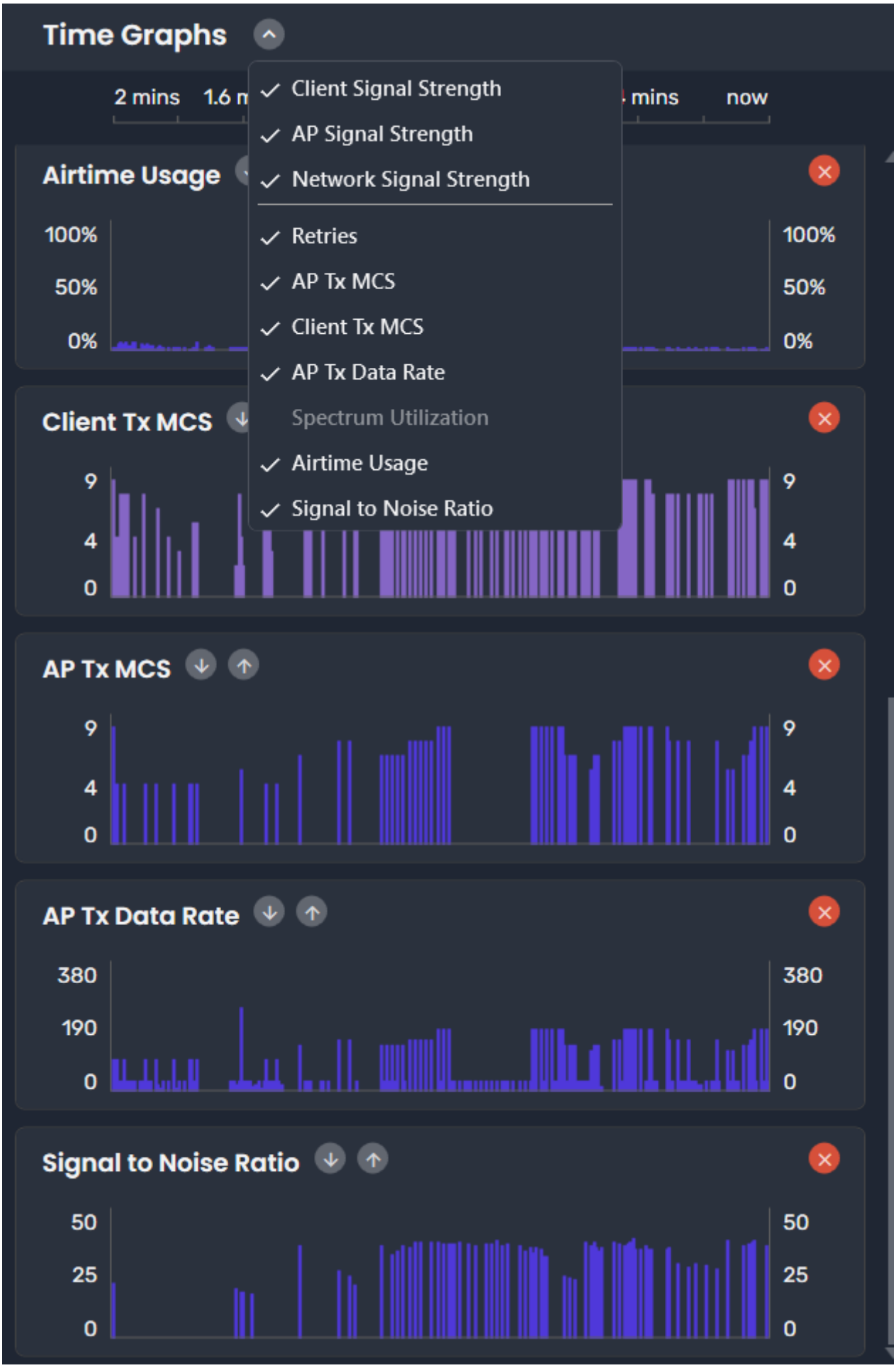
In most cases, even if the capture adapter fails to demodulate the data frames, the capture adapter will still successfully demodulate the Control frames, which are largely responsible for helping coordinate traffic on the Wi-Fi channel. *Note: Control Frames are always colored orange in MetaGeek App.*

It MetaGeek App captures a CTS (Clear-to-send) and ACK (Acknowledgement), it adds an Inferred Data Frame to the to the Packet Counts table and Airtime Usage graph. The Airtime Usage value is derived from the NAV (Network Allocation Vector) timer set by the CTS.

When packets are exported from MetaGeek App, Inferred Data Frames are not included. Instead, they are only calculated at the time of capture, or when reading in a packet capture file.

Time Graphs Pane

Under each Navigation Breadcrumb (ESSID View > BSSID View > Client View), certain Time Graphs become available at the bottom. You can toggle which Time Graphs are displayed under the dropdown. Time Graphs can be moved up or down using the down and up arrow icons.


Time Graphs
2 mins
1.6 m
mins
now
Client Signal Strength
AP Signal Strength
Network Signal Strength
Retries
AP Tx MCS
Client Tx MCS
AP Tx Data Rate
Spectrum Utilization
Airtime Usage
Signal to Noise Ratio
Airtime Usage
100%
50%
0%
Client Tx MCS
9
4
0
AP Tx MCS
AP Tx Data Rate
380
190
Signal to Noise Ratio
50
25

Time Graph	Description	View(s) available in
AP Transmit Data Rate	Data rate (Mbps) of selected object over time	BSSID & Client
AP Transmit MCS	MCS index of the selected radio over time	BSSID & Client
Client Transmit MCS	MCS index of the selected client over time	BSSID & Client
Retries	Retry rate (%) of the selected object over time	BSSID & Client
Signal Strength	Signal strength (dBm) of the selected object over time	ESSID, BSSID, & Client
Airtime Usage	BSSID and its associated client traffic airtime in a time graph.	ESSID, BSSID, & Client
Signal to Noise Ratio	The signal to noise reported by the client to the Access Point. This is only populated when MetaGeek App hears the client report its SNR value	Client
AP Signal Strength	This aggregates all of the APs the client was associated with to show the signal strength over time.	Client

Automatic Adapter Management

MetaGeek App handles capturing significantly differently through Automatic Adapter Management, where the adapter capture channels are automatically changed based on what is being viewed. To change channels, simply navigate to different views, and MetaGeek App will change adapter channels as needed.

Note: This section is technical in nature. Understanding it is not important for the operation of MetaGeek App.

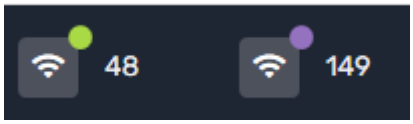
Adapter Roles

MetaGeek App can address up to three packet capture adapters:

- Primary Adapter
- Secondary Adapter

- Tertiary Adapters

The status and current channel of each packet capture adapter is displayed in the Status Pane.



Capture Modes

- **Sweep** - Moves the adapter through the set of channels, usually in a cyclical fashion. The adapter dwells on the channel for 150-300 milliseconds, depending on the current view.
- **Capture** - The adapter stays tuned to the Current Channel, unless an event causes the adapter to be moved elsewhere.

Single Packet Capture Adapter

Using a single packet capture adapter in MetaGeek App provides basic capture functionality. It will not be able to perform Client Follow and it will not capture roams.

View	Primary Adapter
Channels View	Sweep all channels
Clients View	Sweep all channels
Channels View	Sweep all channels
ESSID View	Sweep all ESSID channels
BSSID View	Current channel
Client View	Current channel

Two Packet Capture Adapters

Using two packet capture adapters in MetaGeek App is the minimum recommended number of adapters.

	Primary	Secondary
Channels View	Sweep All 5 GHz	Sweep All 2.4 GHz
Clients View	Sweep All 5 GHz	Sweep All 2.4 GHz
Networks View	Sweep All 5 GHz	Sweep All 2.4 GHz

ESSID View	All ESSID Channels If there are more than 20 ESSID channels: Sweep all 5 GHz	All Non-ESSID Channels If there are more than 20 ESSID channels: Sweep all 2.4 GHz
BSSID View	Current Channel	Sweep All Non-Current Channels listed in 802.11k BSSID Beacon neighbor report 2x then all remaining channels. Prioritize by highest signal strength
Client View	Current Channel	Sweep All Non-Current Channels listed in 802.11k BSSID Beacon neighbor report 2x then all remaining channels. Prioritize by highest signal strength.

Three Packet Capture Adapters

Using three packet capture adapters is recommended in MetaGeek App, and further increases the speed at which channels are updated.

	Primary	Secondary	Tertiary
Channels View	All Low 5 GHz	All High 5 GHz	All 2.4 GHz
Clients View	All Low 5 GHz	All High 5 GHz	All 2.4 GHz
Networks View	All Low 5 GHz	All High 5 GHz	All 2.4 GHz
ESSID View	All ESSID Channels	All Non-ESSID 5 GHz Channels	All Non-ESSID 2.4 GHz Channels
BSSID View	Current Channel Capture neighbor report announcements from AP.	Respecting the list of channels selected and assigned to this NIC, Sweep All Non-Current Channels listed in 802.11k BSSID Beacon neighbor report 2x then all remaining channels. Prioritize by highest signal strength	Respecting the list of channels selected and assigned to this NIC, Sweep All Non-Current Channels listed in 802.11k BSSID Beacon neighbor report 2x then all remaining channels. Prioritize by highest signal strength

Client View	Current Channel Capture neighbor report announcements from AP.	Respecting the list of channels selected and assigned to this NIC, Sweep All Non-Current Channels listed in 802.11k BSSID Beacon neighbor report 2x then all remaining channels. Prioritize by highest signal strength	Respecting the list of channels selected and assigned to this NIC, Sweep All Non-Current Channels listed in 802.11k BSSID Beacon neighbor report 2x then all remaining channels. Prioritize by highest signal strength