Chanalyzer 6 User Guide

Casey Cathey
Updated 6 months ago

User Guide

Note: This user guide is a work-in-progress, and will reach completion over the coming weeks.

Index

Introduction

Chanalyzer 6 (formerly Tonic) is a blend of MetaGeek's best ideas, including:

- Graphical Wi-Fi scanning (from inSSIDer 2)
- Airtime-based, visual packet analysis (from Eye P.A.)
- Combining Wi-Fi scanning and spectrum analysis (Chanalyzer)

The result is a fast and detailed "Swiss Army Knife" Wi-Fi tool that can be used for a variety of tasks, such as:

- Discovering non-Wi-Fi interference
- Measuring Wi-Fi channel congestion
- Identifying clients and access points that are consuming air time on the channel
- Spot-checking signal strength
- Discovering and monitoring client device behaviors
- Viewing packet exchanges between clients and access points
- Capturing packets to perform deeper protocol analysis

Chanalyzer 6 focuses on being information-dense to help Wi-Fi network engineers gather as much data as possible, all with a clean user interface that is easy to read and navigate.

Is Chanalyzer 6 a Wi-Fi Scanner?

While Chanalyzer 6 does feature graphical Wi-Fi scanning views, the way that it collects data is significantly different from a Wi-Fi scanner.

Wi-Fi scanners work by asking their host operating system (such as Windows) for a list of nearby access points. The operating system then checks each Wi-Fi channel Beacons (and in some cases, Probe Responses) from access points, and then reports back to the Wi-Fi scanner. While every operating system (Android, macOS, and Windows) handles Wi-Fi scanning differently, results are usually only returned once about every 4 seconds.

Additionally, the results that the operating system returns are only the contents of the Beacons and Probe Responses. Wi-Fi scanning is extremely useful for performing site surveys (in other words, plotting signal strength and other measurements on a map), for spot-checking coverage, performing channel planning, and checking access point security and configurations. It's an important tool, but it does not provide as much data as packet capture and/or spectrum analysis.

Real-time Packet Analysis

Instead, Chanalyzer 6 is a **real-time packet analyzer**. It leverages full Wi-Fi packet capture to listen to all Wi-Fi activity. This includes Beacons, Probe Responses, Data, Acknowledgement, and many other types of 802.11 frames. With this data, Chanalyzer 6 is able to provide a much more complete picture of the Wi-Fi environment.

Getting Started

To perform packet capture and live packet analysis, Chanalyzer 6 requires at least one packet capture adapter. The adapters that Chanalyzer 6 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 begin, connect one to three supported packet capture adapters, and launch Chanalyzer 6. As Chanalyzer 6 launches, it will swap out the packet capture adapter's default driver for the special packet capture driver.

Note: While Chanalyzer 6 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 Chanalyzer 6.

Optionally, a Wi-Spy DBx can be connected to provide Layer 1 spectrum analysis data.

Supported Packet Capture Adapters

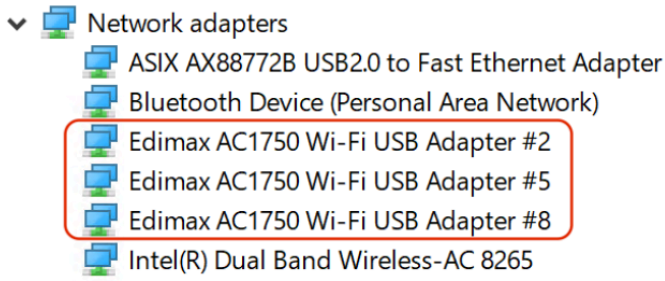
Chanalyzer 6 supports several standard, off-the-shelf Wi-Fi adapters. You can bring your own adapter(s), or purchase adapters from MetaGeek or a MetaGeek Partner.

Supported Packet Capture Adapters

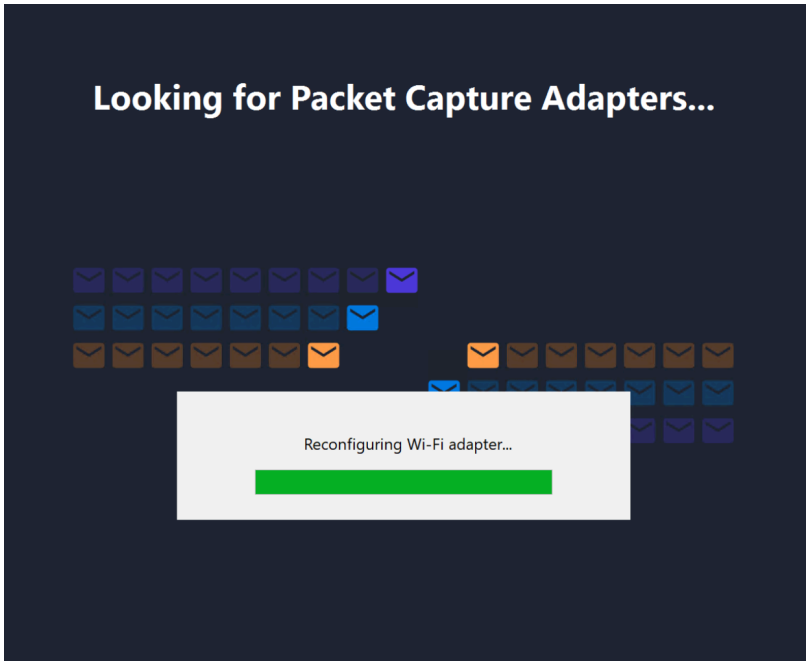
Driver Installation

To perform packet capture functions, Chanalyzer 6 installs a special packet capture driver for each supported adapter. This process happens automatically when Chanalyzer 6 launches, and is why Chanalyzer 6 requires Administrator privileges.

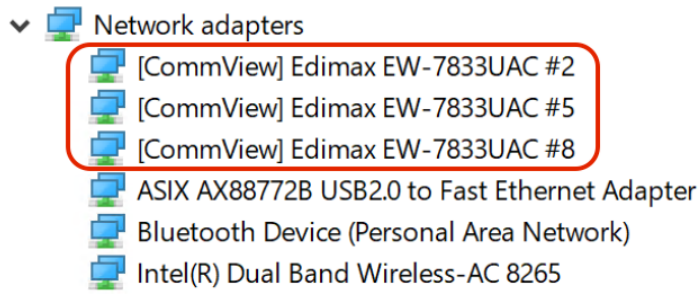
Before Chanalyzer 6 launches, supported packet capture adapters will either have no driver installed, or a standard driver.



While Chanalyzer 6 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 Chanalyzer 6 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 Chanalyzer 6 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 Breadcrumbs

At the top level, Chanalyzer 6 has three views:

- Networks View, which shows a list of all of the ESSID's that have been observed

- Clients View, which shows all of the client devices that have been observed
- Channels view, which 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 Chanalyzer 6 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 Chanalyzer 6.

Navigation Table

A table of selectable objects, depending on the current view. For example, the Navigation Pane shows a list of ESSID's (i.e. Networks) in the Networks View, and a list of active clients in the BSSID (i.e. AP Radio) View.

Click any object in the Navigation Table to drill down into it.

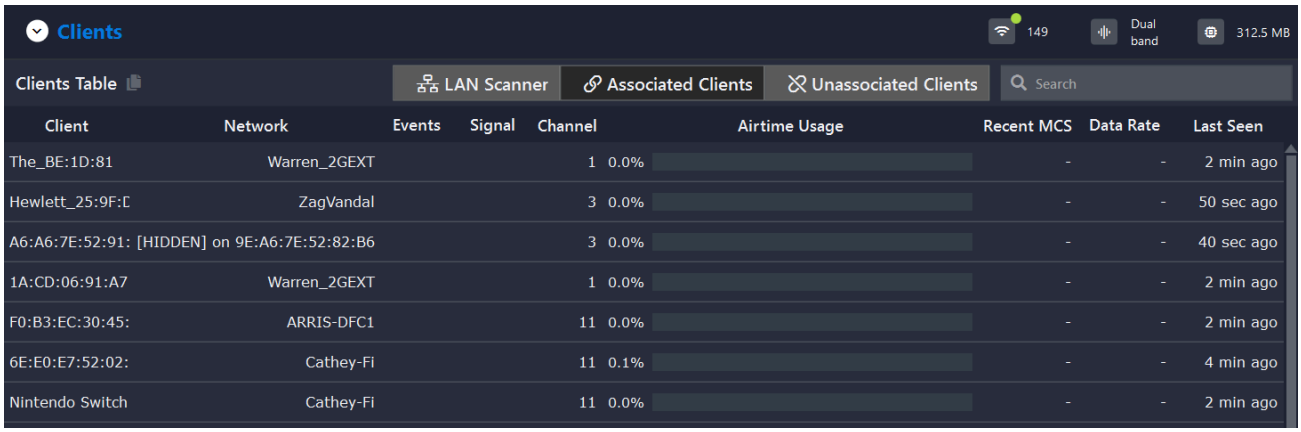
Networks View

The Networks View is analogous to the "home" screen in Chanalyzer 6. It's where Chanalyzer 6 begins by default, and is the top-level of the Networks > ESSID View > BSSID View > Client drill down.

Airtime Usage	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).



Airtime Usage	Client airtime for the whole channel. Graph is percentage of BSSID.

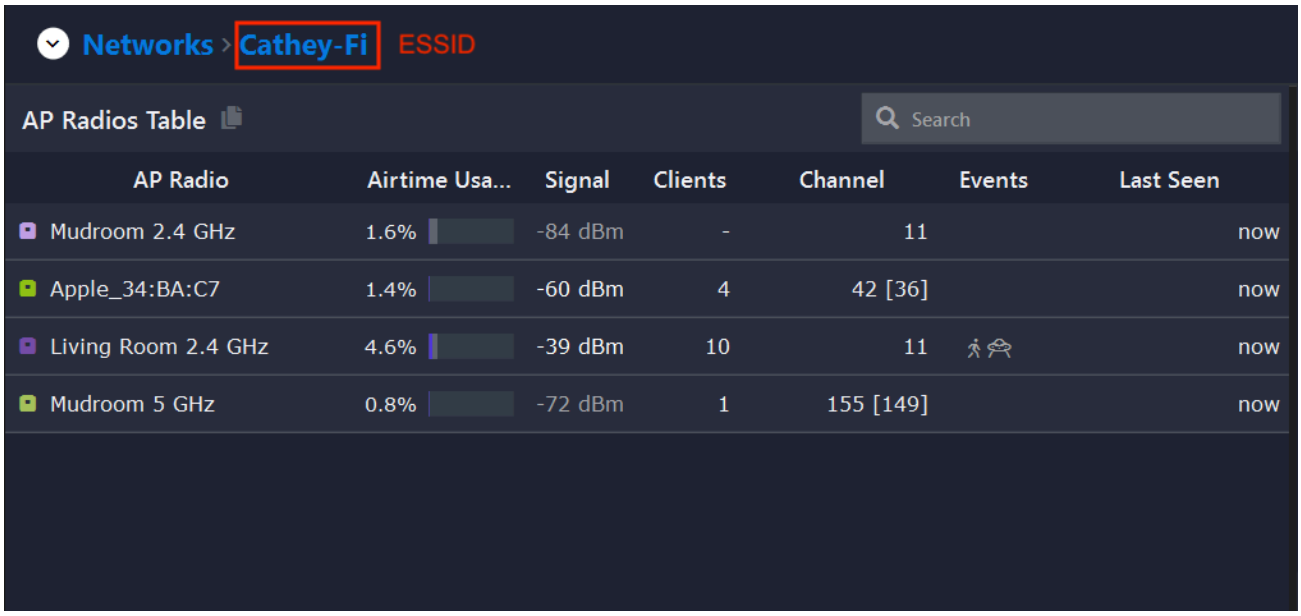
Channels View

The Channels View will display all relevant information for each channel in the 2.4 and 5 GHz bands. This is helpful for understanding which channels are at at capacity, or which channels are the most clear.

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 (grey)
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

ESSID View

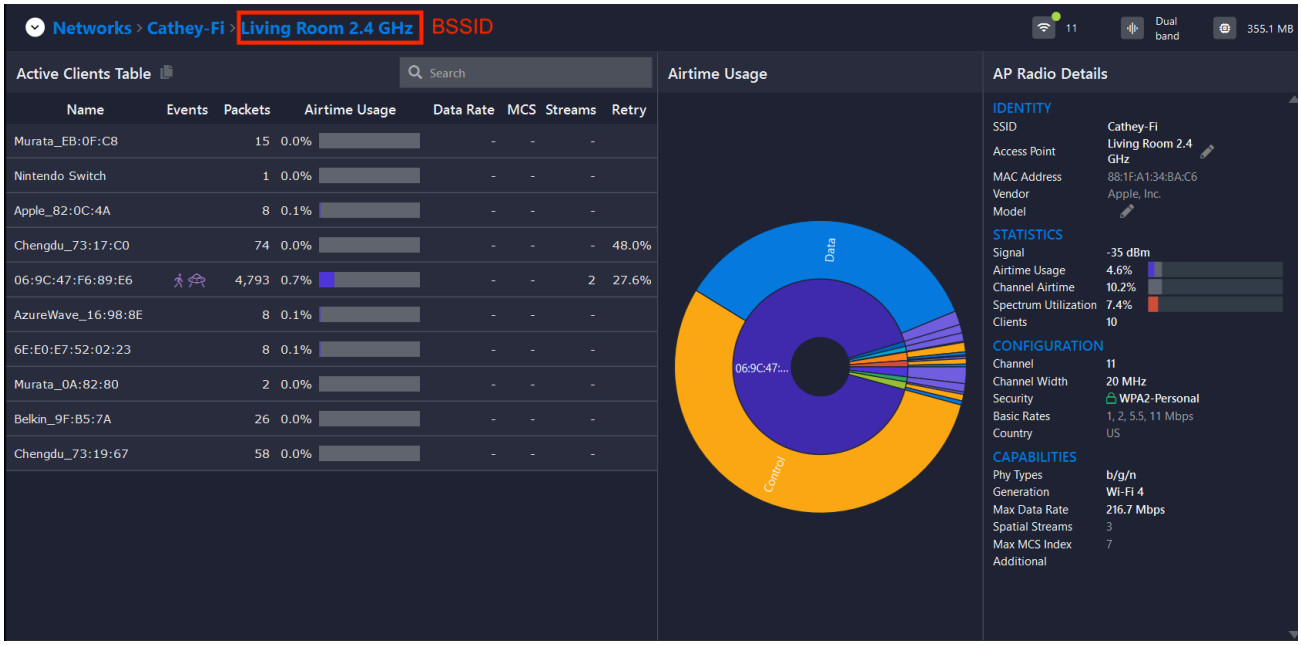
The first "drilldown" from the Networks view by clicking on an ESSID. This view will display the radios or BSSIDs underneath the selected ESSID. This view is helpful to understand client distribution per radio.



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

BSSID View

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 percentage of traffic within BSSID. client percentage (purple) other clients on bssid (gray).

AP Radio Details Pane

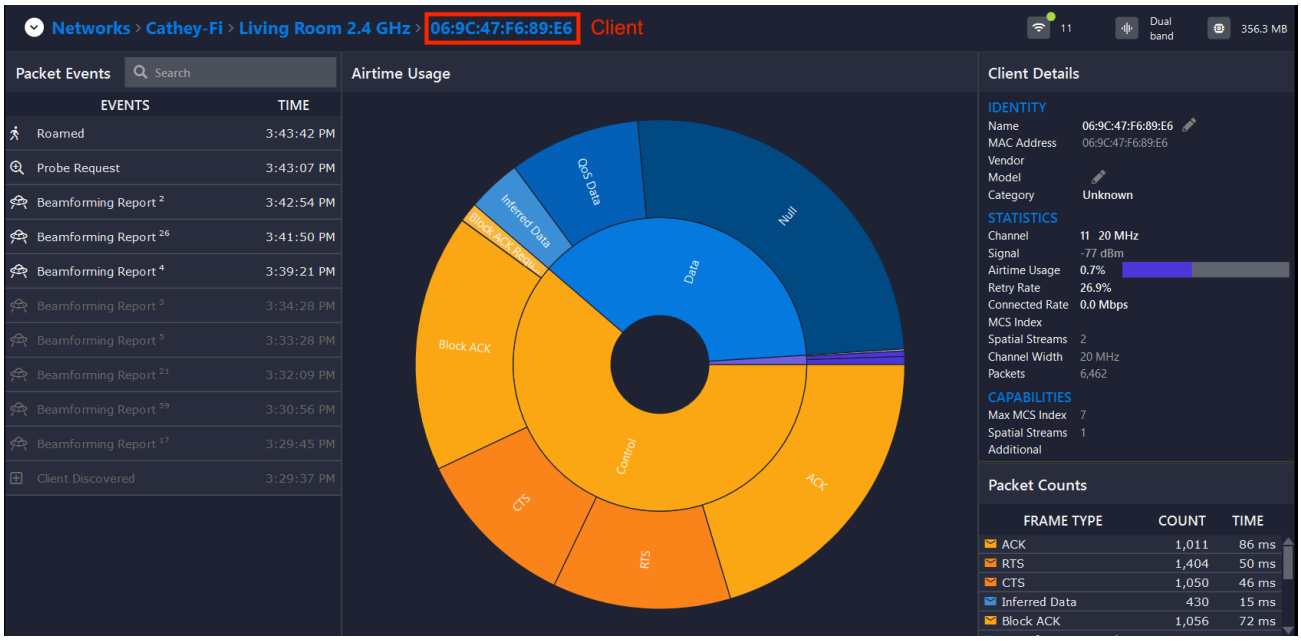
In the AP Radio Details Pane, you can find live information about the client.

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 View

The Clients View is the furthest extent of "drilldown" in Chanalyzer 6. 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

Packet Events

By performing live analysis of captured packets, Chanalyzer 6 detects Packet Events that occur to clients. In some cases, Packet Events are detected due to the capture of a specific type of packet, or due to a series of events.

For example, if a Deauthentication Frame is heard, then a Deauthentication Packet Event is assigned to the client.

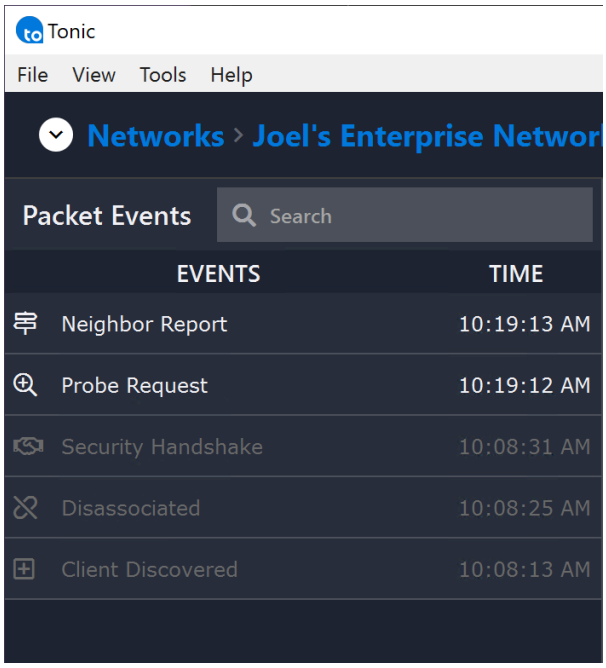
If a client is associated to a BSSID (access point radio), and is seen sending frames to another BSSID (other than Probe Requests), then a "Roamed" Packet Event occurs, indicating that the client must have roamed to a different access point.

Selecting a Packet Event

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

Disabled Packet Events

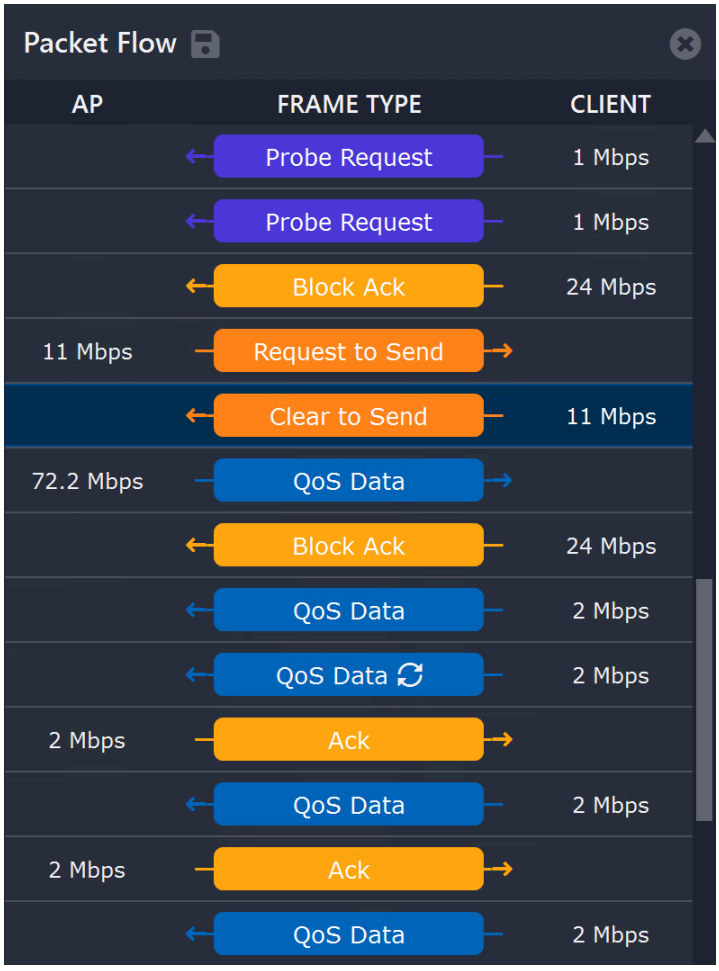
Chanalyzer 6 keeps a 10-minute buffer of all packets in memory. When a Packet Event becomes older than 10 minutes, the packets from the event are no longer available for Chanalyzer 6 to reference. As a result, Packet Events old than 10 minutes are greyed out and are no longer selectable.



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 Usage Pane

The Multi-Layer Pie Chart (or "treepie") shows how much airtime was consumed in the conversation between the access point and the client.

Client Details Pane

In the Client Details Pane, you can find 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.

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 Chanalyzer 6.*

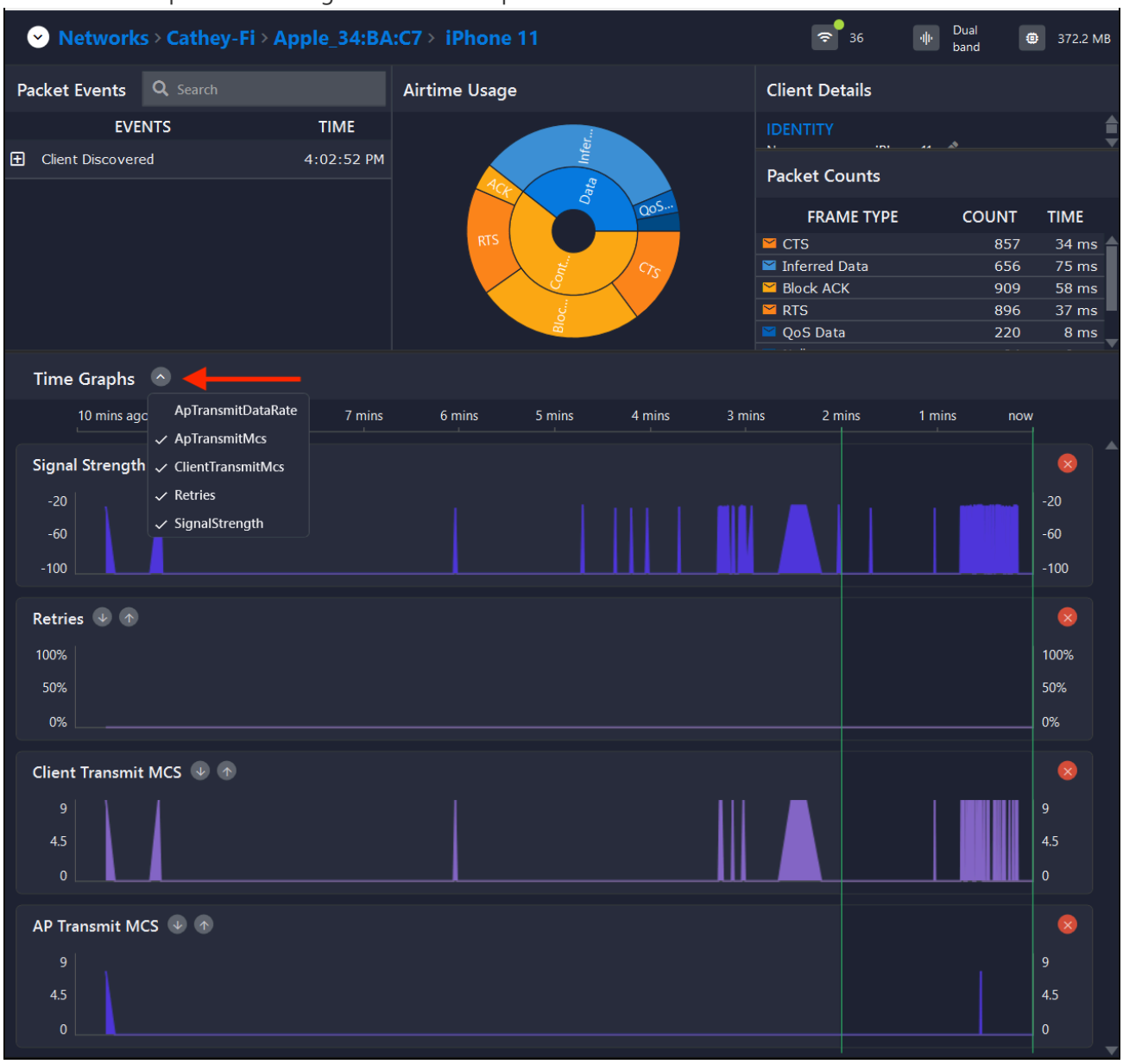
It Chanalyzer 6 captures a CTS (Clear-to-send) and ACK (Acknowledgement), it adds an Inferred Data Frame to the to the Packet Counts table and Airtime Usage graph. The Airtime Usage value is derived from the NAV (Network Allocation Vector) timer set by the CTS.

When packets are exported from Chanalyzer 6, 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 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

Automatic Adapter Management

Most packet capture tools require the user to manually configure what channel or channels to capture on. Chanalyzer 6 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, simple navigate to different views, and Chanalyzer 6 will change adapter channels as needed.

Note: This section is technical in nature. Understanding it is not important for operation of Chanalyzer 6

Adapter Roles

Chanalyzer 6 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. Hover the mouse over the capture adapter to see details about it.

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.

Channels Sets

Chanalyzer 6 uses Channel Sets to define what the packet capture adapter will sweep or continuously capture on. Some channel sets are variable.

- **Current Channel** - The channel that the Current Object (see below) is on.
- **Non-Current Channels** - Channels that the Current Object (see below) is not on.
- **All Channels** - Sweeps all channels in the 2.4 and 5 GHz bands.
- **ESSID Channels** - Sweep all channels occupied by the current ESSID.
- **non-ESSID Channels** - Sweep all channels that are not occupied by the current ESSID.
- **All 2.4 Channels** - Sweep channels 1-14 (14 channels)
- **All 5 GHz Channels** - Sweep channels 36-165 (25 channels)
- **Lower 5 GHz Channels** - Sweep channels 36-116 (15 channels)
- **Upper 5 GHz Channels** - Sweep channel 120-165 (12 channels)

Current Object

In Chanalyzer 6, a Current Object can be:

- An ESSID, which can occupy many channels
- A BSSID, which can only occupy one channel
- A Client, which can only occupy one channel
- A channel

The Current Object changes depending on the view that is selected in Chanalyzer 6. If the Current Object is an object type that only occupies one channel (such as a BSSID, client, or a channel itself), then that single channel is defined as the Current Channel.

Single Packet Capture Adapter

Using a single packet capture adapter in Chanalyzer 6 provides basic capture functionality, but requires the adapter to occasionally go off-channel to detect the presence of new BSSID's, and to detect Unobserved Client Roam events.

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 Chanalyzer 6 is ideal, as it allows the primary to focus on capturing the Current Object, while the secondary adapter is free to monitor for new BSSID's and Unobserved Client Roam events on other channels. It also splits the workload between 2.4 and 5 GHz in many places, which drastically increases the speed at which channels (and their child objects) are updated.

View	**Primary Adapter**	**Secondary Adapter**
Channels View	• Sweep all 5 GHz channels	• Sweep all 2.4 GHz channels
Clients View	• Sweep all 5 GHz channels	• Sweep all 2.4 GHz channels
Channels View	• Sweep all 5 GHz channels	• Sweep all 2.4 GHz channels

ESSID View	• Sweep all ESSID channels • If the current ESSID consumes more than 20 channels, sweep all 5 GHz channels	• Sweep all non-ESSID channels • If the current ESSID consumes more than 20 channels, sweep all 2.4 GHz channels
BSSID View	• Current channel	• Sweep all non-current channels
Client View	• Current channel	• Sweep all non-current channels

Three Packet Capture Adapters

Using three packet capture adapters is supported in Chanalyzer 6, and further increases the speed at which channels are updated.

View	Primary	Secondary	Tertiary
Channels View	• All lower 5 GHz	• All upper 5 GHz	• All 2.4 GHz
Clients View	• All lower 5 GHz	• All upper 5 GHz	• All 2.4 GHz
Channels View	• All lower 5 GHz	• All upper 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	• All non-current 5 GHz channels	• All non-current 2.4 GHz channels
Client View	• Current channel	• All non-current 5 GHz channels	• All non-current 2.4 GHz channels

clients.png

70 KB · Download

networks.png

50 KB · Download

channels.png

60 KB · Download

ch6-logo.8ecdab9.png

10 KB · Download

Was this article helpful?

✓ Yes ✕ No

0 out of 0 found this helpful

Have more questions? Submit a request

Return to top