

MeerCAT[®]-Pro

User Manual

MeerCAT[®]-Pro

Version 4.5 Release

© Copyright 2007-2014. All rights reserved. Applied Visions, Inc.

Distribution of this work is prohibited unless prior written permission is obtained from the copyright holder.

MeerCAT is a trademark of Applied Visions, Inc.




All other trademarks and copyright are the property of their respective owners.

TABLE OF CONTENTS

1	Introducing MeerCAT	8
1.1	What is MeerCAT?	8
1.2	What are the Benefits of MeerCAT?.....	8
1.3	What are MeerCAT’s Key Features & Functions?.....	9
2	Getting Help With MeerCAT	11
2.1	MeerCAT Technical Support	11
2.2	MeerCAT Feedback and Additional Information	11
2.3	Licensing.....	11
3	Accessing and Navigating MeerCAT.....	12
3.1	Controlling MeerCAT	12
3.1.1	Coordinated Views.....	12
3.1.2	Context Menus.....	12
3.2	Customizing the MeerCAT Console	13
3.2.1	Views.....	13
3.2.2	Preferences	15
4	Importing Data into MeerCAT	17
4.1	Importing Kismet Data	17
4.2	Importing NetStumbler Data	18
4.3	Bulk Import Kismet Data	19
4.4	Known Devices	20
4.4.1	Manually Adding Known Devices.....	21
4.4.2	Importing Known Devices from a CSV File.....	23
4.4.3	Marking existing devices as Known	24
4.5	Importing Wired Capture Data	24
4.6	Manufacturers	25
5	Using MeerCAT – Fundamental Tools.....	26
5.1	MeerCAT Console	26

5.2	Device Explorer View	26
5.2.1	Search.....	27
5.2.2	Toolbar	27
5.2.3	Illustrative Discovery Comparison Examples	28
5.3	Networks View	30
5.3.1	Toolbar	31
5.4	Clients View.....	31
5.4.1	Toolbar	31
5.5	Geographic View	32
5.5.1	Tour of Geo View Capabilities.....	32
5.5.2	Controls.....	33
5.5.3	Toolbar	34
5.5.4	3D Specialized Controls.....	36
5.5.5	Modifying the Geo View cache location	37
5.5.6	Adding additional Geo View imagery sources	38
5.5.7	Adding Bing Imagery	39
5.6	Layers View	40
5.7	Bounds View	40
5.7.1	Toolbar	40
5.7.2	Bounds Tool	40
5.8	Models View	41
5.9	Network Topology View.....	42
5.9.1	Toolbar	44
5.10	Navigator View.....	45
5.10.1	Selection / Highlighting.....	45
5.10.2	Panning	46
5.10.3	Zooming	46
5.10.4	Searching.....	46
5.10.5	Toolbar	46

5.11	Channels View.....	51
5.12	Timeline View.....	52
5.12.1	Toolbar	52
5.13	Device History View	55
5.13.1	Toolbar	55
5.14	Overlays View.....	56
5.14.1	Toolbar	56
5.15	Alert Patterns View	58
5.15.1	Toolbar	59
5.16	Alerts View	59
5.16.1	Toolbar	59
5.16.2	Alert Submenu	60
5.17	Dashboard View	61
5.17.1	Toolbar	62
5.18	Legend View.....	63
5.19	Image Viewer	65
5.19.1	Adding Images.....	65
5.19.2	Displaying Images	66
5.19.3	Removing Images.....	66
5.19.4	User Controls	66
5.19.5	Toolbar	66
5.20	Status Line.....	67
6	Mission Mapping.....	68
6.1	Preferences for Mission Mapping.....	68
6.2	Choosing a Color for the Mission.....	68
6.3	Assigning the Mission to an Access Point.....	69
6.4	Color the Network by Mission	70
6.5	Colored by Mission	71
6.6	Group by Mission	72

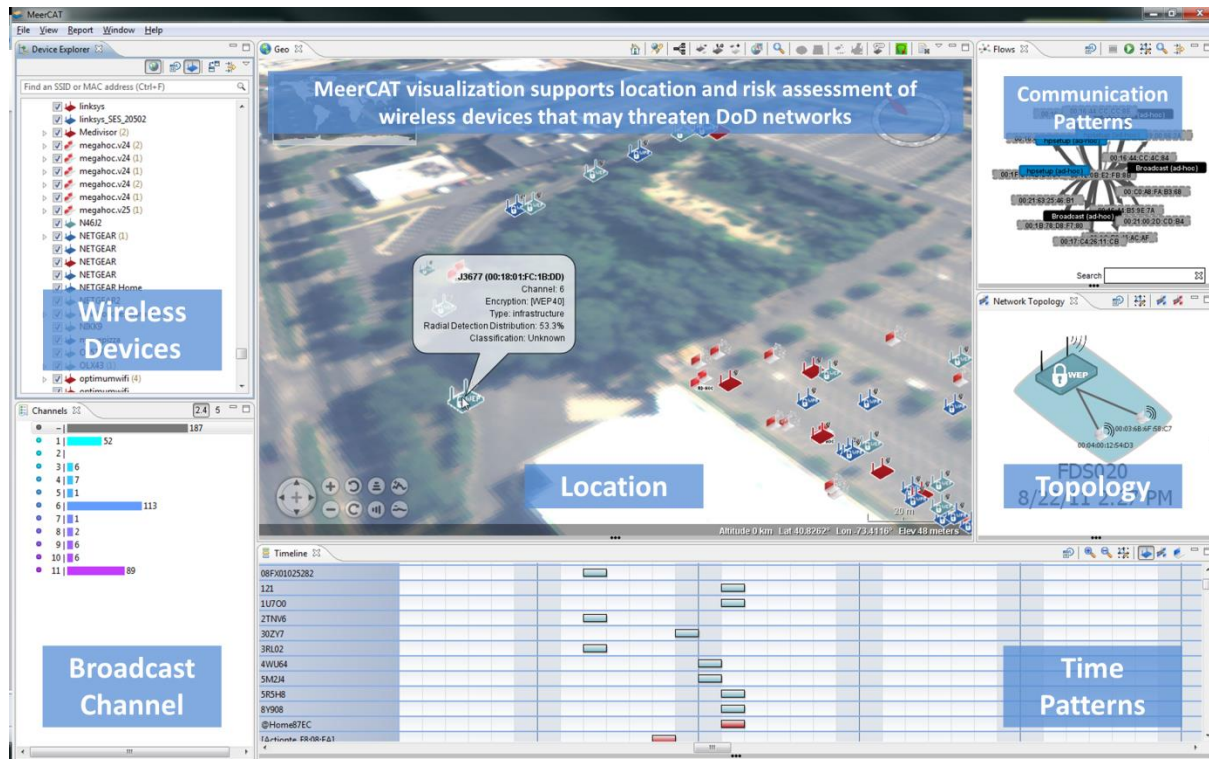
7	Communication Flow Graph	73
7.1	Flows View	73
7.1.1	Graph Type.....	73
7.1.2	Nodes	74
7.1.3	Links	75
7.1.4	Filter	76
7.1.5	Preferences for Flows	77
7.1.6	User-Graph Interaction	78
7.1.7	Toolbar	79
7.1.8	Communication Patterns Usage Scenario	79
7.1.9	WiFi LAN Example	83
7.1.10	WiFi Broadcast Domain Example	86
7.2	Flow Details View	88
7.2.1	Toolbar	88
7.3	Wired Captures	89
7.3.1	Wired Captures View	89
7.3.2	Flows View	89
7.3.3	Flow Details View	89
8	Reporting.....	90
8.1	Reporting Features	90
8.2	Generate Report	90
8.2.1	Report Generation Criteria	90
8.2.2	Copy Screenshot of Active View 	91
8.2.3	Save Screenshot of Active View 	92
8.2.4	Email Screenshot of Active View 	92
8.2.5	Drag and Drop	92
8.2.6	View Annotations.....	92
8.3	Report Templates.....	93
8.3.1	Images.....	93

8.3.2	Tables	93
8.3.3	Annotations.....	93
9	Other Preference Options.....	94
9.1	Flow Colors.....	94
9.2	General Colors.....	95
9.3	Import	95
9.4	Maintain Perspectives.....	96
9.5	Reporting Options.....	96
9.6	Tags	97
10	Frequently Asked Questions.....	100
11	Glossary of Terms	103

1 Introducing MeerCAT

1.1 What is MeerCAT?

MeerCAT (Mobile Cyber Asset Tracks) is a visualization tool specifically developed to help users locate wireless assets and networks, and assess the risks to their organization. It is designed for post-hoc analysis of data acquired from site surveys or wireless security audits such as ‘wardrives’ that discover, identify and locate wireless transmitters.



1.2 What are the Benefits of MeerCAT?

Organizations are deploying or being exposed to wireless local area networks (LANs) to support mobile connectivity. However, wireless LANs present unique security challenges, as it is easy to introduce unauthorized or intercept authorized wireless signals in organizational networks. While there are numerous systems designed to help locate and assess wireless activity, they generate significant data that require experience and expertise to correlate and interpret. One of the challenges is to quickly turn the wealth of data into meaningful and actionable information. Visualization is an effective way to make sense of this data.

MeerCAT arms users with advanced **visual analytics** specifically **designed to facilitate and expedite the analysis of wireless discovery data** to quickly locate and assess the risks of wireless assets. Professionals can use MeerCAT to locate both authorized and unauthorized

(rogue) access points and unsecured wireless devices. MeerCAT users can also ‘see’ with what assets are wireless devices connecting to.

Among the benefits of using MeerCAT to analyze wireless risks:

- **Supports post-hoc analysis of multiple wireless discovery sessions** for periodic security audits and on-going assessment of external and internal wireless networks.
- Provides interactive and coordinated geospatial, topological and spatio-temporal views to **quickly locate potential security issues**, and efficiently identify relevant vulnerabilities and threats.
- Integrates current and historical information to **show trends in the behavior of mobile assets and networks** that highlight anomalies.
- **Interfaces to a variety of wireless discovery and security tools** to provide users the flexibility to use MeerCAT with their preferred tools.

1.3 What are MeerCAT’s Key Features & Functions?

- **Geo-locates Wireless Devices.** MeerCAT visualizes detected wireless devices and their status on 3D geographic maps, topographic satellite imagery and imported floor plans. Users can navigate anywhere on the globe down to street and building views.
- **Generates Network Topology Maps.** MeerCAT creates a topological view of detected wireless networks to understand the impact of wireless vulnerabilities and threats. Users can ‘see’ the detected access points and clients connected to them.
- **Visually Captures Wireless Device Classification and Security Events.** MeerCAT’s color-coded and user-customizable iconographic representation of device classification and security status allows users to immediately identify wireless devices that present risks to their networks. Device details include the SSID, location coordinates, encryption, type, and configuration.
- **Maps Access Point Coverage and Channels.** MeerCAT generates wireless coverage maps based upon the location and RF signal strength of detected access points from wardrives. It displays RF signal coverage areas to help users identify interference by neighboring networks and unauthorized stations, and signal spillage in unsecured perimeters.
- **Charts Channel Usage.** MeerCAT charts the RF channel distribution for all detected networks. A histogram displays the frequency distribution of access points on each channel to determine potential interference.
- **Displays Events and Changes.** MeerCAT users can interactively compare the results of wardrives with comparative views between two points in time, such as before and after remediation. Geospatial and topological views allow users to track wireless asset movement and state changes over time.
- **Helps Analyze Device Behavior Over Time.** MeerCAT users can benefit from the ability to analyze the activity of suspicious wireless devices over time. Events and

trends can be viewed over days, weeks, or even months to help improve network security posture, assist in forensic investigation and ensure policy compliance.

- **Visualizes Communication Flows.** MeerCAT's wireless network traffic visualization improves the visibility of network performance and security concerns. The visual analytic tool processes packet capture files and visually aggregates network traffic and wireless packet flow.
- **Coordinates Views for Investigation.** MeerCAT users can drill down from any window view for additional details about detected wireless networks and clients. Coordinated views allow users to quickly select a device of interest in one MeerCAT window and highlight the device in all other views for various perspectives.
- **Supports Data Filtering.** MeerCAT enables users to view, analyze, and filter wireless discovery and security data by a range of variables including the operating channel, SSID, asset, security policies, or events.
- **Helps Assess Risks.** MeerCAT users can assign missions to devices to help assess security risks due to network vulnerabilities and threats.
- **Generates Reports.** MeerCAT auto-generates a range of reports to present the results of an audit or security analysis, such as in Word or Power Point. MeerCAT also allows users to copy a MeerCAT view and place on a clipboard, export to an image file, drag and drop to other applications, and e-mail to colleagues and decision makers.
- **Delivers Out-of-the-Box Integration.** MeerCAT's data integration with wireless discovery and other security tools allow users to get immediate visual results from site surveys and security audits.

2 Getting Help With MeerCAT

2.1 MeerCAT Technical Support

All technical inquiries and bug reports can be submitted via email to meercat-support@securedecisions.com.

2.2 MeerCAT Feedback and Additional Information

Applied Visions, Inc. welcomes and encourages feedback on its products from its customers. Please submit your product inputs, user requirements and feedback to meercat@securedecisions.com.

2.3 Licensing

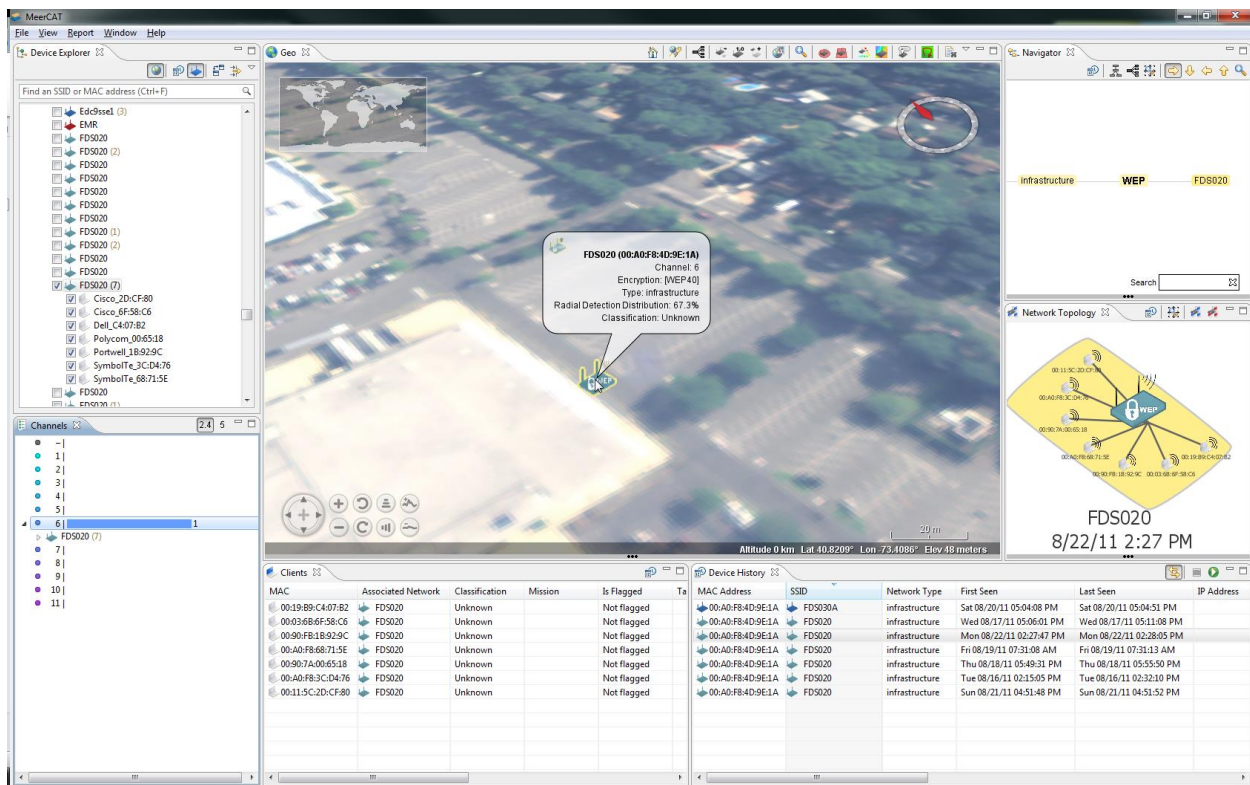
The MeerCAT software is distributed with license key(s) for each qualified licensed user in your organization. Please refer to your MeerCAT Software License Agreement for terms and conditions. If you require additional licenses, please contact Applied Visions, Inc. at meercat@securedecisions.com.

3 Accessing and Navigating MeerCAT

3.1 Controlling MeerCAT

3.1.1 Coordinated Views

Interactions between two or more views in the MeerCAT workspace are coordinated through MeerCAT's highlighting features. Selecting data in any view highlights the data in yellow in the other views.



The screenshot displays the MeerCAT interface with several panels:

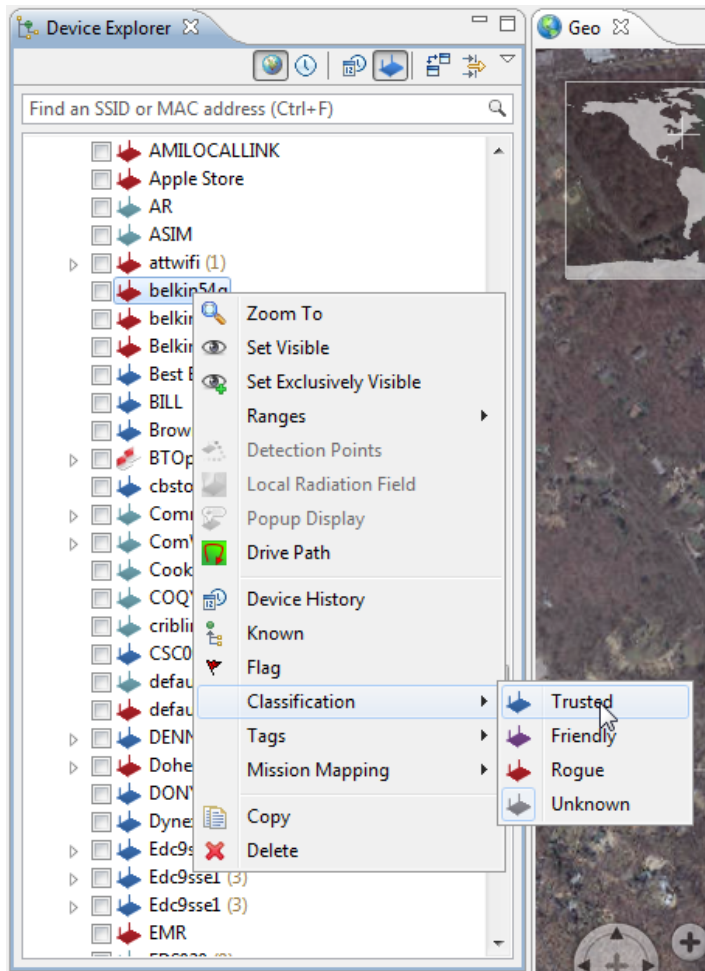
- Device Explorer:** A tree view on the left showing a list of devices, including multiple instances of 'FD5020' and various manufacturer MAC addresses like 'Cisco_2D-CF-80' and 'Dell_C4-07-B2'.
- Map View:** A central aerial map showing a building complex. A callout box for 'FD5020 (00:A0:F8:4D:9E:1A)' is displayed, providing details: Channel: 6, Encryption: (WEP40), Type: infrastructure, Radial Detection Distribution: 67.3%, and Classification: Unknown.
- Network Topology:** A diagram on the right showing a central 'WEP' node connected to several peripheral nodes, with the text 'FDS020 8/22/11 2:27 PM' below it.
- Clients Table:** A table at the bottom showing a list of clients with columns for MAC, Associated Network, Classification, Mission, Is Flagged, and IP Address.

MAC	Associated Network	Classification	Mission	Is Flagged	IP Address
00:19:89:C4:07:B2	FD5020	Unknown		Not flagged	
00:03:68:6F:58:C6	FD5020	Unknown		Not flagged	
00:50:F8:1B:92:9C	FD5020	Unknown		Not flagged	
00:A0:F8:68:71:5E	FD5020	Unknown		Not flagged	
00:50:7A:00:65:18	FD5020	Unknown		Not flagged	
00:A0:F8:3C:D4:76	FD5020	Unknown		Not flagged	
00:11:5C:2D:CF:80	FD5020	Unknown		Not flagged	

By placing different views in separate monitors (by dragging the view title bar) the user has access to simultaneous views of summary and detailed information.

3.1.2 Context Menus

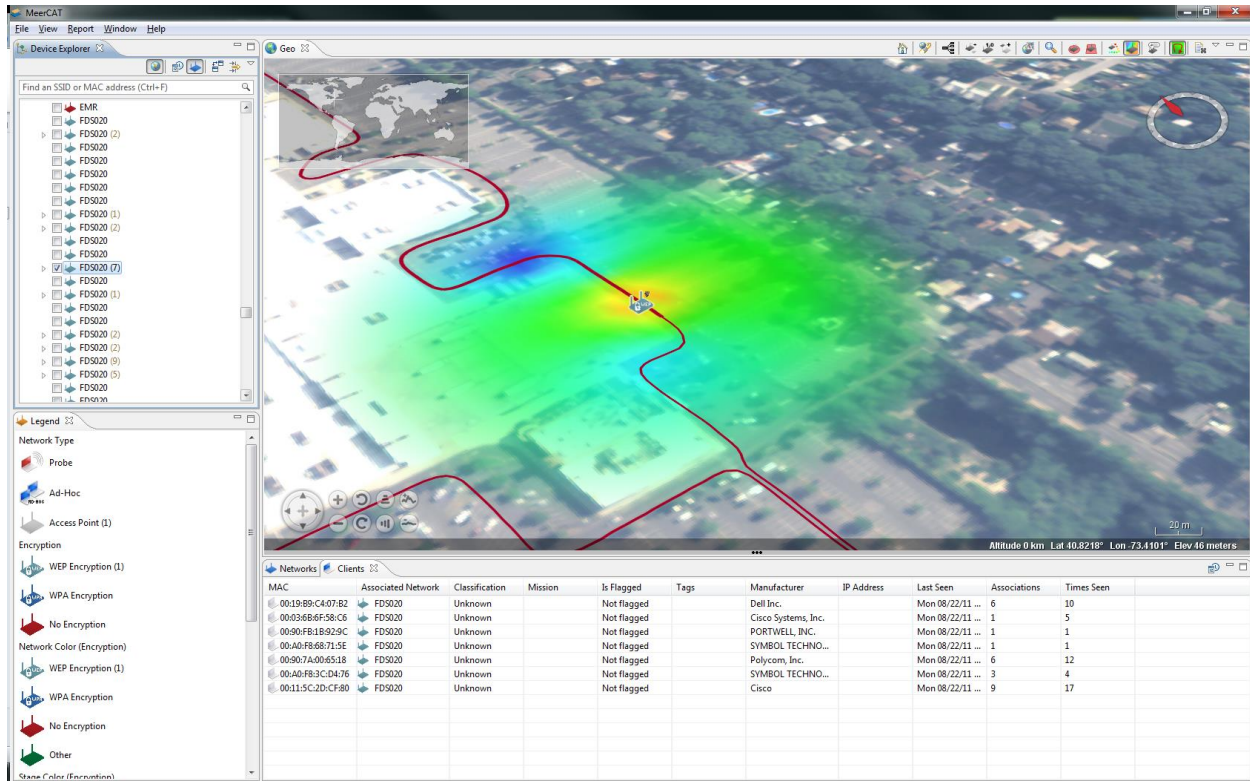
Pressing the right mouse button within some views displays contextual menus based on the data represented by a selected data element. The example below shows the contextual menu for an access point listed in the Device Explorer.



3.2 Customizing the MeerCAT Console

3.2.1 Views

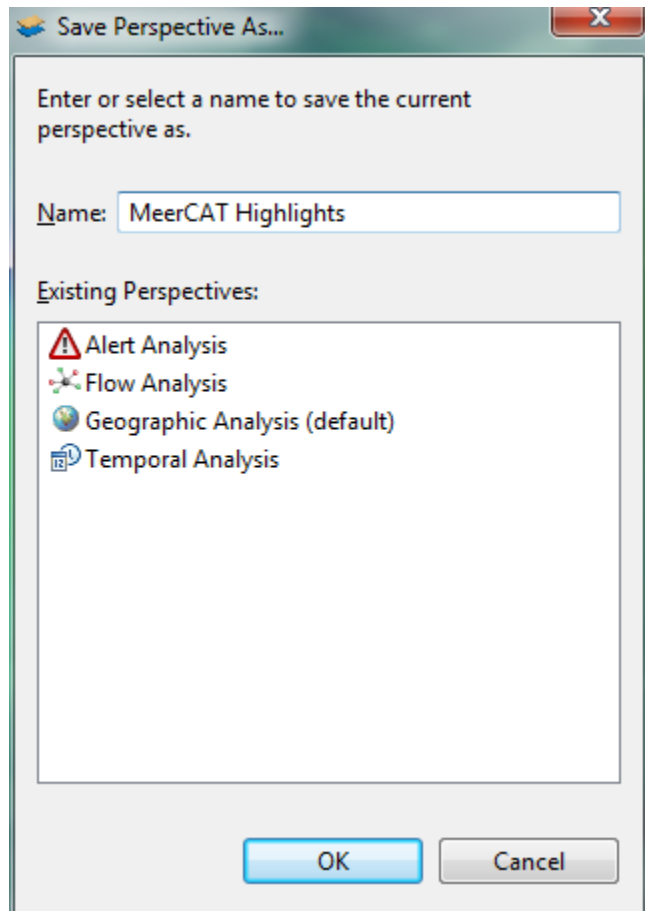
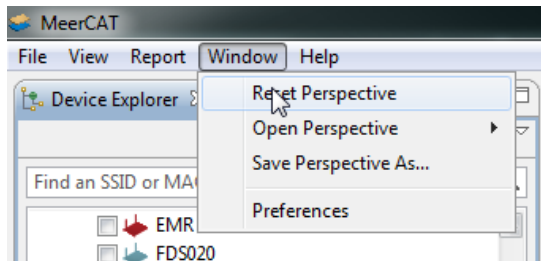
There are several windows in the default perspective of MeerCAT; each window is called a view. The individual views are described in detail in *Using MeerCAT - Fundamental Tools*.



Views can be re-sized by grabbing and dragging the view bounds, or by using the minimize or maximize buttons. Views can be rearranged by dragging the view's title bar to another location. *Docking a View* is changing the location of the view in the current layout. *Detached Views* are views that are shown in a separate window with a smaller trim. When working with multiple monitors, it can be useful to put a detached view on a separate monitor. To detach a view, drag the view to the outside of the application window and release the mouse button.

The layout of the views is called a *Perspective*. The first time MeerCAT is launched the following views are displayed: Device Explorer, Legend, Known Devices, Geo, Networks, and Clients. This is referred to as the *Default Perspective*. You can always return to the default perspective by choosing *Window -> Reset Perspective* from the main menu bar. To save the current layout, choose *Save Perspective As*.

The default perspective may be customized. To save the current perspective (layout), choose *Save Perspective As* under the *Window* menu item.



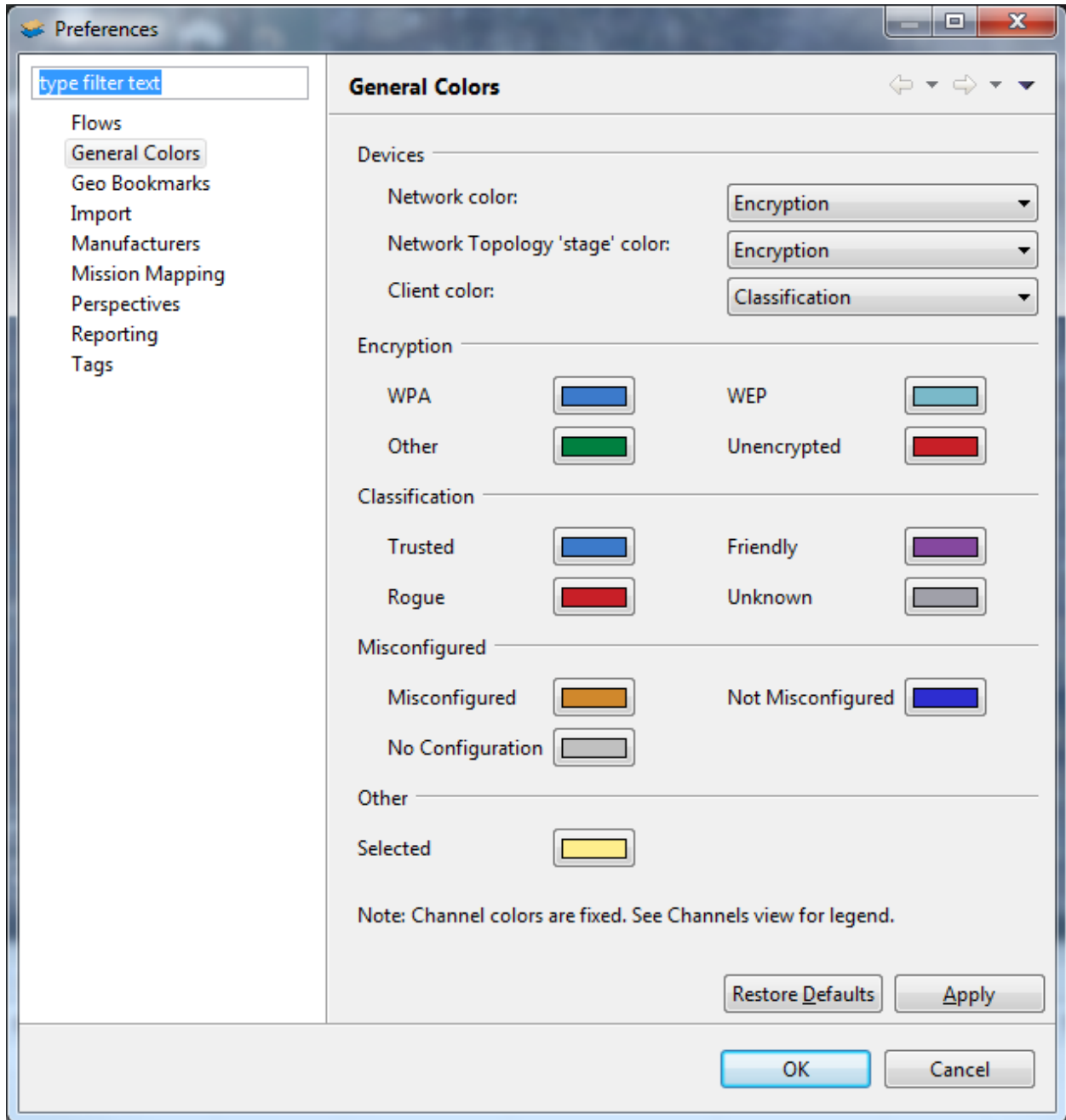
Any view that has been closed can be reopened by choosing the *View* menu from the main MeerCAT menu.

3.2.2 Preferences

Preferences allow you to customize colors, and set various options for some views. To access Preferences, select from the *MeerCAT Window* menu:

Window -> Preferences

The default colors for Flows view are shown below.



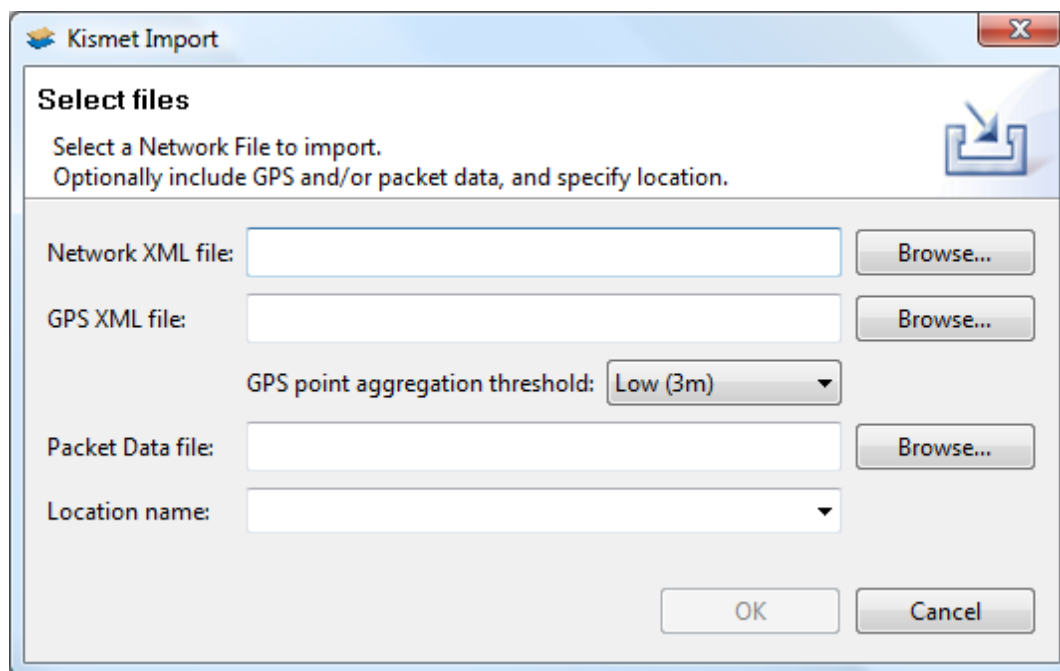
4 Importing Data into MeerCAT

4.1 Importing Kismet Data

1. To import Kismet (including Newcore) data you have collected, or the sample data set supplied with the MeerCAT CD, select from the MeerCAT File Menu:

File -> Import Kismet Data...

This will launch the pop-up window:



2. On the Network XML file edit, click 'Browse', and then search for the folder with the Kismet network data formatted file (.xml or .netxml for Newcore) you want to import into MeerCAT. The default location of the sample Kismet data is: C:\Program Files\MeerCAT\demo.
3. On the GPS XML file edit, click 'Browse', and then search for the folder with the Kismet GPS XML file (.gps or .gpsxml for Newcore) you want to import into MeerCAT. This file is optional, but if selected will provide more analysis on the location of devices, such as range-based displays, like the radiation field.

The MeerCAT database supports the storage of large number of data files and high performance data queries to quickly view and compare multiple wardrives. Nevertheless, you can choose to aggregate GPS detection points that are close to each other, in order to minimize the number of points that are stored in the database. The default setting is 3

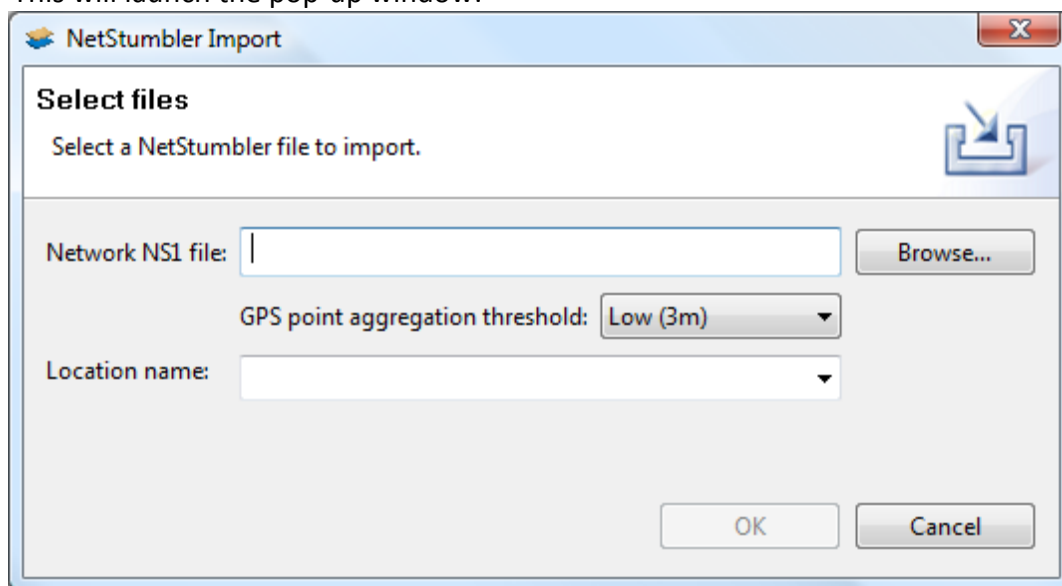
meters; this means that if two points are less than 3 meters apart, they will be combined and treated as one point. Increasing this threshold will allow more points to be combined, and reduce the number of points that need to be stored. If you have a very long detection run you may wish to increase this threshold in order to reduce the time it takes to import the data.

4. On the Packet Data file edit control, click 'Browse', and then search for the folder with the Kismet Packet Data file (.pcap, .dump, or .pcapdump) you want to import into MeerCAT. This file is optional, but if selected will provide data for the Flows and Flow Details packet views.
5. On the Location name edit enter the name of the location you would like to import the data into, such as the name of the site or building that was scanned. If you perform subsequent scans of the same location, you should select that location in the dropdown menu. If no location is specified, the data will get added to an 'Unspecified Location' entry.
6. Once you have selected the file, click 'OK' to import the data into the MeerCAT database.
7. To import more than one file, repeat Steps 1-5 above for each file you choose to import for analysis.

4.2 Importing NetStumbler Data

1. To import NetStumbler data you have collected, select from the *MeerCAT File Menu*
File -> Import NetStumbler Data...

This will launch the pop-up window:



2. On the *Network NS1 file edit*, click 'Browse', and then search for the folder with the *NetStumbler data formatted file (.ns1)* you want to import into MeerCAT.

The MeerCAT database supports the storage of large number of data files and high performance data queries to quickly view and compare multiple wardrives. Nevertheless, you can choose to aggregate GPS detection points that are close to each other, in order to minimize the number of points that are stored in the database. The default setting is 3 meters; this means that if two points are less than 3 meters apart, they will be combined and treated as one point. Increasing this threshold will allow more points to be combined, and reduce the number of points that need to be stored. If you have a very long detection run you may wish to increase this threshold in order to reduce the time it takes to import the data.

3. On the *Location name edit* control enter the name of the location you would like to import the data into, such as the name of the site or building that was scanned. If you perform subsequent scans of the same location, you should select that location in the dropdown menu. If no location is specified, the data will get added to an 'Unspecified Location' entry.

4. Once you have selected the file, click 'OK' to import the data into the *MeerCAT database*.

5. To *import more than one file*, repeat Steps 1-3 above for each file you choose to import for analysis.

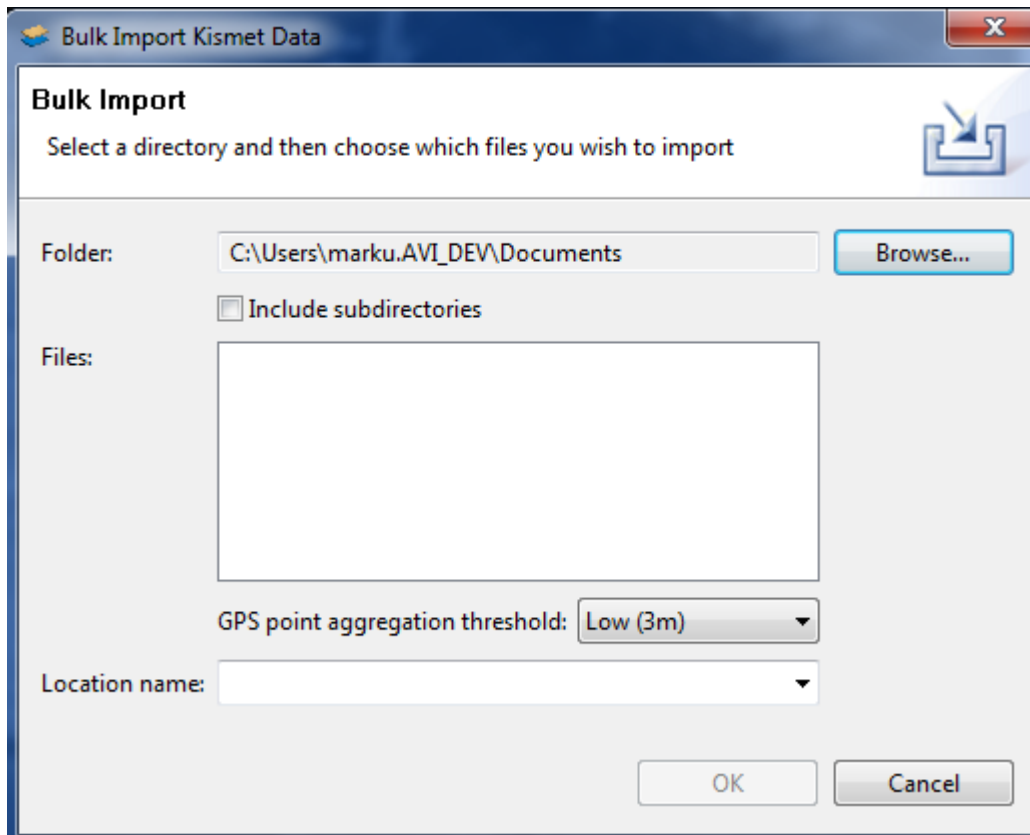
Note: NetStumbler only reports no encryption or WEP encryption. Devices may be a higher encryption, but only show as WEP. Also, NetStumbler does not collect client information nor does it collect packet data. Therefore the Network Topology view will be limited and the Flows and Flow Details views cannot be used.

4.3 Bulk Import Kismet Data

MeerCAT can import multiple Kismet data files in a single command. Access this feature through the *MeerCAT File Menu*:

File -> *Bulk Import Kismet Data ...*

This will launch the pop-up window:



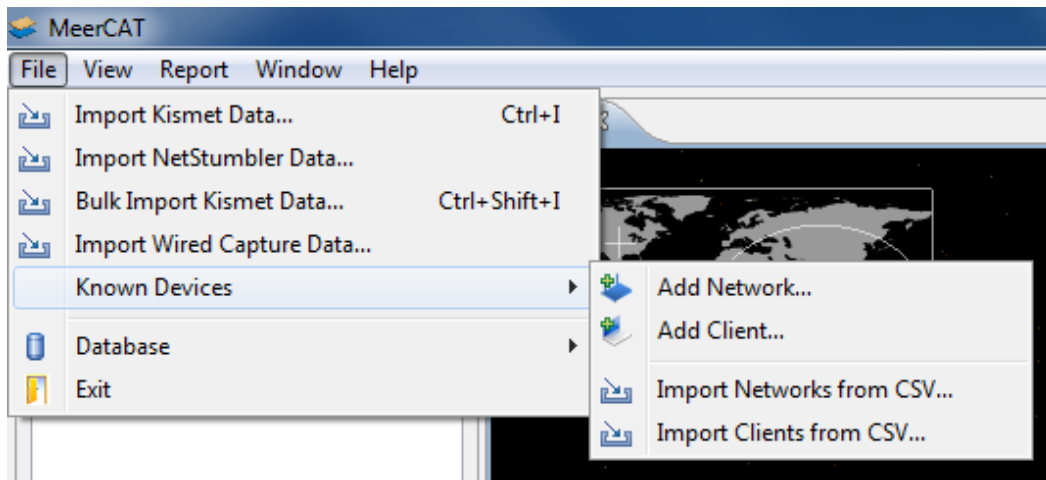
The Include subdirectories checkbox allows MeerCAT to search subdirectories for Kismet data to import.

The Location name can be entered manually, or, if an existing location is associated with the detection run, it can be selected from the dropdown.

4.4 Known Devices

MeerCAT allows you to add known devices, which serve as a baseline to alert MeerCAT users of unexpected changes, such as misconfigured devices or new devices that were not previously identified. This information is critical in defending one's network and enforcing security policies.

The Known Devices submenu can be selected from the *MeerCAT File Menu*.



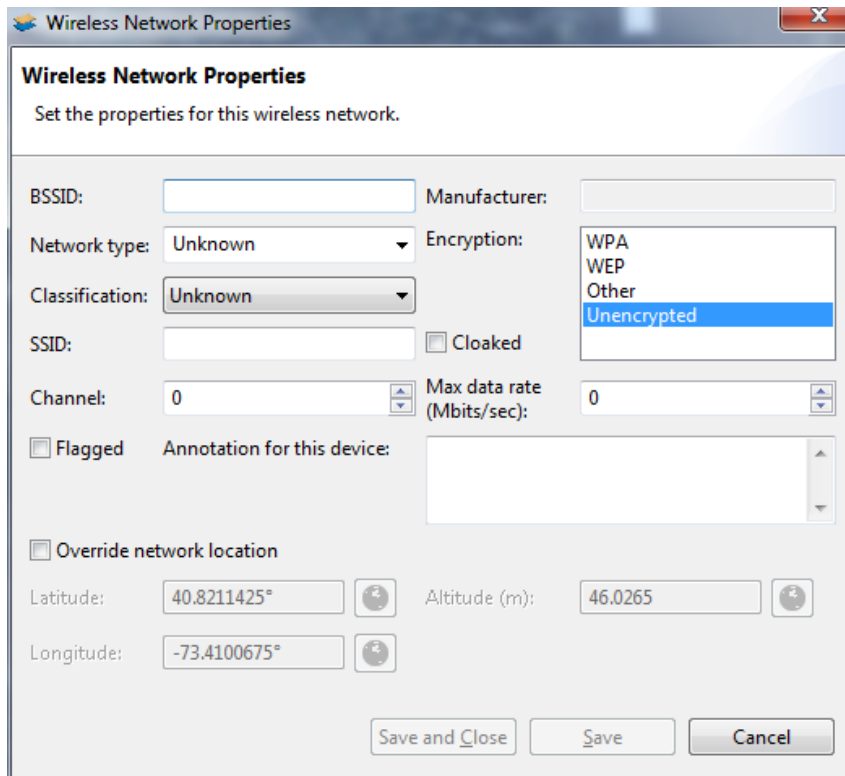
4.4.1 Manually Adding Known Devices

4.4.1.1 Known Networks

To add a known Network, select from the MeerCAT File Menu:

File -> Known Devices -> *Add Network...*

This will open a properties dialog where you can fill in the expected information for the network:



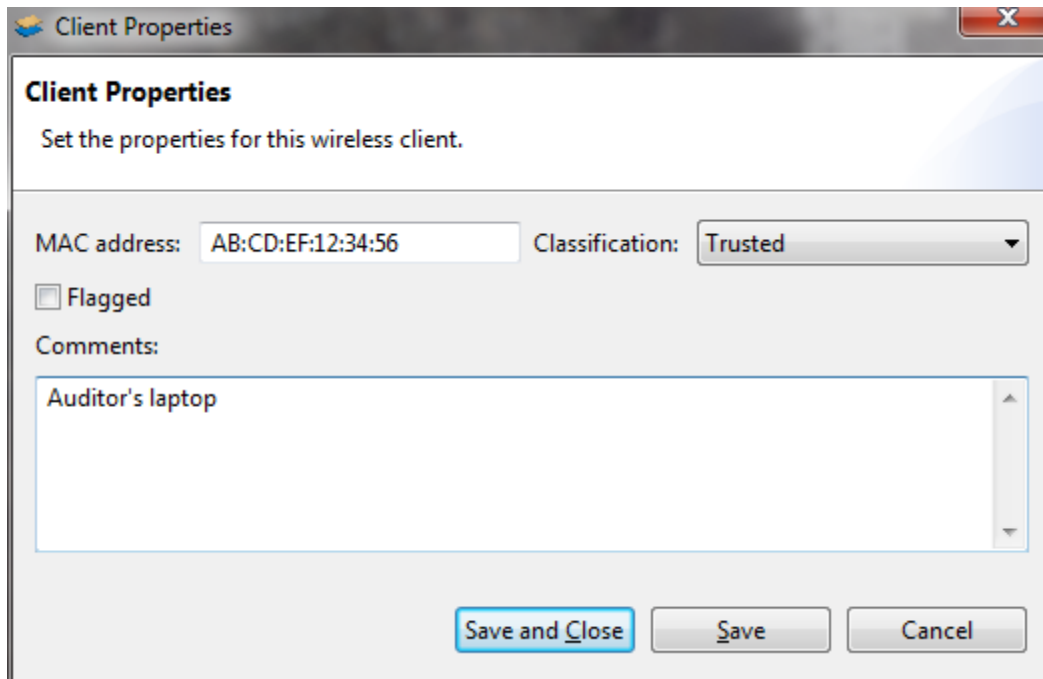
The information will be applied to any instances of the network that have been detected or that are detected in the future.

4.4.1.2 Known Clients

To add a known client device, select from the *MeerCAT File Menu*:

File -> Known Devices -> *Add Client...*

This will open a properties dialog where you can fill in the expected information for the client. The information will be applied to any instances of the client that have been detected or that are detected in the future.



4.4.2 Importing Known Devices from a CSV File

MeerCAT also supports importing CSV (Comma Separated Values) files. Its purpose is to import a list of known devices into MeerCAT.

1. To import a CSV file, select from the **MeerCAT File Menu**:

File -> Known Devices -> Import [Networks/Clients] from CSV...

This will launch a browser window to locate and select the CSV file to import.

Tip 1: *Sample CSV files* are provided on the MeerCAT CD.

Tip 2: The expected **order of the CSV file fields** are as follows:

Known Networks: SSID, BSSID, Classification (trusted, friendly, rogue, unknown), Channel, Type (infrastructure, ad-hoc, probe), Max Rate, Encryption (WPA, WEP, None), Cloaked

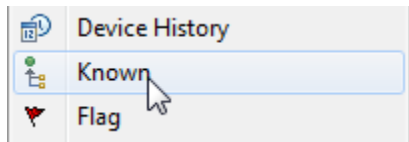
Known Clients: MAC address, Classification (trusted, friendly, rogue, unknown)

Tip 3: Users can **manually redefine the classification of wireless devices** or set the 'baseline expected configuration' of known devices in the Device Explorer.

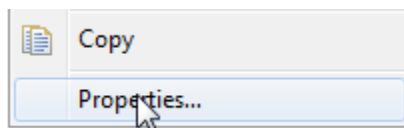
2. To **import more than one CSV file** (for example, to import a CSV file for wireless networks, and a separate CSV file for wireless clients), repeat Step 1 for each file.

4.4.3 Marking existing devices as Known

To mark a device that has already been imported as Known, right-click it in the Device Explorer and choose the Known option.

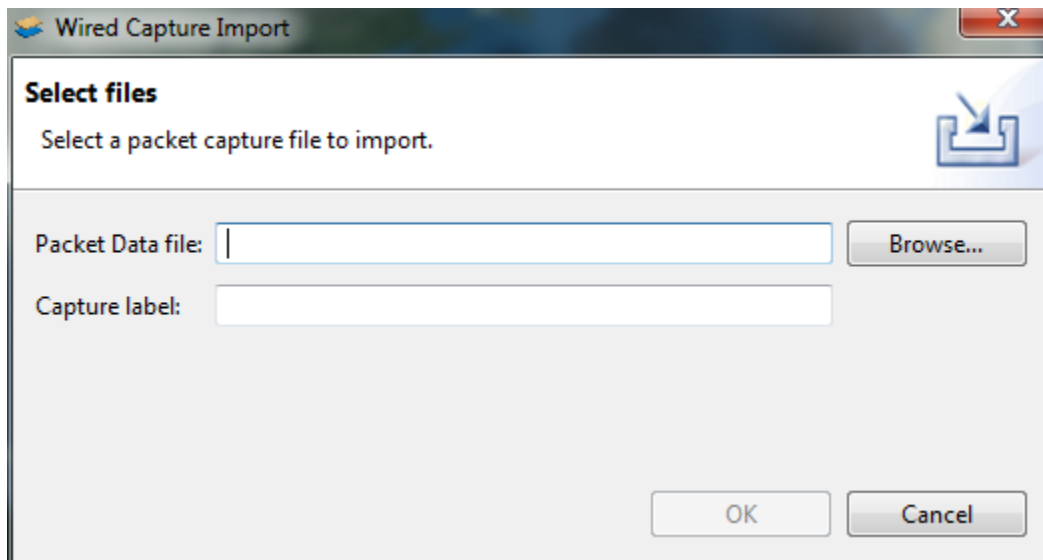


This will add the device to the Known Devices view and allow for its properties to be changed via a new Properties context menu command:



4.5 Importing Wired Capture Data

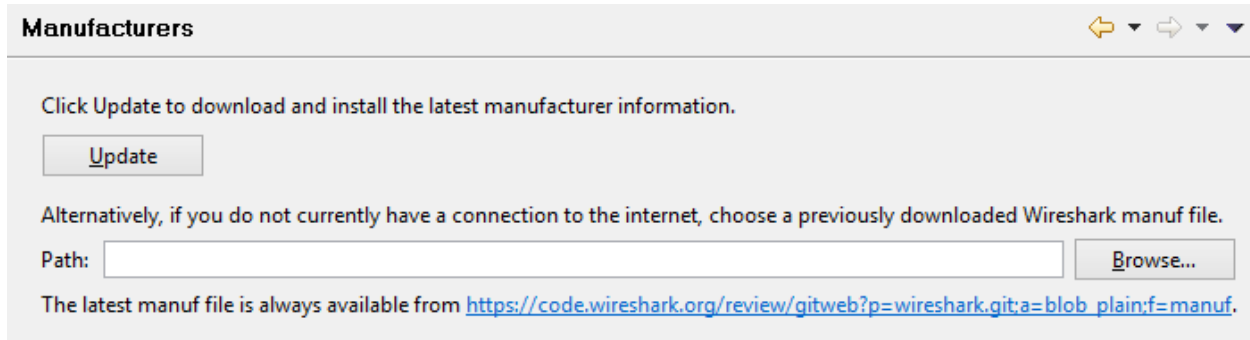
MeerCAT allows users to import Ethernet packet captures for limited use in some views, namely in the Flow Details View and the IP flow graph type of the Flows View.



To import a wired (Ethernet) capture, click File on the MeerCAT menu and select “Import Wired Capture Data...” This will bring you to an import dialog as illustrated above.

4.6 Manufacturers

MeerCAT determines the manufacturers of each device based on their MAC address. If some manufacturers are appearing as 'Unknown manufacturers', it is possible that a newer version of the manufacturers list containing a mapping is available. To update the manufacturers list, go to the Manufacturers section of the Preferences (Window → Preferences).



The list can either be updated online or from a previously downloaded file.

5 Using MeerCAT – Fundamental Tools

5.1 MeerCAT Console

The MeerCAT Console provides multiple coordinated views of the same data for faster incident investigation. You can select a device of interest in one MeerCAT window, which will highlight the device in all other views to provide you various perspectives.

5.2 Device Explorer View

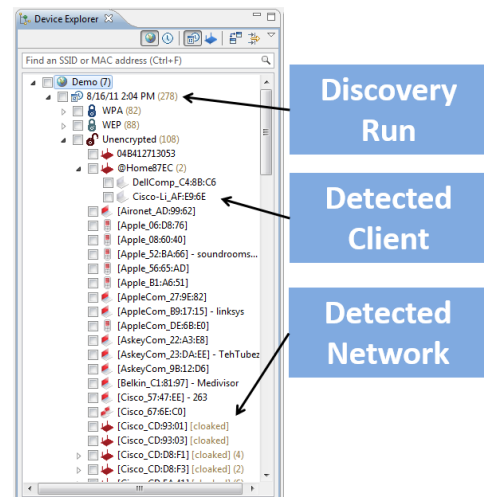
The Device Explorer view shows the imported *discovery runs* and lists the detected networks and connected clients for each run. It enables you to view, analyze, and filter wireless discovery and security data by a range of variables such as the device type, manufacturer, SSID and other device property. The Device Explorer also provides a number of tools for coordinating other MeerCAT Console views and identifying the attributes of detected wireless devices:

1. Expand each *discovery run* to display the individual networks detected.

Click on the arrow symbol adjacent to each session run to expand the view of detected networks. See sample showing circled icon below.

Tip 1: Number of detected networks in a discovery run is the number adjacent to the run.

Tip 2: Networks with unknown locations are annotated with a '?' mark on the device icon.



2. Expand each discovered network to show the discovered clients connected to that network.

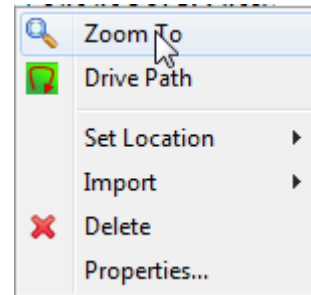
Click on the arrow symbol adjacent to each network to expand the view of detected connected clients.

3. Zoom in on a discovery run or network for all MeerCAT Views

Right-Click [discovery run or network] -> Zoom To

-or-

Double-Click [discovery run, network or device]



Tip 3: Delete discovery run data by:

Right Click [on Discovery Run in Device Explorer] ->
Select Delete.

5.2.1 Search

The Device Explorer can be searched based on SSID (networks) or MAC address (networks and clients). Valid queries consist of SSIDs of at least three characters or MAC addresses of at least two octets. An asterisk (*) can be used within the query to represent any series of characters, and a question mark (?) can be used in place of any single character. There is no need to supply a leading or trailing asterisk, as partial matches will be returned by default.

5.2.2 Toolbar

The toolbar of the Device Explorer view contains the following buttons:

Toggle Detection Run Location Grouping

Determines whether or not to group the networks and detection runs by the 'location' that was specified when the data was imported.

Toggle Last Seen Grouping

Groups items by when they were last seen, relative to the current time. For example, 3 days ago, 2 weeks ago, 6 months ago, 1 year ago.

Detection Runs

Shows a list of detection runs, and expanding each detection run will show the individual devices that were detected on that run.

Networks

Displays the latest history for all devices detected across all detection runs. The user can then select a network and look at the 'Device History' view to see the instances when the device was seen (if 'Link With Selection' is enabled in that view).

If a particular historical instance is selected within the Device History view, that instance will be shown instead of the latest (except in the Network and Clients table views).

Compare Detection Runs

Allows the user to select detection runs and compare them by showing only the devices that changed from one detection run to another by looking at several attributes.

Filter Wireless Networks

Shows only wireless devices that fit criteria specified by the user in the selection window.

View Menu

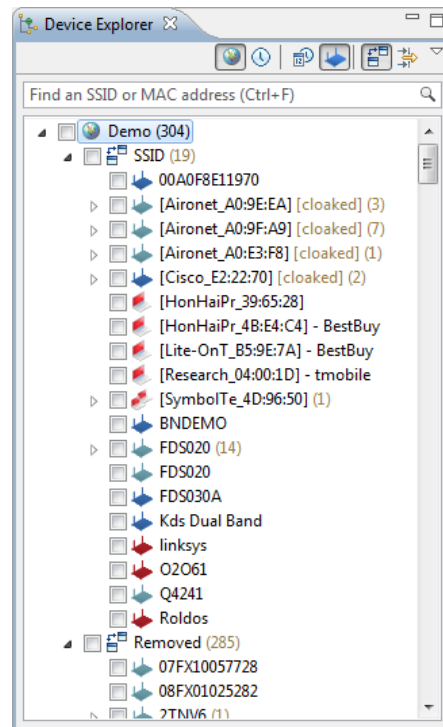
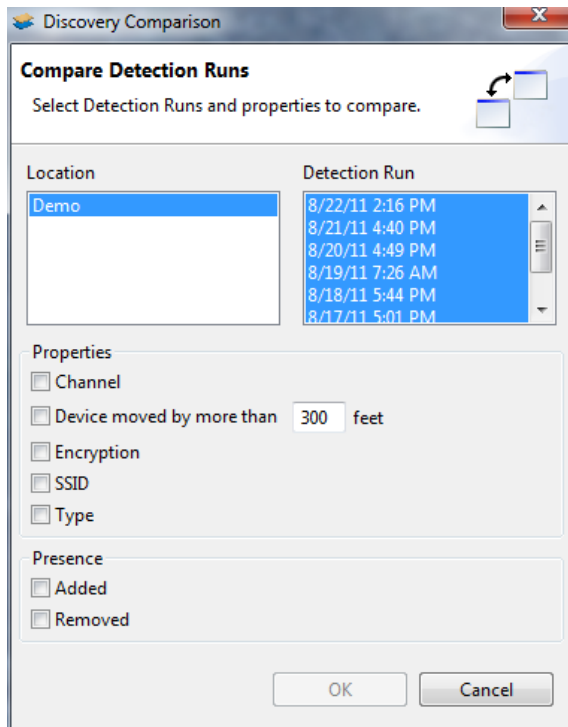
Allows user to change the order that the devices show up ('Sorting') and optionally group the devices by a criterion (e.g., grouped by encryption type). You can also export or import the list of items that are currently checked off in the Device Explorer.

5.2.3 Illustrative Discovery Comparison Examples

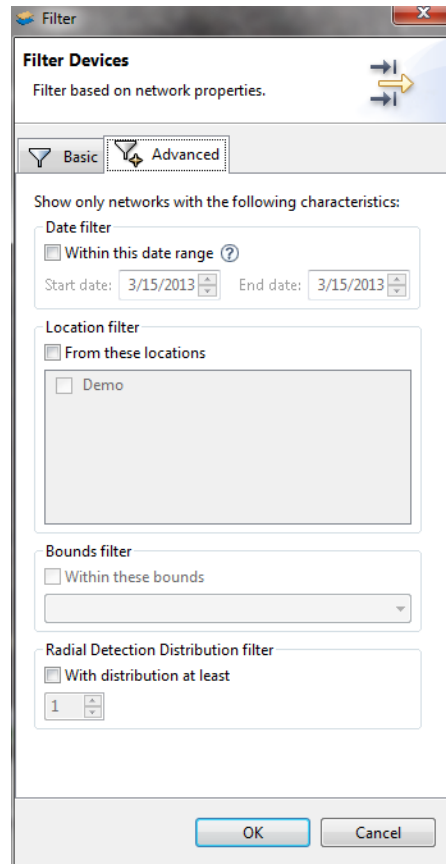
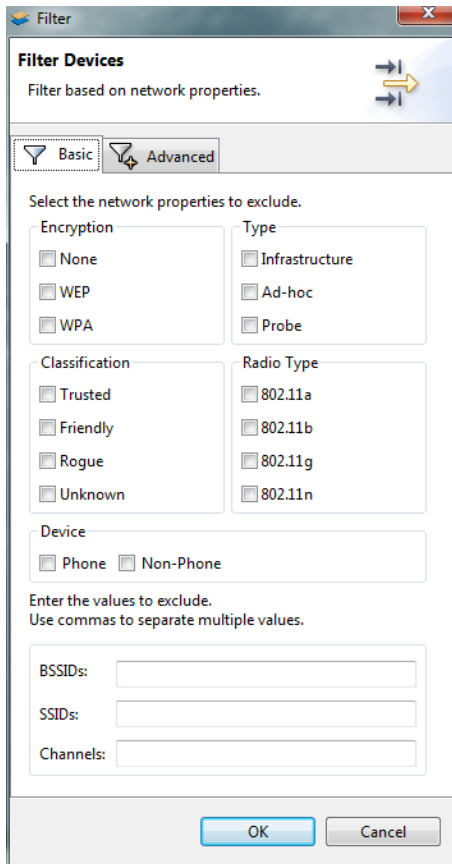
With Compare Detection Runs you can see if a particular network has changed its channel, location, encryption, SSID, or type which is beneficial in alerting you to security concerns or validating whether a corrective action has resolved an issue. Additionally, it is possible to determine whether a device that was present in an earlier detection run is absent in a later run, or vice versa.

Choose the detection runs you want to compare by holding the SHIFT or CTRL key down to select them. Check off the attributes you want to compare.

The devices that remain match the comparison criteria you have selected, grouped by the property in which the change occurred:

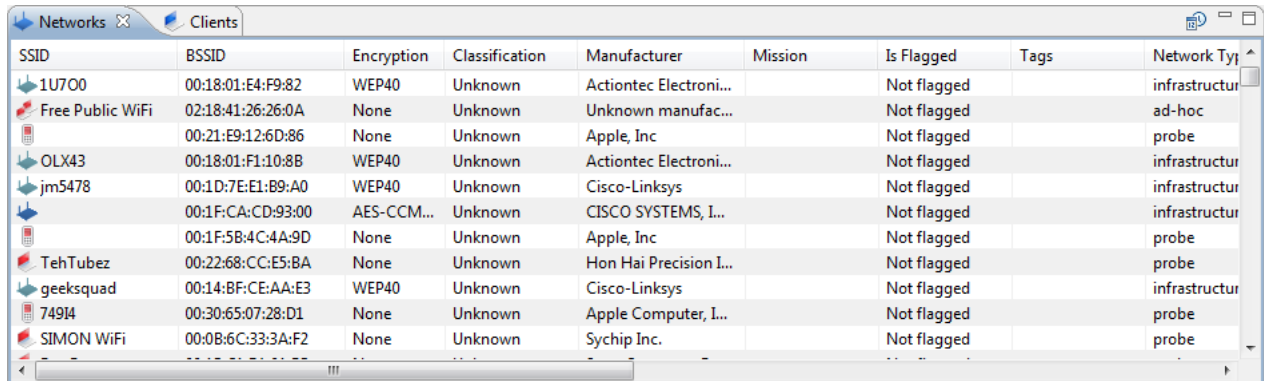


The Wireless Network filter shows only wireless devices that fit the criteria specified by the user in the selection window.



5.3 Networks View

The Networks View offers another tool to simplify wireless device management and security, and helps you identify network devices based on their properties including their MAC address, SSID, vendor, security, or channel. With the Network Device table you can easily browse and sort through the various categories of detected devices to quickly validate unauthorized devices.



SSID	BSSID	Encryption	Classification	Manufacturer	Mission	Is Flagged	Tags	Network Type
1U700	00:18:01:E4:F9:82	WEP40	Unknown	Actiontec Electroni...		Not flagged		infrastructur
Free Public WiFi	02:18:41:26:26:0A	None	Unknown	Unknown manufac...		Not flagged		ad-hoc
OLX43	00:21:E9:12:6D:86	None	Unknown	Apple, Inc		Not flagged		probe
jm5478	00:1D:7E:E1:B9:A0	WEP40	Unknown	Cisco-Linksys		Not flagged		infrastructur
	00:1F:CA:CD:93:00	AES-CCM...	Unknown	CISCO SYSTEMS, I...		Not flagged		infrastructur
	00:1F:5B:4C:4A:9D	None	Unknown	Apple, Inc		Not flagged		probe
TehTubez	00:22:68:CC:E5:BA	None	Unknown	Hon Hai Precision I...		Not flagged		probe
geeksqquad	00:14:BF:CE:AA:E3	WEP40	Unknown	Cisco-Linksys		Not flagged		infrastructur
74914	00:30:65:07:28:D1	None	Unknown	Apple Computer, I...		Not flagged		probe
SIMON WiFi	00:0B:6C:33:3A:F2	None	Unknown	Sychip Inc.		Not flagged		probe

5.3.1 Toolbar

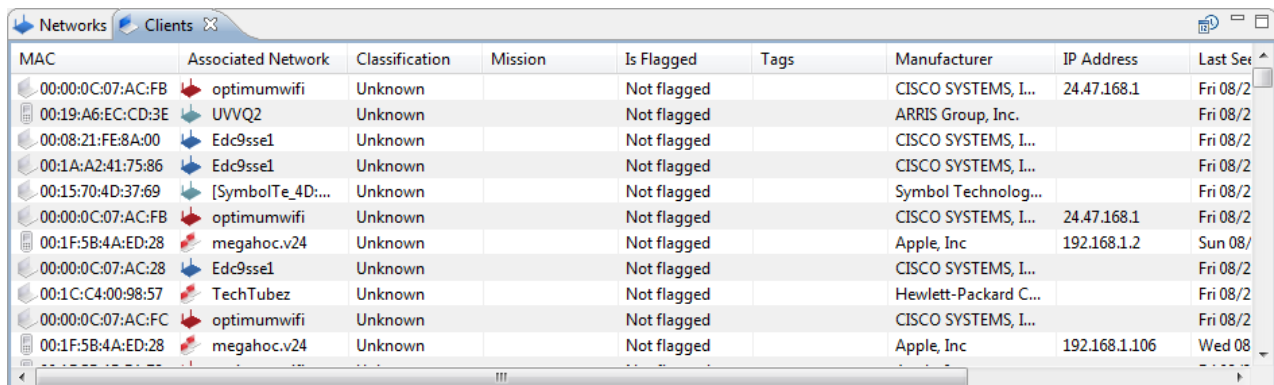
The toolbar of the Networks view contains the following button:



This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of the particular wireless network(s) in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s).

5.4 Clients View

The Clients View is a companion to the Networks View, offering another tool to simplify wireless device management and security. The Clients View helps you identify individual client devices based on their properties including their MAC or IP address, associated network, classification, or when they were last seen. With the Clients View you can easily browse and sort through the various categories of detected client devices to quickly validate unauthorized devices. The Associations column can be useful for finding clients that have made connections to multiple networks.



MAC	Associated Network	Classification	Mission	Is Flagged	Tags	Manufacturer	IP Address	Last Seen
00:00:0C:07:AC:FB	optimumwifi	Unknown		Not flagged		CISCO SYSTEMS, I...	24.47.168.1	Fri 08/2
00:19:A6:EC:CD:3E	UVVQ2	Unknown		Not flagged		ARRIS Group, Inc.		Fri 08/2
00:08:21:FE:8A:00	Edc9sse1	Unknown		Not flagged		CISCO SYSTEMS, I...		Fri 08/2
00:1A:A2:41:75:86	Edc9sse1	Unknown		Not flagged		CISCO SYSTEMS, I...		Fri 08/2
00:15:70:4D:37:69	[SymbolTe_4D:...	Unknown		Not flagged		Symbol Technolog...		Fri 08/2
00:00:0C:07:AC:FB	optimumwifi	Unknown		Not flagged		CISCO SYSTEMS, I...	24.47.168.1	Fri 08/2
00:1F:5B:4A:ED:28	megahoc.v24	Unknown		Not flagged		Apple, Inc	192.168.1.2	Sun 08/
00:00:0C:07:AC:28	Edc9sse1	Unknown		Not flagged		CISCO SYSTEMS, I...		Fri 08/2
00:1C:C4:00:98:57	TechTubez	Unknown		Not flagged		Hewlett-Packard C...		Fri 08/2
00:00:0C:07:AC:FC	optimumwifi	Unknown		Not flagged		CISCO SYSTEMS, I...		Fri 08/2
00:1F:5B:4A:ED:28	megahoc.v24	Unknown		Not flagged		Apple, Inc	192.168.1.106	Wed 08

5.4.1 Toolbar

The toolbar of the Clients view contains the following button:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of the particular wireless client(s) in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s).

5.5 Geographic View

Modern network management tools integrate 3D Geographic tools with network diagrams to improve legibility and provide logical groupings of sub-networks. In MeerCAT, the Geo View provides this capability.

5.5.1 Tour of Geo View Capabilities

The **Geo View** provides the tools to locate wireless networks and clients on 3D topographic satellite imagery. Users can navigate anywhere on the globe down to street and building views to locate friendly and rogue devices.

Using the 'Zoom To' tool on a discovery run in the Device Explorer as described in Device Explorer View, the coordinated Geo View below that shows all the detected devices in the selected discovery run. The **Geo View** also provides tools to further analyze the attributes of detected wireless devices:

1. Display a **device attributes** by:

Right Click [Device] ->Show Popup Display

2. Invoke **Coordinated Views** to inspect wireless devices by:

Left Click [on any device on the map]

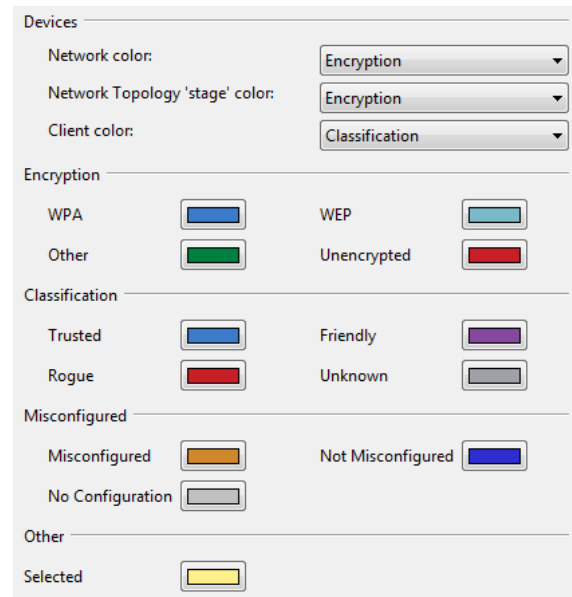
Tip 1: Encrypted devices show a lock symbol.

Tip 2: The **device encryption level** is displayed on the device icon (e.g., WPA or WEP).



This will highlight the device in the other MeerCAT Console views.

3. User customizable views are supported including the ability to **redefine the color coding of wireless networks**:
 - a. *MeerCAT Windows Menu -> Preferences... -> General Colors*
 - b. *Select the attribute that the device color will represent (Encryption, Classification or Channel)*
 - c. *Click on any color buttons to select the color code for the selected attribute.*



Tip 3: The **network color** is preconfigured to represent device classification. The default is:

Blue=Secure/Trusted Red =Unsecure/Rogue; Purple=Friendly; Orange=Misconfigured

5.5.2 Controls

Mouse with scroll wheel:

Pan:	Left mouse button click & drag - all directions or arrow keys or double-left-click an area.
Zoom:	Use the scroll wheel on the mouse or Hold CTRL and arrow up or down on the keyboard or Use + (zoom in) and – (zoom out) keys.
Tilt:	Right mouse button click & drag - up and down or Use PAGE UP and PAGE DOWN on the keyboard or Hold SHIFT and arrow up or down on the keyboard.
Rotate:	Right mouse button click & drag - left and right or Hold SHIFT and arrow left or right on the keyboard.
Stop:	Spacebar

Reset Heading:	N
Reset all:	R

Single button mouse:

Pan:	Left mouse button click & drag - all directions. Left mouse button click once to center view or arrow keys or double-left-click an area.
Zoom:	Hold CTRL on the keyboard and left mouse button click & drag - up and down or hold "Ctrl" and arrow up or down on the keyboard.
Tilt:	Hold SHIFT on the keyboard and left mouse button click & drag - up and down or use "Page Up" and "Page Down" on the keyboard.
Rotate:	Hold SHIFT on the keyboard and left mouse button click & drag - left and right.
Stop:	Spacebar
Reset Heading:	N
Reset all:	R

5.5.3 Toolbar

The toolbar of the Geo view contains the following buttons:



Go Home

Zoom Geo View to the Home location, or set the Home location if it has not been set.



Go to Location

Zoom Geo View to a city or zip code.



Set Icon Display Options

Set icon display options – controls automatic aggregation / sizing of icons of the map.



Decrease icon size

Decreases the size of all the icons on the map by half.



Set icon size to 1.0x

Sets all icons back to their original size.



Increase icon size

Increases the size of all the icons on the map by 2x.



Zoom to the Location on the map

Enabled when one or more networks are selected – zooms to those networks when clicked.



Show circular area depicting the longest distance a network was detected

Enabled when one or more networks are selected – draws a circle around the network showing the max detection radius.



Toggle polygonal area of points where a network was detected

Enabled when one or more networks are selected – draws a polygon (convex hull) enclosing all the points where the network is detected.



Show all points where the network was detected

Enabled when one or more networks are selected – shows all the points that a network was detected.



Toggle a display of the access point's interpolated signal strength

Enabled when one or more networks are selected – shows a “heatmap” which shows the signal strength around the network by interpolating from the detection points.



Show extra information about an item on the map

Enabled when one or more networks are selected – shows a callout with detailed information about the network(s):



Toggle display of the drive path for a detection run

Enabled when one or more detection runs are selected – draws a line depicting the drive path.



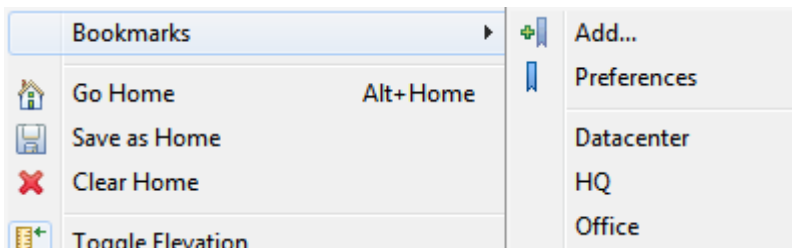
Clear Extra Display Info

Clears out all extra info on the map (annotations, range overlays).

Options Menu



Bookmarks: Add the current Geo View camera position as a bookmark, change the bookmark preferences or zoom Geo View to an existing bookmarked location.



Go Home: Zoom Geo View to the Home location, or set the Home location if it has not been set.

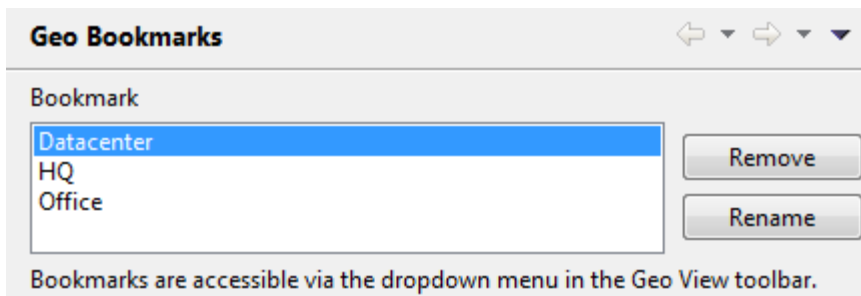
Save as Home: Save the current position as the Home position. Geo View will open at the Home position if it has been defined.

Clear Home: Clear the currently saved Home position

Toggle Elevation: Toggle between displaying elevation data and a flat globe.

Adhere Icons to Surface: Toggle between displaying icons on the surface of the earth and at their observed altitude according to GPS information.

Bookmarks can be removed or renamed from the Geo Bookmarks preference page.



5.5.4 3D Specialized Controls

Additional controls are available in this View to supplement navigation within the view. These

controls are shown below:



This set of controls and buttons can be found in the lower left corner of the Geo View.



Directional Control

Use this control to move the 3D image left, right, up or down.



Zoom

Use these buttons to zoom in or out.



Rotation

Use these buttons to rotate the image to the left or right.



Tilt

Use these buttons to tilt the image forward or backward.



Vertical Exaggeration

Use these buttons to increase or decrease vertical exaggeration.

5.5.5 Modifying the Geo View cache location

By default, MeerCAT will cache Geo View imagery to the MeerCATImagery directory within the ProgramData directory (typically C:/ProgramData).

The cache location can be changed by modifying the MeerCATDataFileStore.xml file within the MeerCAT directory in the user's home directory (created after the first time MeerCAT is launched).

For example, to read from and write to a cache on another drive (or possibly a network share mapped

as a drive), MeerCATDataFileStore.xml might look like the following:

```
<?xml version="1.0"?>
<dataFileStore>
  <readLocations>
    <location wwDir="Z:/MyData/MeerCATImagery"/>
  </readLocations>
  <writeLocations>
    <location wwDir="Z:/MyData/MeerCATImagery" create="true"/>
  </writeLocations>
</dataFileStore>
```

5.5.6 Adding additional Geo View imagery sources

Additional WMS imagery sources can be added to Geo View by adding configuration files for them to the Geo View cache location (see 5.5.5). For example, to add an aerial with labels layer for an OnTerra subscription, a file called OnTerraAerialWithLabels.xml can be placed into the Geo View cache location with the following contents:

```
<?xml version="1.0" encoding="UTF-8"?>
<Layer version="1" layerType="TiledImageLayer">
  <DisplayName>OnTerra Aerial with Labels</DisplayName>
  <Service serviceName="OGC:WMS" version="1.1.1">

<GetCapabilitiesURL>http://wms.onterrasystems.com/WMSService.svc/[key]/WMSLatLon?request=GetCapabilities</GetCapabilitiesURL>

<GetMapURL>http://wms.onterrasystems.com/WMSService.svc/[key]/WMSLatLon</GetMapURL>
  <LayerNames>OnTerraWMS</LayerNames>
  <StyleNames>AerialWithLabels</StyleNames>
</Service>
<RetrievePropertiesFromService>true</RetrievePropertiesFromService>
<LastUpdate>26 03 2009 00:00:00 GMT</LastUpdate>
<DataCacheName>OnTerra/AerialWithLabels</DataCacheName>
<ImageFormat>image/png</ImageFormat>
<AvailableImageFormats>
  <ImageFormat>image/png</ImageFormat>
</AvailableImageFormats>
<FormatSuffix>.png</FormatSuffix>
```

```

<TileOrigin>
    <LatLon units="degrees" latitude="-90" longitude="-180"/>
</TileOrigin>
<LevelZeroTileDelta>
    <LatLon units="degrees" latitude="36" longitude="36"/>
</LevelZeroTileDelta>
<TileSize>
    <Dimension width="512" height="512"/>
</TileSize>
<Sector>
    <SouthWest>
        <LatLon units="degrees" latitude="-85" longitude="-180"/>
    </SouthWest>
    <NorthEast>
        <LatLon units="degrees" latitude="85" longitude="180"/>
    </NorthEast>
</Sector>
<ForceLevelZeroLoads>true</ForceLevelZeroLoads>
<RetainLevelZeroTiles>true</RetainLevelZeroTiles>
<UseTransparentTextures>>false</UseTransparentTextures>
<RetrievalTimeouts>
    <ReadTimeout>
        <Time units="milliseconds" value="30000"/>
    </ReadTimeout>
</RetrievalTimeouts>
</Layer>

```

The layer will show up in Layers View as the value of DisplayName in the configuration file the next time MeerCAT is launched.

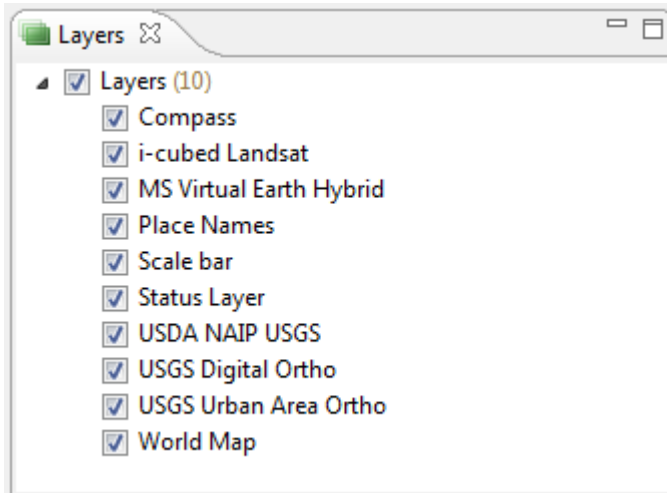
5.5.7 Adding Bing Imagery

Bing imagery can be displayed by using a key obtained from the Bing Maps Account Center (<http://www.bingmapsportal.com/>). Append the following line to MeerCAT.ini, located in the same directory as the MeerCAT executable, replacing [key] with a Bing Maps key.

```
-DbingMapsKey=[key]
```

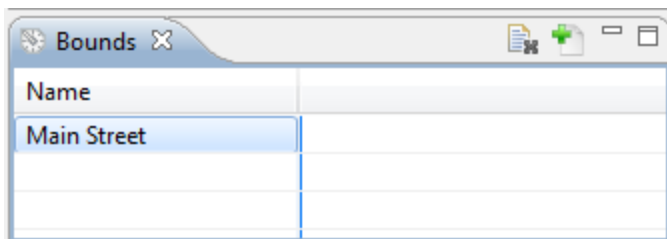
If a key is present, the Bing layers will show up in Layers View the next time MeerCAT is launched.

5.6 Layers View



The Layers view can be used to selectively disable and enable individual Geo View imagery sources.

5.7 Bounds View



The Bounds view displays a table of all of the bounds that have been stored by the Bounds Tool. Bounds can be used as criteria in the Device Explorer Filter or as part of an Alert Pattern. Clicking one of the Bounds will display it in the Geo View. If the entity is not within the visible area of the current view, double-clicking will zoom to it.

5.7.1 Toolbar

The Bounds View toolbar contains the following buttons:



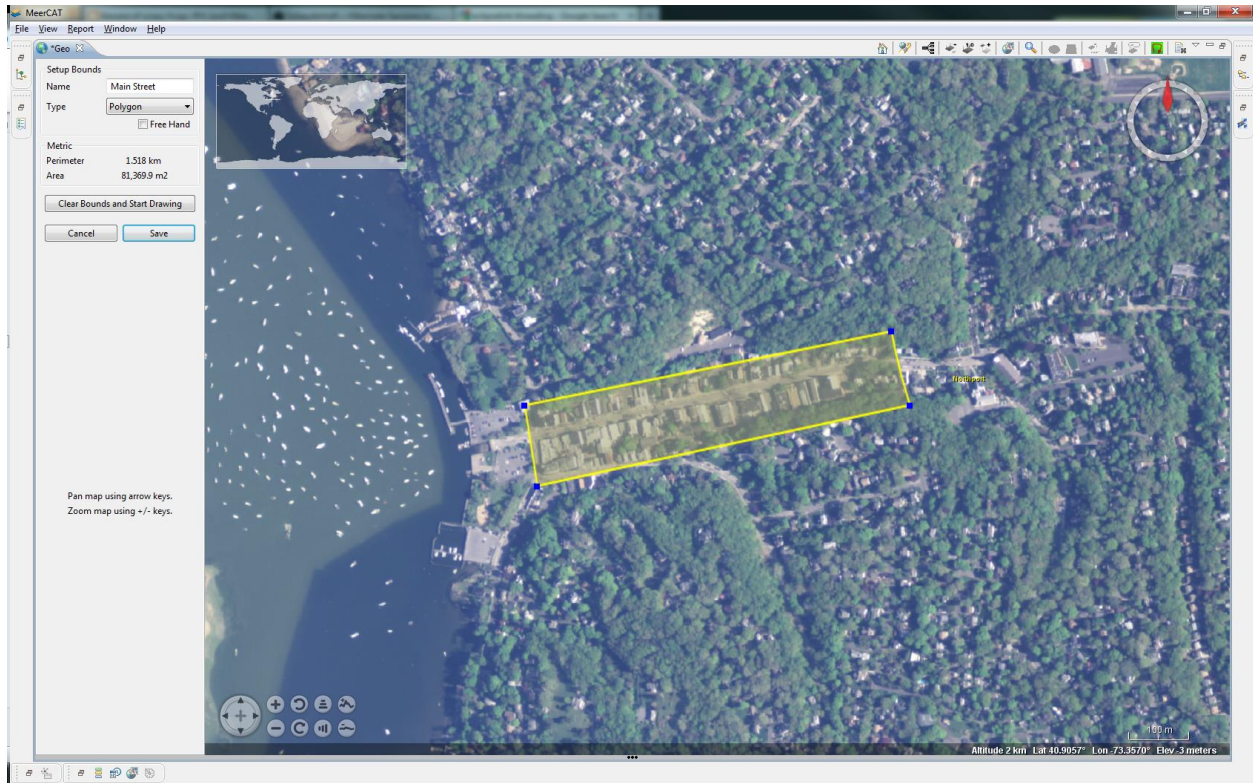
Clear Bounds Selection: De-select all Bounds to clear them from the Geo View



Add Bounds: Open the Bounds Tool to create new Bounds


5.7.2 Bounds Tool

The Bounds Tool is used to create and modify Bounds. Each Bounds entity must have a unique name.

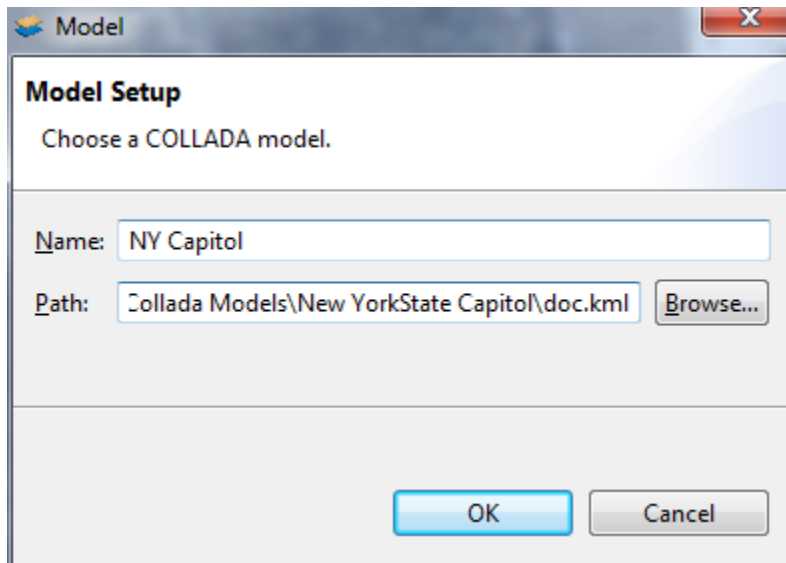


5.8 Models View

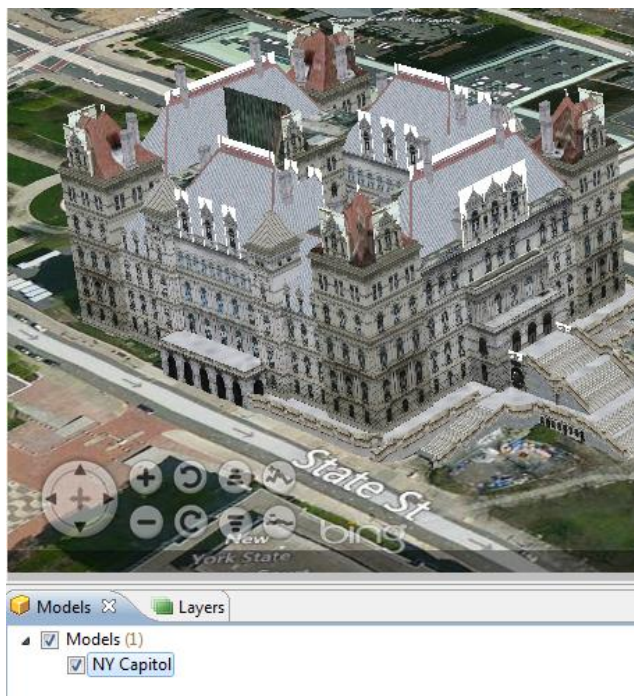
The Models view is used to import COLLADA models, such as those available from the 3D Warehouse (<http://sketchup.google.com/3dwarehouse/>), for viewing within the Geo view.

To add a model, click the 'Add Model' button in the Models view toolbar: 

Browse to the location of the model's KML file:



The model can now be toggled on and off of in Geo View via the corresponding checkbox in the Models view.



5.9 Network Topology View

MeerCAT automatically constructs topological maps of the discovered networks and connected clients to help you better understand the impact of wireless vulnerabilities and threat and

determine the appropriate remediation. MeerCAT helps you ‘see’ the detected access points and clients connected to them, including rogue and unsecure devices.

Coordinated views allow MeerCAT users to quickly spot a network of interest in the Network Topology View to help identify connected clients and potential risks for further investigation. If multiple networks are checked off in the Device Explorer, then the latest information for that network will be shown. If only one network is selected, then all histories will be shown side-by-side over time.

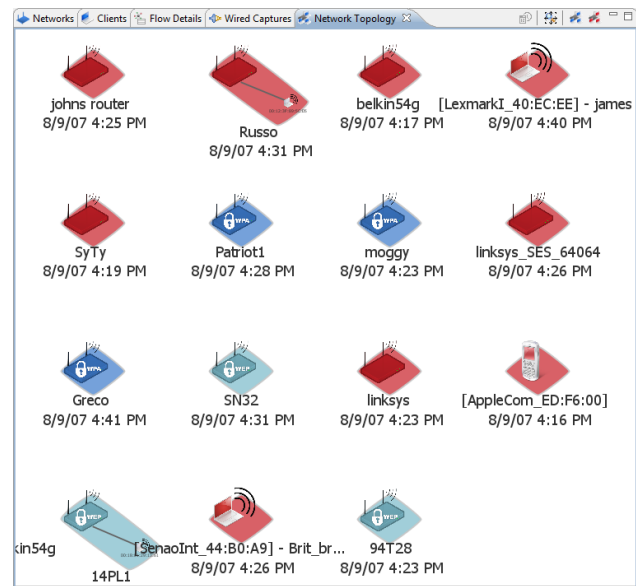
Tip 1: The **network ‘stage’ color** is preconfigured to represent the network security state, where the default coding is:

Red = unencrypted

Blue = encrypted

Stages highlighted in **yellow** indicate the device has been user-selected for coordinated views.

The ‘stage’ is user configurable MeerCAT Windows Menu ->Preferences...



MeerCAT provides tools to analyze device attributes in the Network Topology View:

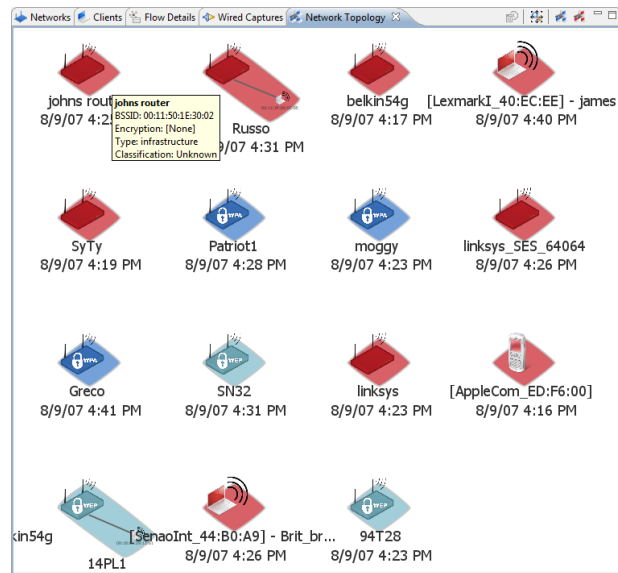
1. Place the mouse cursor over any device

A **'tooltip'** will appear with the devices attributes.

2. Invoke **Coordinate views** by:

Left Clicking any device

The device will be highlighted in all MeerCAT Console views.



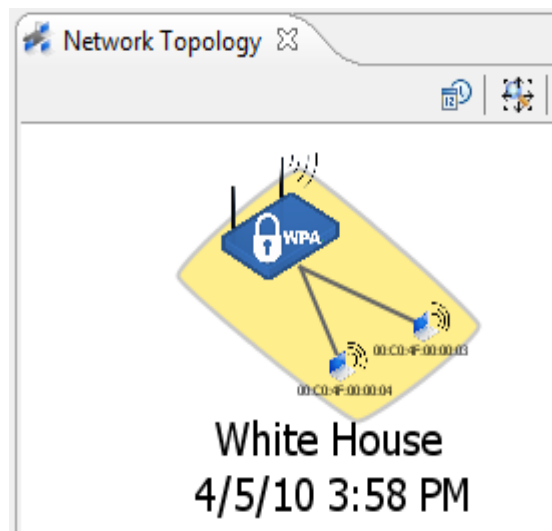
Tip 2: There are a number of tools to navigate in the Network Topology View:

- a) To **center a network of interest** in Network Topology View

Left Click and hold (anywhere in white space around network icon) -> Move mouse to area

- b) To **'Zoom In/Out'** on any network by:

Right Click and hold -> Move mouse forward and back



5.9.1 Toolbar

The toolbar of the Network Topology view contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in

which case the view will be updated to show only the selected instance of the particular network.

 **Zoom the display such that all of its contents are visible**

 **Show only networks with clients**

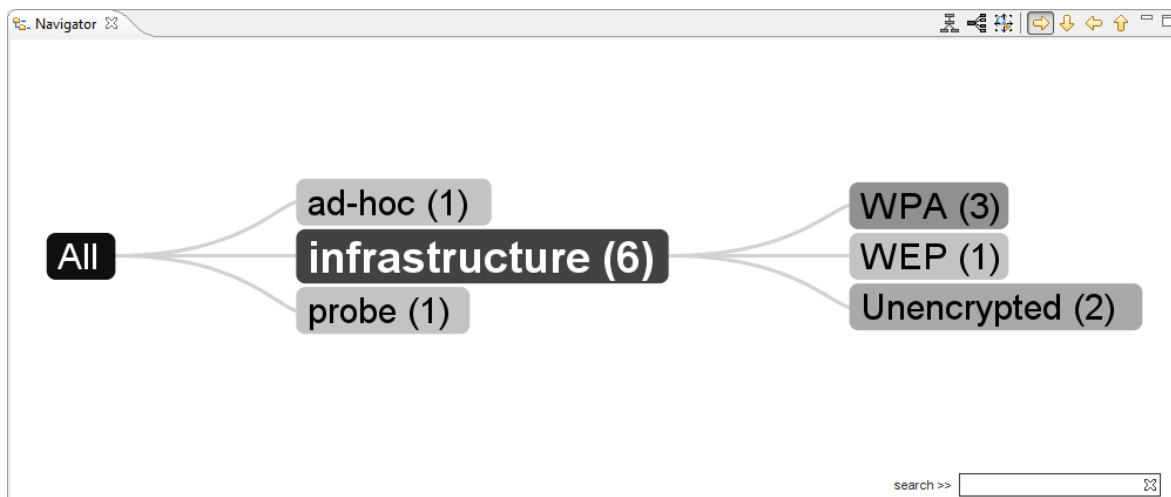
 **Show rogue clients connected to trusted networks and trusted clients connected to rogue networks**

5.10 Navigator View

The Navigator View provides an alternative tree representation of the networks checked in the Device Explorer. The Navigator view is helpful for visualizing and navigating large amounts of data. As nodes are selected in the tree, the view changes its focus to that item, maximizing screen space.

This view also provides extensive grouping, aggregation, filtering, and searching capabilities.

In the example below, color darkness is used to indicate groups with a greater count. Alternatively, coloring can be based on packets or number of clients connected to the network. Here we see that the bulk of the networks are of type infrastructure. We know this based on the darker color and the count of 6 displayed in the label.



5.10.1 Selection / Highlighting

If a node has not been expanded, double clicking it will cause focus to that node and expand any available children. If an item represents a specific device in the data set, selecting it will cause it to become highlighted, and all the other views within MeerCAT will highlight that group as well. In addition, if you hold the SHIFT key and select an item, the item becomes highlighted as well as all of its children. For example, if you hold SHIFT and click to select the WPA node, all devices that have WPA enabled will become highlighted in all of the views. By holding CTRL

while selecting individual networks and/or clients, you can select several devices to become highlighted in all of the views.

5.10.2 Panning

Left-clicking on the display allows you to pan.

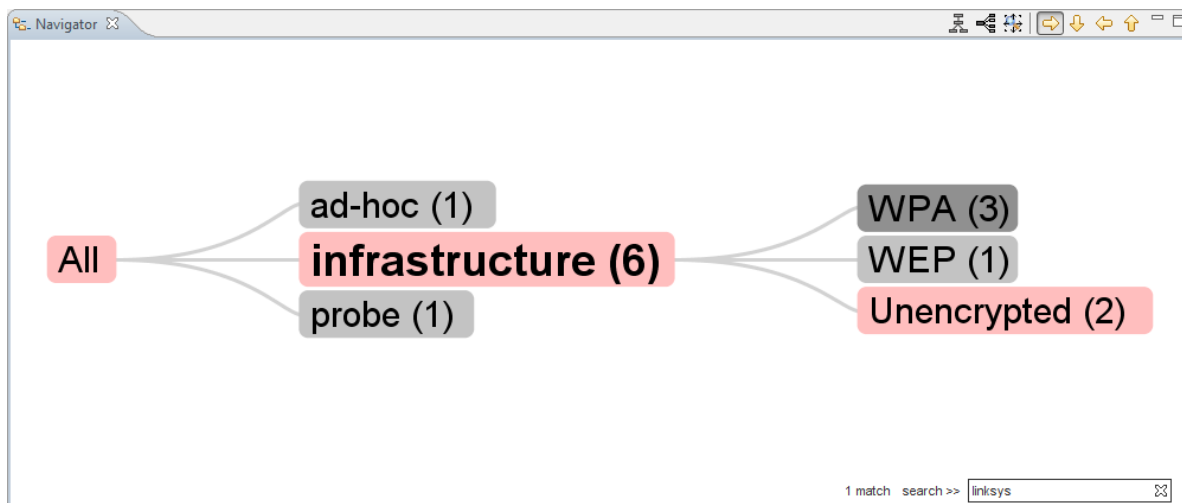
5.10.3 Zooming

Holding the right mouse button and moving the mouse up or down causes the view to zoom out/in. Right-clicking without moving the mouse will cause the display to refit to the current window size.

5.10.4 Searching

The search bar in the lower right of the display allows you to query for a particular BSSID, SSID, MAC address, or other label currently in the display, such as WEP. The sample below shows that two unencrypted devices were found, and that they are currently classified as type ‘infrastructure.’ Search is incremental; as you type, matching nodes will be highlighted.

Clicking on the text “matches” next to the search box will pop up a list of search results if there are any. The user can then click on a search result and the navigator will expand and zoom into that particular item in the graph.



5.10.5 Toolbar

The toolbar of the Navigator view contains the following buttons:

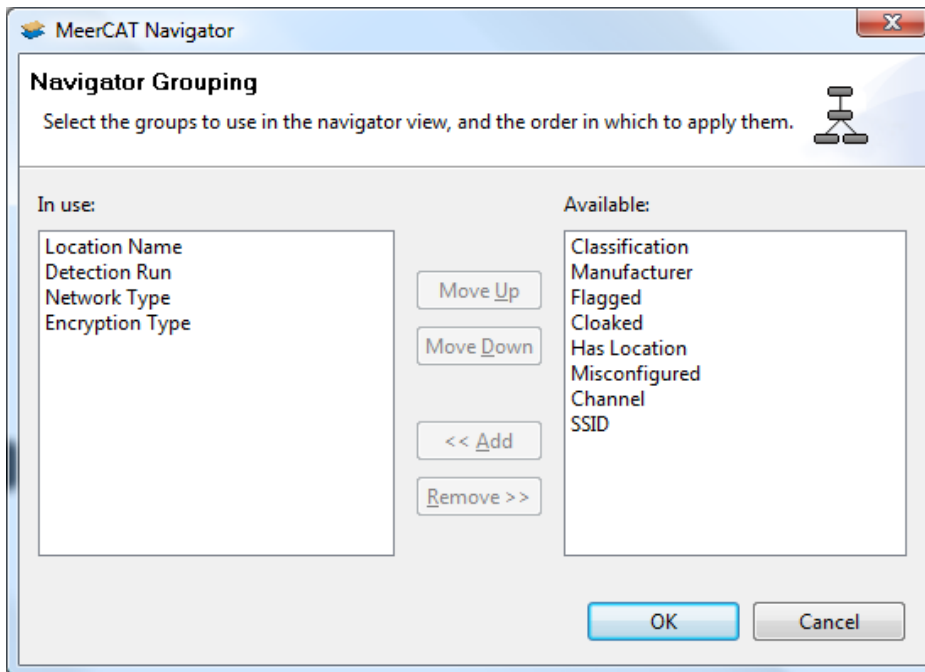
History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest

historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

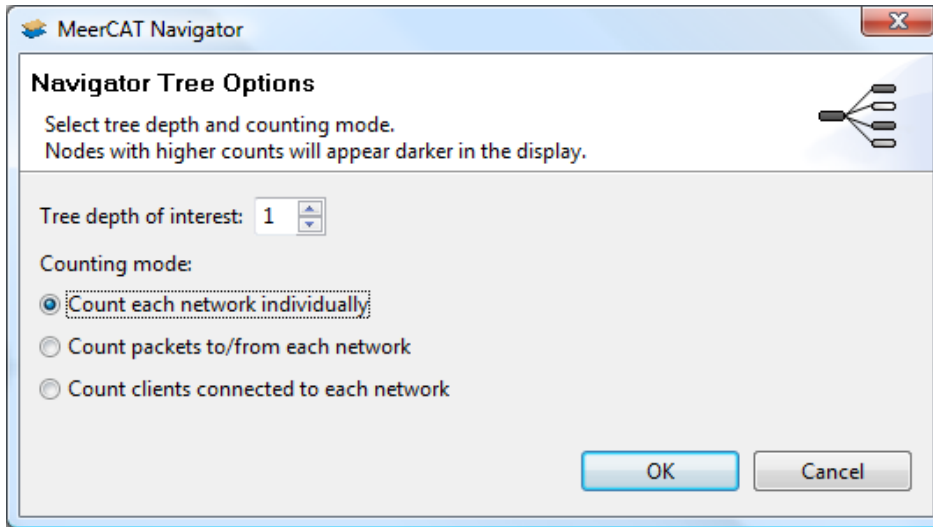
Navigator Grouping

This option allows you to set the grouping order of the Navigator View tree.



Navigator Tree Options

This dialog allows you to set the depth of the tree, meaning how many children will be shown from the focused node. The dialog also allows you to select how the node should be colored, either by count, number of packet, or number of clients.

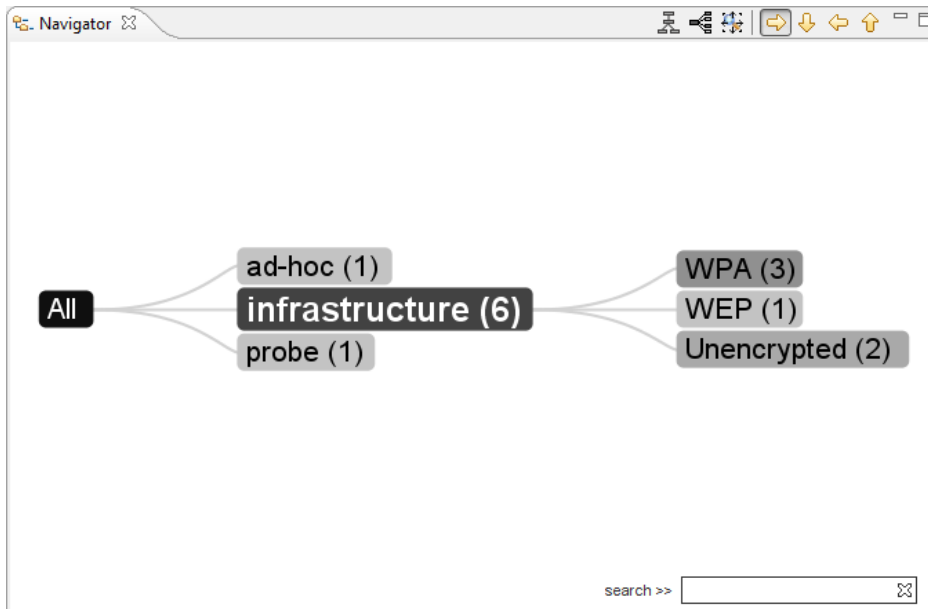


 **Zoom to Fit**

This option will refit the display to fit the size of the current display.

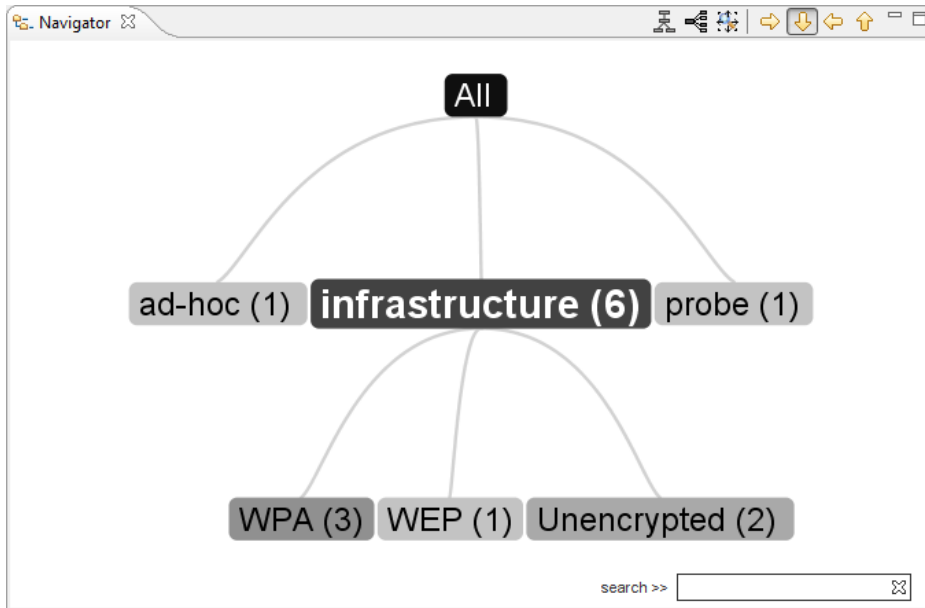
 **Orient Left-Right**

The left-right button will cause the display to show from left to right as shown below:



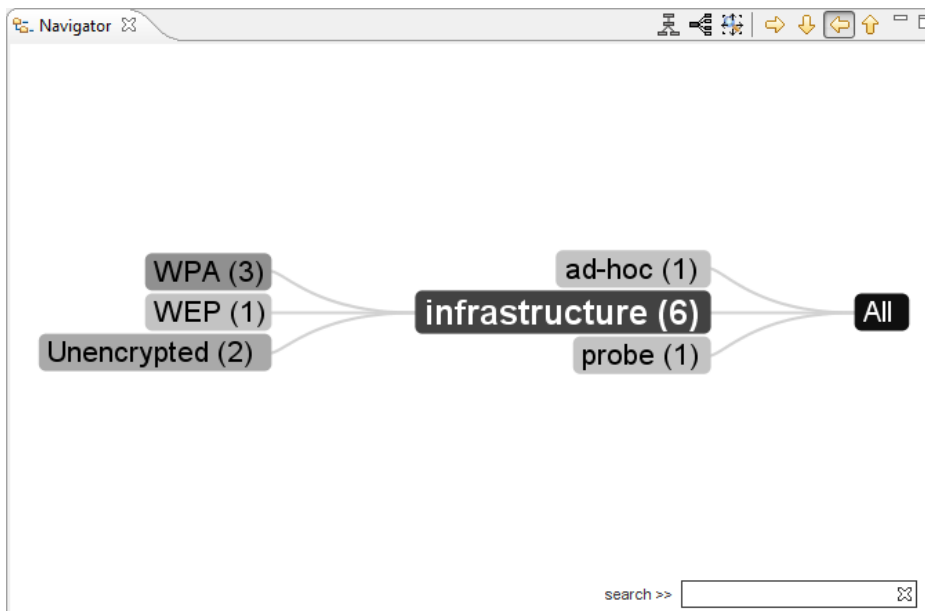
 **Orient Top-Bottom**

This option will cause the display to show from top to bottom as shown below:



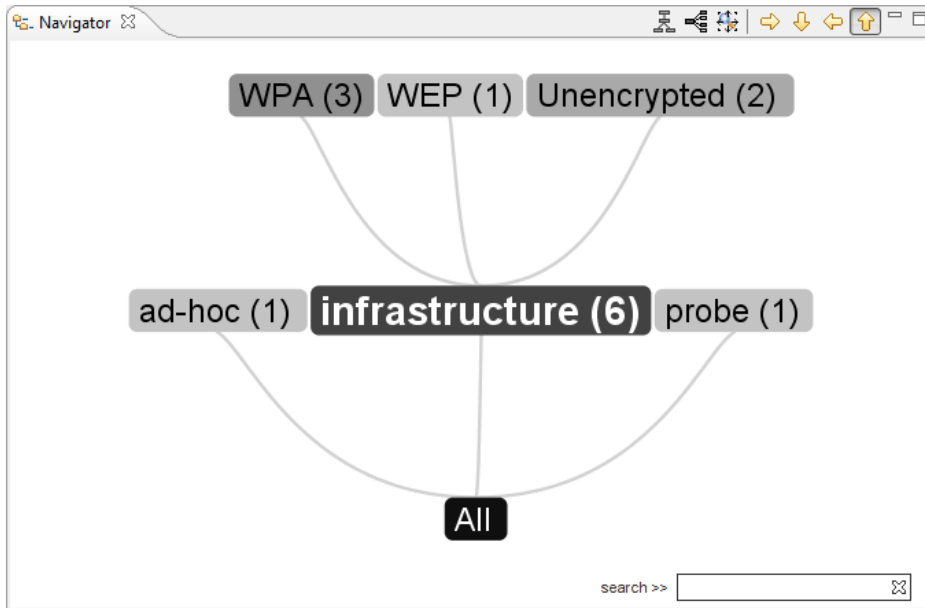
← **Orient Right-Left**

This option will cause the display to show from right to left as shown below:



↑ **Orient Bottom-Top**

This option will cause the display to show from bottom to top as shown below:



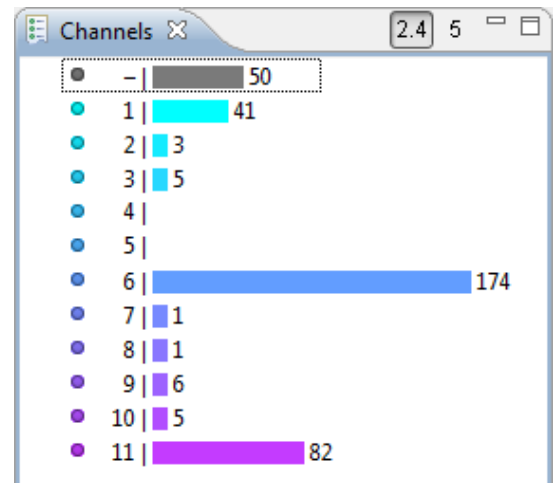
5.11 Channels View

Another beneficial feature of MeerCAT is that it can display the channel distribution of detected devices. For example, the screen below shows that Channel 6 is most widely used, which is to be expected since Channel 6 is the default channel used by most access point vendors.

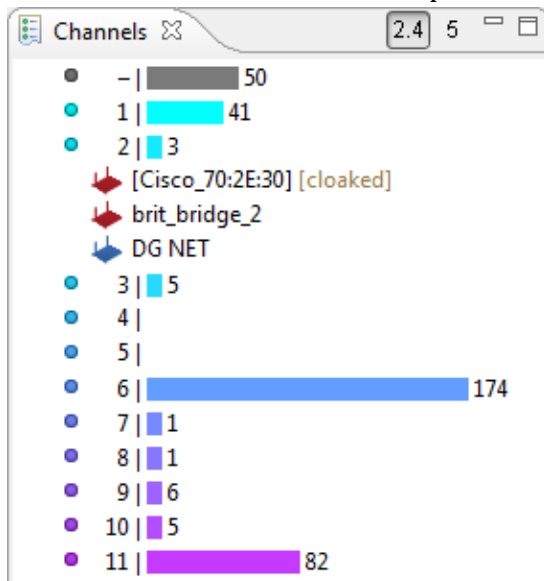
1. **Expand a channel to display the individual devices operating at a channel.**

Click on the right arrow symbol adjacent to each channel to expand the view of detected devices using this channel.

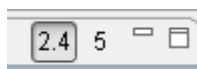
Tip: Number of detected devices operating at each channel is the number adjacent to the bar chart.



The Channels View will look like this once the right arrow to the left of a channel is expanded:

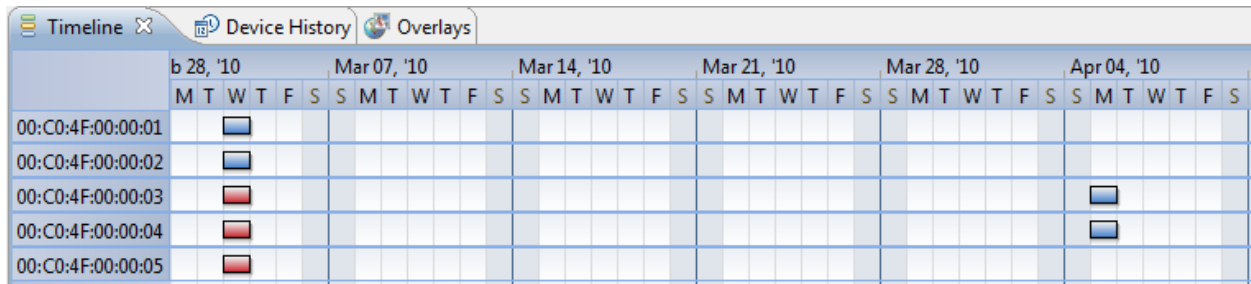


Two Channels View toolbar buttons allow selection of 2.4 or 5 GHz channel usage to be displayed.

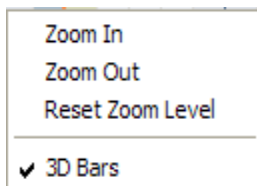


5.12 Timeline View

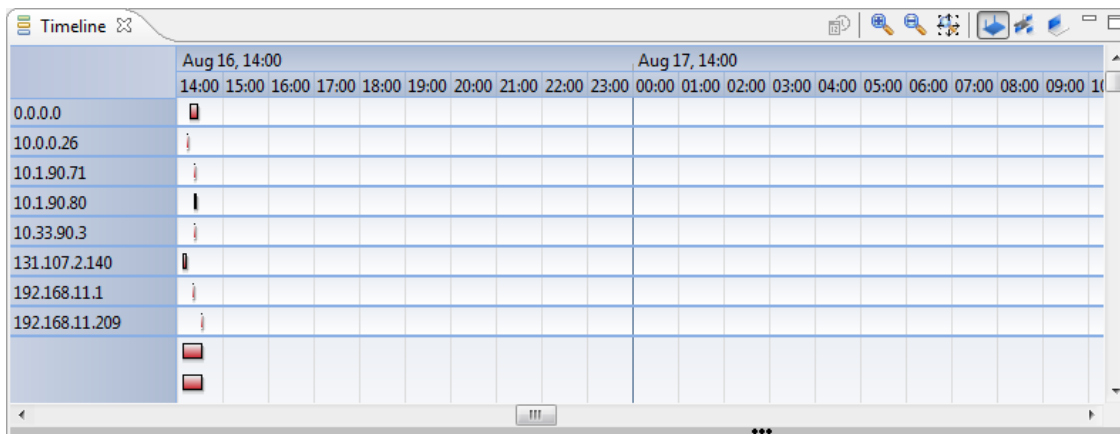
The Timeline View displays data in the chronological sequence it was obtained. One can view wireless networks relative to each other on the basis of the time they were obtained. With detection runs on the same route, devices can be compared over time.



A right-mouse click anywhere in the view will bring up the following menu:



Selecting Zoom In will increase the calendar scale, which can be repeated to allow hourly details to be seen. Zoom Out will shrink the calendar scale; Reset Zoom Level will return to the default view.



5.12.1 Toolbar



The toolbar of the Timeline view contains the following buttons:

 **History Mode**

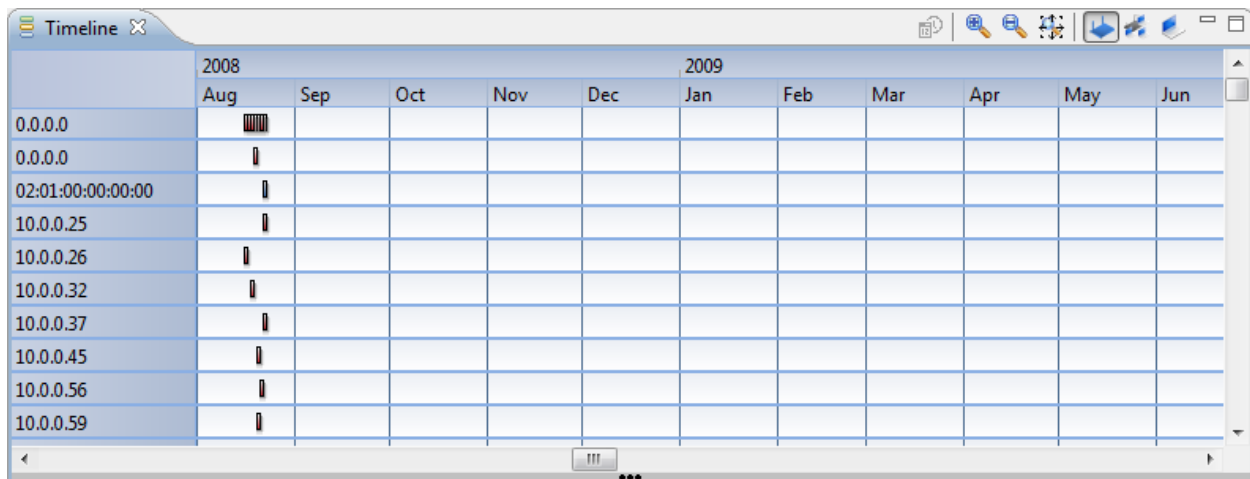
This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

 **Zoom In**

This option will increase the calendar scale, as pictured above. Zoom In is also available using Ctrl + mouse wheel up.

 **Zoom Out**

This option shrinks the calendar scale. Zoom Out is also available using Ctrl + mouse wheel down.

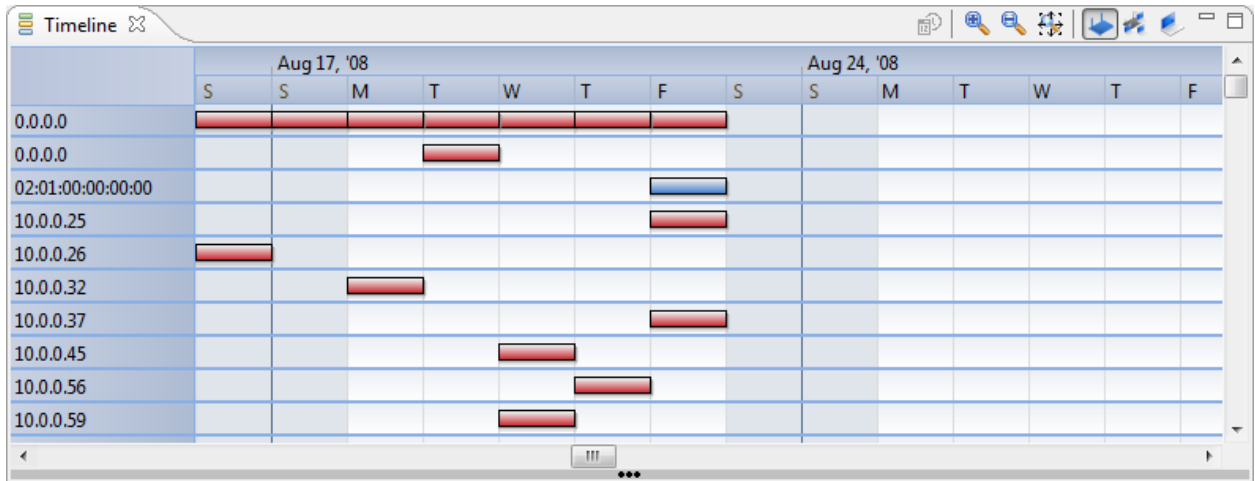


 **Reset Zoom**

This option returns the time line to its default view.

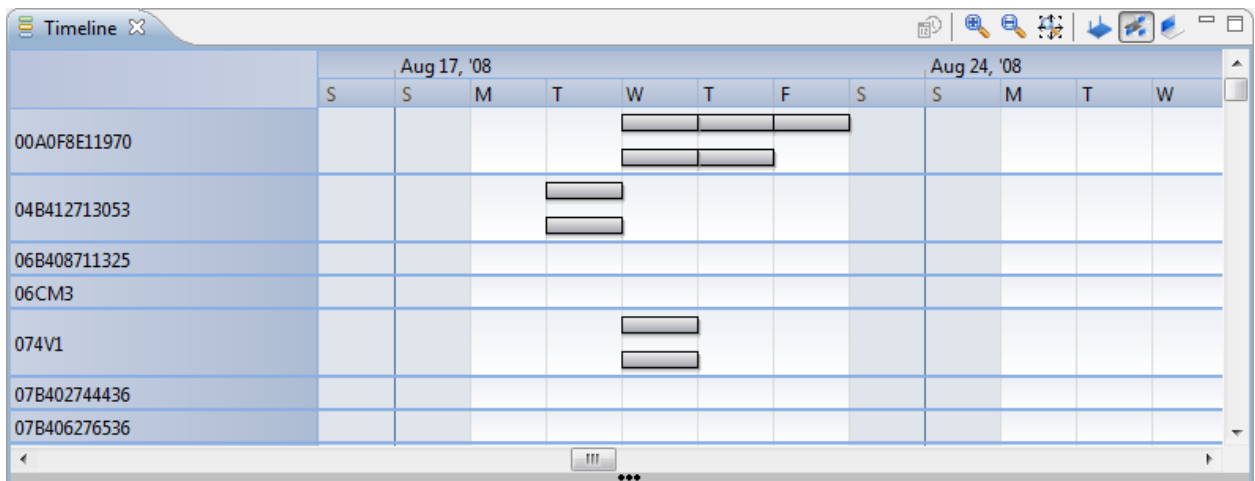
 **Networks**

Lists all discovered network devices and shows an event indicator on dates network devices were actually detected.



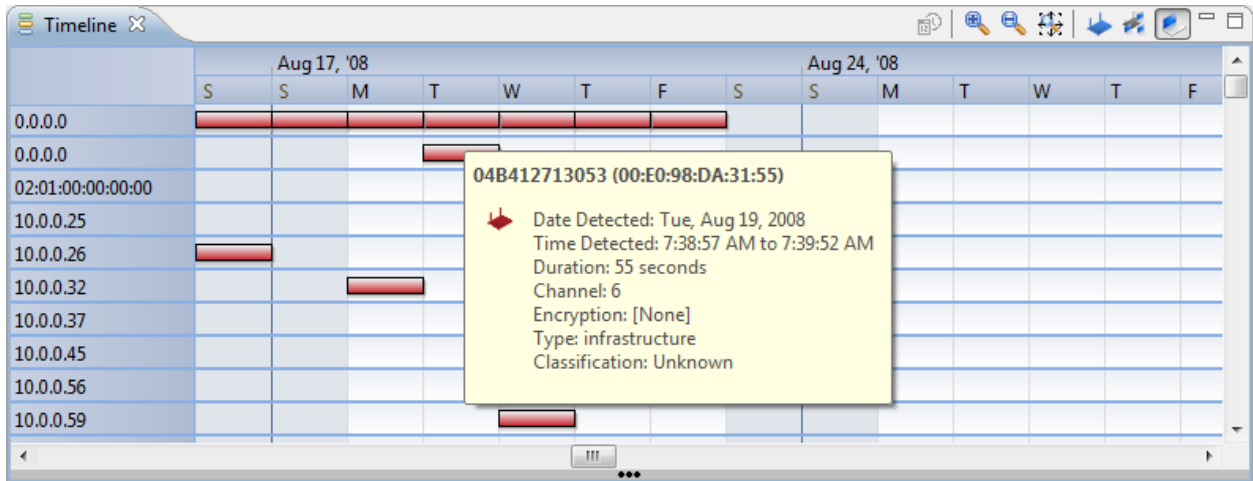
Networks with Clients

Lists all discovered network devices with an event indicator shown on dates when clients were attached to those networks. Individual event indicators are shown for individual clients. In this view, holding the mouse over an event indicator will show a pop-up window with the client details.



Clients and Networks


Lists all discovered clients with an event indicator on dates they connected to network devices. Holding the mouse over an event indicator will show a pop up with the individual network device details.



5.13 Device History View

This view displays data in the chronological sequence it was obtained, based on MAC address. If a device was once a network and then a client, that pattern can be seen here. You can also click the play button to animate the devices location on the Geo View.

MAC Address	SSID	First Seen	Last Seen	IP...	Latitude	Longitude	Encryption	Network Type	Channel	Carrier	Min Si...
00:C0:4F:00:00:04	White House	Wed 03/03/10 03:58:11 PM	Wed 03/03/10 04:18:11 PM		38.89767	-77.03565	[None]	tods	6	[]	
00:C0:4F:00:00:04	White House	Mon 04/05/10 03:58:11 PM	Mon 04/05/10 04:18:11 P...		38.89767	-77.03565	[None]	tods	6	[]	

If multiple histories for a given device are selected, they will be displayed in Geo view with varying opacities according to their age (the earlier the history, the lower the opacity). Additionally, their aggregated center position will be marked with the following symbol: 

5.13.1 Toolbar

The toolbar of the Device History view contains the following buttons:

 **Link with Selection**

Click on this toolbar button to activate or inactivate linking this view with device selection in other views. If not linked, device history will not change unless the Device History menu option is selected in the context menu for a device.

 **Stop Animation**

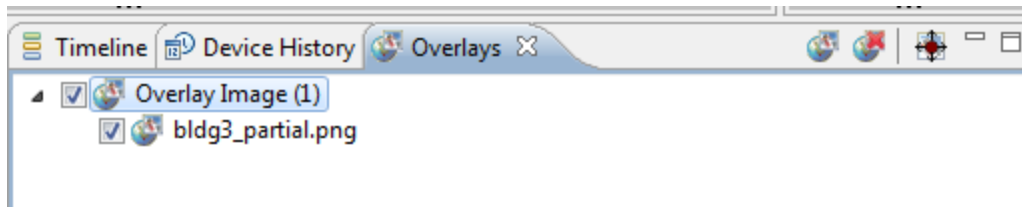
Stops the animation in the Geo view.

 **Start Animation**

Displays an animation in the Geographic view indicating the changing location of a device over the course of the selected discovery runs.

5.14 Overlays View

The Overlays View allows you to add an image such as a floor plan to the Geo View. Images must be in .bmp, .gif, .jpg or .png file formats. MeerCAT scans available directories for imagery when it launches, and these images will be shown here.



Use the checkbox to the left of an overlay to enable display of the overlay in the Geo View. The example below shows a building blueprint placed over an aerial view of a building's roof.

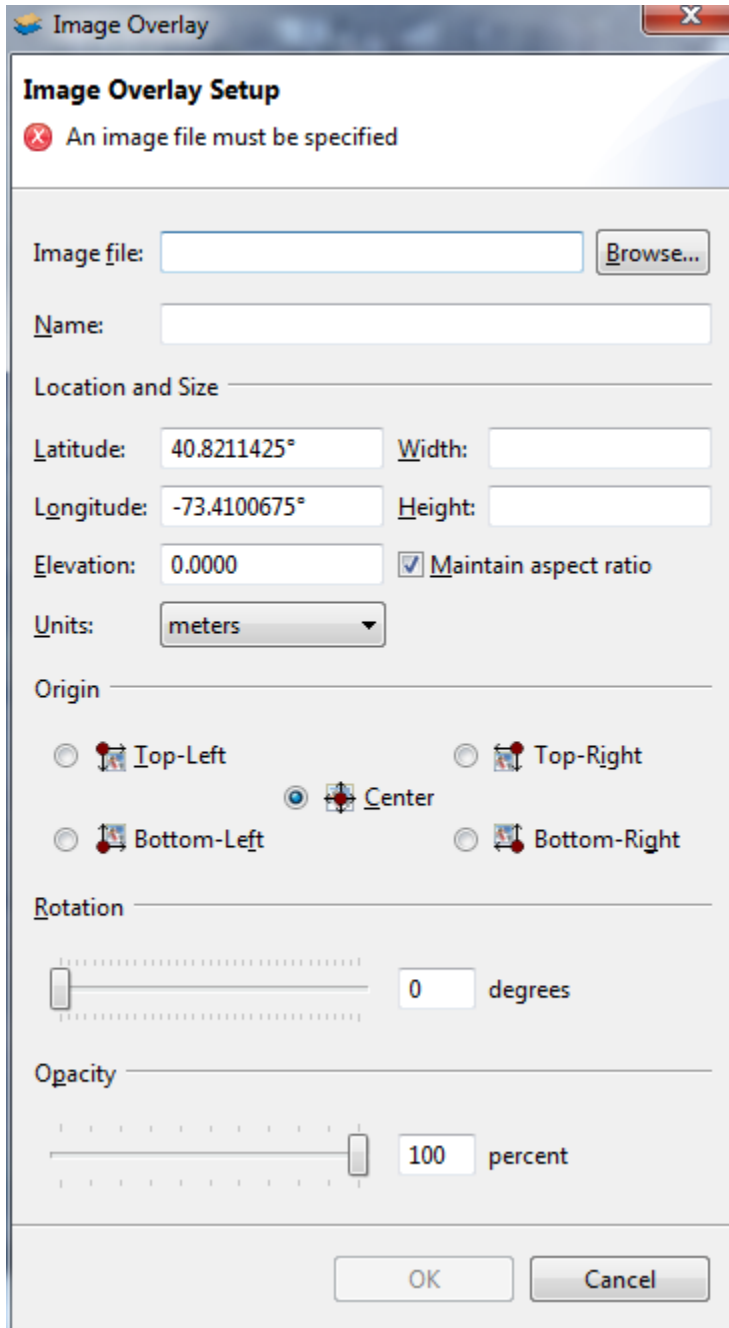


5.14.1 Toolbar

The toolbar of the Overlays view contains the following buttons:

Add Image Overlay

Opens the setup window to import an image.



 **Remove Image Overlay**

Removes the image overlay from the Geo View.

 **Allow Image Dragging**

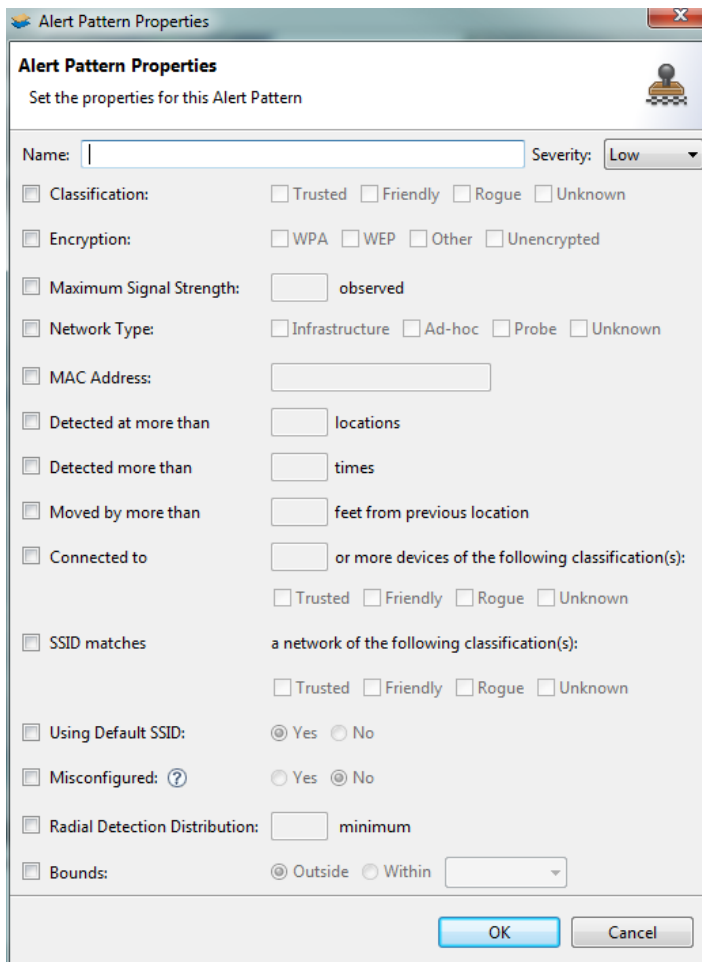
Click to allow or disallow image dragging of the overlay in the Geo View.

5.15 Alert Patterns View

In order to generate alerts, criteria need to be provided. Sets of criteria are stored in the form of Alert Patterns. MeerCAT includes a number of alert patterns for common wireless threats:

Name	Severity	Description	Is Enabled
Evil Twin	High	Classified as Unknown, Rogue - SSID matches a Trusted network	Yes
Misconfigured	Medium	Classified as Trusted - Misconfigured	Yes
Mobile AP	High	Network Type is infrastructure - Moved at least 1000 feet from previous location	Yes
Trusted Ad-Hoc	Low	Classified as Trusted - Network Type is ad-hoc	Yes
Trusted Default SSID	Low	Classified as Trusted - SSID is default.	Yes
Trusted Mobile AP	High	Classified as Trusted - Network Type is infrastructure - Moved at least 500 feet from previous location	Yes
Trusted Unencrypted	Low	Classified as Trusted - Using Unencrypted	Yes
Trusted WEP Encryption	Low	Classified as Trusted - Using WEP encryption	Yes

To add a new Alert Pattern, click the 'Create Alert Pattern' button in the Alert Patterns View toolbar. To disable or enable a pattern, right-click it and toggle the Enabled setting. To modify an existing pattern, right-click it and choose Modify. The Alert Pattern Properties dialog will appear:



Alert Pattern Properties
Set the properties for this Alert Pattern

Name: Severity: **Low**

Classification: Trusted Friendly Rogue Unknown

Encryption: WPA WEP Other Unencrypted

Maximum Signal Strength: observed

Network Type: Infrastructure Ad-hoc Probe Unknown

MAC Address:

Detected at more than locations

Detected more than times

Moved by more than feet from previous location

Connected to or more devices of the following classification(s):
 Trusted Friendly Rogue Unknown

SSID matches a network of the following classification(s):
 Trusted Friendly Rogue Unknown

Using Default SSID: Yes No

Misconfigured: Yes No

Radial Detection Distribution: minimum

Bounds: Outside Within

OK Cancel

5.15.1 Toolbar



Create a new Alert Pattern

Presents the above dialog to create a new alert pattern/

5.16 Alerts View

The Alerts view displays a table of alerts that have been generated based on Alert Patterns. Each alert in the table displays eight fields: the name of the device, the time it was detected, the location of detection, its status (pending, notified, resolved, ignored), Alert Pattern category, type, severity, and a description.

The Alerts view enables the user to quickly identify problems and visualize them in the Geo view. To zoom to a particular device in the Geo view, double click on that device in the Alerts view table then open the Geo view.

5.16.1 Toolbar

The Alert Patterns Toolbar contains the following buttons:

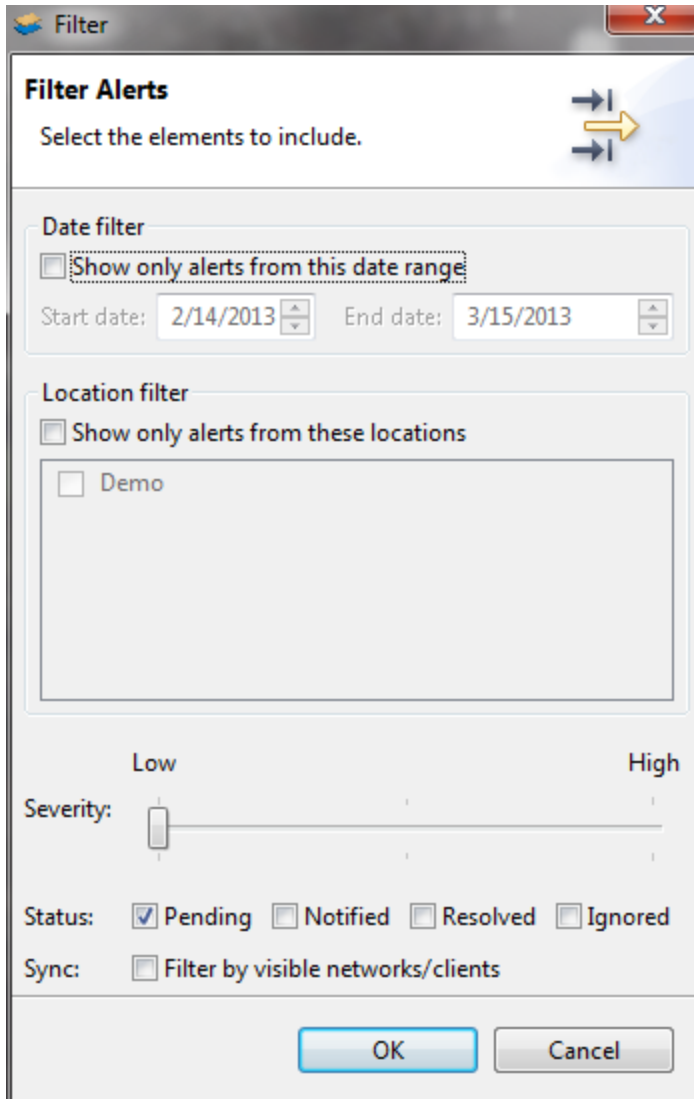


Alert Patterns

Selecting this button will display the Alert Patterns view.

Filter Alerts

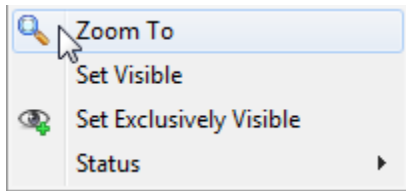
Customize which alerts are displayed in the Alert view table by selecting this option. The following dialog will be displayed:



This dialog enables the user to filter alerts by date, location, severity and/or status. When filtering by severity, the ‘low’ setting (as shown) displays all alerts and the ‘high’ setting only displays high severity alerts. Additionally, filtering by currently visible networks/clients can be specified.

5.16.2 Alert Submenu

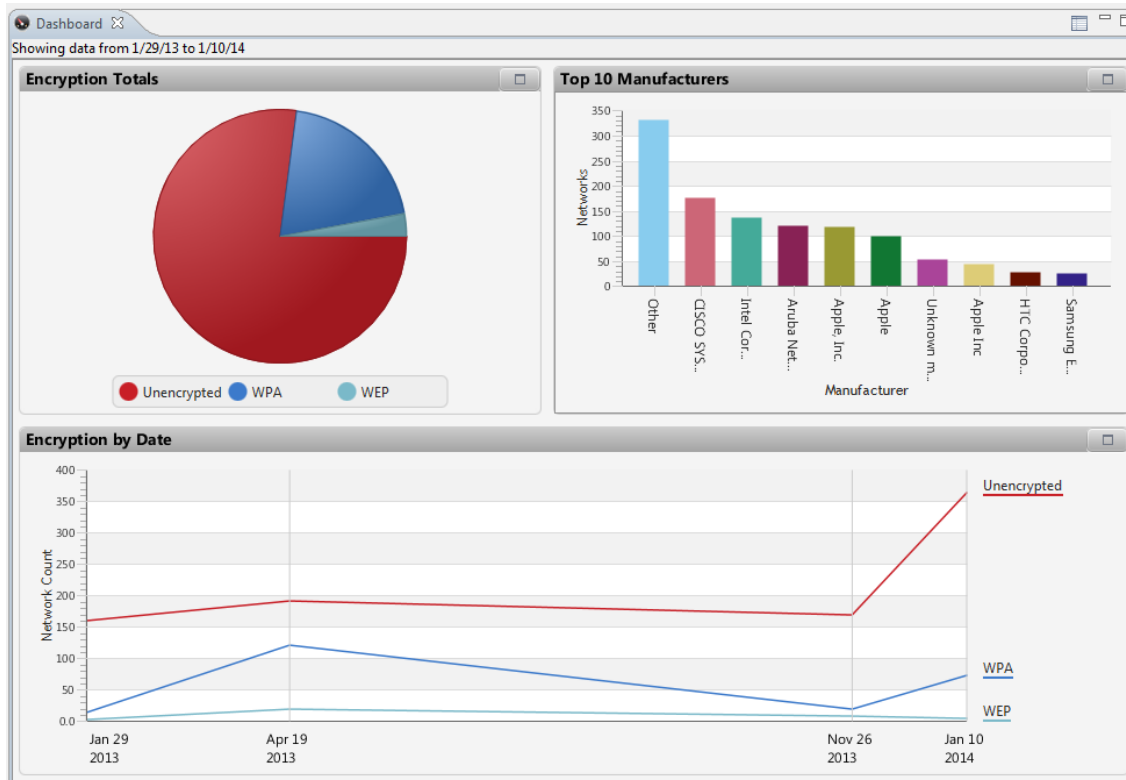
Right clicking on a device in the Alerts view table will display the following submenu:



Selecting *Zoom To* will cause the Geo View to zoom to the selected device. *Set Visible* will highlight the selected device in various other views and will result in this device being checked in the Device Explorer view. Similarly, *Set Exclusively Visible* will result in the selected device being the only visible device. *Status* can be selected to alter the status of the selected alert.

5.17 Dashboard View

The Dashboard View displays three different charts for Alerts or Wireless Networks.



The top left chart is a pie chart, top right a bar chart, and bottom a line chart. Each of these charts can depict a number of different data queries, allowing the user to choose what data each chart will display based on the contents selected in the toolbar button (see below). These charts allow the user to easily see alert patterns and summary network information.

Across the top of the window is a date range that represents the time frame the data is from.

To highlight specific networks or alert patterns in the Device Explorer and other views, click on an item in any of the dashboard's charts. Any networks related to the selected item will be highlighted in the other charts as well as other views in MeerCAT.

Each chart can be expanded to utilize all of the space available to the dashboard view, hiding the other two charts in the process. This can be accomplished by clicking on the button in the upper right hand corner of the frame of the chart that is to be expanded. The view can be restored to show all three charts by clicking the same button a second time.

Charts from the Dashboard view can be included in a report. See Chapter 7 for information.

5.17.1 Toolbar

The toolbar of the Dashboard view contains the following button:

Set Dashboard Contents

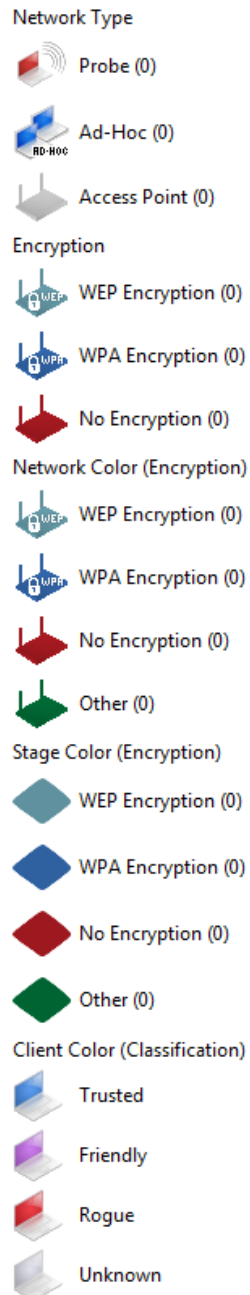
This option allows the user to determine which categories are displayed in each chart of the Dashboard view. The following options are available for each chart:

Pie Chart: Alert Patterns, Alert Severities, Encryption Totals, Network Types, Top 10 Manufacturers

Bar Chart: Alert Pattern Trend, Alert Patterns, Alert Severities, Alerts by Location, Alerts by Severity/Location, Encryption by Date, Encryption by Network Type, Encryption Totals, Network Types, Networks by Day, Top 10 Manufacturers

Line Chart: Alert Pattern Trend, Encryption by Date

5.18 Legend View



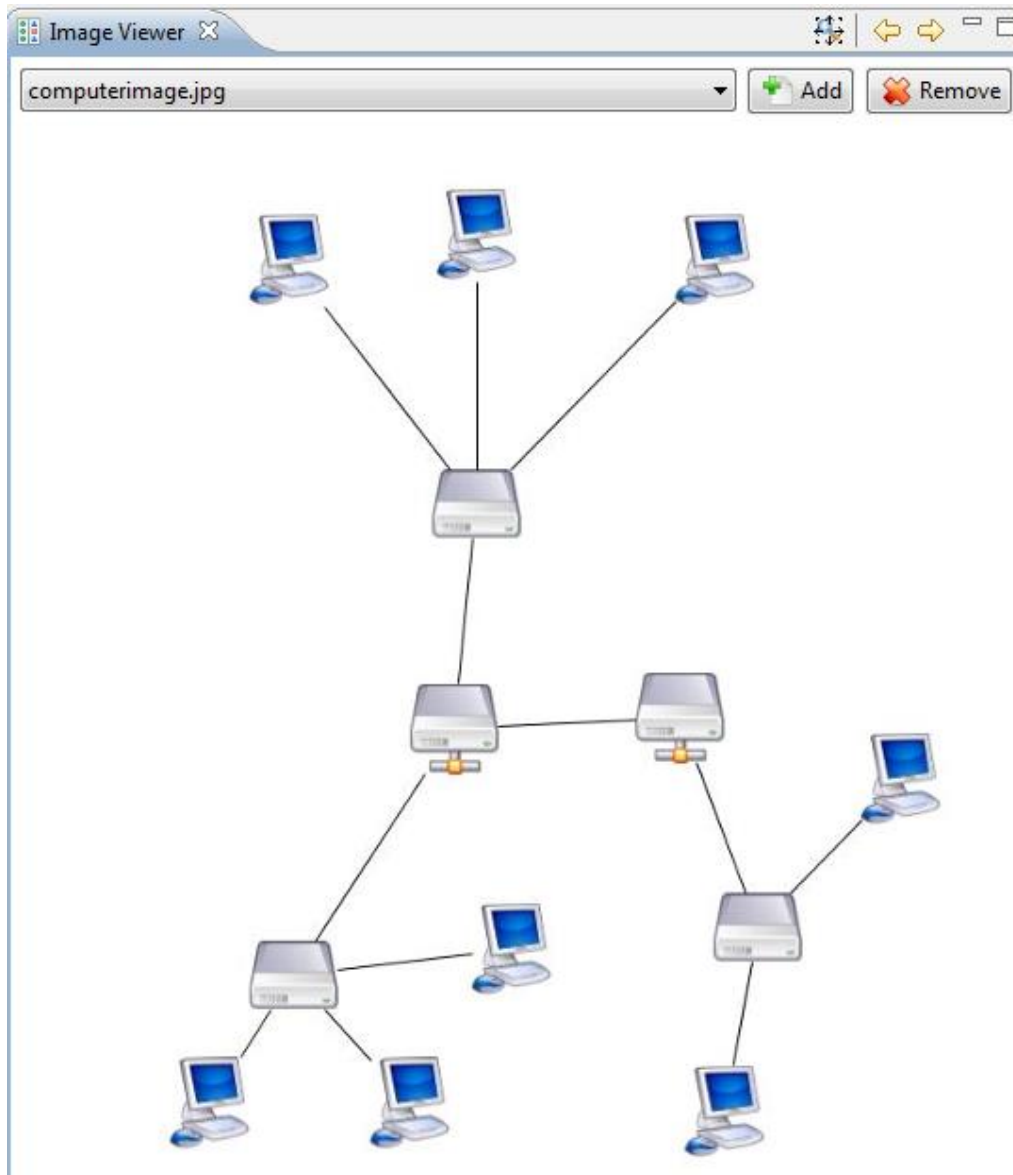
The Legend View provides quick reference to the meaning of certain visual attributes such as icons and colors within the various MeerCAT views. It allows the user to quickly see which attribute the network icons are colored by as well as which attribute the network topology “stage” is colored by. In addition, icons are provided to show the difference between Probe, Ad-Hoc, and Access Point (or infrastructure) wireless networks as they appear in the various views.

The appropriate icons for encryption type are also listed. Finally, next to each entry in the legend view is a number in parenthesis (#). This number represents how many networks in the visible data set are classified by this entry.

Legend View Interactions


The legend view is automatically updated when new data becomes visible or the user changes one of the colors in the MeerCAT Preferences. In addition, double clicking on one of the icons in the legend view will bring up the preferences page that is associated with the particular attribute.

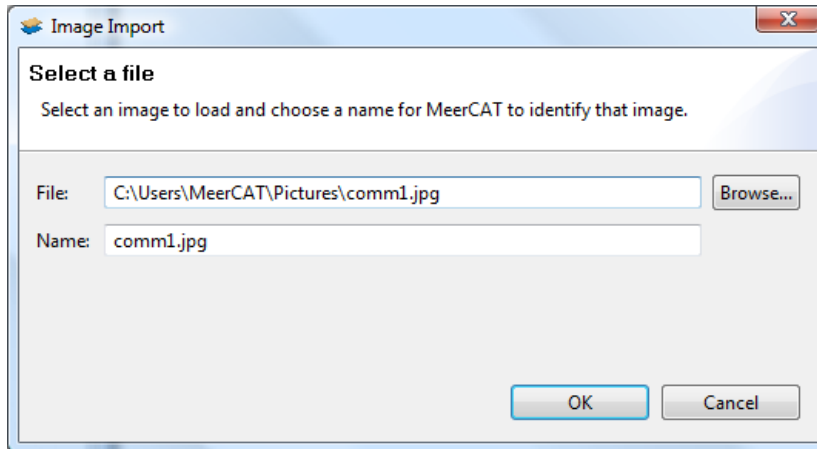
5.19 Image Viewer



Above is a screen shot of a random image being shown by the Image Viewer.

5.19.1 Adding Images

To add an image, click on the  button at the top of the view. A dialog will appear, enter the image file's location or click the Browse... button to select a file. The PNG, GIF, JPEG, BMP, and WBMP file formats are supported by default.

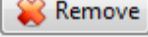


Next, pick a unique Name for the image to be shown in the image list. MeerCAT will suggest a name based on the image's original file name, but be sure to pick a name that you will remember. If an image by that name already exists in the image list then a dialog will pop up asking if you would like to go back or overwrite the previous item on the image list.

5.19.2 Displaying Images

To display an image, simply select it from the image list at the top of the view. All images that have been successfully added will be in this list, represented by the name given during the 'add image' process.

5.19.3 Removing Images

To remove an image, select it in the image list and click on the  Remove button at the top of the view. This will delete the image from the list.

5.19.4 User Controls

In the Image Viewer there are a number of mouse and keyboard controls that assist in the image viewing. Use the mouse wheel to zoom in and out of image. Likewise, the Page Up and Page Down keys will zoom in and out of the image, respectively. Click and hold the left mouse button anywhere in the display and move the mouse to pan the image up, down, left, or right. Likewise, the arrow keys can be used to pan the image around the display.

5.19.5 Toolbar

The toolbar of the Image Viewer contains the following buttons:

Zoom to Fit

This option will refit the image to fit the size of the current display.

Previous Image

This option brings up the previous image in the viewer's image list.

➔ **Next Image**

This option brings up the next image in the viewer's image list.

5.20 Status Line

The status line can be found at the bottom of the main window. There are 6 different items that can be shown.

1. Access Point
2. Ad-Hoc Network
3. Probes
4. Alerts

The number on the left shows the number that are visible. The number on the right shows the total number of items.

If you forget which item is which you can hover over them and the tooltip will tell you the full name of the item.

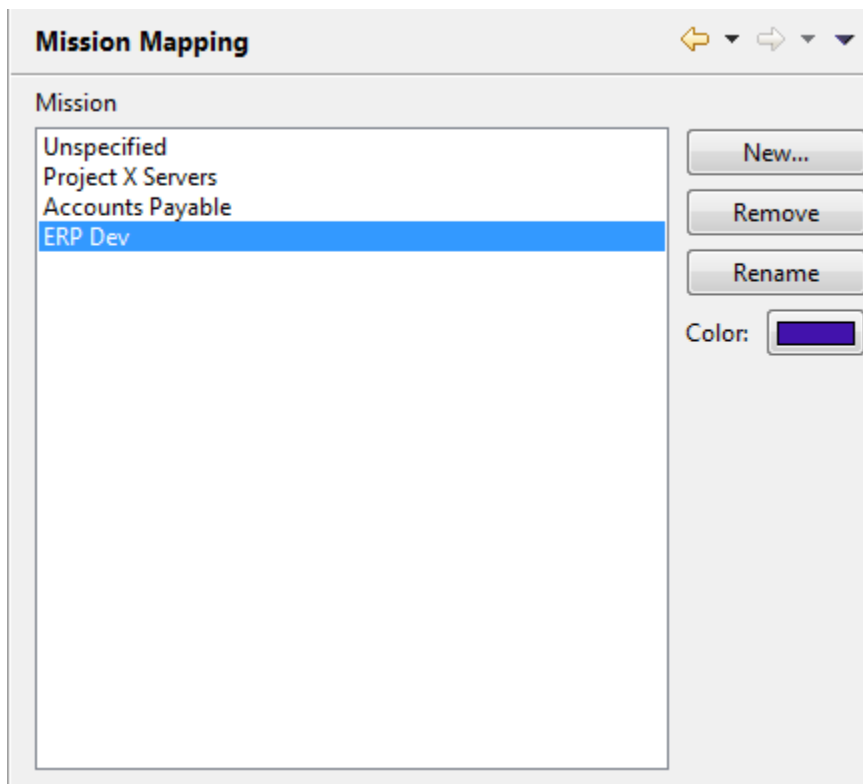


6 Mission Mapping

Mission mapping permits analysts to add a functional name to a device. For example, a wireless asset could have a mission of “Logistics,” “Invoicing,” or “Personnel.” These access points can be grouped and colored by mission, improving their visibility in MeerCAT views.

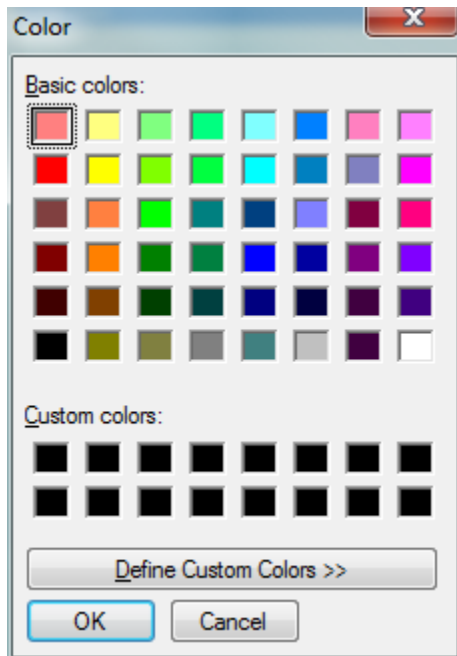
6.1 Preferences for Mission Mapping

Access the Mission Mapping page by Window -> Preferences -> Mission Mapping. From this dialog, you can create, rename, and remove mission names, and assign colors to them. (Missions can also be added through the Device Manager – select “Other” when prompted for Mission.)



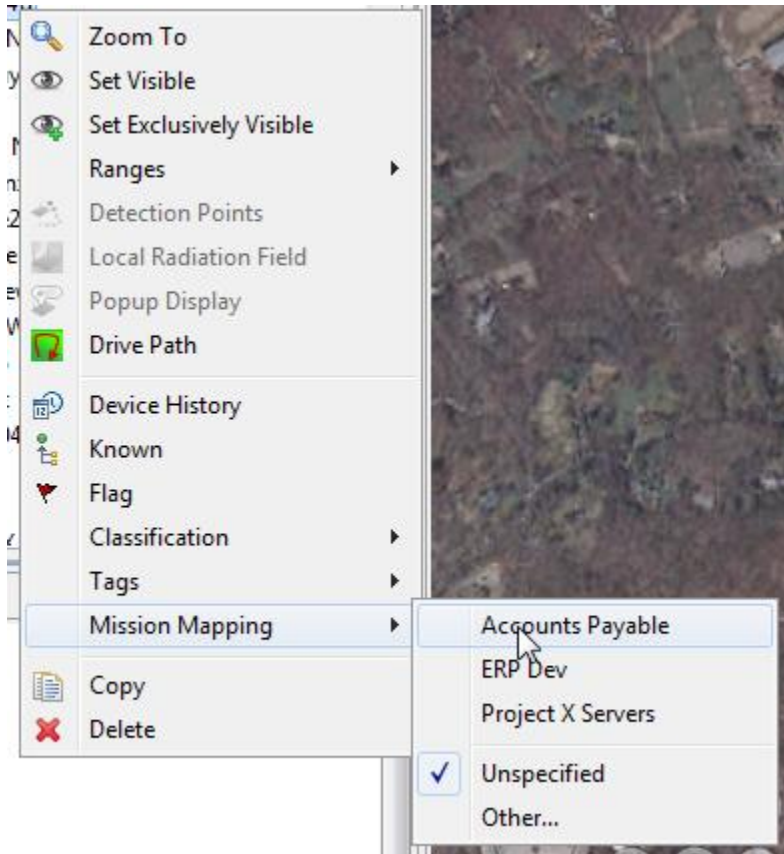
6.2 Choosing a Color for the Mission

Clicking on ‘Color’ brings up the color picker.



6.3 Assigning the Mission to an Access Point

Once missions are created, any access point can be assigned the mission by clicking on the choice.



6.4 Color the Network by Mission

Access points (networks) can be colored by mission, use the Window -> Preferences again, this time selecting General Colors.

General Colors

←
→

Devices

Network color: Mission ▼

Network Topology 'stage' color: Mission ▼

Client color: Classification ▼

Encryption

WPA 	WEP
Other 	Unencrypted

Classification

Trusted 	Friendly
Rogue 	Unknown

Misconfigured

Misconfigured 	Not Misconfigured
No Configuration 	

Other

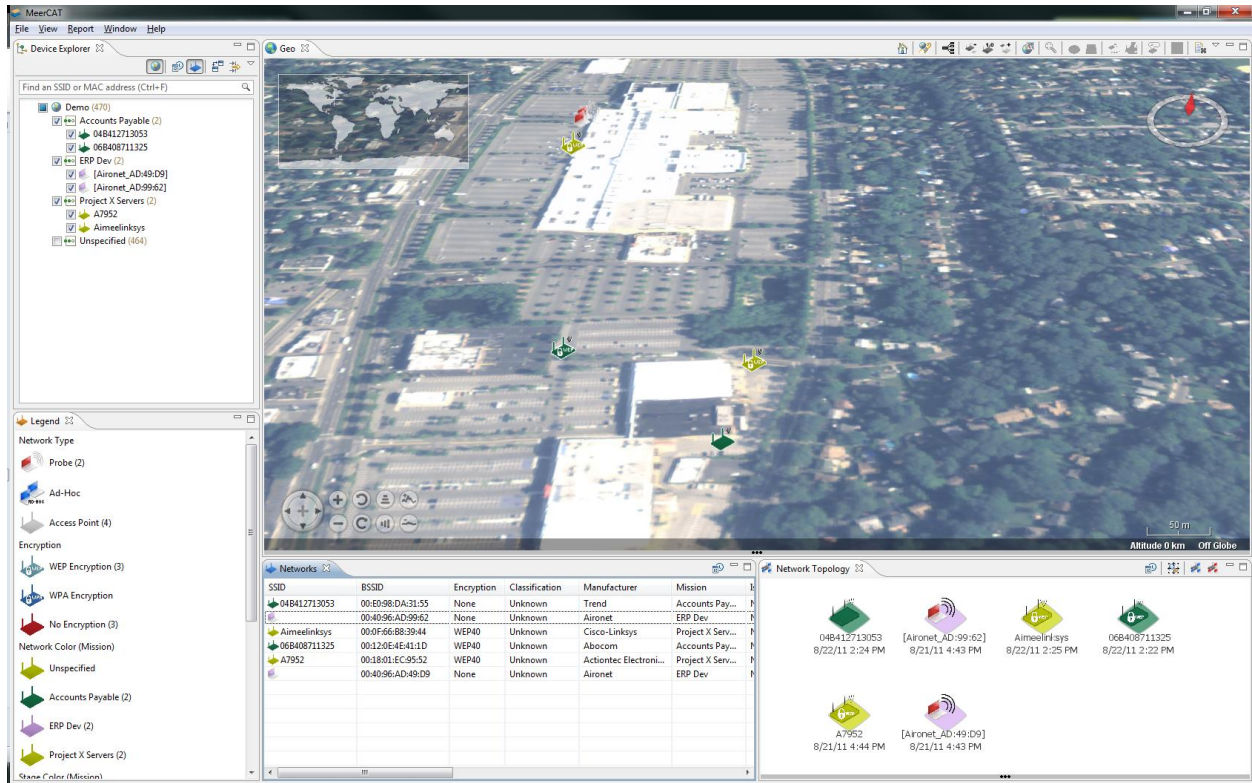
Selected

Note: Channel colors are fixed. See Channels view for legend.

Restore Defaults
Apply

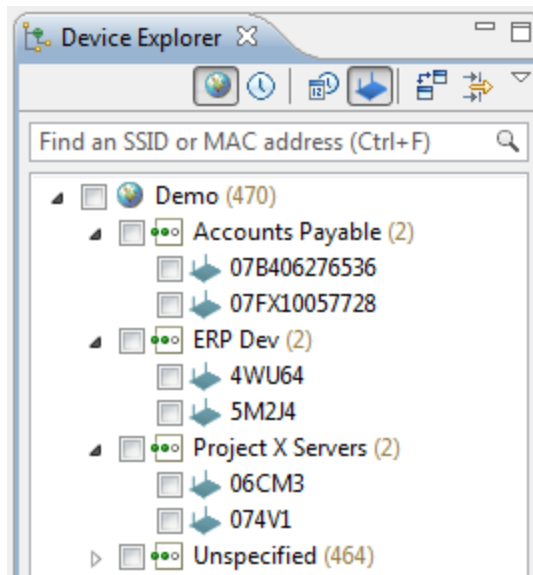
6.5 Colored by Mission

It is easy to see what function the access points have now.



6.6 Group by Mission

Access points with missions can be grouped by mission, allowing easy detection.

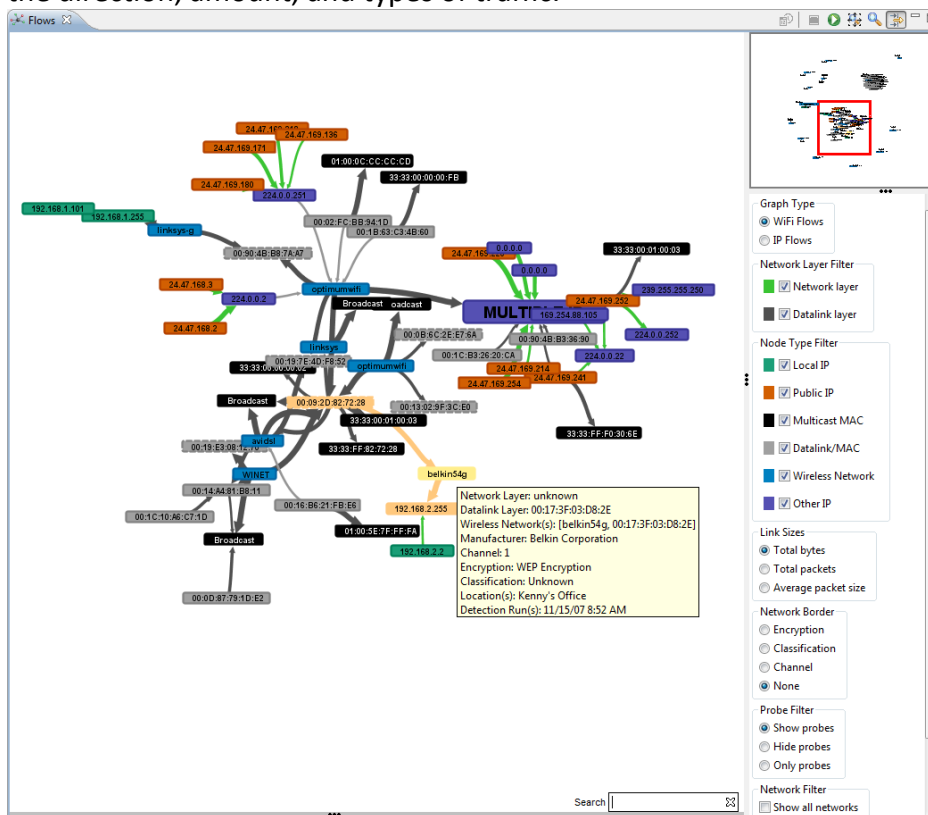


7 Communication Flow Graph

A communication flow graph is an analytical tool designed to visualize the relationships of and data flow among IEEE 802.11 wireless devices (e.g. laptops and peripherals with network cards, network access points, personal digital assistants). The flow graph is derived from processing a packet capture file. It allows users to observe data flow relationships across multiple layers of the TCP/IP and OSI network models.

7.1 Flows View

This view is a visual representation of network communication flows across multiple network layers. The nodes represent network addresses and the connections between them represent the direction, amount, and types of traffic.



Once the data is loaded, the display will lay out the graph and a small overview ('mini-map') at the top right of the filter shows the entire graph as well as a red box representing the area viewable in the main display.

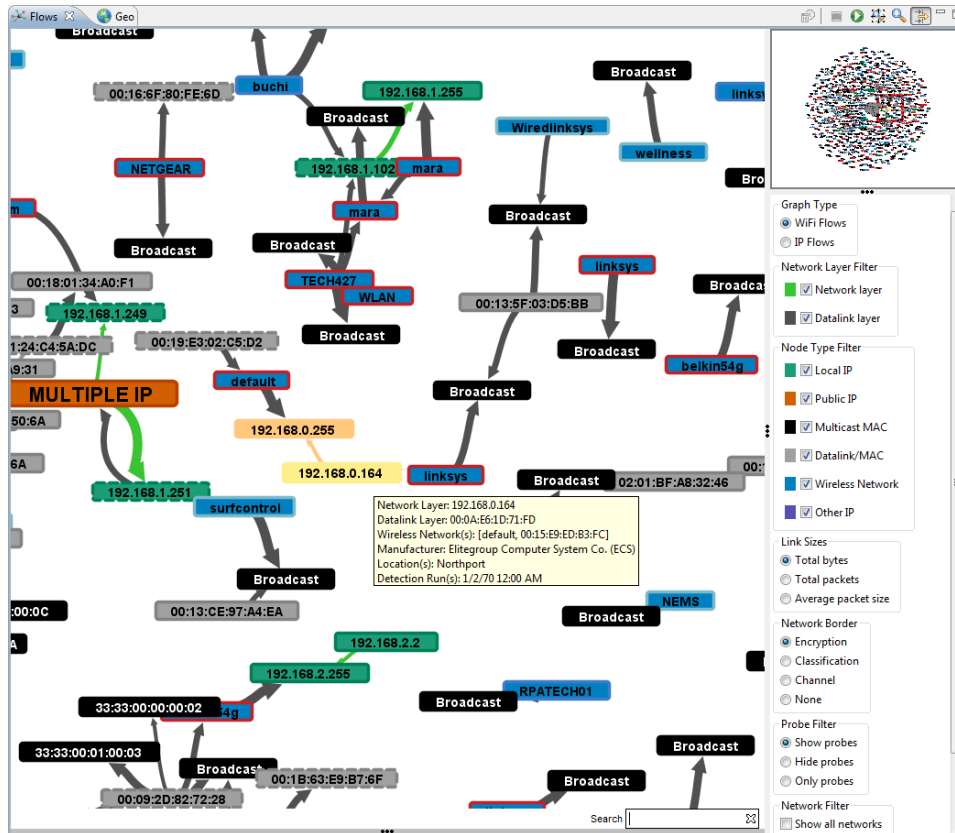
7.1.1 Graph Type

There are two modes in which the Flows graph can be displayed: IP Flows and WiFi Flows (default). Both graphs represent the same data set using a different method for building the

actual graph. WiFi Flows uses the data link layer addresses of packet flows to distinguish between nodes and then layers any IP information on top of that. IP Flows does the opposite. That is, each node in the WiFi Flows graph belongs to a unique MAC address (there may be several Multicast MAC nodes with the same address, but only one per wireless network) but may have several IP addresses associated with it. Conversely, each node in the IP Flows view belongs to a particular IP address and may have several MAC addresses associated with it. These two modes can assist administrators in determining the ways in which different network layers act on the traffic being analyzed.

7.1.2 Nodes

The graph nodes each contain a label which represents a network address associated with them and they all have a fill color associated with the attributes of their communication patterns. These colors are all user manageable in the WiFi Flows area of the MeerCAT preferences. Wireless Network nodes represent a known wireless network and are labeled with their SSID (or BSSID if the SSID is not known), Multicast MAC nodes represent datalink layer broadcast and multicast addresses, and Datalink/MAC nodes represent generic datalink layer MAC addresses. These are the types of nodes that fall under the 'Datalink Layer' categorization because they represent link layer hardware addresses. On the other hand, there are three classifications for nodes that exhibit network (IP) layer information. Local IP nodes are nodes that have at least one IP address in the private IPv4 range (10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255), while Other IP nodes are nodes that contain at least one multicast, broadcast, loop back, or any other reserved, non-public address. Public IP nodes represent IPv4 addresses that are public.



In WiFi Flows mode, nodes with multiple IP addresses will be depicted larger and labeled 'MULTIPLE IP'. In addition, Wireless Network nodes that are associated with any IP information will be depicted larger than normal nodes since their color will not be overridden by additional network layer information like their client and multicast counterparts.

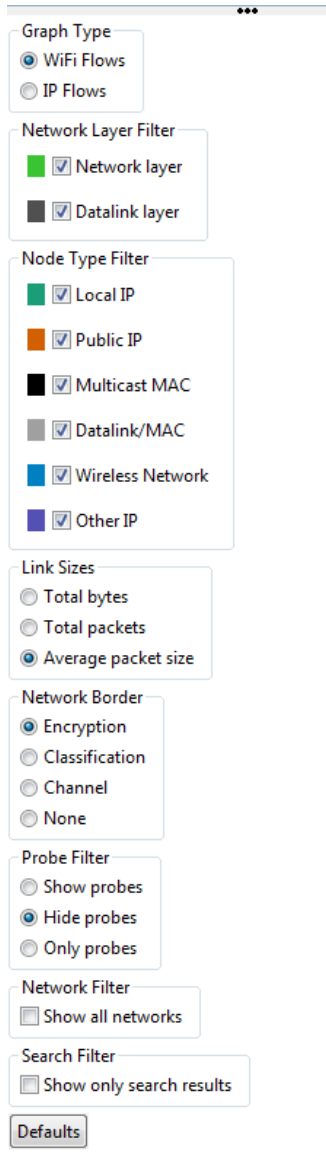
A dashed border around a node shows that the node is known to be a wireless transmitter, even if it is not designated as a 'wireless network' device. A node that is defined as a 'wireless network' (and shown in blue by default) is known to be a wireless transmitter and always has a solid border with a color based on encryption or classification.

7.1.3 Links

The graph links represent one-way communication between two network addresses. There are color distinctions for Datalink Layer links (that is, links that exhibit Ethernet or IEEE802.11 link layer communication) and Network Layer links (links that exhibit IP communication). Their thickness is based on the amount of data passed between the devices. In addition, in the WiFi Flows mode there are symbolic connections which show the user a symbolic association between a node and one of its associated access points. If the node can be traced to the access point without adding a symbolic connection, one is not added.

7.1.4 Filter

The Flows filter pane is shown below.



The screenshot shows a vertical filter pane with the following sections:

- Graph Type:** Radio buttons for WiFi Flows and IP Flows.
- Network Layer Filter:** Checkboxes for Network layer and Datalink layer.
- Node Type Filter:** Checkboxes for Local IP, Public IP, Multicast MAC, Datalink/MAC, Wireless Network, and Other IP.
- Link Sizes:** Radio buttons for Total bytes, Total packets, and Average packet size.
- Network Border:** Radio buttons for Encryption, Classification, Channel, and None.
- Probe Filter:** Radio buttons for Show probes, Hide probes, and Only probes.
- Network Filter:** Checkbox for Show all networks.
- Search Filter:** Checkbox for Show only search results.
- Defaults:** A button at the bottom of the pane.

The Flows filter is composed of several parts:

Graph Type: toggles graph mode (IP Flows or WiFi Flows)

Network Layer Filter: toggles visibility of network or data link layer information. If network layer is disabled, nodes and links will revert to their data link layer attributes and label or disappear if they have none. If data link layer is disabled, any node or link without network layer information will disappear. If both are disabled, nothing is shown in the graph unless 'show all networks' is selected.

Node Type Filter: toggles visual attributes and/or visibility of the various node types. A node will show visual attributes for the highest layer of information that is not filtered out.

Search Filter: when enabled, will hide any item that is not a search result or is not somehow connected to a search result in the graph.

Link Sizes Filter: toggles which attribute should be used to determine the size (thickness) of the links. The options are Total Bytes (total number of bytes in the flow represented by the link), Total Packets (total number of packets passed), and Average Packet Size (average size of packets passed through this link).

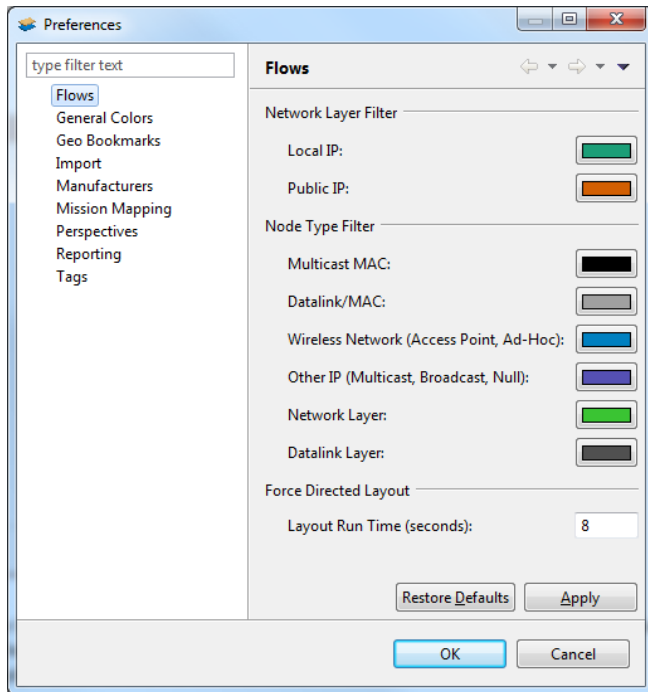
Network Border Filter: toggles which attribute should be used to determine the border color of a Wireless Network node. This can be based on the network's encryption or its device classification. It can also be disabled to show a border that is slightly darker than its fill color.

Probe Filter: allows the user to show or hide probe requests and responses. It also allows the user to show only probe requests and responses.

Show All Networks: option to force all wireless networks to be shown on the graph, even if they do not exhibit any non point-to-point communication.

7.1.5 Preferences for Flows

The Preferences for the flows are shown below.



Clicking a color located next to a Network Layer and Node Type filter brings up the color picker. Customizing the colors affects the appearance of the Flows View filters. After changing the color, click Apply then OK to use the selected color.

Entering values in the Layout Run Time affects how fast or slow the Flows View loads and how spread out or compact it appears. The range is 0 to 99 seconds. Entering the value of 0, causes the Flows View to load slowly and appear compact. Entering the value of 99 causes the Flows View to load fast and appear more spread out. After changing the value, click Apply then OK to use the value.

Restore the default colors and Layout Run Time by clicking Restore Defaults then OK.

7.1.6 User-Graph Interaction

Clicking on a node or link will globally select its associated network(s), client(s), or flow(s). Double clicking on a node will select all network, client, and flow objects associated with it or its connections. You can select multiple items by holding the CTRL key. Likewise, when a network, client, or flow is selected globally, it will be highlighted in the display.

The search box will highlight link and nodes corresponding to a relevant MAC address, IP address, port, port name, network SSID or BSSID, and IEEE 802.11 frame types/subtypes. Typing “www” will highlight all nodes and link with a www port associated with them. Typing “192.168.1.” will highlight all nodes and links in the 192.168.1.0/24 network.

Clicking on the text “matches” next to the search box will pop up a list of search results if there are any. The user can then click on a search result to zoom into that particular item in the graph.

For additional information on using the Flows view, see the Communication Patterns section below and the Flow Details View help section.

7.1.7 Toolbar

The toolbar of the Flows View contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

Stop Layout

This option stops the force directed layout from acting on the graph.

Run Layout

This option will run the force directed layout for the length of time specified in the WiFi Flows preferences.

Zoom to Fit

This option will refit the display to fit the size of the current display.

Magnifier

This option will turn the magnifier on or off. The magnifier will make nodes within the 'glass' around the mouse point appear larger. Use the mouse wheel to determine the level to which the nodes are enlarged. Hold the CTRL key and use the mouse wheel to change the range (size of the glass) around the mouse point that the magnification should affect.

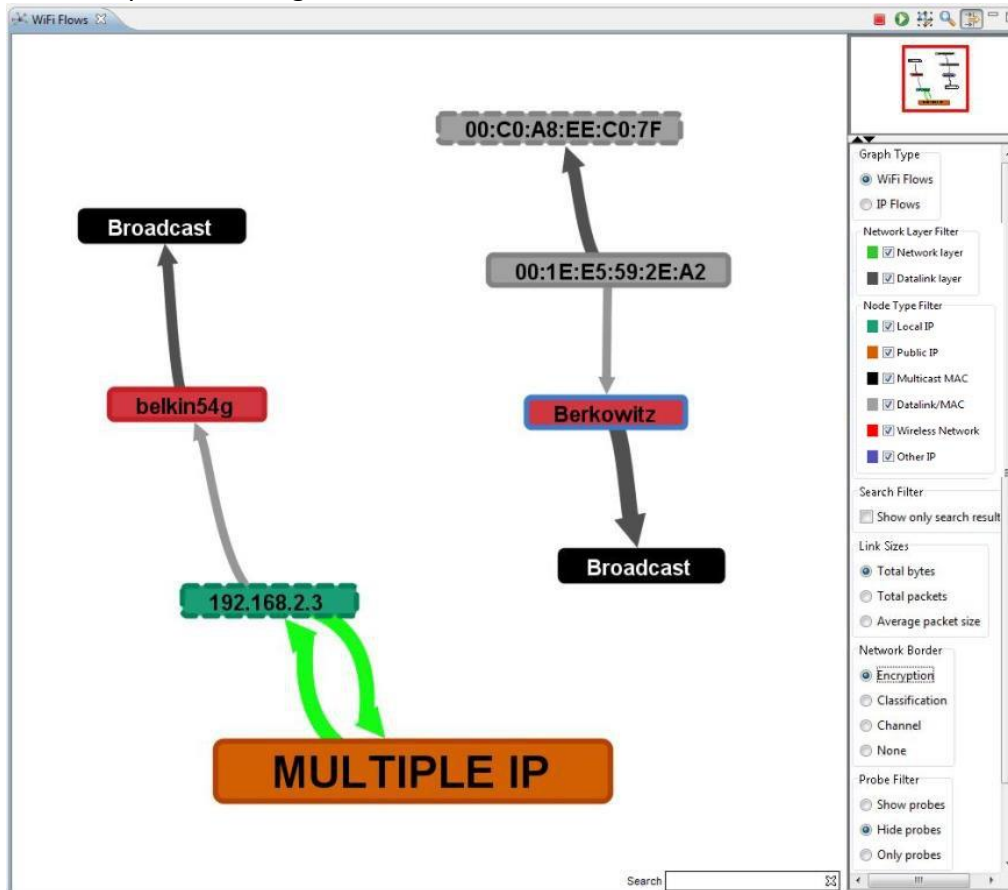
Toggle Filter

This option will hide or show the WiFi flows filter.

7.1.8 Communication Patterns Usage Scenario

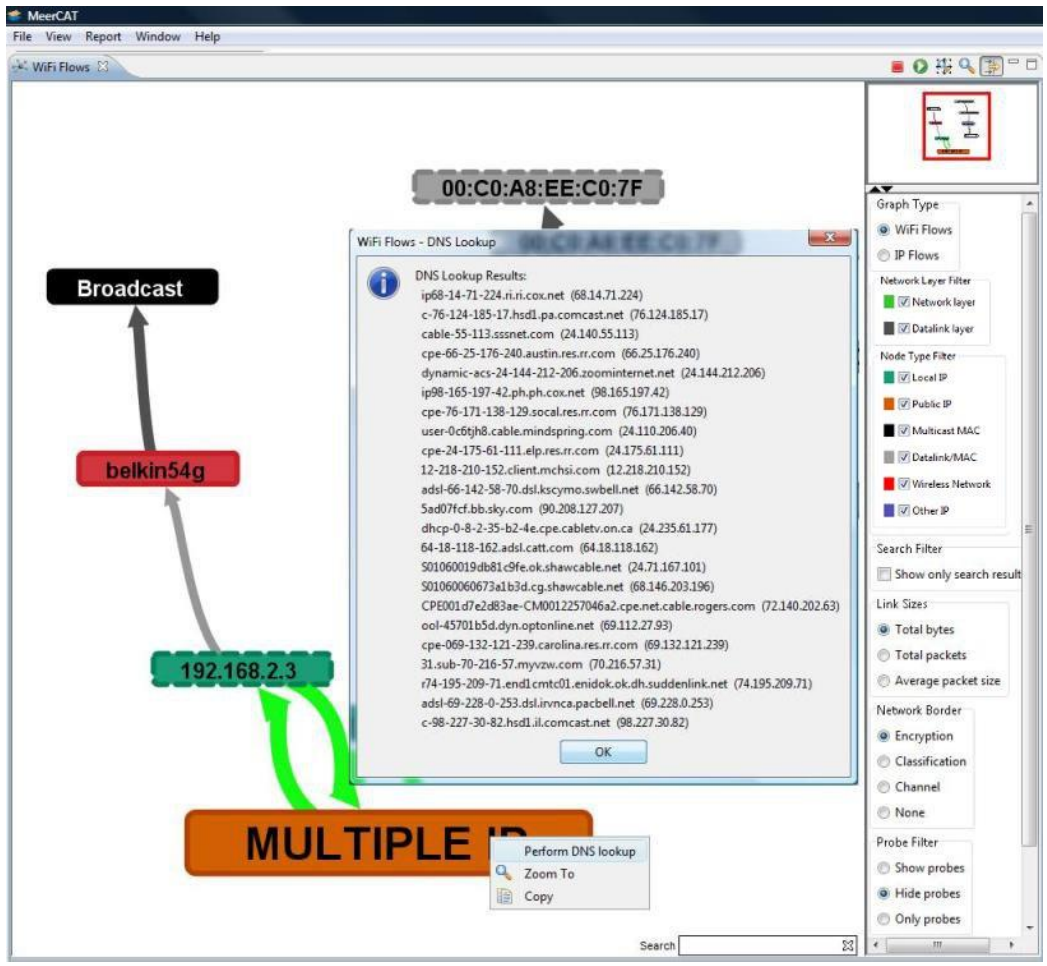
The Flows View is a useful tool in analyzing wireless network flows. This section contains examples on how to use the Flows View to learn more about the structure and vulnerability of wireless networks. For a general approach to understanding the Flows view, please see the

Flows help in the Using MeerCAT - Fundamental Tools section.

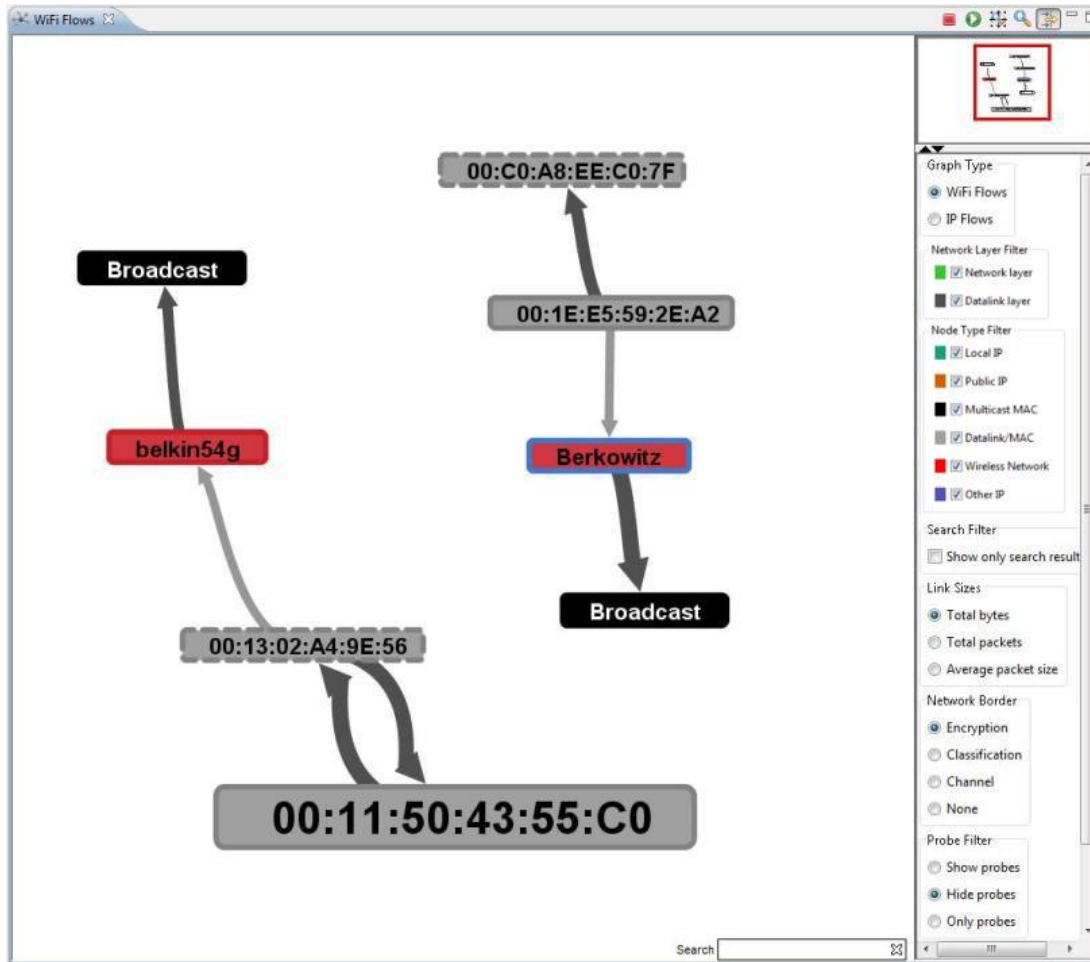


Above is a picture depicting two wireless access points: Berkowitz and belkin54g. Since the border filter is set to 'encryption' this means that Berkowitz is using an encryption standard that is not WEP or WPA and belkin54g is using no encryption. These color classifications are available in the legend view and can be edited in the MeerCAT preferences. What's important to note here is that the two of these wireless networks are set up and behave very similarly except for their encryption, which makes a world of difference in wireless networking.

A good indication of whether or not a node belongs to a wireless interface is to look at its border. If it has a dashed border, then the available packet data shows sufficient evidence to suggest that the particular address belongs to a wireless transmitter. That makes the 192.168.2.3 and 00:C0:A8:EE:C0:7F nodes known wireless assets, probably somebody's laptop.



In this second screen shot, we have decided to go straight to the large node labeled 'MULTIPLE IP' in the belkin54g network. In addition to this link layer address being the owner or next hop of multiple IP addresses, they are also remote IP addresses that we are concerned with. To begin, we right click on the node and perform a DNS lookup. This gives us an idea as to what sort of IP addresses belong to this link layer entity.



Using the 'Network Layer' filter we told the WiFi Flows graph to ignore network layer information when displaying the visual attributes of the nodes. As a result, we are shown the MAC address of each of these nodes. The important thing that we discover is that the large node's MAC address is very close to that of the belkin54g BSSID, 00:11:50:43:55:C1. This suggests that it is probably an Ethernet interface on the wireless access point while 00:11:50:43:55:C1 is the MAC address belonging to the wireless interface. A similar thing is going on with the 00:1E:E5:59:2E:A2 node of the Berkowitz network, suggesting the same thing is going on there.

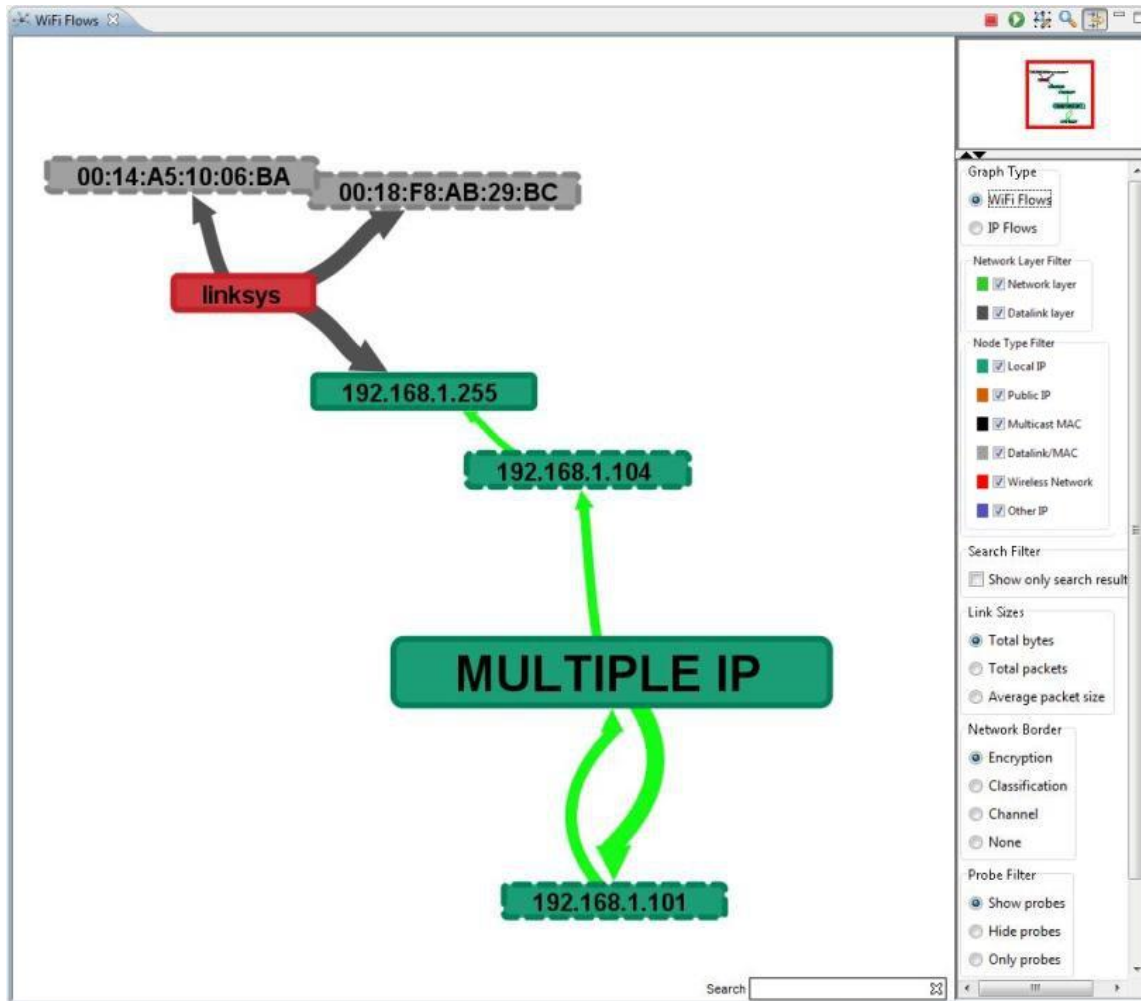
The belkin54g example is a very common signature for someone who plugged a wireless access point into an active switch port and started using it with 'out of the box' open configuration. This is a problem for a network security officer, because anybody listening to the radio signals nearby can see any connections and information being passed by the network's client(s). Unless you have decrypted the packet files ahead of time with software such as Wireshark (<http://www.wireshark.org>), seeing IP layer communication in this view should draw an immediate red flag.

Analyzing part of the edge tooltip between the MULTIPLE IP node and 192.168.2.3 as well as the DNS results shows that the local wireless client on belkin54g is connected to many home

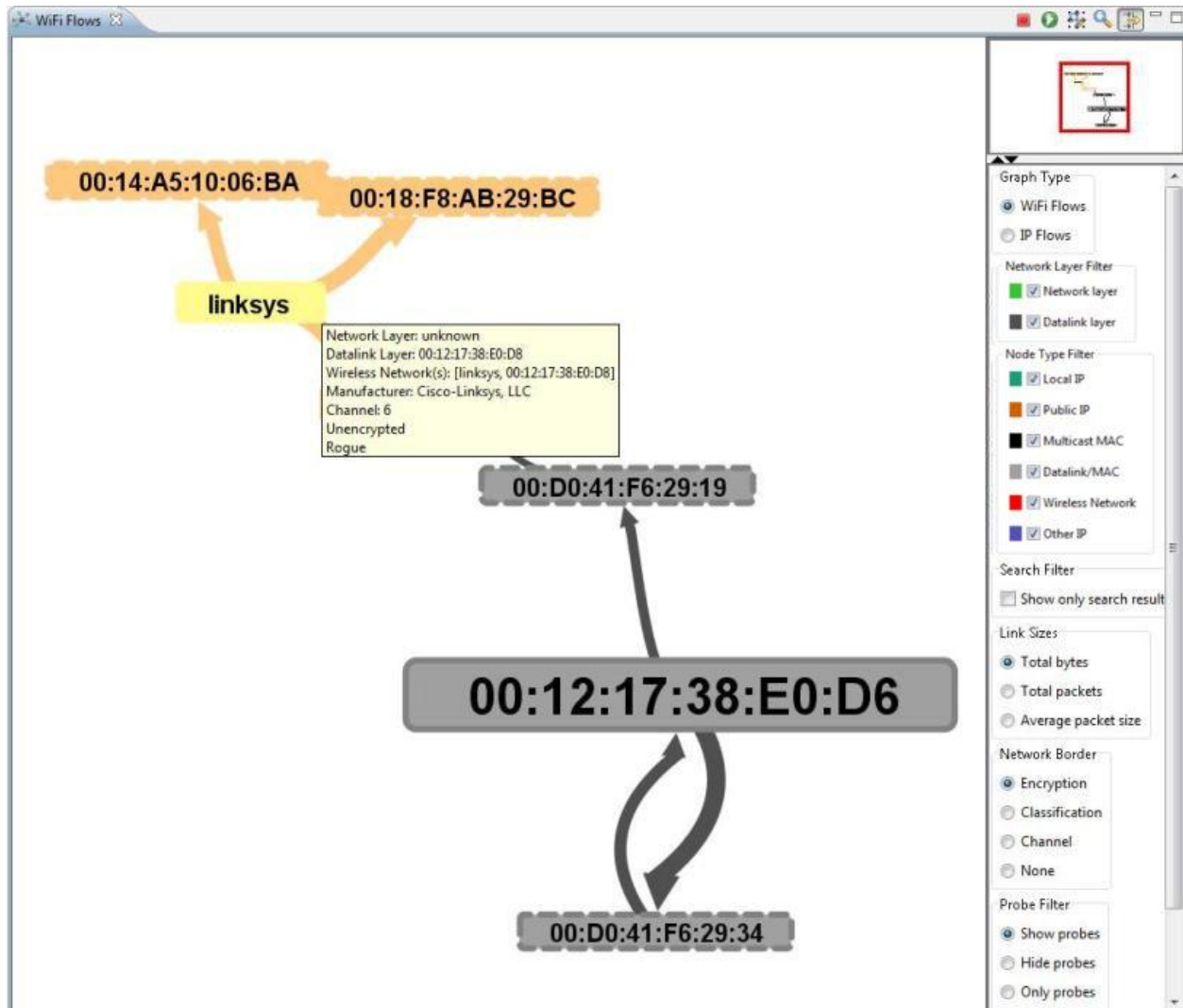
broadband computers on various unreserved ports, possibly indicating that the access point is being used as a gateway for an Internet gamer.

In the Berkowitz network, we cannot see any IP layer information because the packets are encrypted. As such, we cannot determine how many or what kind of computers 00:C0:A8:EE:C0:7F is talking to if 00:1E:E5:59:2E:A2 is a routing interface. This is ideal for a network administrator, because the only thing that is being broadcast is that there is traffic passing between the access point and one of its clients.

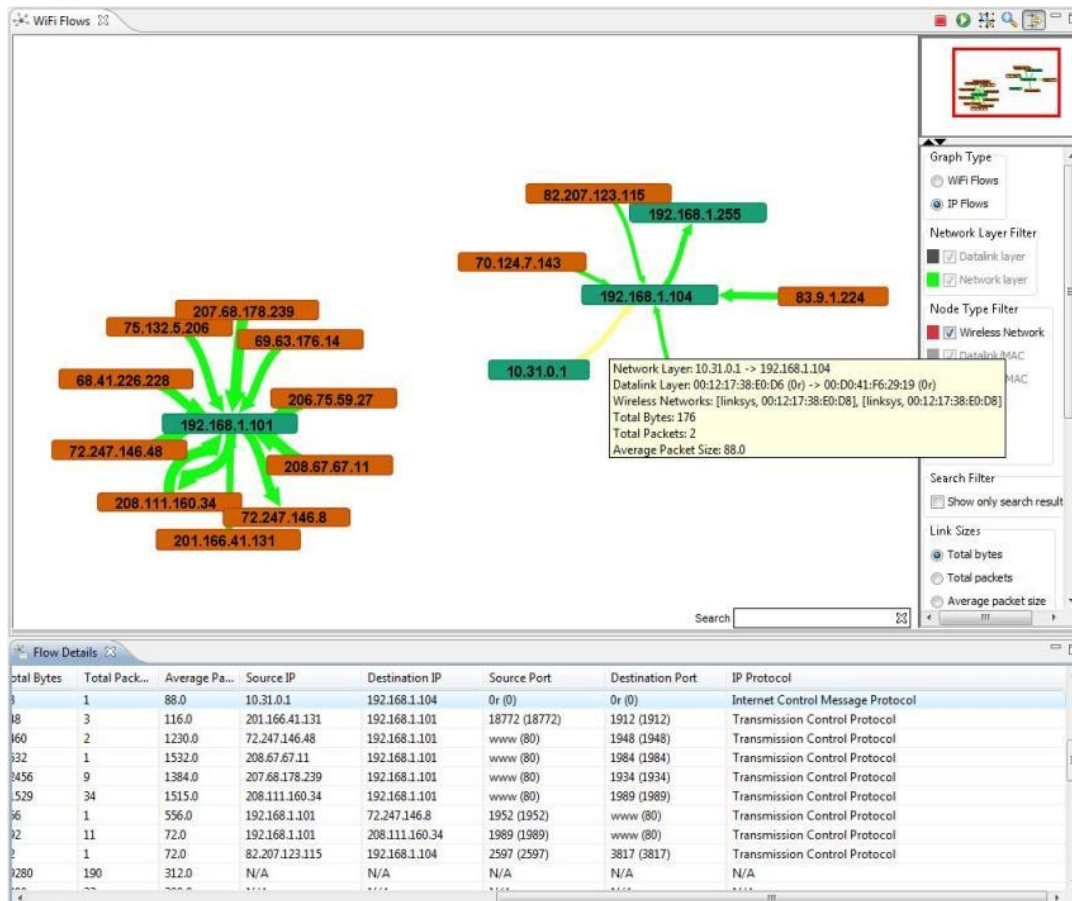
7.1.9 WiFi LAN Example



In the example above, we see two wireless clients, 192.168.1.104 and 192.168.1.101, communicating with a local node 192.168.1.255 (probably broadcast, which we will find out soon) and another 'MULTIPLE IP' node that is labeled local.



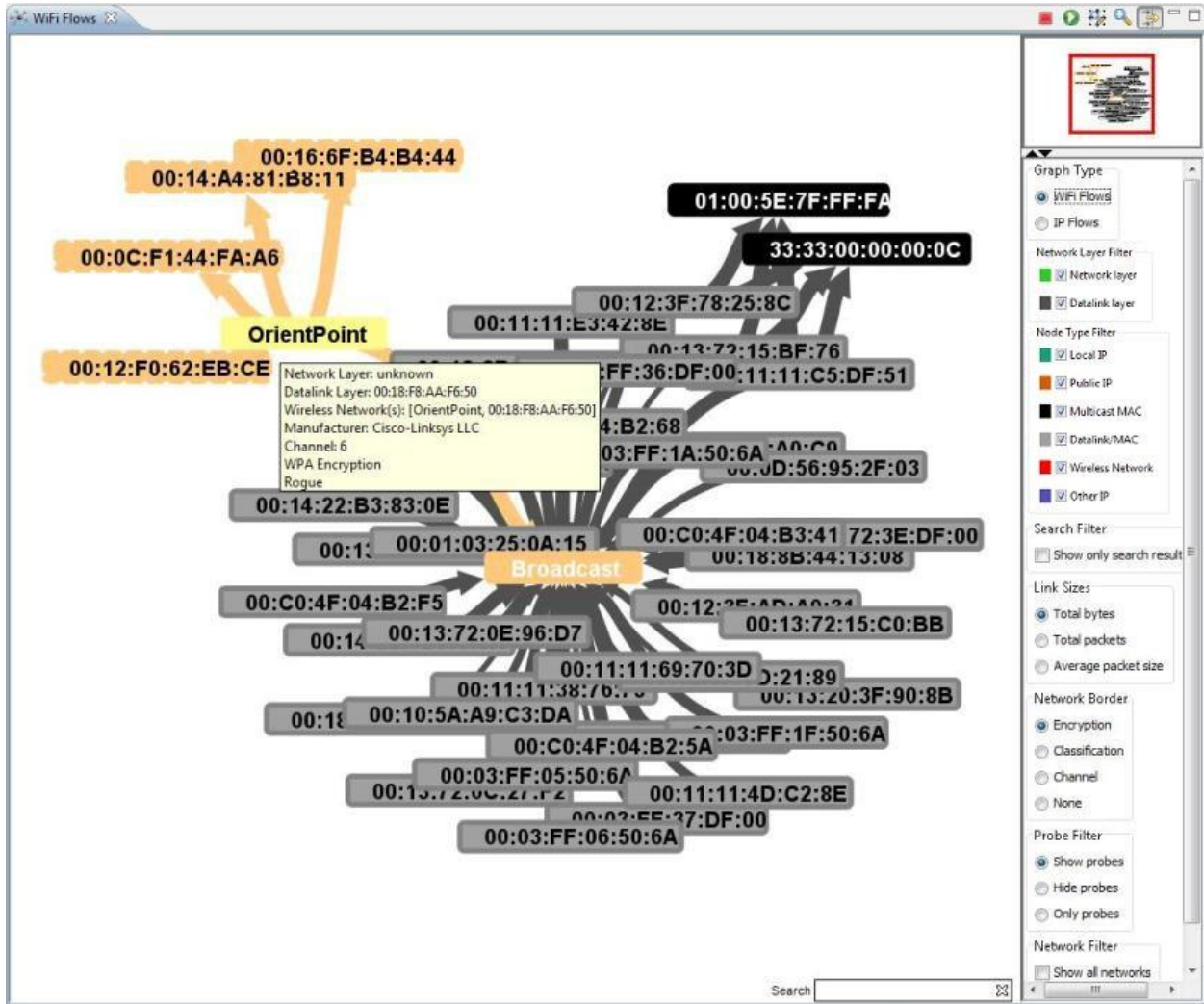
Above, we have disabled the network layer information of the graph and can see the similarities between the BSSID of the Linksys access point and the MAC address of the local IP node associated with multiple IP addresses in our capture. Again, this suggests that the latter is the interface to which traffic is sent that will pass over a wired network.



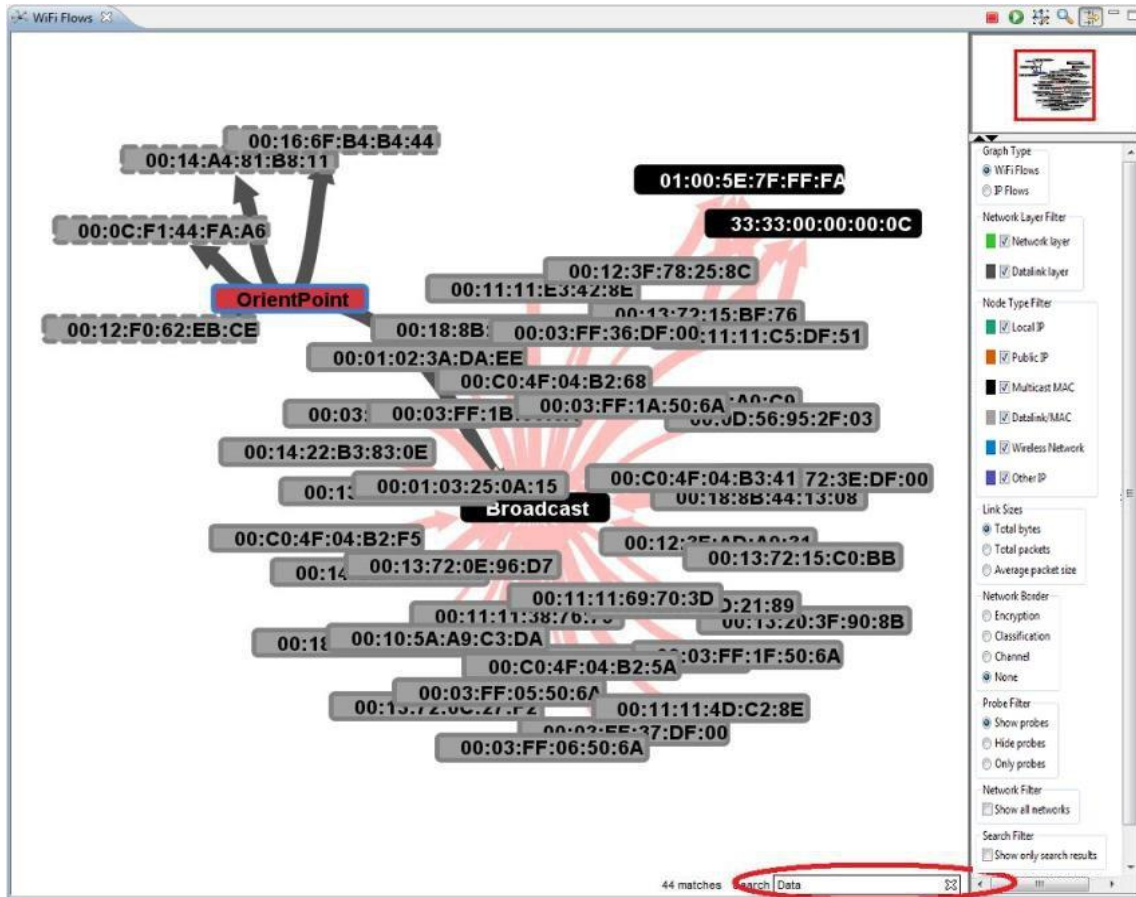
Since we are observing IP communication and there are several IP addresses aggregated into the single node, we switch the graph type over to IP Flows mode. This mode builds the graph nodes based on IP address, giving us a flow graph similar if not the same to other network layer flow graphs.

In this view, with the help of the flow details table, we can see that information is being passed from the IP address 10.31.0.1 to 192.168.1.104 via port 0 in an Internet Control Message Protocol (ICMP) packet. If 10.31.0.1 happens to belong to a router interface on the LAN to which the Linksys access point is connected to, which is probably the case, we can identify that not only is the unencrypted Linksys access point a back door to the LAN but also that a potentially vital network asset's IP address is being exposed through unencrypted radio broadcast.

7.1.10 WiFi Broadcast Domain Example



In this example, we see the access point OrientPoint talking to its broadcast MAC address. In addition, there are several other generic data link layer nodes that are also sending broadcast messages through the air. Since it looks like there's over 30 nodes sending broadcast messages to the air through the access point this should draw a red flag, if not for security issues but for performance since large broadcast domains can cripple network performance.



In trying to figure out what's going on here, we can run a quick search for Data frames. IEEE 802.11 frames contain a type and subtype field which describes what kind of frame is being transmitted. There are three major types: Data, Management, and Control and each one has a number of subtypes associated with it. It turns out that all of these nodes are broadcasting data (rather than beacon frames for example which don't always imply a connection) so it's safe to assume that all of these nodes lie in the same broadcast domain.

A more important thing to notice here is that none of these data link layer MAC addresses can be considered wireless transmitters since there were no frames intercepted that would suggest that they have this capability. This is visualized by the network border, and only nodes with a dashed border can be affirmed as wireless transmitting devices. Upon further analysis of the network topology (trying to figure out what devices belong to what MAC address), we found that the reality of this graph is that most if not all of the data link layer clients are actually machines on the same wired LAN segment as the access point. This is just not good practice, if not for performance then for security as well as considering all broadcast traffic from the wired LAN is being transmitted in the air as well, not only exposing the MAC addresses of several assets on the wired network but also providing a steady flow of data through the air which could be used to aid a hacker in exploiting encryption key vulnerabilities that exist in protocols such as WEP.

One possible fix to this is to put the access point on a different VLAN or subnet than the other clients, allowing a router to take care of passing any traffic that might need to be passed between the wired and wireless segments of the LAN rather than just automatically forwarding the broadcasts.

7.2 Flow Details View

The Flow Details View is a companion to the Flows View, and requires that packet data was captured during the detection run and loaded into MeerCAT. This view allows the users to see detailed information about a particular packet capture. It can also be sorted by any one of the data fields.

This table view is tied in with selecting wireless networks and clients in other views, which will allow analysts to quickly associate traffic with individual networks.

- IEEE 802.11 and Ethernet frame details are shown for all intercepted packets that are encapsulated in one of these link layer frames.
- IP and ARP flows also show detailed information about network and transport (TCP/IP) layer attributes of a communication flow such as source and destination ports, addresses, and protocols.

Start Time	Duration	Source MAC	Destination MAC	BSSID	SSID	802.11 Type	Total Bytes	Total Pac
08-16-08 10:08:46	00:03:30	00:15:70:7A:D8:05	FF:FF:FF:FF:FF:FF	00:15:70:7A:D8:05		Management (0) Beacon (8);	34,304	134
08-16-08 10:08:48	00:03:16	00:17:9A:32:63:D2	FF:FF:FF:FF:FF:FF	00:17:9A:32:63:D2	AMILOCALLINK	Management (0) Beacon (8);	4,158	21
08-16-08 10:08:46	00:00:30	00:17:3F:80:EC:4E	FF:FF:FF:FF:FF:FF	00:17:3F:80:EC:4E	belkin54g	Management (0) Beacon (8);	2,880	15
08-16-08 10:08:46	00:03:40	00:A0:F8:CE:1A:12	FF:FF:FF:FF:FF:FF	00:A0:F8:CE:1A:12		Management (0) Beacon (8);	19,234	59
08-16-08 10:08:46	00:03:31	00:1F:33:2E:67:5E	FF:FF:FF:FF:FF:FF	00:1F:33:2E:67:5E	NETGEAR Home	Management (0) Beacon (8);	4,370	19
08-16-08 10:08:46	00:00:30	00:17:3F:80:EC:4E	FF:FF:FF:FF:FF:FF	00:17:3F:80:EC:4E	belkin54g	Management (0) Beacon (8);	2,880	15
08-16-08 10:08:46	00:03:31	00:1F:33:2E:67:5E	FF:FF:FF:FF:FF:FF	00:1F:33:2E:67:5E	NETGEAR Home	Management (0) Beacon (8);	4,370	19
08-16-08 10:08:48	00:03:16	00:17:9A:32:63:D2	FF:FF:FF:FF:FF:FF	00:17:9A:32:63:D2	AMILOCALLINK	Management (0) Beacon (8);	4,158	21
08-16-08 10:08:46	00:03:42	00:A0:F8:CE:1A:10	FF:FF:FF:FF:FF:FF	00:A0:F8:CE:1A:10		Management (0) Beacon (8);	12,330	45
08-16-08 10:09:12	00:00:00	00:A0:F8:CE:1A:10	00:A0:F8:B9:68:7D	00:A0:F8:CE:1A:10		Management (0) Probe Respo...	270	1
08-16-08 10:08:46	00:03:36	00:1E:2A:00:69:72	FF:FF:FF:FF:FF:FF	00:1E:2A:00:69:72	nyavenizza	Management (0) Beacon (8);	16,724	74

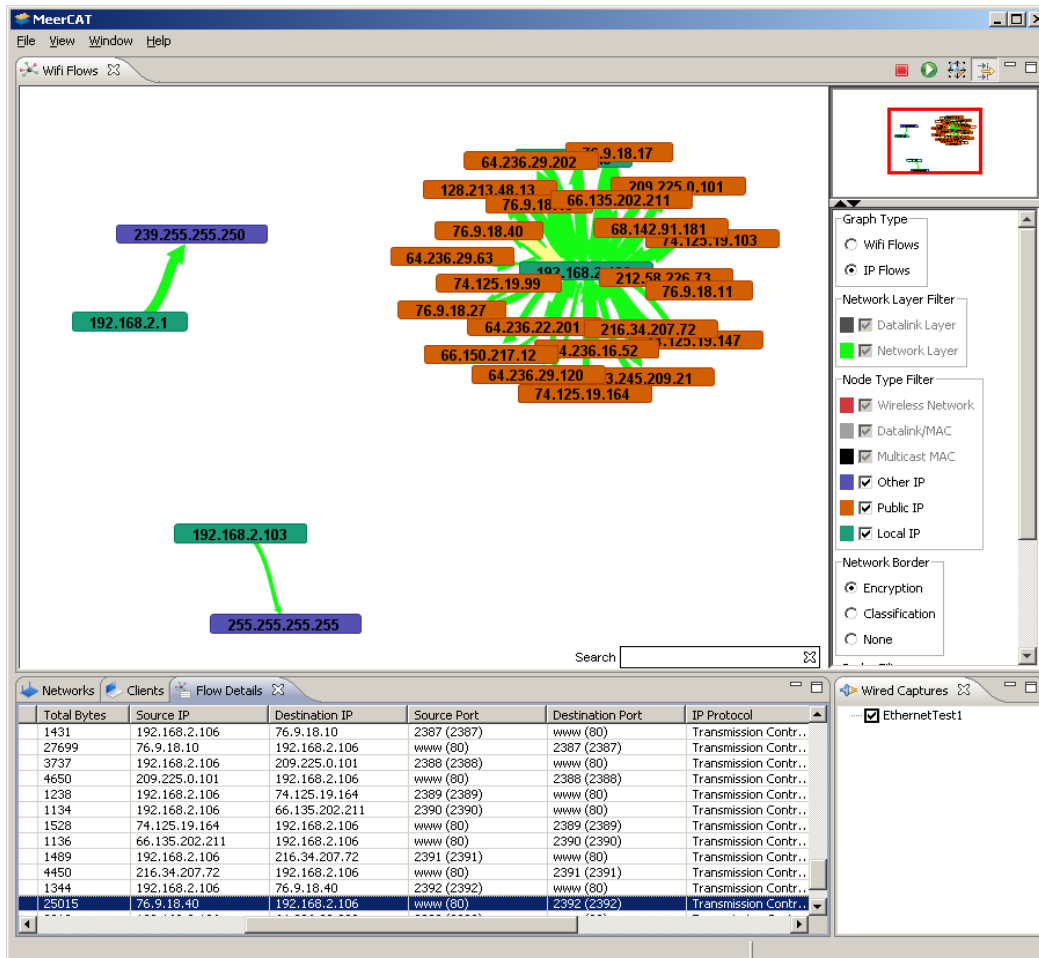
7.2.1 Toolbar

The toolbar of the Flow Details View contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

7.3 Wired Captures



Above is an example of the three views that wired capture data has an effect on in MeerCAT.

7.3.1 Wired Captures View

In the Wired Captures view, each wired capture that was imported is listed and may also be removed by right clicking on the capture and selecting "Delete." Checking off the capture will make the capture details data visible to any view that will handle it.

7.3.2 Flows View

In the Flows view, wired capture data is only considered when the graph is in IP Flows mode. For more information on the Flows View, see the Flows View help section.

7.3.3 Flow Details View

In the Flow Details view, wired data is displayed just like wireless data, except the BSSID and SSID fields will be blank for each of these flows as there are no associated wireless networks.

8 Reporting

8.1 Reporting Features

MeerCAT contains various ways to report and present the results of an audit or security analysis. This includes copy to clipboard, exporting a view to an image file, drag and drop views to other applications, e-mail views, and template based report generation to Word or PowerPoint. Most of these features are available via the main Report menu. Annotations can also be added to views, which are then included in the report and also in e-mail reports.

8.2 Generate Report

The Report -> Generate Report menu creates a document or presentation based on one of a number of templates.

8.2.1 Report Generation Criteria

- **Select Report** – Select the type of report to generate, and the format if applicable.
 - **Snapshot of Current Analysis** – report on the currently open views and their annotations
 - **Alert Summary** – report on the alerts that have been generated
 - **Repeat Offender List** – report on devices that have caused multiple alerts
- **Configure Report options** (if applicable)
 - **Include alerts only in this range** – if unchecked, all dates will be included
 - **Include alerts only from these locations** – if none selected, all locations will be included
 - **Include only severity** – select the severities to report on
 - **Include only status** – select the statuses to report on
 - **Organize alerts by** – select how alerts should be grouped. One of the following:
 - **Alert Pattern**
 - **Alert Status**
 - **Device**
 - **Location**
 - **Severity**
 - **Analyst Name** - Name to be inserted into the report template when generating report. The default analyst name can be changed in the Reporting Preferences options in Window -> Preferences, or by modifying the Analyst Name and generating a new report.
- **Output Directory** - Browse to the location where the report should be saved. The default directory can be changed in the Reporting Preferences options in Window -> Preferences, or by modifying the path and generating a new report.
- **Output File** - The filename to be used when saving the report.
- **Open report after generation** - If this is checked, the report will automatically open after being generated, in the selected document format (the default Word or PowerPoint viewer).

- *Note:* The associated application will launch automatically with Windows. For Linux, save the file, then open with Open Office or a compatible application.

Generate Report

Report Parameters

Select the report type, configure its options, specify where to save the report, and then generate the file.

Select Report

- Snapshot of Current Analysis (document)
- Snapshot of Current Analysis (presentation)
- Alert Summary (document)
- Alert Summary (presentation)
- Repeat Offender List (document)

Configure Report Options

Include alerts only in this range

Start: 6/11/2012 3:16:23 PM End: 7/10/2012 3:16:23 PM

30 days ago 15 days ago 5 days ago Yesterday Today

Include alerts only from these locations

Demo

Include only severity: Low Medium High

Include only status: Pending Notified Resolved Ignored

Organize alerts by: Alert Pattern

Analyst Name: ChrisE

File Save Location

Output Directory: C:\Users\ChrisE\MeerCAT\reports Browse...

Output File: MeerCAT Report 2012-07-10

Open report after generation

Generate Cancel

8.2.2 Copy Screenshot of Active View

This menu option will copy the active view to your systems clipboard. This can be useful if you simply want to paste the view to another application. Ctrl+Shift+C is the shortcut key for this operation.

8.2.3 Save Screenshot of Active View

This menu option will export the active view to an image file. Available image types are PNG, JPEG, GIF, and Bitmap. Ctrl+Shift+S is the shortcut key for this operation.

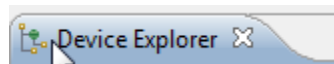
8.2.4 Email Screenshot of Active View

This menu option will create a new email message using your default mail client (e.g. Outlook). This message will include the active view as an image attachment and a view's annotation will be used for the body of the email message. Ctrl+Shift+E is the shortcut key for this operation.

Note: In Windows, the email client will be launched automatically with the associated attachment.

8.2.5 Drag and Drop

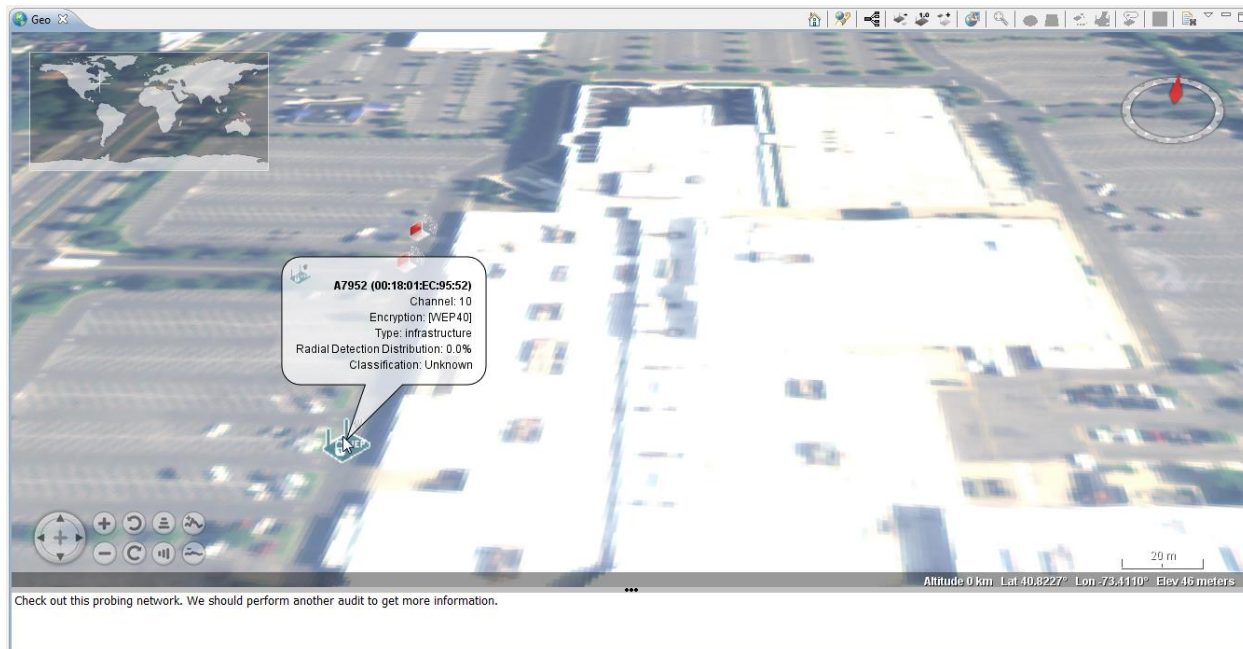
Each view can be dragged and dropped into other applications. This can be done by holding down the Alt key while dragging a views title as shown here:



Note: Not all applications will support this feature.

8.2.6 View Annotations

Annotations can be added to the Geo, Flows, Network Topology, Navigator, and Timeline views, similar to notes in PowerPoint. To show the view annotations, double-click or drag the gray bar at the bottom of each view. This will expand the view's annotations control. Here you can type in notes, which will be including in Word, PowerPoint, and email report.



8.3 Report Templates

MeerCAT comes with two default templates, one for Word and one for PowerPoint. These templates can be modified using Word, PowerPoint, OpenOffice, or a new template can be created and used within MeerCAT. Templates are stored and configured in the reportConfig folder, located in your user home MeerCAT folder. To have a new template appear within MeerCAT, you must add the template to the reports.xml file in the reportConfig folder.

8.3.1 Images

Image views can be added to a report template by dragging and dropping the associated view's placeholder JPG file in the reportConfig folder. The position can be placed anywhere within the document or presentation. Only the width of the image is maintained when the report is generated. The height will maintain the aspect ratio based on the width.

There is an additional step for using the placeholder in a PowerPoint presentation. The object associated with the placeholder must be named to match the text shown in the placeholder.

8.3.2 Tables

Table views, including the Networks, Client, Flow Details, and Device History tables, can be added to a document report using the following keyword text. This text will be replaced at report generation time with the actual table data.

- MeerCAT.Networks
- MeerCAT.Client
- MeerCAT.DeviceHistory
- MeerCAT.FlowDetails

8.3.3 Annotations

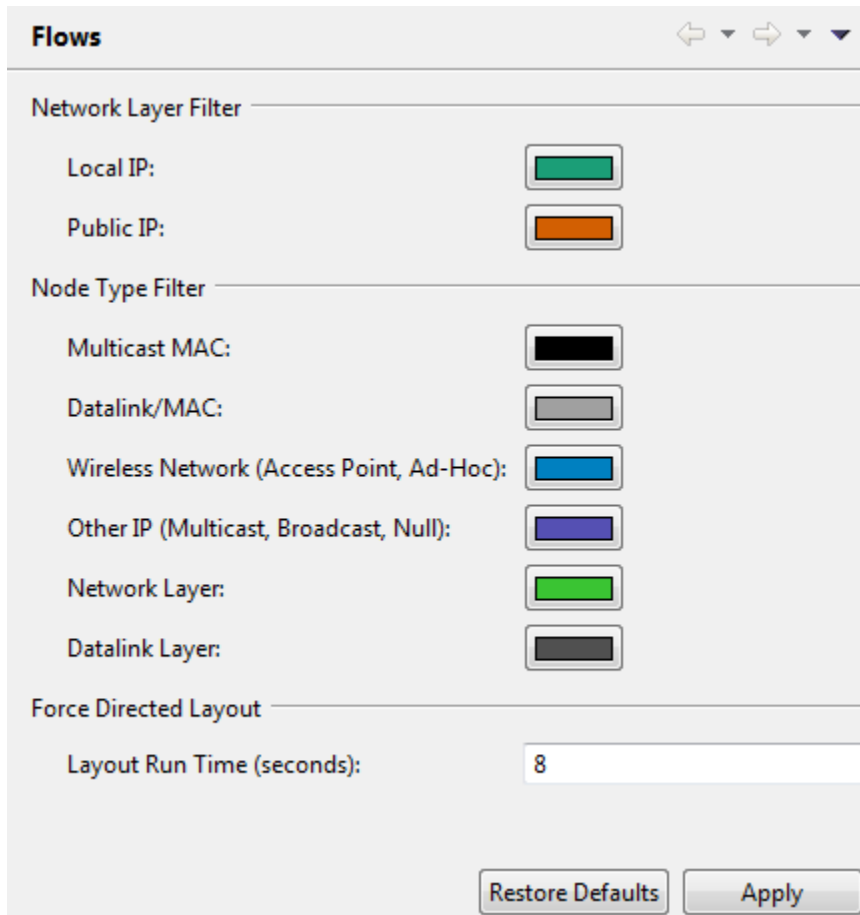
View annotations can be added to a document or presentation. The following keywords are used:

- MeerCAT.Geo3D.Notes
- MeerCAT.Flows.Notes
- MeerCAT.NetworkTopology.Notes
- MeerCAT.Navigator.Notes
- MeerCAT.Timeline.Notes
- MeerCAT.ImageViewer.Notes

9 Other Preference Options

9.1 Flow Colors

The Flows View is capable of displaying many types of connections. To customize the display of connections in this View, from the MeerCAT main menu select **Window -> Preferences**. Then click on the **Flows** selection.



This page allows each address type – Multicast MAC, Datalink MAC, Local IP, Public IP, Wireless Network and Other – to have its own color. To change colors, click on the color to select from the color palette. Colors used to depict the Datalink Layer vs. the Network Layer can also be customized.

Another feature of the Flows View which can be customized is the duration of the force-directed graphing feature of the display. The Flows View uses a technique which positions the nodes depicted in the View so that all the edges are of more or less equal length and which minimizes the crossing edges as much as possible. The number of seconds during which this technique is applied can be controlled by specifying the duration. As of this writing, the default is 8 seconds, seen in the screenshot above.

9.2 General Colors

Colors can be helpful in highlighting specific areas of interest throughout MeerCAT. To further manage color settings, it is possible to color wireless and clients identified by MeerCAT according to Encryption, Channel, Classification or Mission. To perform such customization, select the **Window -> Preferences** submenu. Then choose **General Colors**.

As shown below, select the type of coloring to be performed from the dropdown menu.

General Colors

Devices

Network color: Encryption

Network Topology 'stage' color: Encryption

Client color: Classification

Encryption

WPA [Blue] WEP [Light Blue]

Other [Green] Unencrypted [Red]

Classification

Trusted [Blue] Friendly [Purple]

Rogue [Red] Unknown [Grey]

Misconfigured

Misconfigured [Orange] Not Misconfigured [Dark Blue]

No Configuration [Grey]

Other

Selected [Yellow]

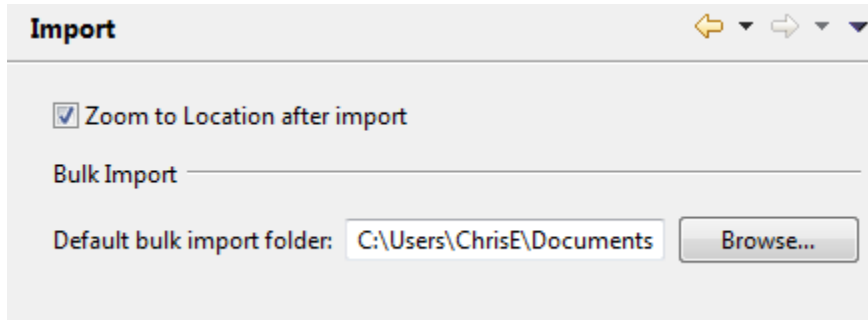
Note: Channel colors are fixed. See Channels view for legend.

Restore Defaults Apply

9.3 Import

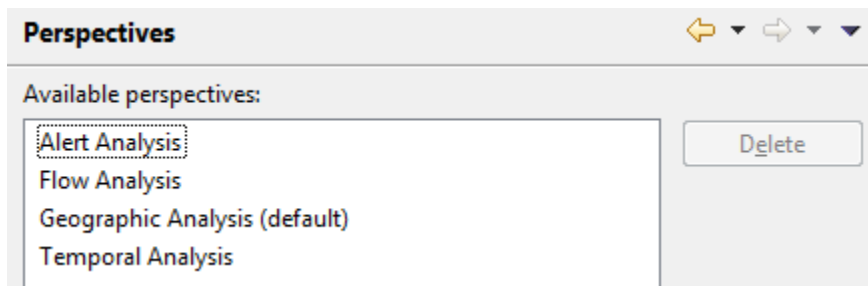
By default, MeerCAT looks for data to import in default user-specific folder, e.g., **c:\Users\username.DOMAIN\Documents** (Windows 7). This can be changed by accessing the Import preference screen shown below.

Use the **Restore Defaults** button to switch back to the original MeerCAT default.



9.4 Maintain Perspectives

MeerCAT allows users to tailor different views to suit the particular style of analysis and type of task. Once these View settings – which views are showing, which options have been invoked, which zoom level is in effect, etc. -- have been created, they can be saved so that the workspace can be restored at any time. A list of available perspectives is available through the **Window -> Open Perspective** submenu. The same list is available through MeerCAT Preferences. Access the list through the **Window -> Preferences** and select **Perspectives** from the option list to the left.

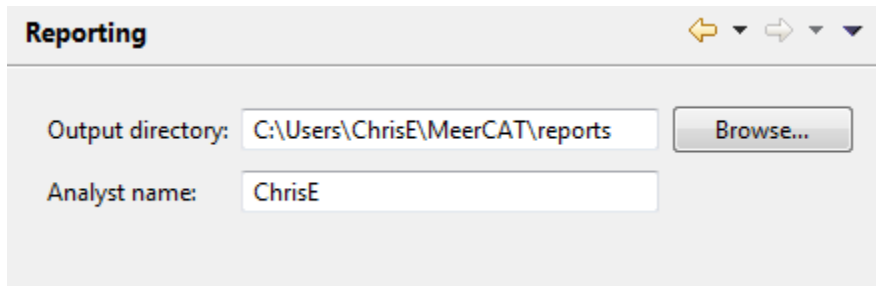


To remove a perspective, highlight it and click **Delete**.

9.5 Reporting Options

By default, reports created using MeerCAT are written to a default folder, e.g., **c:\Users\username.DOMAIN\MeerCAT\reports** (Windows 7). A different folder can be specified by selecting **Window -> Preferences** from the main menu, and then selecting the **Reporting** option from the list on the left of the screen. This screen also permits the default analyst's name to be changed from the default.

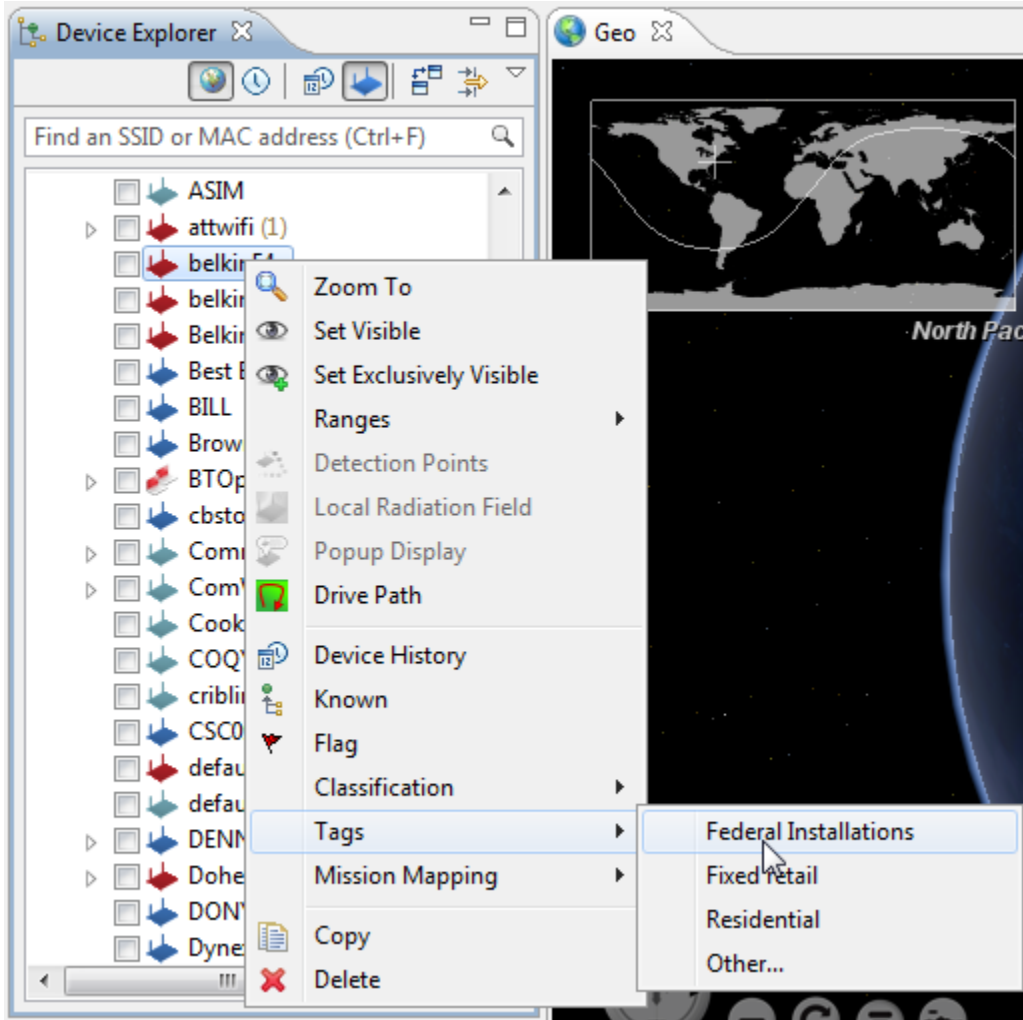
Use the **Restore Defaults** button to return both values to the initial installation values.



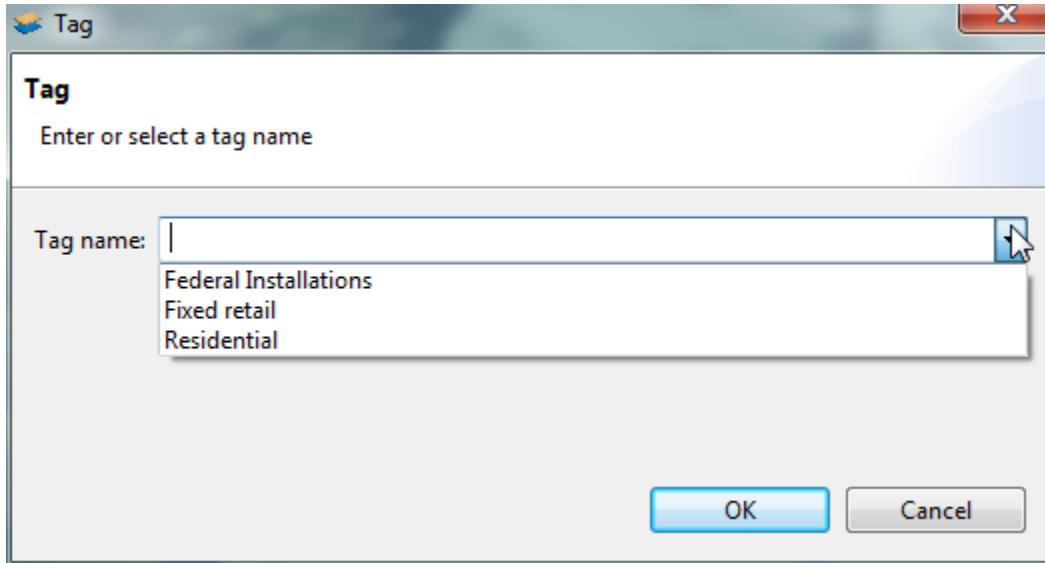
9.6 Tags

The Device Explorer View permits various features of networks and devices to be viewed in more detail. For instance, the Client Properties window allows the MAC address and Classification to be updated if necessary. The Wireless Network Properties window allows these, as well as additional fields, to be maintained. To aid in further grouping networks, wireless networks can be given short keywords, or tags.

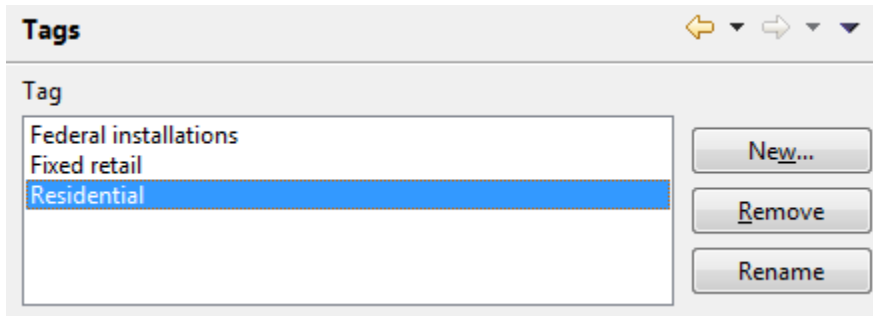
To assign a tag in the Device Explorer View, select a network and right-click. Select tag from the list of options. If tags have already been defined, these will be shown in the tag flyout menu, as shown below.



Existing tags can also be selected by choosing “**Other...**” Use the following screen, which also allows new tags to be added as needed.




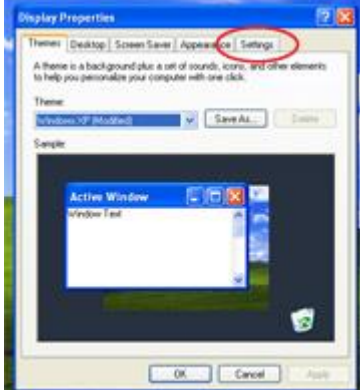

Once defined, tags can be maintained through the **Preferences** menu. Select the **Main Menu -> Window -> Preferences** and then the **Tags** option from the list on the left. The window shown below allows tags to be added, deleted or renamed. Select **New...** to create a new tag. To remove or rename a tag, first highlight it, make changes as needed, then select **Rename** or **Remove**, as appropriate.



10 Frequently Asked Questions

1. The geographic globe appears but no imagery is displayed; only a halo outline.

This is commonly attributed to an outdated video card driver. Follow these steps to update your driver:

<p>Step 1:</p>	<p>(These instructions are for Windows users.) On the desktop, right click and select 'Properties'. This will bring up the Display properties panel.</p>	
<p>Step 2:</p>	<p>At the top of the window, click on the 'settings' tab.</p> <p>This will bring up detailed information for graphics and reveal the hardware vendor. This will be necessary to download the proper driver.</p>	
<p>Step 3:</p>	<p>In the middle of the screen is a pull-down menu labeled 'Display'. Read the contents of the box and look for one of three key words... ATI, Nvidia, or Intel.</p>	
<p>Step 4:</p>	<p>Download the appropriate driver based on the previous step. The drivers for each can be found at...</p> <p>ATI / AMD http://ati.amd.com/support/driver.html</p> <p>Nvidia http://www.nvidia.com/content/drivers/drivers.asp</p> <p>Intel http://www.intel.com/support/graphics/index.htm</p>	

Step 5:	Download the driver to your desktop and run it, following all default instructions. This step may prompt your computer to reboot. Make certain any open applications have saved and allow the computer to reboot.
---------	---

If you still experience problems, this is sometimes related to the amount of memory allocated to MeerCAT. Decreasing the `-JMX` value as described in the next question sometimes resolves this issue.

You will also experience this behavior if running MeerCAT on a virtual machine or Remote Desktop Connection (RDC).

2. What is the best configuration for working with large datasets?

The MeerCAT.ini file located in your installation directory can be modified with a text editor to give MeerCAT more system memory. The `-Xmx` value represent the maximum amount of RAM given to MeerCAT. The default value is 1024 MB. For systems with large amount of available memory, you may want to increase this value to 2048 MB or higher.

Another way to reduce memory requirements is to only have visible the views of interest. Closing views not in use will reduce memory load, especially views that have requested historical data.

Although you may notice memory usage peak, MeerCAT uses advanced caching and performance optimization to use available memory most efficiently.

3. How does MeerCAT determine a device's location?

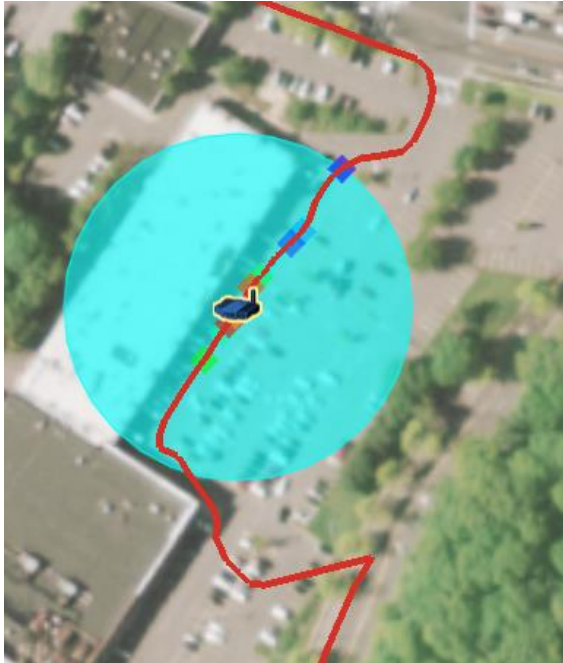
If only the network XML file is imported, MeerCAT uses the center of the detection range (i.e., $\frac{\text{max}+\text{min lat}}{2}$, $\frac{\text{max}+\text{min long}}{2}$). If the GPS file is used then an average of the detected GPS points, weighted by the square of the signal strength is used, but only points whose signal strength is within 10% of the maximum (note that does not mean "top 10% of the points").

4. What is Radial Detection Distribution?

Radial Detection Distribution is a measurement of how well MeerCAT can determine the location of a device, based on the detections that it has been provided. Consider each of a device's detections to lie on a radius extending from its actual location. Radial Detection Distribution is the proportion of the sector enclosed by the smallest angle that includes all of the detections to a complete circle.

For example, to obtain the best possible placement, the detections would be distributed such that they form a complete circle around the device. This would mean that the largest angle between any two adjacent detections would be zero radians, and the Radial Detection Distribution would be 100%.

Consider the common case in which the wardriving vehicle travels along one side of a building containing an access point, as seen below. The Radial Detection Distribution for this device is 50.7% because all of the detection points are in a relatively straight line. MeerCAT has a good idea of the device's latitude because the vehicle traveled from north to south, but has a very little idea of its longitude.



5. How does MeerCAT determine whether a device is a phone?

MeerCAT considers a device to be a phone if the OUI (Organizationally Unique Identifier) portion of its MAC address appears in a list of OUIs of wireless chipsets that are known to be installed in phones. Note that some manufacturers use the same chipsets in multiple product lines, so it is possible that some devices that are not actually phones are depicted as such.

11 Glossary of Terms

<i>Access Point</i>	A central transmitter and receiver of WLAN signals that allows wireless devices to connect to a wired network.
<i>Ad-hoc</i>	A wireless network where nodes directly communicate to each other without the use of a central access point.
<i>Alert</i>	A notification used in MeerCAT to indicate suspicious behavior on a wireless network. What constitutes suspicious behavior can be defined by the analyst via an <i>Alert Pattern</i> .
<i>Alert Pattern</i>	A rule that defines suspicious behavior on a network. MeerCAT uses an Alert Pattern to generate <i>Alerts</i> from <i>Detection Run</i> data.
<i>Association</i>	A distinct connection between a <i>Client</i> and <i>Network</i> . The Associations column in the Clients table indicates the number of networks to which a client has connected.
<i>Authentication Suite</i>	The type of authentication mechanism used by a device to connect to a WLAN. If known, this can be <i>PSK</i> or <i>IEEE 802.1X</i> .
<i>Bounds</i>	A designated geographical area that can be used as filter criteria in the Device Explorer or as part of an <i>Alert Pattern</i> .
<i>BSSID</i>	The identifier of a basic service set. In an infrastructure network, the BSSID is the <i>MAC address</i> of the wireless access point; in an ad-hoc network, the BSSID is a locally administered MAC address that is generated from a random number.

<i>Carrier</i>	The particular IEEE 802.11 standard type used for a network. See <u>IEEE 802.11</u>
<i>CCMP</i>	(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) An encryption protocol used in WPA2 .
<i>Channel</i>	A transmission medium used to send a communication signal. A WLAN channel is one that is allowed using <u>IEEE 802.11</u> . In the 2.3 GHz range, there are 14 designated channels. In the 5 GHz range, there are 23 channels available, although most consumer equipment makers support only 8 of them.
<i>Cipher</i>	An algorithm for performing encryption or decryption.
<i>Classification</i>	A means of organizing wireless devices according to four categories: <u>Trusted</u> , <u>Friendly</u> , <u>Rogue</u> , <u>Unknown</u> .
<i>Client</i>	A device that accesses a network.
<i>Cloaked</i>	Used to describe an <u>Access Point</u> that conceals its SSID .
<i>CSV</i>	(Comma-separated values) A type of file that stores tabular or database-style information in plain-text form.
<i>Detection Point</i>	The location at which a particular wireless network has been detected.
<i>Detection Run</i>	A collection of data accumulated from a detector of WiFi wireless networks.
<i>Device</i>	Used in MeerCAT to denote either a <u>Network</u> or <u>Client</u> .
<i>Drive Path</i>	A route taken by a vehicle on a detection run.

Encryption Type

The security protocol used to secure wireless networks. This can be [WEP](#), [WPA](#), [WPA2](#), or [Unencrypted](#).

Friendly

A [Classification](#) used to denote a device that is known to not be threatening.

Group Cipher

The [Cipher](#) suite used to protect broadcast or multicast traffic from an [Access Point](#) to multiple stations. If known, this can be [WEP40](#), [TKIP](#), [CCMP](#), [WEP104](#).

IEEE 802.11

A collection of IEEE specifications for wireless local area network communication.

802.11a signals in the 5 GHz frequency spectrum and supports a data rate of up to 54 Mbps. Due to this high frequency, 802.11a networks have a shorter range than those of 802.11b/g.

802.11b signals in the 2.4 GHz frequency spectrum and supports a data rate of up to 11 Mbps. It is an expansion of the original standard and has therefore been accepted as the quintessential technology for wireless LANs.

802.11g signals in the 2.4 GHz frequency spectrum and supports a data rate up to 54 Mbps. It is backwards compatible with 802.11b.

802.11n is the newest IEEE standard for WiFi. It uses multiple wireless signals and multiple-input multiple-output (MIMO) antennas. It signals in both the 2.4 GHz and 5 GHz frequency spectrums and supports a data rate of up to 100 Mbps.

<i>IEEE 802.1X</i>	An IEEE standard that provides an authentication protocol for devices connecting to a wireless network.
<i>Ignored</i>	A Status intended to describe a false-positive Alert , or one that should simply be disregarded.
<i>Infrastructure</i>	A mode of operation in which devices communicate through an access point that functions as the connection point to a wired network.
<i>IP Address</i>	A number assigned to a device that is part of a network using the Internet Protocol for communication.
<i>LAP</i>	The Lower Address Part (last three octets) of a Bluetooth address. It is transmitted with every Bluetooth packet. See also: NAP , UAP .
<i>Local Radiation Field</i>	A display of an access point's interpolated signal strength.
<i>Location</i>	A user-defined term used to represent an area at which a detection run took place. It serves as a filtering criteria in the Device Explorer and Alerts table.
<i>MAC address</i>	(Media Access Control address) A unique hardware identifier of a node in a network. It is a 48-bit address space written in hexadecimal in the form xx:xx:xx:xx:xx:xx.
<i>Misconfigured</i>	A network with a configuration that does not match its known configuration.
<i>Mission Mapping</i>	A user-defined term that allows an analyst to identify and group devices belonging to the same function.
<i>NAP</i>	The Nonsignificant Address Part (first two octets) of a

	Bluetooth address. See also: LAP , UAP .
Network	A device serving as an access point.
Notified	A Status intended to describe an Alert whose existence has been passed along to security personnel.
Pairwise Cipher	An encryption Cipher used for unicast data between a station and access point. If known, this can be WEP40 , TKIP , CCMP , WEP104 .
Pending	A Status intended to describe an Alert that has not yet been handled by security personnel. This is the default status of an incoming alert.
Probe	Used to describe a device that is monitoring or collecting data about a network.
PSK	(Pre-Shared Key) An authentication method where both access point and all clients share the same key.
Radial Detection Distribution	Please see the User Manual FAQs.
Repeat Offender	A device that has caused more than one alert.
Resolved	A Status intended to describe an Alert that has been taken care of by security personnel.
Rogue	A user-defined term used to describe a device that could potentially be threatening.
Severity	A user-defined term used to describe the importance or degree of a particular Alert Pattern . Can be High, Medium, or Low.
Signal Strength	The quantity of radiated power that determines the amount of network bandwidth available on a connection.

SSID	(Service Set Identifier) The term used to identify a particular Access Point .
Status	Used to describe the state of an Alert . Can be Pending , Notified , Resolved , Ignored .
TKIP	(Temporal Key Integrity Protocol) A security algorithm that changes the key used for each packet. It is used as a replacement encryption for WEP .
Trusted	A user-defined term used to describe a device that is known and should be protected against threats.
UAP	The Upper Address Part (third octet) of a Bluetooth address. See also: LAP , NAP .
Unencrypted	A device using no method to encipher its signals.
Unknown	A user-defined term used to describe a device that is neither Trusted , Friendly , nor Rogue .
Wardrive	A period during which one drives around collecting WiFi data for later or real-time analysis.
WEP	(Wired Equivalent Privacy) A security algorithm that encrypts each packet separately using a 10 or 26 hexadecimal digit key. It has been widely criticized due to a number of weaknesses.
WEP40	Standard 64-bit WEP that uses a 40-bit key.
WEP104	Extended 128-bit WEP that uses a 104-bit key.
WPA	(WiFi Protected Access) A security algorithm developed in response to the weaknesses found in WEP encryption. It uses the TKIP protocol and includes a message integrity check, intended to prevent packet tampering.