



PILOT CONSOLE

Reference Manual

THE SHARK DISTRIBUTED MONITORING SYSTEM



PUBLISHED BY

CACE Technologies, Inc.

1949 5th Street, Suite 103

Davis, CA 95616

Copyright © 2010 CACE Technologies, Inc.

All rights reserved. No part of the contents of this manuscript may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Wireshark and the Wireshark icon are registered trademarks of Wireshark Foundation, Inc.

Microsoft Word, DOS, Windows XP, Microsoft Excel, Microsoft Wordpad, and Windows Vista are registered trademarks of Microsoft, Inc.

Acrobat Reader is a registered trademark of Adobe Systems, Inc.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein with the exception of those aforementioned, are fictitious.

The Shark Distributed Monitoring System

Pilot Console Reference Manual

Document Revision: 4.1

Document Date: October 2010

<http://www.cacotech.com>

Contents

1. Overview	10
The Shark Distributed Monitoring System	10
Pilot Console – Feature Summary	12
Graphical User Interface	12
Management Interface	12
Interface to the Shark Packet Recorder’s Jobs Repository	12
Wireshark Integration	13
Interactive Views and Charts	13
Drill-Down	13
Time Control	13
Watches	13
Report Generation	13
Hardware and Software Requirements for Pilot Consoles	14
2. Graphical User Interface	15
Graphical User Interface Components	15
Ribbon Panel	15
Sources Panel	16
Views Library	16
Main Workspace	16
Events Panel	17
Menu Button and Status Bar	17
Menu Button	18
Status Bar	18
3. Home Ribbon	19
Trace Files	19
Add Trace File	19
Add Folder	19
Clear List	20
Export	20
Wireshark	20
File	21
Settings	21
Channels	21
Decryption Keys	21
Name Resolution	22
Sub Net Mask	22
General	22
Search	23
Update Sources	23
Close All Tabs	23
Getting Started	23
View	23
Pause	23
Resume	23
Save	24
Restore	24
Detach	24
Selection	24

Send to Wireshark	24
Send to Trace File	25
Drill Down	25
Copy to Clipboard	25
4. Time Control Ribbon	26
Quick Navigation	28
Begin	28
Step Back	28
Step Forward	28
End	28
Selection Duration	29
Time Selection	29
5. Watches and Events Ribbon	30
Creating Watches on Strip Charts and Bar Charts	30
Watch in Sources Panel	31
Context Menu for Watch Applied to a Live Source	31
Context Menu for Watch Applied to a Trace File	31
The Watch Editor	31
Name and Description	32
Severity	32
Enabled	33
Trigger Conditions	33
Expanded Trigger Condition	34
Multi-Line Strip Charts	34
Timing Details for Bar Charts	35
Actions	36
Transition Conditions	36
Notify Me	37
Send an email with the watch event details	38
Start a packet capture	39
Send a remote syslog message over UDP	39
Run a program on the Pilot Probe	39
Send a message to a Twitter account	40
Log the events in the Probe's syslog	40
Start a Capture Job	40
Stop a Capture Job	40
Log the events in a CSV file on the Shark Appliance	41
The Ribbon	41
Add Watch	41
Selected Watches	41
Edit Selected Watch	41
Remove Selected Watch	41
Enable Selected Watch	42
Pause Selected Watch	42
Filtering Events Section	42
Views Filter	43
Probes Filter	44
Severities Filter	44
Watches and Events Filter	44
Events Overlay	45
Predefined Watches	45
6. Reporting Ribbon	48

Generate Report	48
Current View.....	48
All Views	48
Format	49
Open Reports	49
Management.....	49
Recent.....	50
Change Folder.....	50
Browse Folder.....	50
Settings.....	50
Title.....	50
Analyst/Client Information.....	51
Report Designer.....	51
7. Report Designer Ribbon	52
Styles	52
Includes	52
Change Logo	52
Table of Contents	52
MD5 Checksums of Trace Files.....	53
Cover Page.....	53
Data as Table	53
Visual Settings	53
White Chart Background	53
Draft Images (Faster).....	53
Page Setup.....	53
Portrait	53
Landscape.....	54
Display	54
Zoom Amount.....	54
Decrease Zoom.....	54
Increase Zoom	54
Width.....	54
Page.....	54
Close Designer	54
8. Remote Ribbon.....	55
Remote Probe Credential Manager	55
User and Group Access Control.....	55
The Ribbon	56
Probe Management	57
Add Probe.....	57
Probes.....	57
Probe Selection	58
Select All Probes	58
Expand Selection	59
Collapse Selection	59
Disconnect from Selected	59
Web Interface.....	59
Files	59
Import Files into Probes	59
Export Files from Probes	59
View Selection	60
Select All on Probes.....	60

Close Selected	60
Attach to Selected	60
Detach from Selected	60
Share Selected with	60
9. Shark Packet Recorder	61
Capture Jobs (Shark Appliance Packet Recorder)	62
Trending/Indexing Parameters	64
Capture Job Control Buttons	65
Status of a Capture Job	66
Capture Jobs in the Devices Panel	66
Operations on Job Interfaces	67
Capture Jobs in the Files Panel	67
Operating on Job Traces – Trace Clips	68
Creating Trace Clips	68
Time Control Panel for Creating Trace Clips	69
Using Time Selection to Create a Trace Clip	71
Using Views as Job Trace Indices	72
Using Events to Create Trace Clips	73
Lifetime of a Trace Clip	74
10. Sources Panel	75
Devices	75
Wired Ethernet Adapters	75
Wireless Adapters	76
Context Menus in the Devices Panel	76
With Nothing Selected or Local System Selected	76
With a Shark Appliance Selected	77
With an Interface Selected (Local System or Shark Appliance)	77
With a Capture Job Interface Selected (Shark Appliance)	78
With a View Selected	79
Files	80
Context Menus in the File Panel	80
With Nothing or Local System Selected	81
With a Shark Appliance Selected	81
With A Trace Folder Selected on Local System	82
With A Trace File Selected on Local System	83
With A Trace Folder Selected on a Remote Shark Appliance	84
With A Trace File Selected on a Remote Shark Appliance	85
With The Jobs Repository Folder Selected on a Remote Shark Appliance	86
With A Job Trace Selected on a Remote Shark Appliance	86
With A Trace Clip Selected on a Remote Shark Appliance	86
With a View Selected	87
11. Views Panel	88
Regular Views, Fast Views, and Forbidden Views	89
Using Views	89
Applying a View (Local or Remote Sources)	89
Applying a View with a Filter	90
View Library	90
Context Menus	91
Tooltips	92
Recently Used	92
Context Menu	92
Custom Views	93

Context Menus	93
Search Text Box	96
12. Indexing	97
Indexing a Trace File.....	97
Apply an Index to a Trace File	97
Context Menu	97
Add Trend Index	97
Interrupt Trend Index.....	98
Remove Trend Index	98
Index Icons on Trace Files.....	99
Tooltips.....	99
File	99
Apply a View to a Indexed Trace File.....	99
Drag and Drop Cursors for Indexed Trace Files.....	100
Search Text Box	100
13. Main Workspace.....	101
Context Menus	102
Tooltips.....	102
Notes	102
Selection	103
Mini	103
14. Conversation Ring.....	104
Default.....	104
Size Legends	104
Scroll Wheel.....	104
Hover with Tooltip.....	105
Selected	105
Top Conversations.....	106
Mini	106
Context Menu	106
Context Sub-Menus.....	107
Tooltips.....	107
Endpoint	108
Conversation	108
15. Strip Chart	110
Diagram	110
Current Selection Interval	110
Selection	111
Mini	112
Context Menu	113
Context Sub-Menu	114
Dialogs.....	114
Tooltips.....	115
16. Bar Chart	116
Single Bar Chart.....	116
Default.....	116
Selection	116
Mini	117
Stacked Bar Chart.....	117
Default.....	117
Selection	117
Mini	117

Grouped Bar Chart	118
Default	118
Selection	118
Mini	119
Navigation Through Data	120
Context Menu	120
Context Sub-Menus	121
Tooltips	122
17. Scatter Plot	123
Default	123
Selection	124
Mini	124
Context Menu	124
Context Sub-Menus	125
Tooltips	127
18. Pie Chart	128
Default	128
Selection	128
Mini	128
Context Menu	129
Context Sub-Menus	129
Tooltips	130
19. Data Grid	131
Grouping Bar	131
Column Headers	132
Filter Bar	132
Hierarchy	133
Selection	133
Context Menu	133
Context Sub-Menus	134
Tooltips	135
20. Channels Button	136
All Channels	138
2.4GHz Center Frequencies:	138
5GHz Center Frequencies:	138
Channel Names	138
All Channels Panel	138
Channel List	139
Selection Controls	139
Search and Filter Bar	140
Locked Channels	140
Title	140
Selection Controls	140
Transfer Controls	141
Channel List	141
Scan Sequence	141
Duration	141
Selection Controls	141
Transfer Controls	142
Channel List	142
21. Decryption	143
Wireless Decryption Keys Manager	143

Adding a Key.....	144
WPA Related Packet Injection.....	145
22. Drill Down	147
How to.....	147
Example.....	147
23. Filter Dialog.....	148
Filter Library	148
Filter Parameters.....	148
24. Search Dialog.....	149
Search Context	149
Search Style	149
Regular Expression Example.....	150
25. Security Disclosures	151
26. Appendix A Chart Types.....	152
27. Appendix B Report Example Breakdown	153
28. Appendix C Example User/Group Configuration File	155

Overview

The purpose of this reference manual is to document and explain each Pilot Console feature. It is assumed that the reader is familiar with networking protocols and the principles of a networking stack. Care has been taken to avoid technical explanations except when necessary for conceptual understanding or functional explanation.

This manual is not meant to be a tutorial on the use of the Pilot Console. The most appropriate (and quickest) way to gain an appreciation of the capabilities of this unique tool is to watch the introductory videos available through the Pilot Console product page at www.cacetechnology.com. For a complete understanding of the combined operations of the Pilot Console and Shark Appliance, and to optimize your facility with our distributed network analysis solution, we recommend that both this manual and the videos be reviewed.

The Shark Distributed Monitoring System

The SDMS has been designed to provide a complete enterprise-wide solution for increased network visibility through live traffic monitoring, full-line-rate data capture, real-time and historical traffic analysis, monitoring, and reporting from multiple locations.

In this section we introduce the Shark Appliance and the Pilot Console. Together, the Pilot Console and Shark Appliance provide a seamless distributed network analysis, visualization, monitoring, recording, and reporting solution.



Figure 1: SDMS Shark Appliances

The Shark Appliance, which houses a data capture and analysis engine along with a custom packet recording utility, extends the reach of our CACE Pilot analyzer to geographically-dispersed network locations. Shark Appliances are designed for placement at strategic points throughout your network, thereby providing the visibility necessary for global monitoring and troubleshooting. The Shark Appliance comes as a fully-configured rack mount PC, and includes one or more TurboCap™ boards for network traffic capture.

The Shark Appliance software also includes the Shark Packet Recorder, a customized packet storage application for high fidelity, multi-gigabit per second data capture.

Shark Appliance Kit

CACE Technologies also offers the Shark Appliance Kit which includes the complete Shark Appliance software and high-performance 1 GigE or 10 GigE TurboCap cards and the user provides the appliance hardware platform.



Figure 2: Pilot Console

The Pilot Console is an expanded version of CACE Pilot that seamlessly and securely interfaces with one or more Shark Appliances to display, drill down into, rewind, alert, and report on, network traffic captured and/or analyzed by Shark Appliances. All the features of the CACE Pilot analysis tool have been migrated to the distributed environment, including large packet trace file access and manipulation, an extensive collection of network traffic analysis metrics (Views), drag and drop drill-down, visualization and analysis of long-duration capture statistics, flexible trigger-alert mechanism, and simplified, professional report generation. Once connected to a Shark Appliance, interaction through the Pilot Console with a remote Shark Appliance appears as if it were local. Remote traffic sources appear as local sources to which Views can be applied. Views computed by Shark Appliances (live or off-line) are sent to the Pilot Console for rendering. The Pilot Console also can access and analyze live traffic on the Console's local interfaces and trace files.

Together, the Pilot Console and Shark Appliance provide a seamless distributed network analysis, visualization, monitoring, recording, and reporting solution.

Figure 3 depicts a representative Shark Distributed Monitoring System deployment with four Shark Appliances and two Pilot Consoles running on laptops.

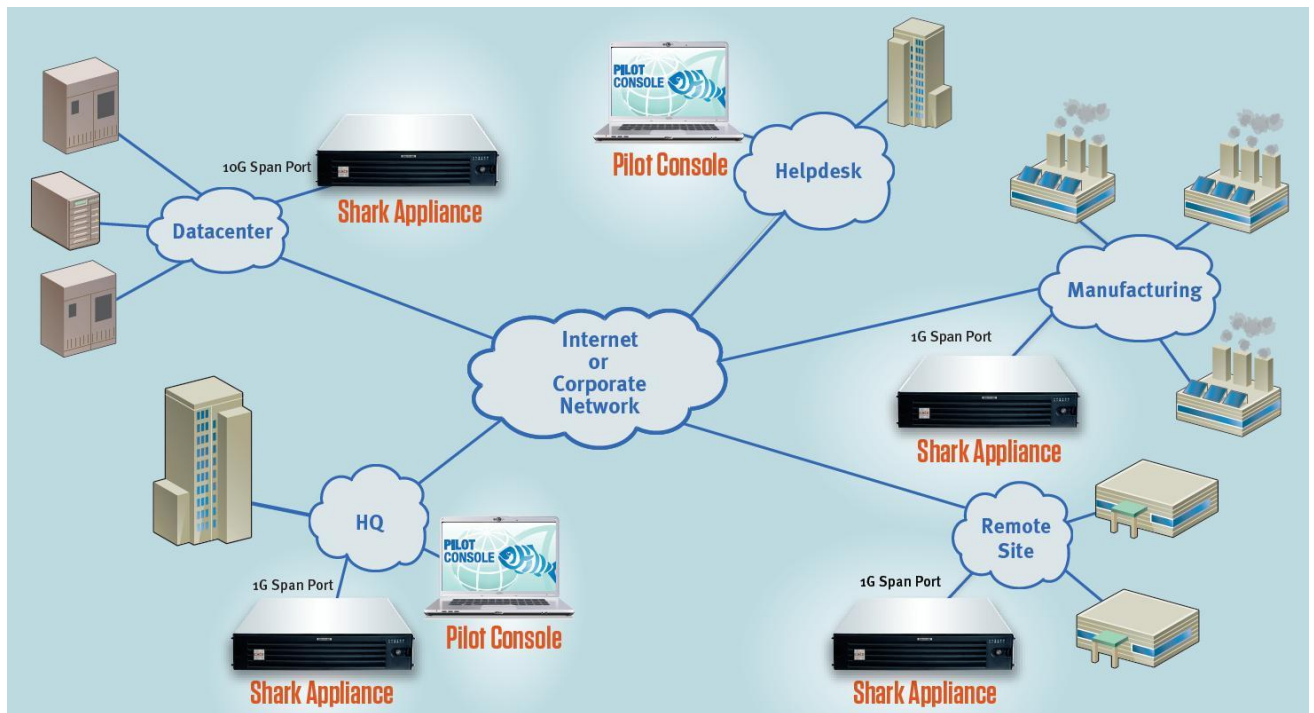


Figure 3: An Example Shark Distributed Monitoring System

Pilot Console – Feature Summary

The Pilot Console, an enhanced version of CACE Pilot for accessing and controlling one or more remote Shark Appliances, includes the following features:

- Graphical user interface for displaying data collected by remote Shark Appliances and local network traffic sources
- Management Interface
- Interface to the Shark Packet Recorder’s Jobs Repository
- Wireshark Integration
- Interactive Views and Charts
- Drill-Down
- Time Control
- Watches
- Report Generation

Graphical User Interface

The Pilot Console can view and analyze network traffic on local interfaces (just like CACE Pilot) and also connect to and manage one or more remote Shark Appliances. When connected to remote Shark Appliances, the Pilot Console can analyze and view traffic from network interfaces of the Shark Appliances as if these remote interfaces were local. All of the features of CACE Pilot work seamlessly in a distributed environment.

A single Pilot Console can simultaneously connect to multiple Shark Appliances, while multiple instances of the Pilot Console can simultaneously connect to the same Shark Appliance. Access to a single Appliance from multiple Console locations can provide excellent visibility into your network as well as an intuitive mechanism for sharing network Views, Watches, and Reports with co-workers and management.

Management Interface

The Pilot Console’s Management Interface provides access to the Shark Appliance configuration manager. The Management Interface supports the following configuration tabs:

- *Appliance Status*. Shows the status of the Shark Appliance and allows for restarting the Appliance, the Shark Probe, and the Shark Packet Recorder
- *Capture Jobs*. Shows the status of all of the current Capture Jobs. This tab is also used for adding/editing/deleting/starting/stopping capture jobs.
- *User Management*. Provides access to users/groups and the ability to add or remove users/groups.
- *Capture Board Setup*. This section is used for configuring the TurboCap board(s) on the Shark Appliance.
- *Port/Protocol Definition*. This section can be used to add new protocol definitions and protocol groups.
- *Logs*. Contain the Shark Probe and the Shark Packet Recorder logs.
- *Shark Probe Configuration*. Contains a basic configuration file for the Shark Probe. Not normally accessed by users.

Interface to the Shark Packet Recorder’s Jobs Repository

The packet storage associated with a Capture Job is called a *Job Trace*. Each Job Trace is shown in the *Jobs Repository* folder of the Files panel. Depending upon how the Capture Job is configured and the speed of the network, the corresponding Job Trace can be a very large, multi- terabyte file. Using the “Trace Clip” creation feature of the Pilot Console, you can have ready access to arbitrary time intervals within a Job Trace. Trace Clip time intervals, their location in time, and their size can be controlled easily. All Pilot Console operations that apply to trace files can be applied to Trace Clips as well.

Wireshark Integration

The Pilot Console and the Shark Appliance are fully integrated with Wireshark, allowing you to leverage your team's existing expertise with the world's most popular and widely-deployed network and protocol analysis tool. At any point of operation, the Pilot Console can select a local or remote traffic source and send it to Wireshark for packet filtering or deep packet inspection.

Interactive Views and Charts

Views are the core analysis and visualization paradigm in the Shark Distributed Monitoring System. The Shark Distributed Monitoring System offers approximately 200 Views providing a broad range of protocol support for both wireless¹ and wired network analysis. The results of applied Views are displayed via a collection of interactive components called Charts. The collection of Charts includes bar, pie, and strip charts, scatter plots, conversation rings, and grids. Charts are interactive – they can be resized, moved, and, most importantly, users can make visual selections on graphical elements within a Chart, such as selecting individual bars within a bar chart or time intervals within a strip chart and drilling down from there. Charts can be customized, saved, exported, imported, and shared with colleagues. Chart data can be exported in a variety of formats and can be included in the Pilot Console's automated report generator.

Drill-Down

Drill-Down is one of the most powerful and unique features of the Shark Distributed Monitoring System. When you apply a View to a packet data source, a Chart is displayed, revealing the network traffic results specified by the chosen View. Drill-Down occurs when you then apply additional View selections to a Charted display. This simple yet powerful exercise increases your analysis capabilities many-fold. By employing this visually-based Drill-Down feature, the Shark Distributed Monitoring System can analyze very large trace files, quickly guiding you to the handful of packets responsible for anomalous network behavior, for example.

Time Control

Viewing metrics computed over days, weeks, and months can be overwhelming. With the Shark Distributed Monitoring System's "back-in-time" technology, however, you can move through View metrics computed over extended periods of time with just a few mouse clicks. Based on your selected time interval, sub-sampling and aggregation techniques are used to optimize the granularity of the visual presentation, allowing you to easily zoom in and out of the View metrics. The SDMS Time Control technology applies to live and off-line traffic.

Watches

The Shark Distributed Monitoring System includes a sophisticated triggering and alerting technology called Watches. With Watches, you are able to create a trigger on many View metrics and be alerted when a specified condition computed on a metric is met. For instance, you can be alerted when unusually-high bandwidth utilization, slow server response times, high TCP round-trip times, and other conditions happen. When a Watch detects that a trigger condition is met, a specified action is taken. Possible actions include event logging, sending email, sending a Twitter message, starting a packet trace capture, and more.

Report Generation

Customized reports can be automatically generated to show elements such as:

- Conversations (at any or all network layers)

¹ Live wireless analysis only applies to locally attached AirPcap traffic sources.

- IP Fragmentation Analysis
- DHCP Address Assignments
- TCP Top Talkers
- Unicast vs. Multicast vs. Broadcast Traffic

And much more. In fact, hundreds of easy-to-use Charts can be scoped and limited to any requested format condition. Charts can be combined in a single report or recreated in separate reports in one or more formats with just a click of the mouse. Supported formats include:

- PDF
- Microsoft Excel
- Microsoft Word
- HTML

All relevant trace files and their MD5 digests can be automatically packaged in a ZIP file along with the generated reports for easy distribution.

Hardware and Software Requirements for Pilot Consoles

The Pilot Console is available on Windows platforms including XP and Vista. Although the system requirements for a Pilot Console scale with usage, in order to use the Pilot Console effectively, the following minimum configuration is recommended:

[Operating System](#)

Windows XP, Windows Vista, Windows 7

[Host Hardware](#)

A dual-core 2.0 GHz CPU or better

[Available Disk Space](#)

A base install requires approximately 300MB of disk space. Additional space is required to store generated reports or trace files created with the Pilot Console.

[Memory](#)

2 GB or more of system memory

[Video Hardware and Settings](#)

A graphics card with a minimum resolution of 1024 x 768

Graphical User Interface

Graphical User Interface Components



Figure 4: User Interface Breakdown (Major)

The graphical user interface of the Pilot Console, broken up into the five main sections, is shown in Figure 4. Each section represents a major topic of this manual. The descriptions below are conceptual overviews of each section.

Ribbon Panel

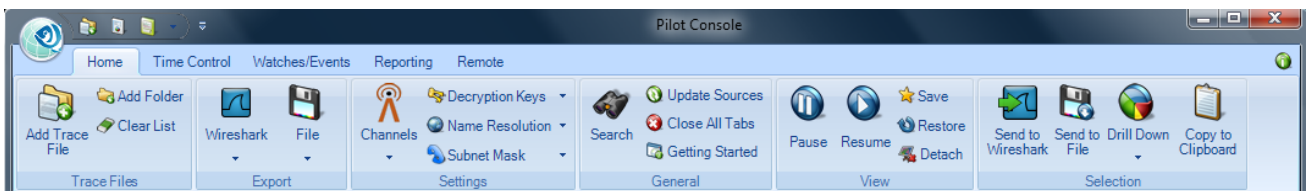


Figure 5 Ribbon Panel

The *Ribbon Panel* provides access to global settings, management, and general actions. There are five ribbon panels (Home, Time Control, Watches/Events, Reporting, and Remote) that can be tabbed through using the mouse wheel.

Sources Panel

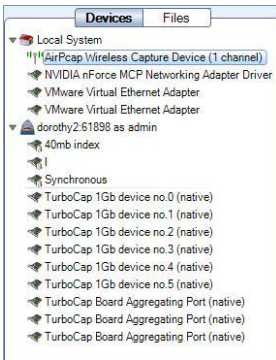


Figure 6: Shark Appliances, Devices, and Files Panel

The *Sources Panel* contains representations of Shark Appliances, interfaces, and trace files and is one of the most important parts of the Pilot Console. It has two tabs, “Devices” and “Files”. These can be cycled through by clicking on them. The meaning of each is the following:

Devices

The Devices tab contains local interfaces under the Local System icon and Shark Appliances with their associated interface offering live sources of network traffic to the Pilot Console.

Files

The Local System with local folders and trace files plus the Shark Appliances with their associated folders and trace files.

Views Library

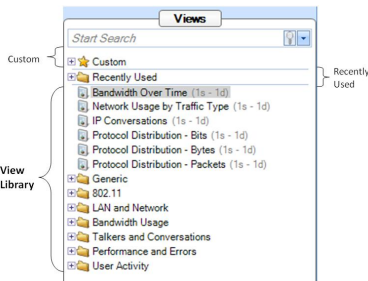


Figure 7: Views Panel

The Views section contains a library of network traffic analyses called “views”. Each View computes a specific metric, such as bandwidth over time, IP conversations, protocol distributions, etc. from either a live or off-line source of network traffic and displays the results in the form of Charts (strip charts, bar charts, grids, etc.).

Views are both general and specific with varying levels of customization available.

Main Workspace



Figure 8 Main Workspace

The Main Workspace has tabbed windows which can be one of the following:

- Views
- Report Preview for the Report Designer
- Getting Started Tab

The windows can be moved by dragging them and can be closed either by clicking on the icon on the left-hand side of the tab name or middle-clicking on the tab itself.

A View tab is shown in the Figure.

Events Panel

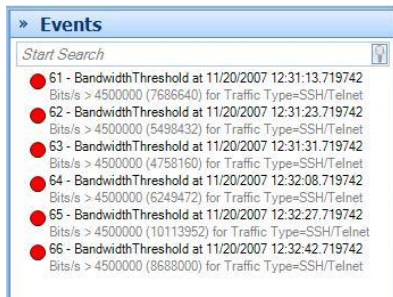


Figure 9: Events Panel

The *Events Panel* contains entries corresponding to both internal and external events. Internal events are generated by “Watches” and external events are generated by external sources.

Menu Button and Status Bar

There are two minor parts of the user interface:

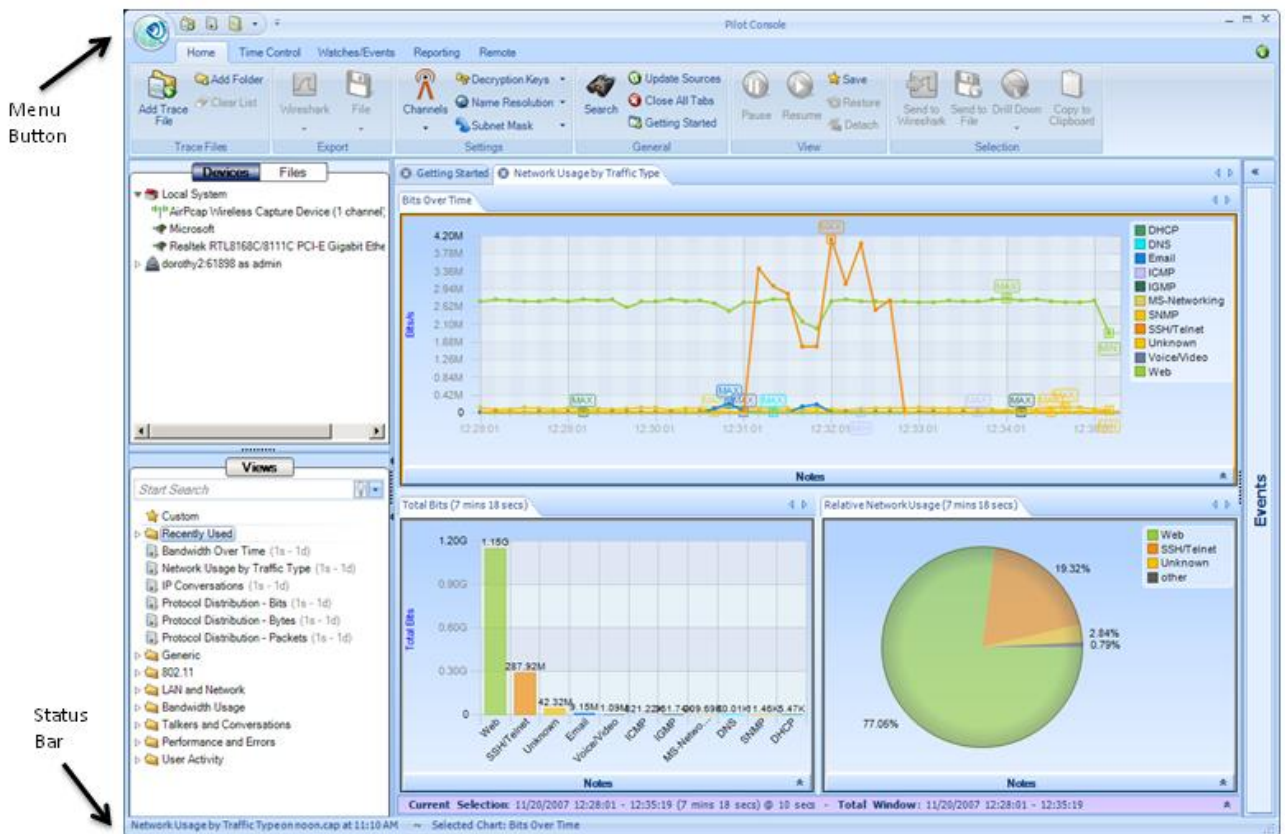


Figure 10 User Interface Breakdown (Minor)

Menu Button

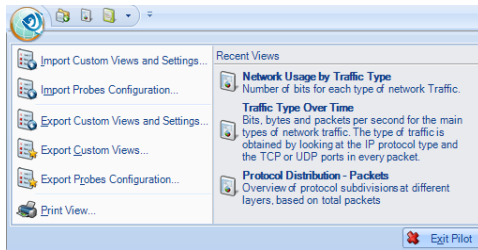


Figure 11 Menu Button

The *Menu Button* has the following components:

Import Custom Views and Settings...

The *Import Custom Views and Settings...* menu option will open a file created by one of the two export menu options described below and apply it to the Pilot Console. This applies to all settings in the global configuration file, which are enumerated throughout this manual. Briefly, it entails items such as

- Remote Shark Appliances and probe groups
- Custom views
- Report settings
- Channel scan sequence
- Decryption keys

Additionally, the custom views from the exported configuration are imported and loaded in the custom views section of the Views panel.

Export Custom Views and Settings...

The *Export Custom Views and Settings...* menu option prepares a file that can be imported into another instance of the Pilot Console. This file contains the global configuration file, whose settings are enumerated throughout this manual.

Export Custom Views...

The *Export Custom Views...* menu option prepares a file that can be imported into another instance of the Pilot Console that contains only the custom views.

Print View...

The *Print View...* creates a default report from the current view and sends it to the printer. The report is not saved to disk.

Recent Views

The *Recent Views* section lists the five most recently applied views and their descriptions. Views can be selected from here and will be applied to the currently selected device or file, as described below in the section “Applying a View”.

Status Bar

Figure 12: Status Bar

The *Status Bar* lists the last operation that was done such as applying a view to a device. During certain operations, the status bar also includes a graphical horizontal bar on its right hand side that displays the percentage completion of an operation.

Home Ribbon

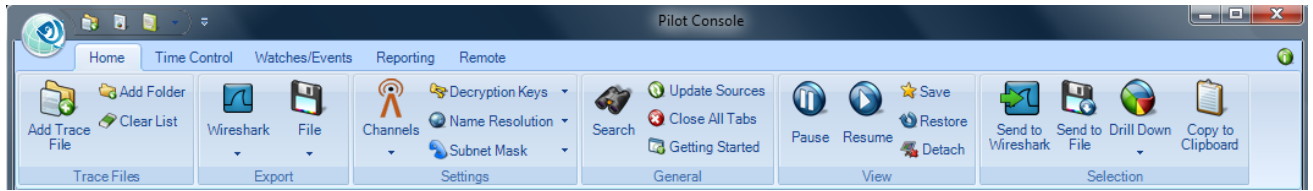


Figure 13: Home Ribbon

The *Home Ribbon* serves as the primary interface to the Pilot Console. Most operations can be executed via this ribbon. Certain parts of the ribbon are disabled by default. This is to be expected, as will be explained below. The sections of the ribbon are broken down going left-to-right, top-to-bottom. The sections of the ribbon going left-to-right are:

- *Trace Files*. Includes operations such as adding a link to a trace file in the Sources panel
- *Export*. Used to export traffic sources (either live or off-line) to Wireshark or to a trace file
- *Settings*. Wireless channel and decryption settings, name resolution, and subnet mask
- *General*. Miscellaneous actions.
- *View*. Buttons to Pause/Resume live analyses. Saving custom views and detaching from a view
- *Selection*. Drill down steps including Send to Wireshark/File

Note: To close any submenu of the ribbon, such as the Decryption Keys or Channel Selector, simply click the button again or somewhere outside of the submenu and it will close. Furthermore, all changes take place immediately hence there is no need for confirmation buttons.

Trace Files

In this section we describe the functionality of the Trace Files section of the Home Ribbon.

Note: The source and destination of “Add Trace File” and “Add Folder” are local to the Pilot Console.

Add Trace File



Icon 1 Add Trace File

The *Add Trace File* button adds a trace file to the Files panel for analysis. This operation only adds a reference to the file and is not a copy operation. If the file moves on disk, the reference will be no longer valid.

Add Folder



Icon 2 Add Trace Folder

The *Add Folder* button adds a directory of trace files to the Files panel for analysis. The selected folder is scanned for all supported trace files. Similar to the add trace file operation, this operation adds a reference to the folder and relevant files and does not copy anything on disk.

This operation is not recursive and does not add subfolders.

Clear List



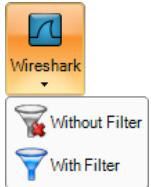
Icon 3 Clear List

The *Clear List* button clears the list of trace files and folders in the Files panel.

Export

The *Export* section lists the functions that will export data out of the Pilot Console either through Wireshark or a PCAP formatted trace file.

Wireshark



Submenu 1 Send to Wireshark

The *Wireshark* button sends traffic from the selected device or file to Wireshark. Note that this is a two click operation.

Note: If the source of traffic is on a remote probe, then the traffic (live or off-line) will be transmitted over the network to Wireshark running on the Pilot Console's local system.

The first click opens a submenu with two options:

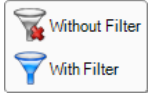
Without Filter

The *Without Filter* menu option sends all traffic from the selected device or trace file to Wireshark. In the case of a device, Wireshark will present, by default, a live scrolling capture. The default behavior can be changed by editing the *Wireshark* preferences.

With Filter

The *With Filter* menu option opens up a filter selection dialog (explained later) to filter the traffic to be sent to Wireshark.

File



Submenu 2 Send to File

The *File* button sends traffic from the selected device or file to a new trace file. Note that this is a two click operation.

Note: If the source of traffic is on a remote probe, then the traffic (live or off-line) will be saved in the “My Files” directory on the remote probe. If the source of traffic is the Pilot Console, then the traffic will be saved as a PCAP file located on the Pilot Console.

The first click opens a submenu with two options:

Without Filter

The *Without Filter* button sends all traffic from the selected device or trace file and places it in a trace file of a specified name.

With Filter

The *With Filter* button opens up a filter selection dialog (explained later) to filter the traffic to be sent to a new trace file of a specified name.

After a trace file is created, it is immediately available in the Files panel of the *Device and Files Panel*.

Settings

The *Settings* section contains global settings that are immediately applicable to all open views and their charts.

Channels



Icon 4 Channel Selector

The *Channel Selector* button opens up a submenu that allows for the management of the set and duration of channels to scan or lock. This interface is a large topic and is explained in its own section later on – Channels Button.

Note: This operation only applies to AirPcap adapters installed on the Pilot Console’s host system.

Decryption Keys



Icon 5 Wireless Decryption Key Manager

The *Wireless Decryption Key Manager* button opens a submenu that allows for the management of the list of keys to decode encrypted wireless traffic. This interface is explained in Decryption.

Note: Decryption is available for live AirPcap traffic sources on the Local Pilot Console and on wireless trace files located on the Local System or remote probes.

Name Resolution



Icon 6 Name Resolution



Submenu 3 Name Resolution

The *Name Resolution* button opens a submenu that allows for the specification of whether certain things should be resolved automatically in a chart. The button gives a submenu with three modal options:

MAC Addresses

When the *Mac Addresses* check box is checked, a passive file-based lookup is done that converts the leftmost 3 bytes of a MAC address to its respective organization (OUI).

IP Address

When the *IP Addresses* check box is checked, an active DNS lookup is done to resolve IP Addresses to domain names.

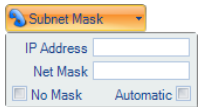
TCP and UDP Ports

When the *TCP and UDP Ports* check box is checked, a passive lookup is done to convert TCP and UDP port numbers into their well-known service names. This is simply a table lookup in a known hosts file and does not do any form of service fingerprint matching.

Sub Net Mask



Icon 7 Sub Net Mask



Submenu 4 Sub Net Mask

The *Sub Net Mask* button opens a submenu allowing for specification of a global sub net mask to all applicable views and functions as a quick way to discard unwanted traffic. A View's tooltip indicates whether the net mask is applicable to that view.

Note: Setting the subnet mask with a remote probe selected will cause the subnet mask to be set in the remote probe. In this way, by selecting remote probes one at a time, a unique subnet mask can be set in each remote probe.

The submenu contains two input boxes and two check boxes:

IP Address

The *IP Address* edit box is used to specify IPv4 address using dot-decimal notation such as 192.168.0.100. The IP address doesn't need to be an actual address currently assigned. It is simply guidance for the filter.

Net Mask

The *Net Mask* edit box is used to specify an IPv4 net mask address such as 255.255.255.0. Together, the IP Address and sub net mask form a CIDR address block. For instance, in the above example, with a net mask of 255.255.255.0 and an IP Address of 192.168.1.100, the CIDR address block would be 192.168.1.0/24.

No Mask

The *No Mask* check box disables the sub net mask entirely.

Automatic

The *Automatic* check box enables heuristic checks that derive sub net mask values from IP level traffic analysis.

General

The *General* section contains buttons that apply to all devices and tabs.

Search



Icon 8 Search

The *Search* button opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section. See Search Dialog.

Update Sources



Icon 9 Update Sources

The *Update Sources* button updates the list of sources for the Devices and Files Panels. Please note that a device will not be available immediately after it is plugged in, nor will the device disappear immediately after being unplugged. It takes about 10 seconds before the Pilot Console recognizes a change of device. Furthermore, the Pilot Console does not check for new adapters automatically and only checks when this button is clicked.

Close All Tabs



Icon 10 Close All Tabs

The *Close All Tabs* button closes all open tabs. This applies to the following tabs:

- Views
- Report designer
- Getting started

Getting Started



Figure 14 Getting Started

The *Getting Started* button opens a tab in the main workspace that provides:

- Access to video tutorials

View

The *View* section has buttons used for view management.

Pause



Icon 11 Pause Live Capture

The *Pause Live Capture* button pauses processing on the current view and charts. This button is only enabled in a live capture. The network traffic continues to be processed while the View is paused and will be available when the Resume button is clicked.

Resume



Icon 12 Resume Live Capture

The *Resume Live Capture* button resumes “viewing” the live metrics on the current view and charts. This button is only enabled in a “paused” live capture.

Save



Icon 13 Save
Custom View

The *Save* button saves the current view as a custom view.

Restore



Icon 14 Restore
Default View

The *Restore* button restores default view settings.

Detach



Icon 15 Detach

The *Detach* button detaches the currently selected View from the source, whether the source is live/off-line or local/remote. Once detached, the View is no longer visible in the Pilot Console main workspace. The View is still visible in the sources panel, but grayed out.

Note: For live captures, the system (local or remote) continues to compute the corresponding View metric.

We can “attach” to the View by right-clicking on the View in the sources panel and selecting the Attach submenu item, thereby making the View visible in the Pilot Console’s main workspace.

Selection

There are some common functions amongst the charts which are only enabled if there is an active selection in a chart. These functions are on the Home ribbon in the Selection group. Each of these functionalities is also available through the context menu of any chart.

Send to Wireshark



Icon 16 Send to
Wireshark

The *Send to Wireshark* button sends traffic from the current selection to Wireshark by spawning a new instance of Wireshark and delivering the selected packets to Wireshark.

Note: If the source of traffic is on a remote probe, then the traffic (live or off-line) will be transmitted over the network to Wireshark running on the Pilot Console’s local system.

Send to Trace File



Icon 17 Send to File

The *Send to File* button sends traffic from the current selection and stores it as a trace file. This is useful for storing a subset of the original capture. If the traffic was encrypted and is being properly decrypted at the time, then the trace file will store the decrypted traffic.

Note: If the source of traffic is on a remote probe, then the traffic (live or off-line) will be saved in the “My Files” directory on the remote probe. If the source of traffic is the Pilot Console, then the traffic will be saved as a PCAP file located on the Pilot Console.

Drill Down



Icon 18 Drill Down

The *Drill Down* button applies a view to the current selection in a chart. This is an important and powerful feature of the Pilot Console and is explained in its own section. See the chapter on Drill Down.

Copy to Clipboard



Icon 19 Copy to Clipboard

The *Copy to Clipboard* button copies textual representation of the chart information of the current selection to the clipboard for exporting to another application.

Time Control Ribbon

The Time Control feature of the Pilot Console allows the user to go “back in time” over a View that has been computed over days, weeks, or months and applies to Views computed over live and off-line sources. Based on the View and the selected time interval, subsampling and aggregation techniques are used to optimize the granularity of the visual presentation of the View metrics.

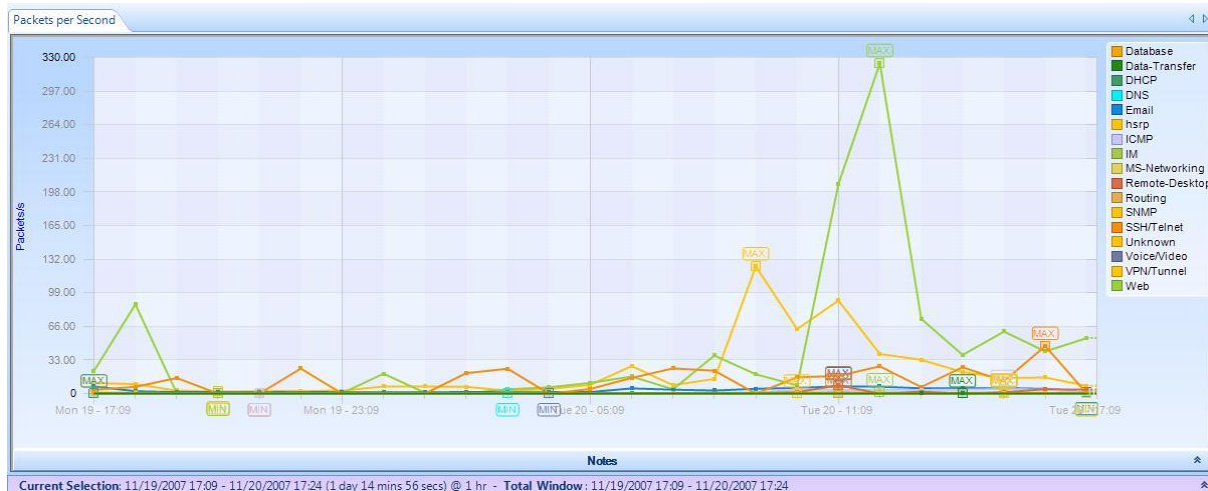


Figure 15 Traffic Type Over Time Showing Time Selection Windows

Figure 15 shows the Traffic Type Over Time View applied to a trace file. The purple bar just below the strip chart is called *Time Controller*. It has two fields, *Current Selection* and the *Total Window*.

The *Total Window* indicates beginning the end time and date of the trace file.

The *Current Selection* is the interval of time displayed in the Charts above the *Time Controller*. The *Time Controller* shows the following information about the Current Selection: beginning date, beginning time, end date, end time, duration (in parenthesis) and sampling time (after the @). The Current Selection can be adjusted as explained later in this chapter, so that the temporal interval can be shorter than the Time Window. Sometimes the captured interval is too large to be displayed in a single Strip Chart at the sample rate indicated in the view metrics (e.g. several days of traffic with 1-second sample rate). In these cases Pilot automatically aggregates displayed data, subsampling the trace file and displaying traffic with a lower granularity. Higher resolution is still available when you zoom in to analyze shorter time intervals. The Pilot Console analysis engine (local or remote Shark Appliance) automatically selects the best level of subsampling based on the duration of the Current Selection.

In Figure 16 we have “zoomed-in” on the View so that the Current Selection interval is shorter and thus the sampling rate is smaller. The change in resolution is handled automatically in the Pilot Console, thereby making it very easy to move around and to zoom in and out of very long-duration trace files and live captures.



Figure 16 Traffic Type Over Time with Multi-Level Zoom Selection

In Figure 17 we show the Time Control Bars in more detail. The bottom bar is called *Time Scroll Bar* and it represents the entire trace file or live capture. The *Time Window* depicts an interval of time within the overall trace file or live capture. The Time Window element within the Time Scroll Bar can be resized and moved throughout the file and it is used only to affect what is visible on the upper bar. The upper bar represents a magnified view of the Time Window and any change to the size and position of the *Current Selection* on it affects what is visible in the View Charts. Indeed, the *Current Selection* is the time interval within the trace file or live capture that we are actually seeing in the View.

It is possible to change the position and size of the two bars as follows:

- using buttons within the Time Control Ribbon to move the Current Selection and change the Current Selection duration
- dragging the Current Selection element or its endpoints
- clicking and dragging just above the expanded Time Window to create a new Current Selection
- double-clicking on the Current Selection to expand the Current Selection to the complete View history (double-clicking again will return the Current Selection to its previous location)

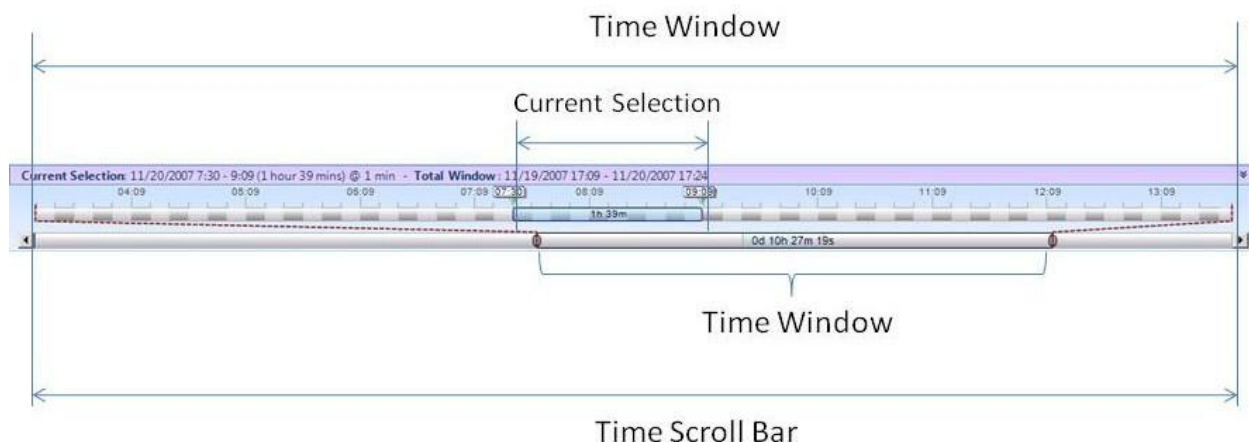


Figure 17 Time Control Bars

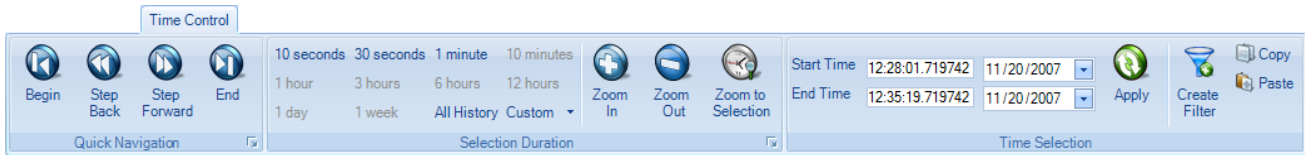


Figure 18 Time Control Ribbon

As we have seen, the Time Control feature of the Pilot Console allows the user to go “back in time” over a View that has been computed over days, weeks, or months. The Time Control Ribbon provides additional mechanisms for moving through a long-duration View. There are three sections within the Time Control Ribbon: Quick Navigation, Selection Duration, and Time Selection. These are described next.

Quick Navigation

Begin



The *Begin* button allows a user to move the Current Selection interval to the beginning of the View (back-in-time).

Step Back



The Step Back button allows the user to move the Current Selection interval one step back in time where the size of the step is equal to the length of the Current Selection interval.

Step Forward



The Step Forward button allows the user to move the Current Selection interval one step forward in time where the size of the step is equal to the length of the Current Selection interval.

End



The End button allows the user to move the Current Selection interval to the end of the current View.

Selection Duration

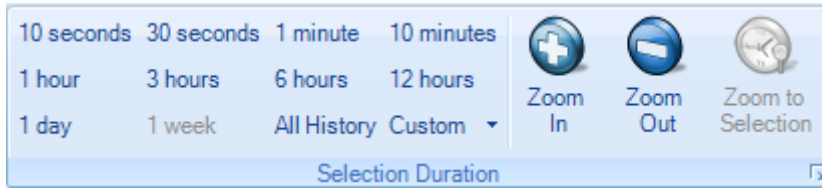


Figure 19 Selection Duration Section of the Time Control Ribbon

The Selection Duration section of the Time Control ribbon provides a number of alternatives for setting the length of the Current Selection interval. Recall that the Current Selection interval corresponds to the portion of the View metric that is displayed in the Charts that make up a View. For example, if the Chart is a strip chart, then the duration of the visible portion of the strip chart is precisely the Current Selection interval. For other charts, the visible portion of the Chart shows the View metric computed of the span of time equal to the Current Selection interval. For example, if the Chart is a conversation ring, then the conversation ring shows the host conversations that have taken place during the Current Selection interval.

The Selection Duration section contains some fixed durations to choose from such as 10 seconds, 10 minutes, etc. An All History choice is available too. For a trace file, the All History selection corresponds to the duration of the entire trace file. For a live capture, All History corresponds to going back in time from the present time to the beginning of the capture or an amount of time equal to the Data Retention Time, whichever is smaller. There is also a Custom setting option.

Finally, there are Zoom In, Zoom Out, and Zoom to Selection options. Clicking on the Zoom In button reduces the Current Selection interval by 66%. Clicking on the Zoom Out button increases the duration of the Selection interval to 150% of its current duration. If a time duration selection is made in a Strip Chart, the Zoom to Selection button will change the Current Selection interval to the selection made on the Strip Chart.

Time Selection

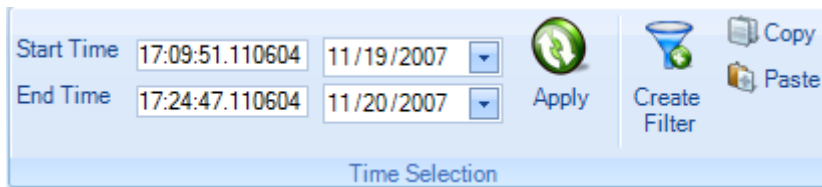


Figure 20 Time Selection Section of the Time Control Ribbon

The *Time Selection* section of the Time Control ribbon allows the user to pick the absolute location and duration of the Current Selection interval within the current View (either live or off-line) – set the *Start Time*, the *End Time*, and then click on *Apply*.

Create Filter: When the user clicks on the Create Filter button a new Filter is created that will filter out all packets that do not fall within the Current Selection interval. This filter can be used when applying a new View to a source and will filter out all packets that do not fall within the Current Selection interval. This is very useful in comparing two different Views with respect to the same time interval. For example, Bandwidth Over Time and IP Conversations during the same interval to see which hosts were talking during a spike in bandwidth.

Copy: Copies the Current Selection interval to the clipboard.

Paste: Changes to Current Selection interval to the interval contain on the clipboard. (the destination Chart must be selected to paste an interval on it)

Watches and Events Ribbon

A Watch consists of a Trigger Condition and one or more associated Actions. The idea is that every time the Trigger Condition is satisfied, then the associated Actions are “executed.”

A Watch is always associated with a particular Chart contained in a View and the trigger condition is based on the metric computing within the Chart. The View itself is applied to a source which can be either live or off-line. The source can be either on the local system or a remote Shark Appliance.

Note: The Trigger Condition is checked at the underlying Sampling Time intervals, even if the chart is showing sub-sampled or aggregated data for larger intervals.

For example, suppose that the View is Bandwidth Over Time with a Sampling Time of one second and the selected Chart within the View is Packet Bandwidth Over Time. This means that for every second, packets-per-second is computed over the packets that arrived during the previous Sampling Time – this is the quantity shown in the Chart. If a Watch were associated with this Chart, then the Trigger Condition would be checked every second using the computed packets-per-second.

In the following sections we show how Watches are created for Strip Charts and Bar Charts.

Note: Watches can only be applied to Strip Charts and Single Bar Charts.

Creating Watches on Strip Charts and Bar Charts

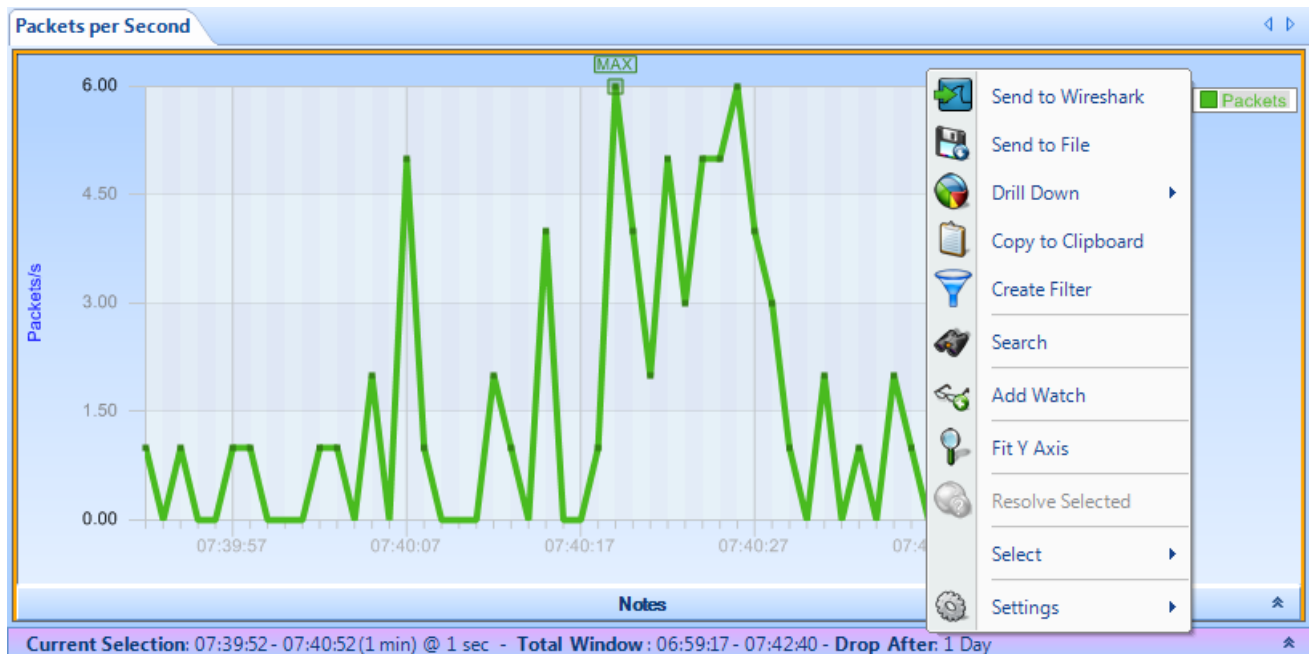


Figure 21 Strip Chart with Context Menu

In Figure 21 we show the context menu associated with the Packets per Second strip chart within the Bandwidth Over Time View. Right clicking in the Packets per Second chart brings up the context menu. The *Add Watch* submenu item brings up the Watch Editor panel (Figure 25) which can be used to create a Watch on the metric (Packets per Second) associated with the selected chart.

We set up the Watch by completing the necessary items in the Watch Editor panel (see Figure 25). Clicking on “OK” in the Watch Editor panel will cause the Watch to be associated with the View. The Watch will appear in the Sources panel under the View.

Watch in Sources Panel

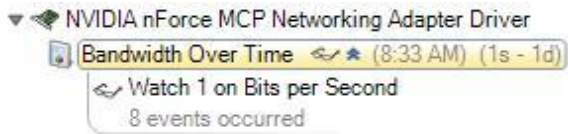


Figure 22 Watch in Device Sources Panel

The Watch appears below its associated View in the sources panel. In this case the View has been applied to a live source. Watches can also be applied to trace files. The small arrows beside the watch icon are used to hide or show the list of watches.

Context Menu for Watch Applied to a Live Source

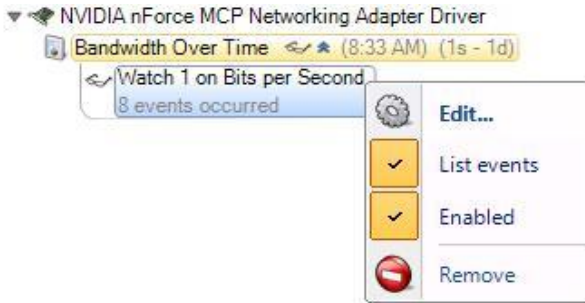


Figure 23:Context Menu For Watch Applied to Live Source

The context menu for a Watch associated with a live source contains the following menu items:

- *Edit*. This menu item brings up the Watch Editor Panel
- *List events*. Lists/Does Not List the events associated with the Watch in the Events panel
- *Enabled*. Enables/Disables the Watch
- *Remove*. The Watch is removed and all of the associated Events are removed from the Events panel

Context Menu for Watch Applied to a Trace File

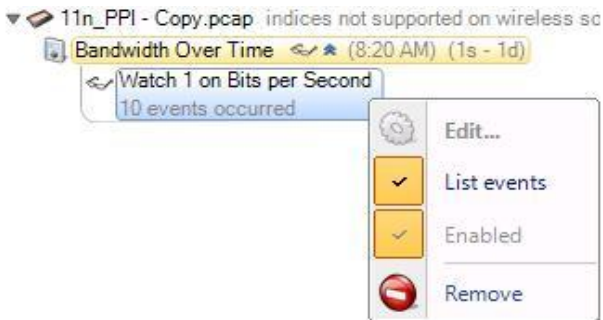


Figure 24:Context Menu for Watch Applied to a Trace File

A Watch applied to a trace file cannot be edited, enabled, or disabled.

The Watch Editor

In Figure 25 Watch Editor Panel we show the Watch Editor. The following section will elaborate on the fields in the Watch Editor panel.

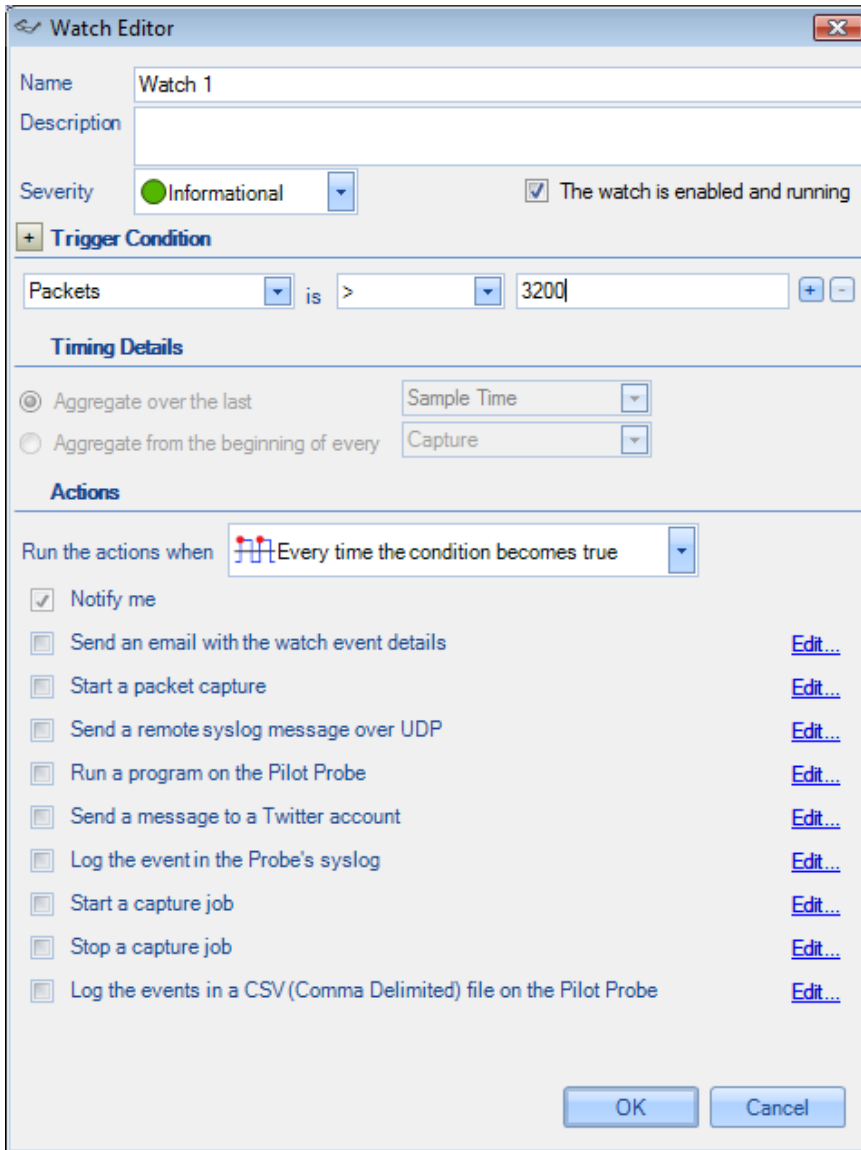


Figure 25 Watch Editor Panel

Name and Description

The *Name* field is used to assign a name to the Watch and the *Description* field is used to provide specific details regarding the Watch.

Severity

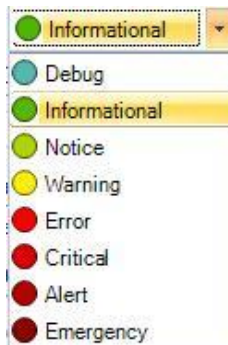


Figure 26 Watch Severity

The *Severity* field contains a drop-down list (see Figure 26) with a number of different “severity” levels. These levels are mainly used to distinguish events (actions) from one another and can be used when searching for specific events.

Enabled

When *The Watch is Enabled and Running* checkbox is checked, the Watch, once it is created, is immediately active. Otherwise, if the box is not checked, the Watch can be created but the Trigger Condition will not be activated until the Watch is enabled.

Trigger Conditions

The Trigger Condition elements are shown in Figure 27 and together they represent a Boolean condition, that is, an expression that evaluates to either True or False.

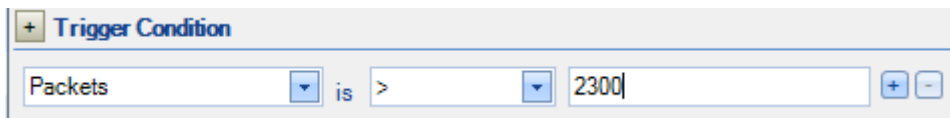


Figure 27 Trigger Condition

The leftmost box contains the value to be tested. Recall that in Figure 21 the Packets (per second) strip chart was selected when the New Watch submenu item was selected. This accounts for the Packets value in the left-most box. The middle box is a drop-down list that contains relational operators that can be selected (see Figure 28 for the list of operators).

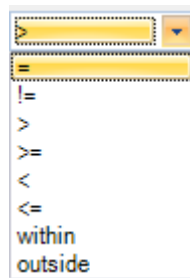


Figure 28 Relational Operators

Finally, there is the rightmost box which contains the comparison value. The Trigger Condition in the example shown in Figure 27 is True whenever Packets is greater than 2,300.

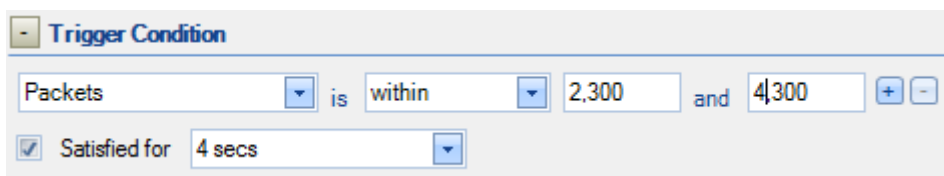


Figure 29 Trigger Condition Expanded

Figure 29 shows the “within” condition and what you get when the Trigger Condition is expanded. The “within” condition requires two values, namely, lower and upper limits in that order. This is also true for the “outside” condition. In the case of the “within” condition, the Trigger Condition is True whenever the value (Packets per second) is less than or equal to the upper limit and greater than or equal to the lower limit.

Expanded Trigger Condition

Expanding the Trigger Condition reveals the “Satisfied for” check box. When the box is checked, then the Trigger Condition becomes the conjunction of the underlying relational expression and the “Satisfied for” condition, that is, both must be True for the Trigger Condition to be True. In the above example (Figure 29), the “Satisfied for” condition is true whenever the underlying relational expression is true for 4 consecutive seconds. If the Sampling Time is 1 second, then the Trigger Condition is true if the underlying relational expression (Packets is within 2,300 and 4,300 for 4 consecutive seconds).

The Expanded Trigger Condition is very useful when we only want to react to a condition if that condition is true for at least a minimum amount of time, in this case 4 seconds.

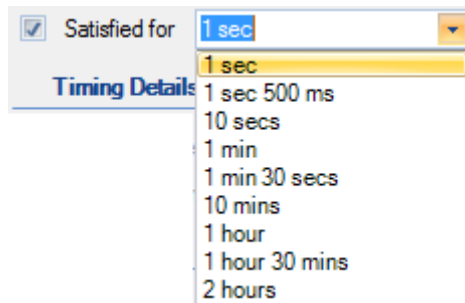


Figure 30 Sample Choices for Satisfied for

In the above figure we show the contents of the drop-down box for the choice of durations for “Satisfied for.” The duration can be selected from this list or created from scratch using the formats shown in the list.

Multi-Line Strip Charts

In the case of a single line strip chart as in Figure 21, The Trigger Condition is evaluated every Sample Time on the single value computed at each sample point. But what happens with multi-line strip charts where multiple values are computed at each Sample Time? There are two cases: 1. Multiple characteristics are computed for each packet, or 2. the packets are partitioned into multiple categories and a single metric is computed for the packets in each category.

Single value, multiple packet types

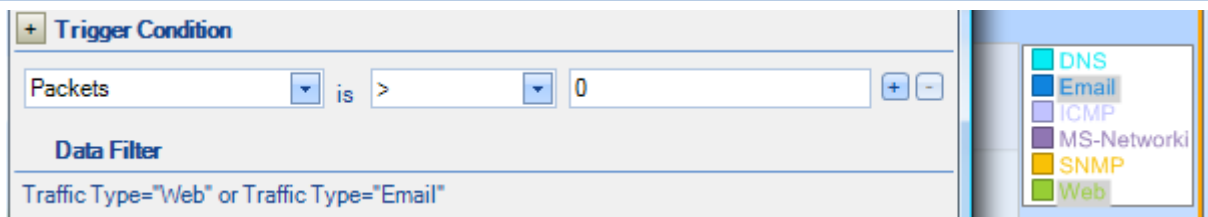


Figure 31 Multi-Line Strip Chart with Filtering

Figure 31 depicts the case where the multi-line strip chart shows Traffic Type Over Time. Each packet is examined and partitioned according to its packet type and the bandwidth per second is computed for each packet type. In general, a Watch on this strip chart would check the Trigger Condition for each traffic type for each Sample Time and generate an event for each traffic type for which the Trigger Condition is met. This means that there could be as many events generated at each Sample Time as there are traffic types. If a line selection is made before the Watch is created, Data Filter field will show the set of lines for which the packet bandwidth will be calculated. In Figure 31 we show that two lines, Email and Web, have been selected. The Watch Editor acknowledges the line selection under the Data Filter section which automatically appears.

Multiple values, single packet type

Figure 33 shows another type of multi-line strip chart. This example comes from the Frame Size Over Time View in the Generic folder. In this case, the Average, Max, and Min frame sizes are computed for *each* packet – there are three different values associated with each packet and the lines in the strip chart represent these values. Now different lines are represented as different “values” in the left-hand-side of the Trigger Condition relational expression.

Timing Details for Bar Charts

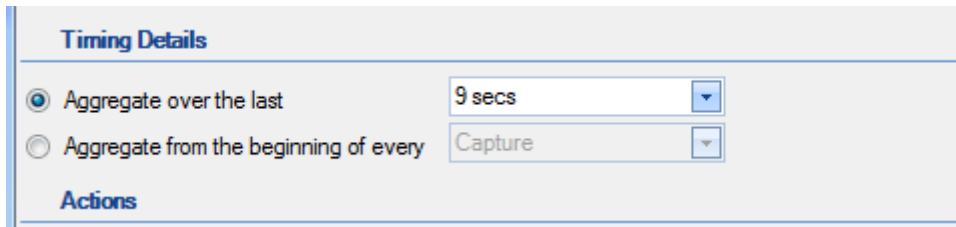


Figure 32 Timing Details

The section called “Timing Details” applies to aggregating charts such as Bar Charts. Strip Charts are not aggregating charts and therefore the Timing Details section is grayed out for strip charts.

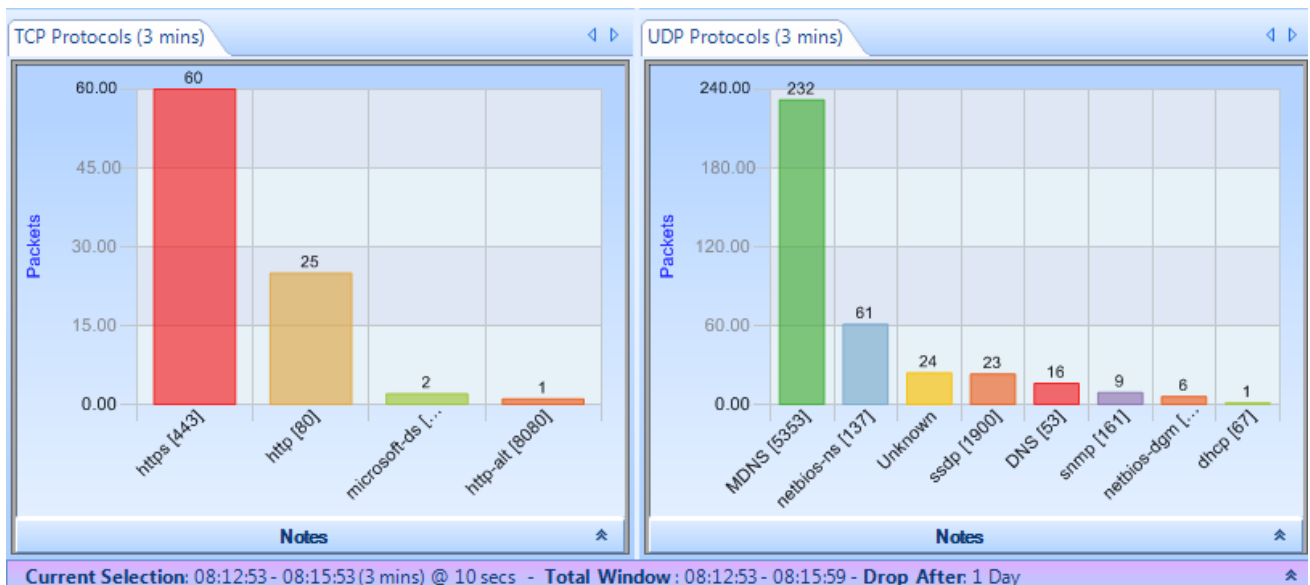


Figure 33 Aggregating Chart

The Current Selection interval in Figure 33 is equal to 3 minutes. The bar chart on the left partitions the incoming packets according to the TCP protocol and counts the number of packets for each protocol. For example, in the left-most chart, there are 60 packets carrying the https protocol. But there is more to the story. The Current Selection interval is 3 minutes which means that the bars are the sums seen over a 3-minute intervals. In the case of the above chart, the interval is from 08:12:53-08:15:53. The aggregation interval for the bar chart is, for convenience, also show in the chart’s tab.

Note: It is important to point out that the Timing Details lets us set an aggregation interval for the Watch that is independent of the aggregation associated with the Current Selection interval.

In setting up a Watch for an aggregating chart it is important to specify the interval over which the aggregation takes place. There are two radio buttons in the Timing Details section, and one or the other must be selected. The first one specifies the aggregation back in time from the current time. At each Sampling Time, the value of each bar is determined by aggregating over the aggregation interval specified. The aggregation intervals are overlapping.

The second radio button is for specifying non overlapping aggregation intervals. Suppose we wanted to aggregate the total packets over every hour for each TCP protocol. For each hour we would begin a new aggregation interval. This means that for each Sample Time, the aggregation interval extends back to the start of the current hour. Therefore the aggregation interval grows until it reaches one hour and then starts again.

In our bar chart example, the aggregation function is SUM. A number of other aggregation functions are used throughout the Pilot Console, namely, MAX, MIN, AVG, TIME AVG, and others.

Actions

The Trigger Condition is an expression which is evaluated at each Sample Time. Even when the trigger is True, we may want some additional context before we execute the corresponding actions. For example, we may only want to execute the associated actions when the Trigger Condition makes a transition from False to True on successive Sample Times. These additional conditions are called *Transition Conditions*.

Transition Conditions

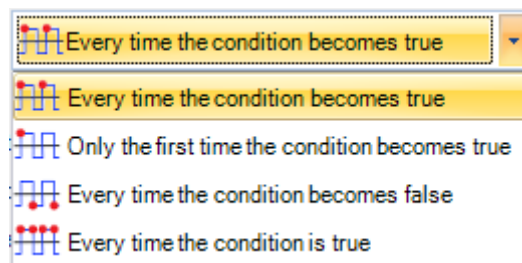


Figure 34 Transition Condition List

In Figure 34 we show the contents of the drop-down box. These are the Transition Conditions that are used, in conjunction with the Trigger Condition, to determine when the associated actions are to be executed. The icons are suggesting: leading edge, every time; leading edge, only once; trailing edge, every time; and every time.

- *Every time the condition becomes true.* Actions are executed whenever the Trigger Condition is True on the current Sample Time and was False on the previous Sample Time. The Actions are also executed if the Trigger Condition is True when the Watch is activated (i.e., before there is any history for the Watch).
- *Only the first time the condition becomes true.* Actions are executed the first time the Trigger Condition is true on a Sample Time and was False on the previous Sample Point. The Actions are also executed if the Trigger Condition is True when the Watch is activated (i.e., before there is any history for the Watch). The Actions are executed at most one time.
- *Every time the condition becomes false.* Actions are executed whenever the Trigger Condition is False on the current Sample Time and was True on the previous Sample Time. The Actions are also executed if the Trigger Condition is True when the Watch is activated (i.e., before there is any history for the Watch).
- *Every time the condition is true.* Actions are executed whenever the Trigger Condition is True.

Note: A Trigger Condition, along with its associated transition condition, is based on a View associated with the Local System or with a remote Shark Appliance. Accordingly, the actions associated with the trigger condition are initiated by the Local System or the remote Shark Appliance

Notify Me

The Notify Me action is always executed and makes a record of the event on the strip chart and in the Events panel.

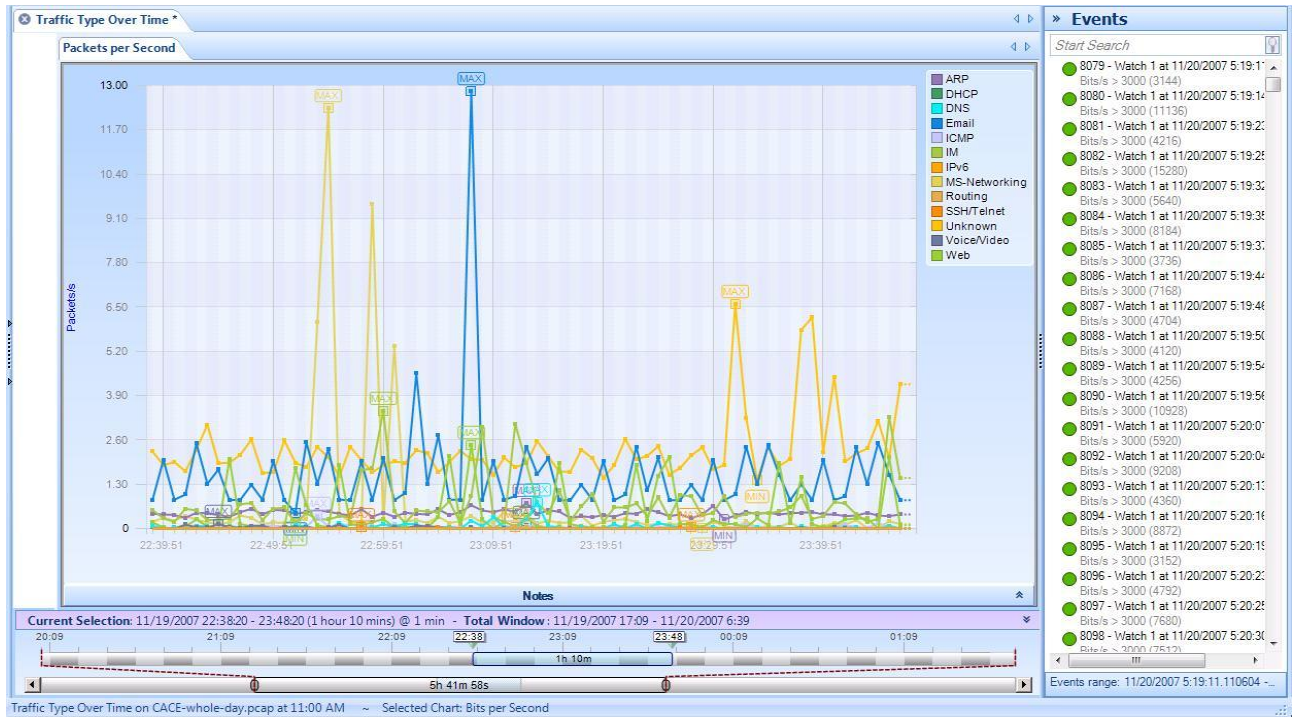


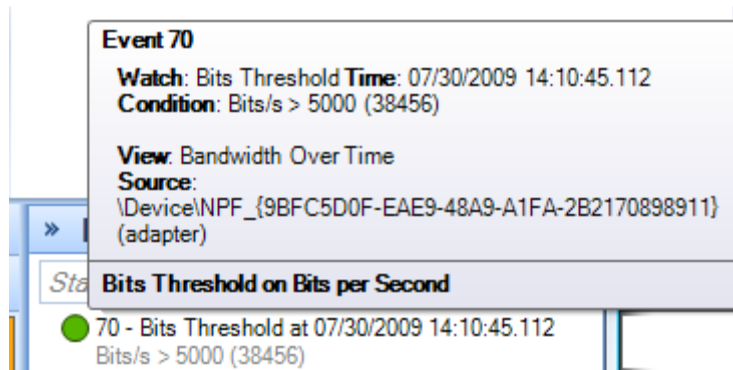
Figure 35 Event Notifications

Figure 35 shows how the event notifications appear on a strip chart and in the Events panel. Notice that the event selected in the Events panel is highlighted in the strip chart and also on the Time Window. If a vertical line representing an event on the strip chart is selected, the corresponding event is shown as selected in the Events panel and in the Time Window. Moreover, if the event line is selected in the Time Window, it is shown as selected in both the Events panel and the strip chart.

● 1792 - Packets Watch at 07/09/2009 20:59:02.101
Packets/s > 80 (159) for Traffic Type=Web

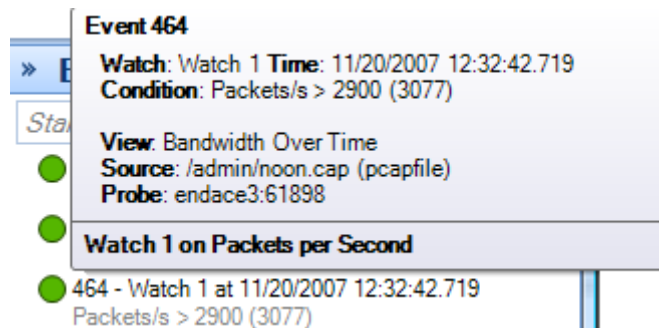
Figure 36 Event Structure

The Event Structure begins with a circle with the color corresponding to the color of the Watch Severity. The following number is the event Unique ID followed by the Name of the event. This is followed by the date and time at which the event occurred. The second line begins with the Trigger Condition and the value, in parentheses, that caused the Trigger Condition to be true followed by the line that was selected in the strip chart when the Watch was defined.



Tooltip 1 Tooltip for an Event

Moving the mouse over a severities icon in the Events Panel will bring up a tooltip for the selected event. The tooltip contains the details regarding the Event.



Tooltip 2 Tooltip for a Remote Event

The Tooltip for a Remote event also identifies the “name” of the Shark Appliance and port number.

Send an email with the watch event details

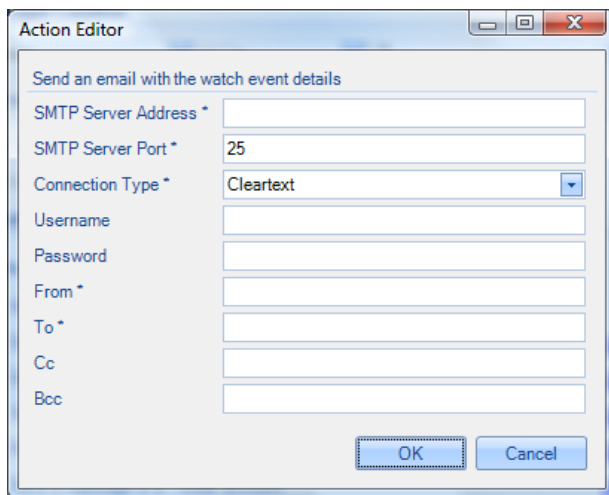


Figure 37 Email Action

If “Send email with the Watch event details” is selected the Send Email Parameters Editor appears. This should be filled in with the mail server information, account, and destination email addresses. When the Action occurs, email will be sent to the destination email addresses with the Event information.

Start a packet capture

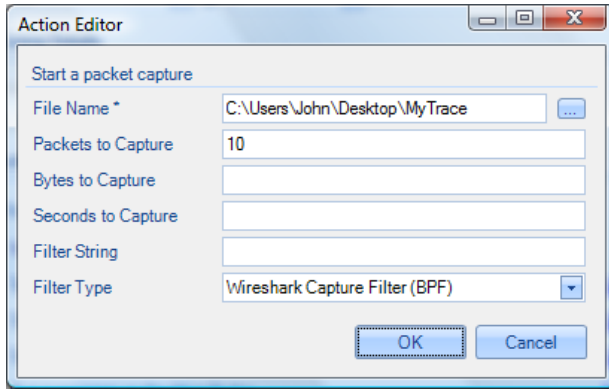


Figure 38 Capture Packets Panel

When “Start a packet capture” is selected the panel in Figure 38 appears. The File name is a mandatory field and specifies the absolute path name of the capture file to be created. The “Packets to Capture,” “Bytes to Capture,” and “Seconds to Capture” are stopping conditions, whichever comes first. An optional Filter String can be specified along with the Filter Type. When the event occurs, a packet capture will be initiated and terminated according to the stopping conditions.

Note: If the Watch is associated with a remote probe, the browser assist for setting the File Name is not available. The capture file will be placed the My Files directory located on the remote probe.

Send a remote syslog message over UDP

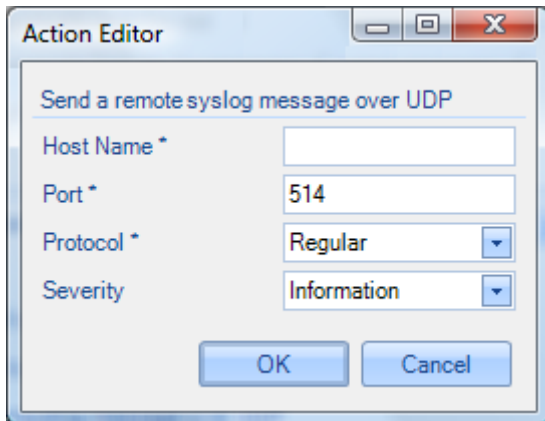


Figure 39 Send to Remote Syslog

Send a syslog message using UDP to a remote host.

Run a program on the Pilot Probe

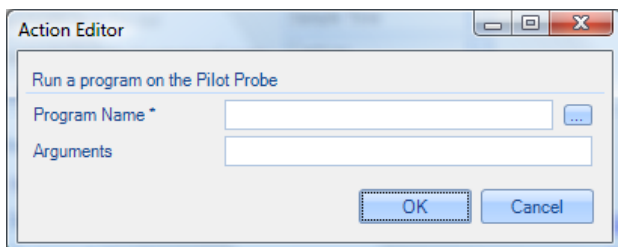


Figure 40 Run a Program

Enter the Program Name (complete path name) and any arguments.

Note: In the case the Watch is associated with a remote probe, the browser assist for setting the Program Name is not available.

Send a message to a Twitter account

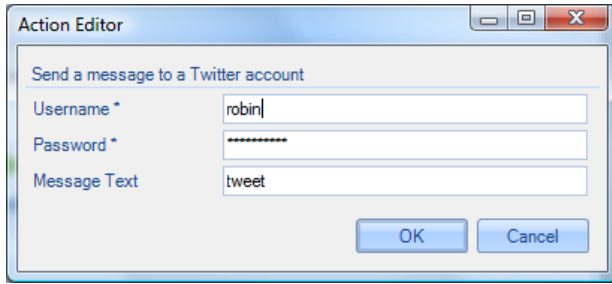


Figure 41 Send to Twitter Account

Enter Twitter account information and a Message. The message will be sent to the Twitter account for every event instance.

Log the events in the Probe's syslog

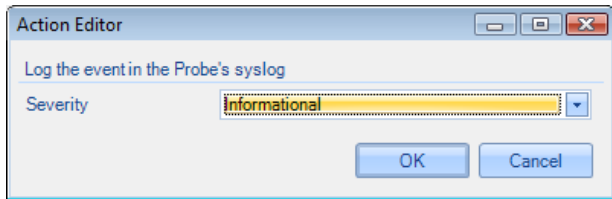


Figure 42 Send to Probe's syslog

The event will be entered into the Probe's syslog. The Severity corresponds to the Windows severities.

Start a Capture Job

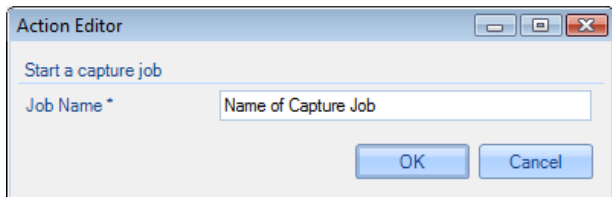


Figure 43: Start a Capture Job

The event will start a currently stopped capture job. If the capture job is already started there is no change.

Stop a Capture Job

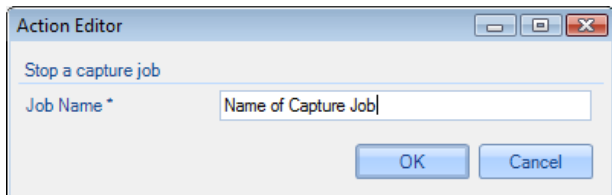


Figure 44: Stop a Capture Job

The event will stop a currently running capture job. If the capture job is already stopped, there is no change.

Log the events in a CSV file on the Shark Appliance

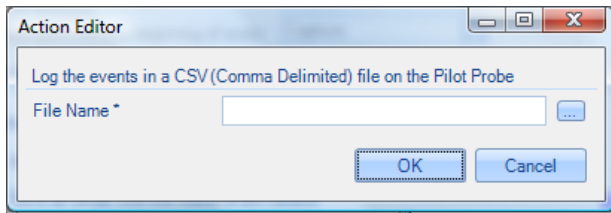


Figure 45 Send to CSV File

The event will be written as a CSV file using the complete pathname provided in the Action Editor.

Note: In the case the Watch is associated with a remote probe, the browser assist for setting the File Name is not available.

The Ribbon

Finally we cover the functionality of the Watches/Events Ribbon itself. As with all the ribbons, this one is divided into a number of sections.

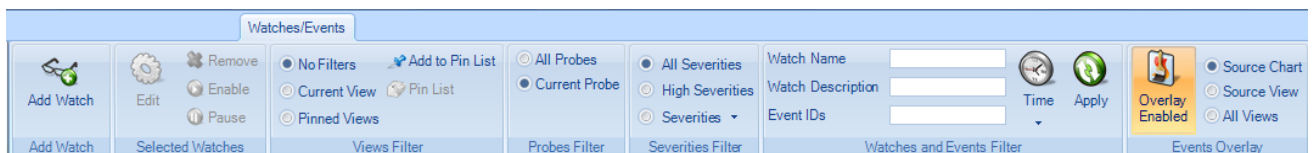


Figure 46 Watches and Events Ribbon

Add Watch



Figure 47 Add Watch

The *Add Watch* button is enabled when there is either a strip chart or bar chart selected within the current View. Clicking on the Add Watch button brings up the Watch Editor panel for creating a new Watch for the selected chart within the current View.

Selected Watches

Edit Selected Watch



Figure 48 Edit Watch

With a Watch selected in the Sources panel, the *Edit* button brings up the Watch Editor. The Watch parameters can be modified with the Watch Editor.

Note: A Watch applied to a trace file cannot be edited.

Remove Selected Watch



Figure 49 Remove Watch

With a Watch selected in the Sources panel, the *Remove* button is used to remove the Watch and all of the associated events in the Events panel

Enable Selected Watch



Figure 50 Enable Watch

With a disabled Watch selected in the Sources panel, the *Enable* button will cause the Watch to become active.

Note: A Watch applied to a trace file cannot be enabled.

Pause Selected Watch



Figure 51 Pause Watch

With an enabled Watch selected in the Sources panel, the *Pause* button is used to disable the Watch. During the time the Watch is disabled, no events will be generated.

Note: A Watch applied to a trace file cannot be disabled.

Filtering Events Section

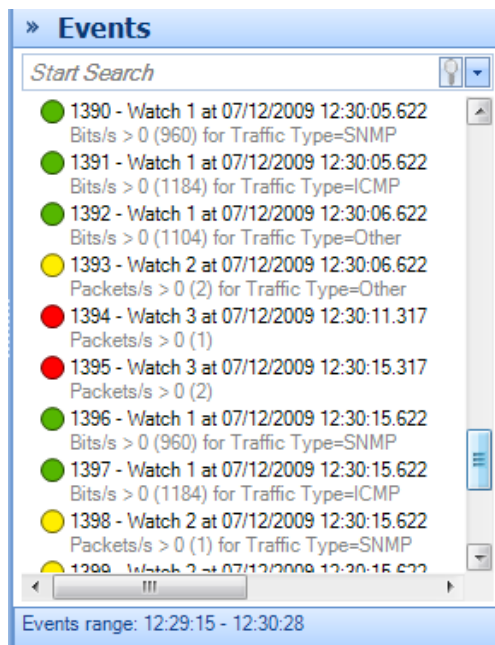


Figure 52 Events Panel

When there are multiple Watches, or even a single Watch, it is possible to generate a very large number of Events. Sorting through these looking for significant ones can be daunting. The Events Panel has a search box that can be used to isolate events of interest.

Another possibility for filtering events can be found in the middle sections of the Watches/Events ribbon.

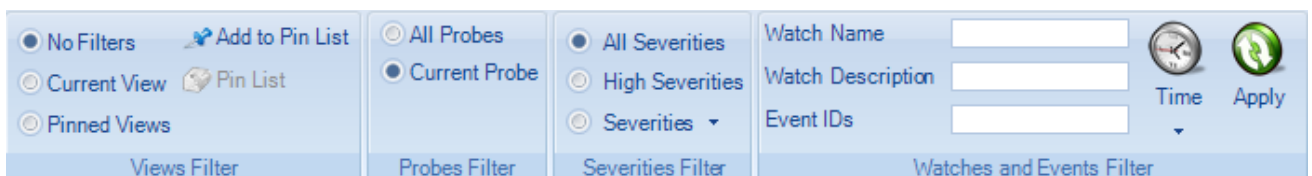


Figure 53 Event Filtering Section of the Watches/Events Ribbon

In Figure 53 we show the sections on the Watches/Events ribbon that deal with locating Events by filtering on:

- Views Filter
- Severity Filter
- Watches and Events Filter

Note: The events filter that results from these three filter sections is the conjunction of the filtering provided by the individual sections.

Views Filter

This section of the ribbon deals with filtering Events based on their associated Views.

- No Filters is selected. Filtering on View is disabled
- Current View is selected. The Views Filter selects only those Events that are associated with the Current View
- Pinned Views is selected. The Pin List contains a list of Views that have been “Pinned.” When Pinned Views is selected, the Views Filter selects only those Events that are selected with some View in the “Pin List”

Add to Pin List



Figure 54 Add to Pin List

With a View selected in the Sources Panel, clicking on *Add to Pin List* will add the selected View to the Pin List.

(Show the) Pin List



Figure 55 (Show the) Pin List

The *Pin List* button is active whenever there is at least one View in the Pin List. Clicking on the Pin List button (when it is active), will show the Pin List.

The Pin List

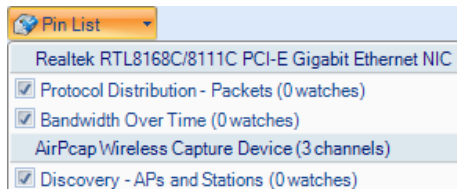


Figure 56 The Pin List

The *Pin List* itself shows the pinned views and their sources. The sources can be either live or a trace file. Views can be removed from the Pin List by clicking on the corresponding check boxes.

Probes Filter



Figure 57 Probes Filter

There are two choices with the Probes Filter. Show the Events from all of the Shark Appliances (including the Local System) in the Events Panel, or only show the Events from the currently selected Shark Appliance in the Sources Panel.

Severities Filter

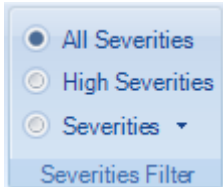


Figure 58 Severities Filter

The Severities Filter section allows us to add filters on the Event severities. The three choices are disjoint.

- *All Severities*. This is equivalent to no Severity filtering.
- *High Severities*. High severities are defined to be Error or higher – Error, Critical, Alert, and Emergency.
- *Severities (List)*. When this button is selected, the Events are filtered on the severity levels in this list. The list can be set/reset by clicking on the down-arrow.

Severities Filter

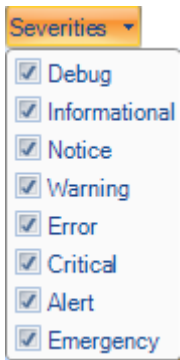


Figure 59 Severities List

The Severities List contains the severities that will be used by the severities filter. The selected severities are those with the checks. Severities can be selected or unselected using the check boxes.

Watches and Events Filter

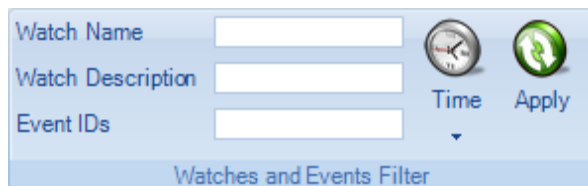


Figure 60 Watches and Events Filter

Event filtering based on the corresponding Watch Name, Watch Description, Event IDs, or Time Interval.

Time Filter

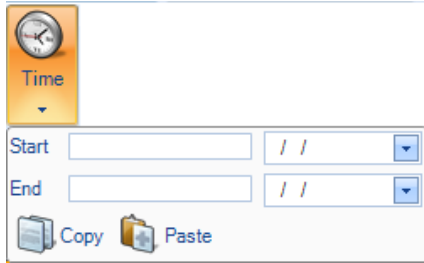


Figure 61: Time Selection

The Start and End times can be filled in manually, or the Paste operation can be used. Typically, the clipboard is carrying a time interval that was obtained using the copy operation in the Time Selection section of the Time Control ribbon. Conversely, if the time interval is available, the Copy operation can be used to save the interval to the clipboard for use in making time selections by pasting it into the Time Selection section of the Time Control ribbon.

Apply



Figure 62 Apply Button

Once all of the parameters in the Watches and Events Filter have been set, click on the *Apply* button for the filter to take effect.

Note: The Watches and Events Filter does not take effect until the user clicks on the Apply button.

Events Overlay

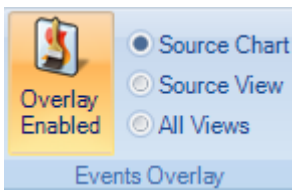


Figure 63 Events Overlay Section

By selecting the *Overlay Enabled* button, the radio buttons are enabled.

- *Source Chart*. Only show the events in a Chart of the Watches that are associated with the Chart. This is the usual case where you see the events only in the chart where the Watch was created.
- *Source View*. Show events associated with all of the Watches in a View in each Chart of a View. This is generally used when one of the charts in a View has a Watch and you want to see these events displayed in the other charts in the View.
- *All Views*. Show all the events of all the Watches in all of the charts of all of the Views. Is often used if only one chart has a Watch and you want to see where these events occur in the charts of all of the other Views.

Predefined Watches

Many of the View folders contain an initial subfolder containing predefined Watches. In Figure 64 we show the expanded Bandwidth Usage folder and its first subfolder is called the *Bandwidth Usage Watches*.

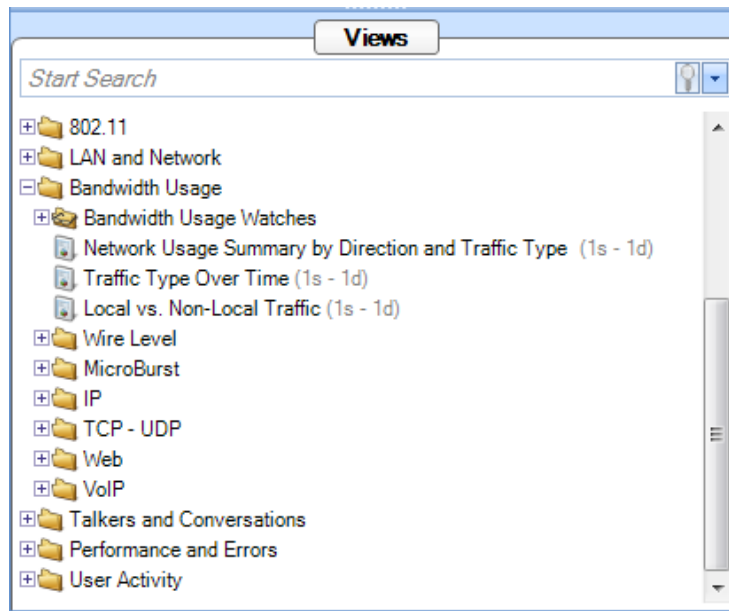


Figure 64 Predefined Watches

Opening the Bandwidth Usage Watches folder we get the following:

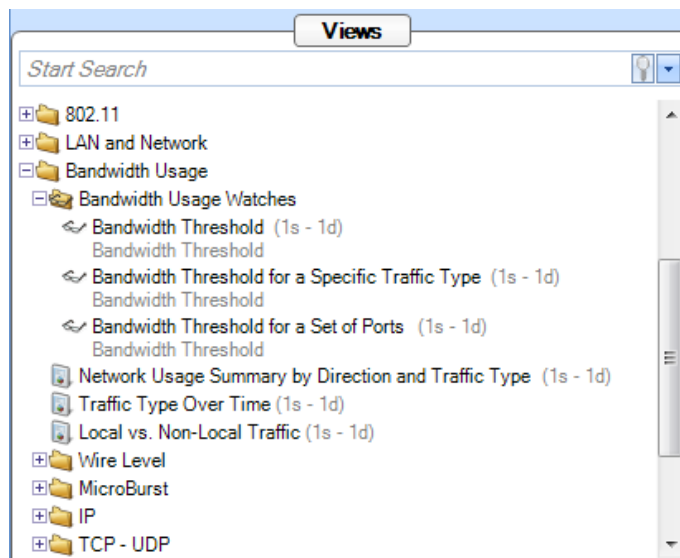


Figure 65 Expanded Bandwidth Usage Watches Folder

The expanded Bandwidth Usage Watches folder contains 3 entries. Each of these entries consists of a View plus a Watch which is associated with the View. For Example, the *Bandwidth Threshold for a Specific Traffic Type* (in Figure 65) is a View with a *Bandwidth Threshold* Watch associated with the View. This View/Watch combination can be applied to either a live or off-line source just like any other View. However, when it is applied, the Watch Editor automatically appears to be filled in with the usual parameters. In this case a Filter Settings section is made available to further modify the Watch before applying the View/Watch combination.

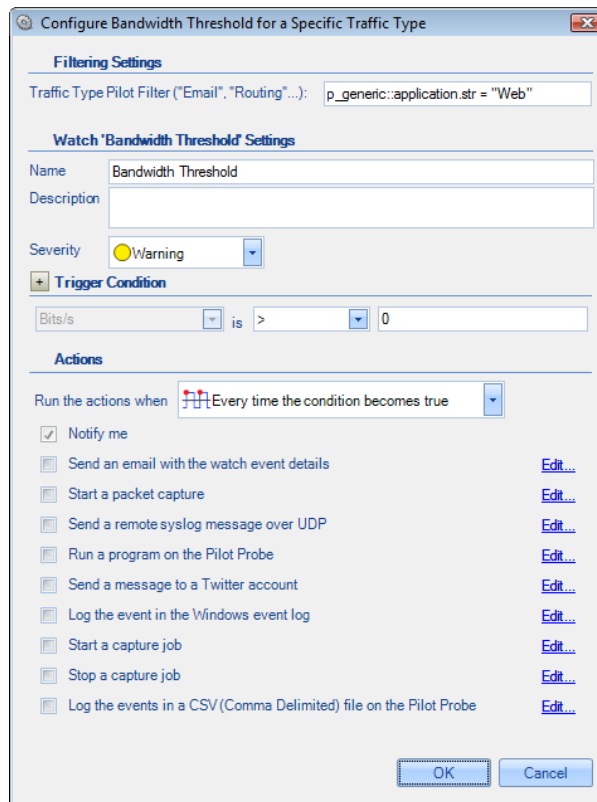


Figure 66 Watch Editor Panel with Filter Settings

Figure 66 shows the watch editor for the Bandwidth Threshold predefined Watch. In addition to the usual Watch settings, the user can specify Filter Settings to select specific traffic types.

Note: Filters that appear in predefined View/Watch combinations are placed between the source and the View to filter out unwanted packets before being processed by the View. The Watch is subsequently applied to the metrics produced by the View.

Once the combined View/Watch is applied, it behaves exactly the same as if the View and the Watch were each applied independently – the View to the source and the Watch to the View.

Reporting Ribbon

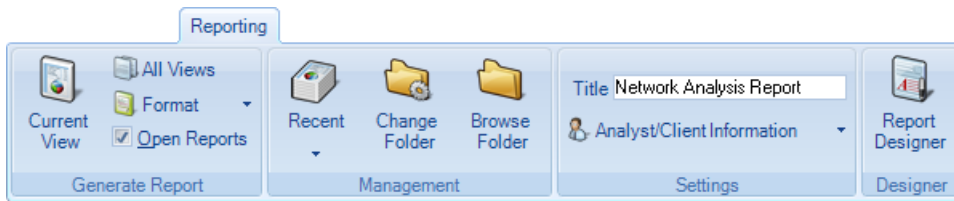


Figure 67 Reporting Ribbon

The *Reporting Ribbon* is used to create and manage reports created from views. Certain sections and buttons of the ribbon are disabled by default. Reports can be made from one view or from all open views. Reports can be generated for a number of different file formats in a single batch operation. Many things can be customized in a generated report. The ribbon will be discussed top-to-bottom, left-to-right, broken up by section.

Generate Report

This section manages how the reports are generated without concern for the style, layout, or what is included in a report. It instead, specifies the format, and how to manage post generation of reports.

Current View



Icon 20 Current View

The *Current View* button is used to generate a report using the current view. In order for this to work, a view must be the foremost tab. Under any other situation, this button is disabled. This button and the next button, “All Views” act differently depending on the settings of the final two buttons of the section, *Format* and *Open Reports*.

All Views



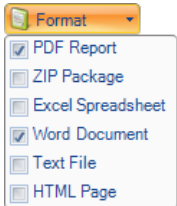
Icon 21 All Views

The *All Views* button is used to generate a report using all open views. This button and the previous button, *Current View*, act differently depending on the settings of the final two buttons of the section, *Format* and *Open Reports*.

Format



Icon 22 Format



Submenu 5 Format

The *Format* button opens a submenu that specifies one or more export formats. These selections are saved in the global configuration file. By default, only the PDF option is selected.

The meaning of each check box is as follows:

PDF Report

The PDF Report checkbox refers to a PDF 1.4 (Acrobat 5.x or newer) PDF document generated with all security turned off. Generated documents have been tested to generate correctly with Acrobat Reader, ghostview 3.6.2, and xpdf 3.01.

Zip Package

The *Zip Package* check box refers to a ZIP file with the following contents:

- Each trace file analyzed in the report.
- The MD5 cryptographic digests (if enabled) of the trace files.
- The PDF version of the report.

Excel Spreadsheet

The *Excel Spreadsheet* check box refers to an excel spreadsheet with the tabular data of the report in a way that can be used to generate further graphs and charts with the spreadsheet graphing options that are available in Excel.

Word Document

The *Word Document* check box refers to a “Rich Text Formatted” (RTF) document that can be viewed in Microsoft Word.

Text File

The *Text File* check box refers to a plain text document. Naturally, no images are available, but the image data is made available in tabular form.

HTML Page

The *HTML Page* check box refers to a generated HTML page and a directory containing the images of the relevant charts in PNG format. The HTML is compatible with all major modern web browsers.

Open Reports



Figure 68 Open Reports

The *Open Reports* check box, selected by default, works in the following way:

When On

Pressing the *Current View* or *All Views* button instantiates the appropriate helper applications to be open with the generated reports. For instance, if generating Word and HTML formatted reports, then the default word processor and web browser will open and display the reports.

When Off

No programs are opened when a report is generated.

Management

Generated reports are saved to a user-specified directory. The default directory is the “My Documents” (or language equivalent) directory in the users “Documents and Settings” (or language equivalent) directory. This can be changed as desired. The *Management* section provides a convenient way to get to the directory, manage recently created reports, and change the report directory.

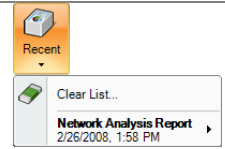
Recent



Icon 23 Recent

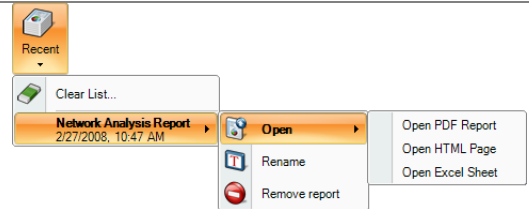
The *Recent* button opens a submenu to manage recently generated reports. By default, before reports are generated, the Recent button is disabled.

After a report is generated, a reference to it is placed in the Recent sub menu list. The list holds at most, the five most recently generated reports and may be cleared at any time. Note that the clear operation does not physically remove any file from disk but simply clears it from the referential list inside of the Pilot Console.



Submenu 6 Recent Reports

Each submenu item has in turn, another submenu to open one of the formatted reports from the generated report package. Additionally, reports can be renamed and removed irrevocably from disk.



Submenu 7 Recent Reports (Detail)

Change Folder



Icon 24 Change Folder

The *Change Folder* button changes where future generated reports will be saved.

Browse Folder



Icon 25 Browse Folder

The *Browse Folder* button opens a browser window to determine the folder where future reports will be saved in the Windows Explorer shell.

Settings

The *Settings* section manages what will go on the cover page of the report, if it is to exist (See the section on the Report Designer about how to turn it off).

Title

Title: Network Analysis Report

Figure 69 Title

The *Title* edit box specifies what to call subsequently generated reports. The title goes on the cover page if the page is included in the report generation. See the section on the Report Designer Ribbon that follows for more information.

Analyst/Client Information



Icon 26 Analyst/Client Information

The *Analyst/Client Information* button presents a submenu that specifies what information will appear on the cover page of a report. Each field is directly analogous to what will appear on the cover page. Refer to the appendix on the example report for more information.

Analyst Information	
Name	Dibert Dobson
E-mail Address	ddobson@phonecorp.com
Phone Number	808 555 1337
Client Information	
Client Name	Pointy Haired Boss
Case Number	3,000,000

Submenu 8 Analyst/Client Information

Report Designer



Icon 27 Report Designer

The *Report Designer* button opens a new tab in the ribbon bar to do specific design actions on subsequently generated reports. This ribbon is described below.

Report Designer Ribbon

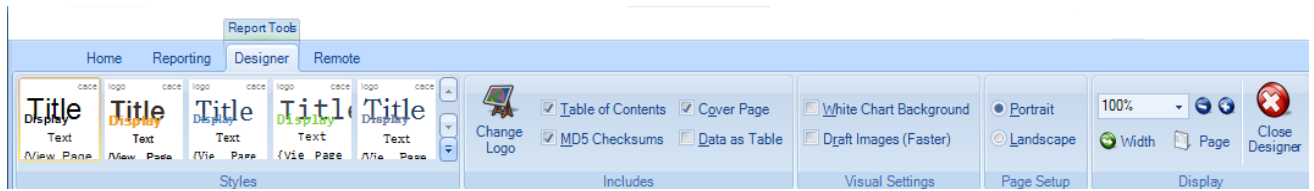


Figure 70 Report Designer Ribbon

The *Report Designer* ribbon is not always available. It is a contextual ribbon that only appears when reports are being designed. In order to get to it, click the *Report Designer* button at the end of the *Reporting* ribbon (described at the end of the previous section).

When clicked, a generic template report appears as a tabbed window which does not correspond to any specific data from a view. All changes made in the report designer take effect immediately and there is no need to save when exiting the designer.

Additionally, the designer can be left open while generating reports for quick changes. Note that any changes made to the template via the report designer will only affect how subsequent reports are generated.

Styles



Figure 71 Styles

The *Styles* section controls the themed look and feel of subsequent reports. There are five choices to choose from and each can be viewed by simply hovering over them with the mouse. A theme can be selected and set as the default by clicking on it. In the depiction on the left for instance, the first style is selected.

Includes

The *Includes* section has options that determine what is presented inside a report.

Change Logo



Icon 28 Change Logo

The Change Logo button is used to specify the logo that will go in the upper right hand side of the cover page of all subsequent reports.

Table of Contents

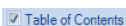


Figure 72 Table of Contents

The *Table of Contents* check box (checked by default) is used to specify whether to include a table of contents in subsequent reports.

MD5 Checksums of Trace Files

MD5 Checksums

Figure 73 MD5 Checksums

The *MD5 Checksums* check box (not checked by default) is used to specify whether MD5 cryptographic digest will be generated for trace files in subsequent reports. These digests are printed on the reports and placed in a separate file for ZIP report output. The MD5 computational throughput is on the order of 7 MB per second or about 420 MB per minute.

Cover Page

Cover Page

Figure 74 Cover Page

The *Cover Page* check box (checked by default) is used to specify whether to include cover pages in subsequent reports.

Data as Table

Data as Table

Figure 75 Data as Table

The *Data as Table* check box (checked by default) is used to specify whether to include quantitative data tables in subsequent reports.

Visual Settings

The *Visual Settings* section has options used to modify the overhead technicalities of the creation process of reports.

White Chart Background

White Chart Background

Figure 76 White Chart Background

The *White Chart Background* check box (not checked by default) is used to specify whether the generated charts will have a white background instead of the gradient one in the Pilot Console. Turning this feature on will

- Increase the visual contrast on monochrome (black and white) printers
- Marginally decrease the file size of generated reports by about 10%.

Draft Images (Faster)

Draft Images (Faster)

Figure 77 Draft Images (Faster)

The *Draft Images (Faster)* check box (not checked by default) is used to specify the quality of the images in subsequent reports. Draft images are a suitable resolution for viewing on a computer while non-draft images are suitable for printing. Turning this feature on will

- Decrease the time needed to generate reports.
- Decrease the file size of the generated report.

Page Setup

The *Page Setup* section controls the page orientation of future generated reports.

Portrait

Portrait

Figure 78 Portrait

The *Portrait* check box makes all subsequent reports generate in portrait orientation.

Landscape



Figure 79 Landscape

The *Landscape* check box makes all subsequent reports generate in landscape orientation.

Display

The *Zoom* section is used to control the magnification of the report template.

Zoom Amount



Figure 80: Zoom Amount

The *Zoom Amount* drop down specifies the magnification of the template in the report designer.

Decrease Zoom



Icon 29 Decrease Zoom

The *Decrease Zoom* button is the “minus” sign and it decreases the magnification level of the template in the report designer by 10%.

Increase Zoom



Icon 30 Increase Zoom

The *Increase Zoom* button is the “plus” sign and it increases the magnification level of the template in the report designer by 10%.

Width



Icon 31 Zoom Width

The *Screen Width* button changes the magnification level of the template in the report designer so the width of a page matches all that is available in the tab.

Page



Icon 32 Zoom Page

The *Page Height* button changes the magnification level of the template in the report designer so that an entire page can be viewed.

Close Designer



Icon 33 Close Designer

The *Close Designer* button closes the report designer ribbon and template view tab. Since all changes are immediate, there is not prompt to save for changes.

Remote Ribbon

Users and Groups play an important role in accessing remote probes. We start this section by describing the remote probe's Credential Manager.

Remote Probe Credential Manager

User and Group Access Control

All communications between the Shark Appliances and the Pilot Console use SSL-encrypted Web communications and require that each request from a Pilot Console contains HTTP basic access authentication credentials ([HTTP Authentication](#)). The Shark Appliance passes the authentication credentials to the Shark Appliance's Credential Manager. The Credential Manager determines if the user has a "privilege" that permits the execution of the requested operation. If the Credential Manager rejects the operation, the Shark Appliance returns the "not enough privileges" error to the Pilot Console making the request. Otherwise the Shark Appliance executes the operation.

Credential Manager

The Credential Manager associated with a Shark Appliance is governed by the User configuration file co-located with the Shark Appliance. A sample User configuration file is included as a reference in Appendix C Example User/Group Configuration File. A user can be part of one or more groups. Each user can "own" a set of resources: for example, the files or the folders that he has created, or the views that he has applied. Unless he is an administrator, a user has **visibility** and **control** only on his resources:

A user cannot see a file or a view created by another user.

A user cannot close a view or to delete a file that have been created by somebody else.

Resources, however, can be *shared*. Members of a group normally share a common folder that has the same name of the group. This folder can be use for trace file sharing, and all the users in the group have read and write access to the folder. When you drag a file into this folder, all the other member of the group will immediately see it and will be able to manipulate it.

Views can be shared with single users or groups by right-clicking on them and selecting "share with". As soon as a view is shared, the selected user or group will immediately see it in their sources panel.

User and groups are configured by editing the User configuration file in the Pilot Console folder.

Privileges

The User Configuration file is used to configure the **privileges** for users and groups. A privilege is a capability that can be granted or revoked, and is specified as an attribute of the User or Group tag in the users file. The privileges that the Shark Appliance currently implements are:

- **IsAdministrator**: if set to true, gives a user or a group full access Shark Appliance. Administrators see all the resources in the system, including views, files and folders that have been created by other users. Administrators have full control on all these resources.
- **CanApplyViewsOnFiles**: if set to true, allows the user or the group to apply views to files residing on the Shark Appliance.
- **CanApplyViewsOnInterfaces**: if set to true, allows the user or the group to apply views to the network interfaces on the Shark Appliance.
- **CanCreateFiles**: if set to true, the user or the group can create files on the Shark Appliance, by selecting the "send to file" buttons in the Pilot Console.

- CanImportFiles: if set to true, the user can import files into the Shark Appliance, through drag and drop or by clicking on the “Import Files Into Shark Appliance” button in the Remote ribbon.
- CanExportFiles: if set to true, allows the user to export files from the Shark Appliance, and move them to the Pilot Console or to another Shark Appliance (assuming the user has sufficient privilege on the target Shark Appliance to create a trace file). When this privilege is not granted, the user is not able to export a trace file to Wireshark, because that involves exporting packets out of the Shark Appliance to the Pilot Console.
- CanShareViews: if set to true, the user can share the views that he created on the Shark Appliance with other users or groups connected to the Shark Appliance from other Consoles.
- CanAccessProbeFiles: if set to true, the user will be able to “see” the trace files located on the Shark Appliance.
- HasFolder: if set, Shark Appliance creates a shared folder for the group with the name of the group (only applies to groups). All the users in the group will have access to this folder. Otherwise, the folder will not be visible to the members of the group.

Privilege Policy

Since both users and groups can be granted or revoked roles, and since a user can be part of one or more groups, conflicts can arise between the user roles and the groups roles. The Shark Appliance solves conflicts through the following rules:

Granting or revoking a role to the user has precedence over granting or revoking it to the groups the user is part of. In other words, if a role is present (both as true or false) under the user tag in the users file, the fact that the same role is present for any of the groups the user is part of is ignored.

If a role is not set for a user, it is inherited from the groups it is part of.

If different groups have conflicting roles, the highest privilege is assigned to the user.

The Ribbon

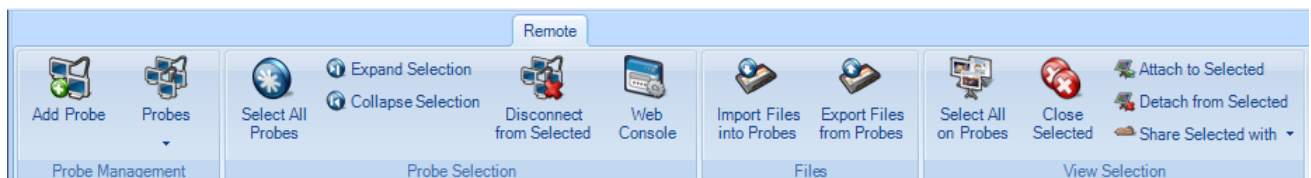


Figure 81 Remote Ribbon

In this section we discuss the sections of the Remote Ribbon: Probe Management, Probe Selection, Files, and View Selection.

Add Probe



Icon 34 Add Probe

Clicking on the *Add Probe* button brings up the *Connect to Probe* panel.

The dialog box 'Connect to Probe' contains the following fields and controls:

- Probe Address:** A dropdown menu showing 'remote.probe.com' and a text box containing '61898'.
- User Name:** A text box containing 'admin'.
- Password:** A text box with masked characters (dots).
- Description:** A text box containing 'Remote probe located in Ohio'.
- Remember password:** A checked checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Figure 82 Connect to Probe Panel

The *Connect to Probe* panel is used to initiate a connection to a Shark Appliance. The Shark Appliance Address can be either a domain name or IP address and the port number of the Shark Appliance. User name and password are also provided along with any descriptive comment regarding the Shark Appliance. When OK is clicked the Pilot Console initiates a request to connect to the Shark Appliance. The information regarding the Shark Appliance is saved in the probe list which is accessible using the *Probes* icon located in the Probe Management section of the Remote ribbon.

Probes



Icon 35 Probes

The *Probes* button brings up the probes panel containing, among other things, the list of probes that have been Added, but not Deleted, using the *Connect to Probe* panel.

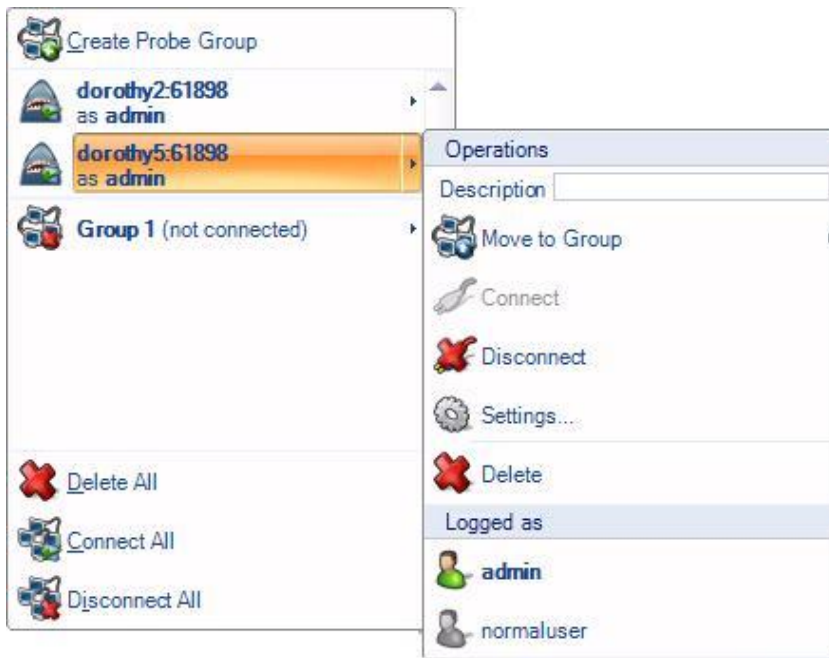


Figure 83 Probes Panel

The first item in Probes Panel is the Create Probe Group. This selection is used to create a collection of probes that can be treated as a single group. A Shark Appliance can be a member of at most one probe group. If a probe is member of a probe group, then it will only appear within the probes group in the Probes Panel.

Below the Create Probe Group is a list of all of the probes to which we have tried to connect using the Add Probe panel and have not been removed from this list. Clicking on the icon to the left of one of the probes on the list will disconnect the Pilot Console from the probe if it is already connected. On the other hand, if the probe is initially disconnected, then clicking on the icon will reconnect the probe as the user shown in the Probes Panel.

The last three items on the main panel act on the list as a whole. Delete All, Connect All, and Disconnect All.

Selecting a Shark Appliance on the list brings up a submenu containing operations permitted on the selected Shark Appliance. Edit the Description, move the Shark Appliance into a probe group, connect or disconnect the Pilot Console from the Shark Appliance, display the Shark Appliance settings, and delete the Shark Appliance from the list. The Logged as list includes the identity of the users having accounts on the selected Shark Appliance. The bold item is the identity of the user who is currently logged into the Shark Appliance from the Pilot Console. Selecting a user on this list will initiate an attempt to connect to the Shark Appliance on behalf of the selected user.

Probe Selection

Select All Probes



Icon 36 Select All Probes

The *Select All Probes* button highlights (selects) all of probes in the Sources Panel (Devices and Files).

Expand Selection



Icon 37 Expand Selection

The *Expand Selection* button expands all of the selected probes in the sources panel, thereby showing all of their associated interfaces and file folders.

Collapse Selection



Icon 38 Collapse Selection

The *Collapse Selection* button collapses all of the selected probes in the sources panel, hiding all of their associated interfaces, files, and views.

Disconnect from Selected



Icon 39 Disconnect from Selected

The *Disconnect from Selected* button disconnects the Pilot Console from the selected probes. The selected probes will continue to process live views and maintain the views associated with trace files.

Web Interface



Icon 40 Web Interface

The *Web Interface* button opens the selected remote probe's Web Interface.

Files

Import Files into Probes



Icon 41 Import Files into Probes

The *Import Files into Probes* button will transfer trace files from the Local System to the selected remote probe. If a directory is selected in a remote probe, then the trace files will be transferred to the selected directory, otherwise the files will be transferred to the My Files folder on the Shark Appliance.

Export Files from Probes



Icon 42 Export Files from Probes

The *Export Files from Probes* button will transfer files from the selected remote probe to the Local System. If a folder on a remote probe is included in the selection, then the folder and its contents will be transferred to the Local System. If a file on a remote probe is in the selection, then just the file will be transferred. Multiple selections are permitted as long as the selections are either all folders or all files.

View Selection

Select All on Probes



Icon 43 Select All on Probes

The *Select All on Probes* button highlights (selects) all of the views on the selected probe.

Close Selected



Icon 44 Close Selected

The *Close Selected* button closes all of the selected views.

Attach to Selected



Icon 45 Attach to Selected

The *Attach to Selected* button attaches to the selected views.

Detach from Selected



Icon 46 Detach from Selected

The *Detach from Selected* button detaches from the selected views.

Share Selected with



Icon 47 Share Selected with

The *Share Selected with* button brings up a panel to allow selected views on Shark Appliances to be shared with other users or groups.

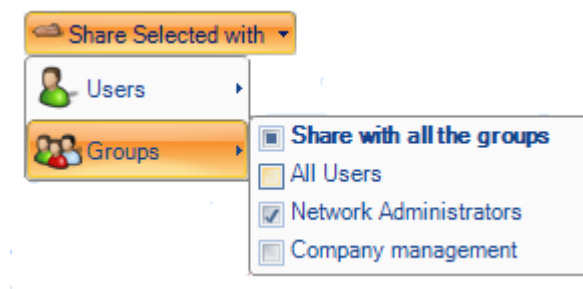


Figure 84 Share Selected with Groups

Shark Packet Recorder

The usual approach to capturing high-speed and/or long duration traffic is to create a file rotation scheme whereby the capture is broken down into a large collection of small trace files with names indicating the time intervals covered by the individual files. It is not difficult to see that this approach can lead to thousands of small files making analysis and troubleshooting extremely tedious, especially when the traffic of interest spans multiple trace files.

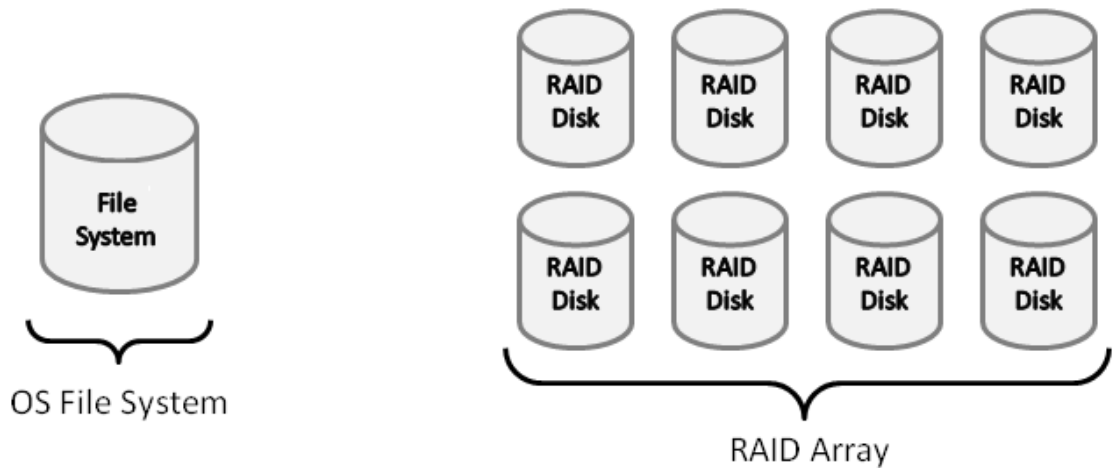
The Shark Appliance includes a “dump-to-disk” facility called the *Packet Recorder*. CACE Technologies’ Packet Recorder is based on an optimized *packet data store* and a novel approach to the use of *time filters* which together eliminate the need for a file rotation scheme for capturing, analyzing, and viewing massive amounts of network traffic. The Packet Recorder saves network traffic in the packet data store as objects called *Job Traces*. CACE Technologies has created a new and intuitive approach for creating *Trace Clips*, which correspond to arbitrary time intervals within a Job Trace. An important feature of a Trace Clip is that it does not require any additional storage beyond the underlying Job Trace. A Trace Clip essentially acts as a time filter on the underlying Job Trace. One of the ways a Trace Clip can be created is by dragging a time selection from a chart on to the underlying Job Trace object – the Trace Clip will be created automatically! Trace Clips are used to isolate specific and manageable portions of a Job Trace for analysis and visualization and behave just like ordinary trace files.

Using *Send To File*, Trace Clips can be converted to ordinary pcap files on the Shark Appliance (no packets leave the appliance).

Some terminology:

- **Capture Job:** A *Capture Job* refers to the specific parameters associated with a “packet recording session.” These parameters include a *name*, the live network traffic *interface* to be used, a BPF filter, *starting* and *stopping* criteria, and an upper bound on the amount of storage to be used by the Capture Job.
- **Job Trace:** Each Capture Job is associated with exactly one *Job Trace* which has the same name as the Capture Job. The Job Trace represents the network traffic saved in the packet data store.
- **Trace Clips:** CACE Technologies has created a new approach which enables quick and easy access to arbitrary time intervals in a Job Trace. Time intervals within a Job Trace are called *Trace Clips* and there are a number of simple and visually oriented ways in which Trace Clips can be created using the Pilot Console. Trace Clips do not require any additional storage and behave exactly like ordinary trace files.
- **Jobs Repository:** The Files Panel for a Shark Appliance contains a folder called the Jobs Repository. This folder has a representation of each Job Trace in the Appliance. This representation consists of an icon and the name of the corresponding Capture Job.
- **Capture Job Interface:** The Devices Panel for a Shark Appliance contains an icon and a name for each of the live capture interfaces associated with Capture Jobs on the Shark Appliance. Views can be applied to the Job Interface creating a visual analysis and representation of the corresponding Job Trace.

Note: Trace clips can be automatically created by dragging a time interval selection from a View on the Job Interface to the corresponding Job Trace!



Contains software, pcap trace files, View data, trending and index data, etc.

Storage used by the Shark Packet Recorder for recording network traffic.

Figure 85: Shark Appliance Storage Systems

The Shark Appliance includes two separate disk configurations:

- Main filesystem for the Shark Appliance software, pcap trace files, view metrics, and indices for Job Traces.
- Shark Packet Recorder storage system for saving Job Traces. This storage system is optimized to provide high-speed writing to disk and fast access to arbitrary time intervals within a Job Trace.

[Capture Jobs \(Shark Appliance Packet Recorder\)](#)

In this section we should how to create a Capture Job and subsequently manage it. Multiple Capture Jobs can exist simultaneously.

Clicking on “Add New Job” brings up a new Capture Job form on the Capture Job page. This form is shown in Figure 12. The form has two tabs: Packet Recording Parameters and Trending/Indexing Parameters. We will consider the Packet Recording Parameters in this section and the Trending/Indexing Parameters in the following section.

Capture Job Settings

Add New Job

Job Description: 0 New Job

Parameters

Capture Port: TurboCap 1Gb device no.0 (00:e0:ed:e.93:8) Start Blink

BPF Filter: [What is this?](#)

Packet Recording Parameters | Trending/Indexing Parameters

Packet Recording Enabled

Packet Portion to Capture:

Absolute Start/Stop		Keep On Disk		Stop Capturing After	
<input type="checkbox"/>	<input type="text" value="01/01/2010 00:00:00"/> Capture Start Time	<input checked="" type="checkbox"/>	<input type="text" value="2048576"/> MB <input type="text" value="53.71"/> % of disk	<input type="checkbox"/>	<input type="text" value="0"/> MB <input type="text" value="0"/> % of disk
<input type="checkbox"/>	<input type="text" value="01/01/2010 00:00:00"/> Capture Stop Time	<input type="checkbox"/>	<input type="text" value=""/> Packets	<input type="checkbox"/>	<input type="text" value=""/> Packets
		<input type="checkbox"/>	<input type="text" value=""/> Seconds	<input type="checkbox"/>	<input type="text" value=""/> Seconds

Status

Job Running	Last Second	Last Minute	Last Hour	
Dumped Packets	192.35 k	10.49 M	628.18 M	-
Dropped Packets	0	0	0	-
Packet Capture Size				2000.73 GB

Stop Save Clear Remove

Figure 86: Adding a Capture Job

Clicking on the “Add New Job” button will create a new job to the Capture Jobs list. There are a number of configuration parameters that need to be set when creating a Capture Job:

- Job Description. Provide a descriptive name for the Capture Job. This will help in identifying the Capture Job since this name will appear in both the Devices and Files source panels.
- Capture Port. The Capture Job takes traffic from a live interface and records it to disk. The available live interfaces appear in the drop-down list. The Job Interface corresponding to this Capture Job is an alias for the selected live interface.
 - Start Blink is used to quickly identify the hardware capture port on the Shark Appliance
- BPF Filter. A BPF filter can be provided to select a subset of the traffic for capturing. For example, the BPF filter “host 172.18.5.4” will only capture the packets with source IP address 172.18.5.4
 - SnapLen is used to put an upper bound on the amount of bytes saved for each packet – at most the first SnapLen bytes from each packet are saved.
- Start/Stop criteria for a Capture Job
 - Absolute Start/Stop. The first check box can be used to specify absolute start time for the Capture Job and the second check box can be used to specify an absolute stopping time for the Capture Job
 - Stop Capturing after. These check boxes can be used to specify stopping conditions based on size of the Capture Job in terms of megabytes or number of packets. Capture duration can also be used as a stopping condition.
- Keep on disk. These parameters are used to limit the maximum amount of storage used by the Capture Job. Once a limit is reached, then the oldest packets are discarded so as to not exceed the limit. If more than one condition is chosen, then the most stringent condition is applied.

Note: When multiple conditions have been selected the most stringent condition is the controlling condition. For example, if an absolute time stopping condition and a stopping condition based on the number of captured packets are selected, then the first condition to be satisfied will stop the capture job.

Trending/Indexing Parameters

In this section we describe the use of Trending/Indexing Parameters.

Capture Job Settings

Add New Job

Job Description: 0 New Job

Parameters

Capture Port: TurboCap 1Gb device no.0 (00:e0:ed:e:93:8) Start Blink

BPF Filter: What is this?

Packet Recording Parameters | **Trending/Indexing Parameters**

Trending/Indexing Enabled

Keep On Disk

7 Days

10240 MB

Synchronize with Packet Recording

Note: indexes are stored in the OS file system. The disk space currently available on the OS partition where the indexes reside is 410.60 GB

Status

	Last Second	Last Minute	Last Hour	
Job Running				
Dumped Packets	192.35 k	10.49 M	628.18 M	-
Dropped Packets	0	0	0	-
Packet Capture Size				2000.73 GB

Stop Save Clear Remove

Figure 87: Trending/Indexing Parameters

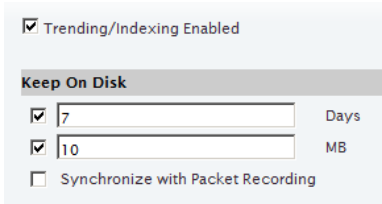


Figure 88: Trending/Indexing Enabled

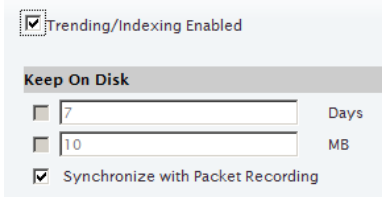


Figure 89: Synchronized Trending

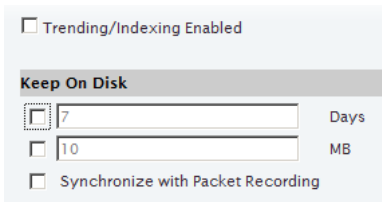


Figure 90: Trending/Indexing Disabled

- **Trending/Indexing Enabled**
With the Trending/Indexing Enabled checkbox selected and the “Synchronize” checkbox not selected, the Keep on Disk parameters control the size and duration of the Trending/Indexing Data

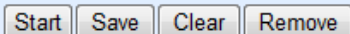
NOTE: The duration of the Trending/Indexing Data is set independently from the Packet Recording “duration” and is typically set to be much longer than the Packet Recording duration.

- **Synchronized Trending/Indexing**
When both the Trending and Synchronize buttons are selected, the duration of the Trending/Indexing data is kept synchronized with the Packet Recording duration
- **No Trending/Indexing**
In this case, no Trending/Indexing data is retained.

Note: The Capture Job recording is stored on the Shark Packet Recorder storage and the Trending/Indexing Data is stored on the OS File System storage.

Capture Job Control Buttons

There are four buttons that are used to control a Capture Job.



Buttons 1: Capture Job Control Buttons

- Start/Stop. If the Capture Job is running then the Stop can be used to stop the Capture Job. If the Capture Job is stopped, then the Start button can be used to start the Capture Job. When a Capture Job is stopped both the packet recording and the creation of Trending/Indexing data are stopped.
- Save. Once the parameters of a Capture Job have been edited, they need to be saved. Assuming the Capture Job is stopped, there are two ways to do this: (1) click on the Save button or (2) click on the Start button. In the first case, the Capture Job parameters are saved and the Capture Job remains stopped. In the latter case, the Capture Job parameters are saved and the Capture Job starts running.
- Clear. The Clear button removes all of the storage associated with the Capture Job and the Trending/Indexing data. The Clear button should only be used when the Capture Job is in the Stopped state.
- Remove. The Remove button deletes the Capture Job recording and the Trending/Indexing data from the Shark Appliance along with the corresponding Job Trace and Job Interface. The Remove button should only be used when the Capture Job is in the Stopped state.

Note: The Start, Save, Clear, and Remove buttons can only be used when the Capture Job is NOT running.

Status of a Capture Job

Status			
Job Running	Last Second	Last Minute	Last Hour
Dumped Packets	34.67 k	2171.32 k	183.28 M
Dropped Packets	0	0	0
Packet Capture Size	2163.25 GB		

Figure 91: Capture Job Status

In Figure 91 we show a configured Capture Job that is Capturing (it say “Job Running” in green). The Status fields indicate whether the Job is Capturing or Not. There are statistics regarding: Dumped (Captured) Packets, and Dropped Packets – these parameters are shown for the Last Second, Last Minute, and Last Hour. The Packet Capture Size is also shown.

If the Job is Running and Trending/Indexing is Enabled, then so also is the computation of the Conversation Index, otherwise the Conversation Index calculation is also stopped.

Capture Jobs in the Devices Panel

Each Capture Job appears as a *Job Interface* in the Devices panel.



Icon 48: Job Interface

Each Capture Job has an associate live interface which corresponds to the Capture Port of the Job. When a Capture Job is created, an icon appears in the Devices panel representing the Job Interface. The name of the interface is the same as the name of the Capture Job.

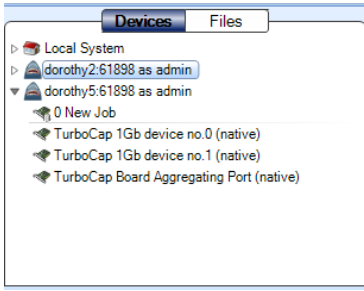


Figure 92: Job Interface in Devices Panel

Figure 92 shows one Job Interface, namely 0 New Job. This interface behaves as ordinary live traffic sources. The actual physical interface corresponds to the Capture Port setting in the corresponding Capture Job.

Operations on Job Interfaces

All of the operations that are available for live interfaces can be applied to a Capture Job Interface.

Note: When drill down is applied to a “live view,” the new view shows results from the time the view was applied. Also, drill down cannot be applied to time selections in a live view. These limitations apply to Capture Job Interfaces.

Capture Jobs in the Files Panel



Icon 49: Job Trace Repository Folder



Icon 50: Job Trace w/o Trending Data



Icon 51: Job Trace with Trending Data



Icon 52: Job Trace with Partial Trending Data

The Files Panel for a Shark Appliance contains a *Job Trace Repository Folder*. The Job Trace Repository folder contains a *Job Trace* for each Capture Job. The Job Trace has the same name as the Capture Job and represents the captured network traffic.

The various icons represent whether there is complete Trending/Indexing data (Icon 51) associated with all of the packets or partial Trending/Indexing data (Icon 52).

In Figure 93 we show the contents of the Job Trace Repository folder in the Devices Panel.

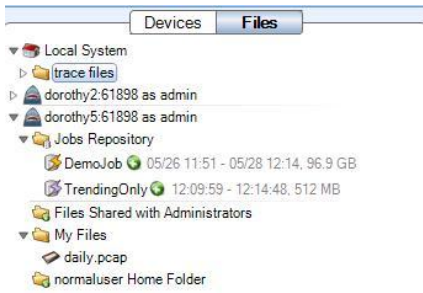


Figure 93: Job Trace Repository Folder in the Files Panel

Operating on Job Traces – Trace Clips

It is not unusual for a Job Trace to be multiple terabytes in size making direct operations impossible. In this section we show how we can easily manage and analyze these potentially massive network traffic recordings. Time intervals within a Job Trace are called *Trace Clips* and there are a number of simple and visually oriented ways in which Trace Clips can be created using the Pilot Console. Trace Clips do not require any additional storage and behave exactly like ordinary trace files.



Icon 53: Trace Clip w/o Trending Data



Icon 54: Trace Clip with Trending Data



Icon 55: Trace Clip w/o Complete Packet Coverage

A Trace Clip identifies a time interval within a Job Trace. Trace Clips are found in the Files Panel and located under the corresponding Job Trace and are identified by the icon shown in Icon 53.

- Icon 53 represents a Trace Clip without any Trending/Indexing data
- Icon 54 represents a Trace Clip with complete Trending/Indexing data
- Icon 55 represents a Trace Clip with limited packet storage

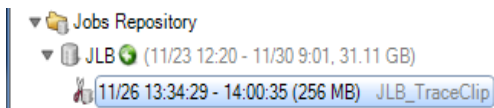


Figure 94: Trace Clip for JLB

In Figure 94 we show a Trace Clip named JLB_TraceClip. In the next sections we will show how to create trace clips.

Creating Trace Clips

There are two ways to bring up the Time Control panel for creating a Trace Clip.

JLB (11/23 12:20 - 11/27 14:24, 25.25 GB)

Figure 95: Creating a Trace Clip

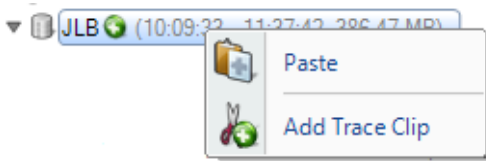


Figure 96: Add a Trace Clip

In Figure 95 we show the Job Trace named JLB. Clicking on the “plus” icon to the right of the name will bring up the Time Control panel shown in

Right clicking on the Job Trace will bring up a context menu (Figure 96) with the Menu Item “Add Trace Clip.” Selecting this menu item will bring up the Time Control Panel.

Recall that a Trace Clip identifies a time interval within a Job Trace. If the clipboard contains a time interval, then the “Paste” menu item can be used to create a Trace Clip corresponding to the time interval on the clipboard.

Time Control Panel for Creating Trace Clips

In this section we show how to create trace clips.

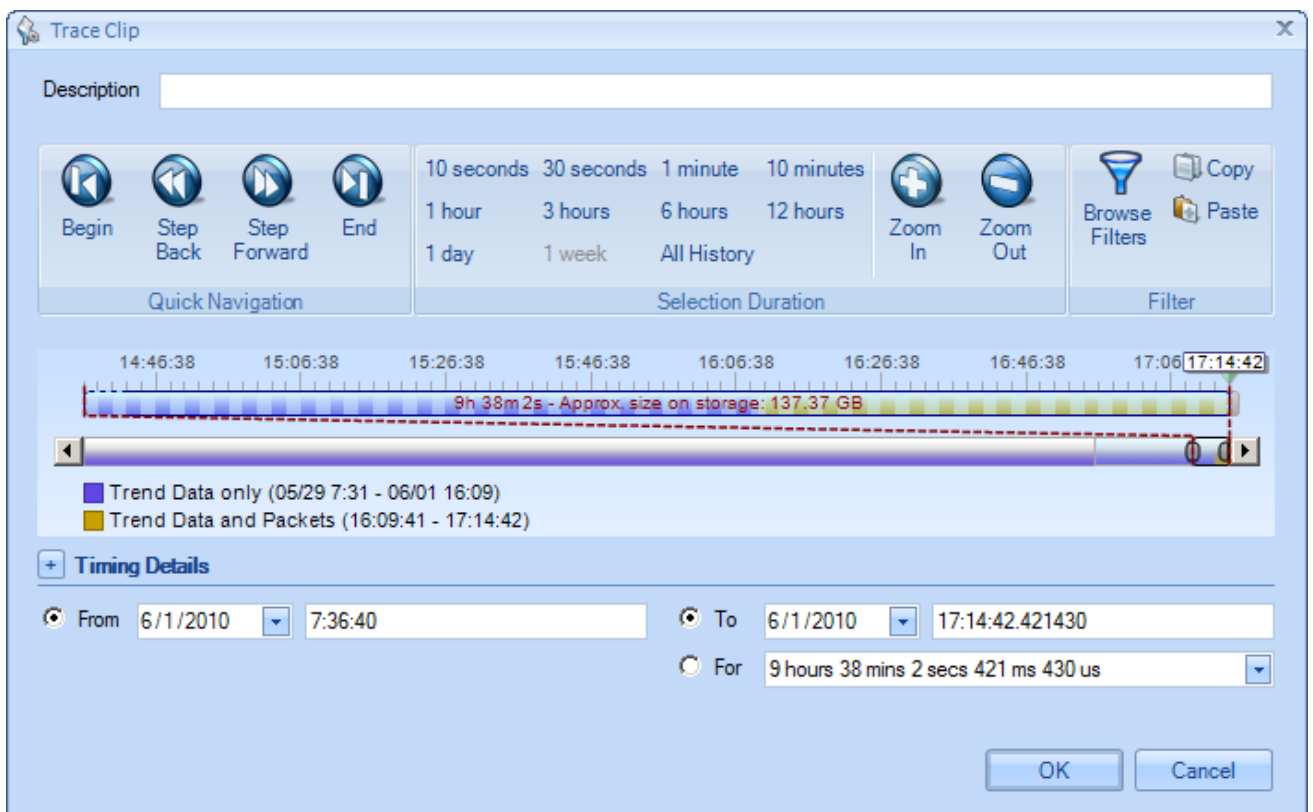


Figure 97: Time Control Panel for Creating Trace Clips

Figure 97 shows the Time Control panel for creating a Trace Clip which is essentially the process of selecting a time filter. The Trace Clip can be named using the Description text field. The rest of the facilities in the Time Control panel provide alternative ways of creating a time filter. Clicking on “OK” will create a Trace Clip corresponding to the selected time filter.

There are multiple ways to select the time interval for creating a Trace Clip.

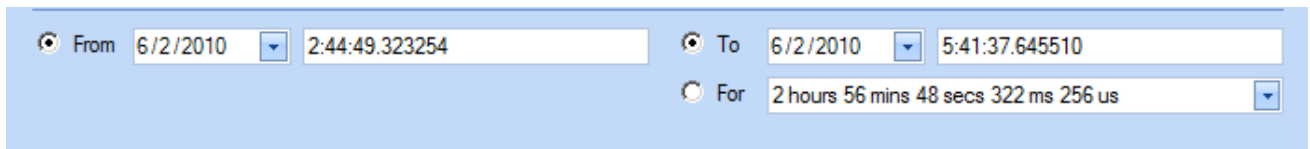


Figure 98: Trace Clip Time Selection

Selecting the Start Time for the trace clip (From) and either the absolute end time (To) or the duration of the Trace Clip from the Start Time is probably the most common way to select a Trace Clip (time interval) using the Time Control panel. The reason for this is that networking issues are most often identified by a particular onset time and duration.

Another set of options use the time “scroll” bars to select a time interval. This has the advantage of making it clear whether the selected time interval contains “Packets only” or “Packets plus Trend Data” or just “Trend Data and no Packets.”

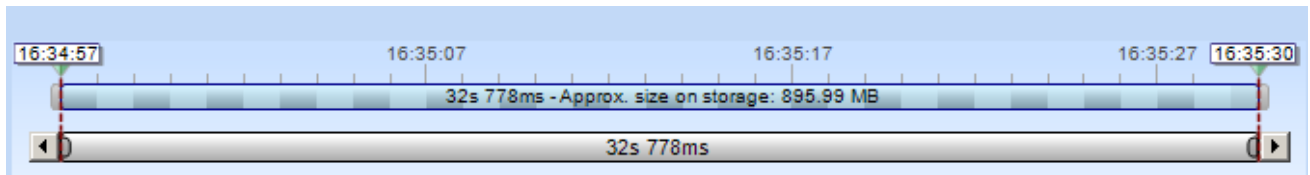


Figure 99: No Trending/Indexing Data

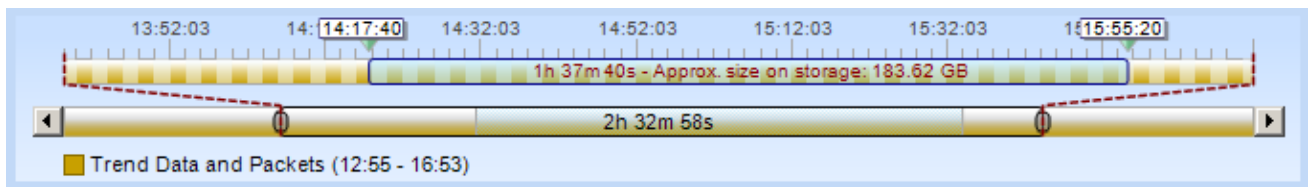


Figure 100: Complete Trending/Indexing Data and Packets

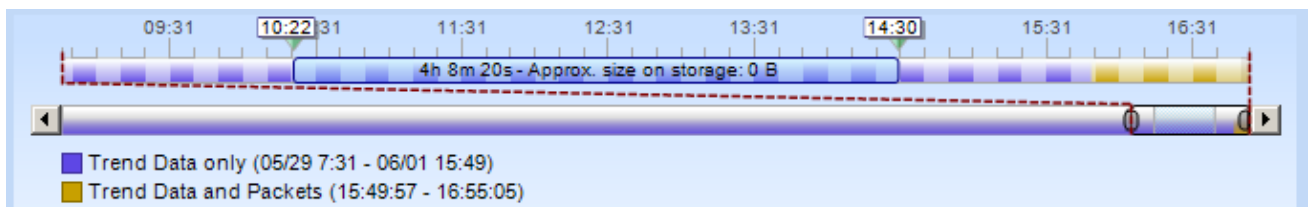


Figure 101: Trending/Indexing Data Only

The above figures show a number of possible configurations of Trending/Indexing Data and Packets.

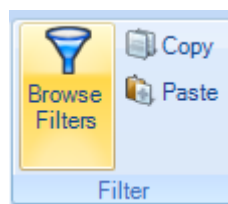


Figure 102: Bring Up Filter Editor

Lastly, In the above figure we show the “Browse Filters” button which brings up the Filter Editor for selecting a filter in addition to the time interval. In this way, the Trace Clip not only represents a time interval, but also contains a packet filter. It is important to select a filter that is compatible with the Trend Data.

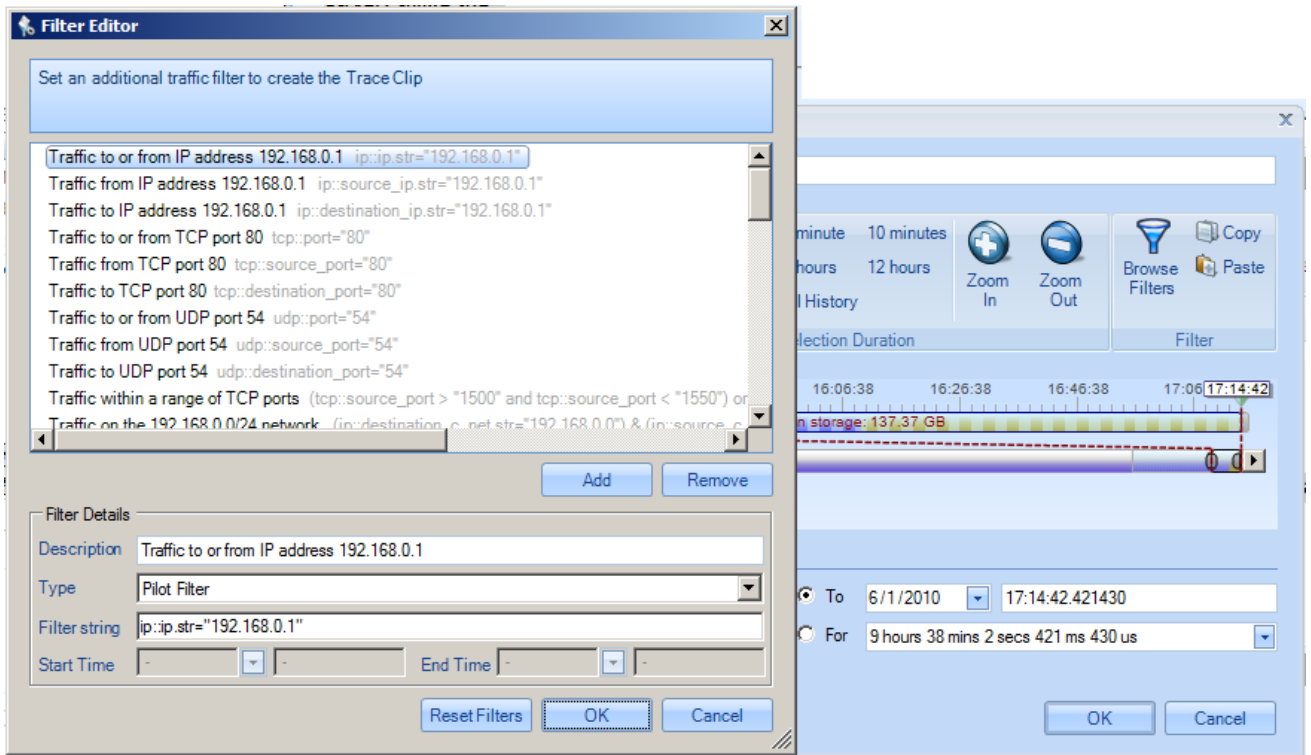


Figure 103: Filter Editor

In Figure 103 we show the Filter Editor. Note that nearly all of the filters are Pilot Filters which are compatible with the Trend Data.

Using Time Selection to Create a Trace Clip

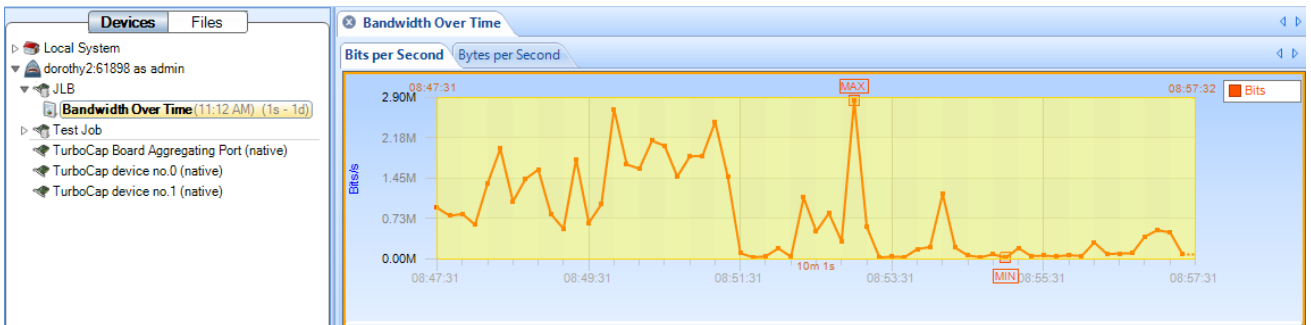


Figure 104: Time Selection in a Strip Chart

In Figure 104 we show a time selection in a strip chart. The strip chart was obtained by applying the Bandwidth Over Time view to the JLB Job Interface. In Figure 105 we switch from the Devices Panel to the Files Panel where we see the corresponding JLB Job Trace. The trace clip was created by clicking and dragging the selected time interval (in the strip chart) over the Job Trace. This automatically created the Trace Clip shown below the JLB Job Trace. Notice that the Job Trace is over 30GB, but the Trace Clip is only 256MB.

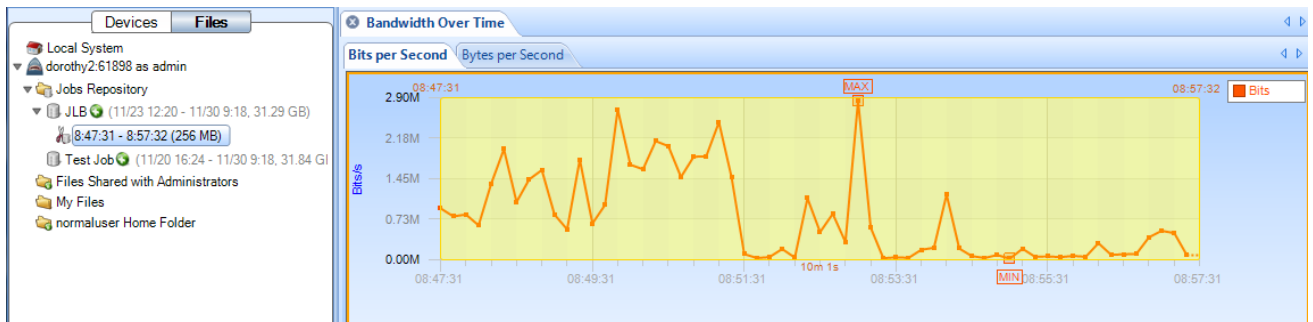


Figure 105: Time Selection Dragged Over Job Trace to Create a Trace Clip

In Figure 106 we have applied the Bandwidth Over Time view to the Trace Clip below JLB. Notice the similarity to the view in Figure 105.

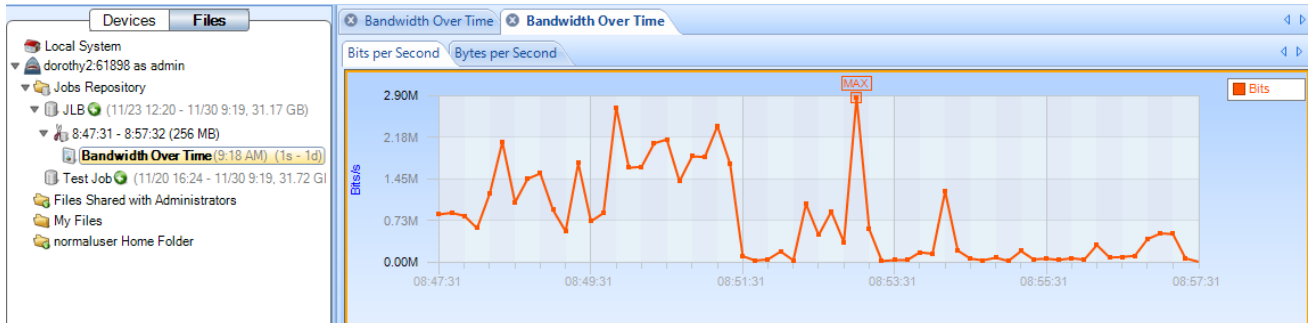


Figure 106: View Applied to a Trace Clip

Note: It is important to note that the view in Figure 105 has been obtained through the analysis of a live source while the view and Figure 106 was obtained by applying the same analysis to the packets saved in the Trace Clip. Trace Clips have all of the properties of ordinary trace files and can be analyzed using all of the capabilities of CACE Pilot.

Using Views as Job Trace Indices

The examples in the previous section show how to use a strip chart to locate time intervals of interest within a Job Trace and to easily create a Trace Clip for further analysis. This is a general technique whereby Views can be used as visual “indices” into a Job Trace.

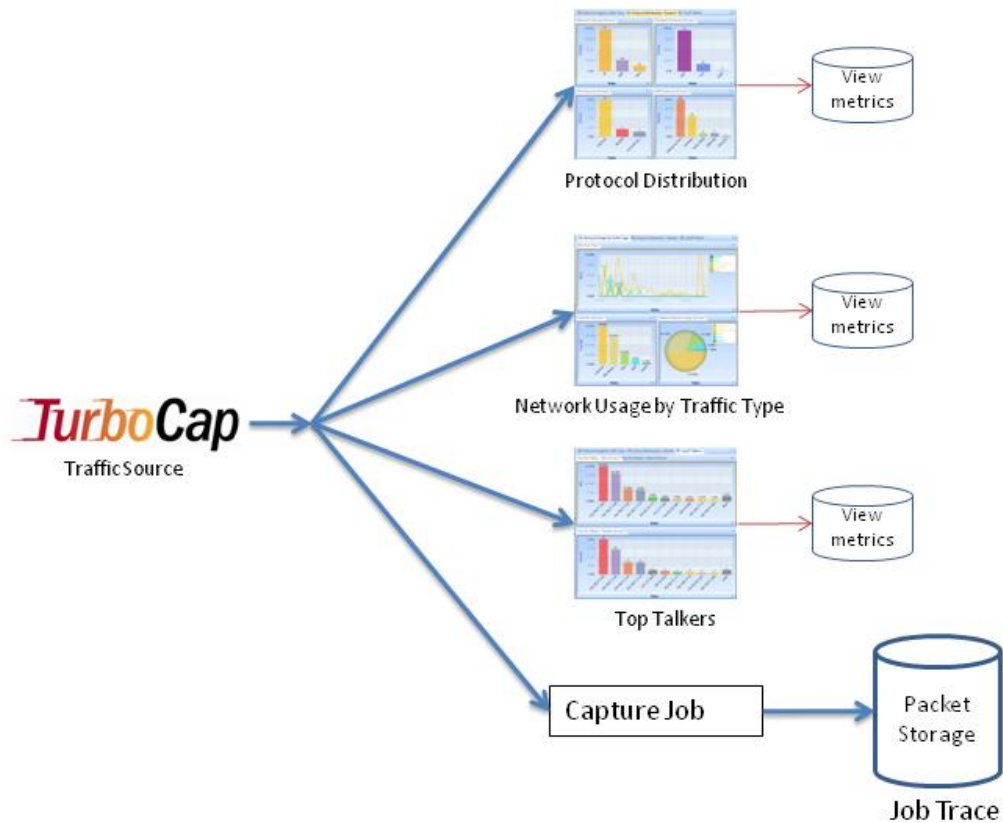


Figure 107: Visual Indices for a Job Trace

Using Events to Create Trace Clips

It is important to be able to easily locate an event in a Job Trace. This is easily accomplished by dragging the event in question over the Job Trace – a Trace Clip will be automatically containing traffic occurring before and after the event. This is illustrated below.



Figure 108: Event List

In Figure 108 we show the Event List and a particular event (4124) that has been highlighted both in the Event List and on the Strip Chart. The events were created using a Watch on the live traffic corresponding to the JLB Capture Job. Creating a Trace Clip around the (temporal) location of the event is as easy as dragging the event from the Event List to the JLB Job Trace. Dragging Event 4124 from the Event List and dropping it on the JLB Job Trace brings up the Time Control panel for creating the Trace Clip. See Figure 109.

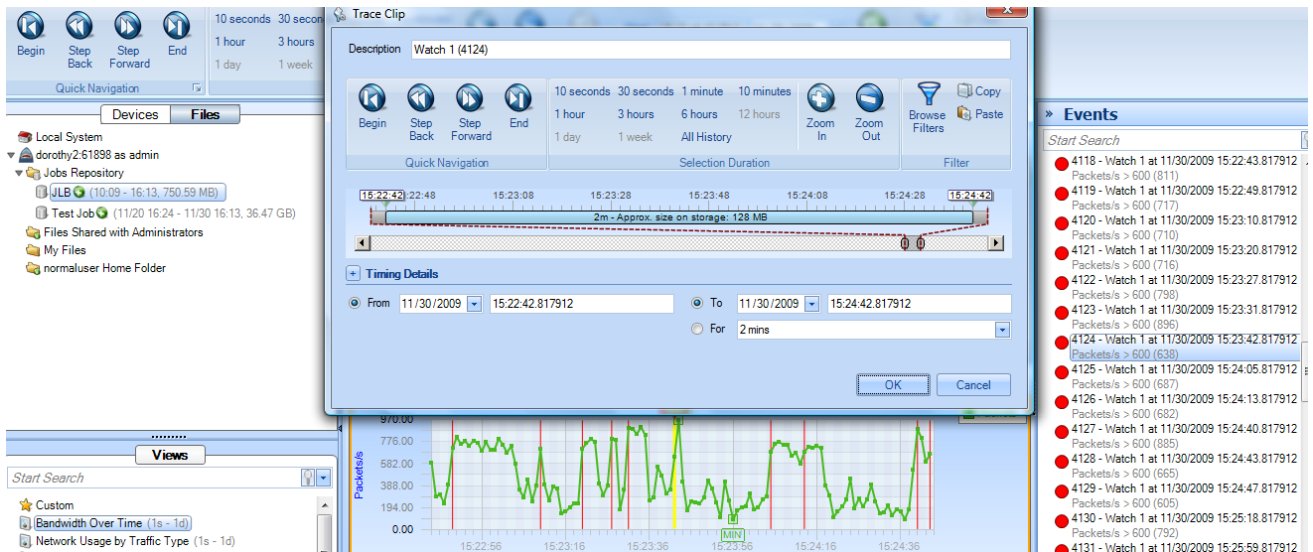


Figure 109: Creating a Trace Clip from an Event

The Time Control panel can be used to enlarge or shrink the time interval of the Trace Clip around the event. The Trace Clip is shown in Figure 110.



Figure 110: Trace Clip Corresponding to an Event

Lifetime of a Trace Clip

When a Capture Job is running, the Job Trace is either growing in size, or has reached its “Keep On Disk” limit. Once the limit is reached, the oldest captured packets will be dropped as new packets are captured. Since a Trace Clip is just a time interval associated with a Job Trace, it can happen that the packets in the Trace Clip’s time interval are eventually dropped. When this happens, the Trace Clip will indicate that there are no captured packets available for the Trace Clip.

If a View has been applied to a Trace Clip, the storage blocks associated with the Trace Clip are “locked” in storage, and will not be dropped.

Sources Panel

The Sources Panel has two tabs, namely, Devices and Files.

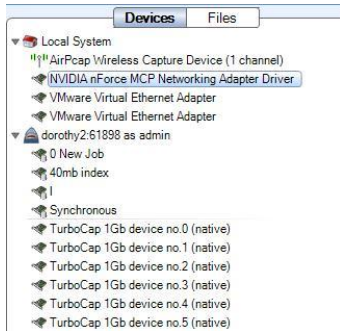


Figure 111 Sources Panel

The *Sources Panel* contains representations of Shark Appliances, live interfaces, trace files, and Capture Jobs and is one of the most important parts of the Pilot Console. It has two tabs, “Devices” and “Files”. These can be cycled through by clicking on them. The meaning of each is the following:

Devices

The Devices tab contains local interfaces under the Local System icon and Shark Appliances with their associated interface offering live sources of network traffic to the Pilot Console.

Files

The Local System with local folders and trace files plus the Shark Appliances with their associated folders and trace files.



Figure 112 Devices and Files Tabs

The Devices and Files panel has two tabs. Clicking on the tabs switches between displaying the devices and the trace files. For instance, on the left hand side and in the previous image, the “Devices” tab is selected.

Devices

The Pilot Console supports two basic classes of networking devices:

- Wired Ethernet
- Wireless (802.11)

Wired Ethernet Adapters



Icon 56 Wired Ethernet Adapter



Icon 57: Wired Ethernet Adapter associated with a Capture Job

Most wired Ethernet network interface cards work in the Pilot Console. There are two types of adapters. One presented by the actual interface -- Icon 56, and one presenting the interface corresponding to a Capture Job -- Icon 57.

Wireless Adapters



Icon 58 Wireless Adapter

Normal wireless adapters in Windows are not designed to do packet capture and analysis. CACE Technologies AirPcap adapters are made specifically to do packet capture and network analysis and are currently the only wireless adapters supported.

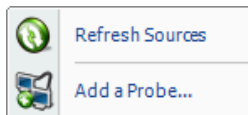
Additionally, multiple AirPcap Adapters are shown as a single device because the wireless adapters share the same airspace and, all adapters being equal, any one adapter can receive the same traffic as any other. Therefore, the Pilot Console will internally break up tasks among multiple adapters so that many channels can be scanned and locked without having to worry about which channel a particular physical adapter scans and locks on.

Note: Wireless adapters are only available on the local Pilot Console.

Context Menus in the Devices Panel

There are five types of *Context Menus* in the Devices panel which will appear under the five conditions below:

With Nothing Selected or Local System Selected



Context Menu 1 Devices Panel (No Selection)

With nothing selected, the options are as follows:

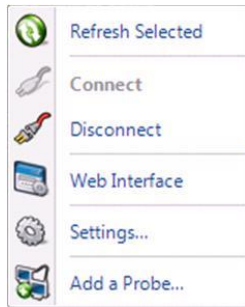
Refresh Sources

The *Refresh Sources* menu option must be executed if you want the Pilot Console to rescan the available interfaces associated with the Local System and all connected Shark Appliances during the runtime for the Pilot Console to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected Shark Appliances are rescanned and updated to reflect whether files have been removed or modified.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel.

With a Shark Appliance Selected



Context Menu 2 Devices Panel (Shark Appliance Selected)

With a Shark Appliance Selected:

Refresh Selected

The *Refresh Selected* menu option rescans the selected Shark Appliance and displays the currently available interfaces. Additionally, the trace folders associated with the selected Shark Appliance are rescanned and updated to reflect whether files have been removed or modified.

Disconnect

The *Disconnect* menu option disconnects the selected Shark Appliance from the Pilot Console. The selected Shark Appliance remains in the Probes list in the Remote ribbon.

Web Interface

The *Web Interface* menu opens the selected remote probe's Web Interface Settings.

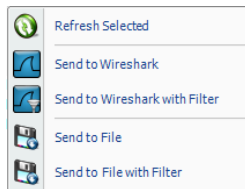
Settings

The *Settings* menu item opens the "Connect to Probe" panel showing the values used to connect to the selected Shark Appliance.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel.

With an Interface Selected (Local System or Shark Appliance)



Context Menu 3 Devices Panel (Interface Selected)

With an interface selected, the options are as follows:

Refresh Selected

The *Refresh Selected* menu option must be executed if you want the Pilot Console to rescan the available interfaces associated with the Local System and all connected Shark Appliances during the runtime for the Pilot Console to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected Shark Appliances are rescanned and updated to reflect whether files have been removed or modified.

Send to Wireshark

The *Send to Wireshark* menu option instructs the Pilot Console to start up Wireshark and send all traffic from the selected interface to Wireshark.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option instructs the Pilot Console to start up Wireshark and send all traffic from the selected device to Wireshark that matches a specified user-defined filter configured through the filter dialog box, which will appear first. The *Filter Dialog Box* is explained in a later section.

Send to File

The *Send to File* menu option instructs the Pilot Console to send all traffic from the selected device to a user-specified trace file.

Send to File with Filter

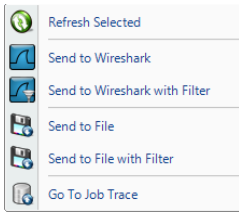
The *Send to File with Filter* menu option instructs the Pilot Console to send all traffic from the selected device to a user-specified trace file with a filter defined in the filter dialog box, which will appear first. The *Filter Dialog Box* is explained in a later section.

With a Capture Job Interface Selected (Shark Appliance)



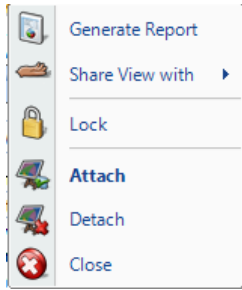
Icon 59: Capture Job Interface

With a Capture Job interface selected, the options are the same as in the previous section with the additional option to Go To Job Trace. Selecting this option takes you directly to the corresponding Job Trace in the Jobs Repository folder.

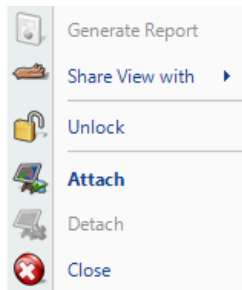


Context Menu 4: Capture Job Interface Selected

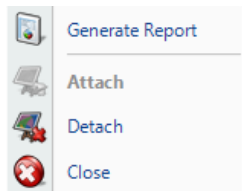
With a View Selected



Context Menu 5 Unlocked View in the Devices Panel



Context Menu 6 Locked View in the Devices Panel



Context Menu 7 Devices Panel (View Selection, Local System)

With a View Selected (Shark Appliance and Local System):

Generate Report

The *Generate Report* menu option generates a report from the selected View.

Share the View with

NOTE: The *Share the View with* menu item only applies to Shark Appliances.

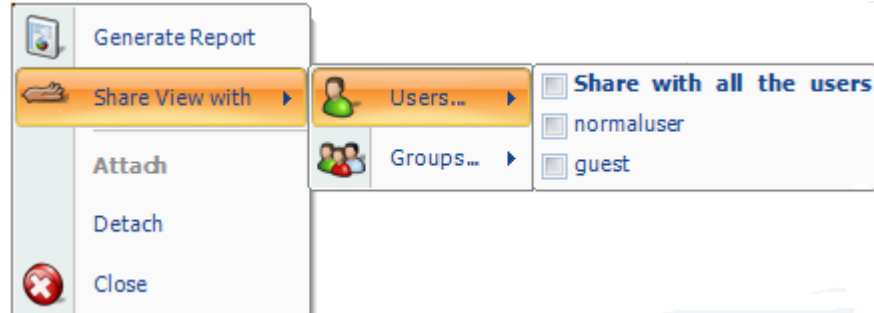


Figure 113 Sharing Views

Views applied to Shark Appliance interfaces on one Pilot Console can be shared with users located at other Pilot Consoles. The privileges associated with each user are determined on a probe-by-probe basis. Except for the administrator, a user cannot close a View or delete a file that has been created by another user. However, Views can be shared with single users or groups using the Share View with menu item. As soon as a View is shared, the selected user or group will immediately see the View in their Sources Panel.

Lock (only applies to Views in the Sources panel that are on remote Shark Appliances)

If Lock is selected, then a small lock (🔒) is added to the View icon. When the View is in the “Locked” state, it cannot be closed. When the View is in the “Locked” state, the Context menu shows an Unlock menu item. The View must be “unlocked” before it can be closed.

Attach

NOTE: The *Share the View with* menu item only applies to Shark Appliances.

If the selected View is Detached, then the *Attach* menu item will attach the Pilot Console to the View.

Detach

NOTE: The *Share the View with* menu item only applies to Shark Appliances.

If the selected View is currently Attached, the *Detach* menu option detaches the selected View.

Close

If the user is the creator of the selected View, then the *Close* menu option will close the selected View. This implies that the corresponding Shark Appliance will terminate the View and it will no longer be available to other users.

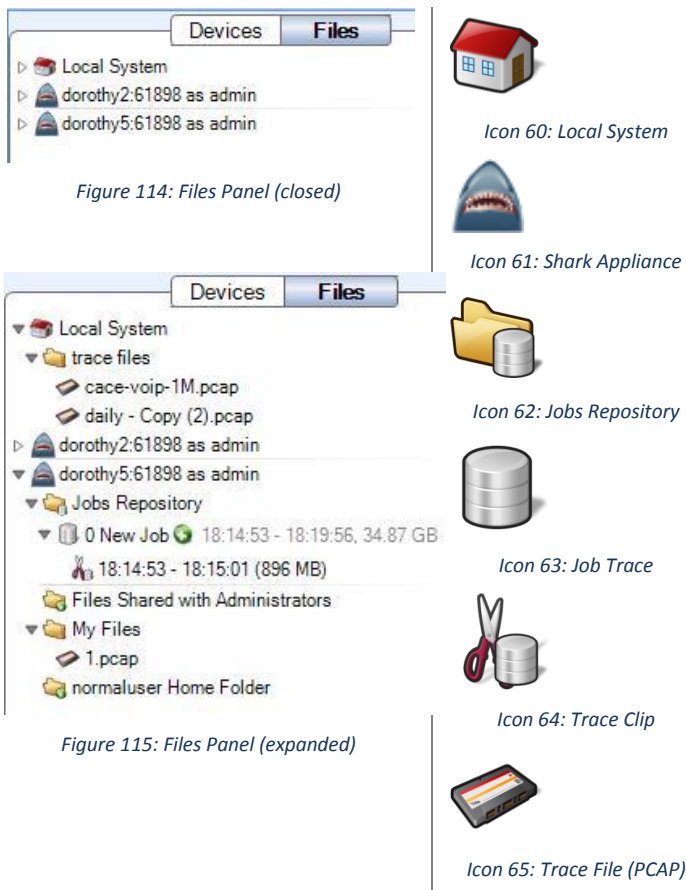
Files

The Pilot Console can analyze trace files of arbitrary size in the PCAP capture format with the following restrictions:

802.11 Wireless trace files must have either a RadioTap² or PPI³ header.

All wired trace files must have an Ethernet header. For instance, trace files created through software loopback devices, software tunnels, software based aggregators, and from non-Ethernet devices (ex. tun⁴, lo⁵, ppp⁶) will not work. In most of these instances, the traffic passing through these interfaces will eventually pass through an Ethernet interface.

Capture Jobs running on remote Shark Appliances create network traffic recordings called Job Traces. Although, Job Traces (and their derivatives, called Trace Clips) are not PCAP files, they can be analyzed by the Pilot Console exactly as if they were PCAP files. Trace Clips that exist on a Shark Appliance can be converted to PCAP format using the Send-to-File feature of the Pilot Console. The resultant PCAP file will be stored in the Shark Appliance's local filesystem.



The Files Panel contains an item for the Local System and one for each attached Shark Appliance.

We show an example file panel with all the items closed and one with all of the items expanded.

We also show the icons for each type of object depicted in the Files panel

Context Menus in the File Panel

The context menus for the File Panel are described below:

² NetBSD: http://netbsd.gw.com/cgi-bin/man-cgi?ieee80211_radiotap+9+NetBSD-current

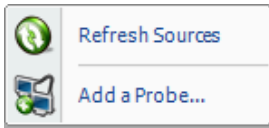
³ CACE Technologies: http://www.cacetech.com/documents/PPI_Header_format_1.0.1.pdf

⁴ FreeBSD: <http://www.freebsd.org/cgi/man.cgi?query=tun&manpath=FreeBSD+7.0-RELEASE&format=html>

⁵ FreeBSD: <http://www.freebsd.org/cgi/man.cgi?query=lo&manpath=FreeBSD+7.0-RELEASE&format=html>

⁶ FreeBSD: <http://www.freebsd.org/cgi/man.cgi?query=ppp&manpath=FreeBSD+7.0-RELEASE&format=html>

With Nothing or Local System Selected



Context Menu 8 Files Panel (No Selection)

The options are as follows:

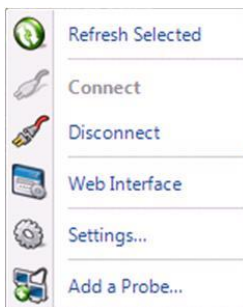
Refresh Sources

The *Refresh Sources* menu option must be executed if you want the Pilot Console to rescan the available interfaces associated with the Local System and all connected Shark Appliances during the runtime for the Pilot Console to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected Shark Appliances are rescanned and updated to reflect whether files have been removed or modified.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel.

With a Shark Appliance Selected



Context Menu 9 Files Panel (Probe Selected)

The options are as follows:

Refresh Selected

The *Refresh Selected* menu option rescans the selected Shark Appliance and displays the currently available interfaces. Additionally, the trace folders associated with the selected Shark Appliance are rescanned and updated to reflect whether files have been removed or modified.

Disconnect

The *Disconnect* menu option disconnects the selected Shark Appliance from the Pilot Console and removes it from the Devices and Files panels. The selected Shark Appliance remains in the Probes list.

Web Interface

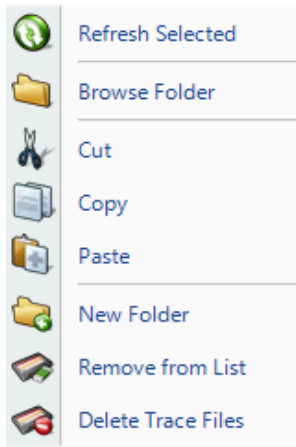
The *Web Interface* menu opens the selected remote probe's Web Interface Settings.

Settings

The *Settings* menu item opens the "Connect to Probe" panel showing the values used to connect to the selected Shark Appliance.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel



Context Menu 10 Files Panel (Trace Folder Selected on Local System)

With a trace folder selected, the options are as follows:

Refresh Selected

The *Refresh Selected* menu option rescans a folder for new trace files and updates the status of those already added.

Browse Folder

The *Browse Folder* menu option opens an explorer window pointed to the selected folder.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” folder. When the Paste operation is invoked, the folder and its contents are copied to the “paste” location and removed from the original location only if the source and destination are on the same system. If the source and destination are on different systems, then Cut behaves like a Copy operation.

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” folder. When the Paste operation is invoked, the folder is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

New Folder

The *New Folder* menu option removes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

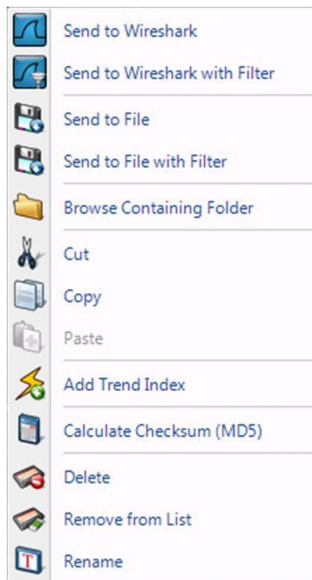
Remove from List

The *Remove from List* menu option removes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

Delete Trace Files

The *Delete Trace Files* menu option irrevocably deletes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

With A Trace File Selected on Local System



Context Menu 11 Files Panel (Trace File Selected on Local System)

With a trace file selected, the options are as follows:

Send to Wireshark

The *Send to Wireshark* menu option starts up Wireshark and sends all traffic from the selected trace file there.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option starts up Wireshark and sends all traffic from the selected trace file there that matches a specified user-defined filter configured through the filter dialog box, which will appear first. The *Filter Dialog Box* is explained in a later section.

Send to File

The *Send to File* menu option sends all traffic from the selected trace file to a user specified trace file. This is a useful function because it allows for the decryption of traffic to be exported as a decrypted trace file.

Send to File with Filter

The *Send to File with Filter* menu option sends all traffic from the selected trace file in a user specified trace file with a filter to be defined in the filter dialog box, which will appear first. This is a useful function because it can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Browse Containing Folder

The *Browse Containing Folder* menu option opens a Windows Explorer window pointed to the folder of the selected trace file.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and removed from the original location only if the paste location references the same system as the Cut operation.

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

Add/Remove Trend Index

Please refer to the Indexing section for further details

Calculate Checksum (MD5)

The *Calculate Checksum (MD5)* menu option calculates the MD5 cryptographic digest of the selected trace file and presents it in a window. This value is remembered and will be used later in tooltips and reports if applicable.

Delete

The *Delete* menu option removes the selected trace file from disk. The trace file is not sent to the recycle bin.

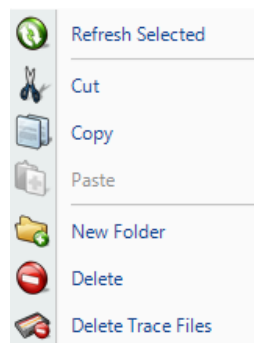
Remove from List

The *Remove from List* menu option removes the selected trace file's reference from the Files List, but not from the local file system.

Rename

The selected trace file can be renamed using the *Rename* menu option. The file name is renamed in the Files Panel and also on the local file system.

With A Trace Folder Selected on a Remote Shark Appliance



Context Menu 12 Files Panel
(Trace Folder Selected on
Remote Shark Appliance)

With a trace folder selected, the options are as follows:

Refresh Selected

The *Rescan Folder* menu option rescans a folder for new trace files and updates the status of those already added.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” folder. When the Paste operation is invoked, the folder and its contents are copied to the “paste” location and removed from the original location only if the source and destination are on the same system. If the source and destination are on different systems, then Cut behaves like a Copy operation.

Note: This option is not available for permanent folders such as “My Files”

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” folder. When the Paste operation is invoked, the folder is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

New Folder

The *New Folder* menu option removes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

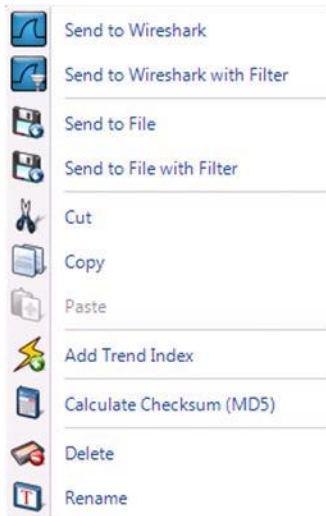
Delete

The *Delete* menu option irrevocably deletes the folder and all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

Note: This option is not available for permanent folders such as “My Files” and “Jobs Repository”

Delete Trace Files

The *Delete Trace Files* menu option irrevocably deletes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.



Context Menu 13 Files Panel (Trace File Selected on Remote Shark Appliance)

With a trace file selected, the options are as follows:

Send to Wireshark

The *Send to Wireshark* menu option starts up Wireshark and sends all traffic from the selected trace file there.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option starts up Wireshark and sends all traffic from the selected trace file there that matches a specified user-defined filter configured through the filter dialog box, which will appear first. The *Filter Dialog Box* is explained in a later section.

Send to File

The *Send to File* menu option sends all traffic from the selected trace file to a user specified trace file. This is a useful function because it allows for the decryption of traffic to be exported as a decrypted trace file.

Send to File with Filter

The *Send to File with Filter* menu option sends all traffic from the selected trace file in a user specified trace file with a filter to be defined in the filter dialog box, which will appear first. This is a useful function because it can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and removed from the original location only if the paste location references the same system as the Cut operation.

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

Add/Remove Trend Index

Please refer to the Indexing section for further details

Calculate Checksum (MD5)

The *Calculate Checksum (MD5)* menu option calculates the MD5 cryptographic digest of the selected trace file and presents it in a window. This value is remembered and will be used later in tooltips and reports if applicable.

Delete

The *Delete* menu option removes the selected trace file from disk. The trace clip cannot be deleted if there is one or more Views currently applied to the trace clip.

Rename

The selected trace file can be renamed using the *Rename* menu option.

With The Jobs Repository Folder Selected on a Remote Shark Appliance

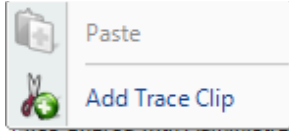


Context Menu 14: Jobs Repository Folder

Refresh Selected

The *Rescan Folder* menu option rescans a folder for new trace files and updates the status of those already added.

With A Job Trace Selected on a Remote Shark Appliance



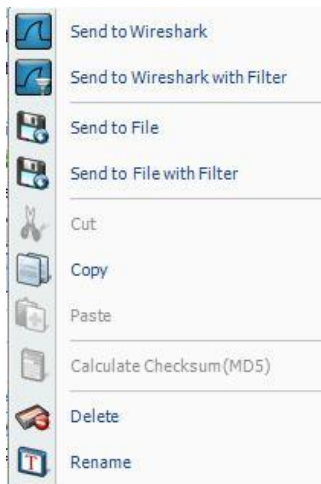
Context Menu 15: Job Trace

With a Job Trace selected, the options are as follows:

Add Trace Clip

The *Add Trace Clip* menu option brings up the Trace Clip time selection panel.

With A Trace Clip Selected on a Remote Shark Appliance



Context Menu 16: Trace Clip

With a Trace Clip selected, the options are as follows:

Send to Wireshark

The *Send to Wireshark* menu option starts up Wireshark and sends all traffic from the selected trace clip there.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option starts up Wireshark and sends all traffic from the selected trace clip there that matches a specified user-defined filter configured through the filter dialog box, which will appear first. The *Filter Dialog Box* is explained in a later section.

Send to File

The *Send to File* menu option sends all traffic from the selected trace clip to a user specified trace file. This is a useful function because it allows for the decryption of traffic to be exported as a decrypted trace file.

Send to File with Filter

The *Send to File with Filter* menu option sends all traffic from the selected trace clip in a user specified trace file with a filter to be defined in the filter dialog box, which will appear first. This is a useful function because it can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Copy

The *Copy* menu option obtains a time filter corresponding to the time interval associated with the trace clip.

Delete

The *Delete* menu option removes the selected trace clip.

Rename

The selected trace file can be renamed using the *Rename* menu option.

The context menu for a view applied on a file is the same as the context menu of view applied on a device. Please refer to the paragraph: "With a View Selected" in the Device Panel section.

Views Panel

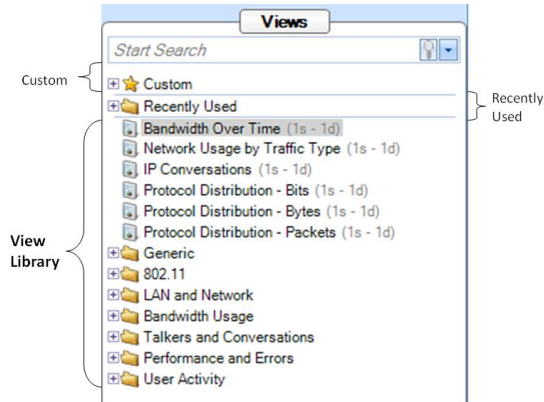


Figure 116 Views Library

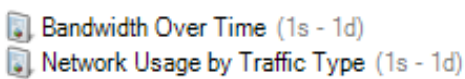






Figure 117 Instance of a View

A Pilot Console View represents a specific set of calculations that can be applied to both live and off-line (trace files) sources. The calculations associated with a View are called the View metrics. These metrics are visually presented to the user in terms of Charts. Charts graphical elements within a Chart are selectable such as bars within a bar chart and time intervals within a strip chart, etc.

Each view is depicted in the following format:

[Icon] [Name] ([Sampling Time] - [Data Retention Time])

For example, in Figure 117:

- The Icon denotes the link type(s) of the source to which the View applies.
 -  all link types
 -  wired Ethernet
 -  Capture Job wired Ethernet
 -  802.11 link type
- The View's name is "Bandwidth Over Time"
- The Sampling Time is 1 second and so the associated metric (average bandwidth over time) is computed for every second.
- The Data Retention Time is 1 day (1d), which means that once a day's worth of samples are calculated, the oldest samples will be dropped as new samples are calculated. This parameter is only used for live sources. In the case of trace files, all of the samples over the duration of the trace file are retained.

The above parameters can be changed and multiple instances of a view can exist with different parameters by utilizing the custom views as explained below. The name of the custom view can also be changed to whatever is desired.

The Views panel above has four sections, which from bottom to top are:

- View Library
- Recently Used
- Custom Views
- Search Text Box

Regular Views, Fast Views, and Forbidden Views

When Views are applied to Sources that have associated Trending/Indexing Data, these Views will run very quickly on huge Indexed Trace Files and Trace Clips with Trending/Indexing Data. When a source is selected, the Icons for the Views change to indicate whether they run as regular views (no lightning icon), fast views (lightning icon), or forbidden (red “X”). The forbidden views are those that cannot be run with the Trending/Indexing data alone. The ordinary views are those that cannot be run with the Trending/Indexing data alone, but the actual packets are available for the View calculation.

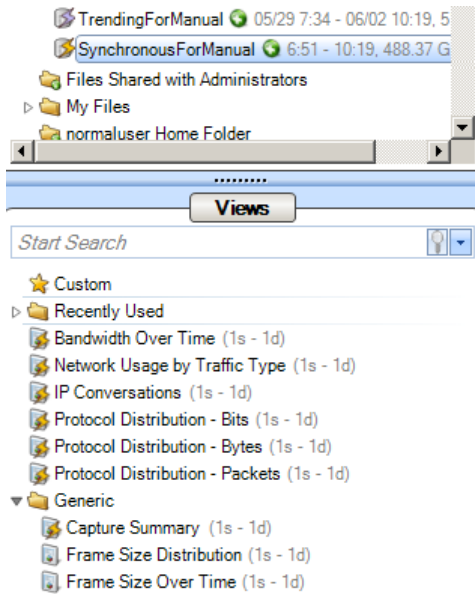


Figure 118: Fast Views

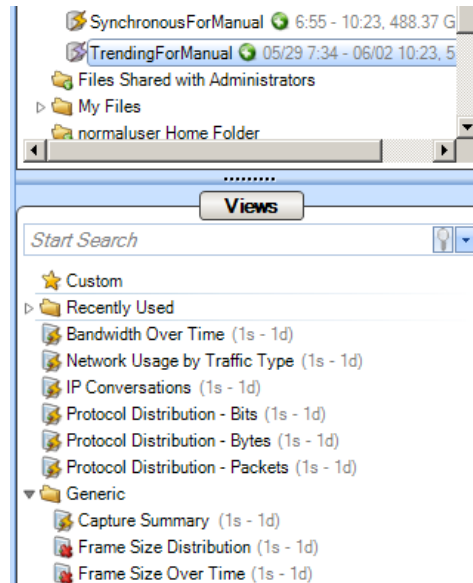


Figure 119: Disallowed Views

Using Views

Views are applied to one of the following:

- Devices, Trace Files, or Trace Clips
- Selections within Charts (also known as Drill Down)

Note: Not all Views can be applied to all devices, trace files, trace clips, or selections and therefore, the operation is sometimes forbidden. This is because certain Views are not applicable in certain contexts. For instance, a wired Ethernet device won't have signal to noise ratio of 802.11 channels.

Applying a View (Local or Remote Sources)

Views can be applied to a device, trace file, or trace clip in the following ways:

Double Clicking on a View

When double clicking on a view, it is applied to the currently selected device or file, depending on which tab is open.

Pressing Enter on a View

This operation has identical consequences to the double click previously described.

Dragging the View on to the Device, File, or Selection within a Chart

This is similar to the above method; however, a view can be dragged on to any device or file. Additionally, after doing a selection within a chart, a view can be dragged on to the selection. The view will be applied to the subset of data that is selected.

When a view is dragged onto a source or selection two different icons can be displayed on the cursor:



Figure 120: Apply Icon



Figure 121: Do Not Apply Icon

- Figure 120 means the view metric can be applied to the source

- Figure 121 means that the view metric cannot be applied to the source.

Drill Down button in the Home Ribbon and Chart context menu option

The effects the same result as applying a view to a selection as described above, however, achieved through a different set of operations. Every chart has a context menu option of “Drill Down” that lists the Custom, Recently Used, and View Library. This context menu option is enabled when a selection is made in the chart. Selecting one of the views results in the view being applied to the subset of data selected. The drill-down menu button works identically and is there to accommodate different usage patterns.

Applying a View with a Filter

The first three ways of selecting a view have a special meta-command operation. When holding down the control key and applying a view either by

- Double Clicking
- Pressing Enter
- Dragging and Dropping

A filter dialog box opens. At this point, a filter can be specified with which the View will be applied. The Filter Dialog is explained in Filter Dialog section.

Note: Application of a View with a Filter does not apply to the drill down operation. The reason for this is that the basis for the drill-down is the visual selection within a Chart which already represents a filtering operation.

When a view is dragged onto a source with a filter two different icons can be displayed on the cursor:



Figure 122: Apply Icon



Figure 123: Do Not Apply Icon

- Figure 120 means the view metric can be applied with filter to the source

- Figure 121 means that the view metric cannot be applied to the source.

View Library

The *View Library* is the main repository of all the views available in the Pilot Console.

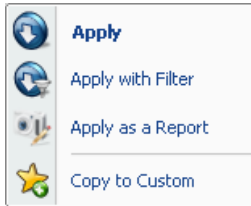
Views are divided into folders which are, in some cases, further subdivided.

Context Menus

The view library has two types of context menus. They are triggered when right clicking on either of the following:

- Folder
- View

Folder



Context Menu 17 View Library Folder

The context menu for a folder in the view library section has the following options:

Apply

The *Apply* menu option applies all the views in the currently selected folder to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the currently selected folder to the selected device or file in the Devices and Files panel with a specified filter. The Filter Dialog (described later) pops up when this option is selected.

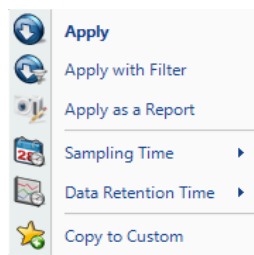
Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “All Views” option as all the views in the currently selected folder applied to file selected in the Files panel. This menu option is disabled when a device is selected.

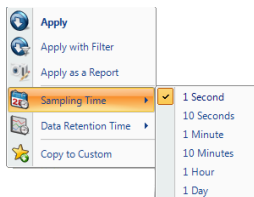
Copy to Custom

The *Copy to Custom* menu option copies the currently selected folder to the Custom folder (described later).

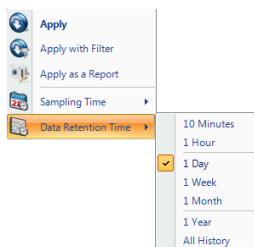
View



Context Menu 18 View Library View



Context Sub Menu 1 Sampling Time



Context Sub Menu 2 Data Retention Time

The context menu for a view in the view library section has the following options:

Apply

The *Apply* menu option applies the selected view to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies the selected view to the selected device or file in the Devices and Files panel with a specified filter. The Filter Dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “All Views” option to the selection view applied to the file selected in the Files panel. Apply as a Report cannot be applied to a live interface.

Sampling Time

The *Sampling Time* menu option is very important. It specifies the ultimate granularity in time of the calculation of the corresponding View metric. All of the metrics shown refer to those that are calculated with reference to a specific time period; by default, usually a second. However, this time period is variable and can be changed to other values (which are shown in the contextual submenu). The value selected is shown at the end of the textual representation of the views in the Views Library along with the Data Retention Time value (described next).

Data Retention Time

The *Data Retention Time* and the Sampling Time menu options are very important options that determine the calculation of View metrics for live sources. The Data Retention Time value is the time period of the View metric history that is retained for a View applied to a live source. Once the Data Retention Time is reached, the oldest View metrics are discarded as new sample points are calculated. The Data Retention time has no effect on the duration of the View metrics retained for trace files. In the case of trace files, the complete View metric over the duration of the trace file is retained.

Copy to Custom

The *Copy to Custom* menu option copies all the views in the currently selected folder to the Custom section (described later).

Tooltips

Tooltips for the View Library act as documentation for the views. They are made visible by hovering over the icon for a view or folder.

Recently Used

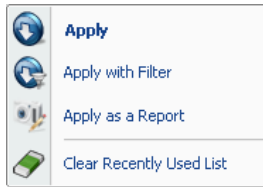
The Recently Used folder contains the five most recently used views. The Recently Used folder is not shown when the folder is empty. This is the case when the Pilot Console is started and whenever the Clear Recently Used List menu item is selected.

Context Menus

The Recently Used section has two types of context menus. They are triggered by right clicking on either of the following:

- Recently Used Folder
- View within the Recently Used Folder

Recently Used Folder



Context Menu 19 Recently Used Folder

The context menu for a folder in the recently used section has the following options:

Apply

The *Apply* menu option applies all the views in the recently used folder to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the recently used folder to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option will automatically create a report with the “All Views” option as all the views in the recently used folder applied to the file selected in the Files panel. Apply as a Report cannot be applied to a device.

Clear Recently Used List

The *Clear Recently Used List* removes the references to all of the views in the Recently Used folder.

The Context menus for Views within the Recently Used Folder are identical to those when applied to Views in the View Library.

Custom Views

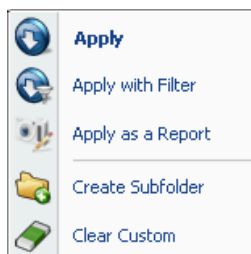
Custom Views are the regular views in the views library with different settings. At the view level, the chart window positions and sizes are saved. At the chart level it varies. In the description of the charts it is noted whether the option is saved or not in a custom view.

Context Menus

The Custom section has two types of context menus. They are triggered when right clicking on either of the following:

- Folder (including the root “Custom” folder with the star icon)
- View

Custom Folder



Context Menu 20 Custom Folder

The context menu for the Custom folder has the following options:

Apply

The *Apply* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “All

Views” option as all the views in the selected folder in the custom section applied to the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

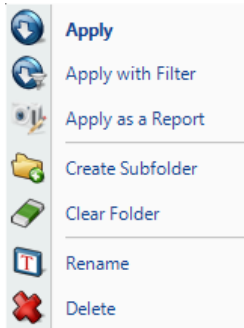
Create Subfolder

The *Create Subfolder* opens a dialog that prompts for the name of a to-be created subfolder in the custom section.

Clear Custom

The *Clear Custom* menu option removes the references to all of the views in the selected folder in the custom section.

Folder within the Custom Folder



Context Menu 21 Custom Folder

The context menu for a folder within the Custom folder has the following options:

Apply

The *Apply* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “All Views” option as all the views in the selected folder in the custom section applied to the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

Create Subfolder

The *Create Subfolder* opens a dialog that prompts for the name of a to-be created subfolder in the custom section.

Clear Folder

The *Clear Custom* menu option removes the references to all of the views and sub folders in the selected folder in the custom section.

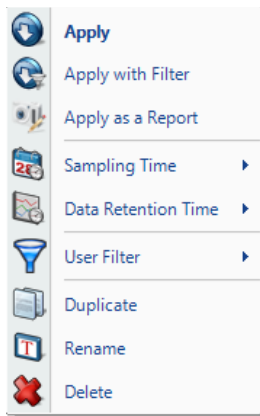
Rename

The Rename menu option prompts for the new name for the folder.

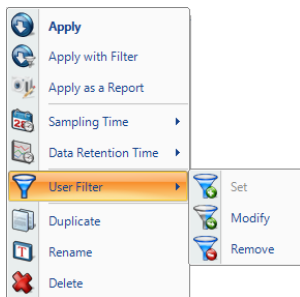
Delete

The Delete menu option will delete the folder and all of its contents.

View within Custom Folder (or Sub Folder)



Context Menu 22 Custom View



Context Sub Menu 3 User Filter

The context menu for a view in the Custom section has the following options:

Apply

The *Apply* menu option applies the selected view to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies the selected view to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “Current View” option as the selected view for the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

Sampling Time

The *Sampling Time* menu option is very important. It specifies the ultimate granularity in time of the calculation of the corresponding View metric. All of the metrics shown refer to those that are calculated with reference to a specific time period; by default, usually a second. However, this time period is variable and can be changed to other values (which are shown in the contextual submenu). The value selected is shown at the end of the textual representation of the views in the Views Library along with the Data Retention Time value (described next).

Data Retention Time

The *Data Retention Time* and the *Sampling Time* menu options are very important options that determine the calculation of View metrics for live sources. The *Data Retention Time* value is the time period of the View metric history that is retained for a View applied to a live source. Once the *Data Retention Time* is reached, the oldest View metrics are discarded as new sample points are calculated. The *Data Retention time* has no effect on the duration of the View metrics retained for trace files. In the case of trace files, the complete View metric over the duration of the trace file is retained.

User Filter

The *User Filter* menu option sets a permanent filter associated with the view so it does not need to be specified each time. Clicking on *Set* brings up the *Filter Dialog* which is described later. After a filter is set, the menu options of *Modify* and *Remove* are enabled, and their functions are self-explanatory.

Duplicate

The *Duplicate* menu option duplicates the reference to a view so that different options can be saved for a view.

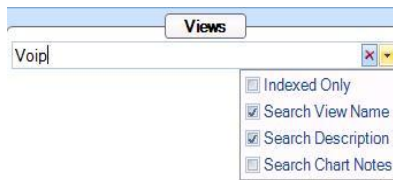
Rename

The *Rename* menu option allows a reference shown in the Custom section to be named to whatever is desired.

Delete

The *Delete* menu option deletes the selected view in the Custom section. All settings for the custom view are lost.

Search Text Box



Context Menu 23 View Panel Search

The Search Box is used to locate Views for specific purposes. In the figure, we have typed VoIP. This search will find all of the Views that have “VoIP” in either the View Name or the View Description. The drop-down check box also allows searches over the Chart Notes of all the charts that are part of a View.

The Search box is a convenient way to find the View that you are looking for. In a sense, it provides an alternative ways of organizing the View Library.

Indexing

Indexing a Trace File

Indexing allows improving performances of several views by 100x to 1000x factor. Loading the index does not take much more time than loading a single view, thus it can be very useful if you have a single large file and you want to apply several views on it. After applying an index to a trace file each supported view is accelerated. Indexes can be applied to any existing trace file except Wi-Fi files. The indexed file shows a small yellow lightning icon on it when the operation is successfully completed. If, for any reason, the index is not completely loaded a red lightning arrow appears on the top of the trace file icon. When the index is applied, it is always possible to see which views are accelerated by the index. Indeed, when an indexed file is selected in the source panel all the views supporting that index show a small yellow lightning icon on the top of them.

Apply an Index to a Trace File

An Index can be applied to a trace file using Add an Index button in the trace file context menu option.

Context Menu

Add Trend Index

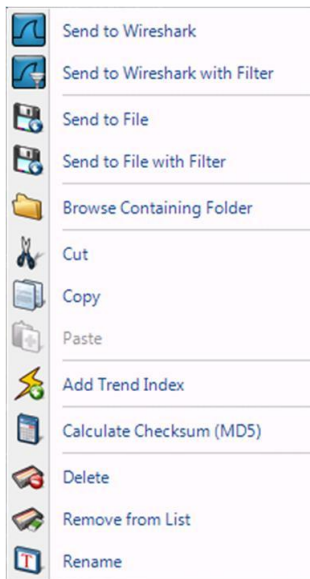


Figure 124 Add Trace Index context menu



Figure 125: Add Trend Index

The context menu for a Trace File without index shows:

[Add Trend Index](#)

The *Add Trend Index* menu option creates an Index on the selected file.

Interrupt Trend Index

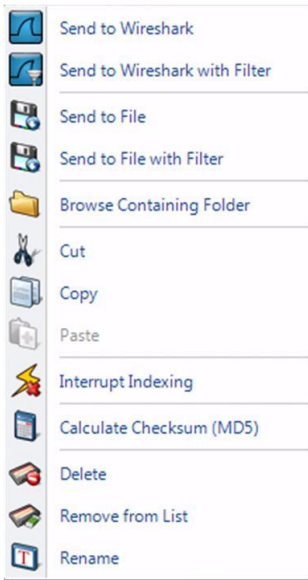


Figure 126 Add Trace Index context menu



Figure 127: Interrupt Indexing

The context menu while the index on a Trace File is created shows:

Interrupting Indexing

The *Interrupting Indexing* menu option interrupts the creation of an Index while it is being created

If the action succeeds over the file will be displayed Figure 131.

Remove Trend Index

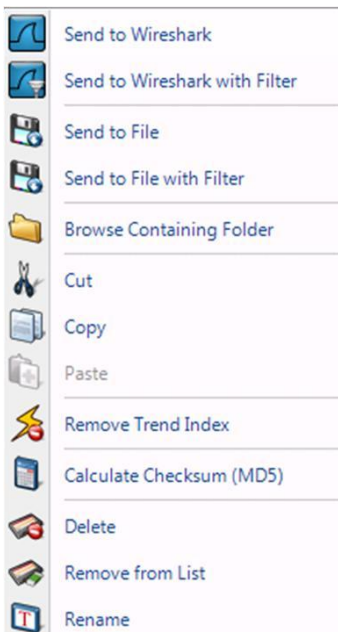


Figure 128 Remove an Index context menu



Figure 129: Remove Trend Index

The context menu for a Trace File with an index applied on it shows:

Remove Trend Index

The *Remove Trend Index* menu option removes the current Index from the selected file.

Index Icons on Trace Files



Figure 130: Index Applied

Index Applied means that the index has been applied successfully and the views will be faster when applied.



Figure 131: Index Broken

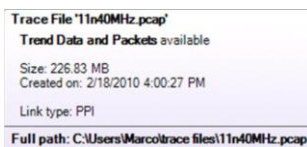
Index Not Working means that either the file does not support the index (e.g. a Wi-Fi file) or the index was interrupted before completion. To display the cause of the broken index a text in gray appears on the right of the trace file:

- *Indices not supported on wireless sources*
- *Index not complete*

Tooltips

Tooltips for the Trace Files with Indexes act as documentation for the views. They are made visible by hovering over the icon for a view or folder.

File



Tooltip 1 Indexed File Tooltip

The *Indexed File* tooltip shows the full path of trace file the mouse is hovering over along with the three metrics:

Trend Data and Packets available

The index has been applied and both accelerated trend data and detailed packet data are available for this trace file.

Trace File

It is the name of the file.

Created On

The date the trace file was created on.

Size

The kilobyte size of the trace file.

Link Type

The link type of the trace file. This is important because not all views can be applied on all files. If the Link type is PPI Pilot indexing feature does not work.

Apply a View to a Indexed Trace File

Views can be applied to an indexed trace file in the usual ways. For more information on how to apply a view refer to the

With a View Selected

The context menu for a view applied on a file is the same as the context menu of view applied on a device. Please refer to the paragraph: "With a View Selected" in the Device Panel section.

Views Panel section. The following drag and drop cursor is shown when you drag a supported view on a indexed Trace File.

Drag and Drop Cursors for Indexed Trace Files



Figure 132: Drag and Drop cursor for Indexed Files

In the figure the *Drag and Drop cursor* for indexed Trace Files

Search Text Box



Context Menu 24 View Panel Search

The Search box has an option to find only views that support indexing. Figure 132 shows how to select this option.

Main Workspace

The *Main Workspace* uses tabbed windows which will usually be referred to as “views” or the more general term “tabs”. A View consists of a number of Charts – the View depicted below consists of a strip chart, a bar chart, and a conversation ring. In general, the specific analyses supported by a View are displayed in the Charts that make up the View.



Figure 133 A View in the Main Workspace

Each View has a main tab that contains the *View Title*. Each of the Charts that make up a View has its own tab.

The Time Control window along the bottom edge of the View provides two time intervals, namely, the *Current Selection* interval and the *Total Window* interval.

- *Current Selection*: The Charts that comprise the View display the View metrics computed over the *Current Selection* interval. The duration following the “@” sign has the following interpretations. For a live View, the interval following the “@” sign is the time between the updates to the View metrics. If one of the Charts in the View is a strip chart, then this value is the subsampling interval for the points in the strip chart. For all other Chart types, this value is not used.
- *Total Window*: In the case of a live source, the *Total Window* is the duration from when the View was first applied until the current time. In the case of a trace file, the Total Window is the interval of time over which the trace file was captured.

Context Menus



Figure 134 Chart Context Menu Overview

Each chart has a context menu that is specific to that chart. However, with few exceptions, all charts share certain options in their context menus:

- Export and Drill Down Operations
- Search over Charts
- Add Watch (only available in Strip Charts and Bar Charts)
- Chart-Specific Operations
- General Chart and Selection Operations

None of these menu options are described here and are instead, elaborated on a per chart basis.

Tooltips

Since some of the methods of data display afford solely qualitative comparison, tooltips are available on some charts to give a quantitative representation of what is graphically displayed.

Notes

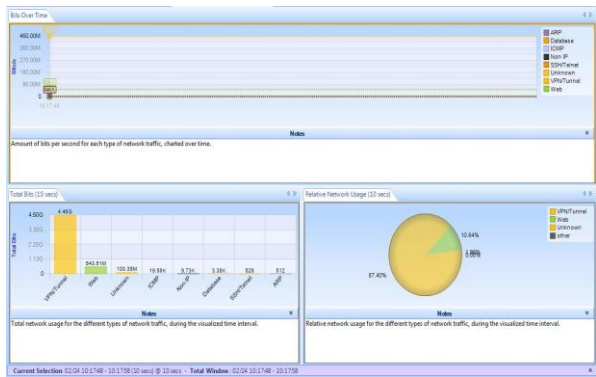


Figure 135 View With Collapsed Notes

Every chart has a section that can be used to place notes that will be included in a generated report and if applicable, saved in a custom view.

In the view on the left, all the note areas are expanded

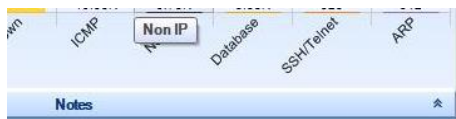
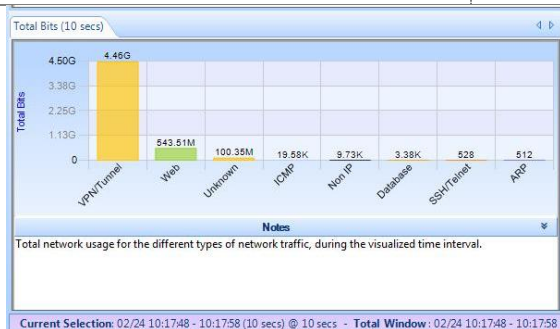


Figure 136: View Notes Toggle Button

Each chart has a long horizontal bar with a small arrow on the right bottom border.



When clicked, a text area will appear under the associated graph for text. There is a default description for each graph provided. The text in the notes section is included in generated reports and the notes are saved in a custom view.

Selection

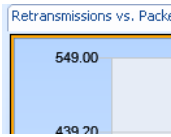


Chart Figure 1 Chart Selected

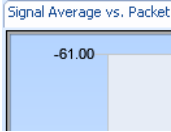


Chart Figure 2 Chart Not Selected

There is a notion of chart selection. This is important for the search button in the Home Ribbon, among other things.

A chart is selected when there is an orange border around it, as depicted to the left. In any view, there is at most one chart selected at any given time.

Mini

Every Chart has a large view with legends and controls, and a mini view with just the graphic itself. The miniature shows up when there is not enough space to display the standard view. In a mini view, none of the elements can be selected and there is no contextual menu.

Conversation Ring

In the *Conversation Ring*, “conversation” endpoints are placed around an ellipse. The Conversation Ring is used where “stations”, represented by the endpoints, communicate (have a conversation) with each other. The endpoints are depicted as circles with a line connecting a pair of endpoints signifying that two endpoints are communicating with each other. The size of the endpoint and the size of the line are proportional to how much traffic occurs over a given time period. End points and lines that have changed in the last update interval are shown in green.

Default

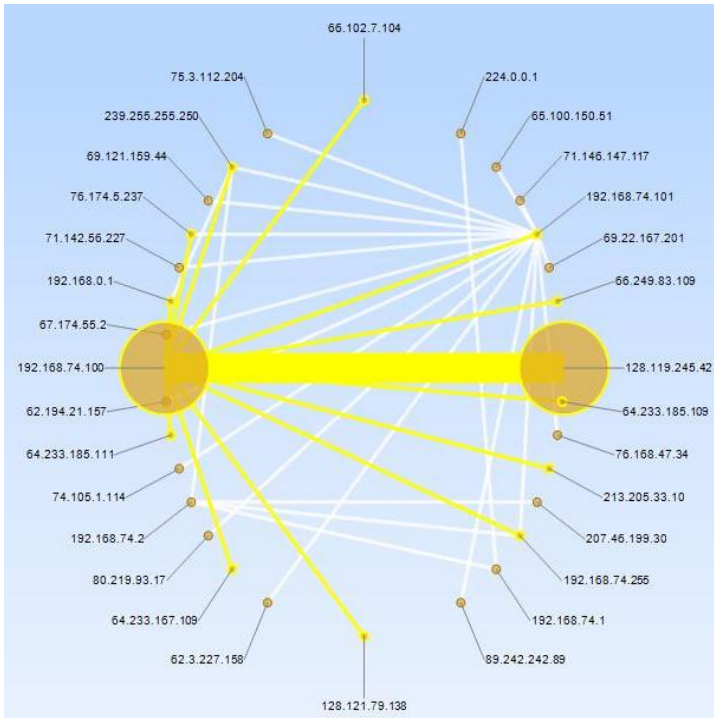


Chart Figure 3 Conversation Ring

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Conversation Ring is customizable in the following ways:

- Magnification with the scroll wheel
- Endpoint color
- Name resolution
- Option of transited bytes or packets to signify endpoint and connection size

There are four distinct mouse based operations for the conversation ring:

- Scroll Wheel
- Hover
- Selection
-

Size Legends



Chart Figure 4 Size Legends in a Conversation Ring

In the top right of the view, the Conversation Ring view shows two size legends that represent the maximum, average and the minimum traffic in all the current endpoints and conversations. An example is shown in the figure besides.

Scroll Wheel

The mouse *scroll wheel* is used to change the magnification level of the conversation ring. This is useful when there endpoints are densely distributed and can't be discerned.

Hover with Tooltip

A hover is when the mouse is over what can be selected, but not clicked. A hover highlights all the connections associated with an endpoint or all the endpoints associated with a connection. The hover operation causes a tooltip to pop up (described later) giving quantitative information regarding a connection or endpoint. Further, while hovering over an endpoint the Size Legends display the current traffic value in red.

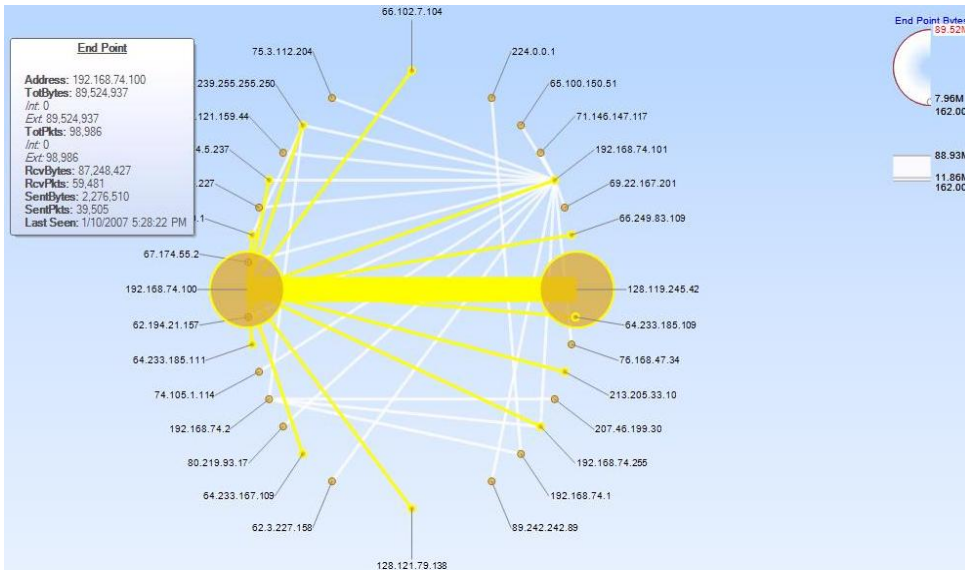


Chart Figure 5 Conversation Ring Hover

Selected

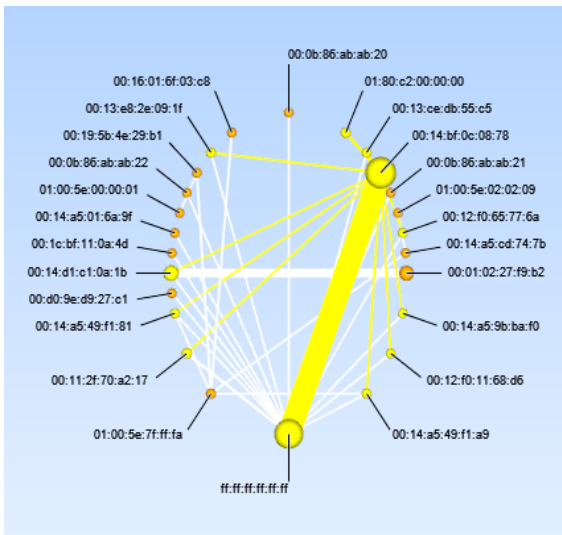


Chart Figure 6 Conversation Ring Selection

Selection in a Conversation Ring is done by clicking on an endpoint or connection. When clicking on a connection, the connection and the associated endpoints become selected. When clicking on an endpoint, all of the connections with that endpoint and the associated endpoints on the other side of the connections become selected.

Control+click is supported for multiple endpoint or connection based selections (which can be mixed).

Top Conversations

Top 53 Conversations (99.77% of Total Bytes)  

Chart Figure 7 Conversation Ring Top Conversations

When there is not enough space to display clearly all the conversations in a single ring, Pilot automatically selects data by relevance. A small label displaying the number of conversations and the percentage of data that are visible appears at the bottom of the view. The number of endpoints in the view can be increased or decreased using the two small yellow + and - buttons.

Mini

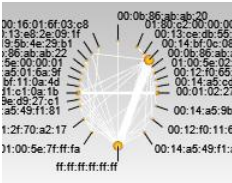
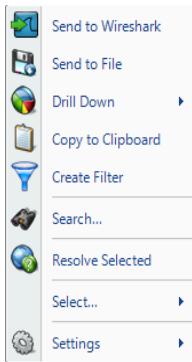


Chart Figure 8 Conversation Ring Mini

This is the miniature view of the Conversation Ring. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Context Menu



Context Menu 25
Conversation Ring
(Selection)

The context menu for the Conversation Ring is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected endpoint(s) and connection(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected endpoint(s) or connection(s) to a user-specified trace file which will appear, after completion, in the Files panel, for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected endpoint(s) or connection(s) and opens a new view tab in the main workspace.

Copy to Clipboard

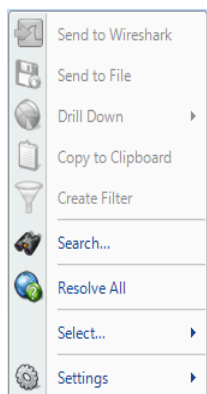
The *Copy to Clipboard* menu option copies tabular values pertaining to the current selection to the clipboard. These are copied in the order that the hosts were discovered in the conversation ring. The data in each row is the same as the data available in that elements tooltip (described below) and ordered left-to-right as the tooltip is ordered top to bottom. For instance, since the endpoint's tooltip is displayed "Address, TotBytes, TotPkts" etc, a single copied row will have a corresponding listing, ordered by tabs. The only exception to this rule is that the "Last Seen" value is not included in what is copied to the clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be



Context Menu 26
Conversation Ring (No
Selection)



searched. The Search Dialog is described in its own section later on.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves the names for the types of things not specified in the Name Resolution menu – since the selected options are resolved automatically.

Select

The *Select* menu option has two submenu options to either select all the connection(s) and endpoint(s) in the Conversation Ring, or to invert the current selection of the endpoint(s) and connection(s).

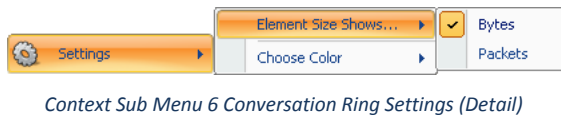
Settings

The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menus

The Conversation Ring has the following contextual submenus:

- Settings



The Conversation ring has the following settings:

- Element Size Shows
- Choose Color

Element Size Shows

The endpoint(s) and connection(s) are drawn in a size which is proportional to the relative quantitative values of either the number of bytes or the number of packets received in a specific time period. This submenu can change that option.

Choose Color

The *Choose Color* contextual submenu is used to change the color of the endpoints.

Tooltips

The conversation ring has two kinds of tooltips:

- Connection Based
- Endpoint Based

Endpoint

```
End Point
Address: 192.168.74.100
TotBytes: 89,524,937
Int: 0
Ext: 89,524,937
TotPkts: 98,986
Int: 0
Ext: 98,986
RcvBytes: 87,248,427
RcvPkts: 59,481
SentBytes: 2,276,510
SentPkts: 39,505
Last Seen: 1/10/2007 5:28:22 PM
```

Tooltip 2 Conversation Ring
Endpoint

When hovering over an endpoint, a tooltip pops up with the following fields:

Address

The *Address* refers to the associated MAC or IP address (as applicable) of the endpoint. This value can be useful if it is still needed after a name resolution takes place.

ResAddr

The *ResAddr* refers to the Resolved name of the of the endpoint.

TotBytes

The *TotBytes* refers to the total number of bytes that have transited either in or out of that endpoint. It is the sum of the *RcvBytes* and the *SentBytes*.

Int and *Ext* are another representation of *SentBytes* and *RcvBytes*.

TotPkts

The *TotPkts* refers to the total number of packets that have transited either in or out of that endpoint. It is the sum of the *RcvPkts* and the *SentPkt*.

Int and *Ext* are another representation of *SentPkts* and *RcvPkts*.

RcvBytes

The *RcvBytes* refers to the total number of bytes received at that endpoint over a given sample period, i.e. the sum packet size of all packets wherein the endpoint was the destination field in the packet.

RcvPkts

The *RcvPkts* refers to the total number of packets received at that endpoint over a given sample period, i.e. the total number of all packets wherein the endpoint was the destination field in the packet.

SentBytes

The *SentBytes* refers to the total number of bytes sent from that endpoint over a given sample period, i.e. the sum packet size of all packets wherein the endpoint was the source field in the packet.

SentPkts

The *SentPkts* refers to the total number of packets sent at that endpoint over a given sample period, i.e. the total number of all packets wherein the endpoint was the source field in the packet.

Last Seen

The *Last Seen* refers to the last time a packet with either the source or the destination field of the endpoint was seen.

Conversation

```
Conversation
SrcAddr(A): 64.12.24.234
DstAddr(B): 192.168.77.115
TotBytes: 716
TotPkts: 5
BytesAB: 577
BytesBA: 139
PktsAB: 3
PktsBA: 2
Last Seen: 3/14/2008 11:00:40 AM
```

Tooltip 3 Conversation Ring
Conversation

When hovering over a connection, a tooltip pops up with the following fields:

SrcAddress(A)

The *SrcAddress(A)* refers to which address was the source address in the first packet regarding that connection.

DstAddress(B)

The *DstAddress(B)* refers to which address was the destination address in the first packet regarding that connection.

TotBytes

The *TotBytes* refers to the total number of bytes sent between the SrcAddress and DstAddress over a given sample period and is the sum of BytesAB and BytesBA.

TotPkts

The *TotPkts* refers to the total number of packets sent between the SrcAddress and DstAddress over a given sample period and is the sum of PktsAB and PktsBA.

BytesAB

The *BytesAB* refers to the total number of bytes sent from the SrcAddress and DstAddress over the view's sample period.

BytesBA

The *BytesBA* refers to the total number of bytes sent from the DstAddress to the SrcAddress over the view's sample period.

PktsAB

The *PktsAB* refers to the total number of packets sent from the SrcAddress to the DstAddress over the view's sample period.

PktsBA

The *PktsBA* refers to the total number of packets sent from the DstAddress to the SrcAddress over the view's sample period.

Last Seen

The *Last Seen* refers to the last time a packet was seen with the source and destination field being the endpoints of the connection.

Strip Chart

The Strip Chart is a useful tool for displaying quantitative data with respect to time.

Diagram

The Strip Chart diagram has the following elements:

- Time Control Area
- Legend
- Data area
- Min/Max

Current Selection Interval

This is an Example of a View containing a Strip Chart:

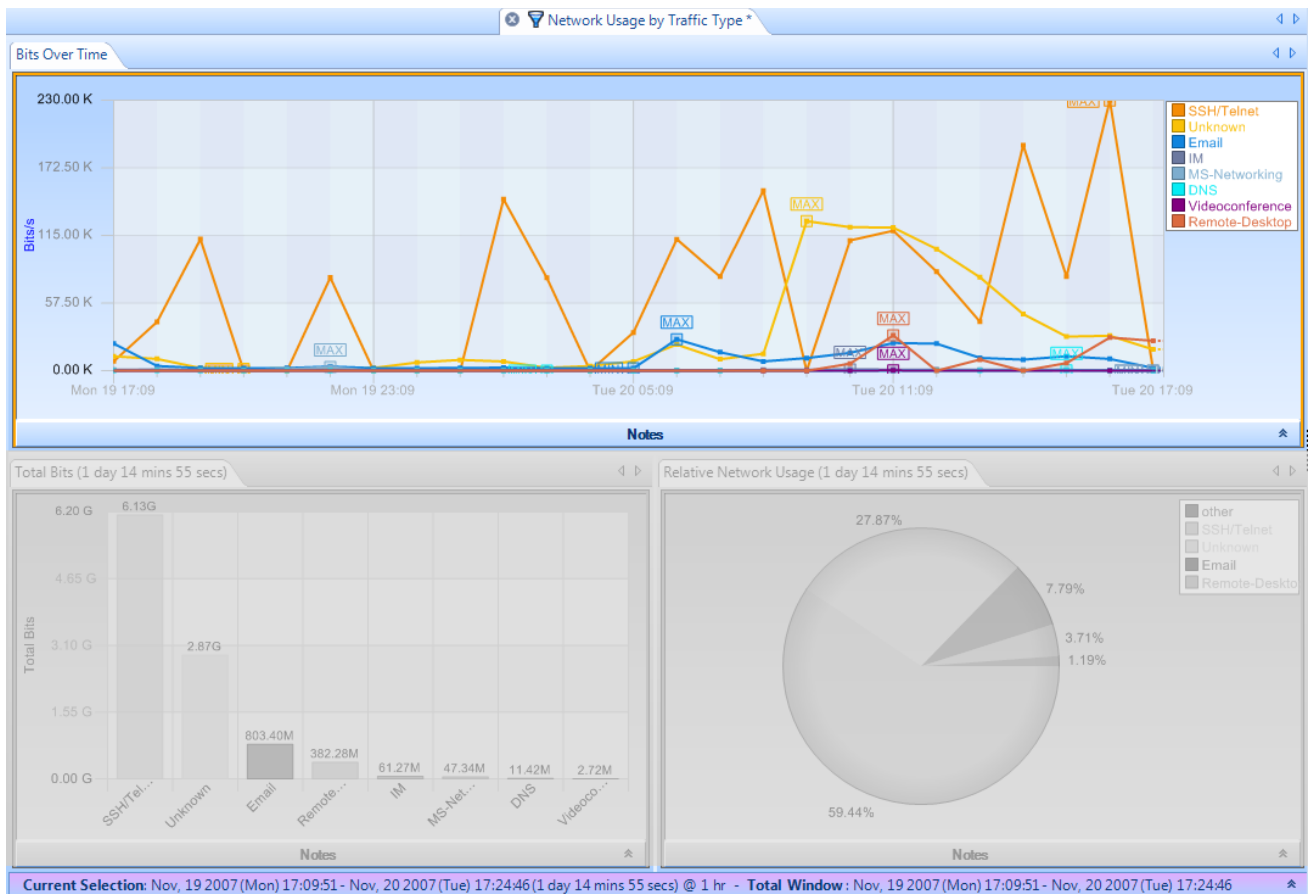


Figure 138: Strip Chart

Note: The Current Selection bar (at the bottom of the View) simultaneously applies to all of the Charts contained in a View.

The View depicted above consists of 3 charts, namely, a strip chart, a bar chart, and a pie chart. In this section we are focused on the strip chart (the top-most chart).

- **Current Selection:** The data points displayed in the strip chart correspond to the View metric (Bits per Second) computed over the *Current Selection* Interval.

- *Total Window*: The *Total Window* interval gives the total duration of the trace file or, in the case of a live capture, the total duration of the capture or the Data Retention Time, whichever is smaller.

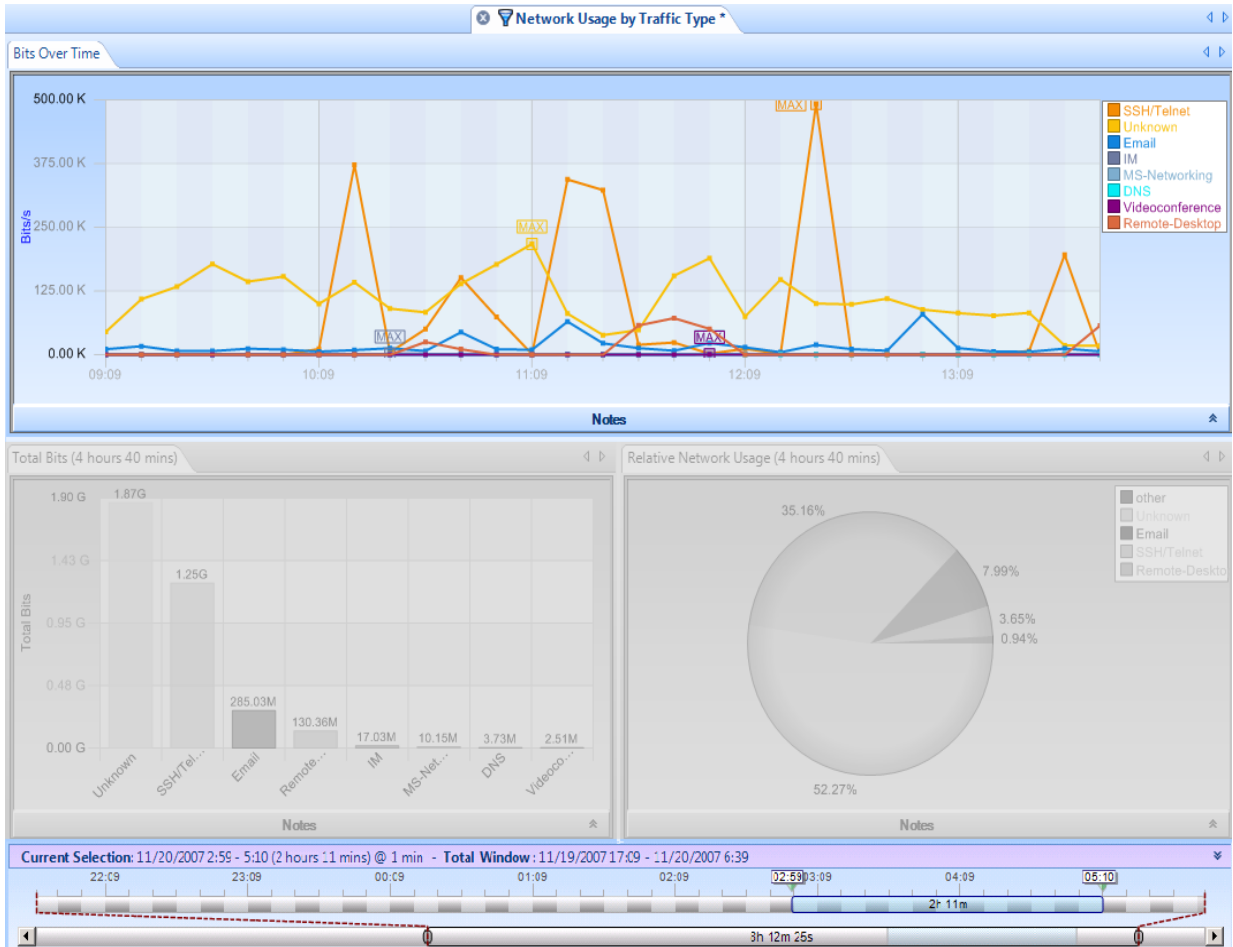


Figure 139: Strip Chart with Horizontal Zoom

Figure 139 shows the strip chart “zoomed” horizontally using the Selection bar in the Time Window. The user can also open the Time Control Ribbon to set the duration and location of the Current Selection. The minimum and maximum values within the Current Selection are displayed (with the exception that of a minimum or maximum is obvious from context, it is not indicated).

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Strip Chart is customizable in the following ways:

- Toggle of legend visibility
- Rescale of Y Axis

Selection

The Strip Chart supports two types of selection:

- Time based
- Line based

Time Based Selection

A *Time Based Selection* is useful on all instances of the Strip Chart and is done by clicking and dragging the mouse over the time to be selected. An example result is shown below:

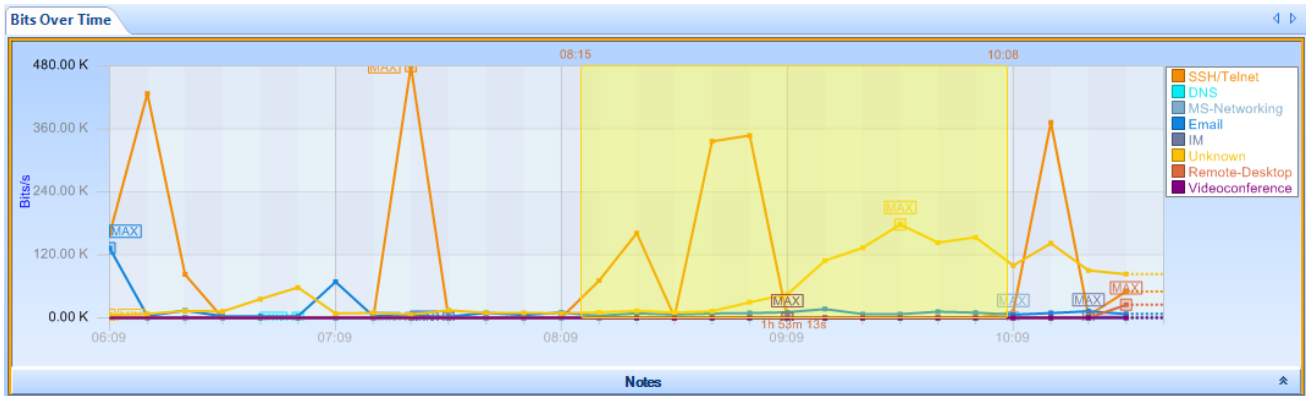


Chart Figure 9 Strip Chart Selection (Time)

Multiple-selection is prohibited for time based selection.

Line Based Selection

A *Line Based Selection* is useful on instances of the Strip Chart where more than one metric is being charted, for instance, showing the bandwidth of the 802.11 b/g channels, as seen below where BG channels 2, 11, and 12 are selected:

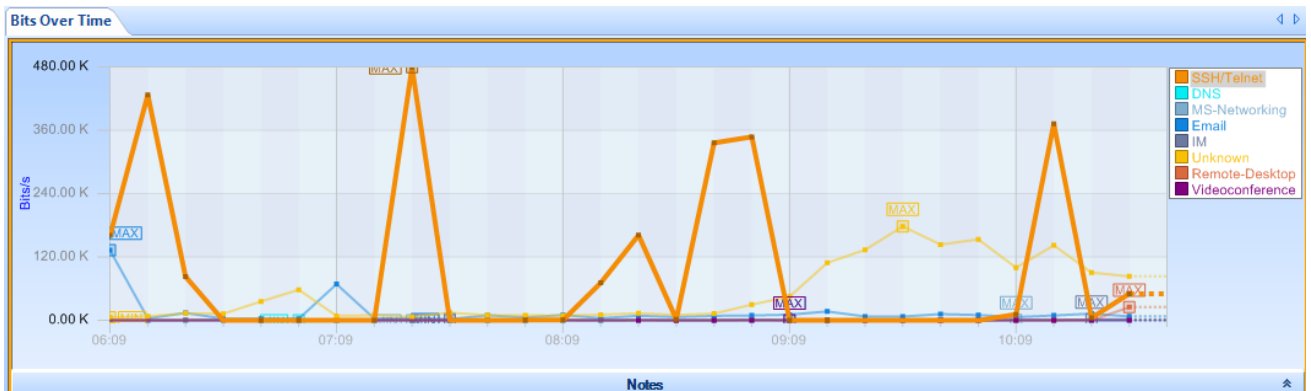


Chart Figure 10 Strip Chart Selection (Element)

Lines are selected by clicking on them or their representation in the legend. Control+click is supported for multiple selections.

Mini

This is the miniature view of the Strip Chart:

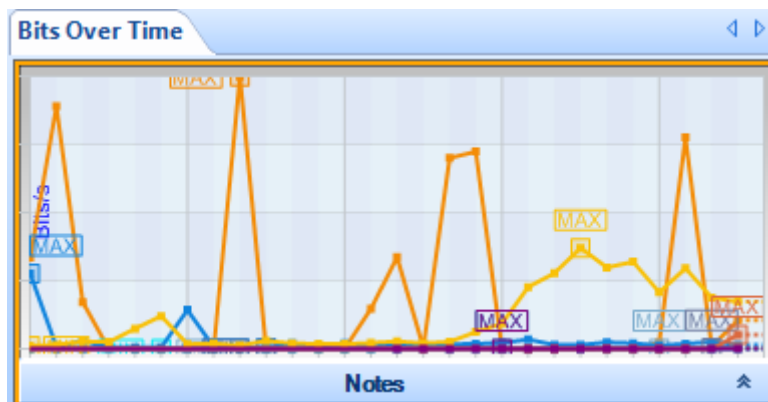
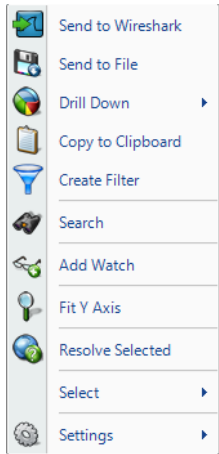


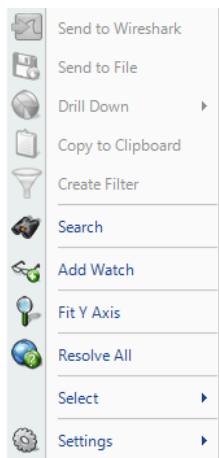
Chart Figure 11 Strip Chart Mini

The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu. The legend disappears and a gray border appears around the image.

Context Menu



Context Menu 27 Strip Chart (Selection)



Context Menu 28 Strip Chart (No Selection)



Context Sub Menu 7 Select

The context menu for the Strip Chart is as follows:

Send to Wireshark

The *Send to Wireshark* menu option will send the traffic from the selected time slice or line(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option will send the traffic from the selected time slice or line(s) to a user-specified trace file which will appear, after completion, in the Files panel, for immediate analysis.

Drill Down

The *Drill Down* menu option will apply the user-specified view to the selected time slice or line(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option respects the Time-Display Format specified. It works the following way for the two selection modes:

- Time Based Selection
All samples in the time slice selected. The format is as follows:

[Time] [Value of highest ordered item in the label] [Value of next item]

- Line Based Selection
All samples of the selected line over the entire time period of the trace file. The format is as follows:

[Time] [Value of selected element at that time]...

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the strip chart and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section later on.

Add Watch

The *Add Watch* menu option opens up the Watch Editor dialog window. The Trigger Condition is based on the currently selected strip chart. The Data Filter, if any, is based on the line selection within the strip chart.

Fit Y Axis

Scale the vertical height of the strip chart to fit within the chart.

Time Display Format

See below.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves, when applicable, either the Port Name, IP Address, or Mac Address of all of the lines of the Strip Chart but only

when that to be resolved is not selected for automatic resolution in the *Name Resolution* submenu available in the Home Ribbon.

Select

The *Select* menu option has two submenu options described at the beginning of this section. However, since multiple selections cannot be done with time slices, the invert option is only available after line selection.

Settings

The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menu

The Strip Chart has the following contextual submenu:

- Settings

Settings



Context Sub Menu & Strip Chart Settings

The Settings contextual submenu for the Strip Chart has the following options:

Show Legend

Toggle off or on the legend for the Strip Chart.

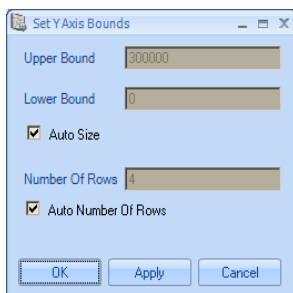
Show Min/Max

Toggle off or on the display of minimum and maximum text indications next to the minimum and maximum values for a line.

Setup Y Axis

Opens up a separate dialog box, which is described next.

Dialogs



Dialog 1 Strip Chart Settings

The Set Y Axis Bounds dialog box is opened from the context menu underneath the Settings submenu. When opened, it has the following parameters:

Upper Bound

Set the upper Y axis bound for the Strip Chart.

Lower Bound

Set the lower Y axis bound for the Strip Chart.

Auto Size

Handle the upper and lower bounds of the Strip Chart automatically.

Number Of Rows

The number of division increments on the Y Axis. For instance, if the lower bound is 0 and the upper bound is 100 and the *Number Of Rows* is set to 10, then the Y axis will increment by units of 10 and there will be 10 alternations of colors for the horizontal depiction of the chart.

Auto Number Of Rows

Handle the Number Of Rows of the Strip Chart automatically.

Tooltips

The tooltips for the Strip Chart are the full quantitative value of a specific sample point of the element in the data area.

Bar Chart

The displays quantitative metrics in a graphical bar based chart. It is used when there is a known domain for a metric and division of the domain is useful. Quantities are graphically represented and restricted to a linear scale.

There are three types of Bar Charts:

- Single Bars
- Stacked Bar Chart
- Grouped Bars

Single Bar Chart

Single Bar Charts are the most basic form of Bar Charts. Each column is a single valued bar. Unlike with the other bars, the colors of the bars have no significance other than their correspondence to the legend.

Along with the “Sampling Time” and “Date Retention Time” options previously described, the Single Bar Chart is customizable in the following ways:

- Sort Bars
- Rescale of Y-Axis
- Toggle of legend visibility
- Toggle of label visibility above individual bars
- Select value or percentage as label

Default

This is an example of the default view for a Single Bar Chart:

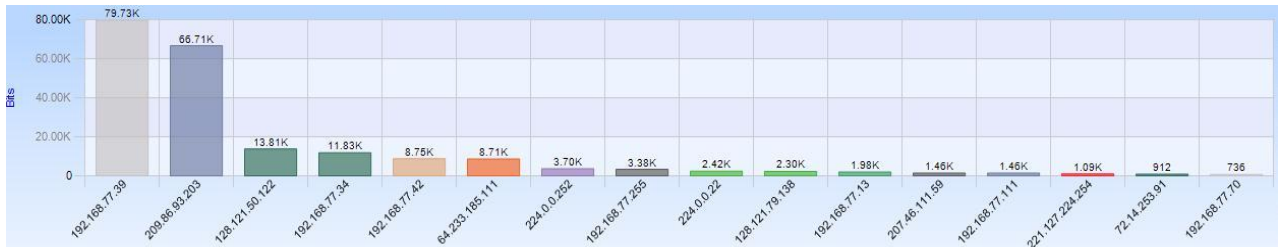


Chart Figure 12 Single Bar Chart

Selection

A bar in a Single Bar Chart is selected by clicking on the bar itself, or the column it lies in, or its representation in the legend. Control+click is supported for multiple selection.

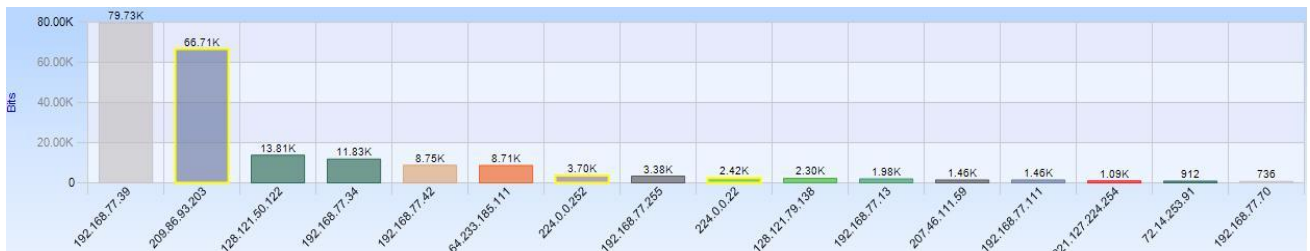


Figure 13: Bar Chart Multiple Selection

Mini

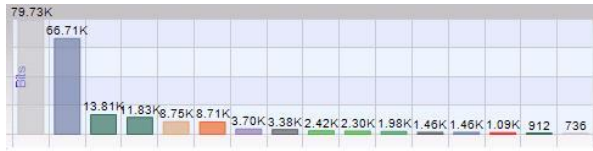


Figure 140: Single Bar Chart Mini

This is the miniature view of the Single Bar Chart. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Stacked Bar Chart

A *Stacked Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into predetermined constituents. These constituent components can be selected and analyzed individually or collectively.

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Stacked Bar Chart is customizable in the following ways:

- Sort Bars
- Rescale of Y-Axis
- Toggle of legend visibility
- Toggle of label visibility above individual bars
- Select value or percentage as label

Default

This is an example of the default view for a Stacked Bar Chart:

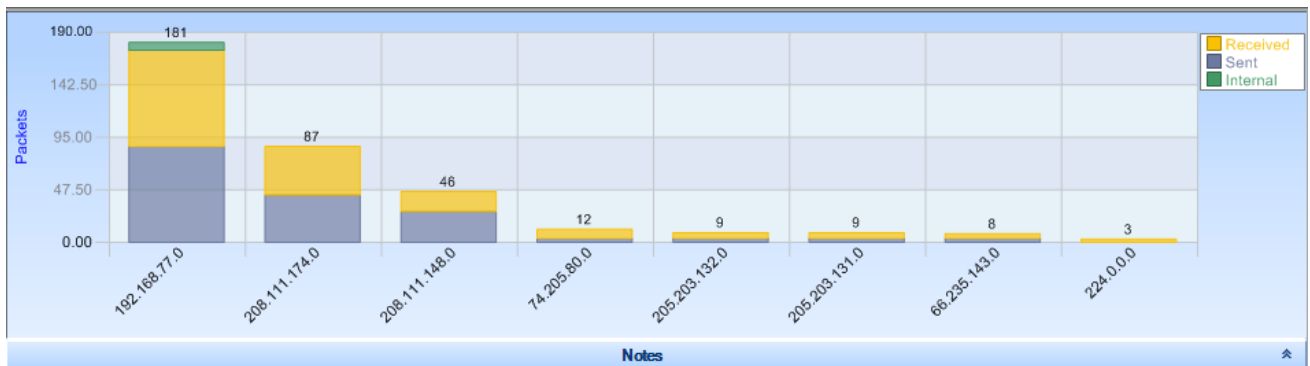


Chart Figure 14 Stacked Bar Chart

Selection

A bar in a Stacked Bar Chart is selected by clicking on the bar itself, or the column it lies in, or its representation in the legend. Control+click is supported for multiple selection.

Mini

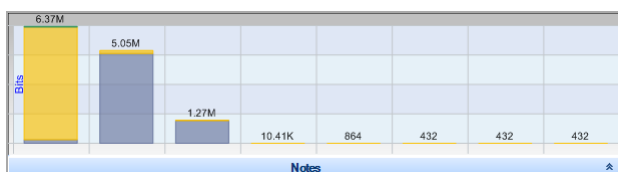


Figure 141: Stacked Bar Chart Mini

This is the miniature view of the Stacked Bar Chart. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Grouped Bar Chart

A *Grouped Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into 2 or more sub columns. The sub columns are used to group similar but distinct things in a Bar Chart.

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Grouped Bar Chart is customizable in the following ways:

- Sort Bars
- Rescale of Y-Axis
- Toggle of legend visibility
- Toggle of label visibility above individual bars
- Select value or percentage as label

Default

This is an example of the default view for a Grouped Bar Chart:

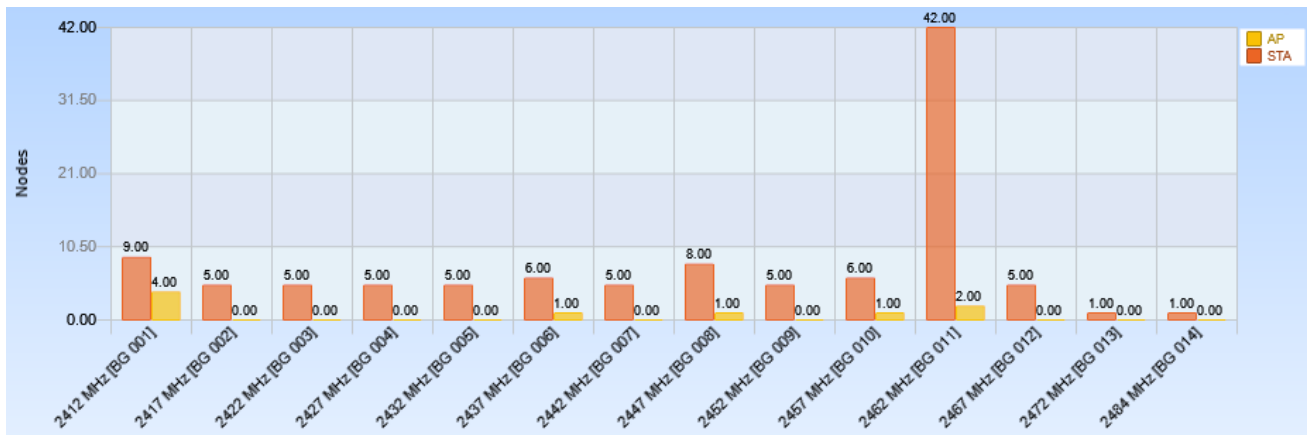


Chart Figure 15 Grouped Bar Chart

Selection

Selection of the Grouped Bar Chart can happen three ways:

- Selection of a column
- Selection of one of the components of a column
- Selection of all instances of a certain subcomponent across all columns

Column

A *column based* selection refers to all traffic with respect to the column name. This method of selection is achieved by selecting the area around the bar with respect to the desired column inside the chart, but not the bar itself.



Component Instance

A *component instance based* selection refers to all traffic with respect to the selected subset of the column name. This method of selection is achieved by clicking on the component.

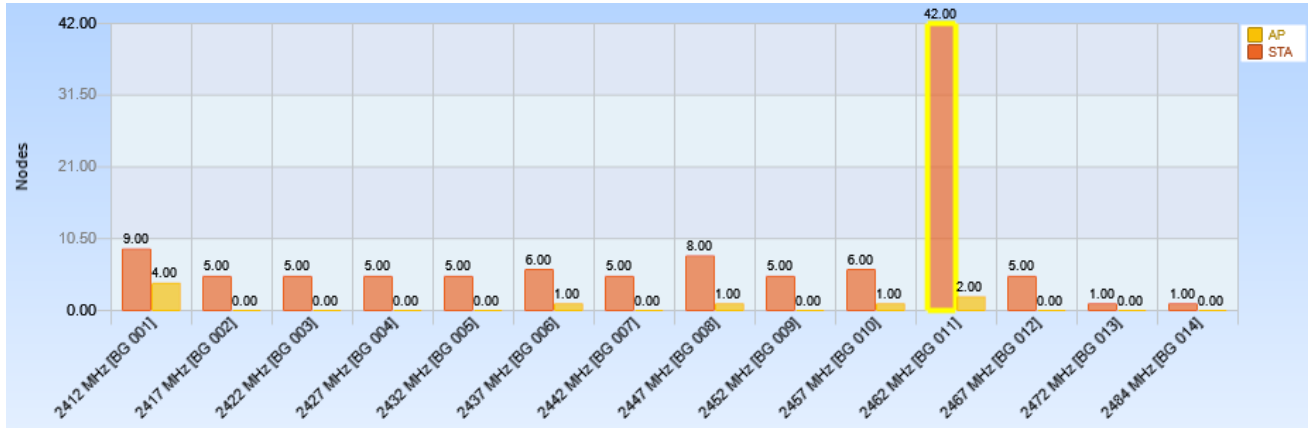


Chart Figure 17 Grouped Bar Chart Selection (Component Instance)

Component

A *component based* selection refers to all traffic with respect to the selected subset. This method of selection is achieved by clicking on the iconic representation of the component to be selected in the legend.



Chart Figure 18 Grouped Bar Chart Selection (Component)

Mini

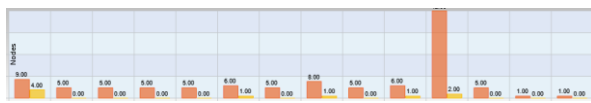


Chart Figure 19 Grouped Bar Chart Mini

This is the miniature view of the Grouped Bar Chart. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

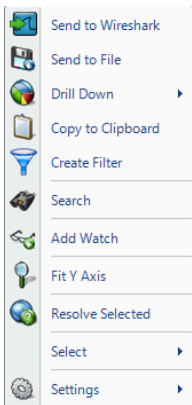


Chart Figure 20 Conversation Ring Top Conversations

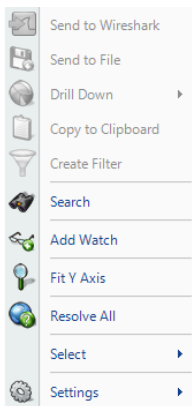
When there is not enough space to display clearly all the bars in a single chart, Pilot automatically ranks and shows data by relevance, according to the sorting option selected. By default, data are sorted from high to low (usually by value). A small label displaying the total number of bars and the current interval appears at the bottom of the view. It is possible to navigate through data using the four buttons in the label. + and - buttons increase or decrease the length of the interval shown, while the arrows (<< and >>) shift the interval inside the data.

Context Menu

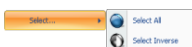
All three types of Bar Charts; Single, Stacked, and Grouped, share the same context menu with a single exception noted below in the context submenus description.



Context Menu 29 Bar Chart (Selection)



Context Menu 30 Bar Chart (No Selection)



Context Sub Menu 9 Select

The context menu for the Bar Chart is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected bar(s) or component(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected bar(s) or component(s) to a user-specified trace file which will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected bar(s) or components(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option works in the following way for each type of Bar Chart:

Single Bars

The format is

[X Axis Label] [Y Axis Value]

Example:

ARP 12

IP 1,217

Stacked Bar Chart

The format is:

[Column Header Name] [Component Name] [Value]

Example:

192.168.77.0 – Sent 34,272

192.168.77.0 – Received 32,480

192.168.77.0 – Internal 4,152

Grouped Bar Chart

The format is:

[Column Header Name] [Component Name] [Value]

Example:
2422 MHz [BG 003]-AP 0

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the bar and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section later on.

Add Watch

The *Add Watch* menu option opens up the Watch Editor dialog window. The Trigger Condition is based on the currently selected bar chart. The Data Filter, if any, is based on the bars selected within the bar chart (if any).

Fit Y Axis

The *Fit Y Axis* menu option resizes the Y scale of the Bar Chart so that the largest bar is equal to the height of the chart.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves, when applicable, either the Port Name, IP Address, or Mac Address of the bar(s) in the Bar Chart but only when that to be resolved is not selected for automatic resolution in the Name Resolution submenu available in the Home Ribbon.

Select

The *Select* menu option has two submenu options described at the beginning of this section with an option to either select the bar(s) and component(s) of the Bar Chart, or invert the selection of bar(s) and component(s).

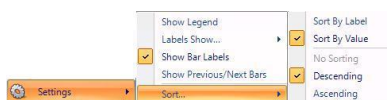
Settings

The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menus

The Bar Charts have one contextual submenu:

- Settings



Context Sub Menu 10 Bar Chart Settings
Single Bar



Context Sub Menu 11 Bar Chart Settings
Stacked Bars or Grouped Bars

The settings submenu for the Bar Chart context menu has several items:

Show Legend

The *Show Legend* menu option toggles off or on the Bar Chart legend.

Show Bar Labels

The *Show Bar Labels* menu option toggles off or on the Bar Chart labels.

Label Show

The *Label Show* menu option opens a submenu with two options for labels: Percentage or Value. This menu is available only in Single Bar Charts.

Sort

The *Sort* menu option opens a submenu with the following two mutually exclusive sets of options

The first set of mutually exclusive options:

Sort By Label

The *Sort By Label* menu option sorts the bars alphabetically by their labeled column names.

Sort By Value

The *Sort By Value* menu option sorts the bars numerically by their quantitative values.

The second set of mutually exclusive options:

No Sorting

The *No sorting* menu option disables sorting. Under this condition, bars are added left to right on a first come basis.

Descending

The *Descending* menu option sorts the bars sequentially from left to right, either by name or value, as specified in the first mutually exclusive group.

Ascending

The *Ascending* menu option sorts the bars sequentially from right to left, either by name or value, as specified in the first mutually exclusive group.

Tooltips

The tooltips for the Bar Chart correspond to the label of the bar over which the mouse is hovering.

Scatter Plot

The *Scatter Plot* is a versatile and flexible chart that can display complex relationships between values. Scatter Plots are display three metrics:

- Y Axis
- X Axis
- Dot size of the circles, referred to as points

Each of these metrics can be assigned to one of a predefined set of options. For instance, the user may specify that the Y-Axis represent 802.11 Channel usage or average frame size.

Scatter Plots are useful when there ought to be a relation between values, such as the total number of packets and the total bytes sent out by a host. Assume the Y Axis is “Packet Count” and the X Axis is “Byte Count”. It can be assumed that there would be roughly a diagonal from the origin outward. An anomaly would be if this relationship was broken or perhaps if it didn’t seem to exist at all (which could be evident of a much more severe networking problem).

Default

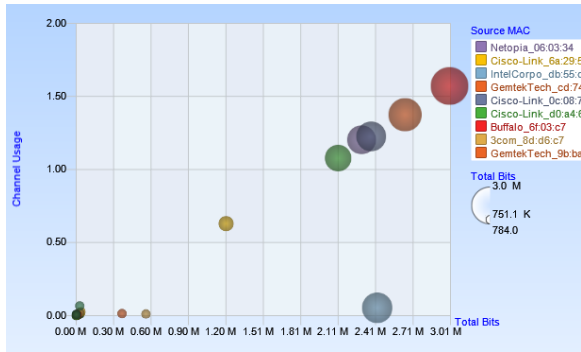


Chart Figure 21 Scatter Plot

Along with the “Sampling Time” and “Data Retention Time” options previously described, the scatter plot is customizable in the following ways:

- Assignment of the dot size relation
- Assignment of X-Axis
- Assignment of Y-Axis

Selection

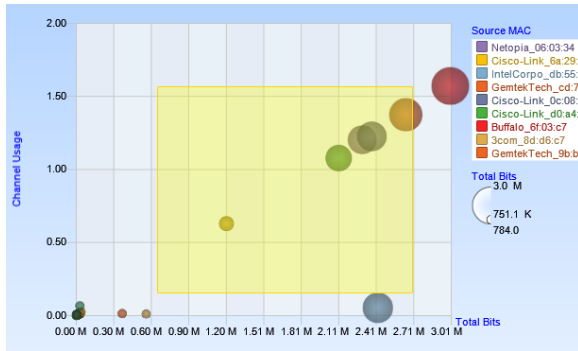


Chart Figure 22 Scatter Plot Draw Box

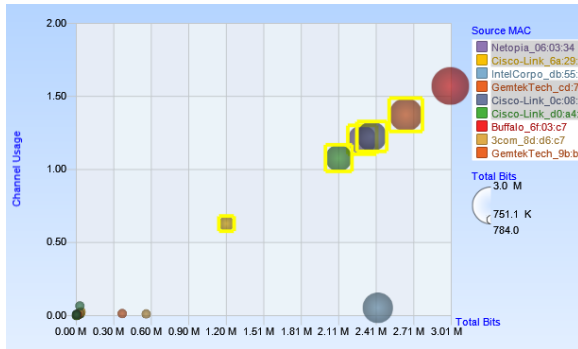


Chart Figure 23 Scatter Plot Multiple Selection

Selection in a Scatter Plot is done by one of four ways:

- Search operation
- Selection from the legend
- Drawing a box around the points
- Clicking on the Points to be selected.

Control+click for multiple selection is supported in point based and legend based selection.

Mini

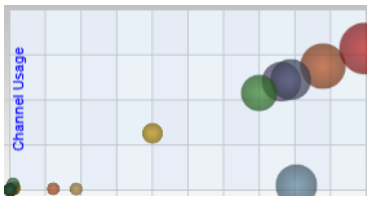
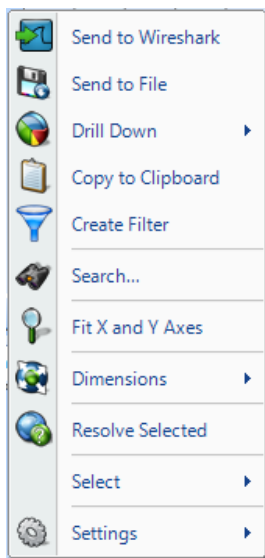


Chart Figure 24 Scatter Plot Mini

This is the miniature view of the Scatter Plot. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Context Menu



The context menu for the Scatter Plot is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected point(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected point(s) to a user-specified trace file which will appear, after completion, in the Files panel for immediate analysis.

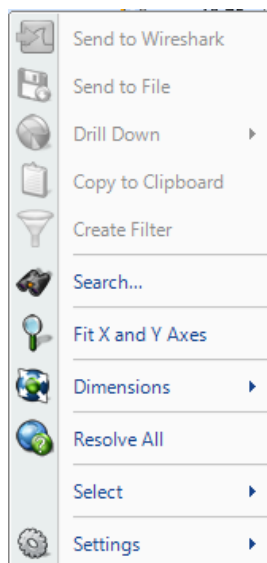
Drill Down

The *Drill Down* menu option applies the user-specified view to the selected point(s) and opens a new view tab in the main workspace.

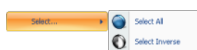
Copy to Clipboard

The *Copy to Clipboard* menu option will copy to the clipboard a tabular list of values of all of the supported metrics with respect to a selection. It also includes

Context Menu 31 Scatter Plot
(Selection)



Context Menu 32 Scatter Plot
(No Selection)



Context Sub Menu 12 Scatter
Plot Select

a column header and notation for appropriate units.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the scatter plot and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section later on.

Fit X and Y Axes

The *Fit X and Y Axes* menu option resizes the X and Y scales of the Scatter Chart so that the largest X and Y excursions fit within the chart.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves the Port Name, IP Address, or Mac Address of the point(s) in the Scatter Plot. This option is available only when the field is not automatically resolved (check the Name Resolution submenu available in the Home Ribbon).

Select

The *Select* menu option has two submenu options described at the beginning of this section with an option to either select the point(s) in the Scatter Plot, or inverts the selection of point(s).

Settings

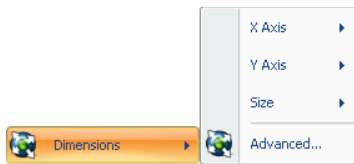
The *Settings* menu option opens up a sub-menu with specific settings for the chart. It is described below.

Context Sub-Menus

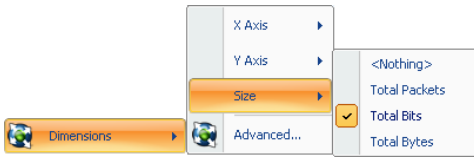
The Scatter Plot has three contextual submenus:

- Dimensions
- Select (shown above)
- Settings

Dimensions



Context Sub Menu 13 Scatter Plot Dimensions



Context Sub Menu 14 Scatter Plot Dimensions (Detail)

The Dimensions submenu for the Scatter Plot context menu has four items:

X Axis

The *X Axis* menu option gives all possible sub choices for the significance of the X-Axis coordinate. Some charts may only have one option, while others may have multiple; for instance, "Bits/s" versus "Bytes/s" or "Packets/s".

Y Axis

The *Y Axis* menu option gives all possible sub choices for the significance of the Y-Axis coordinate. Some charts may only have one option, while others may have multiple; for instance, "Bits/s" versus "Bytes/s" or "Packets/s".

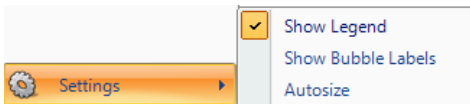
Size

The *Size* menu option has a submenu where the dot size of the points can be enabled and associated with a metric or disabled by selecting "Nothing".

Advanced

The *Advanced* menu option opens up a separate dialog box.

Settings



Context Sub Menu 15 Scatter Plot Settings

The settings submenu for the Scatter Plot context menu has five items:

Show Legend

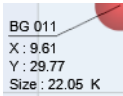
The *Show Legend* check box menu option toggles off or on the Scatter Plot legend.

Show Bubble Labels

The *Show Bubble Labels* menu option toggles off and on what would otherwise be viewed via a tooltip by hovering over a point.

Autosize

The *Autosize* menu option toggles off and on whether the area will resize based on maximum values automatically.



Tooltip 4 Scatter Plot

A tooltip comes up when hovering over a point. It has the following values:

Name

The *Name* of the point being charted, such as an IP address or an 802.11 wireless channel.

X

The *X* value refers to the position the point currently occupies on the X axis and the significance of this with respect to the units for the X axis.

Y

The *Y* value refers to the position the point currently occupies on the Y axis and the significance of this with respect to the units for the Y axis.

Size

The *Size* value refers to the dot size of the point and the significance of this with respect to the units for the dot size.

Pie Chart

The *Pie Chart* shows quantitative values as a percentage of a whole. Pie Charts are useful for instance, when looking at local versus non-local traffic, or finding out what percentage of total traffic is constituted by a particular host. The elements of a Pie Chart are referred to as slices.

Default

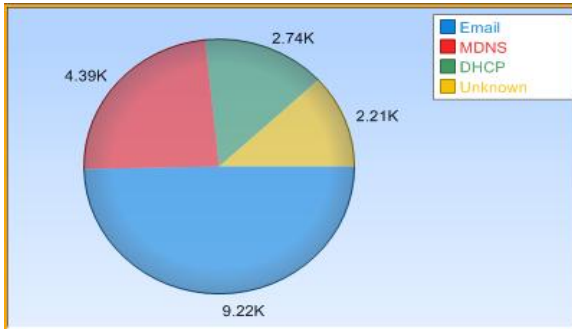


Chart Figure 25 Pie Chart

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Pie Chart is customizable in the following ways:

- Toggle of percentage or quantitative value to be displayed for the time slices.
- Toggle of legend visibility.

The Pie Chart can be zoomed in and out using the scroll wheel on the mouse.

Selection

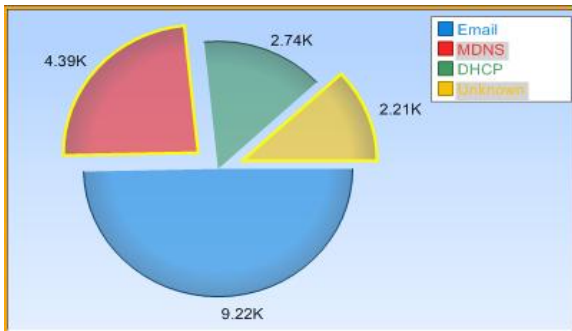


Chart Figure 26 Pie Chart Selection

Selection in a Pie Chart is done either by clicking on a slice in the Pie Chart or on its representation in the legend. Control+click for multiple selections is supported.

Mini

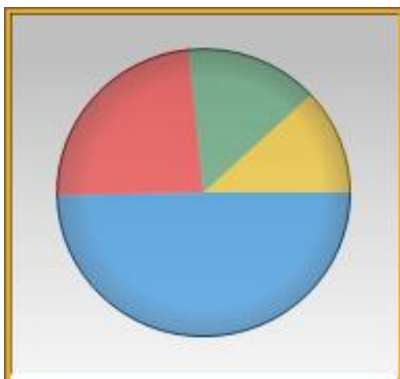
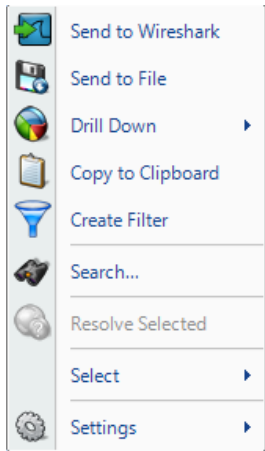


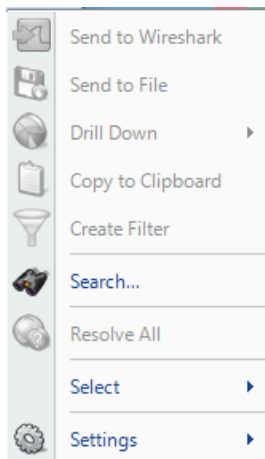
Chart Figure 27 Pie Chart Mini

This is the miniature view of the Pie Chart. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Context Menu



Context Menu 33 Pie Chart
(Selection)



Context Menu 34 Pie Chart
(No Selection)



Context Sub Menu 16 Pie
Chart Select

The context menu for the Pie Chart is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected slice(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected slice(s) to a user-specified trace file which will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected slice(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option has the following format:

[Slice Name] [Quantitative Value] [Percentage Value]
It refers to all selected slices.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the Pie Chart and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section later on.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves, when applicable, either the Port Name, IP Address, or Mac Address of the slice(s) in the Pie Chart but only when that to be resolved is not selected for automatic resolution in the Name Resolution submenu available in the Home Ribbon.

Select

The *Select* menu option has two submenu options described at the beginning of this section with an option to either select the slice(s) in the Pie Chart, or inverts the selection of slice(s).

Settings

The *Settings* menu option opens up a sub-menu with specific settings for the chart. It is described below.

Context Sub-Menus

The Pie Chart has one contextual submenu:

- Settings

Settings



Context Sub Menu 17 Pie Chart Settings



Context Sub Menu 18 Pie Chart Settings (Detail)

The settings submenu for the Pie Chart context menu has two items:

Show Legend

The *Show Legend* check box menu option toggles off or on the Pie Chart legend.

Labels Show...

The *Labels Show...* menu option has a submenu with two mutually exclusive toggles:

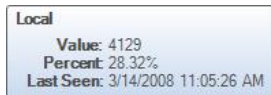
Percentage

The *Percentage* toggle labels the slice value(s) as a percentage of the whole pie.

Value

The *Value* toggle labels the slice value(s) with their quantitative equivalents.

Tooltips



Tooltip 5 Pie Chart

A tooltip comes up when hovering over a slice. It has the following values:

Value

The *Value* refers to the quantitative value associated with that slice.

Percent

The *Percent* refers to the percentage that the slice constitutes of the whole.

Last Seen

The *Last Seen* refers to the last time that element of the slice was seen in traffic. This can give an idea as to what percentage in the time domain the slice refers to.

Data Grid

The *Data Grid* chart shows quantitative information pertaining to a number of metrics in a hierarchically displayed grid. The grid has rows and columns.

The columns can be

- Rearranged to any sequential order desired
- Resized
- Hidden and shown

The rows can be

- Hierarchically defined
- Collapsed and expanded
- Filtered and hidden by a variety of different means
- Sorted by any column or multiple columns simultaneously

In order to explain functionality, a few things have been turned on from the default chart. Additionally, since the grid is very compact, some conventions needed to be broken to make the diagram clear. Only part of the entire control is shown.

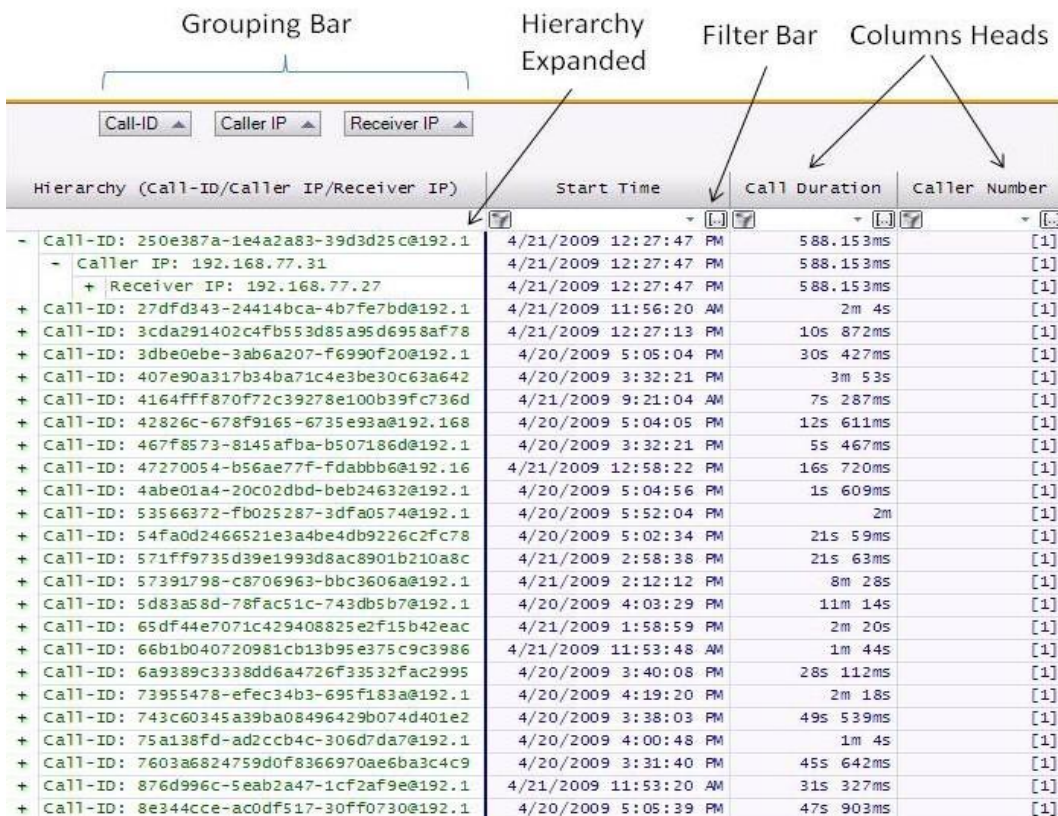


Chart Figure 28 Grid

Grouping Bar

The elements of the *Grouping Bar*, called groups, determine the row hierarchy. For example, the root level has all of the 802.11 B/G channels. Each channel can be expanded to show the associated ESSIDs on it. The individual ESSIDs can then, in turn be expanded to show the APs or stations that are associated with each ESSID.

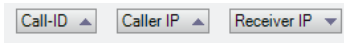


Figure 142 Grid Grouping Bar

Each element of the Grouping Bar also has an arrow after the name. This specifies the sorting order of that level of the hierarchy. For instance, the channels are descending and the ESSIDs are listed alphabetically ascending. Any of these can be toggled by clicking on the group itself.

Additionally, groups forming the hierarchy in the Grouping Bar can be rearranged by dragging the elements to be in different orders. The hierarchy changes are reflected immediately. Things can be removed from the hierarchy by dragging them out of the sequence.

The Grouping Bar is explained in much more details in the videos.

Column Headers

The *Column Headers* refers to columns which can be turned on and off thru the context menu. Rows can be sorted via one or more columns. The first, left-most column header contains the hierarchy specified in the Grouping Bar.

Filter Bar

The Data Grid *Filter Bar* allows for filtering on a column by column basis of all the rows. Two types of filtering are supported:

- Selection Based
- Advanced

Selection Based

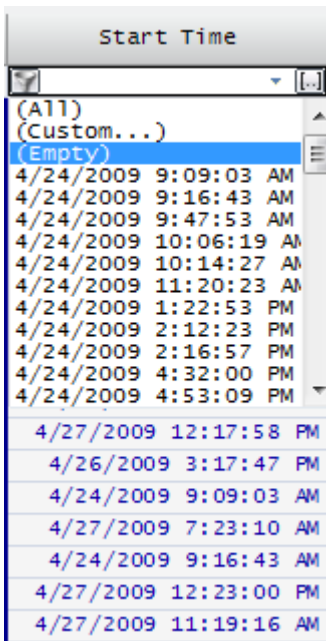


Figure 143 Selection Based Grid Filtering Drop Down

Selection Based filtering is available by clicking on the down arrow on the right of one of the column's filters. A drop down list opens that lists the unique entries of the associated column. After an entry is selected, the rows not satisfying the filter are hidden.

Additionally the icon on the left hand side of the filter box changes, as can be seen in Figure 144. Clicking on the icon removes the filter and shows the hidden rows.



Figure 144 Selection Based Grid Filtering Enabled

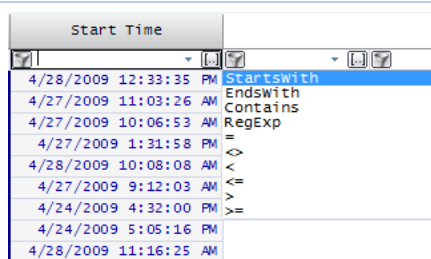


Figure 145 Advanced Grid Filtering

Advanced filtering is available by clicking on the ellipses (...) on the right of one of the column's filters. A drop down opens that which lists a number of string and value manipulations and comparisons.

After an expression is entered, the rows not satisfying the expression are automatically hidden.

Additionally the icon on the left hand side of the filter box changes, as can be seen in Figure 144. Clicking on the icon removes the filter and shows the hidden rows.

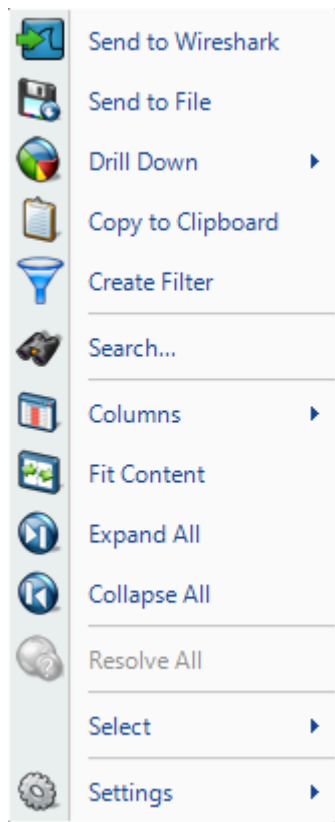
Hierarchy

The data grid rows may be organized in a multi-tiered tree via the grouping bar. They can be fully expanded and collapsed through the context menu.

Selection

Multiple-selection in the Data Grid can only be done on the same hierarchical level. For instance, a child and a parent cannot be simultaneously selected. However, a child and its siblings can.

Context Menu



Context Menu 35 Grid (Selection)

The context menu for the Data Grid is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected row(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected row(s) to a user-specified trace file which will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected row(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies in a tabular form, the values of each row selected. They are copied to the clipboard in a sequential manner that matches how they appear in the grid.

Create Filter

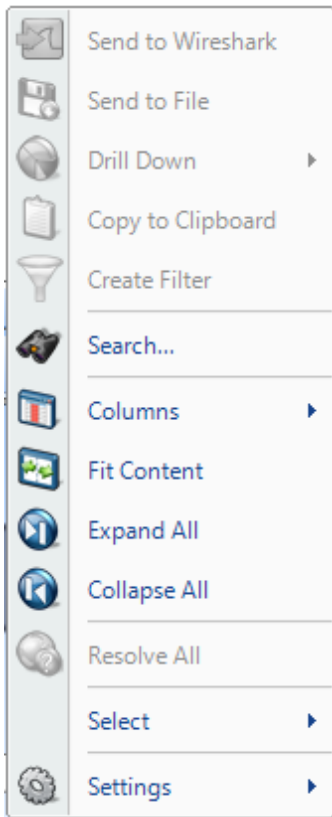
The *Create Filter* menu option creates a filter based on the current selection within the Grid and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section later on.

Columns

The *Columns* menu option expands to a submenu that is used to show



Context Menu 36 Grid (No Selection)



Context Sub Menu 19 Select

and hide columns in the grid. The submenu is described below.

Fit Content

The *Fit Content* menu option resizes the columns making all of the column data visible.

Expand All

The *Expand All* menu option expands the ordered hierarchy of the rows.

Collapse All

The *Collapse All* menu option collapses the ordered hierarchy of the rows.

Resolve All

The *Resolve All* menu option is always disabled for the grid and is included in the context menu in order to be consistent with the other charts.

Select

The *Select* menu option has two submenu options described at the beginning of this section with an option to either select all row(s) at a certain level in the hierarchy or inverts the selection of row(s).

Settings

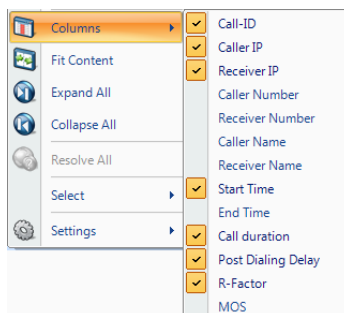
The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menus

The Data Grid has two contextual submenus:

- Columns
- Settings

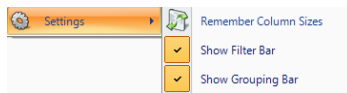
Columns



Context Sub Menu 20 Grid Columns

The *Columns* submenu of the Data Grid context menu has a variable number of non-mutually exclusive toggles which depends on the chart and view. Toggling the submenu options make their corresponding columns visible or hidden in the data grid.

Settings



Context Sub Menu 21 Grid Settings

The *Settings* submenu of the Data Grid context menu has the following options:

Remember Column Sizes

The *Remember Column Sizes* menu option saves the current size of the columns for a custom view. This is the only way to save the size of the columns as they are not automatically saved when a custom view is created or modified.

Show Filter Bar

The *Show Filter Bar* menu option shows or hides the filter bar on the Data Grid Chart.

Show Grouping Bar

The *Show Grouping Bar* menu option shows or hides the Grouping Bar on the Data Grid Chart.

Tooltips

The tooltips on the Data Grid correspond to all entries for a particular row. This is also what will be copied out in a *Copy to Clipboard* operation.

Channels Button

A Pilot Console provides 802.11 wireless analysis on live traffic using the CACE Technologies AirPcap adapters for the wireless interfaces.

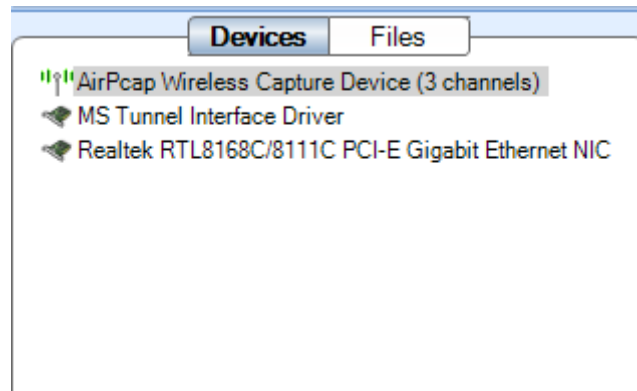


Figure 146 Wireless Interface in Sources Panel

Regardless of the number of AirPcap devices connected to the system, they are shown as a single aggregated capture device, where the number of channels, in parentheses, corresponds to the actual number of AirPcap capture devices (see Figure 146). The AirPcap adapters have been aggregated into a single capture device for convenience in dealing with hopping or scan sequences, where the adapters are sequenced through multiple channels as specified using the Channel Management Panel.

The Channels button in the Home Ribbon brings up the Channel Management Panel. The Channel Management Panel is the way, in wireless captures, to specify on which channels to capture for a particular time interval. The Channel Management Panel is available in the Home Ribbon and is shown below



Figure 147 Channel Management Panel

Note: To close the Channel Management Panel, click the Channels button again or somewhere outside of the submenu. All changes take place immediately hence there is no need for confirmation buttons.

There are three main sections of the Channel Management Panel as shown in the above image:

- All Channels
- Locked Channels
- Scan Sequence

Channel	Frequency	Type
11	2462	N
11	2462	NHigh
11	2462	NLow
12	2467	BG
12	2467	N
12	2467	NHigh
12	2467	NLow
13	2472	BG
13	2472	N
13	2472	NHigh
13	2472	NLow
14	2484	BG
14	2484	N
14	2484	NHigh
14	2484	NLow
240	4920	A
240	4920	N
240	4920	NHigh
240	4920	NLow
241	4925	A
242	4930	A
243	4935	A
244	4940	A
244	4940	N

Figure 148 All Channels

For the purpose of this document, a *channel* corresponds to a center frequency, bandwidth, and type of 802.11 frames that can be received. The types of frames are:

BG – 802.11b or 802.11g

A – 802.11a

N – 802.11n without an extension channel

NHigh – 802.11n with an extension channel above the center frequency

NLow – 802.11n with an extension channel below the center frequency

The available channels depend on the AirPcap devices attached to the system.

2.4GHz Center Frequencies:

AirPcap Classic/Tx – 20 MHz bandwidth, 802.11b,g (BG)

AirPcap Ex – 20 MHz bandwidth, and 802.11b,g (BG)

AirPcap Nx – 20 MHz bandwidth, and 802.11b,g,n (BG or N)

AirPcap Nx – 40 MHz bandwidth, and 802.11b,g,n (BG or N or NHigh or NLow)

5GHz Center Frequencies:

AirPcap Ex – 20 MHz bandwidth, and 802.11a (A)

AirPcap Nx – 20 MHz bandwidth, and 802.11a,n (A or N)

AirPcap Nx – 40 MHz bandwidth, and 802.11a,n (A or N or NHigh or NLow)

For example, the AirPcap Ex adapter at 2.437GHz center frequency will capture BG frames. At 5.260GHz, the AirPcap Ex adapter will capture A frames.

The AirPcap Nx adapter at 2.437GHz center frequency and 20MHz bandwidth will capture BG, A, and N frames. At 5.260GHz center frequency and 40 MHz bandwidth (NHigh), the AirPcap Nx adapter will capture A, N, and NHigh frames.

Channel Names

Channels are generally identified with a by a number and a frequency band. For example, channel 13 in the 2.4 GHz band corresponds to center frequency 2.472GHz. Not every available channel will have an assigned number. This is indicated by N/A for the channel name.

All Channels Panel

The *All Channels* panel includes the following:

- A list of all of the available channels. This list depends on the available AirPcap adapters. The list columns include the channel name, the center frequency, and the type of frame that can be

received.

- A search bar that automatically matches any field in the channel list.
- 4 filter buttons to quickly hide or show the A, BG, N, and Unnamed channels.
- Alternating color rows so that different ways to interpret a channel at the same frequency is visually broken up.
- Selection control buttons

This allows for a flat traditional list of channels that can be quickly navigated and selected without having to worry about the complexities of the standards.

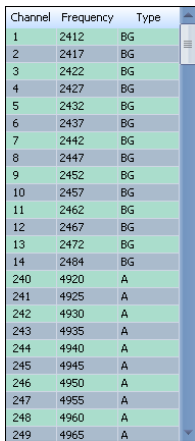
However, given the complexity of the standards, there are some very important restrictions that must be taken into consideration when using multiple classes of AirPcap adapters at once:

N and BG channels are mutually exclusive. If there is 1 N adapter and 1 BG adapter, then only the N adapter can scan the 2.4GHz BGN range.

For the purpose of documentation, the control has been broken into the following components:

- Channel List
- Search and Filter Bar
- Selection Controls

Channel List



Channel	Frequency	Type
1	2412	BG
2	2417	BG
3	2422	BG
4	2427	BG
5	2432	BG
6	2437	BG
7	2442	BG
8	2447	BG
9	2452	BG
10	2457	BG
11	2462	BG
12	2467	BG
13	2472	BG
14	2484	BG
240	4920	A
241	4925	A
242	4930	A
243	4935	A
244	4940	A
245	4945	A
246	4950	A
247	4955	A
248	4960	A
249	4965	A

Figure 149 Channel List

The Channel List is a scroll-able list of all channels supported by all connected AirPcap Adapters. This list automatically changes when the number of adapters changes (which is updated by clicking the *Update Sources* button, described in the Home Panel section).

The colors in the list are to provide contrast for easy navigation. The only rule they follow is that they are alternated based on frequency.

The Channel List has three columns:

Channel

The canonical name for a channel. This is how the channel is usually referred to, such as channel 6. Please note, not all available frequencies have names such as this.

Frequency

The actual center frequency that the row refers to. These are in MHz.

Type

The type of Channel, one of the following: BG, A, N, NHigh, NLow.

Selection Controls



Icon 66 Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.



The *Select Inverse* button inverts the channel list selection(s).



Icon 68 Select All Channels

The *Select All* button selects all of the channel(s) in the channel list.

Search and Filter Bar

The search text box can be edited at any given time and gives the results in real time.

The filter bar contains four buttons, each corresponding to a set of channel types. Since there may be times when not all classes of AirPcap Adapters are plugged in, some of the filter buttons will be disabled. For instance, in the example, since there is no 802.11n wireless adapter plugged in, the N button is grayed out.

Locked Channels

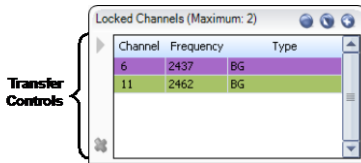


Figure 150 Locked Channels

The *Locked Channels* is a list of channels that are used to assign a wireless adapter dedicated to a channel. It contains 4 elements:

- Title
- Selection controls
- Transfer controls
- Channel list

The following is saved in the global configuration file:

- Locked channels

Title

The *Title* specifies how many channels can be locked. This number is equal to the number of AirPcap adapters recognized by the Pilot Console. If you plug more AirPcap Adapters in, or take some out, then you must click the *Update Sources* button in the Home Ribbon in order for your changes to be reflected in the maximum channel tally.

Selection Controls



Icon 69 Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.



Icon 70 Invert Selection

The *Select Inverse* button inverts the channel list selection(s).



Icon 71 Select All Channels

The *Select All* button selects all channel(s) in the channel list.

Transfer Controls



Icon 72 Transfer Channels

The *Right Arrow* button adds the selected channel(s) to the lock list.



Icon 73 Remove Channels

The *Remove* button removes the selected channel(s) from the lock list. The lock list can legally have zero elements.

Channel List

The *Channel List* is a color coded list of locked channels. The significance of the colors is simply that a distinct color means a distinct wireless adapter.

Scan Sequence

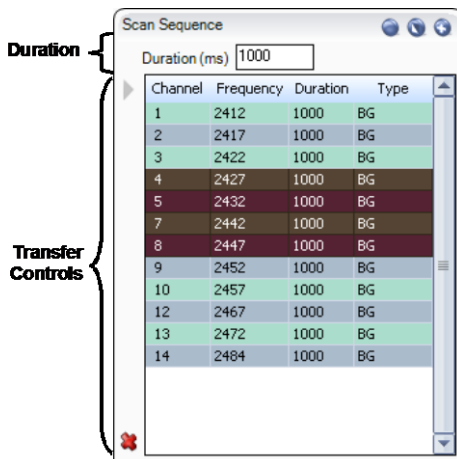


Figure 151 Scan Sequence

The *Scan Sequence* is a list of channels that the wireless adapter(s) will listen on occasionally. It contains 4 elements:

- Duration
- Selection controls
- Transfer controls
- Channel list

The following is saved in the global configuration file:

- Scan sequence elements
- Duration for each element

Note: The scan sequence is determined by the number of AirPcap adapters and their individual capabilities. For consistent results that are independent of the specific scan sequence, it is advisable that to have only one type of AirPcap adapter in the system, e.g., either all AirPcap Ex adapters or all AirPcap Nx adapters. Having both AirPcap Ex and AirPcap Classic/Tx adapters works well in the 2.4GHz band, but not in the 5GHz band.

Duration

Duration (ms) 1000

Figure 152 Channel Duration

The *Duration* edit box sets how long each selected channel will be locked before moving on to the next available channel in the scan sequence.

Selection Controls



The *Select None* button deselects all channel(s) in the channel list, if applicable.



The *Select Inverse* button inverts the channel list selection(s).

Icon 75 Invert Selection



The *Select All* button selects all channel(s) in the channel list.

Icon 76 Select All Channels

Transfer Controls



Icon 77 Transfer Channels

The *Right Arrow* button adds the selected channel(s) to the scan sequence with a duration of 1000 ms each. Durations of previous, deleted channel(s) are not saved if they are retransferred.



Icon 78 Remove Channels

The *Remove* button removes the selected channel(s) from the scan list. The scan list can legally have 0 elements.

Channel List

The *Channel List* is a frequently updated color coded list of scanned channels. The significance of the colors is simply that a distinct color means a distinct wireless adapter. The scan sequence is updated a few times a second to reflect which channels are currently being scanned. Additionally, the channel list in the Scan Sequence has one extra column, named "Duration", which refers to how long that entry will be scanned before moving on to the next. Each entry may have a different duration value.

Decryption

The Pilot Console supports three different types of Wireless decryption:

- WEP (“Wireless Encryption Protocol” or more properly, Wired Equivalent Privacy)
- WPA 1 (Wi-Fi Protected Access with CCMP as specified in IEEE 802.11i)
- WPA 2 (Wi-Fi Protected Access with TKIP as specified in IEEE 802.11i)

Decryption is done through the Wireless Decryption Keys Manager. The decryption keys are global and saved in the configuration file. Please take careful note that, this means that by exporting a configuration file and giving it to someone you are giving them your decryption keys as they are stored in plain human readable text in the configuration file.

Wireless Decryption Keys Manager



Submenu 9 Decryption Keys

The *Wireless Decryption Keys Manager* is available in the Home Ribbon.

When clicked, a submenu appears with the following options:

Add Key

The *Add Key* button, described below, is used to add a new decryption key to be used for future analysis.

Use Injection to Speed Up WPA/WPA2 Decryption

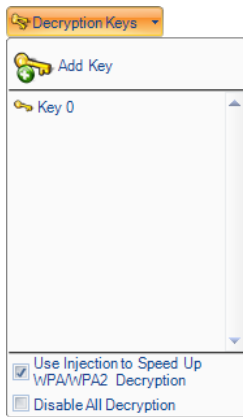
The *Use Injection to Speed Up WPA/WPA2 Decryption* check box, described below in the section entitled “WPA related packet injection” is only enabled if all plugged in AirPcap adapters are Ex. Please note that there are a number of important considerations when using this feature, as discussed below.

Disable All Decryption

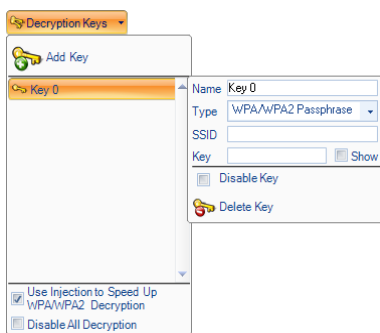
The *Disable All Decryption* check box is used to completely turn off decryption. This may decrease the time required to process a packet if trying to mitigate packet loss on an extremely busy network. It can also be used to confirm that a network is encrypted.

Note: To close the Wireless Decryption Keys Manager, click the button again or somewhere outside of the submenu. All changes take place immediately hence there is no need for confirmation buttons.

Adding a Key



Submenu 10 Decryption Keys with Key



Submenu 11 Decryption Keys with Key (Detail)

To add a key, click on the *Add Key* button. The submenu will change and have a scrollable list with one decryption key. As many decryption keys can be added as desired. Note that there is no need to associate a particular decryption key to a trace file or wireless adapter and that the decryption key will be automatically matched with its specific context.

After a decryption key has been added, its parameters need to be set. This is done by clicking on the decryption key. A submenu opens to the right of the key title with seven controls:

Name

The *Name* field refers to the canonical name of the decryption key. This is used for management of decryption keys, is what will appear as the name in the key gallery, and in no way affects decryption. These names need not be unique.

Type

The *Type* combo box is used to specify the type of decryption key to be added. This is a crucial option as different types equate to entirely different decryption algorithms.

SSID

The *SSID* field is required for WPA related decryption keys but is disabled for WEP decryption keys because the SSID is not needed to decrypt WEP traffic.

Key

The *Key* field is used to specify the shared decryption key needed for a wireless network to be decrypted. Hexadecimal values can be placed here as a single string when appropriate and are not case sensitive. Additionally, 104 bit and 40 bit WEP decryption keys are detected automatically from the Key field input length. For instance, if the type is set to WEP and “A05B06c07d” was put into the Key field, it will be detected as a 40-bit WEP key.

Show

The *Show* check box shows or hides the text in the Key field. By default the Key field uses substitution characters for obfuscation. However, this can be disabled and the field can be seen in plain text by toggling on the Show check box.

Disable Key

The *Disable Key* check box disallows a decryption key from being considered when decrypting traffic. This can be useful for two reasons:

- To confirm that traffic is encrypted
- To speed up decryption; By disabling a decryption key, fewer decryption keys will be considered as candidates for decryption and so therefore, decryption will speed up.

Delete Key

The *Delete Key* button immediately and irreversibly removes a decryption key from the Key list.

WPA Related Packet Injection

Wireless networks secured using the WPA protocol cannot be decrypted as easily as their WEP counterparts. This is because unlike with WEP, simply having a decryption key is not enough to view the traffic of other stations on a network. The access point establishes a different, temporary, ostensibly unique trusted link with each station on the network.

In order to successfully decrypt WPA traffic then, even with a valid decryption key, the set up of this link needs to be captured. However, because stations may not authenticate for hours or possibly longer, in order to view traffic without waiting a long time, the hosts need to re-associate with their access point.

This can be achieved by sending out a de-authentication request which asks the stations to re-associate with their access point.

Note: WPA packet injection only works if all the plugged in AirPcap adapters are EX class. If not all of the plugged in adapters are AirPcap EX, then the checkbox will be disabled.

Note: Although it ultimately depends on the wireless adapter of the station, it is very probable that this action will temporarily drop the connection between a station and its access point.

In Wireshark, the deauthentication frame will look similar to the figure below:

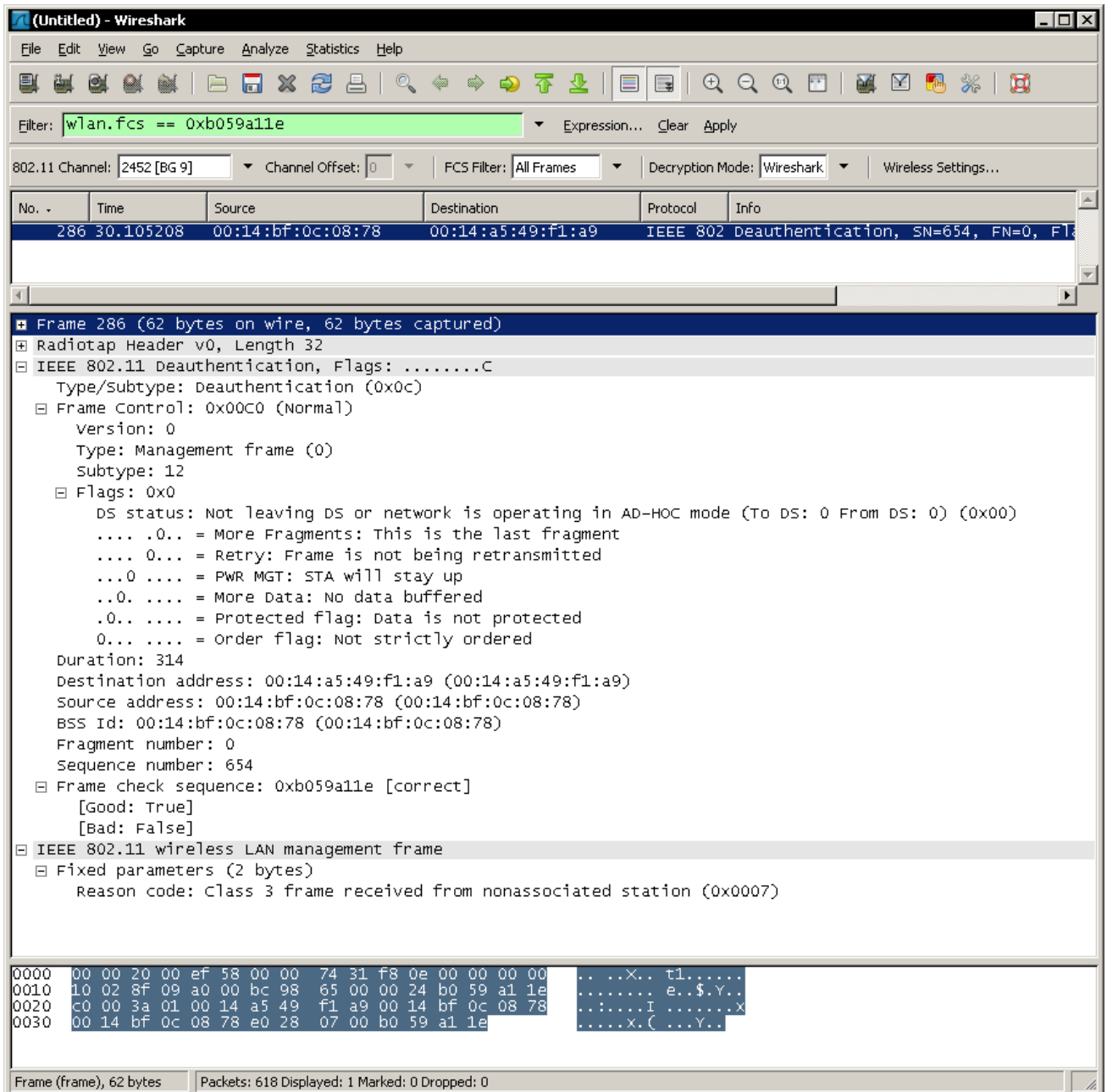


Figure 153 Wireshark analyzing a Pilot Console generated Deauthentication frame

Drill Down

The *Drill Down* feature is one of the most powerful and conceptually oriented features of the Pilot Console. Briefly, Drill Down allows for data to be viewed by iteratively applying views to visually selected subsets of data. This definition will be broken up below:

Data to be viewed

By 'data', this means any information, computation, or meta information; for instance, bytes over time, or all traffic on TCP port 80.

By Iteratively Applying Views

Views cannot only be applied on devices or files, but on data itself. The view that is generated from the data can then, in turn, have another view applied on itself and so on.

To Visually Select Subsets Of Data

Every chart has a method of selecting data subsets that allow for the execution of a drill down operation.

How to

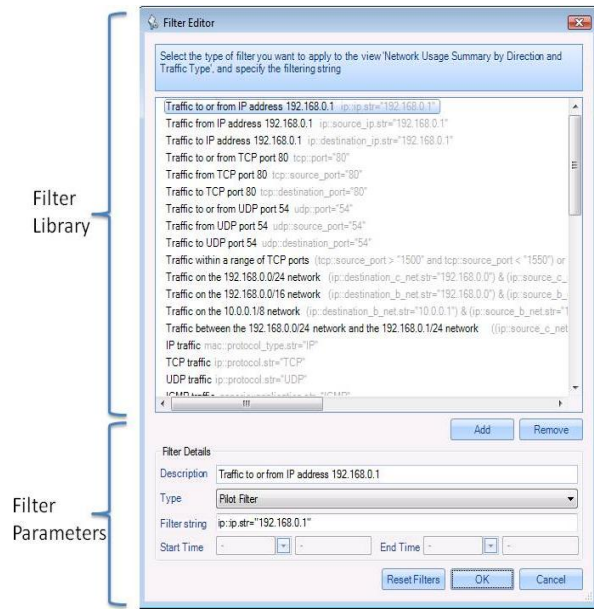
The Drill Down functionality of the Pilot Console is accessible in three ways:

- Home Ribbon Drill Down button available in the Selection Section
- Context click Drill Down option available on any chart
- Dragging a view from the Views Panel over the chart (with a current selection) to be drilled down

Example

For examples of Drill Down sequences and operations please refer to the videos.

Filter Dialog



Dialog 2 Filter Editor

The *Filter Editor* dialog appears after selecting any option to send traffic with a filter either to file or in Wireshark.

The Filter Editor dialog has the following components:

- Filter Library
- Filter Parameters

Filter Library

The *Filter Library*, which is fully expanded in the Filters Manual available on Cace Technology website: <http://www.cacetechnology.com/> contains a list of pre-packaged and user customized filters. Filters can be added and removed with the Add and Remove buttons respectively.

Filter Parameters

The *Filter Parameters* section has three elements:

Description

The name of the filter to be created or modified.

Type

The language the filter is to be written in. There are four languages available:

- Wireshark Capture Filter (BPF)⁷
- Wireshark Display Filter⁸
- Pilot Filter
- Time Interval

Filter String

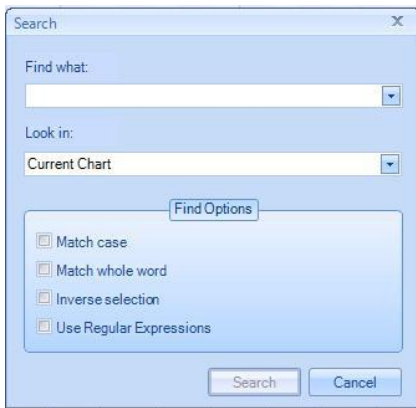
The code for the filter associated with the description as specified above.

For more information refer to the Filters Manual. Please note that an incorrectly written filter may discard all incoming traffic.

⁷ BPF was published in USENIX 93 and can be seen here: <http://www.tcpdump.org/papers/bpf-usenix93.pdf>

⁸ <http://www.wireshark.org/docs/dfref/>

Search Dialog



Dialog 3 Search Dialog

The *Search* dialog can be activated either by clicking on the binocular icon labeled search in the Main Ribbon or by context clicking on a chart and choosing the “Search” option. There are two features of searches:

- Search Context
- Search Style

Search Context

Using the *Look in* drop down selection, searches can be executed over the following three scopes:

Current Chart

The *Current Chart* drop down menu option refers to the currently selected chart with the orange border as documented at the beginning of the section on charts.

Current View

The *Current View* drop down menu option refers to the foremost tab and all associated charts.

All Open Views

The *All Open Views* drop down menu option refers to all open views that have a tab open in the main workspace

Search Style

Different types of searches can be executed based on what is selected in the Find Option subsection of the Search dialog. There are four checkboxes:

Match case

The *Match Case* check box toggles case sensitivity with latin alphanumeric characters [A-Z].

Match whole word

By default, search looks for substrings. If a hostname is “www.cacotech.com” and “cacete” was searched for, then “www.cacotech.com” would still be selected. When *Match whole word* is checked, then only a search term of the full “www.cacotech.com” will select the specific instance.

Inverse Selection

The *Inverse Selection* check box toggles whether the results that match the search term should be selected, or their respective inverse.

Use Regular Expressions

“Regular Expressions” are a technical term which allow for a very flexible match. The Pilot Console supports POSIX regular expressions, which are well documented elsewhere. Here are the basic regular expression syntax:

- ^ Match the beginning of a label.
“^i” would match “intel” but not “cisco”.

- \$ Match the end of a label.
“i\$” would match “intel” but not “airlink”.
- .
- Any single character.
“i.t” would match “intel” or “virtech” but not “cisco”.
- ? Zero or one of the previous character.
“i.?t” would match “intel” and “itech” but not the word “inert”.
- * Zero or more of the previous character.
“i.*e” would match “intel” and “virtech” but not “cisco”.
- + One or more of the previous character.
“i.*n” would match “intel” but “i.+n” would not.
- | Multiplicity operator
“intel|cisco” will match either “intel” or “cisco” but not “virtech”. The parenthesis can be used to encapsulate an expression. For instance “(el|co)\$”
- \ The escape character.
In order to find a dot, “.” will not suffice since it will select any character. Specifying “\.” overrides the default operation of the dot.
- {#,#} A certain count of the previous character.
The “{” operator specifies a range. At least one is required.
“i.{2}e” would match “intel” since there are 2 characters between the l and e.
“{2}” or “{2,}” can be read as “only 1 character”.
“{1,4}” can be read as “between 1 and 4 characters”.
- [range] A range of characters.
Ranges can be either an enumerated list of characters, such as “[abde]” or a hyphenated list such as “[A-Z]” or “[0-9]”. For instance “1[0-3]{2}” would match “103” and “121” but not “140” or “152”.
Additionally, ranges support the ^ operator for inversion. For instance, “^[^i]” would select say “airlink” and “netgear” but not “intel”.

Regular Expression Example

All local IPv4 networks

In IPv4 space, 10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0/16 are reserved for local networks. A regular expression that matches all of them would be as follows:

```
^(192\.168|10\.|172\.16)
```

Security Disclosures


Please carefully read the following important disclosures.

- Unlike with Wireshark, once a valid decryption key is defined, all relevant subsequent traffic is automatically decrypted, and, if saved, will be stored decrypted to disk.
- Independent of whether decryption keys are shown or hidden, they are stored on disk in plain text. Exporting a configuration file equates to exporting the plain text decryption keys that have been entered.

Appendix B Report Example Breakdown

Title

ACME Network Analysis Report



Report Information

Report created on 20 Mar 2008, 11:20.

Analyst Information

Name	Dilbert Dobson
E-mail Address	ddobson@phonecorp.com
Phone Number	808 555 1337
Client Information	
Client Name	Pointy Haired Boss
Case Number	3,000,000

MAC Conversations 2

Data Table 3

Cover Page

View Name

MAC Conversations

Conversations between hosts on a LAN segment

Applied on 3/20/2008 11:56:17 AM.

Source File: C:\Documents and Settings\ddobson\Desktop\decrypt.pcap

File Time: 3/19/2008 6:50:55 PM

File Size: 49Kb

Checksum (MD5): AAEF2E803D34555F6FF3633E83488348

MD5 Checksum

Mac Conversations

Host conversations on a LAN

**Notes section
for this chart**

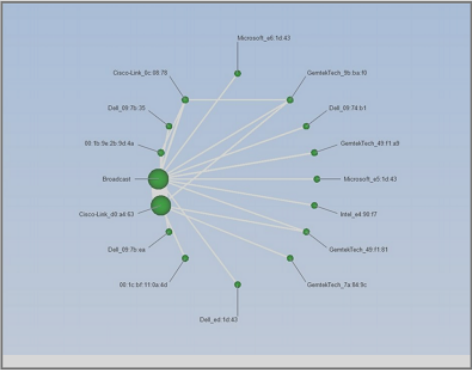


Figure 1 - Mac Conversations

Data

Src (A)	Dst (B)	TotBytes	TotPackets	BytesAB	BytesBA	PacketsAB	PacketsBA
00:03:ffe5:1d:43	ff:ff:ff:ff:ff:ff	130	1	130	0	1	0
00:03:ffe6:1d:43	ff:ff:ff:ff:ff:ff	162	1	162	0	1	0
00:12:3fed:1d:43	ff:ff:ff:ff:ff:ff	176	1	176	0	1	0
00:13:72:09:74:b1	ff:ff:ff:ff:ff:ff	340	1	340	0	1	0
00:13:72:09:7b:35	ff:ff:ff:ff:ff:ff	338	2	338	0	2	0
00:13:72:09:7b:ea	ff:ff:ff:ff:ff:ff	486	3	486	0	3	0
00:14:a5:49:f1:81	ff:ff:ff:ff:ff:ff	156	2	156	0	2	0
00:14:a5:49:f1:a9	ff:ff:ff:ff:ff:ff	680	8	680	0	8	0
00:14:a5:9b:ba:f0	ff:ff:ff:ff:ff:ff	234	3	234	0	3	0
00:14:bf:0c:08:78	00:14:a5:9b:ba:f0	140	1	140	0	1	0
00:14:bf:0c:08:78	00:1b:9e:2b:9d:4a	140	1	140	0	1	0
00:14:bf:0c:08:78	ff:ff:ff:ff:ff:ff	1752	12	1752	0	12	0
00:14:bfd0:a4:63	00:14:a5:49:f1:81	276	2	276	0	2	0
00:14:bfd0:a4:63	00:14:a5:9b:ba:f0	414	3	414	0	3	0
00:14:bfd0:a4:63	00:1b:9e:2b:9d:4a	1518	11	1518	0	11	0
00:14:bfd0:a4:63	00:1c:bf:11:0a:4d	552	4	552	0	4	0
00:14:bfd0:a4:63	00:90:4b:7a:84:9c	138	1	138	0	1	0
00:14:bfd0:a4:63	ff:ff:ff:ff:ff:ff	35568	247	35568	0	247	0
00:19:d1:e4:90:f7	ff:ff:ff:ff:ff:ff	130	1	130	0	1	0

Data as Table

Appendix C Example User/Group Configuration File

```
<PilotUsers>
  <Users>
    <User CanAccessProbeFiles="true" CanApplyViewsOnFiles="true"
CanApplyViewsOnInterfaces="true" CanCreateFiles="true" CanExportFiles="true"
CanImportFiles="true" CanShareViews="true" HasFolder="false" IsAdministrator="true"
Name="admin" PassHash="21232f297a57a5a743894a0e4a801fc3">
      <Groups>
        <Group Name="Administrators"/>
      </Groups>
    </User>
    <User CanAccessProbeFiles="true" CanApplyViewsOnFiles="true"
CanApplyViewsOnInterfaces="true" CanCreateFiles="true" CanExportFiles="true"
CanImportFiles="true" CanShareViews="true" HasFolder="false" IsAdministrator="false"
Name="normaluser" PassHash="34ea4aaaf24efcbb4b30d27302f8657f">
      <Groups>
        <Group Name="NormalUsers"/>
      </Groups>
    </User>
  </Users>
  <Groups>
    <Group Description="Administrators" IsAdministrator="true"
Name="Administrators"/>
    <Group CanAccessProbeFiles="true" CanApplyViewsOnFiles="true"
CanApplyViewsOnInterfaces="true" CanCreateFiles="true" CanExportFiles="true"
CanImportFiles="true" CanShareViews="true" Description="Normal unprivileged users"
HasFolder="true" Name="NormalUsers"/>
    <Group Description="Limited users that can only look at views"
HasFolder="true" Name="Viewers"/>
  </Groups>
</PilotUsers>
```