

SteelCentral™ Packet Analyzer Reference Manual

Version 10.8

January 2015

riverbed®

© 2015 Riverbed Technology. All rights reserved.

Riverbed®, SteelApp™, SteelCentral™, SteelFusion™, SteelHead™, SteelScript™, SteelStore™, Steelhead®, Cloud Steelhead®, Virtual Steelhead®, Granite™, Interceptor®, Stingray™, Whitewater®, WWOS™, RiOS®, Think Fast®, AirPcap®, BlockStream™, FlyScript™, SkipWare®, TrafficScript®, TurboCap®, WinPcap®, Mazu®, OPNET®, and Cascade® are all trademarks or registered trademarks of Riverbed Technology, Inc. (Riverbed) in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

Portions of SteelCentral™ products contain copyrighted information of third parties. Title thereto is retained, and all rights therein are reserved, by the respective copyright owner. PostgreSQL is (1) Copyright © 1996-2009 The PostgreSQL Development Group, and (2) Copyright © 1994-1996 the Regents of the University of California; PHP is Copyright © 1999-2009 The PHP Group; gnuplot is Copyright © 1986-1993, 1998, 2004 Thomas Williams, Colin Kelley; ChartDirector is Copyright © 2007 Advanced Software Engineering; Net-SNMP is (1) Copyright © 1989, 1991, 1992 Carnegie Mellon University, Derivative Work 1996, 1998-2000 Copyright © 1996, 1998-2000 The Regents of The University of California, (2) Copyright © 2001-2003 Network Associates Technology, Inc., (3) Copyright © 2001-2003 Cambridge Broadband Ltd., (4) Copyright © 2003 Sun Microsystems, Inc., (5) Copyright © 2003-2008 Sparta, Inc. and (6) Copyright © 2004 Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, (7) Copyright © Fabasoft R&D Software; Apache is Copyright © 1999-2005 by The Apache Software Foundation; Tom Sawyer Layout is Copyright © 1992 - 2007 Tom Sawyer Software; Click is (1) Copyright © 1999-2007 Massachusetts Institute of Technology, (2) Copyright © 2000-2007 Riverbed Technology, Inc., (3) Copyright © 2001-2007 International Computer Science Institute, and (4) Copyright © 2004-2007 Regents of the University of California; OpenSSL is (1) Copyright © 1998-2005 The OpenSSL Project and (2) Copyright © 1995-1998 Eric Young (eay@cryptsoft.com); Netdisco is (1) Copyright © 2003, 2004 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; SNMP::Info is (1) Copyright © 2003-2008 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; mm is (1) Copyright © 1999-2006 Ralf S. Engelschall and (2) Copyright © 1999-2006 The OSSP Project; ares is Copyright © 1998 Massachusetts Institute of Technology; libpq++ is (1) Copyright © 1996-2004 The PostgreSQL Global Development Group, and (2) Copyright © 1994 the Regents of the University of California; Yahoo is Copyright © 2006 Yahoo! Inc.; pd4ml is Copyright © 2004-2008 zefer.org; Rapid7 is Copyright © 2001-2008 Rapid7 LLC; CmdTool2 is Copyright © 2008 Intel Corporation; QLogic is Copyright © 2003-2006 QLogic Corporation; Tarari is Copyright © 2008 LSI Corporation; Crypt_CHAP is Copyright © 2002-2003, Michael Bretterkieber; Auth_SASL is Copyright © 2002-2003 Richard Heyes; Net_SSMTP is Copyright © 1997-2003 The PHP Group; XML_RPC is (1) Copyright © 1999-2001 Edd Dumbill, (2) Copyright © 2001-2006 The PHP Group; Crypt_HMAC is Copyright © 1997-2005 The PHP Group; Net_Socket is Copyright © 1997-2003 The PHP Group; PEAR::Mail is Copyright © 1997-2003 The PHP Group; libradius is Copyright © 1998 Juniper Networks. This software is based in part on the work of the Independent JPEG Group the work of the FreeType team.

This documentation is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation. Individual license agreements can be viewed at the following location: https://<appliance_name>/license.php

This manual is for informational purposes only. Addresses shown in screen captures were generated by simulation software and are for illustrative purposes only. They are not intended to represent any real traffic or any registered IP or MAC addresses.



Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com

712-00094-14

Contents

Overview.....	1
SteelCentral NetShark architecture	1
SteelCentral Packet Analyzer	2
Packet Analyzer– Feature Summary	2
Graphical User Interface	3
Wireshark Integration	3
AppResponse with NetShark Module Integration.....	3
Transaction Analyzer Integration.....	5
Views and Charts.....	7
Drill-down.....	7
Time Control	7
Filtering.....	7
Watches.....	8
Report Generation	8
NetShark web interface.....	8
Interface to the NetShark Packet Recorder Jobs Repository	8
Hardware and Software Requirements for Packet Analyzer	9
Graphical User Interface.....	11
Graphical User Interface Components.....	11
Ribbon Panel	12
Sources Panel.....	12
Views Panel.....	13
Main Workspace	13
Events Panel	14
Filters panel.....	14
Menu Button, Quick Access Toolbar, and Status Bar.....	15
Menu Button.....	16
Quick Access Toolbar	17
Settings Menu	18
Status Bar	23
Home Ribbon.....	24

Trace Files	24
Add Trace File.....	24
Add Folder.....	25
Clear List.....	25
Remote.....	25
Probes.....	25
General.....	25
Search.....	25
Update Sources	26
Close All Tabs.....	26
Getting Started	26
Wireless.....	26
Channels.....	26
Decryption Keys	27
View	27
Create.....	27
Save.....	27
Restore	27
Detach.....	28
Chart Selection	28
Send to Wireshark.....	28
Send to SteelCentral Transaction Analyzer.....	29
Send to File	29
Drill Down.....	29
Copy.....	29
Copy Chart.....	29
Time Control.....	31
Time Control Fundamentals	31
Time Control Ribbon.....	34
Quick Navigation	34
Begin.....	34
Step Back.....	34
Step Forward	34
End	35

Selection Duration	35
Time Selection	35
Watches and Events	37
Creating Watches on Strip Charts and Bar Charts	37
Watch in Sources Panel	38
Context Menu for Watch Applied to a Live Source.....	38
Context Menu for Watch Applied to a Trace File	38
The Watch Editor	38
Name and Description.....	39
Severity	40
Enabled.....	40
Trigger Conditions.....	40
Entering Values in Watch Triggers.....	41
Expanded Trigger Condition	42
Multi-line Strip Charts.....	42
Timing Details for Bar Charts.....	43
Actions	44
Transition Conditions.....	44
Notify Me	46
Send an email with the watch event details.....	47
Start a packet capture	48
Send a remote syslog message over UDP.....	48
Log the events in the Probe's syslog	49
Start a Capture Job.....	49
Stop a Capture Job.....	49
Log the events in a CSV file on the NetShark.....	49
Watches/Events Ribbon.....	50
Add Watch.....	50
Selected Watches.....	50
Edit Selected Watch	50
Remove Selected Watch	50
Enable Selected Watch.....	51
Disable Selected Watch.....	51
Filtering Events Section.....	51

Views Filter	53
Probes Filter	53
Severities Filter	54
Severities List	54
Watches and Events Filter	54
Events Overlay.....	55
Predefined Watches	56
Reporting Ribbon	58
Generate Report.....	58
Current View.....	58
All Views	59
Format.....	59
Open Reports	60
Management.....	60
Recent	60
Change Folder.....	60
Browse Folder	61
Settings	61
Title.....	61
Analyst/Client Information.....	61
Designer	61
Report Designer Ribbon	62
Styles	62
Includes	62
Change Logo	62
Table of Contents	62
Checksums	63
Cover Page	63
Data as Table.....	63
Visual Settings	63
White Chart Background.....	63
Draft Images (Faster)	63
Page Setup.....	64
Size	64

Orientation.....	64
Display	64
Page Width.....	64
Full Page.....	64
Custom.....	64
Close Designer	65
Accessing Remote Probes	67
Remote Ribbon	67
Probe Management.....	68
Add Probe.....	68
Probes.....	76
Probe Selection.....	77
Select All Probes	77
Expand Selection	77
Collapse Selection	77
Disconnect from Selected	77
Web Interface	77
Files.....	78
Import Files into Probes.....	78
Export Files from Probes	78
View Selection.....	78
Select All on Probes.....	78
Close Selected	78
Attach to Selected	78
Detach from Selected.....	78
Share Selected with.....	79
NetShark Packet Recorder.....	80
Terminology	80
Capture Jobs	81
Add/Edit Capture Jobs	83
Capture Settings	84
Retention Settings.....	85
Capture Job control buttons	87
Capture Jobs in the Packet Analyzer Devices panel.....	88

Capture Jobs in the Packet Analyzer Files panel.....	89
Sources Panel	103
Devices.....	103
Wired Ethernet Adapters.....	104
Wireless Adapters.....	104
Context Menus in the Devices Panel.....	105
With No Probes Selected.....	105
With a NetShark Selected	105
With an Interface Selected on Local System	106
With an Interface Selected on a NetShark	107
With a Job Virtual Device Selected (NetShark).....	107
With a View Selected (Local System and NetShark).....	108
Files	109
Context Menus in the Files Panel.....	111
With Nothing or Local System Selected.....	111
With a NetShark Selected	111
With a Trace Folder Selected on Local System	113
With a Trace File Selected on Local System.....	114
With a Trace Folder Selected on a Remote NetShark	116
With a Trace File Selected on a Remote NetShark	117
With the Jobs Repository Folder Selected on a Remote NetShark	119
With a Job Trace Selected on a Remote NetShark	119
With a Trace Clip Selected on a Remote NetShark.....	120
With a View Selected	122
Multi-Segment and Merged Sources	122
Views Panel.....	126
Using Views.....	127
Applying a View (Local or Remote Sources).....	127
Applying a View with a Filter	128
Applying Views in Multi-Segment Contexts	128
Using Views with Application Metrics.....	128
View Library	129
Context Menus.....	129
Tooltips	131

Recently Used	131
Context Menus.....	131
Custom Views.....	132
Context Menus.....	132
Search Text Box.....	135
Interactive Views.....	137
Regular Views, Fast Views, and Forbidden Views	140
View Editor	141
The General Approach	141
Activating the View Editor	151
The View Editor Interface	153
Saving a View and Exiting the View Editor	169
Applying Views	170
Multi-Chart Views	171
Microflow Indexing.....	177
Indexing a Trace File.....	177
Apply an Index to a Trace File	177
Context Menu.....	177
Add Microflow Index	177
Interrupt Microflow Index	178
Remove Microflow Index.....	178
Index Icons on Trace Files.....	179
Tooltips	179
Drag and Drop Cursors for Indexed Trace Files.....	179
Search Text Box.....	180
Main Workspace	181
Context Menus.....	182
Tooltips	182
Notes.....	182
Selection.....	183
Undocking Views.....	184
Conversation Ring.....	191
Default	191
Size Legends.....	192

Scroll Wheel.....	192
Hover with Tooltip	192
Selected	193
Top Conversations.....	193
Context Menu	194
Tooltips.....	196
Endpoint	196
Conversation	197
Sequence Diagram.....	199
Layers.....	199
Multi-Segment Sequence Diagram	200
Node.....	201
Node Layout	202
Selection.....	202
Highlight	202
Drag	203
Context Menu.....	203
Tooltip	206
Message	206
Selection.....	208
Highlight	208
Double click.....	208
Context Menu.....	208
Tooltip	211
Legend area.....	211
Scroll bar	212
Time Filter.....	212
Context Menu.....	212
Ruler Mode.....	214
Time Hints.....	215
Message Labels.....	216
Strip Chart	217
Diagram.....	217
Current Selection Interval	217

Display Modes	219
Data Display	220
Stacking Order.....	221
Custom sampling interval.....	222
Selection.....	223
Context Menu	224
Tooltips.....	226
Bar Chart.....	227
Single Bar Chart	227
Default	227
Selection.....	227
Stacked Bar Chart.....	228
Default	228
Selection.....	228
Grouped Bar Chart.....	228
Default	229
Selection.....	229
Navigation Through Data.....	231
Context Menu	232
Tooltips.....	234
Scatter Plot.....	235
Default	235
Selection.....	236
Context Menu	237
Tooltips.....	239
Pie Chart.....	240
Default	240
Selection.....	240
Context Menu	241
Tooltips.....	242
Data Grid	243
Grouping Bar	244
Column Headers.....	244
Sorting.....	244

Filter Bars	244
Values.....	245
Operators.....	246
Selection	246
Summaries	247
Context Menu	248
Channels Button.....	251
All Channels.....	253
2.4GHz Center Frequencies:	253
5GHz Center Frequencies:	253
Channel Names	253
All Channels Panel	254
Channel List.....	255
Selection Controls	255
Search and Filter Bar	255
Locked Channels	256
Title.....	256
Selection Controls	256
Transfer Controls	256
Scan Sequence	257
Duration.....	257
Selection Controls	257
Transfer Controls	258
Scan Sequence	258
Decryption.....	259
Wireless Decryption Keys Manager.....	259
Adding a Key	260
WPA Related Packet Injection	261
Drill Down.....	263
How to.....	263
Examples.....	263
Filtering	264
Filter panel.....	264
Apply	265

Prepare	265
Edit	266
Delete	266
Duplicate.....	266
Move to Top.....	266
New Filter/Folder	266
Sort.....	267
Reset Filters.....	267
Filter Bar	268
Save.....	269
Delete	269
Apply	269
Prepare	269
Delete All.....	270
Filter Dialog.....	271
Search Dialog.....	272
Search Context.....	272
Search Style.....	272
Regular Expression Example.....	274
Multi-Segment Analysis (MSA)	275
General approach	276
Review timestamp settings at the packet source	276
Assemble the data.....	276
Make a multi-segment source.....	277
Adjust time skews (if necessary).....	277
Apply views	280
Navigating a multi-segment sequence diagram	282
Select and zoom.....	282
Use the slider	283
Use the mouse wheel or the up- and down-arrow keys	283
View delays and round-trip times.....	284
Estimate network delays	287
Label message lines.....	289
Simplify a sequence diagram.....	289

Security Disclosures	292
Appendix A Chart Types	293
Appendix B Report Example Breakdown	295

About this guide

This manual discusses the Riverbed® SteelCentral™ Packet Analyzer (Packet Analyzer), as it is used in conjunction with local sources of network data and with the Riverbed® SteelCentral™ NetShark (NetShark), and the Riverbed® SteelCentral™ NetExpress.

The purpose of this reference manual is to document and explain each Packet Analyzer 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 intended to be a tutorial on the use of Packet Analyzer. Video tutorials on how to perform common actions are available in the product. Upon startup, the Packet Analyzer displays links to video tutorials. These can also be accessed at any time by clicking the *Getting Started* icon, located in the “General” section of the “Home” tab.



This page intentionally left blank.

Overview

Riverbed® SteelCentral™ Packet Analyzer works with a Riverbed® SteelCentral™ NetShark Model xx00 or Model xx70 or a Riverbed® SteelCentral™ NetExpress to provide a complete enterprise-wide solution for increased network visibility through live traffic monitoring, line-rate packet capture, real-time and historical traffic analysis, monitoring, and reporting from multiple locations.

SteelCentral NetShark architecture



SteelCentral NetShark Model xx00 appliances



SteelCentral NetShark Model xx70 appliances

The SteelCentral NetShark, which houses the traffic analysis engine along with a custom packet recording facility, extends the reach of the Packet Analyzer to geographically-dispersed network locations. NetShark appliances are designed for placement at strategic points throughout your network, thereby providing the visibility necessary for global monitoring and troubleshooting. The NetShark comes as a fully configured rack mountable appliance including one or more network interfaces for network traffic capture.

A NetShark also includes the NetShark Packet Recorder, a customized packet capture application for high fidelity, multi-gigabit per second network traffic recording.

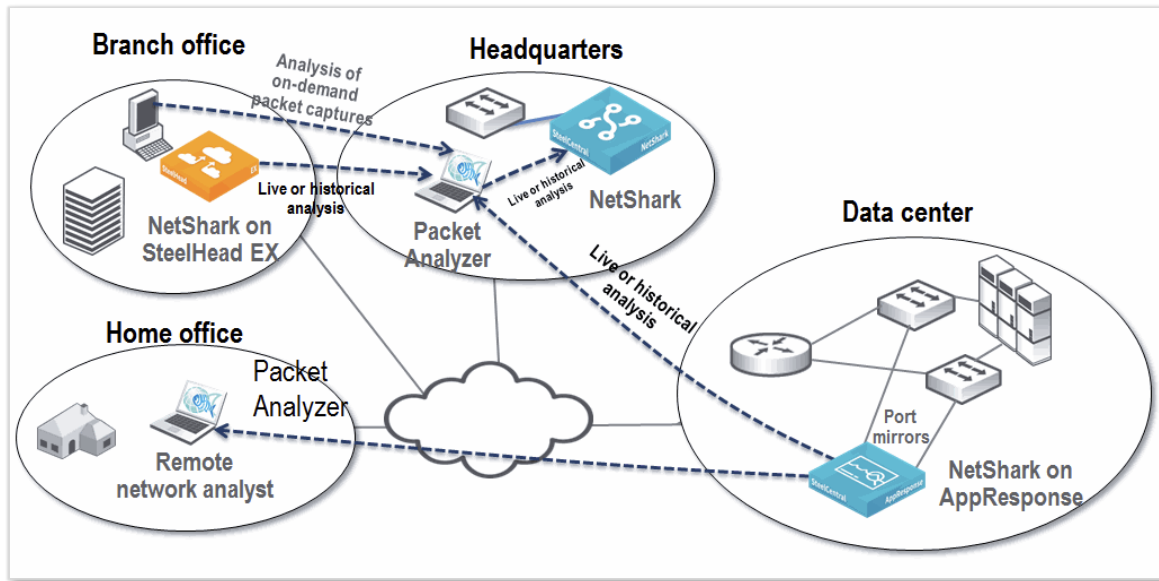
A NetShark virtual edition performs similar functions running as a virtual machine in a virtual environment.

A NetExpress provides packet capture and export functions, in addition to flow data collection and reporting. Note: In the NetExpress Wireshark filters and all custom views created using Wireshark fields do not work on any traffic source (capture interfaces, capture jobs, trace clips, trace files).

In this manual, references to NetShark appliances generally include NetShark virtual edition and NetExpress.

SteelCentral Packet Analyzer

Packet Analyzer seamlessly and securely interfaces with one or more NetShark appliances to display, drill down into, rewind, alert on, and report on, network traffic captured and/or analyzed by NetShark appliances. Packet Analyzer is an analysis tool tailored to distributed environments with the ability to efficiently access and manipulate large packet trace files. It contains an extensive collection of network traffic analysis metrics (Views), drag and drop drill-downs, visualization and analysis of long-duration capture statistics, flexible trigger-alert mechanisms, and report generation.



Deployment example

Packet Analyzer– Feature Summary

Packet Analyzer includes the following features:

- Graphical user interface for displaying data collected by remote NetShark appliances and local network traffic sources
- Wireshark Integration
- Riverbed® SteelCentral™ AppResponse with NetShark Module Integration
- Riverbed® SteelCentral™ Transaction Analyzer Integration
- Views and Charts, including a View Editor for editing existing views or creating new ones
- Drill-down
- Time Control
- Watches
- Report Generation
- Access to the NetShark web interface
- Interface to the NetShark Packet Recorder's Jobs Repository

Graphical User Interface

Packet Analyzer can view and analyze network traffic on local interfaces or trace files, and also connect to and manage one or more remote NetShark appliances. When connected to remote NetShark appliances, Packet Analyzer can analyze and view traffic from network interfaces of the NetShark appliances as if these remote interfaces were local.

Packet Analyzer can simultaneously connect to multiple NetShark appliances, while multiple instances of Packet Analyzer can simultaneously connect to the same NetShark. Access to a single appliance from multiple locations provides excellent visibility into the network as well as an intuitive mechanism for sharing network Views, Watches, and Reports with co-workers and management.

Wireshark Integration

Packet Analyzer and NetShark 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. During any stage of the analysis, Packet Analyzer can select a local or remote traffic source and send it to Wireshark for packet filtering or deep packet inspection.

AppResponse with NetShark Module Integration

Starting with version 10.5, Packet Analyzer can connect to a NetShark Module (version 10.0.7-arx2) running on most SteelCentral™ AppResponse appliances. This requires you to install the RPM Integration Version 2 patch and a license on the AppResponse. See the *SteelCentral AppResponse RPM Integration Getting Started Guide* for information on specific software requirements and supported AppResponse appliances.

All AppResponse with NetShark Module configuration is done through the AppResponse, using the ARX CLI. There is no web interface access from Packet Analyzer to an AppResponse with NetShark Module appliance.

ARX traffic capture

Capture jobs are automatically configured when a NetShark Module starts.

- One capture job is configured for the aggregating interface (**arx**) and each Monitoring Interface Group (MIFG) virtual interface (**arxN**). For example, the capture job for the MFIG_1 interface is **arx1**.
- A NetShark Module capture job cannot be modified and it cannot be stopped or started. You cannot use filters or specify any retention settings (space or time) for a capture job.
- Indexing is enabled by default and the NetShark Module computes a microflow index for each capture job. Each index is synchronized with the retention time of the capture job.

You enable or disable indexing globally, for all capture jobs, not for individual capture jobs. Use the NetShark Module subsection of the AppResponse CLI to manage indexing. **Note:** When indexing is disabled, all index data are deleted.

Packet Analyzer lists all capture jobs, with a capture job's status shown as **active** or **inactive**, the same as the interface's status. When inactive is displayed in an interface's description, no traffic is received on that interface. The aggregating port (**arx**) and MIFG ports are mutually exclusive - when MIFGs are enabled, the **arx** port status is **inactive**; when MIFGs are disabled, the aggregating port is **active**. **Note:** When MIFGs are enabled, a MFIG port requires a connection to at least one physical port to have an active status. For more information, see the "Monitoring Interface Groups

(MIFGs) and Packet Captures” section in the “Packet Captures” chapter of the *SteelCentral AppResponse User Guide*.

Sending capture files or trace clips to Packet Analyzer for analysis requires the use of AppResponse Java Console, version 8.6.8 (or later); it must be installed on the same system as Packet Analyzer. For more details and an example, see the *SteelCentral AppResponse RPM Integration Getting Started Guide*.

NetShark Module live sources, capture files, and trace clips can be analyzed with any Packet Analyzer views except the following:

- 802.11 Views
- Interactive Views
- Network Usage by Application
- Multi-Segment Analysis (MSA) Views
- Sequence Diagram Views
- Network Usage Analysis

Packet Analyzer also can send trace files to SteelCentral™ Transaction Analyzer for analysis. For details, see “Transaction Analyzer Integration” below.

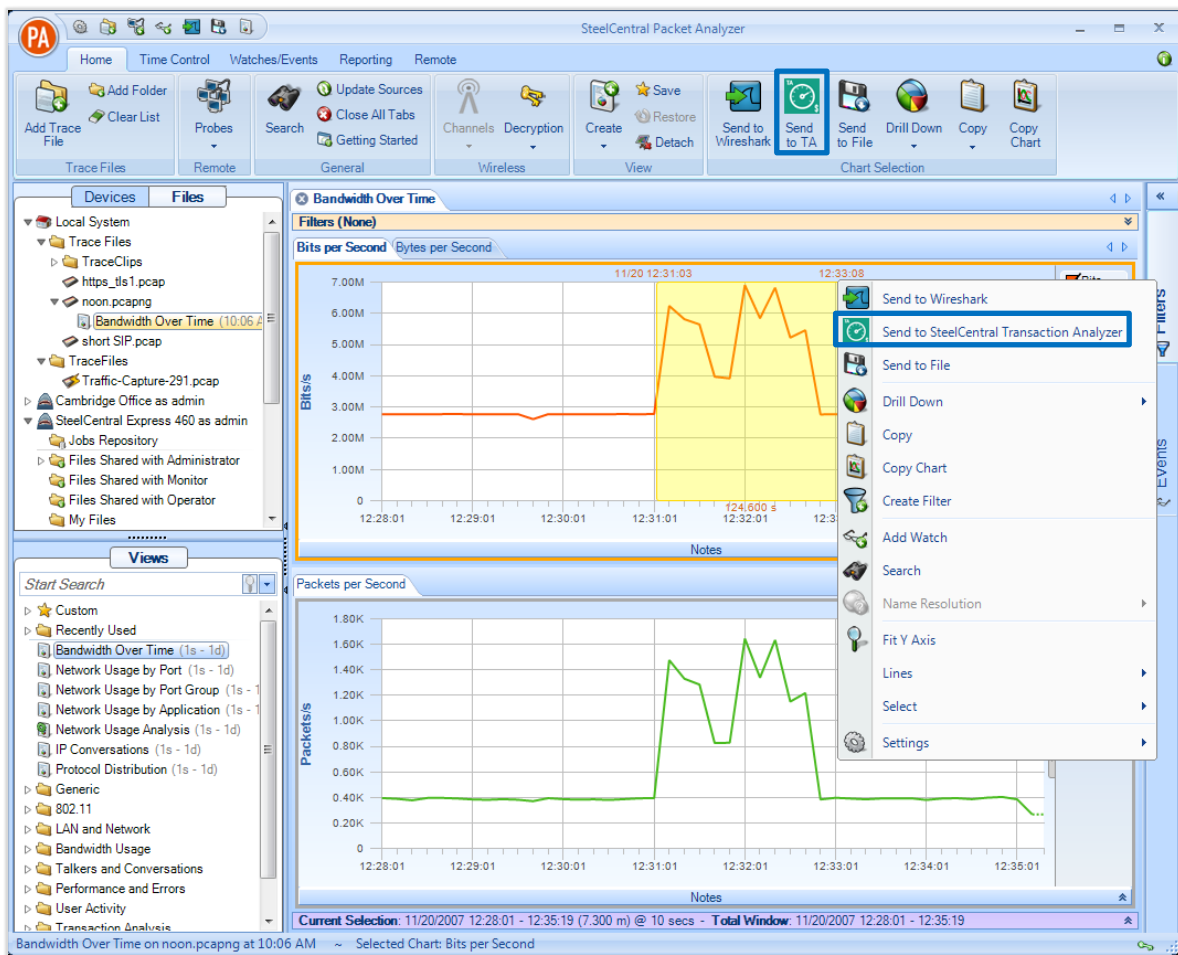
Transaction Analyzer Integration

Starting with version 10.0.7, Packet Analyzer can be used to quickly scan local and remote capture files and send selected packets to Transaction Analyzer for analysis. Version 16.5.T PL1 (or later) of Transaction Analyzer must be running on the same local system as Packet Analyzer.

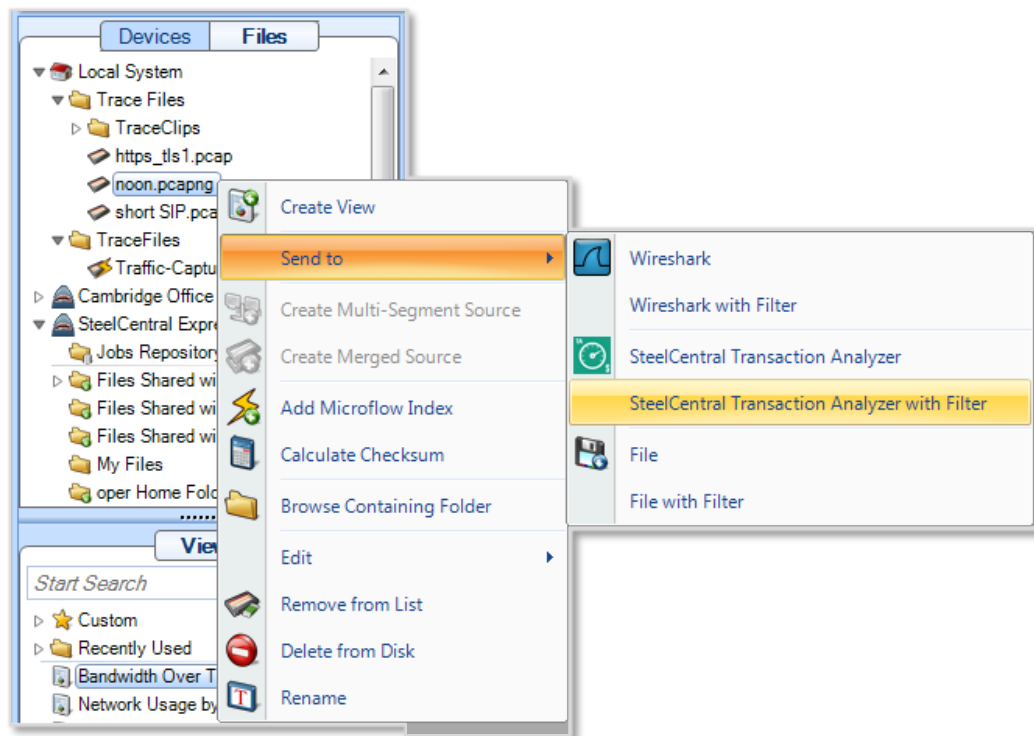
Sources include local and remote capture files; trace clips; and merged files. Pcap-ng and pcap (nanosecond) files are converted to Pcap (microsecond) files when sent to Transaction Analyzer.

The following sources cannot be sent to Transaction Analyzer: live interfaces, multi-segment files, and 802.11 link type files.

In Packet Analyzer, packets can be sent to Transaction Analyzer by right clicking on a file and using the “Send to” item on the displayed context menu or by clicking on a chart or making a selection on a chart in the main workspace and selecting “Send to TA” from the “Chart Selection” section of the “Home Ribbon.” Also, right clicking on a chart or a selection on a chart opens a context menu where you can select “Send to SteelCentral Transaction Analyzer” (see an example below).



Using Packet Analyzer, filters can be applied to packet sources before sending them to Transaction Analyzer. When using the “Send to” item on a context menu, select “SteelCentral Transaction Analyzer with Filter” to apply a filter before sending files to Transaction Analyzer, thereby reducing the size of a trace file and sending only those packets of interest.



Selections on charts, as well as Views and Filters applied to a source, filter a source before sending packets to Transaction Analyzer.

When a large file (more than 100,000 frames) is sent to Transaction Analyzer, a message appears recommending you reduce the file size by filtering the file using Trace Explorer. If you choose to continue, it may take a long time to import the file into Transaction Analyzer.

Sending a Source to Transaction Analyzer

Note: For help in using Packet Analyzer to analyze trace files, view the Quick-Start Video Tutorials, opened by clicking the **Getting Started** icon in the General section of the Home tab.

1. Choose a packet source in Packet Analyzer.
2. To send a trace file, right click the file, and then, on the “Send to” sub-menu of the context menu, choose **SteelCentral Transaction Analyzer** or **SteelCentral Transaction Analyzer with Filter**.

Alternatively, you can apply Packet Analyzer Views and Filters to identify traffic you wish to analyze in Transaction Analyzer. Use Drill Down to apply additional views to selected chart elements and narrow down the traffic further.

3. Select a chart or select data of interest on a chart, then right-click it, and choose **Transaction Analyzer** from the pop-up Context Menu. You also can click the **Send to TA** button in the Chart Selection section of the Home tab.

If the source is remote, the packets are first downloaded to the Local System before being sent to Transaction Analyzer.

If processing is needed, for example, converting a Pcap-ng file to Pcap (microsecond), a temporary file is prepared for use by Transaction Analyzer, otherwise the original source is used. When the transfer is completed, Transaction Analyzer is opened and begins processing the packets.

4. When you complete your investigation in Transaction Analyzer, you can save the packets as a Transaction Analyzer file (*.atc).

Views and Charts

Views are the core analysis and visualization paradigm in Packet Analyzer. The system offers over 200 views providing a broad range of protocol support for both wireless¹ and wired network analysis. When views are applied to a traffic source, the results are displayed via a collection of interactive components called Charts. The collection of Charts includes bar, pie, and strip charts, sequence diagrams, scatter plots, conversation rings, and grids. All charts are interactive – they can be resized, moved, and, most importantly, users can make visual selections on graphical elements within a Chart (such as individual bars in a bar chart or time intervals in a strip chart) and drill down from there. Charts can be customized, saved, imported/exported in a variety of formats, and shared with colleagues. Chart data can also be exported included as part of Packet Analyzer automated report generator.

Drill-down

Drill-down is one of the most powerful and unique features of Packet Analyzer. 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 Chart display. This simple yet powerful exercise increases your analysis capabilities many-fold. By employing this visually based drill-down feature, Packet Analyzer can analyze very large trace files quickly, guiding you to the handful of packets responsible for anomalous network behavior.

Time Control

Viewing metrics computed over days, weeks, and months can be overwhelming. With the Packet Analyzer “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 Time Control technology applies to live and off-line traffic.

Filtering

In addition to Drill-down, filtering is a powerful resource to analyze data and focus down on packet data sources. Filters can be chosen from the Filter panel and easily applied to the current view by dragging them over existing charts. In addition, the currently applied filters can be edited and/or combined by using the Filter Bar on the top of the view, which enables fast and responsive data analysis. Users can create filters from existing charts by selecting elements such as time ranges, or

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

choose among NetShark, BPF, Wireshark and time filters. Users can also organize custom filters in folders in the Filter panel.

Watches

The Packet Analyzer 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 occur. When a Watch detects that a trigger condition is met, a specified action is taken, such as logging the event, sending email, 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)
- IP Fragmentation Analysis
- DHCP Address Assignments
- TCP Top Talkers
- Unicast vs. Multicast vs. Broadcast Traffic
- And others

NetShark web interface

Packet Analyzer provides access to the NetShark configuration manager. The web interface supports the following configuration tabs:

- **Status** – Shows the status and enables restart of the NetShark.
- **Capture Jobs** – Shows the status of all of the current Capture Jobs, and enables adding, editing, deleting, starting, or stopping capture jobs.
- **NetProfiler Export** – Allows exporting network flow data to NetProfiler.
 - Beginning with version 10.8.0, NetShark can export NetFlow v9 flows to third-party flow collectors.
- **Interfaces** – Views and configures the packet capture board(s) on the NetShark.
- **Settings** – Configures various settings of the appliance.
- **System** – Performs licensing, update, and maintenance tasks.

Note that Packet Analyzer does not support access to the web interface of the SteelCentral™ NetExpress. Packet Analyzer can view capture jobs on a NetExpress, but it cannot add or edit them.

Interface to the NetShark Packet Recorder 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 may be a very large, multi-terabyte file. Using the “Trace Clip” creation feature of Packet Analyzer, 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 Packet Analyzer operations that apply to trace files can be applied to Trace Clips as well.

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.

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 Packet Analyzer

Beginning with release 10.5, Packet Analyzer no longer requires administrator privileges to install the product for use by a single user on a PC. To enable all users on a PC to run Packet Analyzer, the installer must be run by a user with administrative privileges. Starting with release 10.6 (and later), “Install for All users” is the default selection on the first screen of the installer.

Once installed, Packet Analyzer requires activation by a license to operate. Two types of user licenses are available: single-seat licenses, activated by an administrator using a product key, or concurrent licenses, requiring a concurrent license server on your network and a temporary license activated by an administrator. Each user must have a license to operate Packet Analyzer. For installation instructions, see the *SteelCentral Packet Analyzer Installation Guide*.

Although the system requirements for a Packet Analyzer scale with usage, the following minimum configuration is recommended in order to use Packet Analyzer effectively:

Operating System

Windows XP (SP3), Windows Vista, Windows 7, Windows 8, Windows 8.1

System Software

Microsoft NET Framework 4.0 (or later)

Host Hardware

A dual-core 2.0 GHz CPU or better

Available Disk Space

A base installation requires approximately 300MB of disk space. Additional space is required to store generated reports or trace files created with Packet Analyzer.

Memory

2 GB or more of system memory

Video Hardware and Settings

A graphics card with a minimum resolution of 1024 x 768

Display Setting

Text size: 100% (default) -displayed text may be truncated when a larger text size is used – see Control Panel > All Control Panel Items > Display.

Network Connection

A network connection to a NetProfiler, a NetExpress, or a NetShark (including virtual editions) is needed if you are using a concurrent license server. See the Riverbed SteelCentral NetShark Release Notes, version 10.7, for more information on the NetShark concurrent license server.

This page intentionally left blank.

Graphical User Interface

Graphical User Interface Components

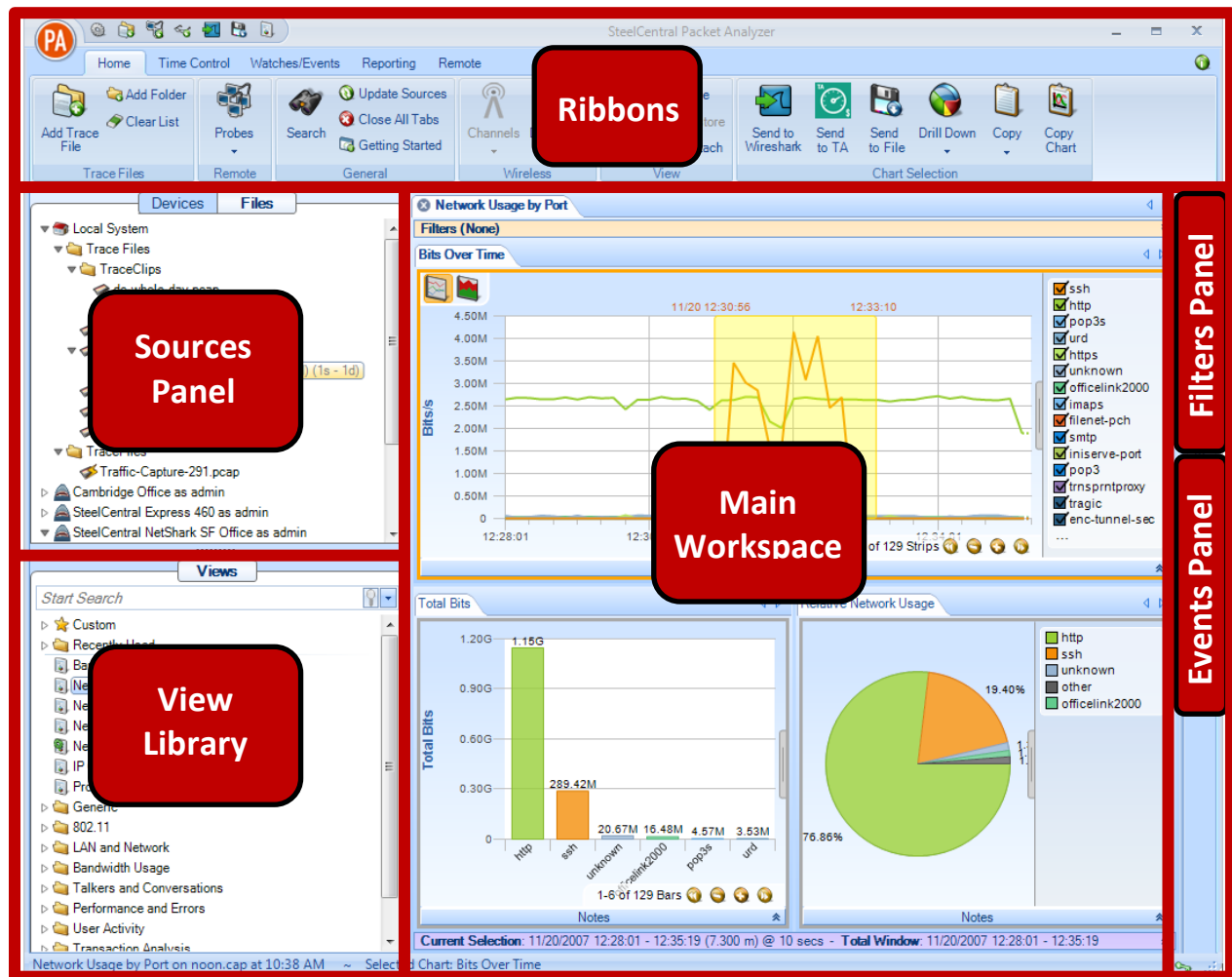


Figure 1: User Interface Breakdown (Major)

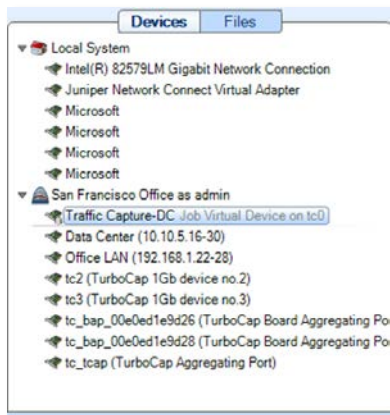
The graphical user interface of Packet Analyzer, divided into the six main sections, is shown in Figure 1. Each section represents a major topic in this manual. The descriptions below are conceptual.

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



The *Sources Panel* contains representations of NetShark appliances, interfaces, and trace files and is one of the most important parts of Packet Analyzer. It has two tabs, “Devices” and “Files” that can be cycled through by clicking on them.

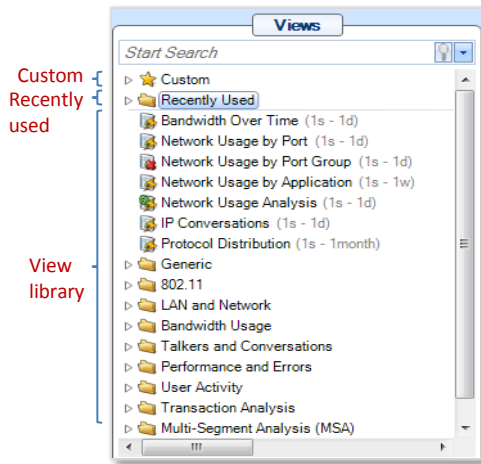
Devices

Shows both local interfaces under the Local System icon and interfaces on connected NetShark appliances that offer live sources of network traffic.

Files

Shows folders and trace files on the local system and connected NetShark appliances.

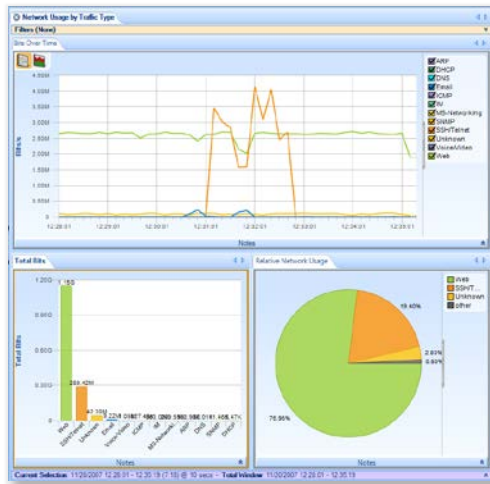
Views Panel



The *Views Panel* contains a set of network traffic analyses called “Views”. Each View computes specific metrics, such as bandwidth over time, IP conversations or protocol distributions 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.).

To find Views and Folders quickly, enter one or more keywords in the Search box at the top of the Views Panel. The scope of the search includes titles and descriptions by default; you can expand the scope using the drop-down menu (down arrow) on the right side of the search box.

Main Workspace



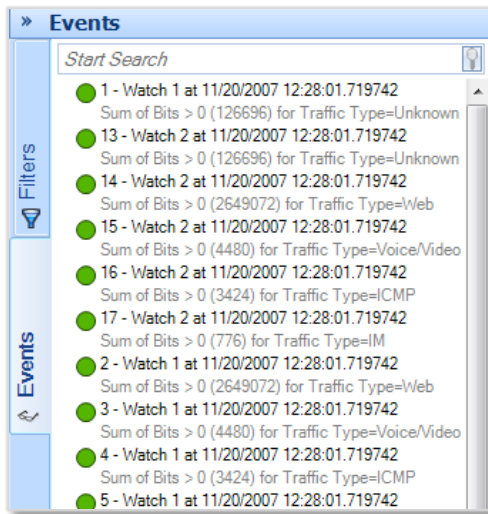
The *Main Workspace* has tabbed windows that can be one of the following:

- Getting Started Tab
- Applied Views
- Report Preview

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 by middle-clicking the tab itself.

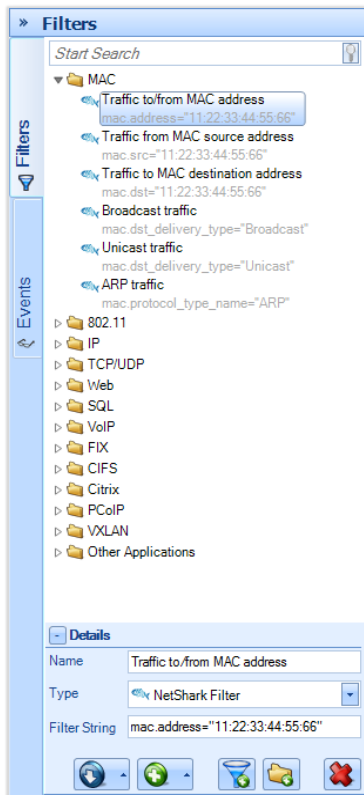
In addition, you can “undock” the main workspace to create a separate window that you can enlarge and place wherever you want, even on a second monitor.

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.

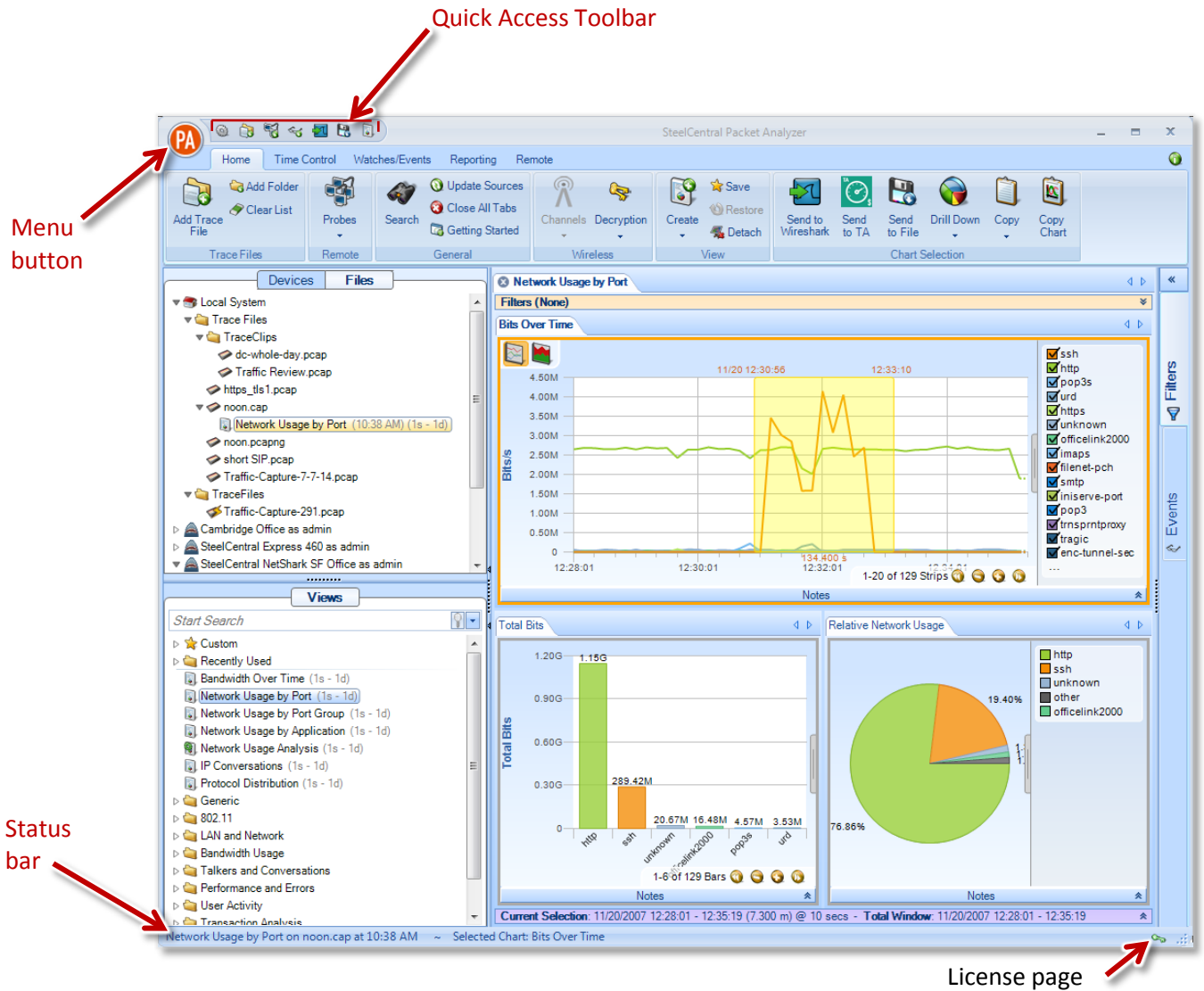
Filters panel



The *Filters Panel* contains all the user filters organized in folders. All existing filters can be copied or moved through folders, edited and removed. New filters can be created from scratch or dragged into the panel from a chart selection.

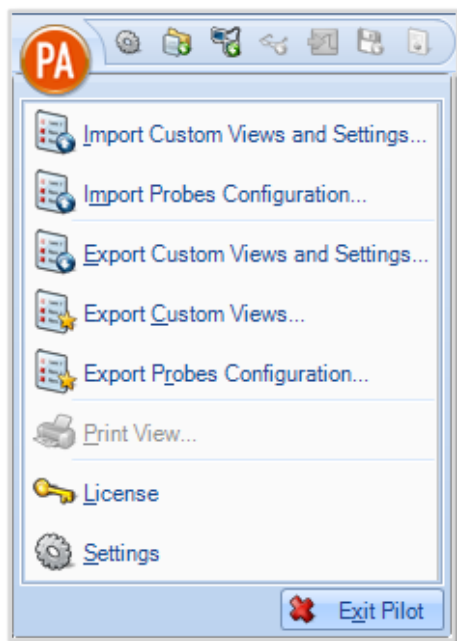
Menu Button, Quick Access Toolbar, and Status Bar

The user interface also includes a Menu button and Quick Access toolbar at the top and a Status bar at the bottom.



User Interface Breakdown (Minor)

Menu Button



The *Menu Button* has the following components:

Import Custom Views and Settings

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

- Remote NetShark appliances and probe groups
- Custom views
- Custom filters
- 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.

Import Probes Configuration...

Imports a probes configuration from a saved probes configuration file (.ppf format). The new settings are applied after a restart.

Export Custom Views and Settings...

Prepares a file that can be imported into another instance of Packet Analyzer. This file contains the global configuration file, whose settings are enumerated throughout this manual.

Export Custom Views...

Prepares a file that can be imported into another instance of Packet Analyzer that contains only the custom views.

Export Probes Configuration...

Exports the current probes configuration to a probes configuration file (.ppf extension).

Print View...

Creates a default report from the current view and sends it to the printer. The report is not saved to disk.

License

Opens the Packet Analyzer personal edition License page, providing a direct way to activate, deactivate or review your license information.

Settings

Opens the Settings menu, described [below](#).

Quick Access Toolbar

The Quick Access Toolbar has the following buttons:



Settings

Opens the Settings menu, described below.



Add a Trace File

Adds a trace to the Files panel.



Add Probe

Connects to a probe.



Add Watch

Opens the Watch Editor and creates a new watch on the current selection in the currently selected chart in the view.



Send to Wireshark

Sends traffic from the current selection to Wireshark. This button is enabled only if a selection is made in the currently selected chart in the view.



Send to File

Extracts traffic from the current selection and sends it to disk as a PCAP trace file. This button is enabled only if a selection is made in the currently selected chart in the view.



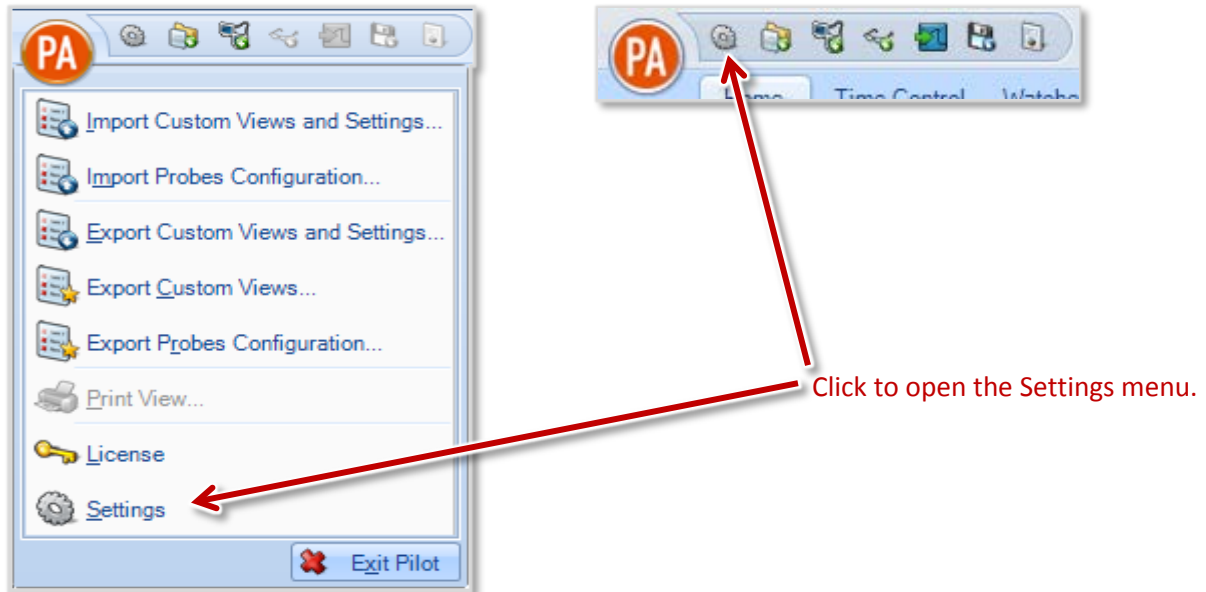
Create Report from Current View

Creates a report from the currently selected view.

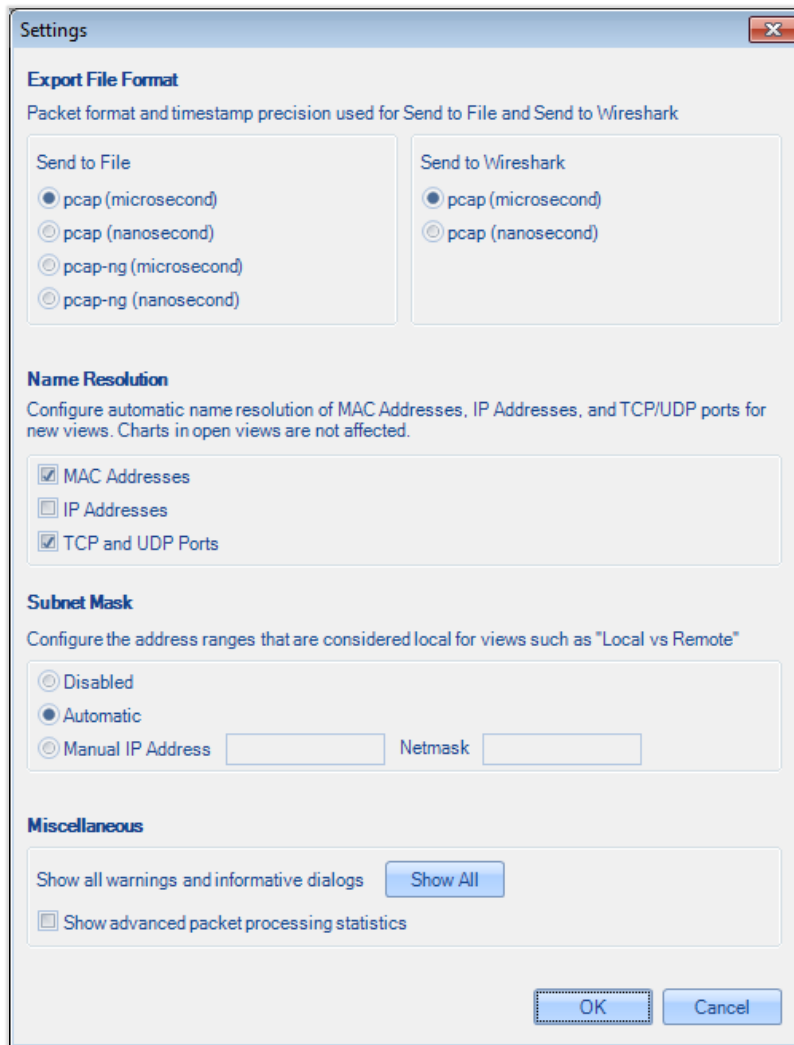
Settings Menu

The Settings menu lets you configure parameters for some of the operations available in Packet Analyzer.

Open the Settings menu by clicking the Menu button and selecting Settings from the drop-down list or by clicking the Settings icon in the Quick Access Toolbar.

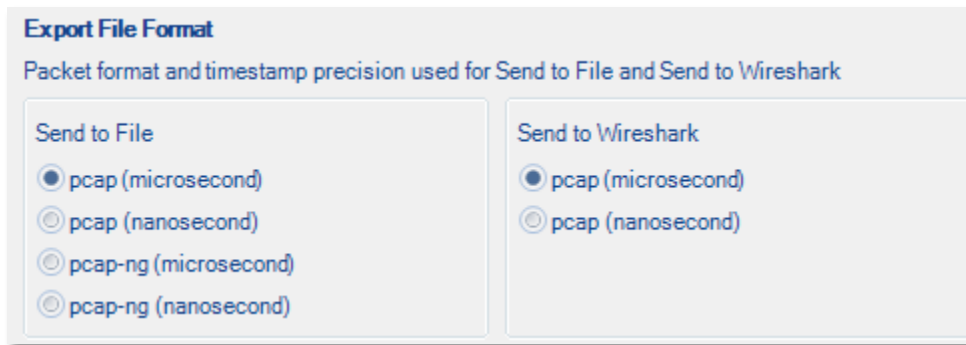


The Settings menu appears. The image below shows the default values.



Export file format

These settings determine the format and timing precision for “Send to...” operations.



The “Send to File” option lets you configure the format that Packet Analyzer uses to create a trace file from another trace file or from a subset of one. In addition, this option is used when Packet Analyzer exports packets from a trace clip. This option is especially useful if you need to use a trace file with a tool that does not support the pcap-ng format or nanosecond timestamps.

The “Send to Wireshark” option lets you configure the format that Packet Analyzer uses to export a trace file or a subset of a trace file to Wireshark. Due to a limitation of Wireshark versions before 1.8.2, it is not possible to export packets with pcap-ng format to Wireshark.

Name resolution

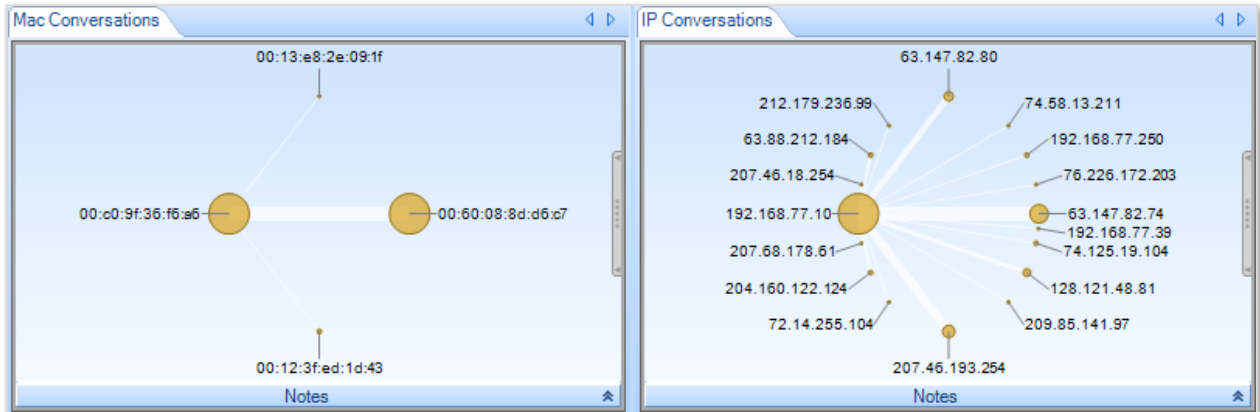
These settings let you determine whether MAC or IP addresses or TCP/UDP port numbers are presented as numbers or names (when possible). In views, name resolution can be set per chart using the Name Resolution item on a chart’s submenu.



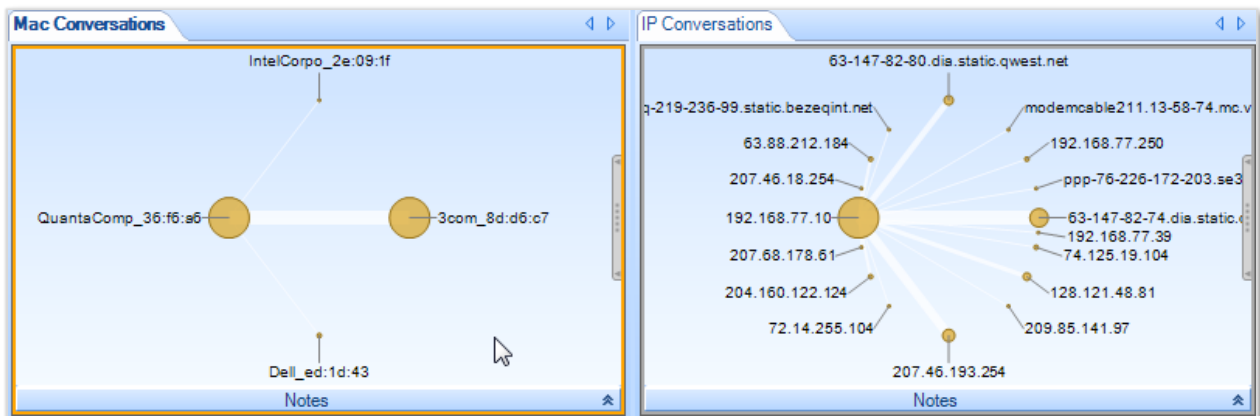
When a box is checked, Packet Analyzer searches its configuration files for names that are equivalent to MAC addresses, IP addresses, or TCP/UDP port numbers.

When you modify an option, only new views reflect the new options. There may be a brief delay while names are resolved.

For instance, here is a view with MAC and IP addresses not resolved:



And here is the same view with both MAC and IP addresses resolved:



Note that names have replaced some of the numbers in the addresses.

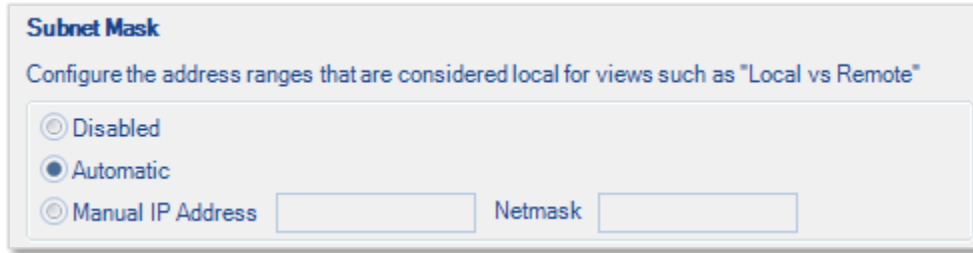
The name resolution is performed in Packet Analyzer, not in NetShark appliances. MAC addresses and TCP/UDP port names are stored in these files:

- MAC addresses: [Packet Analyzer installation folder]\data\Manufacturers.xml
- TCP/UDP port names: [Packet Analyzer installation folder]\data\PortNumbers.xml

When you modify an option, only new views reflect the new options. There may be a brief delay while names are resolved.

Subnet mask

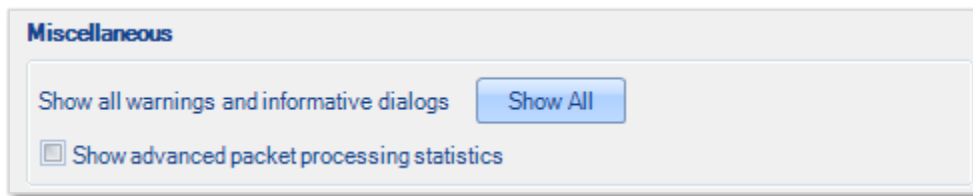
This option allows you to configure which addresses are considered to be “local” for some views.



- **Disabled:** All IP addresses are considered local.
- **Automatic:** Local System or NetShark determines which is the best local address range (for instance, 192.168.0.0/16).
- **Manual:** You specify the local address range by entering an IP address and a subnet mask.

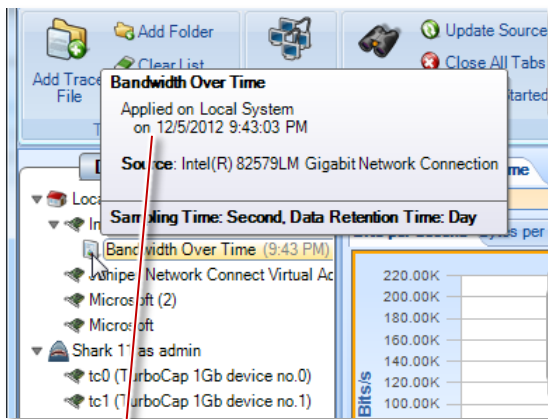
Changes are applied to the source type currently selected in the Devices/Files panel. This allows you to maintain separate configurations for both Local System and remote NetSharks.

Miscellaneous

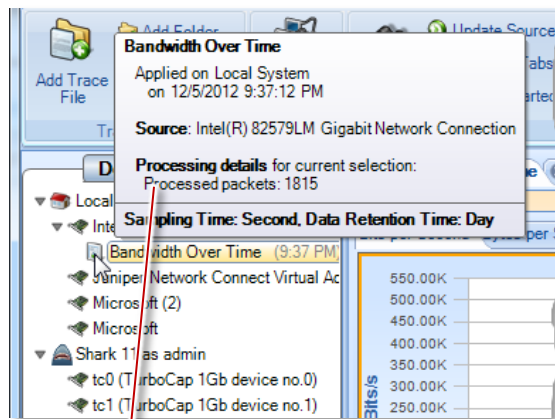


The “Show all warnings and informative dialogs” button lets you turn on the display of all warnings and dialogs. This can be useful if you have previously turned off the display of some messages (by checking a “Do not show this again” box), but want to start seeing those messages again.

The “Show advanced packet processing statistics” option defines whether Packet Analyzer exports processing statistics in tooltips or not.



Processing statistics disabled



Processing statistics enabled

Status Bar

A screenshot of a status bar with a light blue background and a thin border. The text inside is "Network Usage by Traffic Type on noon.cap at 12:27 PM" followed by a tilde symbol and "Selected Chart: Bits Over Time".

Network Usage by Traffic Type on noon.cap at 12:27 PM ~ Selected Chart: Bits Over Time

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



The *Home Ribbon* serves as the primary interface to Packet Analyzer. 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** – Operations such as adding a link to a trace file in the Sources panel.
- **Remote** – Connection to a NetShark.
- **General** – Miscellaneous actions.
- **Wireless** – Wireless channel and decryption settings.
- **View** – Buttons for creating Interactive Views, saving custom views, and detaching from a view.
- **Chart Selection** – Operations apply to active selection in a chart in the “Main Workspace.” Drill-down steps including Send to Wireshark/ SteelCentral Transaction Analyzer /File.

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

Trace Files

This section describes 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 Packet Analyzer.

Add Trace File



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

Add 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



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

Remote

The *Remote* section allows you to manage probes. The *Probes* button in this section is the same as the Probes button on the Remote Ribbon.

Probes



The *Probes* button allows you to manage probes. For full details, refer to the [Probe Management](#) description in the Remote Ribbon, on page 68.

General

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

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 that can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section.

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 Packet Analyzer recognizes a change of device. Packet Analyzer does not check for new adapters automatically. It checks only when this button is clicked.

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



The *Getting Started* button opens a tab in the main workspace that provides access to video tutorials

Wireless

The *Wireless* section contains settings for configuring wireless device and traffic monitoring.

Channels



The *Channels* 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: [Channels Button](#).

Note: This operation applies to only AirPcap adapters installed on the Packet Analyzer host system.

Decryption Keys



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” later in this document.

Note: Decryption is available for live AirPcap traffic sources on the local Packet Analyzer and on wireless trace files located on the local system or remote probes.

View

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

Create



The *Create* button opens the View Editor with a blank, fully editable new view. The submenu (drop-down arrow) gives you the choice of creating either a new view or an interactive view.

Create View

Save



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

**Save
Custom
View**

Restore



The *Restore* button restores default View settings.

**Restore
Default
View**

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 Packet Analyzer 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.

You can “attach” to the View by right-clicking the View in the sources panel and selecting the Attach submenu item, thereby making the View visible in the Packet Analyzer main workspace.

Detaching a View from a capture job running on a NetShark is an excellent way to leave a View running overnight or over a weekend. When you start up Packet Analyzer again and reconnect to the NetShark, you can attach the View and see all the information that has been collected since the capture job started.

Chart Selection

Several functions are common among the charts and are enabled only if there is an active selection in a chart. These functions are on the Home Ribbon in the Chart Selection group. Each of these functions is also available through the context menu of any chart.

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 is transmitted over the network to Wireshark running on the Packet Analyzer local system.

Send to SteelCentral Transaction Analyzer



The Send to SteelCentral Transaction Analyzer button sends traffic from the current selection to Transaction Analyzer (formerly known as App Transaction Xpert (ATX)) by spawning a new instance of Transaction Analyzer on the local system and delivering the selected packets to it for analysis (requires Transaction Analyzer version 16.5.T PL1 (or higher) installed on local system). “Send to SteelCentral Transaction Analyzer” cannot be used with data from a live interface.

Note: If the source of traffic is on a remote probe, then the traffic is transmitted over the network to Packet Analyzer before being sent to Transaction Analyzer, running on the local system.

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 stores the decrypted traffic.

Note: If the source of traffic is on a remote probe, then the traffic is saved in the “My Files” directory on the remote probe. If the source of traffic is local to Packet Analyzer, then the traffic is saved as a PCAP file located on the local system.

Drill Down



The *Drill Down* button applies a View to the current selection in a chart. This is an important and powerful feature of Packet Analyzer and is explained in its own section. See “Drill Down” later in this document.

Copy



The *Copy* button copies a textual representation of the chart information from the current selection to the system clipboard (text or Excel format) to enable exporting to another application.

Copy Chart



The *Copy Chart* button copies the selected chart as a metafile to the system clipboard for pasting into another application. A chart must be selected for this button to be enabled.

This page intentionally left blank.

Time Control

The Time Control feature of Packet Analyzer allows the user to go “back in time” over a View that has been computed over days, weeks, or months. It applies to Views computed over live and off-line sources.

Time Control Fundamentals

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.

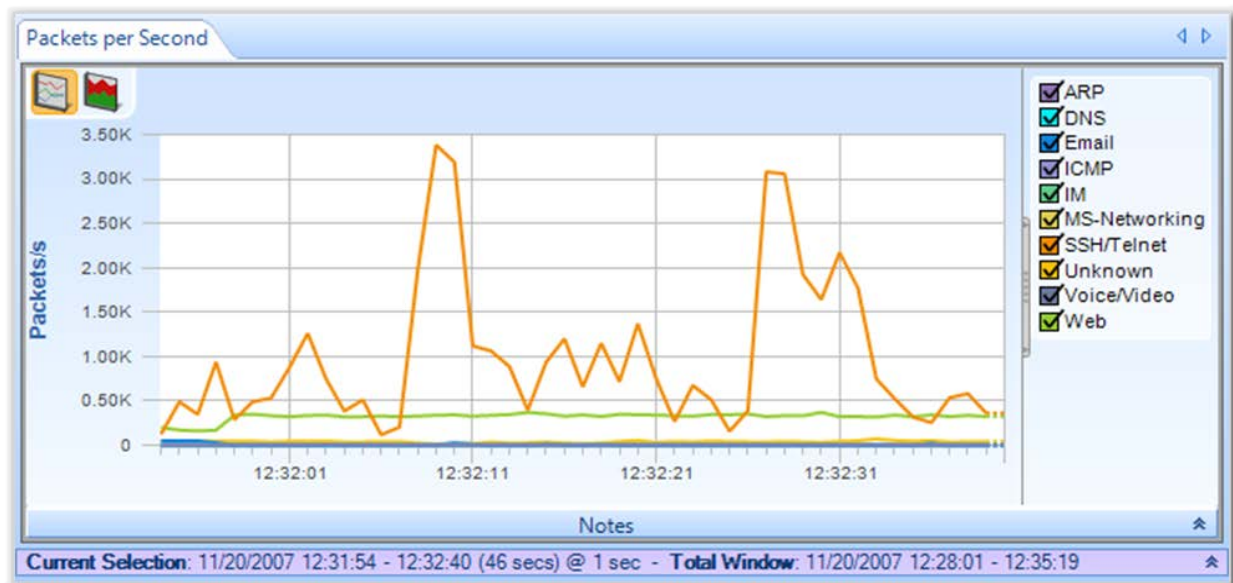


Figure 2 Port Groups Over Time Showing Time Selection Windows

Figure 2 shows the Port Groups 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 the beginning and 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: start date, start 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 Packet Analyzer 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 Packet Analyzer analysis engine (the local or remote NetShark) automatically selects the best level of subsampling based on the duration of the Current Selection.

Note: A view applied to a live source has a configurable “Data Retention Time” found on the view’s context menu. The current setting is shown after *Drop After:* in the Time Controller.

Figure 3 shows the time control “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 Packet Analyzer, thereby making it very easy to move around and to zoom in and out of very long-duration trace files and live captures.

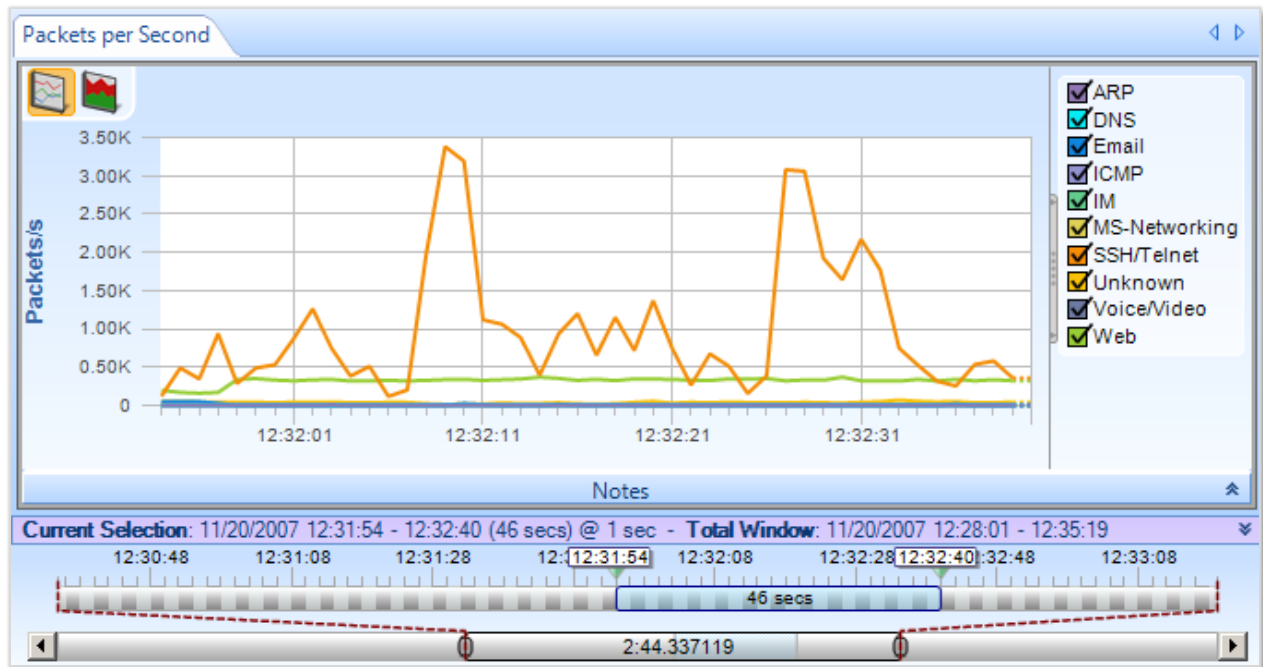


Figure 3 Port Groups Over Time with Multi-Level Zoom Selection

Figure 4 shows the Time Control Bars in more detail. The bottom bar is called the *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. It affects only 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. The *Current Selection* is the time interval within the trace file or live capture that is displayed in the View.

You can 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 the Current Selection to expand the Current Selection to the complete View history. (Double-clicking again returns the Current Selection to its previous location.)

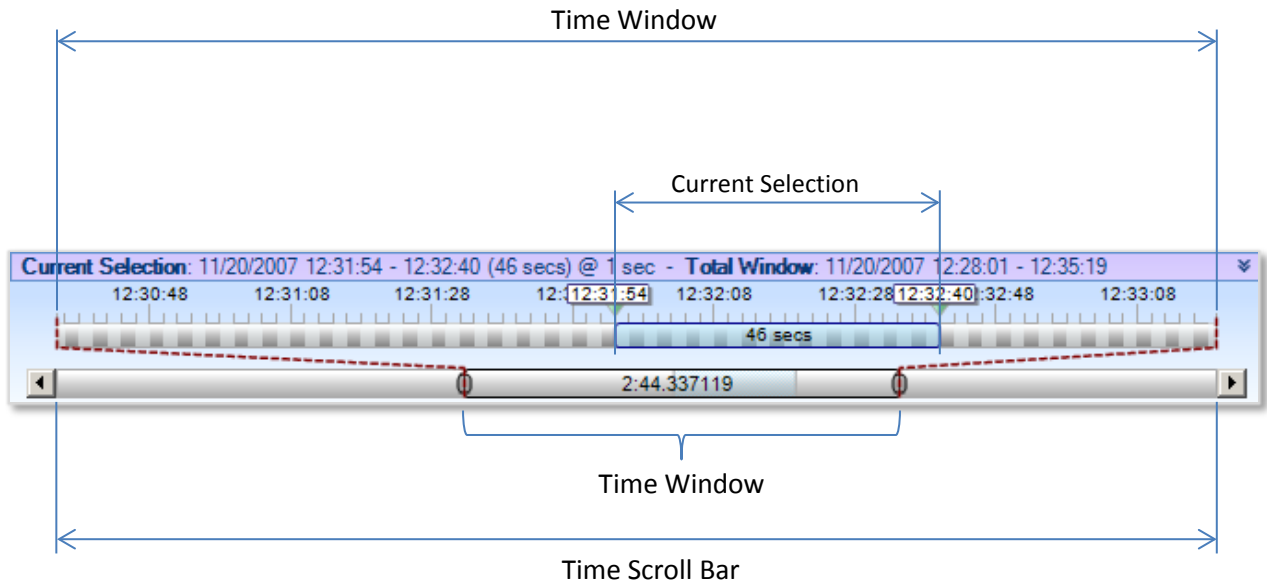
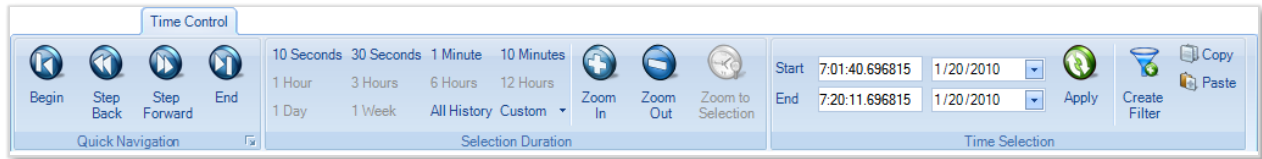


Figure 4 Time Control Bars

Time Control Ribbon



Time Control Ribbon

The Time Control feature of Packet Analyzer 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



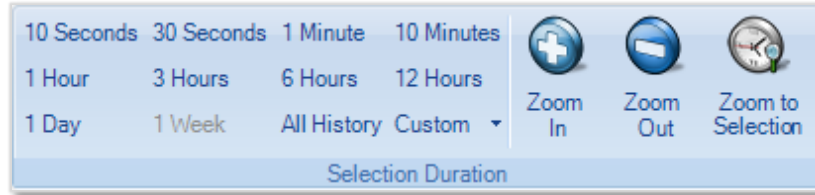
The *Step Forward* button allows the user to move the Current Selection interval one step forward in time where the size of the step is equal to the length of the Current Selection interval.

End



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

Selection Duration



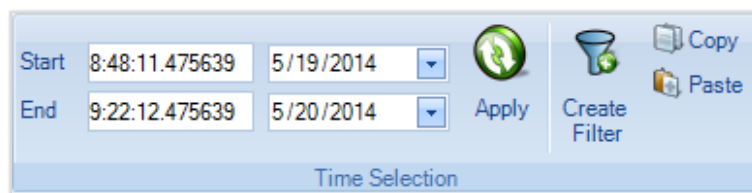
Selection Duration Section of the Time Control Ribbon

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 for 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, All History, etc. For a trace file, the All History selection corresponds to the duration of the entire trace file. For a live capture, All History ends at the present time and begins either at the start of the capture or at an amount of time equal to the Data Retention Time of the capture, whichever is smaller. There is also a Custom option allowing a user to pick an arbitrary time interval.

Finally, there are Zoom In, Zoom Out, and Zoom to Selection options. Clicking the Zoom In button reduces the Current Selection interval by 66%. Clicking 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 changes the Current Selection interval to the selection made on the Strip Chart.

Time Selection



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) by setting the *Start Time*, the *End Time*, and then clicking *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 is very useful for comparing two different Views with respect to the same time interval. For example, one can compare Bandwidth Over Time and IP Conversations during the same time interval to see which hosts were contributing to the spike in bandwidth.

Copy – Copies the Current Selection interval to the clipboard.

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

Watches and Events

A Watch consists of a Trigger Condition and one or more associated Actions. 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 computed in the Chart. The View itself is applied to a source, which can be either live or off-line, and can be either on the local system or a remote NetShark.

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.

The following sections show how Watches are created for Strip Charts and Bar Charts.

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

Creating Watches on Strip Charts and Bar Charts

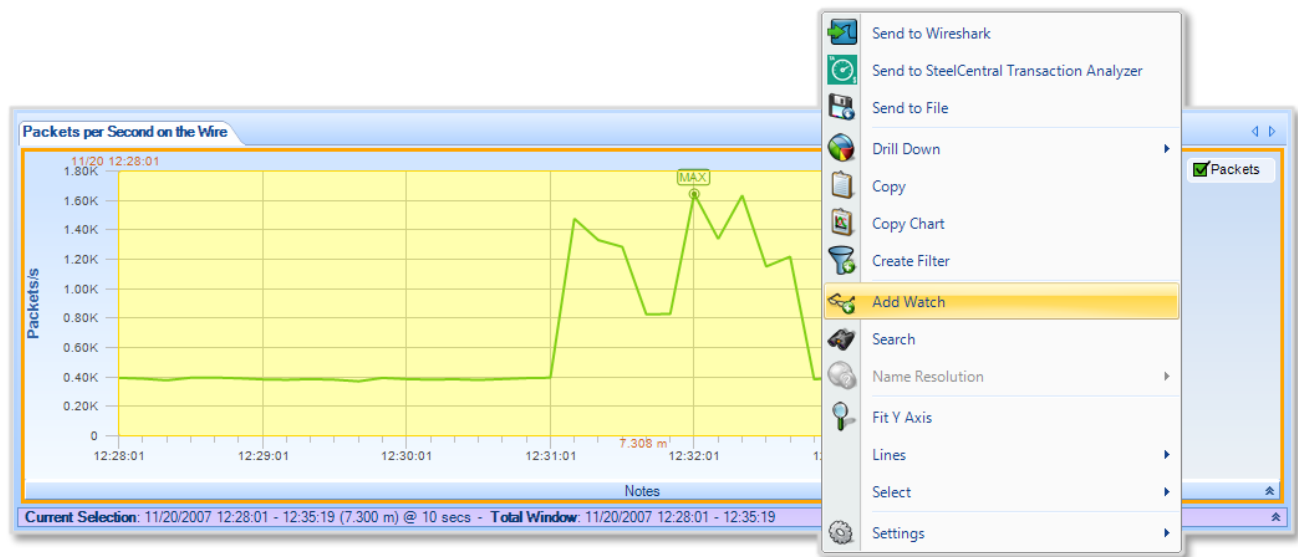
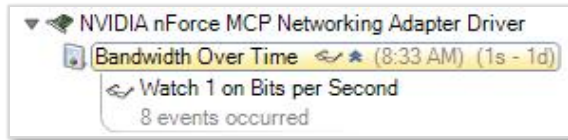


Figure 5 Strip Chart with Context Menu

Figure 5 shows 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 displays the context menu. The *Add Watch* submenu item brings up the Watch Editor panel (Figure 6), which can create a Watch on the metric (Packets per Second) associated with the selected chart.

The user sets up the Watch by completing the necessary items in the Watch Editor panel (see Figure 6). Clicking “OK” in the Watch Editor panel causes the Watch to be associated with the View. The Watch appears in the Sources panel under the View.

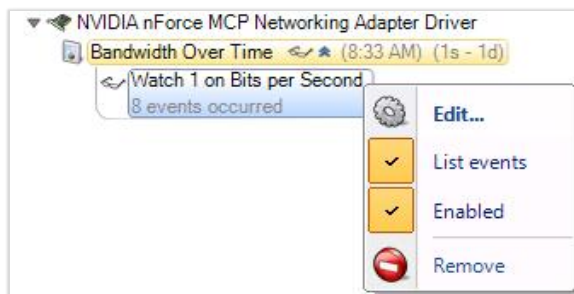
Watch in Sources Panel



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.

Watch in Device Sources Panel

Context Menu for Watch Applied to a Live Source

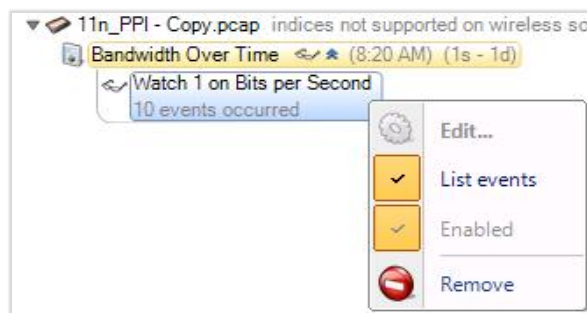


The context menu for a Watch associated with a live source contains the following menu items:

- *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 Live Source

Context Menu for Watch Applied to a Trace File



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

Context Menu for Watch Applied to a Trace File

The Watch Editor

Figure 6 shows the Watch Editor. The following section describes the fields in the Watch Editor panel.

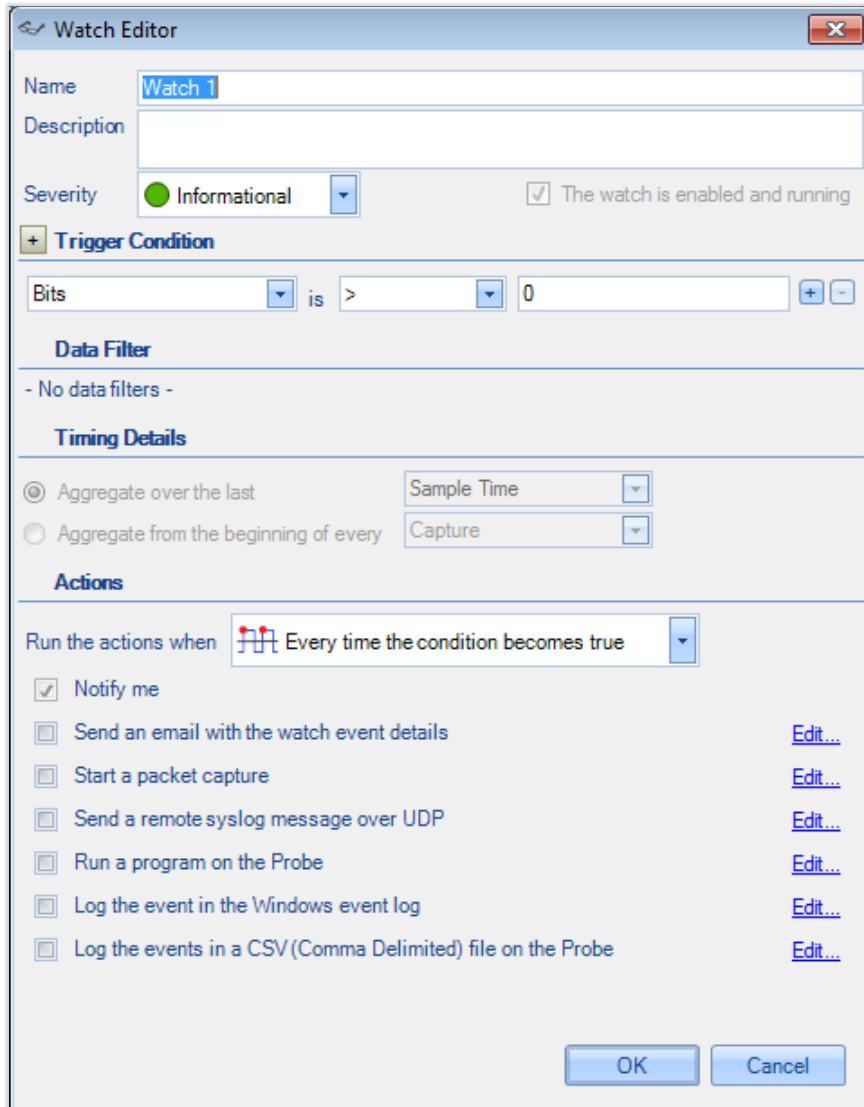


Figure 6 Watch Editor Panel

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

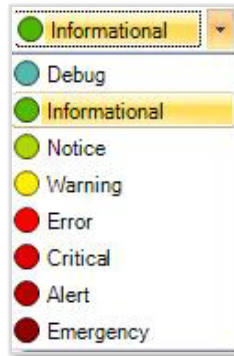


Figure 7 Watch Severity

The *Severity* field contains a drop-down list (see Figure 7) 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 is not activated until the Watch is enabled.

Trigger Conditions

The Trigger Condition elements are shown in Figure 8. Together they represent a Boolean condition; that is, an expression that evaluates to either True or False.

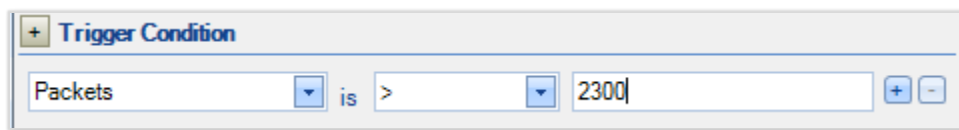


Figure 8 Trigger Condition

The left-most box contains the value to be tested. Recall that in Figure 5 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 9 for the list of operators).

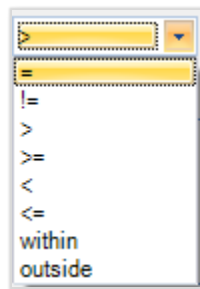


Figure 9 Relational Operators

Finally, there is the right-most box, which contains the comparison value. The Trigger Condition in the example shown in Figure 8 is true whenever Packets is greater than 2,300.

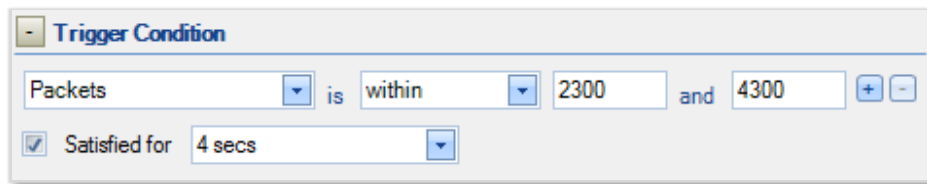


Figure 10 Trigger Condition Expanded

Figure 10 shows the “within” condition and what is shown when the Trigger Condition is expanded. The “within” condition requires two values, namely, lower and upper limits in that order. In this case, 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 (\geq *lower limit* and \leq *upper limit*). Similarly, the “outside” condition is specified with lower and upper limits and is true when the value falls out of the specified range (\leq *lower limit* or \geq *upper limit*).

Entering Values in Watch Triggers

Beginning in Packet Analyzer version 10.7 (and later) an expanded set of units are available for specifying a trigger value. Values can be entered as a number and a unit that specifies a multiplier. For example, a Trigger Condition value of 1000000 now can be entered as 1M. The available units and their multiplier are listed below.

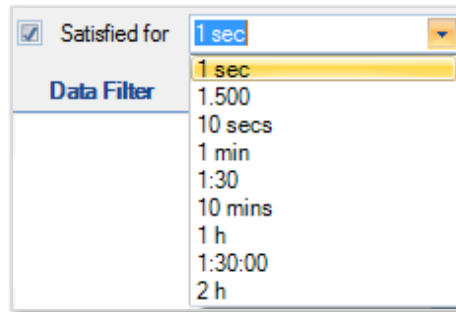
Unit	Multiplier	Multiplier value
k,K, kilo, Kilo	10^3	1000
M, mega, Mega	10^6	1000000
G, g, giga, Giga	10^9	1000000000
T, t, tera, Tera	10^{12}	1000000000000
P, peta, Peta	10^{15}	1000000000000000
E, e, exa, Exa	10^{18}	1000000000000000000
ki, Ki	2^{10}	1024
Mi, mi	2^{20}	1048576
gi, Gi	2^{30}	1073741824
Ti, ti	2^{40}	1099511627776
Pi, pi	2^{50}	1125899906842624
Ei, ei	2^{60}	1152921504606846976
m, milli, Milli	10^{-3}	0.001
u, micro, Micro	10^{-6}	0.000001
n, nano, Nano	10^{-9}	0.000000001
p, pico, Pico	10^{-12}	0.000000000001
f, femto, Femto	10^{-15}	0.000000000000001
a, atto, Atto	10^{-18}	0.000000000000000001

Entries for values (number times multiplier) must evaluate to integers. Engineering notation using “e” or “E” also is supported, for example, 2E6 corresponding to $e*10^6 = 2000000$. Time values cannot be entered using multipliers.

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. In other words, both must be true for the Trigger Condition to be true. In the above example (Figure 10), 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 2300 and 4300 for 4 consecutive seconds).

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



Sample Choices for Satisfied for

The figure above shows the contents of the drop-down box for the choice of durations for “Satisfied for.” The duration can be selected from this list or you can supply your own using the formats shown in the list.

Multi-line Strip Charts

In the case of a single line strip chart as in Figure 5, the Trigger Condition is evaluated every Sample Time on the single value computed at each sample point. In the case of 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

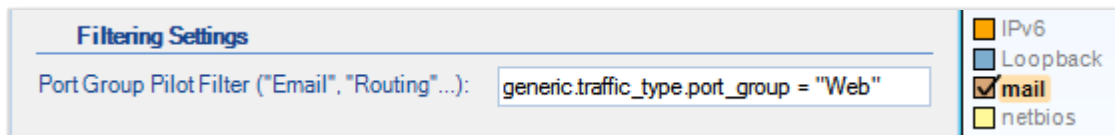


Figure 11 Multi-line Strip Chart with Filtering

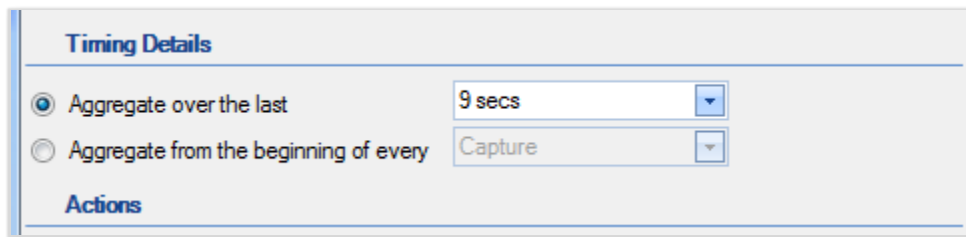
Figure 11 depicts the case where the multi-line strip chart shows Port Groups Over Time. Each packet is examined and partitioned according to its packet type and the bandwidth per second is computed for each packet type. In general, a Watch on this strip chart would check the Trigger Condition for each port group for each Sample Time and generate an event for each port group for which the Trigger Condition is met. This means that there could be as many events generated at each Sample Time as there are port groups. If a line selection is made before the Watch is created, the Data Filter field will show the set of lines for which the packet bandwidth will be calculated.

Figure 11 shows that one line, **mail**, has been selected. The Watch Editor acknowledges the line selection under the Data Filter section and automatically appears.

Multiple values, single packet type

Figure 12 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, maximum, and minimum 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



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.

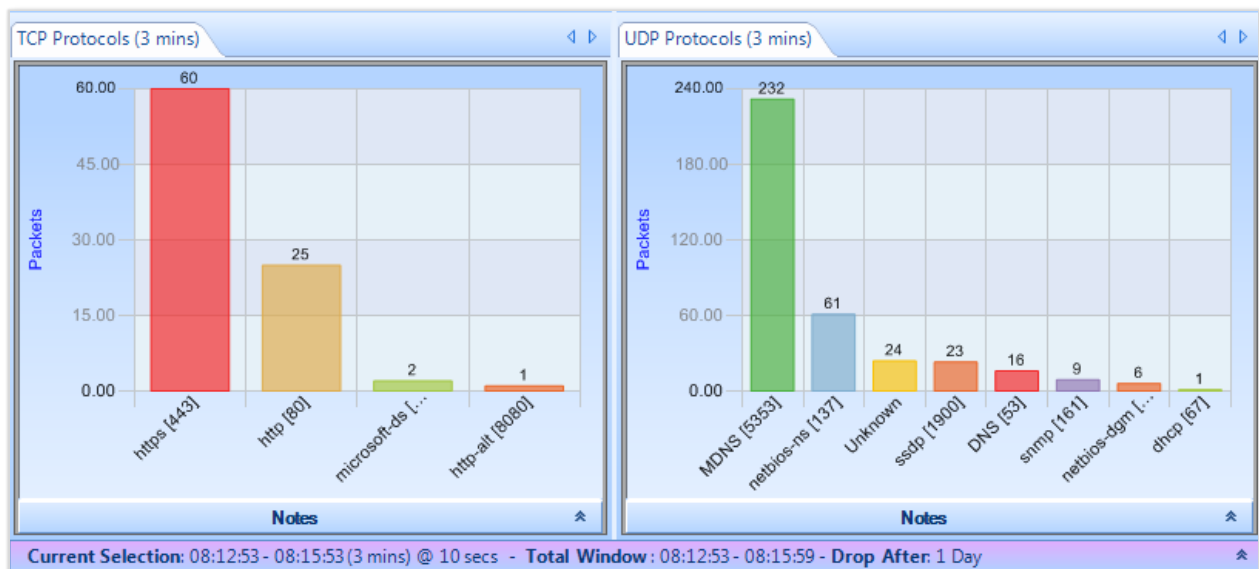


Figure 12 Aggregating Chart

The Current Selection interval in Figure 12 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 interval. In the case of the above chart, the interval is from 08:12:53 to 08:15:53. The aggregation interval for the bar chart is, for convenience, also show in the chart’s tab.

Note: *The Timing Details sets 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. For example, suppose a user 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 the bar chart example, the aggregation function is SUM. A number of other aggregation functions are used throughout Packet Analyzer, namely, MAX, MIN, AVG, TIME AVG, and others.

Actions

The Trigger Condition is an expression that is evaluated at each Sample Time. Even when the trigger is true, you may want some additional context before you execute the corresponding actions. For example, you may want to execute only 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

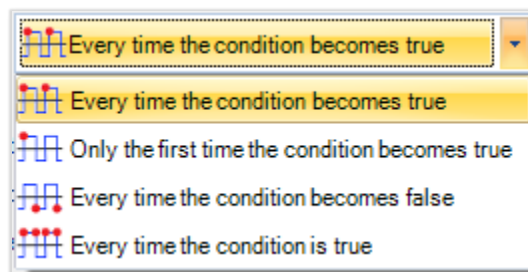


Figure 13 Transition Condition List

In Figure 13 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 NetShark. Accordingly, the actions associated with the trigger condition are initiated by the local system or the remote NetShark

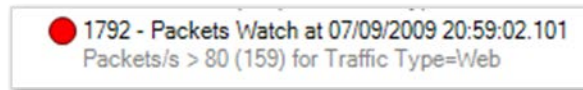
Notify Me

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



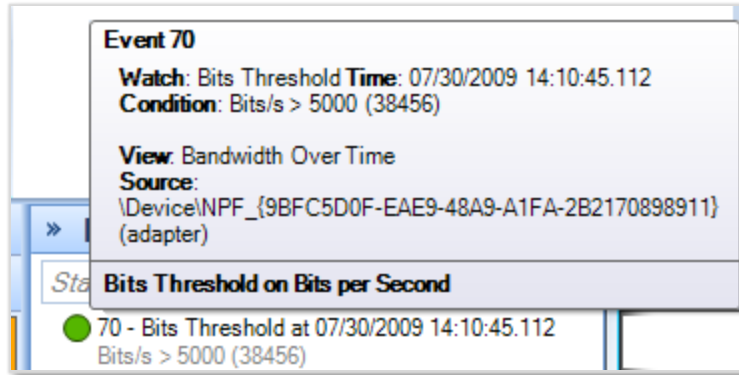
Figure 14 Event Notifications

Figure 14 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.



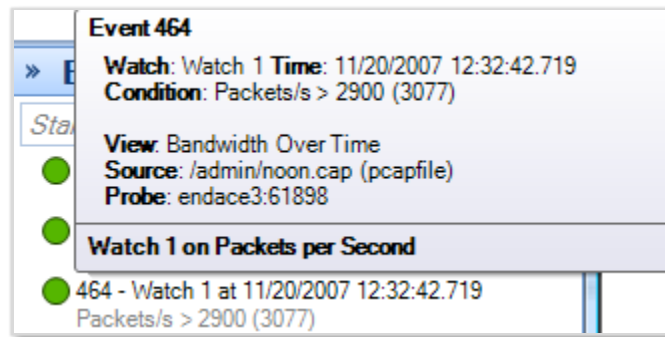
Event Structure

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 for an Event

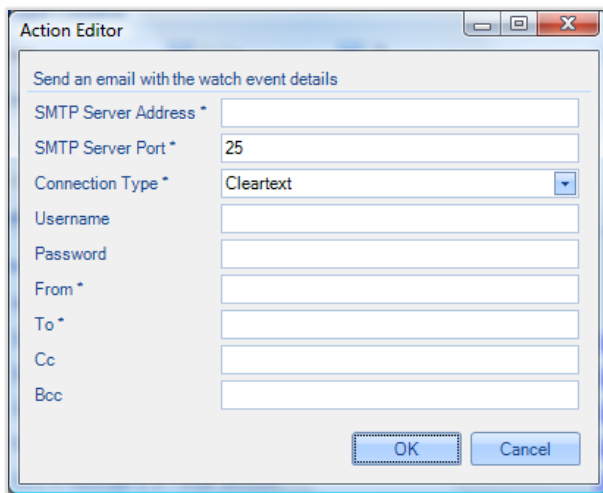
Moving the mouse over a severities icon in the Events panel displays a tooltip for the selected event. The tooltip contains the details regarding the Event.



Tooltip for a Remote Event

The tooltip for a Remote event also identifies the “name” of the NetShark and port number.

Send an email with the watch event details



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 is sent to the destination email addresses with the Event information.

Email Action

Start a packet capture

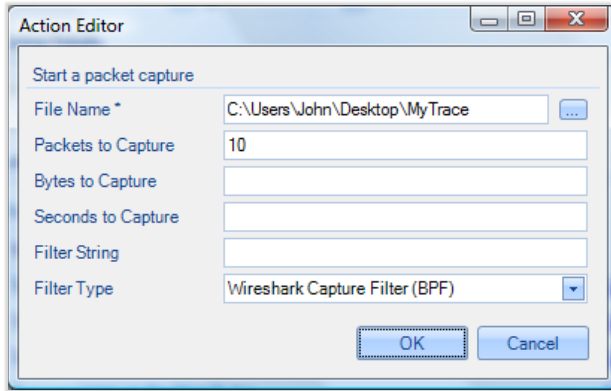
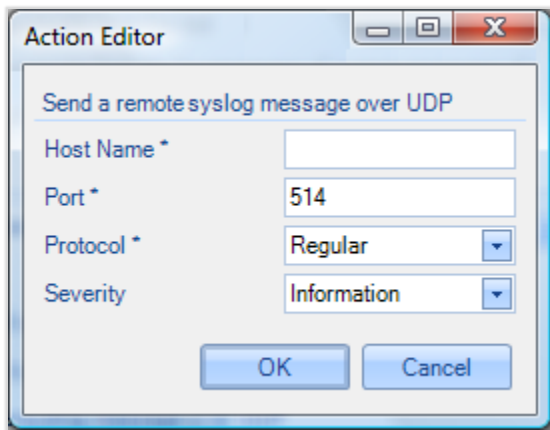


Figure 15 Capture Packets Panel

When “Start a packet capture” is selected, the panel in Figure 15 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 is 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 is placed in the My Files directory located on the remote probe.

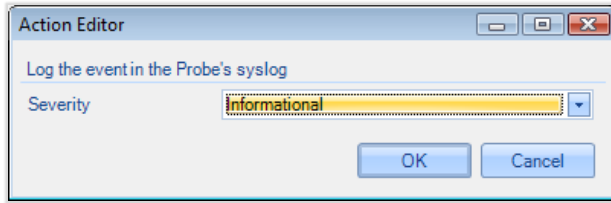
Send a remote syslog message over UDP



Send a syslog message using UDP to a remote host.

Send to Remote Syslog

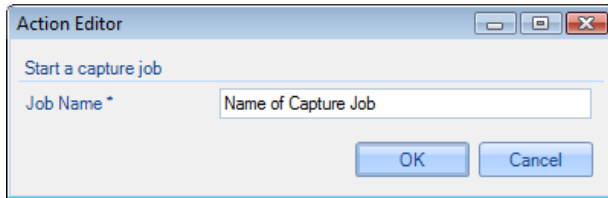
Log the events in the Probe's syslog



The event is entered into the Probe's syslog with the indicated severity.

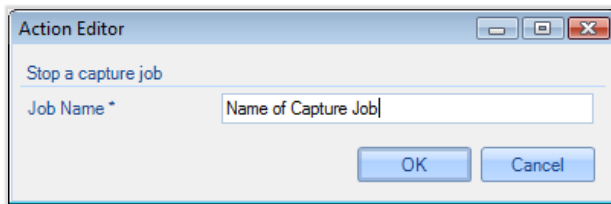
Send to Probe's syslog

Start a Capture Job



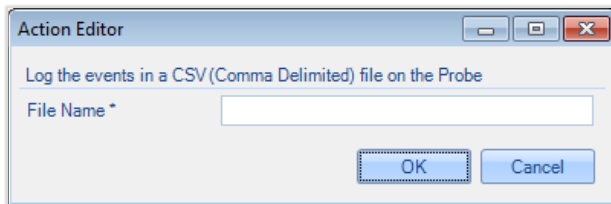
The event starts a currently stopped capture job. If the capture job is already started there is no change.

Stop a Capture Job



The event stops 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 NetShark



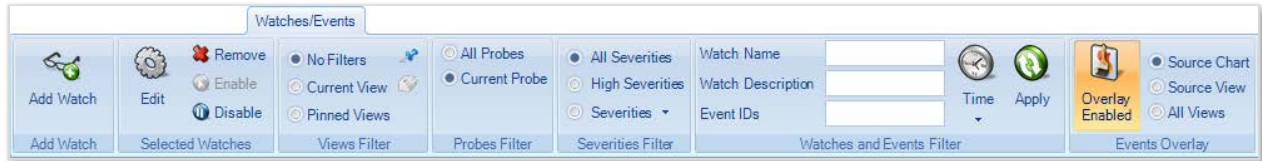
The event is written as a CSV file using the complete pathname provided in the Action Editor.

Send to CSV File

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

Watches/Events Ribbon

The Watches/Events Ribbon is divided into a number of sections.



Watches and Events Ribbon

Add Watch



The *Add Watch* button is enabled when there is either a strip chart or bar chart selected within the current View. Clicking 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



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



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



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

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

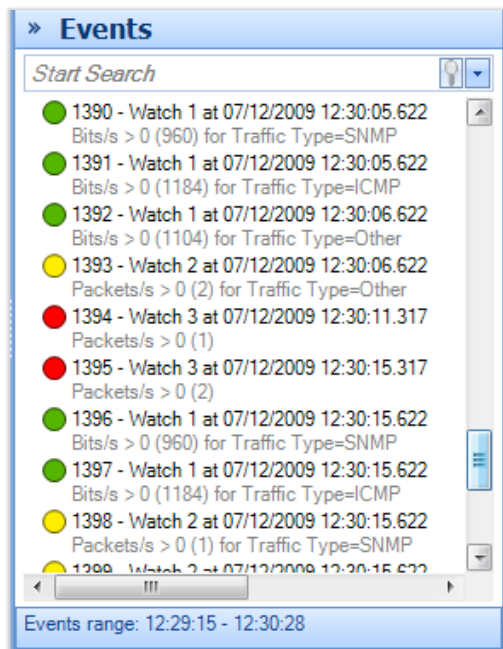
Disable Selected Watch



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

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

Filtering Events Section



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 16 Event Filtering Section of the Watches/Events Ribbon

Figure 16 shows 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



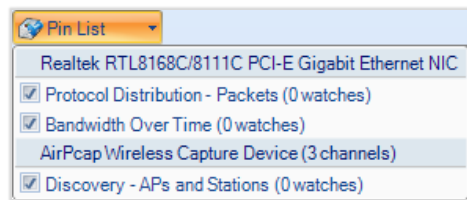
With a View selected in the Sources panel, clicking *Add to Pin List* adds the selected View to the Pin List.

(Show the) Pin List



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

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 the corresponding check boxes.

Probes Filter



There are two choices with the Probes Filter. Show the Events from all of the NetShark appliances (including the Local System) in the Events panel, or only show the Events from the currently selected NetShark in the Sources panel.

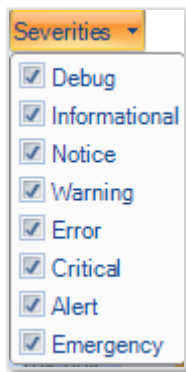
Severities Filter



The Severities Filter section allows you 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 the down-arrow.

Severities List



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

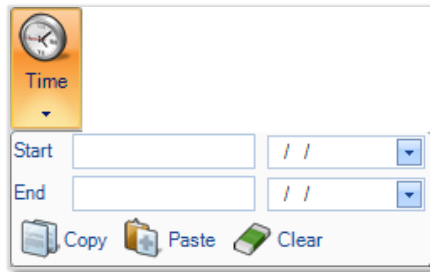
Severities List

Watches and Events Filter



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

Time Filter



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.

Time Selection

Apply



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

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

Events Overlay



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. Figure 17 shows the expanded Bandwidth Usage folder. Its first subfolder is called the *Bandwidth Usage Watches*.

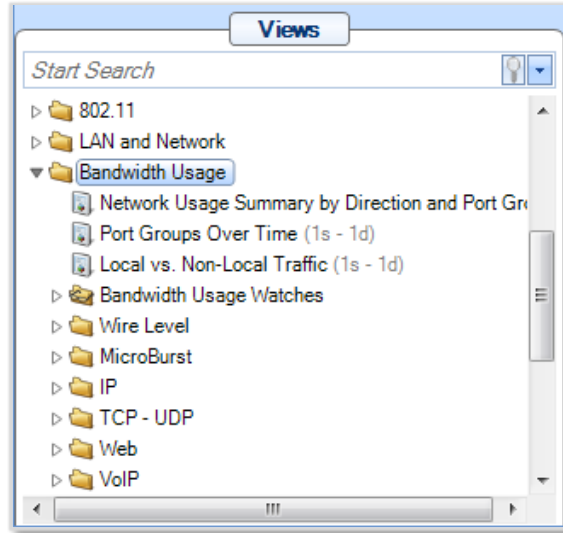


Figure 17 Predefined Watches

Opening the Bandwidth Usage Watches folder displays the following:

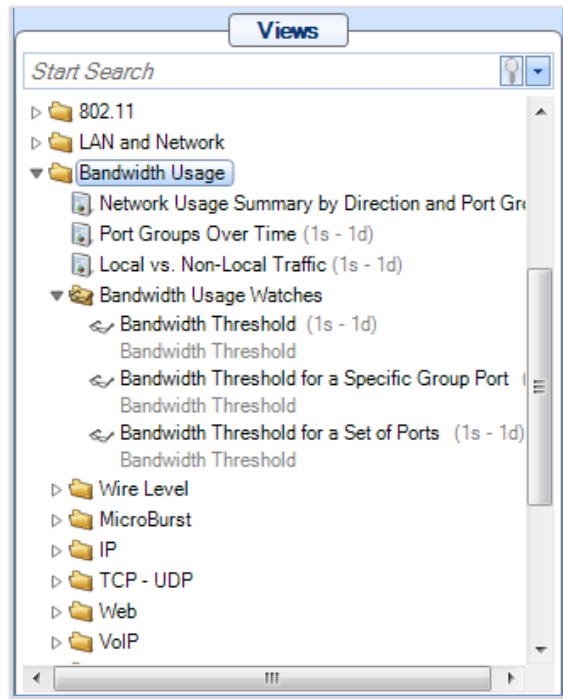


Figure 18 Expanded Bandwidth Usage Watches Folder

The expanded Bandwidth Usage Watches folder contains three entries. Each of these entries consists of a View and a Watch that is associated with the View. For Example, the *Bandwidth*

Threshold for a Specific Port Group (in Figure 18) 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 is displayed 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.

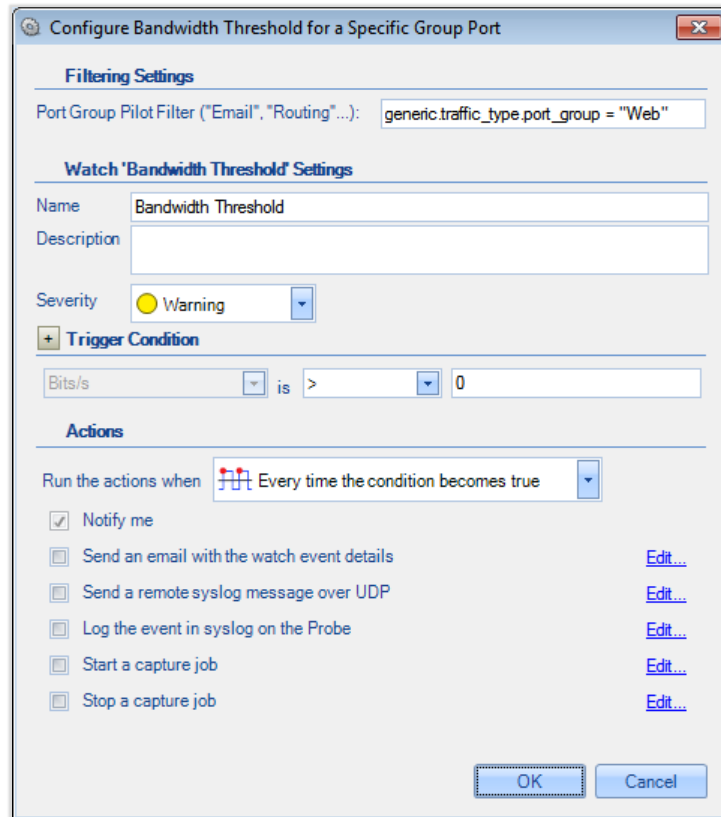


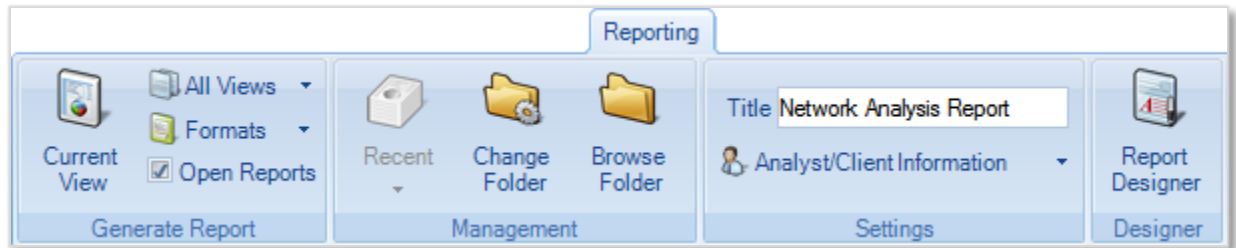
Figure 19 Watch Editor Panel with Filter Settings

Figure 19 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 port groups.

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



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.

Supported report formats are:

- PDF Report
- Zip Package
- Excel Spreadsheet
- Word Document
- Text File
- HTML Page

Many things can be customized in a generated report. The ribbon is described below top-to-bottom and left-to-right, by section.

Generate Report

This section manages how the reports are generated.

Current View



The *Current View* button is used to generate a report using the current View, which requires that a View 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



Button

The *All Views* button gives you options for generating a report using more than one view. 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*.

Clicking the *All Views* button directly generates a report using all views that are currently open in the main window.



Submenu

Clicking the drop-down arrow beside the *All Views* button gives you a choice of generating a report for all views or for views that are currently selected. You can select multiple views by clicking them in the Sources panel while holding down the Ctrl or Shift key.

Format



Button

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.

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 of the trace files (smaller than 50 MB).
- The PDF version of the report.

Excel Spreadsheet

The *Excel Spreadsheet* check box refers to a Microsoft 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

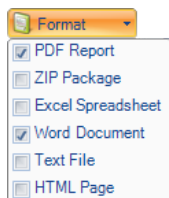
The *Word Document* check box refers to a “Rich Text Formatted” (RTF) document that can be viewed in Microsoft Word.

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.

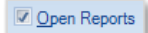
HTML Page

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.



Submenu

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, when generating Word and HTML formatted reports, then the default word processor and web browser open and display the reports.

When Off

No programs are opened when a report is generated.

Management

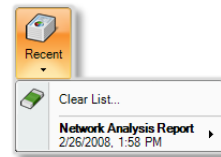
Generated reports are saved to a user-specified directory. The default directory is the “My Documents” directory in the user’s “Documents and Settings” directory (or the language equivalent). This can be changed as desired. The *Management* section provides a convenient way to get to the directory, manage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

Recent



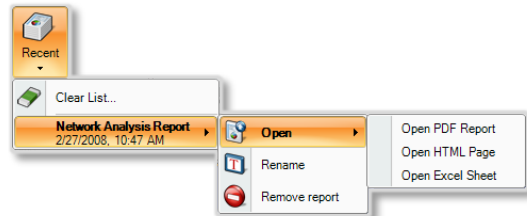
The *Recent* button opens a submenu to manage recently generated reports. By default, reports are generated, the Recent button is disabled.

After a report is generated, a reference to it is placed in the Recent submenu list. The list holds the five most recently generated reports and can be cleared at any time. Note that the clear operation does not remove the file(s) from disk but simply clears the referential list inside of Packet Analyzer.



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.



Recent Reports (Detail)

Change Folder



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

Browse Folder

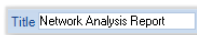


The *Browse Folder* button opens a browser window to show the folder where future reports will be saved.

Settings

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

Title



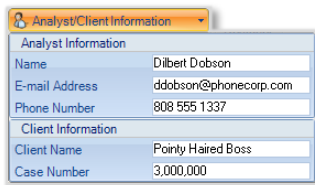
The *Title* edit box specifies what to call subsequently generated reports. The title goes on the cover page if the page is included in the report generation. See the section on the Report Designer Ribbon that follows for more information.

Analyst/Client Information



Button

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



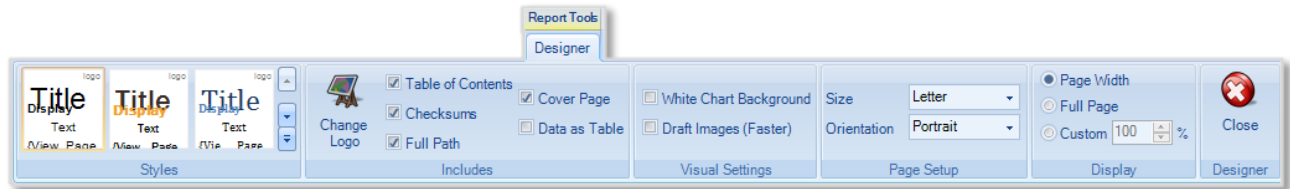
Submenu

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



The *Report Designer* Ribbon is not always available. It is a contextual ribbon that appears only 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).

This displays a generic template report as a tabbed window that 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, not any existing reports.

Styles



The *Styles* section controls the thematic 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 it. In the depiction on the left for instance, the first style is selected.

Includes

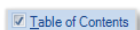
The *Includes* section has options that determine what is presented inside a report.

Change Logo



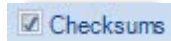
The *Change Logo* button is used to specify the logo that goes in the upper right hand side of the cover page of all subsequent reports.

Table of Contents



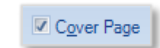
The *Table of Contents* check box (checked by default) is used to specify whether to include a table of contents in subsequent reports.

Checksums



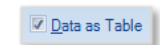
The *Checksums* check box (not checked by default) is used to specify whether SHA256 cryptographic digests are generated for trace files in subsequent reports. These digests are printed on the reports and placed in separate files when using the ZIP output format.

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

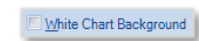


The *Data as Table* check box (checked by default) is used to specify whether to include quantitative data tables in subsequent reports.

Visual Settings

The *Visual Settings* section has options used to modify some technical aspects of the creation process of reports.

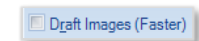
White Chart Background



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

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

Draft Images (Faster)



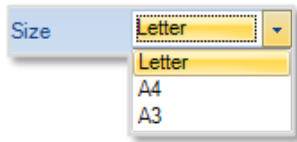
The *Draft Images (Faster)* check box (not checked by default) is used to specify the quality of the images in subsequent reports. Draft images are a suitable resolution for viewing on a computer while non-draft images are suitable for printing. Turning this feature on:

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

Page Setup

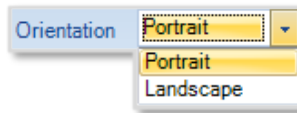
The *Page Setup* section controls the format of future generated reports.

Size



Use the *Size* drop-down menu to select the report size.

Orientation



Use the *Orientation* drop-down menu to select the report orientation.

Display

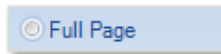
The *Display* section controls the magnification of the report template.

Page Width



Selecting *Page Width* changes the magnification level of the template so the width of a page matches all the space available in the tab.

Full Page



Selecting *Full Page* changes the magnification level of the template so that an entire page can be viewed.

Custom



Selecting *Custom* enables you to specify the magnification level of the template. Magnification can range from 25% to 400%. Enter a desired magnification level in the box (default is 100), or use the up or down arrow to increase or decrease the magnification by 25% each time an arrow is clicked.

Close Designer



The *Close Designer* button closes the Report Designer Ribbon and template view tab. Since all changes are immediate, there is no prompt to save for changes.

This page intentionally left blank.

Accessing Remote Probes

Users and Groups play an important role in accessing remote probes. All communication between NetShark appliances and a Packet Analyzer uses SSL-encrypted web communications and requires HTTP basic access authentication credentials (HTTP Authentication). The NetShark appliance passes the authentication credentials to the Credential Manager, which determines whether the user has the permission to execute the requested operation. If not, the NetShark appliance returns a *not enough privileges* error to the Packet Analyzer making the request.

User and groups are configured using the NetShark web interface. For more information, see “Managing users and groups” in the chapter “Tasks” in the *SteelCentral NetShark User’s Guide*.

Remote Ribbon



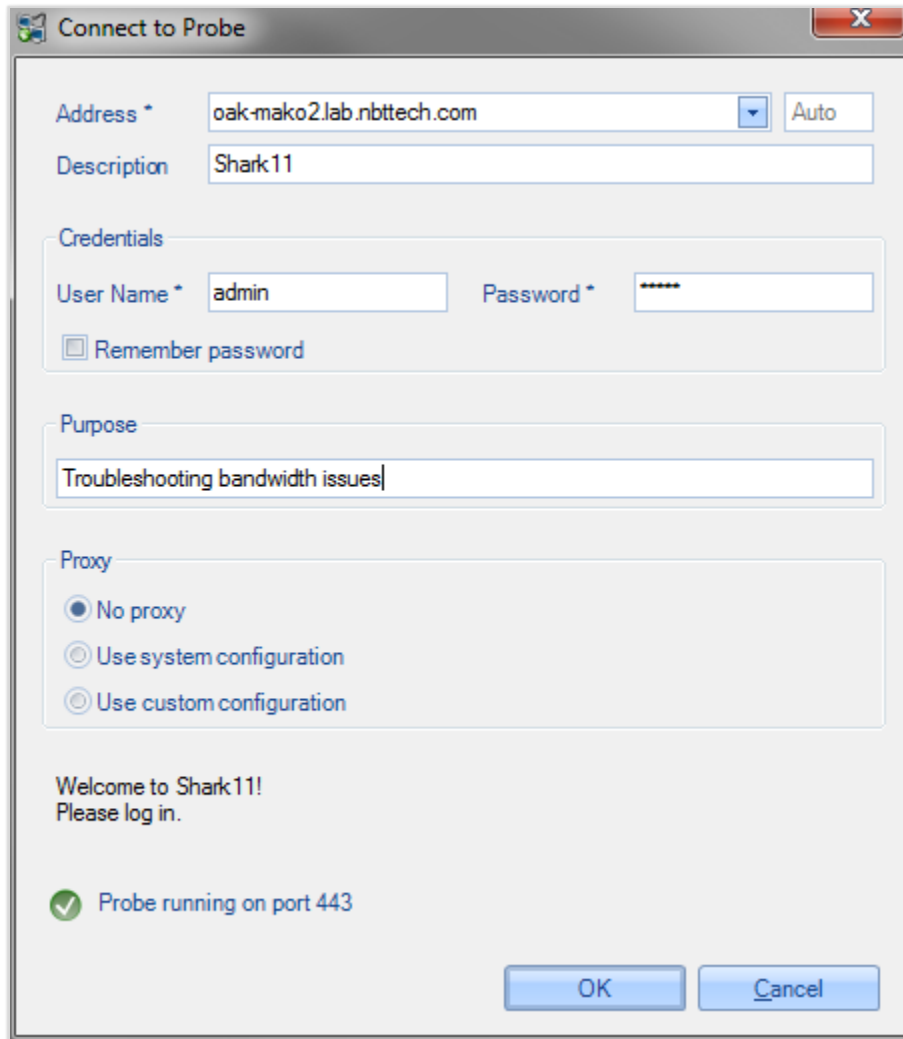
This section describes sections of the Remote Ribbon: Probe Management, Probe Selection, Files, and View Selection.

Probe Management

Add Probe



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



Typical Connect to Probe Panel

The *Connect to Probe* panel is used to initiate a connection to a NetShark. (This includes NetShark virtual edition and NetExpress).

Required parameters are indicated by an asterisk (*). Parameters are:

Address—the probe name and port

The *probe name* is the hostname or IP address of the NetShark. This is a dropdown list that maintains a probe history; you can add a new probe or select one from the list. Selecting an item from this list automatically fills out the known fields in the dialog box. This information is also saved in the probe list, accessible through the *Probes* icon in the Probe Management section of the Remote Ribbon.

The *port number* is the TCP port number of the appliance. The default value is Auto, which uses the port number read from the NetShark; alternatively, you can specify a port number. For NetShark appliances with software version 9.5 or later, the port number is 443; for earlier software versions, the port number is 61898.

Description—an optional name for the probe; this name is used in the Device list

Credentials—a user name and password. Checking the *Remember password* box stores this information in the config file. If the *Remember password* box is checked, the Connect to Probe dialog does not appear—the password is already stored—unless the appliance requires a purpose or displays a banner. **Note:** In version 10.6 (and later) a NetShark can be configured not to allow passwords to be remembered by Packet Analyzer. A password must be entered each time a user connects to a NetShark. Any pre-existing passwords are removed from the Packet Analyzer.

Note: **Beginning with release 10.7, if the Remember password checkbox is selected, the credentials are encrypted when stored in the Packet Analyzer configuration file.**

Purpose—This field appears only if specified by the NetShark. It allows you to enter a purpose for the probe connection, and may be used by the appliance manager for security purposes.

Proxy—allows you to specify whether the Packet Analyzer connects to the NetShark via an HTTPS proxy server and, if so, allows you to specify the URI and credentials.

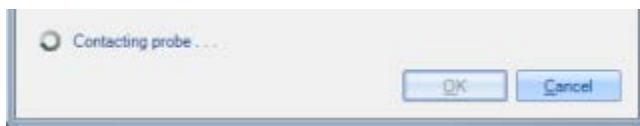
No proxy—connects directly to the NetShark. This is the default value.

Use system configuration—uses the proxy information set in the operating system to establish the connection. (From the Internet Options control panel, click the Connections Tab and the LAN Settings button to get to the Proxy Server settings. The Internet Options control panel is available through Start > Control Panel > Network and Internet or through the Internet Explorer browser.) If credentials are needed, two text fields appear to allow you to enter username and password.

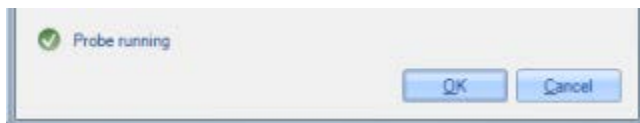
Use custom configuration—uses a custom proxy configuration. Four text fields allow you to specify port name, port number, username, and password.

Banner—an optional label returned from the probe

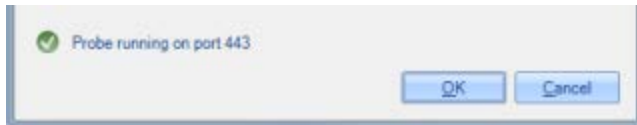
The information bar at the bottom of the dialog gives the status of the connection using one of these messages:



Packet Analyzer is scanning for the probe. A timeout limits the duration of the scan. Clicking the *Cancel* button interrupts the scan.



The probe has been found, and it is running on the port specified in the *Port* text box.



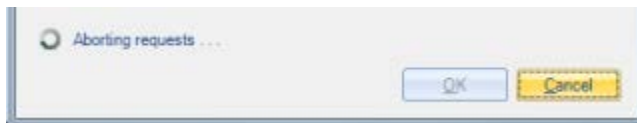
The probe has been found, and it is running on the indicated port. The port number is shown when *Auto* is specified in the *Port* text box.



The probe is running on a specified (or auto) port, but a certificate warning has occurred. You can view the certificate and choose to permanently accept it; proceed anyway; retry; or cancel.



The port does not exist or the timeout expired. You can retry the connection request by clicking the *retry* link.



The Cancel button has been clicked while connection requests are in progress. Each request is cancelled and the dialog waits for them to complete.



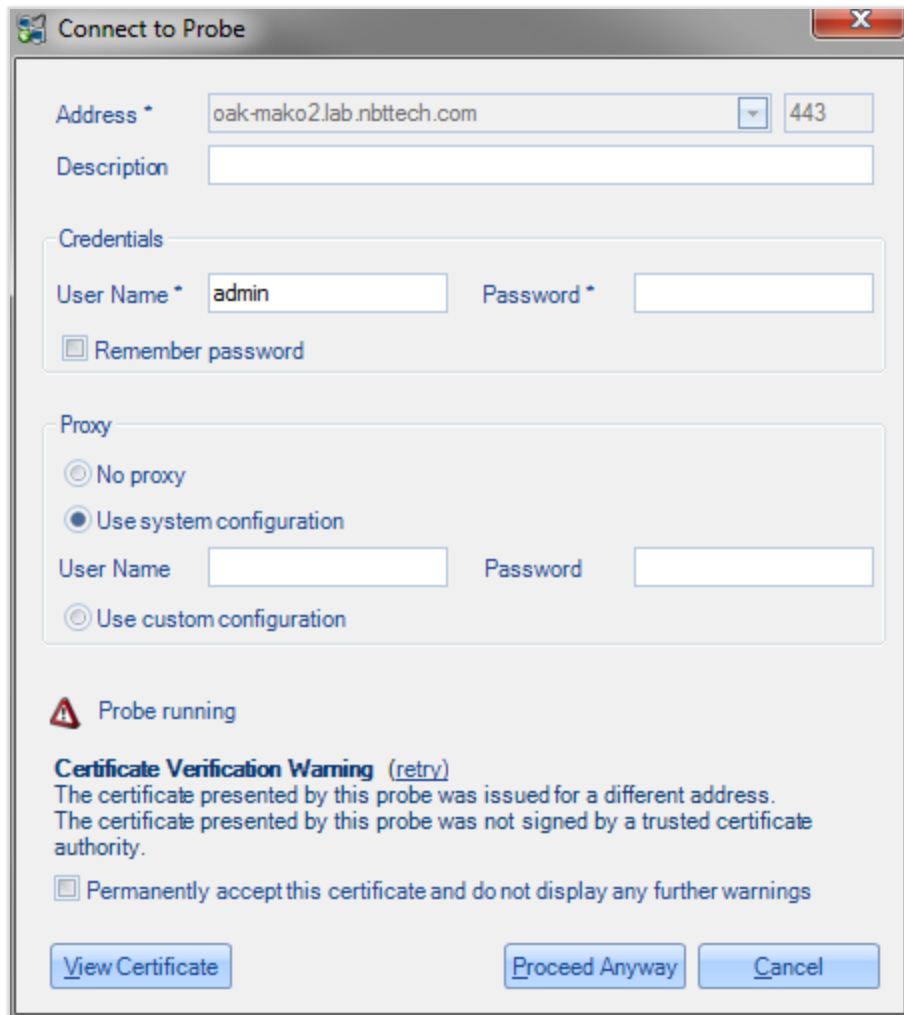
The proxy credentials are invalid. You can retry the connection request by clicking the *retry* link.

During the connection sequence the Packet Analyzer checks the security certificate presented by the NetShark. The *Connect to Probe* dialog shown above appears if the certificate is valid.

A NetShark appliance's security certificate might be invalid for a number of reasons:

- The certificate presented by the NetShark appliance was not signed by a trusted certificate authority.
- The certificate presented by the NetShark appliance was issued for a different address than the one expected by the Packet Analyzer.
- Both of the above simultaneously.

If the certificate is invalid, a *Certificate Verification Warning* appears at the bottom of the *Connect to Probe* dialog, giving the reason or reasons that the certificate is invalid.

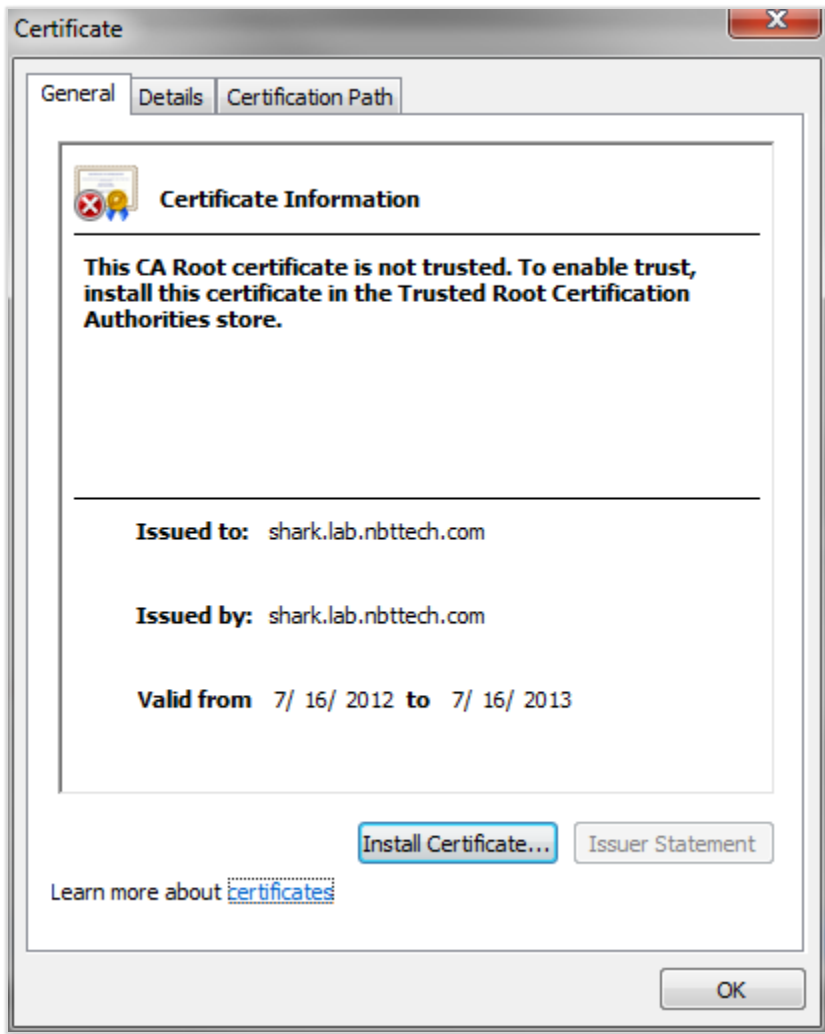


In this case you have four options:

- Click *Cancel*. The connection will be aborted.
- Click *Proceed Anyway*. The connection will proceed and the warning will be presented each time you attempt to connect.
- Check the *Permanently accept this certificate* checkbox and click *Proceed Anyway*. The connection will proceed and the certificate will be accepted from now on. (The certificate thumbprint for the specific NetShark is stored in the Packet Analyzer configuration and it affects Packet Analyzer installation only.)
- Click *View Certificate*.

Note: If the certificate presented is for a different address, the only workaround is to check *Permanently accept this certificate* and click *Proceed Anyway*.

If you choose *View Certificate*, a dialog with information about the certificate appears. This information includes the reason that the certificate is invalid, and may indicate where to store the certificate if you choose to install it. Note that this installation is handled by Windows, and that installing the certificate will affect Windows and all installed applications (for instance, Internet Explorer). For more information on Windows certificate management, look in the help pages for Windows Certificate Manager.

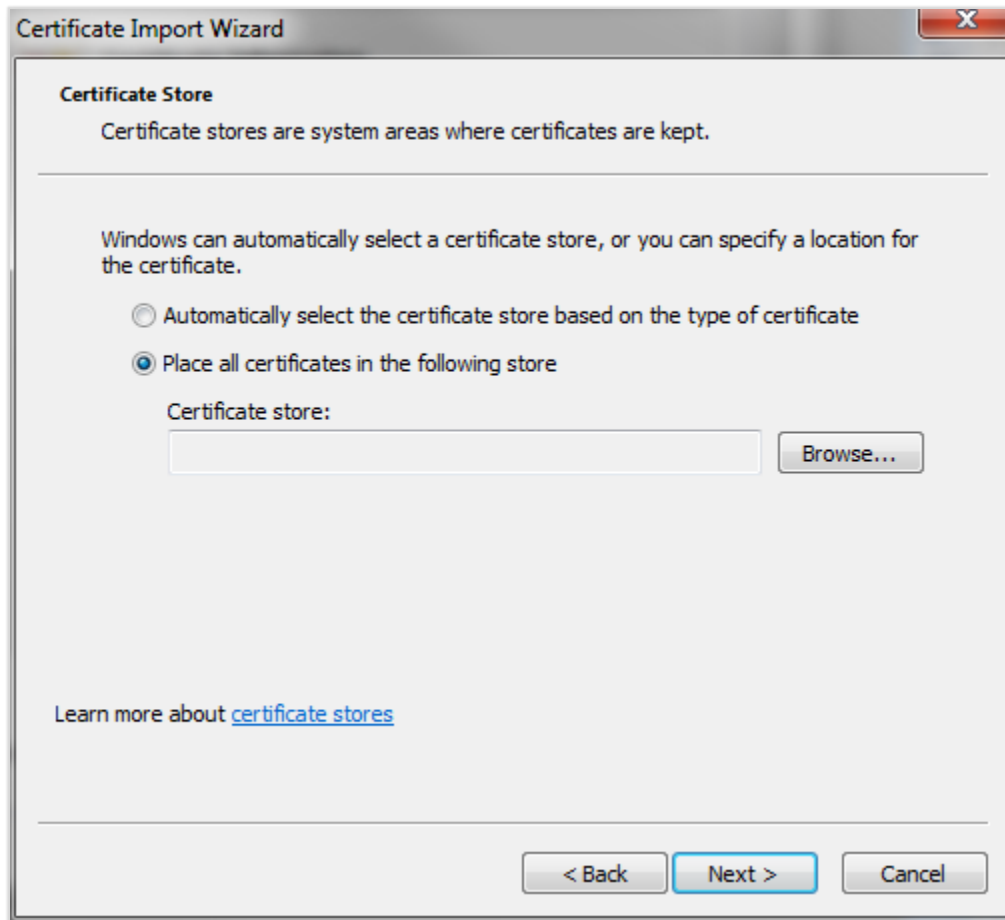


If you click *Install Certificate*, Windows will install the certificate in its configuration and will recognize it as valid for future connections. To install the certificate:

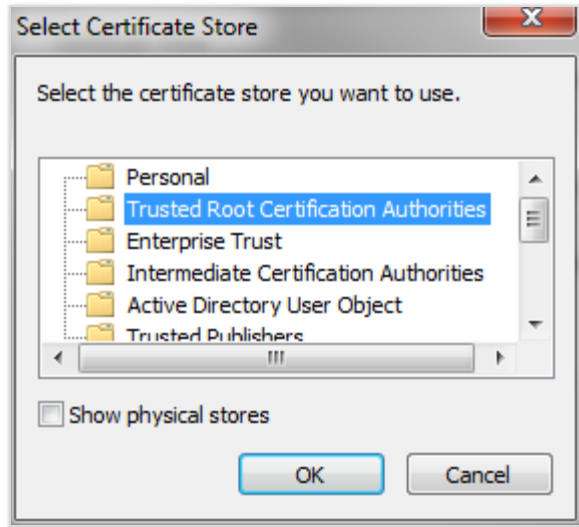
1. Click *Install Certificate* in the *Certificate* information dialog (shown above). This starts the Certificate Import Wizard.
2. In the *Welcome to the Certificate Import Wizard* dialog, click *Next*.



3. In the *Certificate Store* dialog, click the *Place all certificates in the following store* radio button and click *Browse* to search for the appropriate certificate store.



4. Choose the certificate store where you want to place the certificate. Note that if the certificate does not go into the proper store, you will continue to see the certificate warning.
 - If the certificate was invalid because it was not signed by a trusted certificate authority, place the certificate in the Trusted Root Certification Authorities store.



Click OK to return to the Certificate Store dialog.

5. Click Next to proceed to the Completing the Certificate Import Wizard dialog.
6. Click Finish.
7. Click Yes to dismiss the Security Warning.
8. Click OK to acknowledge that the import was successful and return to the Connect to Probe dialog.
9. Click Proceed Anyway to continue with the connection.

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 shown in Figure 20.

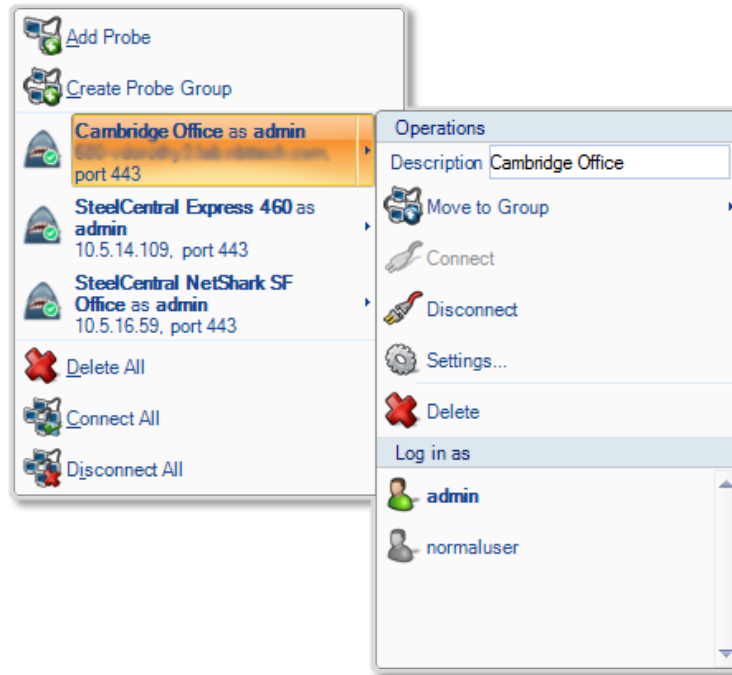


Figure 20 Probes Panel

The first item in the 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 NetShark can be a member of at most one probe group. If a probe is member of a probe group, then it appears only within the probes group in the Probes Panel.

Below the Create Probe Group is a list of all of the probes that have been added using the Add Probe panel and have not been removed from this list. Clicking the icon to the left of one of the probes on the list disconnects Packet Analyzer from the probe if it is already connected. On the other hand, if the probe is initially disconnected, then clicking the icon reconnects 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 NetShark on the list brings up a submenu for operations on the selected NetShark, enabling the user to edit the appliance description, move the appliance into a probe group, connect to or disconnect from the appliance, display the appliance settings, and delete the appliance from the list.

When a NetShark is configured for local authentication mode, the “Log in as” list includes the identity of all users having accounts on the selected NetShark. The item in bold is the identity of the user who is currently logged into the NetShark from Packet Analyzer. Selecting a user on this list

initiates an attempt to connect to the NetShark on behalf of the selected user. When remote authentication is being used this list is not shown.

Probe Selection

Select All Probes



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

Expand Selection



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

Collapse Selection



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

Disconnect from Selected



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

Web Interface



The *Web Interface* button opens the selected remote probe's web interface. Note that connection to the web interface of a NetExpress is not supported.

Files

Import Files into Probes



The *Import Files into Probes* button transfers trace files from the Local System to the selected remote probe. The trace files are transferred to the selected directory of the remote probe.

Export Files from Probes



The *Export Files from Probes* button transfers 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 are transferred to the Local System. If a file on a remote probe is in the selection, then just the file is transferred. Multiple selections are permitted as long as the selections are either all folders or all files.

View Selection

Select All on Probes



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

Close Selected



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

Attach to Selected



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

Detach from Selected



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

Share Selected with



The *Share Selected with* button brings up a panel to allow selected views on NetShark appliances to be shared with other groups.

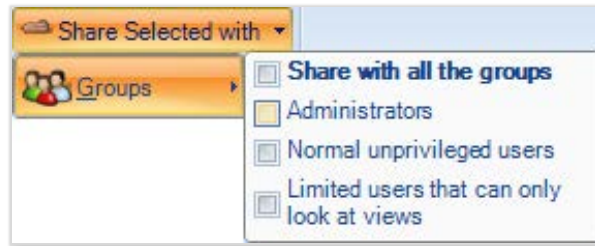


Figure 20 Share Selected with Groups

NetShark Packet Recorder

A traditional approach to capturing high-speed and/or long duration network traffic is to create a file rotation scheme, whereby the capture is divided into a 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, which makes analysis and troubleshooting extremely tedious, especially when the traffic of interest spans multiple trace files.

The NetShark includes a facility called the NetShark *Packet Recorder* that uses a new approach for dealing with high-speed and/or long-duration traffic capture scenarios. The Packet Recorder is based on an optimized *packet data store* called *SharkFS* - a novel approach that saves network traffic as objects called Job Traces. It also makes use of *time filters* to efficiently index the packet data, which eliminates the need for a cumbersome file rotation scheme.

Furthermore, a user can isolate specific and manageable portions of a Job Trace for analysis and visualization by 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. Trace Clips behave just like ordinary trace files for analysis and can be converted to ordinary pcap files on the NetShark.

Terminology

- **Capture Job:** A *Capture Job* refers to the specific parameters associated with a packet recording session. These parameters include the job name, the network interface, a BPF filter, start and stop criteria, and an upper bound on the amount of storage to be used by the Capture Job.
- **Job Trace:** The *Job Trace* represents the network traffic saved in the packet data store. Each Capture Job is associated with exactly one Job Trace, which has the same name as the Capture Job.
- **Trace Clips:** *Trace Clips* represent user-defined time intervals within a Job Trace.
- **Jobs Repository:** In Packet Analyzer, the Files panel for a NetShark contains a folder called the *Jobs Repository* that has an icon and the name for each Job Trace in the appliance.
- **Capture Job Interface:** In Packet Analyzer, the Devices panel for a NetShark contains an icon and the name for each *Capture Job Interface* representing the network interface associated with a Capture Job on the appliance. Views can be applied to these Capture Job Interfaces creating a visual analysis and representation of the corresponding Job Trace.

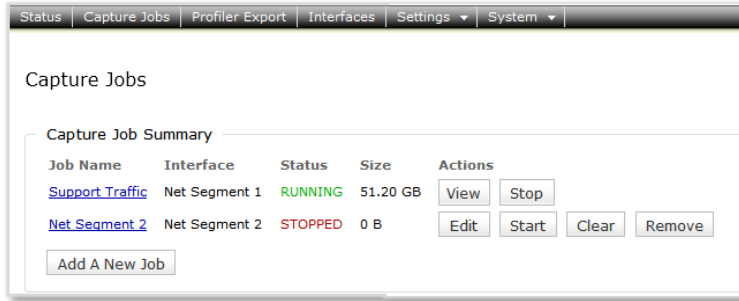
A NetShark includes two separate storage subsystems:

- System Storage containing the NetShark file system, software, pcap trace files, View metrics, and Microflow Indexing data for Job Traces and pcap files. User Data Storage is a subset of System Storage that stores data resulting from customer-specified operations, such as index files and pcap files.
- Packet Storage containing the RAID Array used by the NetShark Packet Recorder to store Job Traces. This storage system is optimized to provide high-speed writing to disk and fast read access for arbitrary time intervals within a Job Trace.

Note that Packet Analyzer can view capture jobs on a NetExpress, but it cannot add or edit capture jobs on a NetExpress.

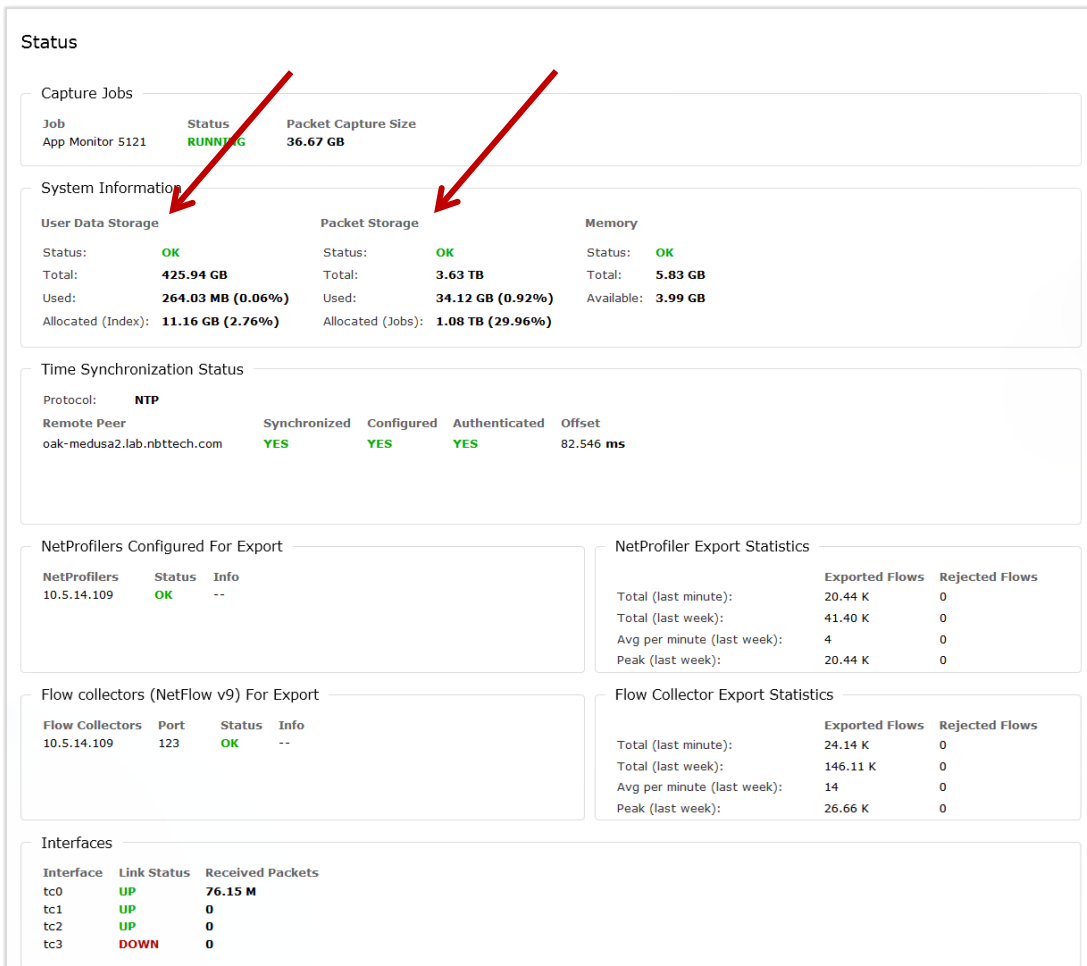
Capture Jobs

The Capture Jobs tab takes you to a screen showing currently running capture jobs.



NetShark Packet Recorder – Two Capture Jobs

The Status tab shows the status and usage of User Data Storage and Packet Storage.



To reformat the packet storage, click the System tab, select Maintenance, and go to the Storage Status section.

The New Reserved Space field can be used to prevent use of the inner tracks of hard disks that can have slower transfer rates. Setting this value to something other than 0% can in some cases provide more uniform write-to-disk speeds although it reduces the amount of storage available for packet capture.

Clicking the **Reformat Packet Storage** button reformats the Packet Storage and applies the specified New Reserved Space parameter to the hard disks.

*Note: **Reformatting the packet storage destroys all recorded packet data on the appliance and should be done only when instructed by Riverbed Support.***

[Status](#) | [Capture Jobs](#) | [NetProfiler Export](#) | [Interfaces](#) | [Settings](#) | [System](#)

[Licenses](#)
[Update](#)
[Maintenance](#)
[Copyright Information](#)

Maintenance

System Info

SteelCentral NetShark Version: **10.8 (10.8.1005.8744)**
 REST API Version: **5.3**
 Serial Number: **LD5RT00001863**

Log Download

Current
(Includes current NetShark Probe and NetShark Packet Recorder logs.)
 NetShark Probe
(Includes all NetShark Probe logs.)
 Select Log: Packet Recorder
(Includes all NetShark Packet Recorder logs.)
 Complete
(Includes all NetShark Probe logs and all NetShark Packet Recorder logs.)

Case ID:

Storage Status

System Storage Status: **OK**
 Packet Storage Status: **OK**
 Packet Storage RAID level: **0**
 Packet Storage Total Space: **65.48 TB**
 Packet Storage Available Space: **65.48 TB**
 Packet Storage Used Space: **128 MB**

Model: SCAN-06170 Serial: LD5RT00001863 Status: **OK**

Model: SCAN-SU-72TB Serial: LD0000 Status: **OK**

New Reserved Space: %

Write speed tends to be slower at the end of hard drives. By setting the 'New Reserved Space' parameter, you can prevent the appliance from writing at the end of packet storage. This will reduce the available storage size, but it will make disk write performance more uniform.

Important: Reinitializing or reformatting packet storage will cause all packets in the capture jobs to be lost.

System Halt

Storage status and options

Add/Edit Capture Jobs

This section describes how to create a Capture Job and subsequently manage it. Multiple Capture Jobs can exist simultaneously.

Clicking **Add New Job** displays a new Capture Job form on the Capture Job page. This form is shown in Figure 22. The form has a Capture Settings section and a Retention Settings section with two tabs: Data Retention and Start/Stop Settings.

Add New Job

Capture Settings

Name:

Status: **Stopped**

Interface:

(NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

Enable Indexing

Enable DPI

Start new job immediately

Retention Settings

Packet Data (Packet Storage Total Space: 65.48 TB, Unallocated Space: 44.84 TB)

Packet Retention Size: % Of Disk

Additional Retention Criteria: Packets

Seconds

Microflow Index (User Data Storage Total Space: 2.96 TB, Unallocated Space: 2.57 TB)

Retain Index On Disk Up To: % Of Disk

Additional Retention Criteria: Days

Synchronize With Packet Recording

Note: Packets are stored in specially formatted packet storage. Indexes are stored in the conventional User Data Storage.

Figure 21: Adding a Capture Job

Capture Settings

A few basic configuration parameters need to be set when creating a Capture Job:

- *Name* provides a descriptive name for the Capture Job and identifies the Capture Job in the Packet Analyzer Devices and Files source panels.
- *Interfaces* shows the available network interfaces. The Capture Job takes traffic from the selected interface and records it to disk.

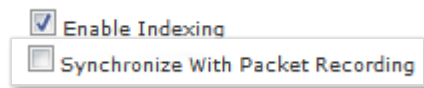
- *BPF filter* can be provided to select a subset of the traffic for capturing. For example, the BPF filter `src host 172.18.5.4` captures only the packets with source IP address 172.18.5.4.
- *Packet Bytes to Capture* puts an upper bound on the number of bytes saved for each packet (the *snaphen*). The default value of 65535 captures the entire packet.

Retention Settings

Data Retention

On the **Data Retention** tab you can specify these parameters:

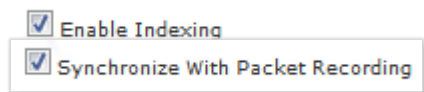
- **Packet Data:** These fields limit the amount of storage used by the Capture Job. They can be specified in terms of storage (either in megabytes or a percentage of the total packet store), a maximum number of packets, and/or a maximum time interval of packets. After the limit is reached, the oldest packets are discarded as new packets arrive.
Note: Retention criteria are evaluated after each 128 MB capture block, then enforced.
- **Microflow Index:** There are a number of microflow indexing parameters that need to be set when creating a Capture Job, as shown below.



Microflow Indexing Enabled

- Microflow Indexing Enabled – With the **Enable Indexing** checkbox selected and the **Synchronize** checkbox not selected, the Retain Index on Disk parameters control the size and duration of the Conversation Index.
 - If the Days checkbox is selected, then the duration of the indexing data is limited in duration by the number of days entered in the field
 - If the Days checkbox is not selected, then the size in bytes of the indexing data is bounded by the value in the Retain Index on Disk field.

Note: The duration of Microflow Indexing is typically set to be significantly longer than the duration of the Packet Recording since it consumes much less storage.



Synchronized Microflow Indexing

- Synchronized Microflow Indexing – When both **Enable Indexing** and **Synchronize with Packet Recording** are selected, then the duration of the indexing data is kept synchronized with the duration of the corresponding Capture Job. This ensures that all views (both those that use only the index and those that require the packet data) are available for the same time period, although it likely limits the amount of index that can be retained.
- No Microflow Indexing – If the **Enable Indexing** checkbox is not selected, then the indexing data



Microflow Indexing Disabled

are not created for this Capture Job. In general, disabling indexing is not recommended, and this should be done only in cases where the index computation impacts the performance of the packet capture.

The following is a *simplified* version of the underlying computation performed by the NetShark when the Microflow Indexing feature is enabled.

For each packet, the *Conversation Identifier* consists of the 5-tuple:

1. Source IP address
2. Source Port
3. Destination IP address
4. Destination Port
5. IP Protocol

When the Microflow Indexing feature is enabled, the NetShark computes the total bytes and number of packets for each unique conversation identifier in the traffic stream for each second. This information is stored in a file and is referred to as *Microflow Indexing data*.

The Microflow Indexing data is all that is needed to compute many of the View metrics associated with the traffic stream. For example, Bandwidth Over Time, Network Usage By Port Group, IP Conversations, and Protocol Distribution are just a few of the Views that can take advantage of the existence of indexing data.

Start / Stop Settings

On the **Start / Stop Settings** tab you can specify these parameters:

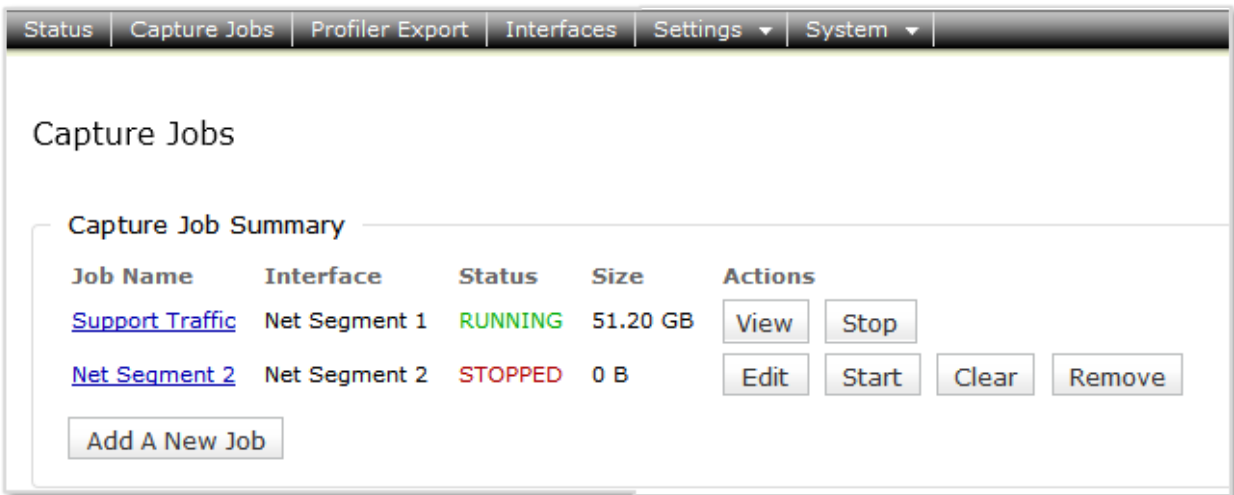
- **Absolute Start/Stop Time:** These fields specify absolute starting and stopping times for the job.
- **Stop Capturing After:** These fields specify conditions for stopping the job based on the consumed storage (in megabytes or a percentage of the total packet store), the number of packets, or the duration of the capture.

Note: When multiple conditions are selected, the most restrictive condition is the controlling condition. For example, if stop conditions for both the absolute stop time and a maximum number of captured packets are selected, then the first condition to be satisfied stops the capture job.

Note: The Capture Job Recording is stored in Packet Storage and the Microflow Indexing data are stored on the System Storage.

Capture Job control buttons

To get to the buttons that control a Capture Job, click the Capture Jobs tab to see the Capture Job Summary on the Capture Jobs screen.



This summary includes the job control buttons:

- View—shows the Job Details screen for the capture job.
- Edit—shows the Job Details screen for the capture job and allows you to edit job parameters.
- Start—starts the capture job.
- Stop—stops the capture job. When a capture job is stopped both the packet recording and the calculation of the Microflow Indexing data are stopped.
- Clear— removes all data associated with the capture job, including the Packet Recording and the Microflow Indexing data storage. This should be used only when the capture job is in the stopped state. The definition and configuration of the job remain and the job can be restarted later.
- Remove— removes all of the data and configuration associated with the capture job. The **Remove** button should be used only when the capture job is in the stopped state.

To see the job statistics, click the job name to go to the Job Details screen. Figure 23 shows the job statistics. The Total Packet Capture Size shows the amount of storage currently used by the capture job. The screen also shows statistics regarding the number of Written (Captured) and Dropped Packets for the last second, minute, and hour.

The screenshot shows the 'Statistics' screen with the following information:

Start Packets: 4/25/2014 08:02:52 (-0700)
End Packets: 4/25/2014 14:12:48 (-0700)
Packet Capture Size: 1.08 TB
Microflow Index Size: 11.16 GB

Packets	Last Second	Last Minute	Last Hour
Written:	90.49 K	5.61 M	306.78 M
Dropped:	0	0	0

Figure 22: Managing a Capture Job

Capture Jobs in the Packet Analyzer Devices panel

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



Job Interface icon

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

Figure 24 shows five Job Interfaces:

- Application Watch
- NFS Traffic Study #32
- Test Area Traffic
- Traffic Capture #12936
- VoIP Monitor

These interfaces behave as ordinary live traffic sources. The actual physical interface corresponds to the interface setting in the corresponding Capture Job. NetShark interfaces **tc0 – tc2** use custom names and descriptions, listed alphabetically by name, configured on the “Interfaces” tab of the NetShark web UI. Interface **tc3** uses its default name and description.

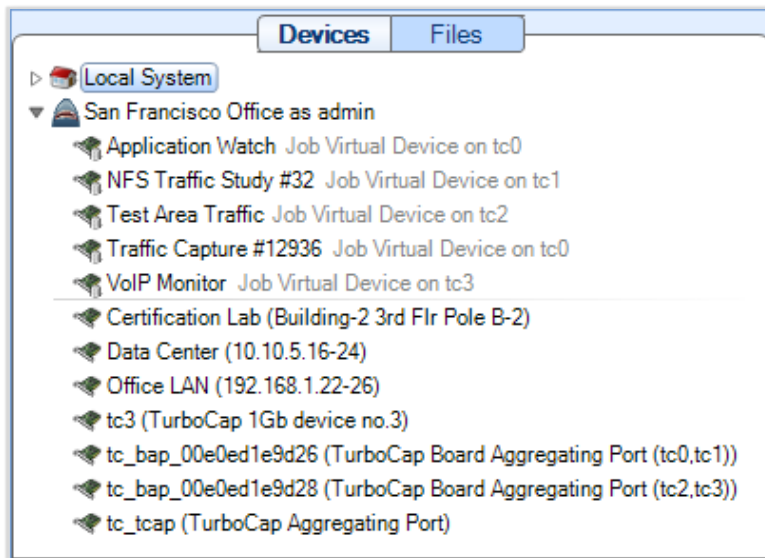


Figure 23: Job Interface in Devices panel

Packet Analyzer Operations on Job Interfaces

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

Capture Jobs in the Packet Analyzer Files panel

The Files panel for a NetShark contains a *Jobs Repository Folder*. The Jobs Repository folder contains a *Job Trace* for each Capture Job. The Job Trace has the same name as the Capture Job and represents the network traffic recording. Each Job Trace has an associated icon that represents the extent to which the Microflow Indexing data is available, as follows.



Denotes a Capture Job without Microflow Indexing data

Job Trace without Microflow Indexing



Denotes a Capture Job with Microflow Indexing enabled in which the Microflow Indexing data and the Job Trace packet recording durations are the same.

Job Trace with Microflow Indexing



Job Trace with Mixed Microflow Indexing

Denotes a Capture Job with Microflow Indexing enabled, but for which the duration of Microflow Indexing data is longer than the duration of the Job Trace recording. Some views can operate on index data alone, while other views require the underlying trace (packet) data as well.

Figure 25 shows the contents of the Jobs Repository folder in the Files Panel of Packet Analyzer. It contains five Job Traces with varying options for Microflow Indexing as shown by the icons.

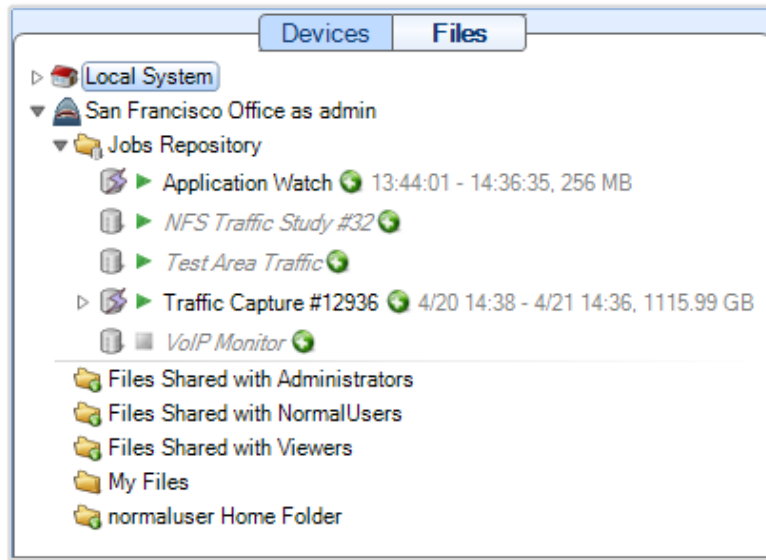


Figure 24: Jobs Repository folder in the Files panel

Packet Analyzer Operations on Job Traces – Trace Clips

It is not unusual for Job Traces to be multiple terabytes in size, making direct operations on them inefficient and slow. A Trace Clip identifies a time interval within a Job Trace. Trace Clips divide

these potentially massive network traffic recordings into user-defined time intervals. There are a number of simple and visually oriented ways in which Trace Clips can be created using Packet Analyzer. Trace Clips do not require any additional storage and behave exactly like ordinary trace files.

Note: Unlike trace files, Trace Clips can expire, depending on a Capture Job’s Retention Settings. When a Capture Job reaches its maximum packet retention size, new packets overwrite the oldest Job Trace packets, expiring all Trace Clips whose time interval included those overwritten packets. Expired Trace Clips are shown in red under a Job Trace in the Files panel. A Trace Clip that must be kept can be sent to a file (right click on the Trace Clip and select “Send to > File”) or locked (right click on the Trace Clip and select “Lock”). Lock is best used to retain a Trace Clip for a short period of time, as it decreases the storage available for the Capture Job.

Trace Clips are found in the Files panel under its corresponding Job Trace in the Jobs Repository folder. They are identified by the icons shown below.



Trace Clip



Trace Clip with Index



Trace Clip with Microflow

Trace Clip with packets and no Microflow Indexing data

Trace Clip with packets and Microflow Indexing data available throughout the time interval

Trace Clip with packets for some or none of the interval, and Microflow Indexing data throughout the interval

Figure 26 shows a Trace Clip named JLB Trace Clip for which there is no Microflow Indexing data available. Figure 27 shows two trace clips that have associated Microflow Indexing data.

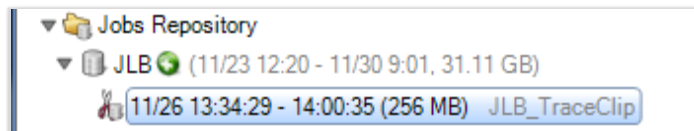
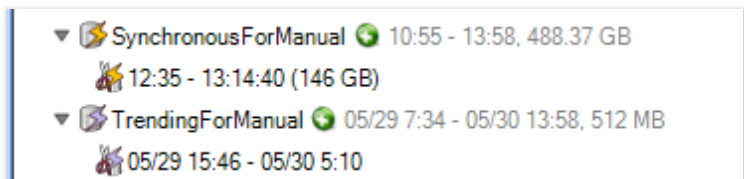


Figure 25: Trace Clip for JLB



Time Scroll

Figure 26: Trace Clips with Microflow Indexes

Creating Trace Clips

Trace Clips can be created in three ways:

- Using the Time Control panel (not to be confused with the Time Control Ribbon described earlier)
- Dragging a time interval from a Strip Chart in a View and dropping it on a Job Trace
- Dragging an event from the Events Panel and dropping it on a Job Trace

Using the Time Control panel to create a Trace Clip

There are two ways to display the Time Control panel used to create a Trace Clip.



Figure 27: Creating a Trace Clip

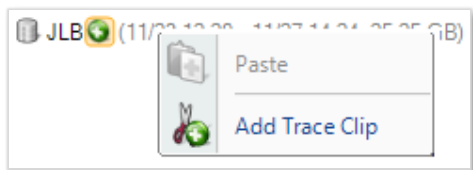


Figure 28: Add a Trace Clip

- Figure 28 shows the Job Trace named JLB. Clicking the **plus** icon to the right of the name displays the Time Control panel shown in Figure 30.
- Right clicking the **Job Trace** displays a context menu (**Figure 29**) with the menu item **Add Trace Clip**. Selecting this menu item displays the Time Control Panel.

If the clipboard contains a time interval, then the **Paste** menu item can be used to create a Trace Clip corresponding to that time interval. See Paste in the Filter section of the panel for more information.

Figure 30 shows the Time Control panel for creating a Trace Clip. Create a Trace Clip by selecting a time interval (time filter) and an optional filter (see the funnel button in “Filter Details” at the bottom of the panel). A Trace Clip is automatically assigned a name made up of the starting date and its time interval. The **Description** text field can be used to add additional information about the Trace Clip. Beginning in release 10.7, a filter used when creating a trace clip is displayed under the trace clip name in the Files panel. The rest of the options in the Time Control panel provide various ways of selecting a time interval and an optional filter. After the selections are made, clicking **OK** creates a Trace Clip corresponding to the selections made.

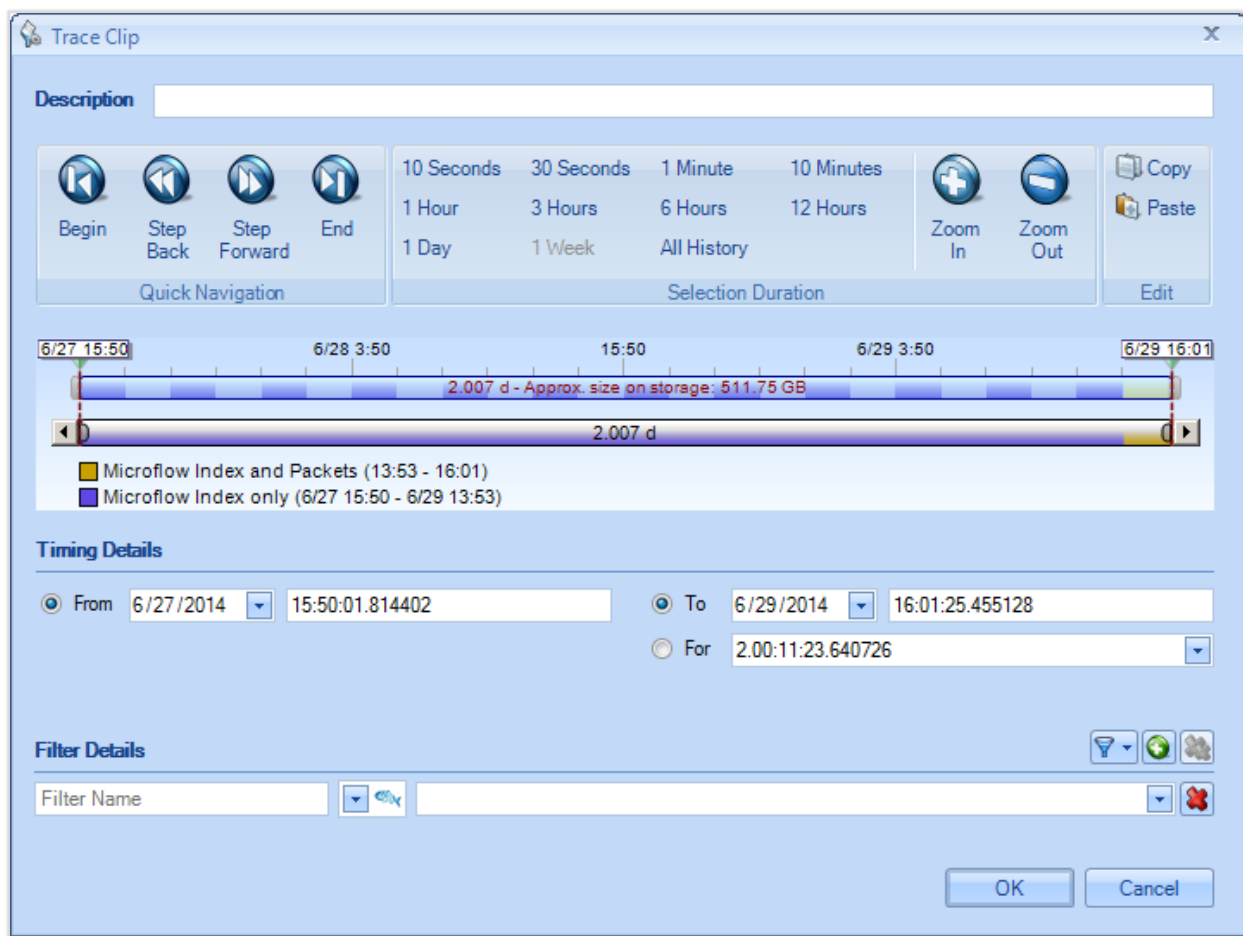
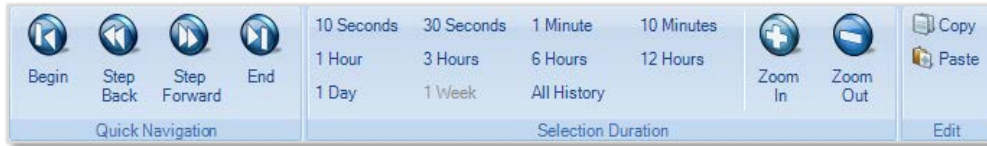


Figure 29: Time Control panel for creating Trace Clips

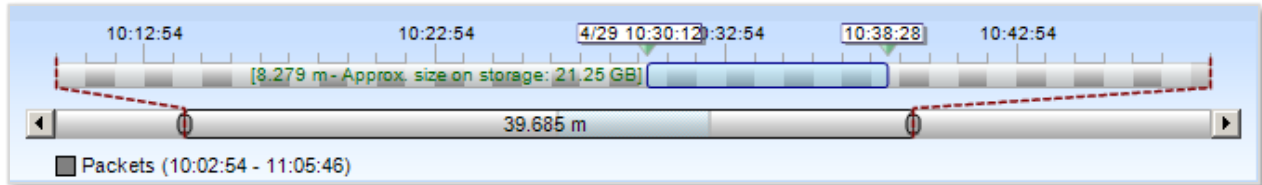
Selecting a Time Interval using the Time Control Panel

There are multiple ways to create the time interval for a Trace Clip using the Time Control Panel. The most common approach for networking issues identified by a particular onset time is to specify the **From** time in the Timing Details section. Then, specify either the **To** time or the **For** duration. The Quick Navigation, Selection Duration, and Filter sections at the top of the panel also can be used to select a time interval. See the “Time Control Ribbon” section earlier in this document for a detailed explanation of the Quick Navigation and Selection Duration controls and their use. The Filter control is described below.



Trace Clip time selection

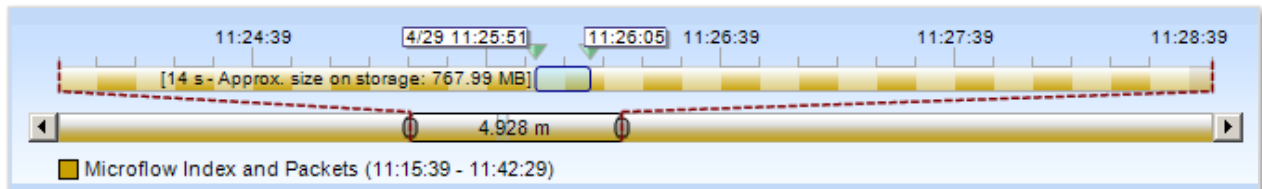
Another set of options for selecting a time interval involve using the multi-level zoom scroll bars in the middle of the Time Control panel. This has the advantage of making it clear whether the selected time interval contains packets and/or Microflow Indexing data.



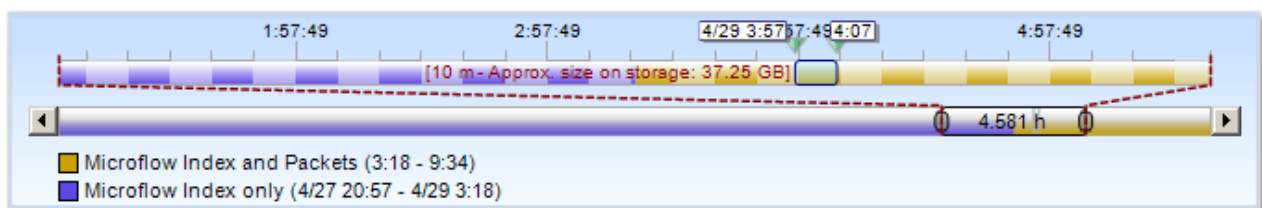
Packets Only

When the Time Control panel is first opened, the upper bar is a graphical representation of the duration of the entire Job Trace, and the lower Time Scroll Bar enables zooming in and out over the duration. In cases where the Job Trace contains both packets and Microflow Indexing data, the duration of the upper bar represents the *maximum* of the packet capture duration and the duration of the index data. A Trace Clip time interval can be selected by moving the triangular markers on top of the upper bar or by resizing the blue rectangle in the bar, representing the selected time interval.

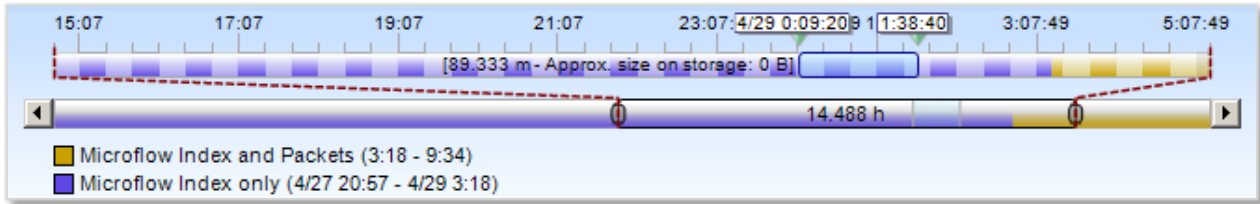
The following are a series of images representing the various configurations of packets and Microflow Indexing data that may be found and selected in a Job Trace.



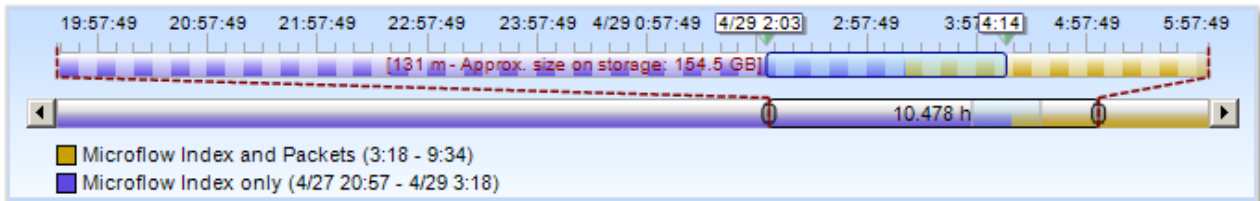
Packets plus Microflow Indexing Data



Packets plus Microflow Indexing Data - Only Packets Selected



Packets plus Microflow Indexing Data - Only Microflow Indexing Data Selected



Packets plus Microflow Indexing Data - A Combination of Packets plus Microflow Indexing Data Selected

Selecting a Filter using the Time Control Panel

A Trace Clip not only represents a time interval, but it also can contain filtered packets. Figure 31 shows the Filter Details section of the Time Control panel for creating Trace Clips. Click the funnel button to display the Filter Editor for selecting a filter. It is important to select a filter that is compatible with the Microflow Indexing data of the selected time interval, discussed above.



Figure 30: Show Filter Editor

Figure 32 shows the Filter Editor. Note that nearly all of the filters in the default set are Microflow Indexing-compatible NetShark Filters.

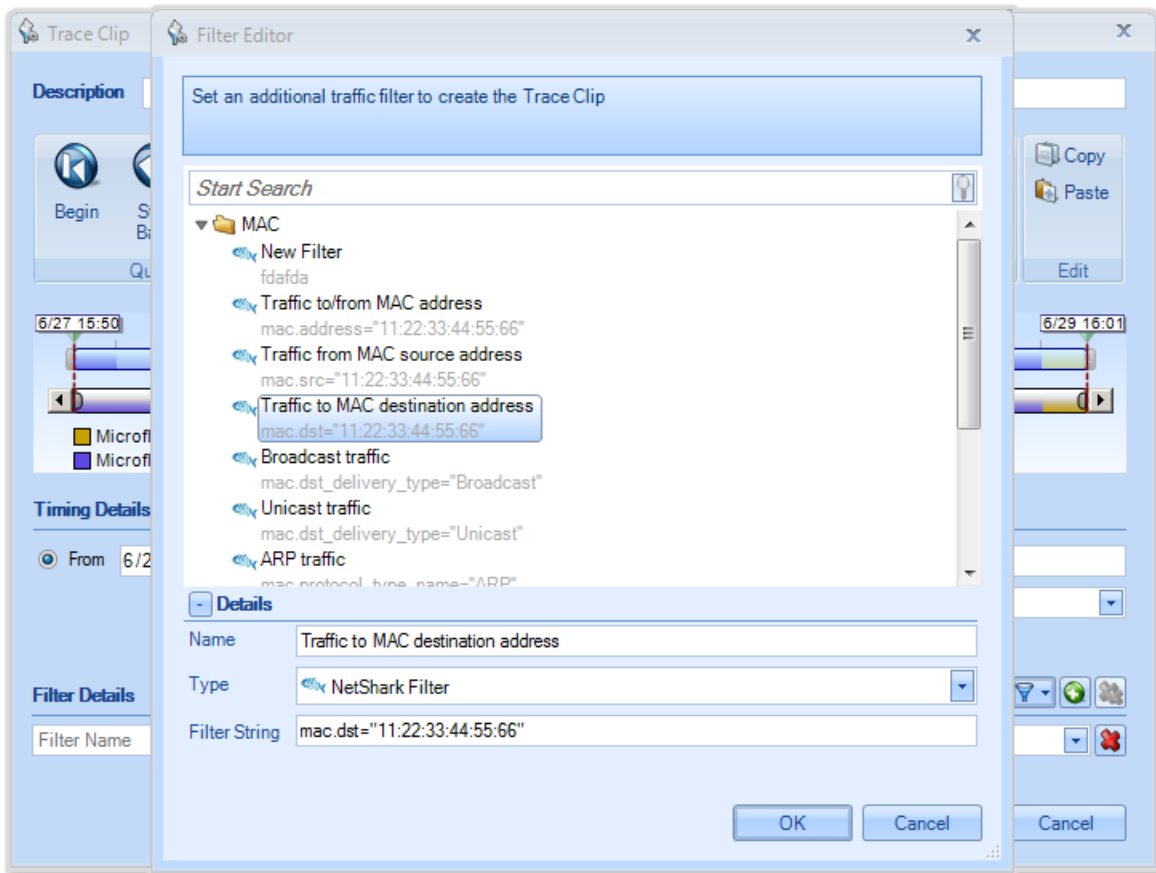
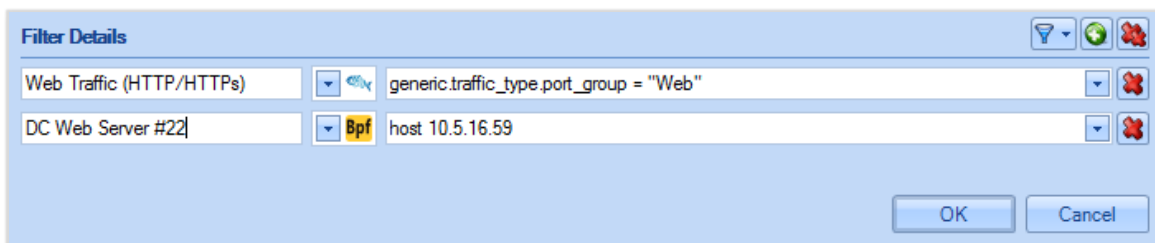


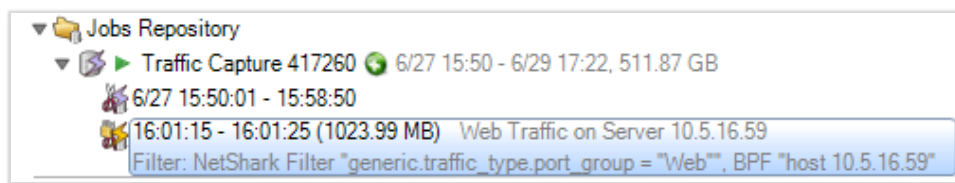
Figure 31: Filter Editor

By clicking plus button in the Filter Details section, you can add additional filters, the same way you do when adding filters to a view. Clicking the funnel button opens the Filter Editor for adding additional filters. See “XXX” for more information on entering filters.

The filter below creates a trace file of web traffic to or from a specific web server (10.5.16.59).



The trace clip appears in the Files panel with the filters used appearing under the trace clip’s name.



Follow these steps to apply a filter when creating a Trace Clip.

1. Click on the funnel in the “Filters Details” section to open the Filters Editor (Figure 31).
2. Select an existing filter, modify an existing filter or right click in the Filter Editor and select “New Filter” to create a filter that meets your requirements.
3. Click OK when your filter is defined. The Filter Editor closes.
4. Click OK on the Time Control panel and a filtered Trace Clip is created.

Important: When sending a trace clip to a file for saving, be sure to add filter information to the file name for reference. No filter information is captured from the trace clip.

A quick way to create a new filter is to drag a chart element to the Filters tab. The filters panel opens and a new filter is created.

Here is an example: A Network Usage by Port view was applied to a Trace Clip. The NFS traffic in the chart warranted further investigation, so the NFS line in the chart was selected and dragged onto the Filter tab, as shown below.

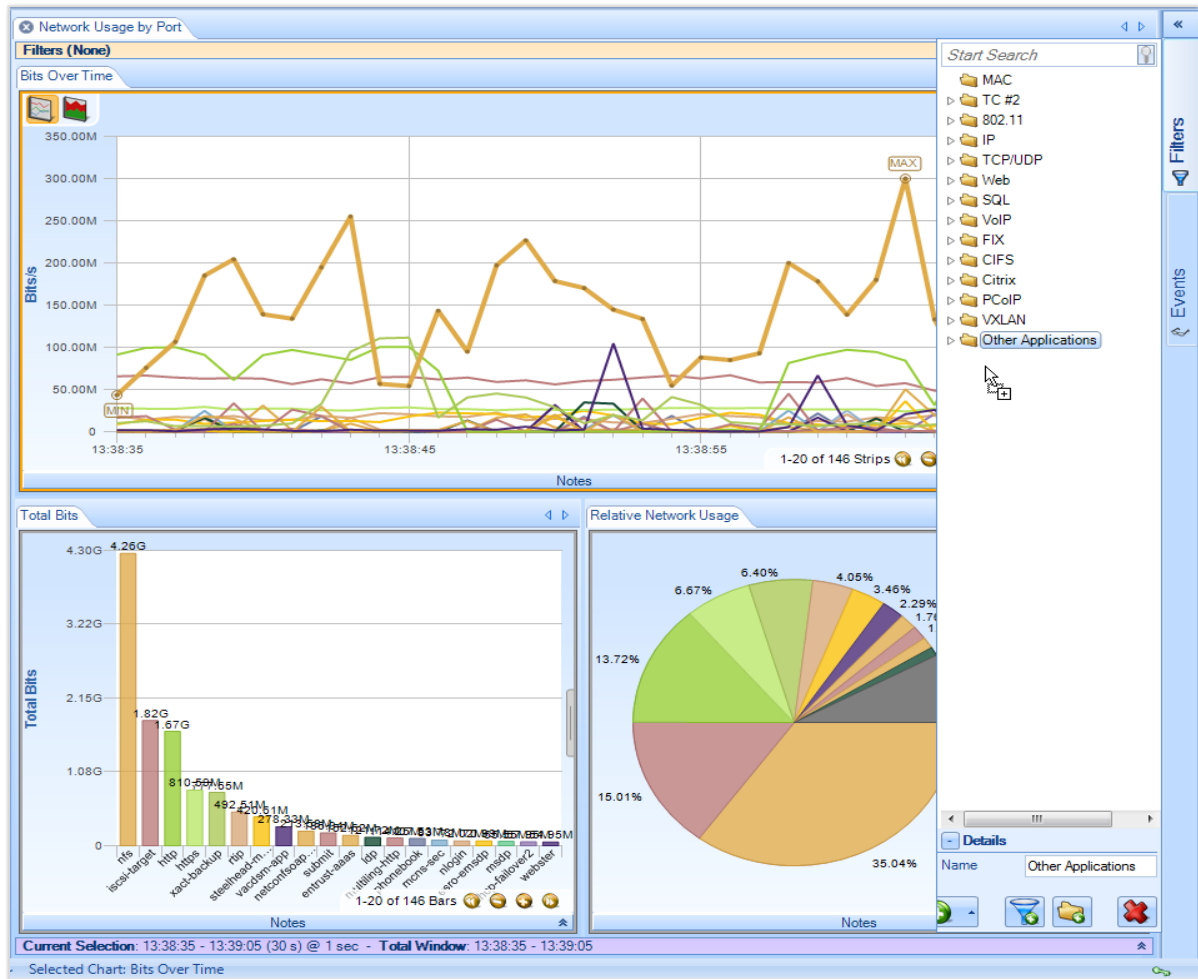
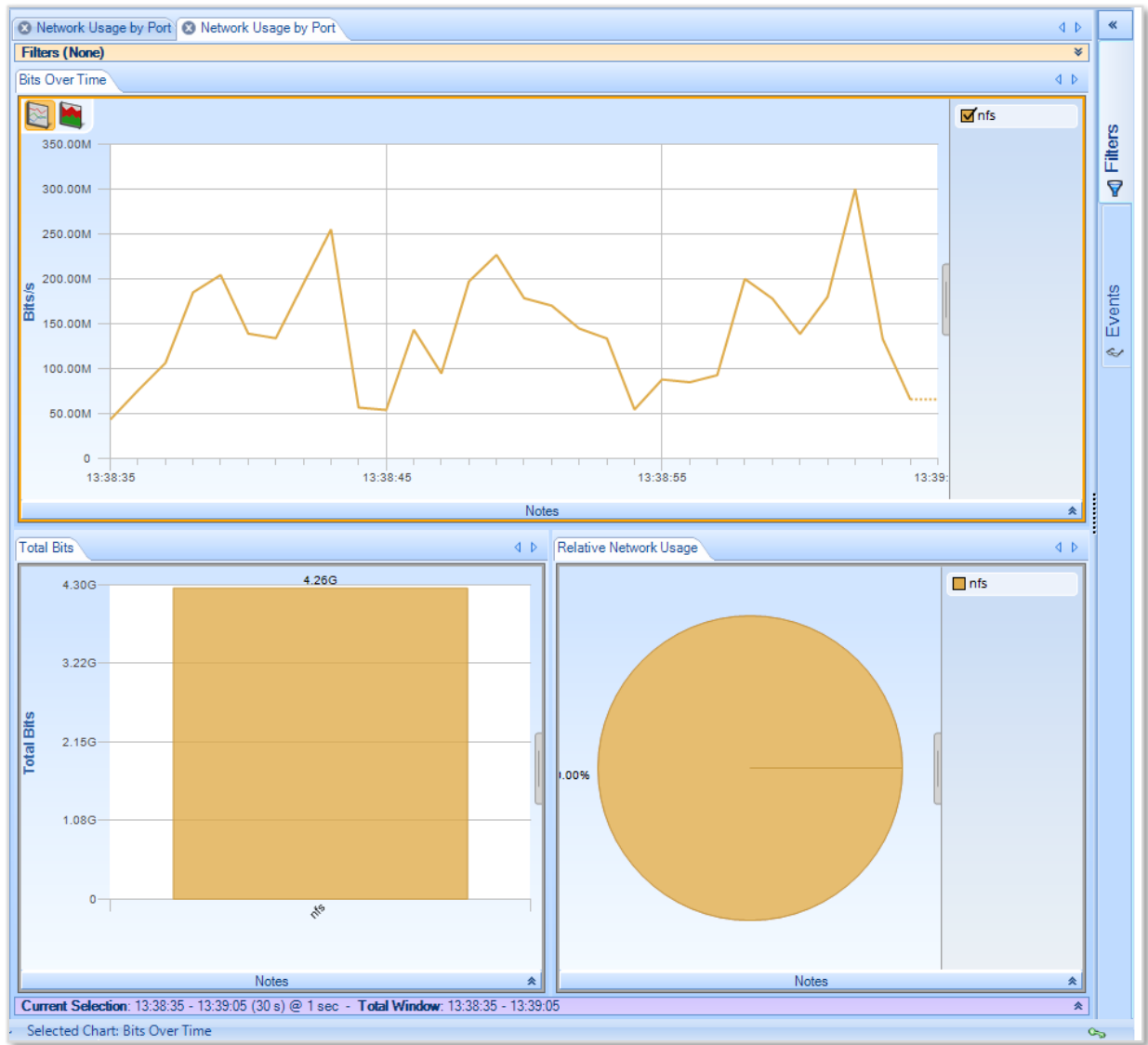


Chart Element dragged to Filter panel to create a Filter

A new Trace Clip was made using the same time interval as the first Trace Clip and applying the NFS filter. When the Network Usage by Port view is applied to the new Trace Clip the resulting chart shows just the NFS traffic. Drill down can be used for further investigation of this traffic.



Filtered Trace Clip with Network Usage by Port View

When creating Trace Clips over the same time interval from multiple Job Traces captured over the same time period, use the Copy and Paste buttons in the Filter section of the Time Control panel.

1. Select the time period in the Time Control panel for the first Trace Clip.
2. Before pressing **OK**, press **Copy** to place the selected time interval on the clipboard.
3. Go to the next Job Trace and right click on it, then select **Paste** from the context menu to create a Trace File over the same selected time interval used in the first Job Trace.

With this method, you can quickly create Trace Clips covering the same time interval to review traffic from multiple Job Traces.

Using Time Selection to create a Trace Clip

Figure 33 shows a time selection in a strip chart. The strip chart was obtained by applying the Bandwidth Over Time view to the Traffic Monitor #41414 Interface. Figure 34 switches from the

Devices panel to the Files panel, showing the corresponding Traffic Monitor #41414 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 Traffic Monitor #41414 Job Trace (11:52:20 – 12:02:19). Note that the Job Trace is over 511 GB, but the Trace Clip is only 32 GB.

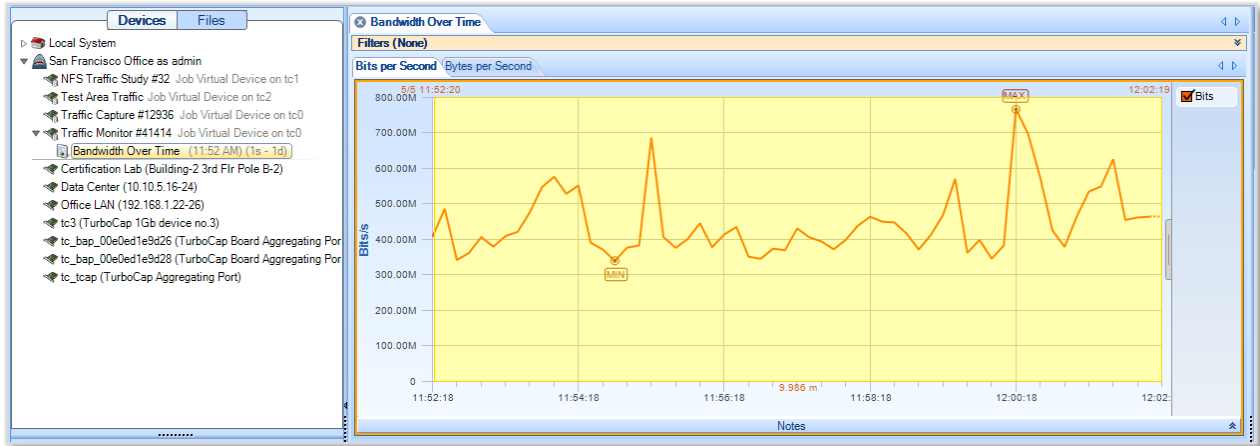


Figure 32: Time Selection in a Strip Chart

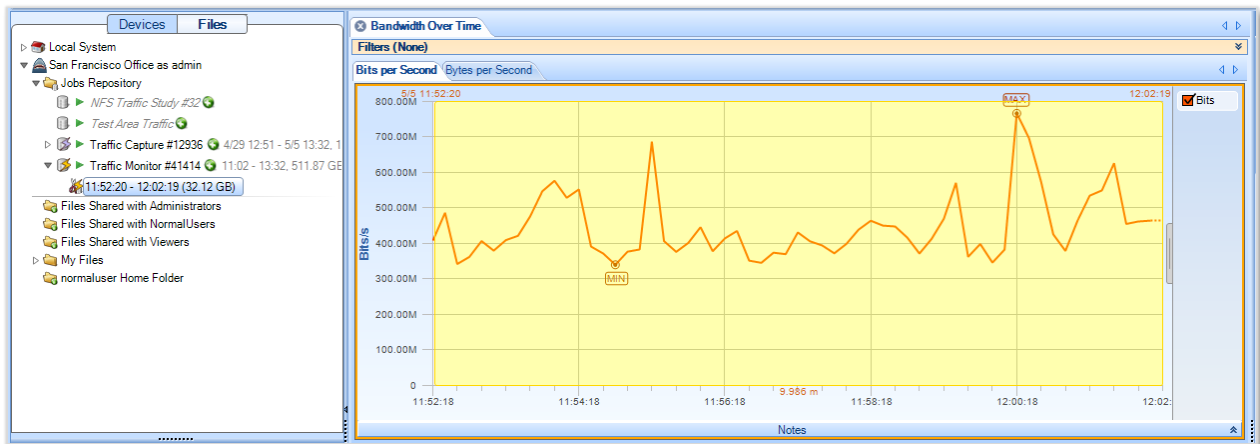


Figure 33: Time Selection dragged over Job Trace to create a Trace Clip

In Figure 35 the Bandwidth Over Time view is applied to the Trace Clip below the Traffic Monitor #41414 Job Trace. Note the similarity to the view in Figure 33.

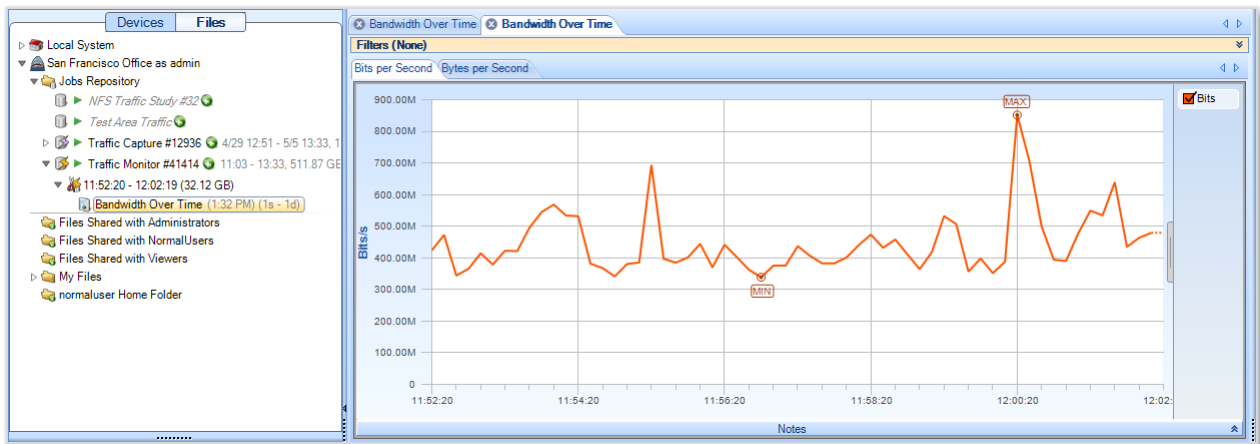


Figure 34: View applied to a Trace Clip

Note: The view in Figure 33 was obtained through the analysis of a live source, while the view in Figure 35 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 Packet Analyzer.

Using Events to create Trace Clips

It is important to be able to easily isolate network traffic associated with an event for troubleshooting and diagnostics. This is easily accomplished by dragging the event in question over the Job Trace. A Trace Clip is automatically created that contains traffic occurring before and after the event.

Figure 36 shows the Event Panel and a particular event, 6017, that has been highlighted both in the Event Panel and on the Strip Chart. The events were created using a Watch on the live traffic corresponding to the Traffic Monitor #41414 Capture Job.

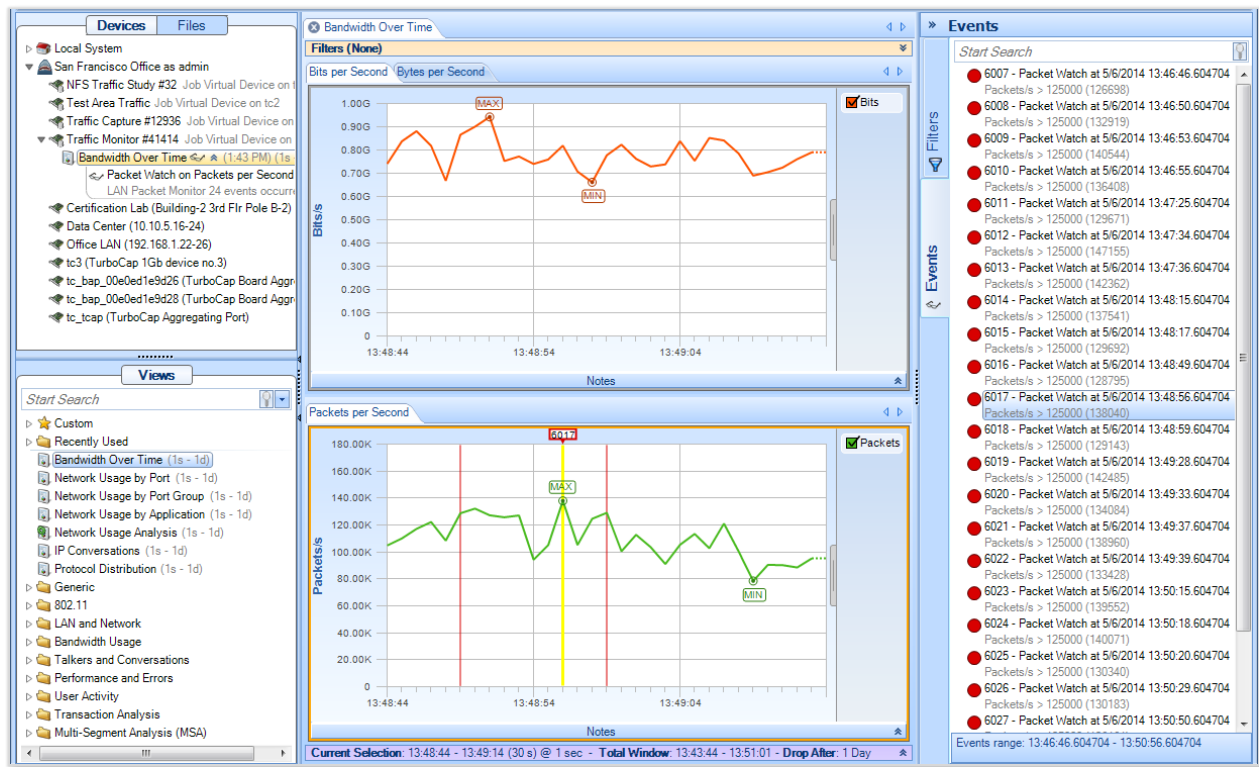


Figure 35: Event Panel

Creating a Trace Clip around the (temporal) location of the event is as easy as dragging the event from the Event Panel to the Traffic Monitor #41414 Job Trace. Dragging Event 6017 from the Event Panel and dropping it on the Traffic Monitor #41414 Job Trace displays the Time Control panel for creating the Trace Clip. See Figure 37.

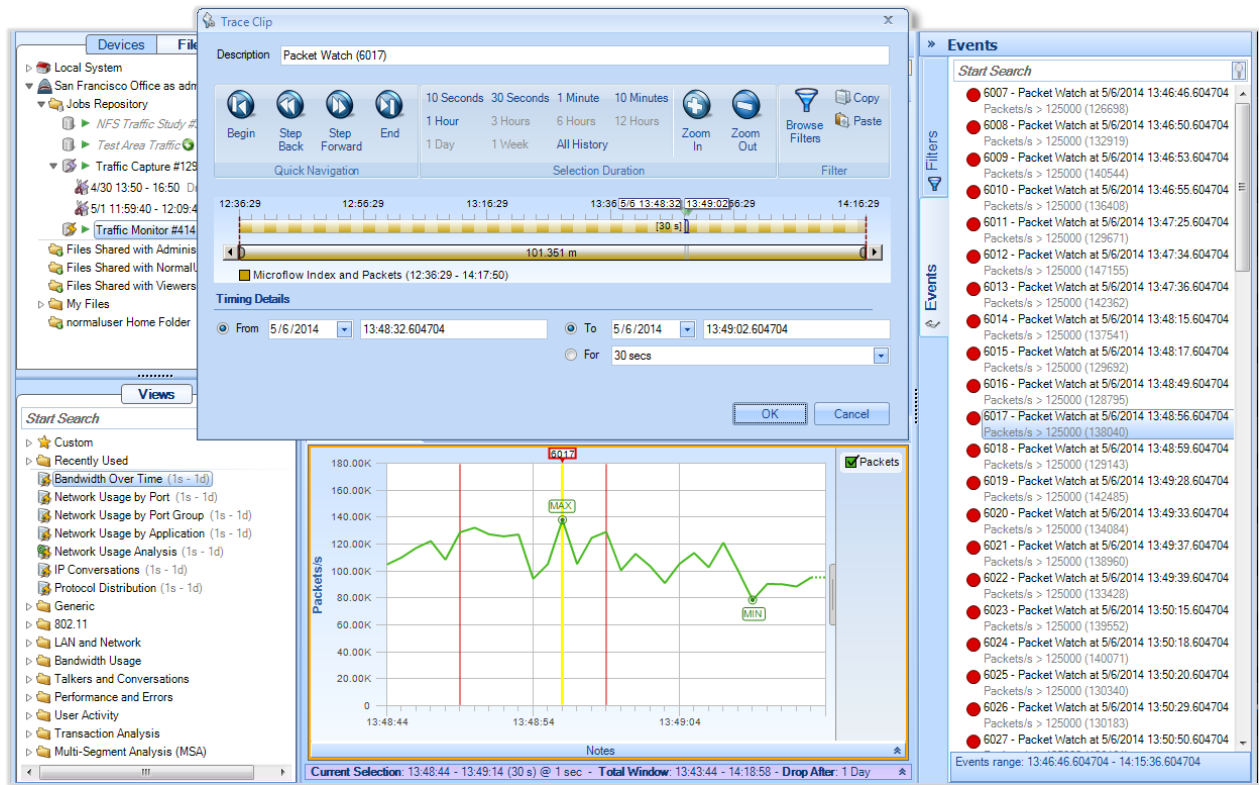


Figure 36: Creating a Trace Clip from an Event

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 38.

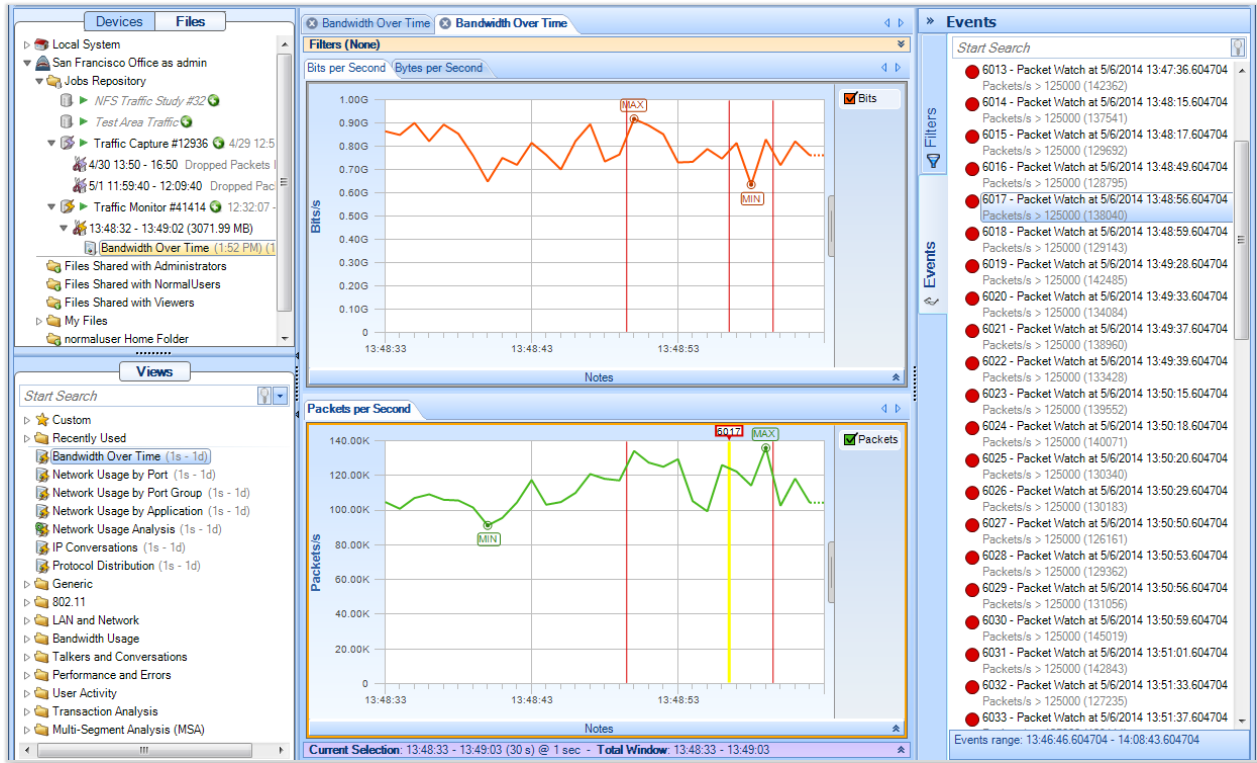
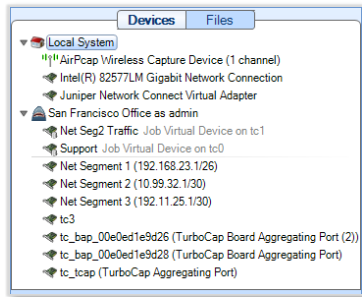


Figure 37: Trace Clip corresponding to an Event

To investigate the event, select a time period of interest and use drill down.

Sources Panel

The Sources Panel has two tabs: Devices and Files.



Sources Panel

The *Sources Panel* contains representations of NetShark appliances, live interfaces, trace files, and Capture Jobs and is one of the most important parts of Packet Analyzer.

Clicking the tabs switches between displaying the devices and the trace files.

Devices

Shows local interfaces under the Local System icon and NetShark appliances with their associated interface offering live sources of network traffic to Packet Analyzer.

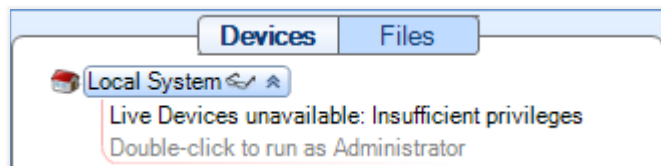
Files

Shows local folders and trace files under Local System and NetShark appliances with their associated folders and trace files.

Devices

Devices on your local system require administrator privileges to capture network data. Remote capture devices, such as NetShark appliances, do not require administrator privileges.

If you are running Packet Analyzer in non-administrator mode, you will see the following prompt as the software initiates and tries to connect to your local resources.



If you have administrator privileges on the system, you can double-click on the prompt to make those resources available for capture jobs.

Packet Analyzer supports two basic classes of networking devices:

- Wired Ethernet
- Wireless (802.11)

Wired Ethernet Adapters



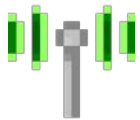
Most wired Ethernet network interface cards work in Packet Analyzer. There are two types of adapters—one presented by the actual interface and one presenting the interface corresponding to a Capture Job.

Wired Ethernet Adapter



Wired Ethernet Adapter associated with a Capture Job

Wireless Adapters



Wireless Adapter

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

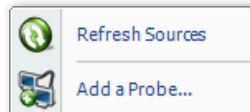
Additionally, multiple Riverbed AirPcap adapters are shown as a single device because the wireless adapters share the same airspace and, all adapters being equal, any one adapter can receive the same traffic as any other. Therefore, Packet Analyzer internally breaks up tasks among multiple adapters so 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 Packet Analyzer system, not on the NetShark.*

Context Menus in the Devices Panel

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

With No Probes Selected



Devices Panel (No Selection)

With nothing selected, the options are as follows:

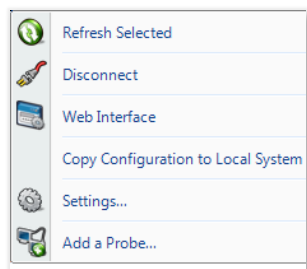
Refresh Sources

The *Refresh Sources* menu option causes Packet Analyzer to rescan the available interfaces on the local system and all connected NetShark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected NetShark 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 NetShark Selected



Devices Panel (NetShark Selected)

With a NetShark selected:

Refresh Selected

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

Disconnect

The *Disconnect* menu option disconnects the selected NetShark from Packet Analyzer. The selected NetShark remains in the Probes list in the Remote Ribbon.

Web Interface

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

Copy Configuration to Local System

The *Copy Configuration to Local System* menu item initiates a manual synchronization of a Shark's port names, port groups, L4 mappings, and L7 fingerprints with the local system. This includes Service Response Time (SRT) ports (defined in Port Definitions on a Shark). This configuration is then used to analyze local files or views on local interfaces. Port names and port groups are effective immediately when downloaded from a Shark.

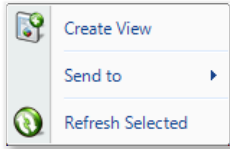
Settings

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

Add a Probe

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

With an Interface Selected on Local System



Devices Panel (Interface Selected)

With an interface selected, the options are as follows:

Create View

The *Create View* menu option opens the “View Editor” where you can build a custom view. The new view is saved to the Custom folder of the View Library. It can now be applied to other sources. See “View Editor” for details.

Send to

The *Send to* menu option instructs Packet Analyzer to send traffic from the selected interface to another application or a trace file, as described below.



Wireshark

The *Wireshark* menu option instructs Packet Analyzer to start up Wireshark and send all traffic from the selected interface to Wireshark.

Wireshark with Filter

The *Wireshark with Filter* menu option instructs Packet Analyzer to start up Wireshark and send traffic that matches a user-defined filter from the selected device to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

File

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

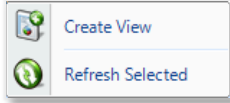
File with Filter

The *File with Filter* menu option instructs Packet Analyzer to send traffic that matches a user-defined filter from the selected device to a user-specified trace file. The filter is specified using the filter dialog box, which appears first and is explained in a later section.

Refresh Selected

The *Refresh Selected* menu option causes Packet Analyzer to rescan the available interfaces on the local system and all connected NetShark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected NetShark appliances are rescanned and updated to reflect whether files have been removed or modified.

With an Interface Selected on a NetShark



Devices Panel (Interface Selected)

With an interface selected, the option is:

Create View

The Create View menu option opens the “View Editor” where you can build a custom view. The new view is saved to the Custom folder of the View Library. It can now be applied to other sources. See “View Editor” for details.

Refresh Selected

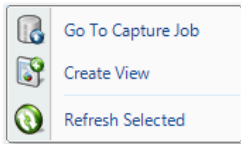
The *Refresh Selected* menu option causes Packet Analyzer to rescan the available interfaces on the local system and all connected NetShark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected NetShark appliances are rescanned and updated to reflect whether files have been removed or modified.

With a Job Virtual Device Selected (NetShark)



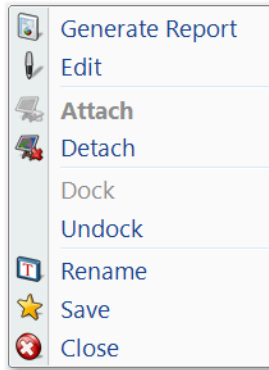
Job Virtual Device Selected Icon

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

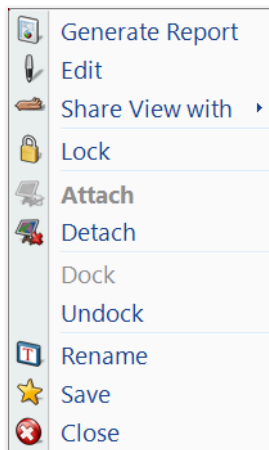


Job Virtual Device Selected Context Menu

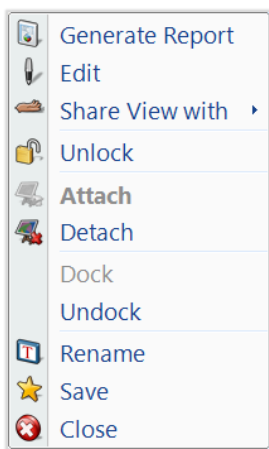
With a View Selected (Local System and NetShark)



View Selected, Local System



View Selected, Unlocked NetShark



View Selected, Locked NetShark

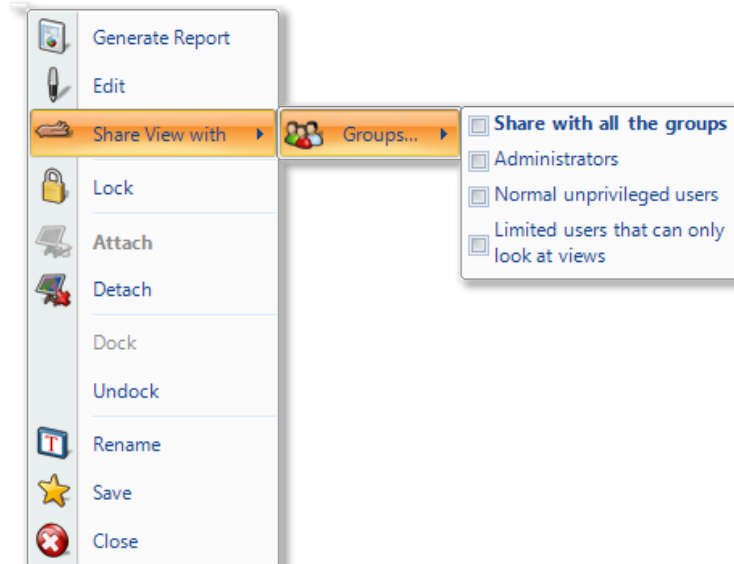
Generate Report

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

Edit

The *Edit* menu option opens the View Editor. The View Editor cannot be used with live devices.

Share the View with



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

Note: The *Share the View with* menu item only applies to NetShark appliances.

Lock, Unlock

If Lock is selected, then a small padlock image 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.

Note: The *Lock* menu item applies to only NetShark appliances.

Attach

If the selected View is Detached, then the *Attach* menu item attaches Packet Analyzer to the View.

Note: The *Attach* menu item applies to only NetShark appliances.

Detach

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

Note: The *Detach* menu item applies to only NetShark appliances.

Dock

If the View has been undocked from the Main Window, the *Dock* menu option re-docks it.

Undock

If the View is docked to the Main Window, the *Undock* menu option undocks it and places it in a separate window. For more information on undocking Views, see “**Error! Reference source not found.**”

Rename

The *Rename* menu option opens a dialog box that allows you to rename the View.

Save

The *Save* menu option saves the View as a Custom View.

Close

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

Files

Packet Analyzer 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 RadioTap¹ or PPI² 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. tun³, lo⁴, ppp⁵) are not readable. In most of these instances, the traffic passing through these interfaces will eventually pass through an Ethernet interface.

Capture Jobs running on remote NetShark 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 Packet Analyzer exactly as if they were PCAP files. Trace Clips that exist on a

¹ NetBSD: http://netbsd.gw.com/cgi-bin/man-cgi?ieee80211_radiotap+9+NetBSD-current

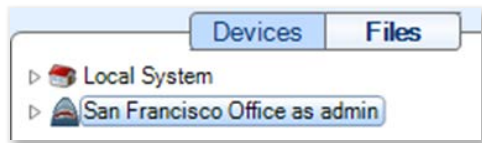
² CACE Technologies: http://www.cacetechnologies.com/documents/PPI_Header_format_1.0.1.pdf

³ FreeBSD: <http://www.freebsd.org/cgi/man.cgi?query=tun&manpath=FreeBSD+7.0-RELEASE&format=html>

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

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

NetShark can be converted to PCAP format using the Send-to-File feature of Packet Analyzer. The resultant PCAP file will be stored in the NetShark appliance's local file system.



Files Panel (closed)



Local System

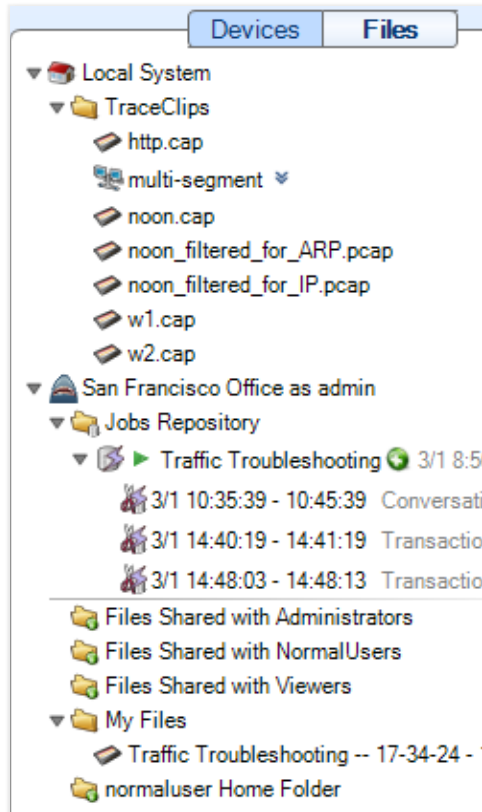


NetShark appliance

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

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

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



Files Panel (expanded)



AR with Shark Module



Jobs Repository



Job Trace



Trace Clip

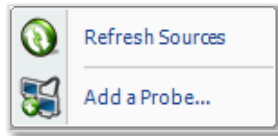


Trace File (PCAP)

Context Menus in the Files Panel

The context menus for the Files Panel are described below:

With Nothing or Local System Selected



Files Panel (No Selection)

The options are as follows:

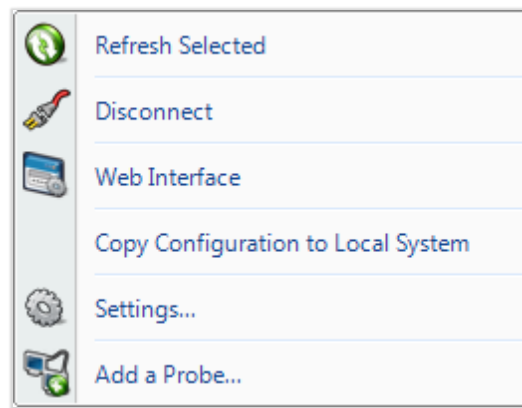
Refresh Sources

The *Refresh Sources* menu option causes Packet Analyzer to rescan the available interfaces on the local system and all connected NetShark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected NetShark 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 NetShark Selected



Files Panel (Probe Selected)

The options are as follows:

Refresh Selected

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

Disconnect

The *Disconnect* menu option disconnects the selected NetShark from Packet Analyzer and removes it from the Devices and Files panels. The selected NetShark remains in the Probes list.

Web Interface

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

Copy Configuration to Local System

The Copy Configuration to Local System menu item initiates a manual synchronization of a Shark's port names, port groups, L4 mappings, and L7 fingerprints with the local system. This includes Service Response Time (SRT) ports (defined in Port Definitions on a Shark). This configuration is then used to analyze local files or views on local interfaces. Port names and port groups are effective immediately when downloaded from a Shark.

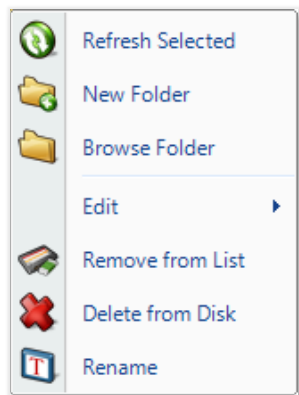
Settings

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

Add a Probe

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

With a Trace Folder Selected on Local System



Files Panel (Trace Folder Selected on Local System)Trace-file-sel-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.

New Folder

The *New Folder* menu option creates a new folder in the selected one. The user is asked to enter the name of the folder to create.

Browse Folder

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

Edit



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.

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 copies a previously Cut or Copied file to the selected “paste” location.

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.

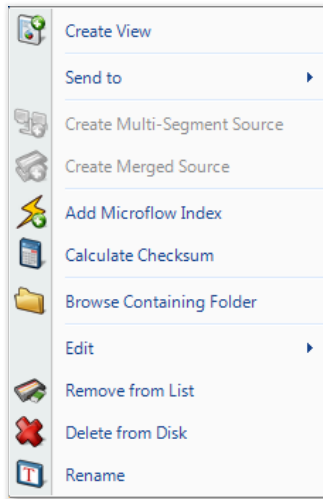
Delete From Disk

The *Delete Trace Files* menu option irrevocably deletes from the local system disk all trace files from the selected folder that do not have a view open on them.

Rename

The *Rename* menu option opens a dialog box that allows you to rename the View.

With a Trace File Selected on Local System



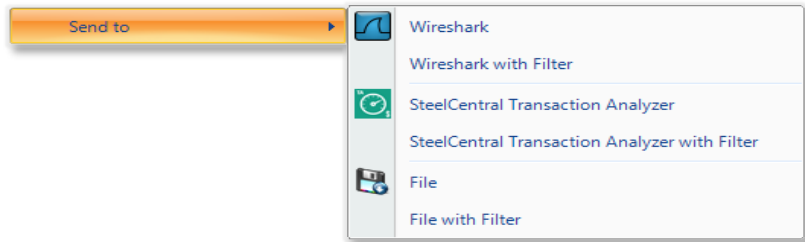
Files Panel (Trace File Selected on Local System)

Create View

The *Create View* menu option opens the “View Editor” where you can build a custom view. The new view is saved to the Custom folder of the View Library. It can now be applied to other sources. See “View Editor” for details.

Send to

The *Send to* menu option lists destination and filter use choices for the selected trace file.



Wireshark

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

Wireshark with Filter

The *Wireshark with Filter* menu option instructs Packet Analyzer to start up Wireshark and send traffic that matches a user-defined filter from the selected file to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

SteelCentral Transaction Analyzer

The *SteelCentral Transaction Analyzer* menu option starts up SteelCentral Transaction Analyzer and sends all traffic from the selected trace file there.

SteelCentral Transaction Analyzer with Filter

The *SteelCentral Transaction Analyzer with Filter* menu option starts up SteelCentral Transaction Analyzer and instructs Packet Analyzer to send it traffic that matches a user-defined filter applied to the selected traffic. The filter is specified using the *Filter Dialog Box*. The *Filter Dialog* is explained in a later section.

File

The *File* menu option instructs Packet Analyzer to send all traffic from the selected trace file to a user-specified trace file.

File with Filter

The *File with Filter* menu option sends traffic from the selected trace file through a filter to a new trace file. 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.

Create Multi-Segment Source

When two or more files or traces are selected, the *Create Multi-Segment Source* option creates a multi-segment source file. For more information, please refer to “Multi-Segment and Merged Sources” at the end of this section.

Create Merged Source

When two or more files or traces are selected, the *Create Merged Source* option creates a merged source file. For more information, please refer to “Multi-Segment and Merged Sources” at the end of this section.

Add Microflow Index

The *Add Microflow Index* option adds microflow index information to the selected file or trace. For more information, please refer to “Microflow Indexing.”

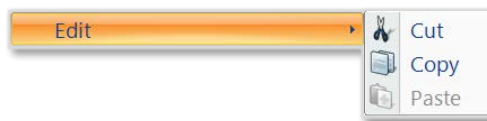
Calculate Checksum

The *Calculate Checksum* menu option calculates the SHA256 cryptographic digest of the selected trace file and presents it in a window. This value is stored and will be used later in tooltips and reports if applicable.

Browse Containing Folder

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

Edit



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.

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 copies a previously Cut or Copied file to the selected “paste” location.

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.

Delete from Disk

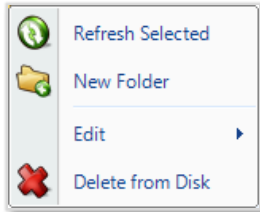
The *Delete from Disk* menu option removes the selected trace

file from disk. The trace file is not sent to the recycle bin.

Rename

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

With a Trace Folder Selected on a Remote NetShark



Files Panel (Trace Folder Selected on Remote NetShark)

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.

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.

Edit



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.

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

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

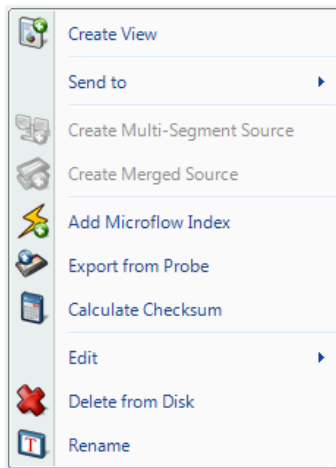
The *Paste* menu option will copy a previously Cut or Copied file to the selected “paste” location.

Delete from Disk

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

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

With a Trace File Selected on a Remote NetShark



Files Panel (Trace File Selected on Remote NetShark)

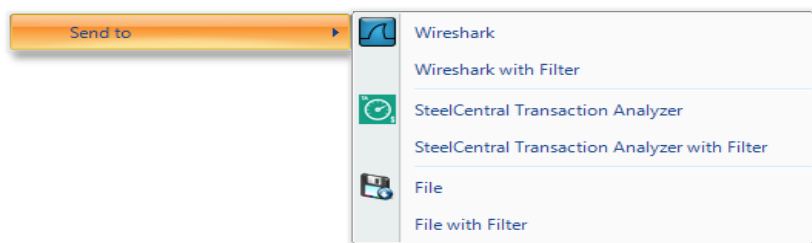
With a trace file selected, the options are as follows:

Create View

The *Create View* menu option opens the “View Editor” where you can build a custom view. The new view is saved to the Custom folder of the View Library. It can now be applied to other sources. See “View Editor” for details.

Send to

The *Send to* menu option lists destination and filter use choices for the selected trace file.



Wireshark

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

Wireshark with Filter

The *Wireshark with Filter* menu option instructs Packet Analyzer to start up Wireshark and send traffic that matches a user-defined filter from the selected file to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

SteelCentral Transaction Analyzer

The *SteelCentral Transaction Analyzer* menu option starts up SteelCentral Transaction Analyzer and sends all traffic from the selected trace file there.

SteelCentral Transaction Analyzer with Filter

The *SteelCentral Transaction Analyzer with Filter* menu option starts up SteelCentral Transaction Analyzer and instructs Packet Analyzer to send it traffic that matches a user-defined filter applied to the selected traffic. The filter is specified using the Filter Dialog Box.

File

The *File* menu option instructs Packet Analyzer to send all traffic from the selected trace file to a user-specified trace file.

File with Filter

The *File with Filter* menu option sends traffic from the

selected trace file through a filter to another trace file. This can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Create Multi-Segment Source

When two or more trace files are selected, this option creates a multi-segment source file. Please refer to “Multi-Segment and Merged Sources” at the end of this section.

Create Merged Source

When two or more trace files are selected, this option creates a merged source file. Please refer to “Multi-Segment and Merged Sources” at the end of this section.

Add Microflow Index

The *Add Microflow Index* option adds microflow index information to the selected file or trace. For more information, please refer to “Microflow Indexing.”

Export from Probe

The *Export from Probe* menu option transfers the selected files from the selected remote probe to the Local System.

Calculate Checksum

The *Calculate Checksum* menu option calculates the SHA256 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.

Edit



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.

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 copies a previously Cut or Copied file to the selected “paste” location.

Delete from Disk

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

Rename

The selected trace file can be renamed—in the panel and on disk—using the *Rename* menu option.

With the Jobs Repository Folder Selected on a Remote NetShark

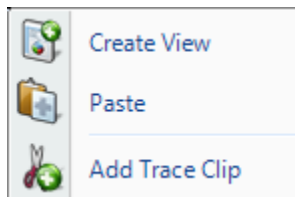


Jobs Repository Folder

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 NetShark



Job Trace

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

Create View

The Create View menu option opens the “View Editor” where you can build a custom view. The new view is saved to the Custom folder of the View Library. It can now be applied to other sources. See “View Editor” for details.

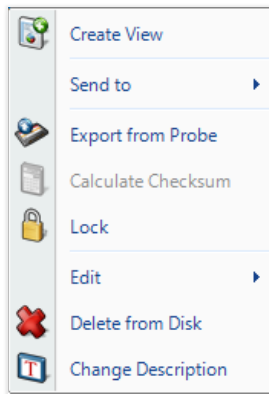
Paste

Paste a copied trace clip.

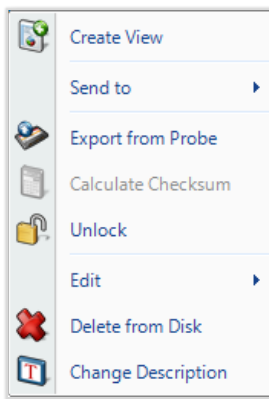
Add Trace Clip

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

With a Trace Clip Selected on a Remote NetShark



Trace Clip, Unlocked



Trace Clip, Locked

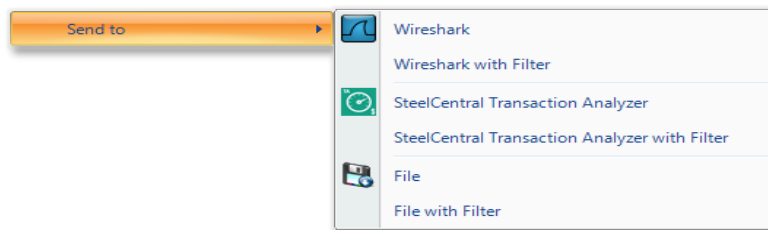
With a Trace Clip selected, the options are as follows:

Create View

The *Create View* menu option opens the “View Editor” where you can build a custom view. The new view is saved to the Custom folder of the View Library. It can now be applied to other sources. See “View Editor” for details.

Send to

The *Send to* menu option lists destination and filter use choices for the selected trace file.



Wireshark

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

Wireshark with Filter

The *Wireshark with Filter* menu option instructs Packet Analyzer to start up Wireshark and send traffic that matches a user-defined filter from the selected file to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

SteelCentral Transaction Analyzer

The *SteelCentral Transaction Analyzer* menu option starts up SteelCentral Transaction Analyzer and sends all traffic from the selected trace file there.

SteelCentral Transaction Analyzer with Filter

The *SteelCentral Transaction Analyzer with Filter* menu option starts up SteelCentral Transaction Analyzer and instructs Packet Analyzer to send it traffic that matches a user-defined filter applied to the selected traffic. The filter is specified using the *Filter Dialog Box*. It is explained in a later section.

File

The *File* menu option instructs Packet Analyzer to send all traffic from the selected trace file to a user-specified trace file.

File with Filter

The *File with Filter* menu option instructs Packet

Analyzer to send traffic that matches a user-defined filter from the selected trace file to a user-specified trace file. The filter is specified using the *Filter Dialog Box*. It is explained in a later section.

Export from Probe

The *Export from Probe* menu option transfers the selected files from the selected remote probe to the Local System.

Calculate Checksum

The *Calculate Checksum* menu option is not applicable to trace clips.

Lock, Unlock

By selecting the *Lock* menu option, the remote NetShark will lock the clip on disk, ensuring that the packet data is retained even as more traffic arrives on the system. The *Unlock* option unlocks a locked trace clip.

Edit



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.

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 copies a previously Cut or Copied file to the selected “paste” location.

Delete from Disk

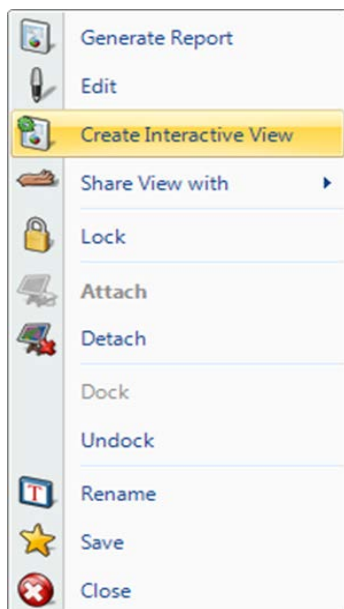
The *Delete from Disk* menu option removes the selected trace clip. The trace clip cannot be deleted if one or more Views are currently applied to the trace clip.

Change Description

The selected, unlocked trace file’s description can be revised using the *Change Description* menu option.

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, with one additional option, Create Interactive View, explained below. Please refer to “With a View Selected (Local System and NetShark)” in the Device Panel section for information on the other context menu options.



Create Interactive View

The Create Interactive View menu option creates an interactive view from a series of drill downs made on a view. Right-click the last view in a drill down chain and select this menu option. An interactive view is created and selections made in the first view now automatically update the other views in the drill down chain.

Multi-Segment and Merged Sources

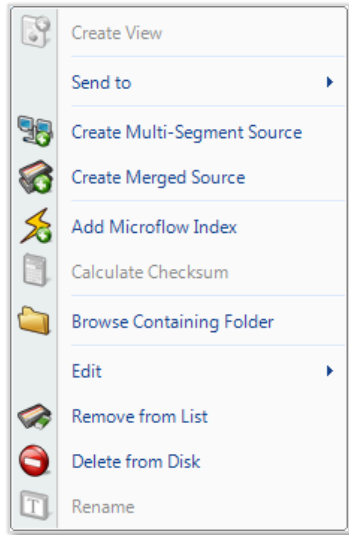
If you have selected multiple capture files or trace clips, you can combine them to form multi-segment or merged sources.

Multi-segment sources generally include information in the same time span from capture points in different locations. A typical use for a multi-segment source is to follow packets through a network.

Merged sources generally include information from the same capture point at different points in time. A typical use for a merged source is to combine sequential capture sessions to make a single session.

Note: *All of the capture files or trace clips used to make a multi-segment or merged source must be located on a single NetShark or on the local system.*

The paragraphs below tell how to create multi-segment and merged sources. For a fuller description of using multi-segment sources, refer to the section on “Multi-Segment Analysis (MSA).”



File context menu when two or more sources are selected

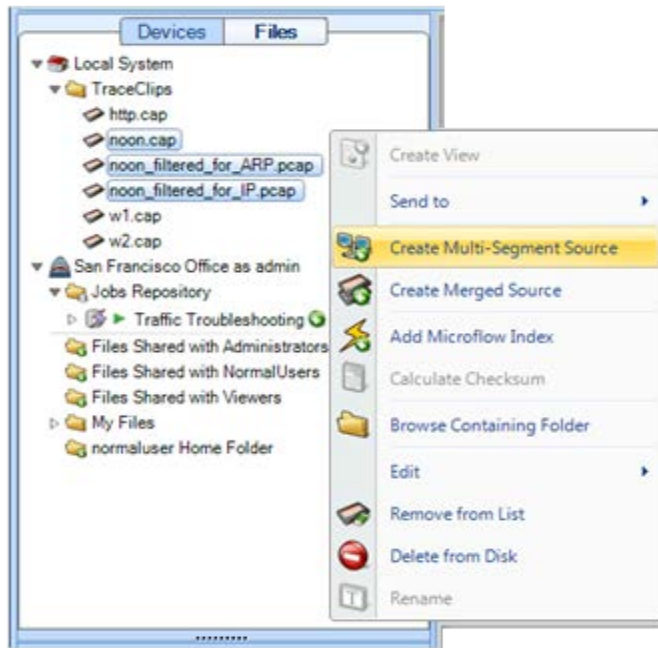
Context Menus

With a *single source* selected, right-clicking the source displays the context menu shown in the preceding pages. (See “With a Trace File Selected on Local System” or “With a Trace File Selected on a Remote NetShark Appliance.”)

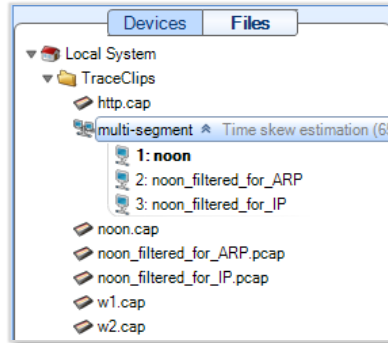
When you select *two or more* Trace Files or Trace Clips, two more context menu items become active in addition to the ones described previously:

Create Multi-Segment Source

This option creates a multi-segment source from the selected sources. The sources must be capture files or trace clips, not devices. And the files/clips must all be stored on the same NetShark or on the Packet Analyzer console.



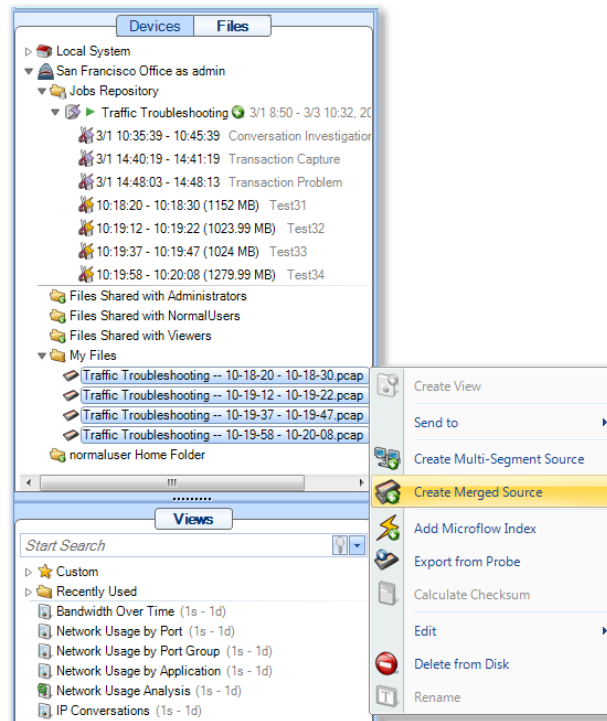
The resulting multi-segment source is listed in the Files panel. One of the segments is designated as the primary segment and shown in bold type. The primary segment is generally used when a single-segment view is applied to the multi-segment source.



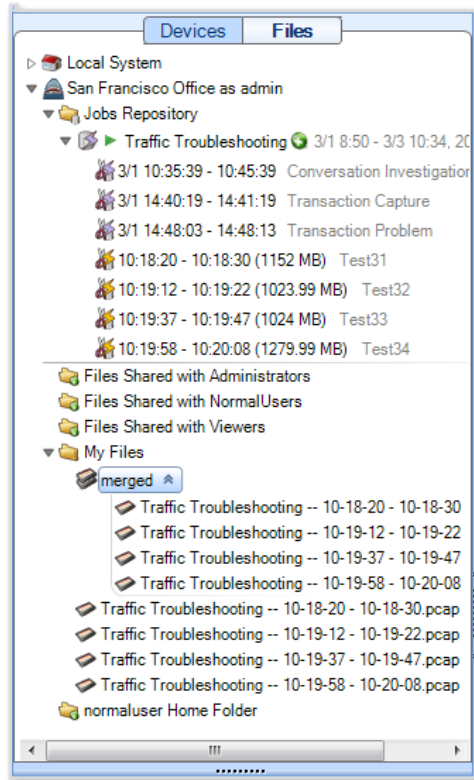
Create Merged Source

This option creates a single merged source from the selected sources. The sources must be capture files or trace clips, not devices. And the files/clips must all be stored on the same NetShark or on the local system.

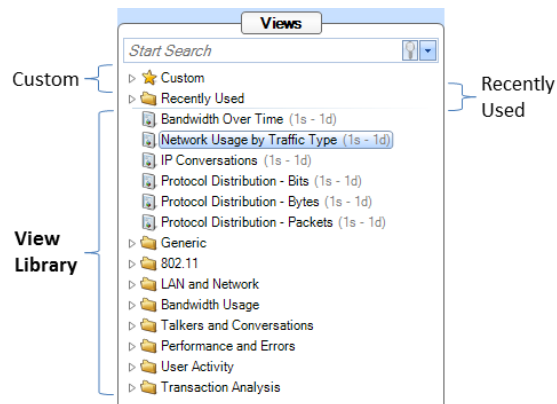
Note: Trace clips must first be Sent to File (see context menu) before merging.



The resulting merged source is listed as “merged” in the Files menu.



Views Panel



Views Library

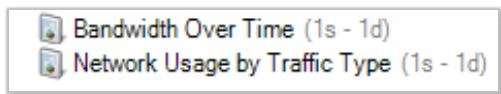


Figure 39 Instance of a View

A Packet Analyzer 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. 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 an example, see Figure in the left column.

The Icon denotes the link type(s) of the source to which the View applies, which in this case is:

 all link types

Other possible icons for the link type include:

 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.

These parameters can be changed, and multiple instances of a view can exist with different parameters by utilizing the custom views feature, as explained below.

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

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

Using Views

Views can be 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, as they are not applicable in certain contexts. For instance, a wired Ethernet device does not 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

Same as the double click previously described.

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

A view can be dragged on to any device or file, which opens the view on that source, similar to the above.

Additionally, after performing a selection within a chart, a view can be dragged on to the selection, and 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 40: Apply Icon

- Figure 40 means the view metric can be applied to the source



Figure 41: Do Not Apply Icon

- Figure 41 means that the view metric cannot be applied to the source.

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

Every chart has a “Drill Down” context menu option that lists the Custom, Recently Used, and View Library. This option is enabled when a selection is made in the chart, and selecting one of the views results in the view being applied to the subset of data selected. The drill-down menu button works identically.

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 the live Interfaces only.

Applying a View with a Filter

It is possible to enable a filter when applying a view to limit the view to a subset of the original data. When holding down the control key and applying a view either by pressing enter, or dragging and dropping, a filter dialog box opens, enabling a filter to be specified. The Filter Dialog is explained further below.

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 intrinsically 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 42: Apply Icon



Figure 43: Do Not Apply Icon

- Figure 42 means the view metric can be applied with filter to the source
- Figure 43 means that the view metric cannot be applied to the source.

Applying Views in Multi-Segment Contexts

Multi-segment views are contained in the Multi-Segment folder of the View Library. When a multi-segment view is applied to a multi-segment source, all the linked sources are used to compute the multi-segment metrics. Multi-segment views may not be applied to normal sources (single capture files and trace clips).

Normal views—those that are not specifically multi-segment views—are not intended to be applied to multi-segment sources. If a normal view is applied to a multi-segment source, the primary source (marked in bold type in the source list) is processed.

If a Send to File/Wireshark action is requested on a multi-segment source, a dialog box appears and allows you to select which capture points to send to File/Wireshark.

Using Views with Application Metrics

Application metrics can be added to a capture job by enabling Indexing and DPI when the capture job is added on a NetShark. DPI, using LL7 Fingerprints, and System Applications, along with Layer

4 Mappings, identifies and tags applications in the captured traffic. Two new views have been added to visualize and analyze this information:

- Network Usage by Application View
 - View is supported on remote (NetShark) live interfaces and offline sources (trace files and trace clips).
 - Traffic that is not TCP or UDP, is shown using the Layer 3 or Layer 4 protocol name.
 - When multiple tags apply, tags are concatenated and separated by a space, for example, HTTP Facebook.
 - Drill-down from this view is not supported.
- Network Usage Analysis View
 - A comprehensive, interactive view to analyze traffic based on
 - Applications
 - Port groups
 - Port names
 - Supported on remote (NetShark) offline sources (trace files and trace clips), as are all interactive views.
 - Begin by selecting an application of interest (Chart 1), then select an IP conversation (Chart 2). Chart 3 lists TCP Connections or UPD Flows.
 - Drill-down supported from the last chart only (Chart 3).

Packet Analyzer does not support DPI, so these two views cannot be used on local sources (online or offline). Port names, port groups, Layer 4 Mappings and L7 Fingerprints can be copied from a NetShark, for use on local sources. See “With a NetShark Selected” in “Context Menus in the Devices Panel” for details.

View Library

The *View Library* is the main repository of all the views available in Packet Analyzer.

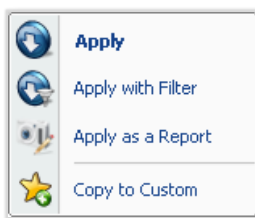
Views are divided into folders that are, in some cases, further subdivided.

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



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.

View Library Folder

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.

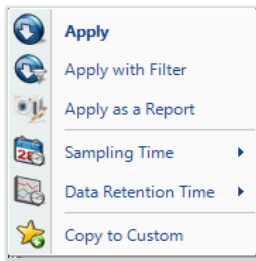
Apply as a Report

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



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.

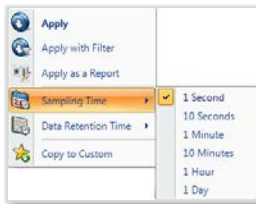
Sampling Time

The *Sampling Time* menu option specifies the time granularity of the calculation for the corresponding View metric. The view calculations and time control options are performed with a specific time sampling interval, which typically defaults to one second. This context menu enables changing this interval, and the selected value is shown at the end of the textual representation of the view in the Views Library (along with the Data Retention Time value, described next).

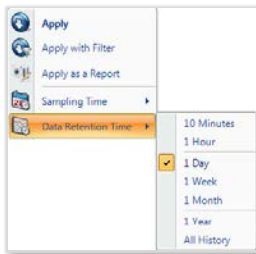
Data Retention Time

The *Data Retention Time* value specifies the time period for the View metric history that is retained for a View applied to a live source. Once the Data Retention Time is reached, the oldest 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, since the complete View metric

View Library View



Sampling Time



Data Retention Time

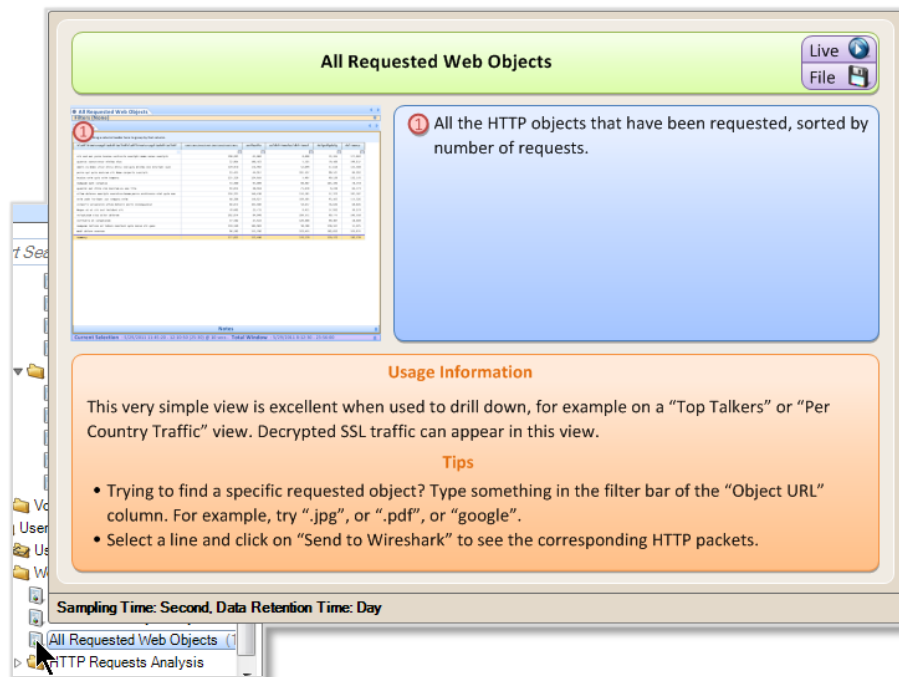
history over the duration of the trace file is retained.

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 are enabled for each of the views and display a summary of the calculated view metrics and the various charts that comprise the view. A tooltip also may include usage information and tips. Tooltips are made visible by hovering over the icon for a view or folder (see screen shot below). For example, here is the tooltip for the All Requested Web Objects view.



Recently Used

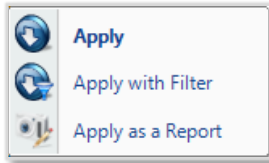
The Recently Used folder contains the five most recently used views. The Recently Used folder is not shown when the folder is empty, as is the case when Packet Analyzer is started.

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



Recently Used Folder Context Menu

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.

Recently Used View

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

Custom Views

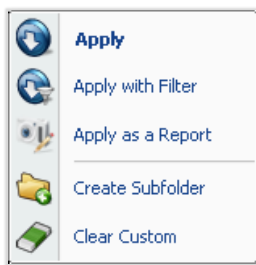
Custom Views are the views in the views library that have been saved with different settings. At the view level, the chart window positions and sizes are saved. At the chart level it varies. In the description of the charts it is noted whether the option is saved or not in a custom view.

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



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.

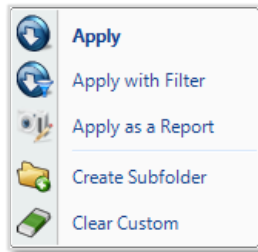
Create Subfolder

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



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.

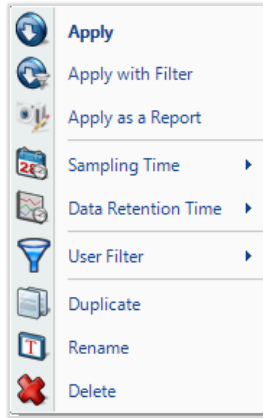
Create Subfolder

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

Clear Custom

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

View within Custom Folder (or Sub Folder)



Custom View

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

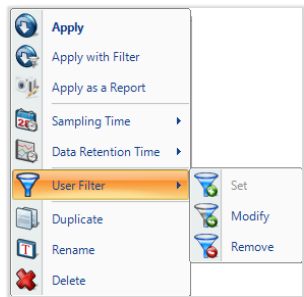
As described above, this context menu option enables modification of the underlying sampling time used in the view calculations.

Data Retention Time

As described above, this context menu option enables modification of the duration that data is retained for a live view.

User Filter

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



User Filter

Duplicate

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

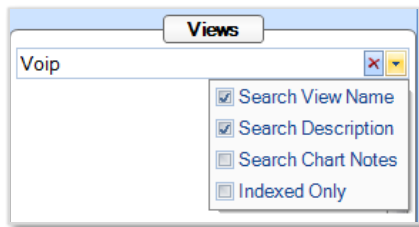
Rename

The *Rename* menu option allows the view to be renamed.

Delete

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

Search Text Box



View Panel Search

The Search Box is used to locate Views for specific purposes. For example, if VoIP is entered, the 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.

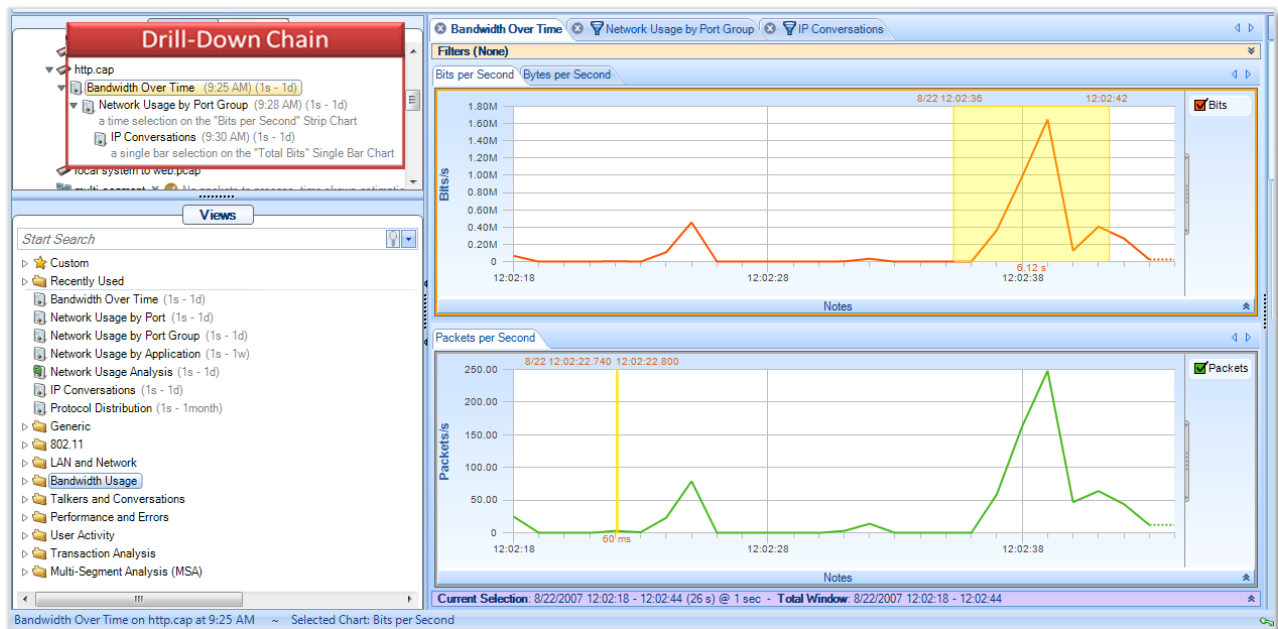
The Search box is a convenient way to find the View that you are looking for. In a sense, it provides an alternative way of organizing the View Library.

This page intentionally left blank

Interactive Views

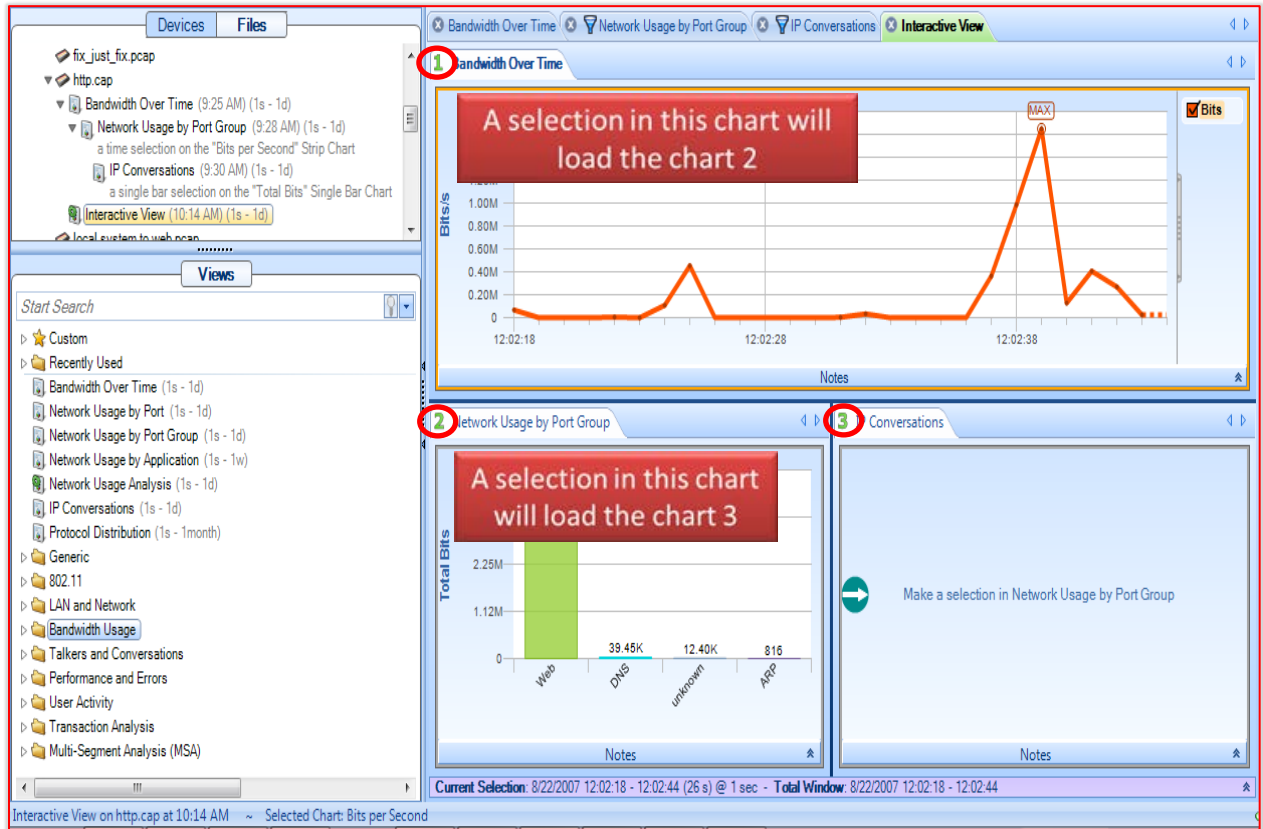
As discussed previously, one of the most powerful features of Packet Analyzer is Drill Down, which enables a user to select a subset of the data in one view and apply a second view for an alternative metric or more details about the selected data, and perhaps a third or fourth view for additional details. This chain can then be converted into an Interactive View, which means that as the user changes selections in the first view(s), the subsequent views are automatically updated.

In the following example, a Bandwidth Over Time view is applied to the trace file http.cap, a time selection in the strip chart is used to drill-down using the Network Usage by Port Group view, and finally, the Web bar is selected to drill-down with the IP Conversations view.



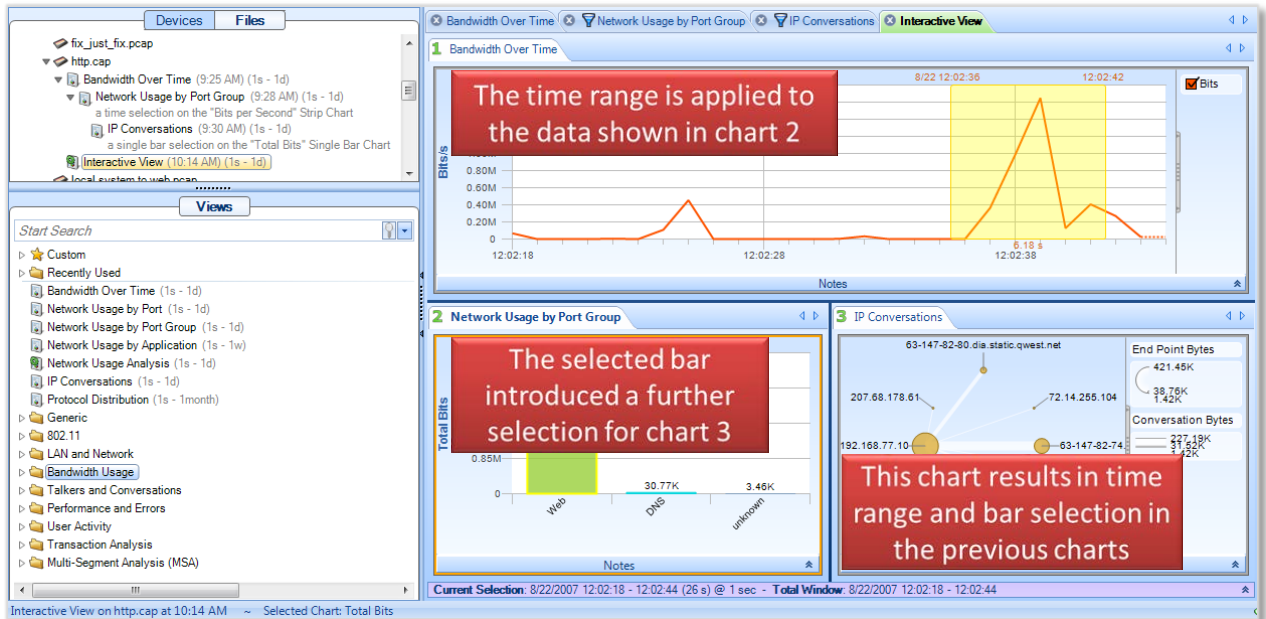
Drill-down chain

To create an Interactive View, right-click the last drill-down view in the chain (*IP Conversations* in this example) and choose *Create Interactive View*. A new Interactive View is generated with the selected charts from the views in the drill-down chain.



Steps for drilling down

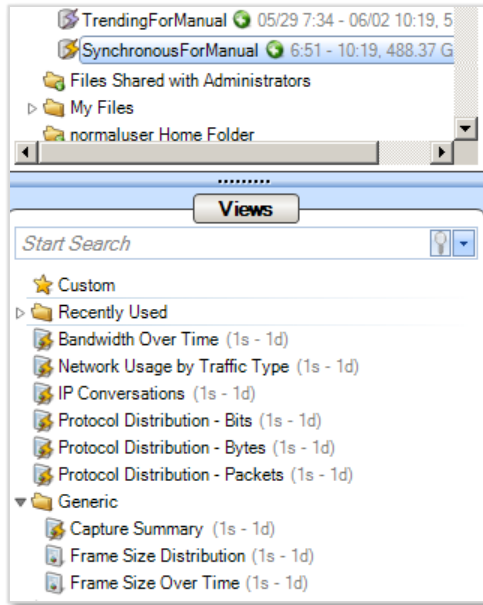
The numbers in the chart titles, arrows and instructions illustrate how to enable each chart. Once a time range has been selected in the Bandwidth Over Time chart, the selection result is applied to the Network Usage by Port Group chart for the time range selected in the first chart. A further selection in the Network Usage by Port Group chart shows the IP conversations ring, constrained to the time selection in the first chart and the port group selected in the second chart.



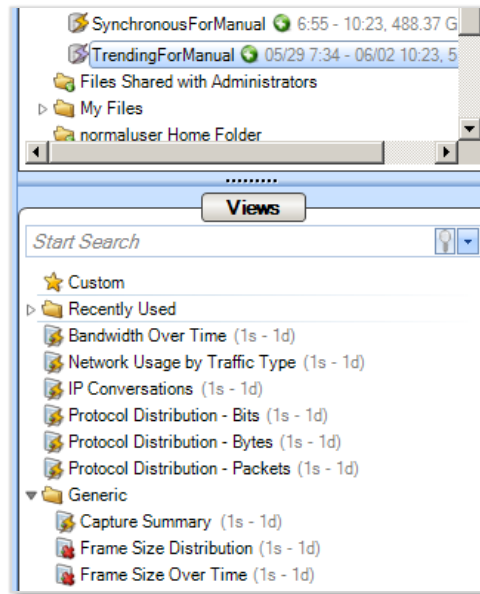
Drill-down example

Regular Views, Fast Views, and Forbidden Views

When some Views are applied to Sources that have associated Microflow Indexing Data, they can make use of the index to run very quickly, even on large data sets. 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 Microflow Indexing data alone. The ordinary views are those that cannot be run with the Microflow Indexing data alone, but the actual packets are available for the View calculation.



Fast Views



Disallowed Views

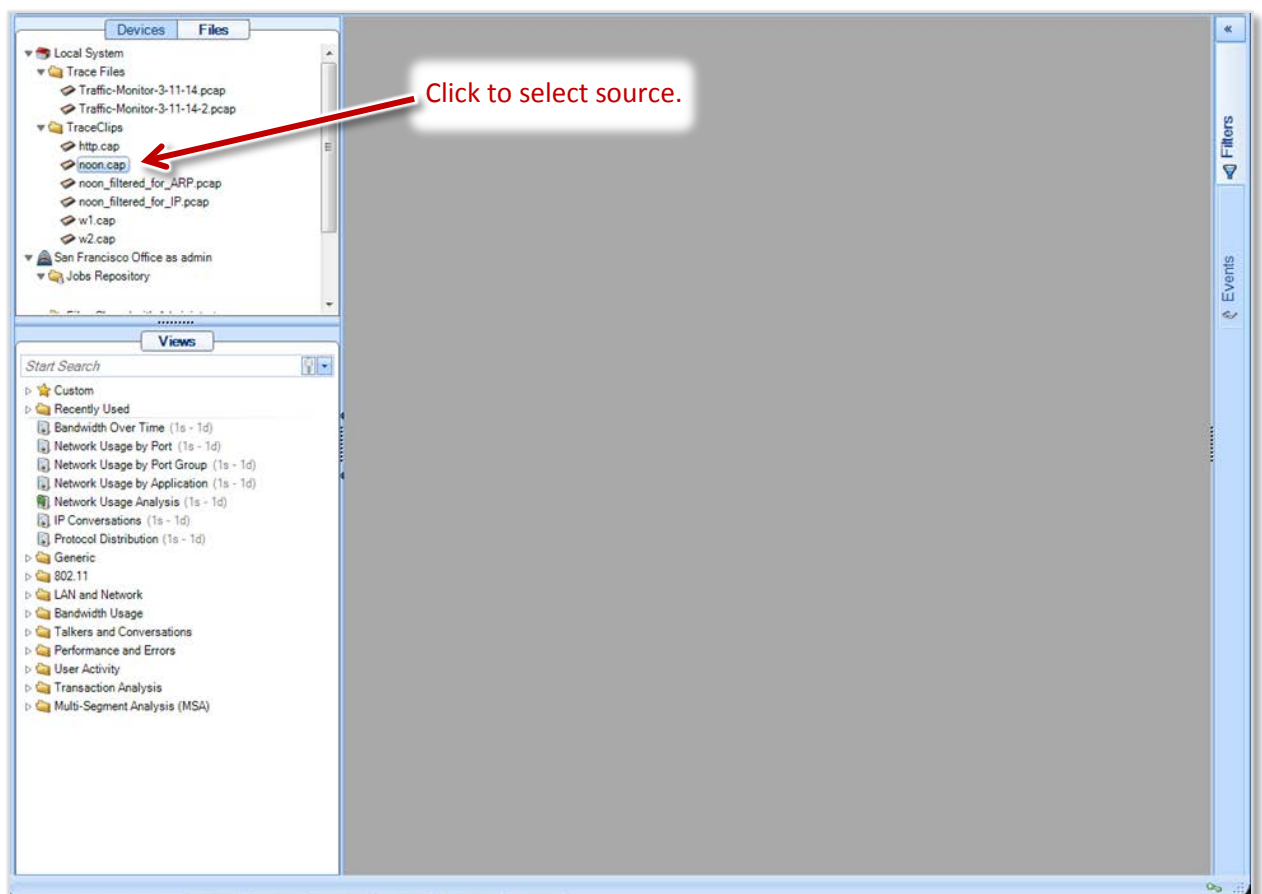
View Editor

In addition to applying standard views from the View Library, you can use the View Editor to edit an existing view or to create your own view. When you have the view you want, you can use it as you would any other view—drill down, create reports, and so on. In addition, you can save the view and apply it to other sources in the same way as any of the standard views.

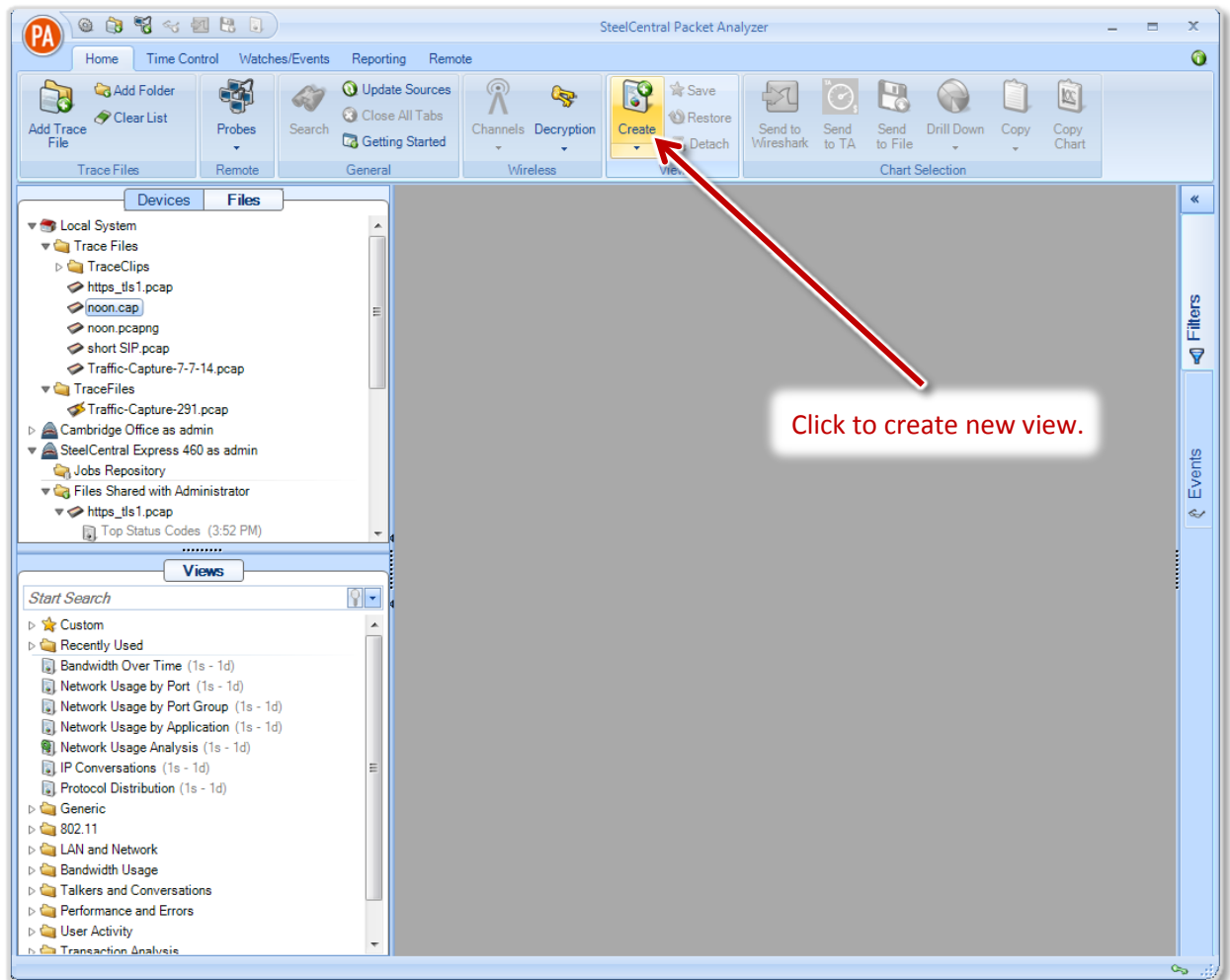
The General Approach

A quick example will give a general idea of how the View Editor works. This example shows how to create a view of IP protocol activity over time.

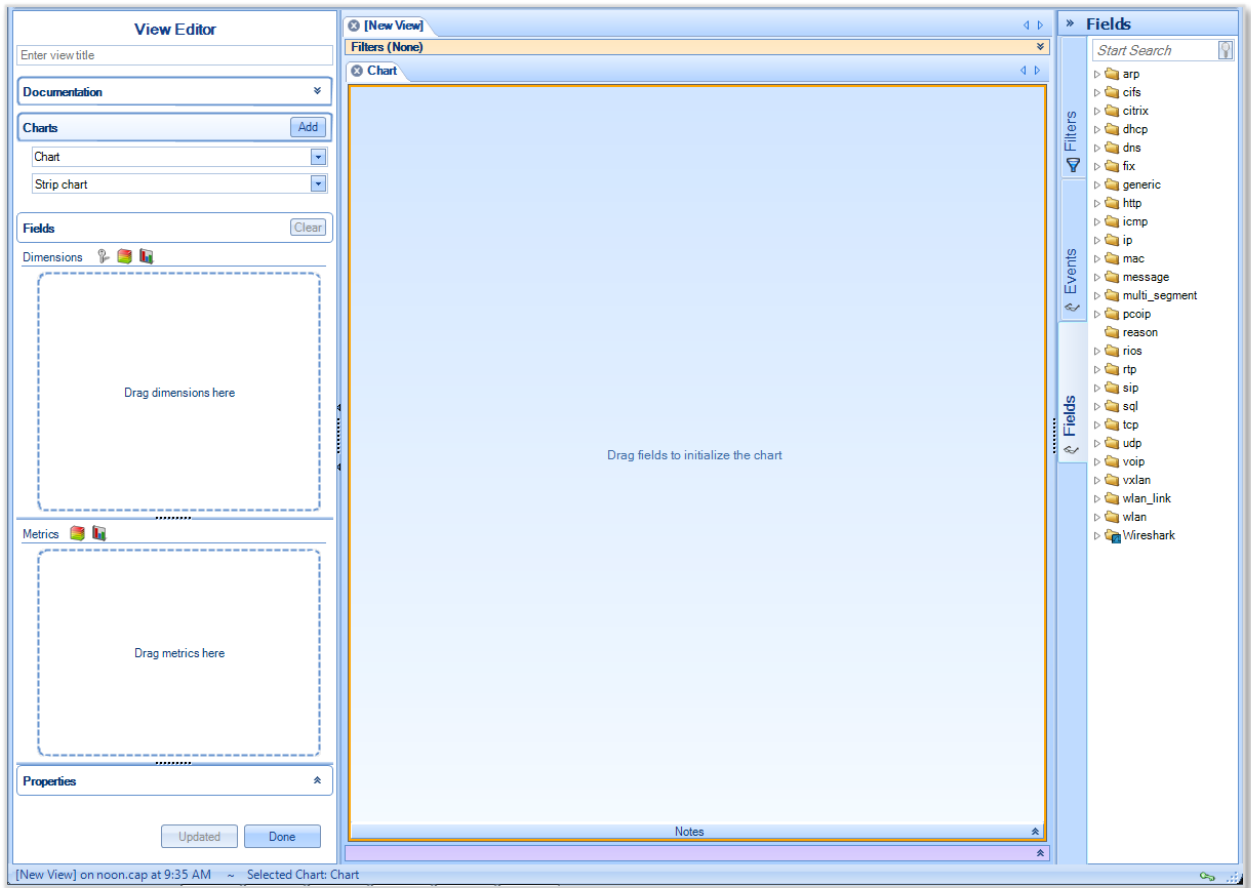
1. Select a source from the Files panel.



2. Create a new view by clicking View > Create in the Home Ribbon.



The View Editor appears.

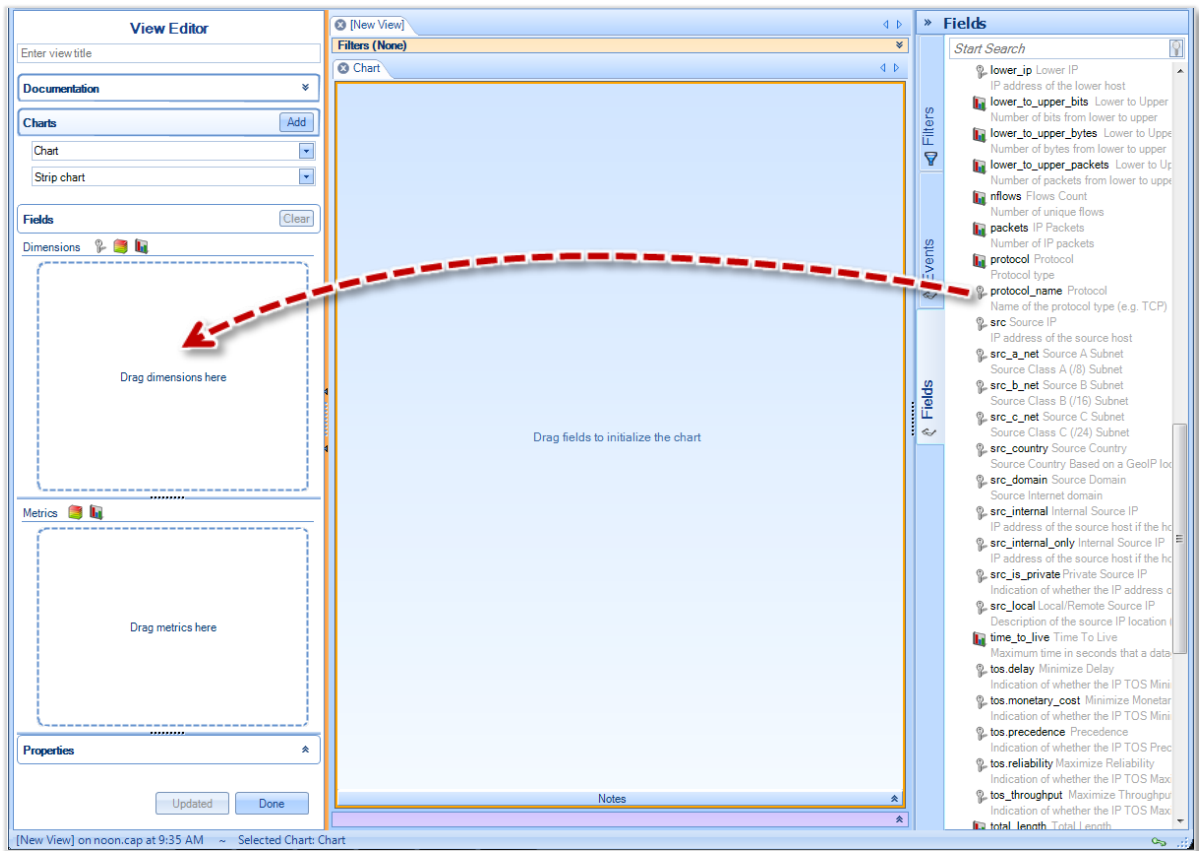


View Editor

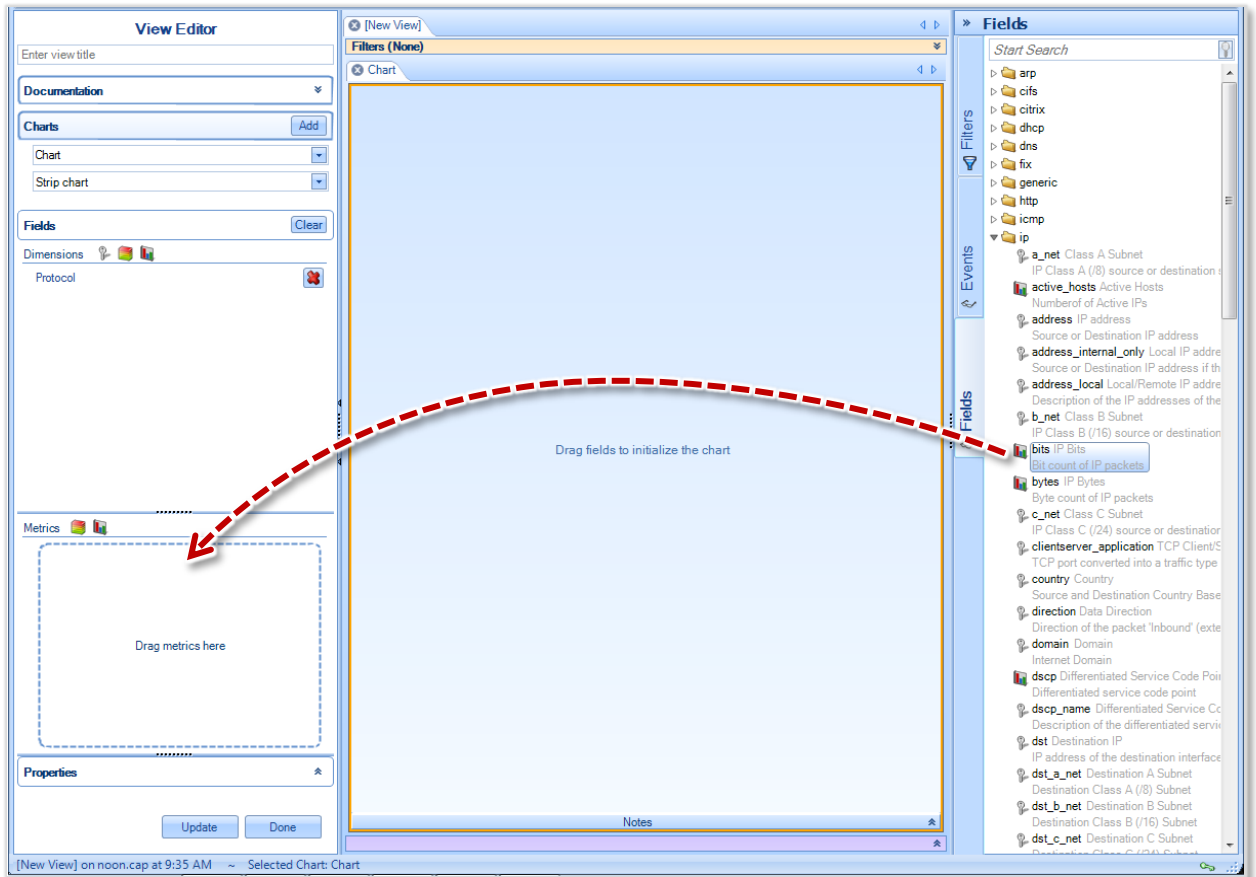
View

Fields

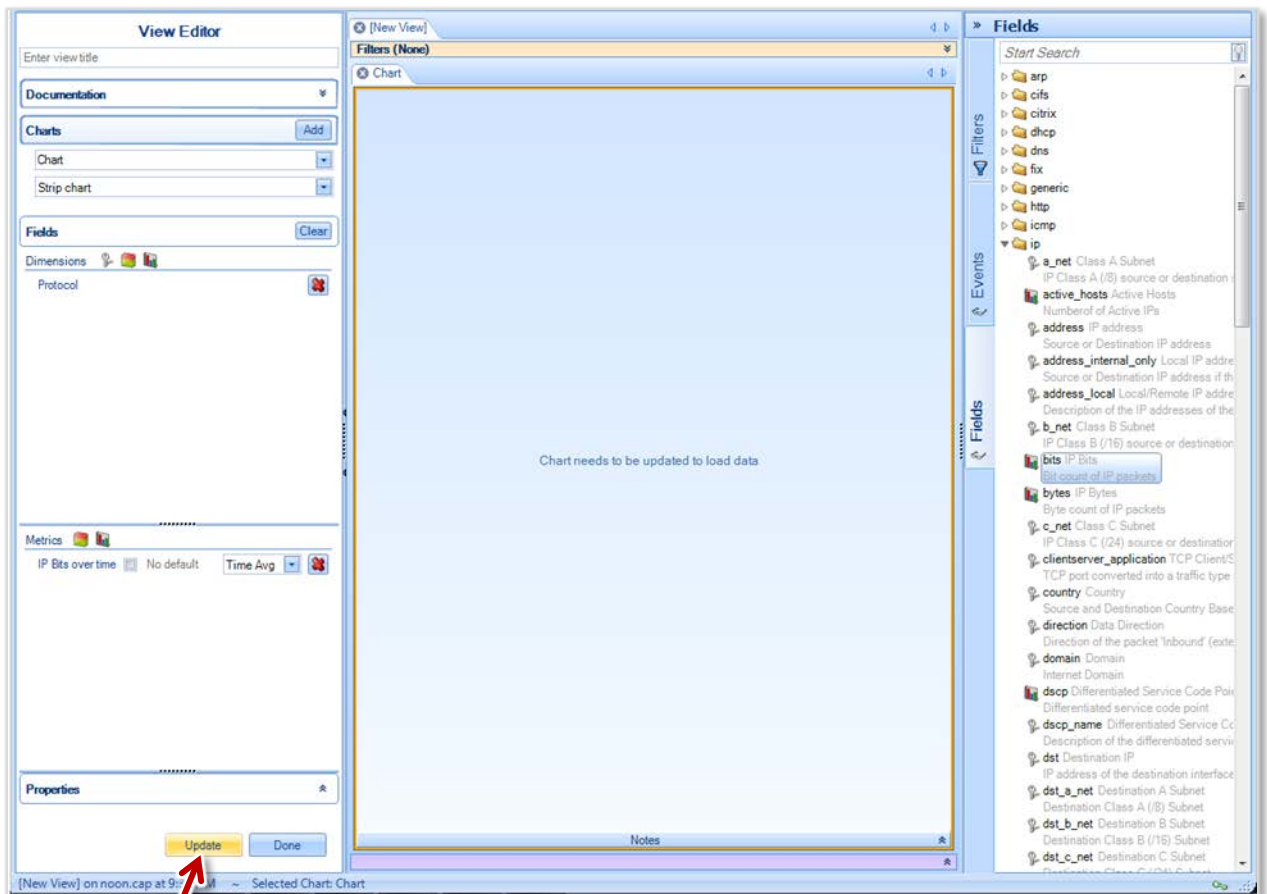
3. Drag a field to the Dimensions panel. For this example, the field is `protocol_name`. Open the `Fields` folder in the Fields panel, scroll down to find the `protocol_name` field, and drag the field to the Dimensions panel.



4. Drag a field to the Metrics panel. For this example, the field is **bits**. Open the **IP** folder in the Fields panel, scroll down to find the **bits** field, and drag the field to the Metrics panel.



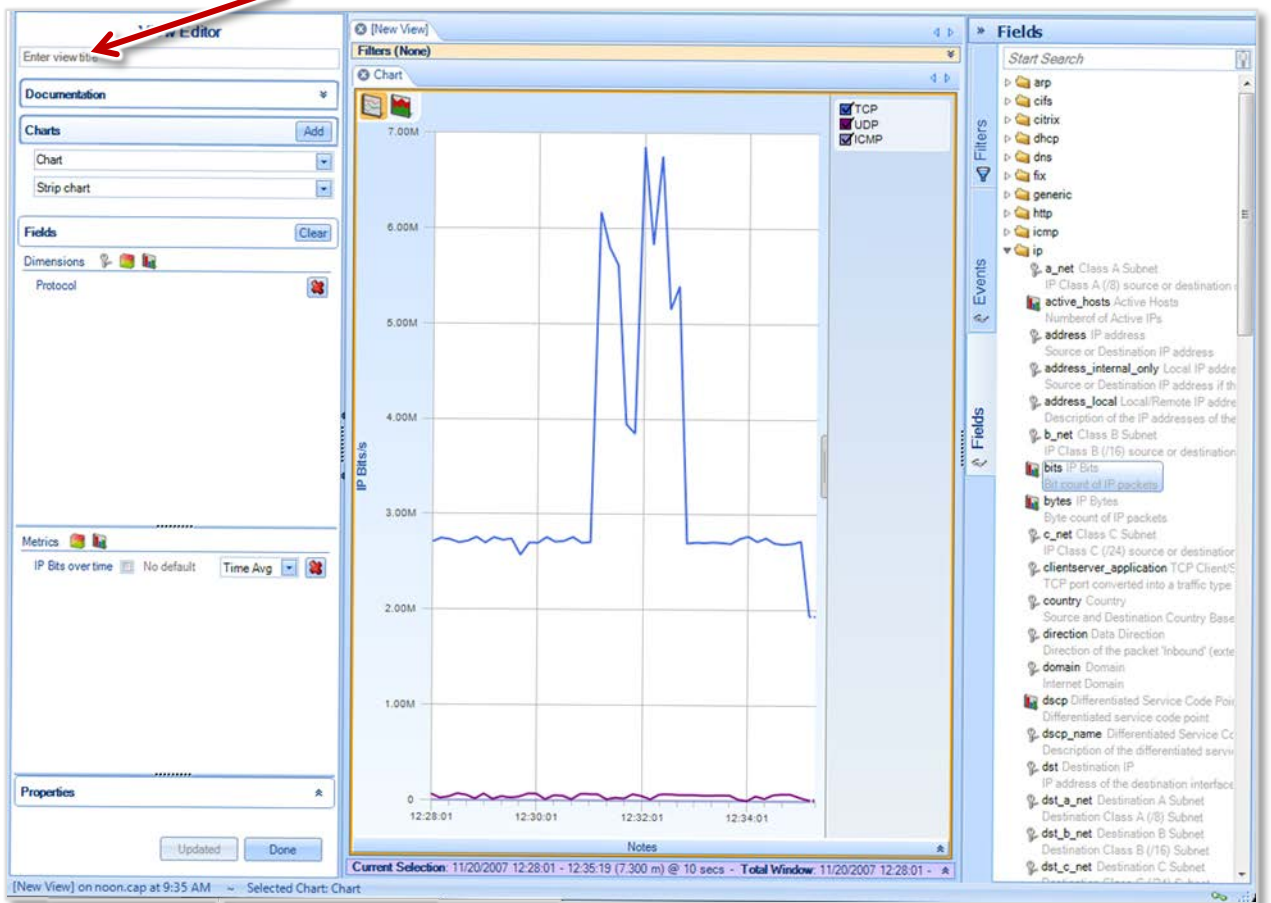
5. Click Update to display the view.



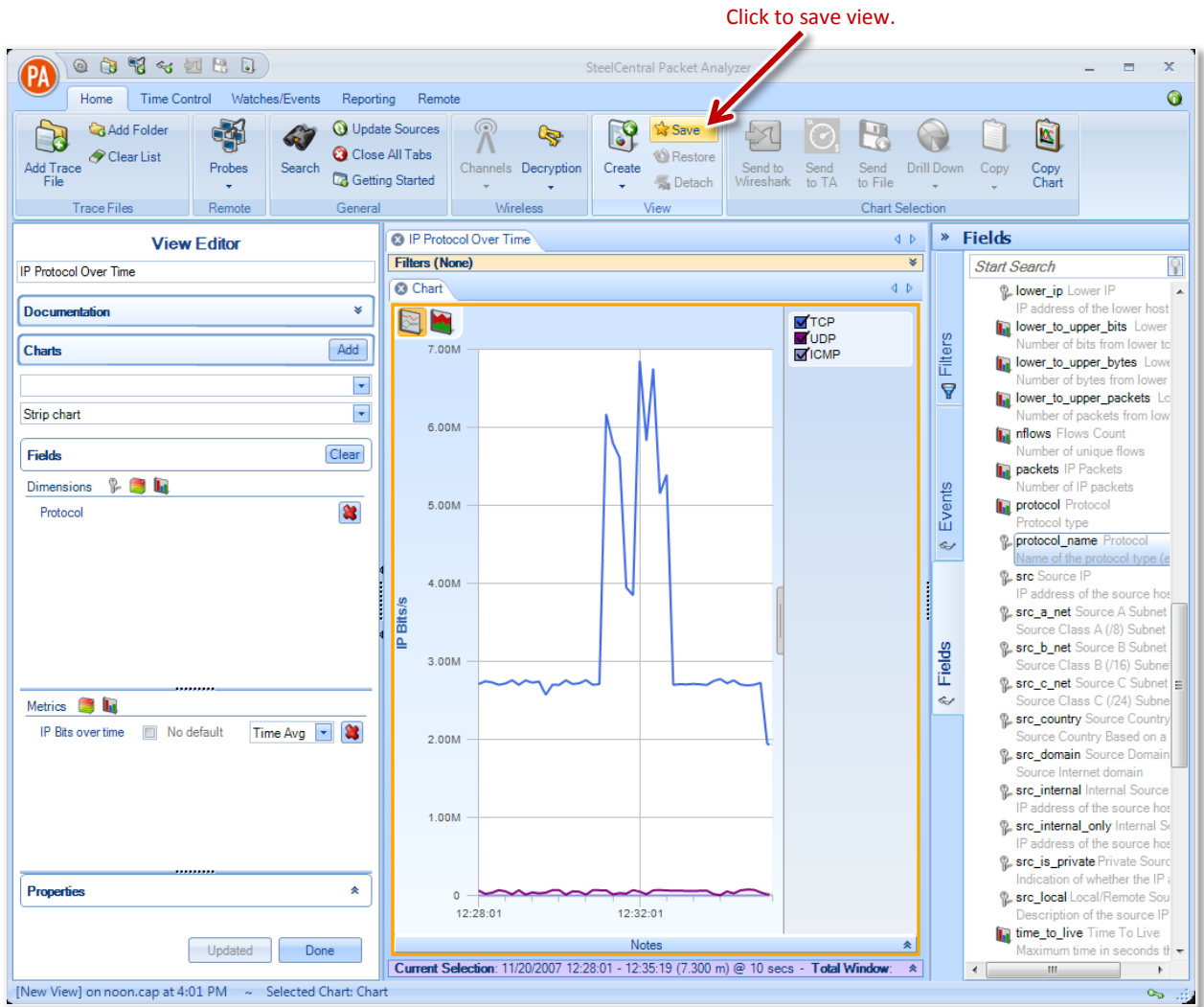
Click to display view.

6. Give the view a name.

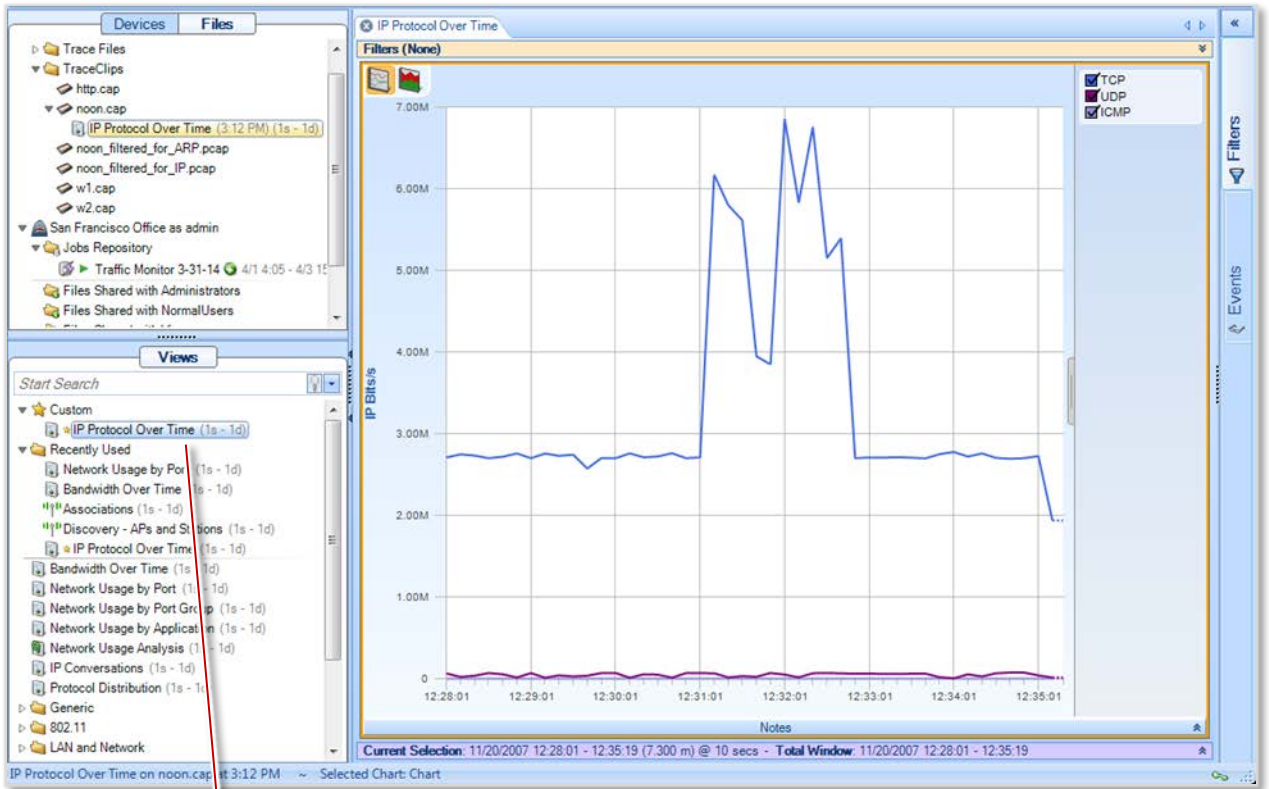
Name the view.



7. Save the view by clicking View > Save in the Home Ribbon.



The new view is saved to the Custom folder of the View Library. It can now be applied to other sources.



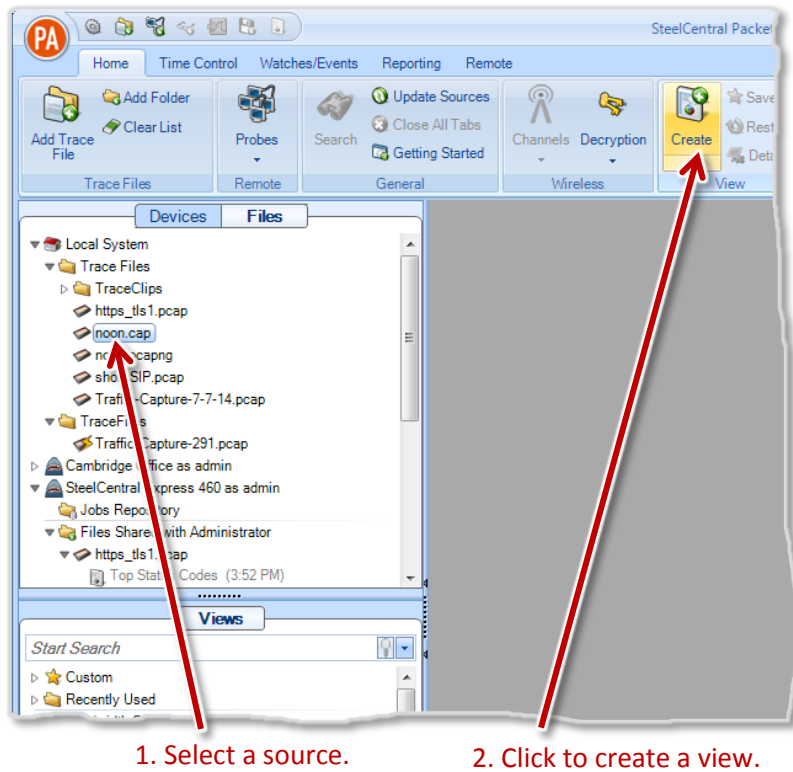
New view is ready to be applied.

A detailed explanation of the View Editor follows.

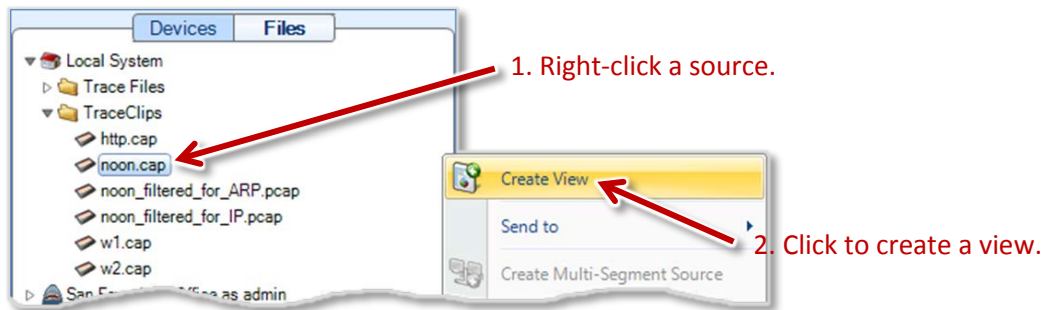
Activating the View Editor

You can activate the View Editor in any of the following ways:

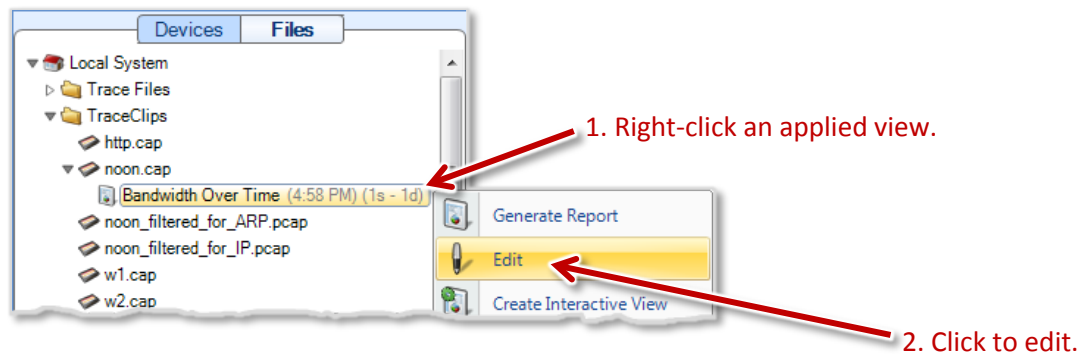
- Select a source from the Files panel, and then click the Create button in the View section of the Home Ribbon.



- Right-click a source in the Files panel and select Create View in the context menu.

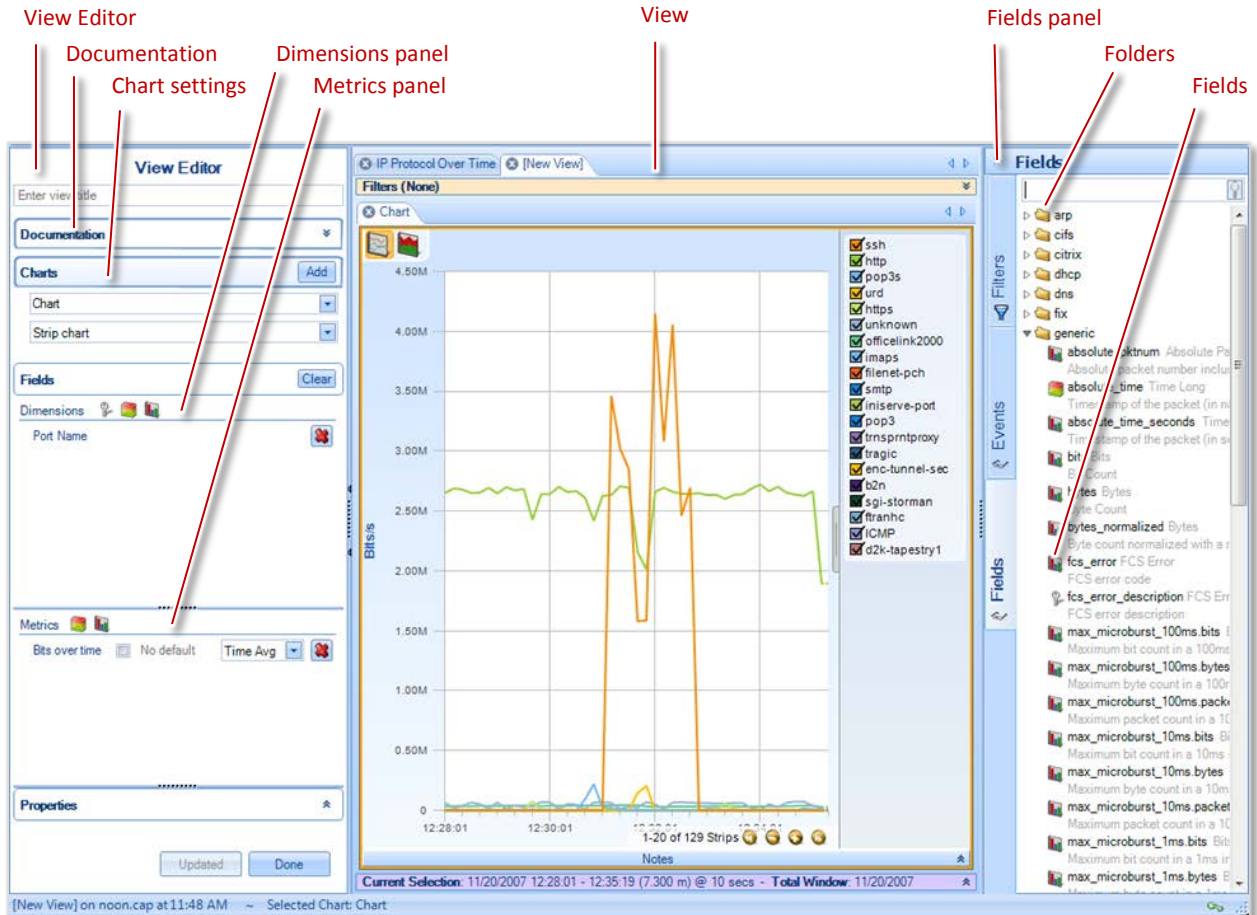


- Right-click a view that has been applied to a source in the Files panel and select Edit. The view may be a standard view that was supplied with the Packet Analyzer or a custom view that you created. Note that all charts in the view must be of a type supported by the View Editor (strip charts, conversation rings, bar charts, pie charts, or grids).



The View Editor Interface

The View Editor interface consists of a central View window, the View Editor panel on the left, and the Fields panel on the right. These are explained in detail below. To create a view you drag fields from the Fields panel to the Dimensions and Metrics panels in the View Editor, set other parameters as appropriate, and update the View window.

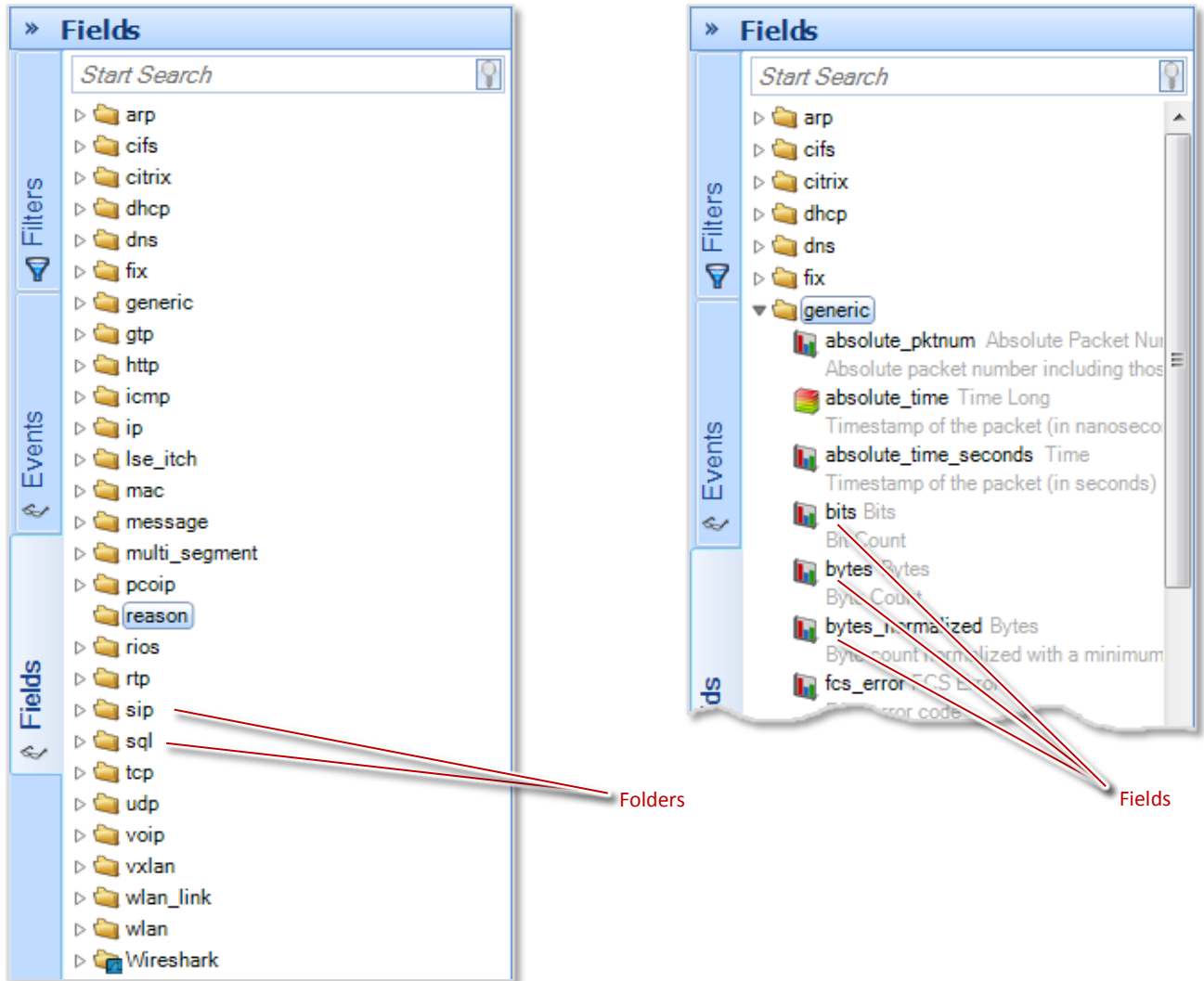


Fields

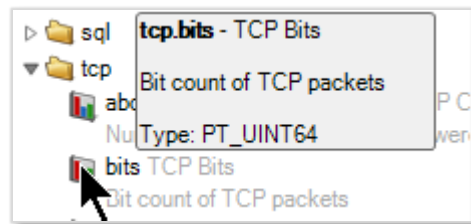
The Fields panel contains several folders, which generally group related fields according to protocol type or networking layer.

At the end of the list of folders is the Wireshark folder, which contains hundreds of sub-folders.

Each folder contains several fields. Each of these fields represents an entity that defines part of a view.



A field's type is displayed when you hover over the field's tooltip, as shown below.



Fields come in three types, represented by icons:



Categories: The key icon indicates that the field defines a category, and it will be used to define the “key” of the data set. For instance, in a bar chart there will be one bar per field value. Category fields can be used only as dimensions. (See description of dimensions, below.)



Qualitative values: The colored stack icon indicates that the field defines a qualitative value. Qualitative fields can be used for either dimensions or metrics (see descriptions below). Since the only meaningful operation you can apply to a qualitative value is sorting, you can specify either a **min** or **max** calculation when using it as a metric.

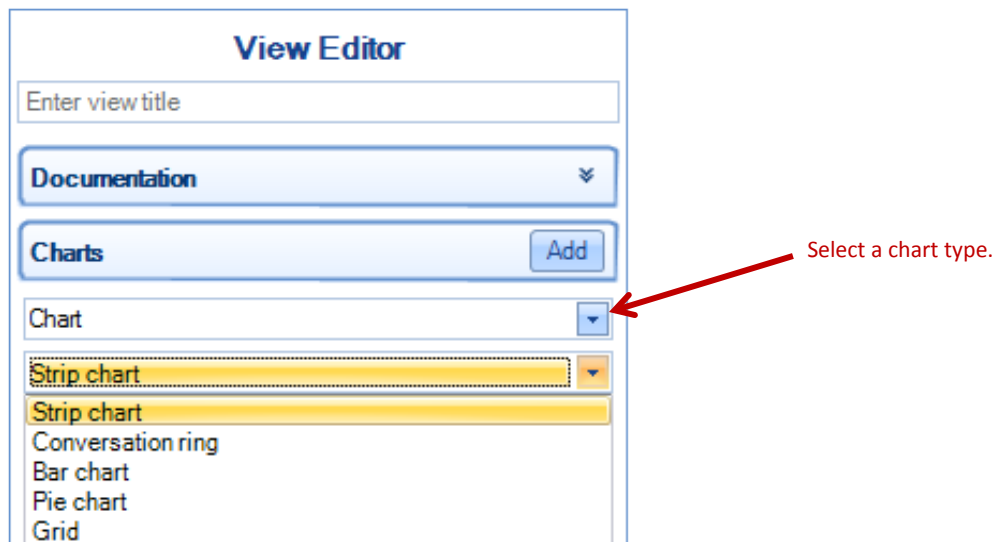


Quantitative values: The bar chart icon indicates that the field defines a quantitative value. Quantitative fields can be used for either dimensions or metrics (see descriptions below). When used as a metric, all calculations are available: **min**, **max**, **sum**, **average**, **time average**.

Chart Types

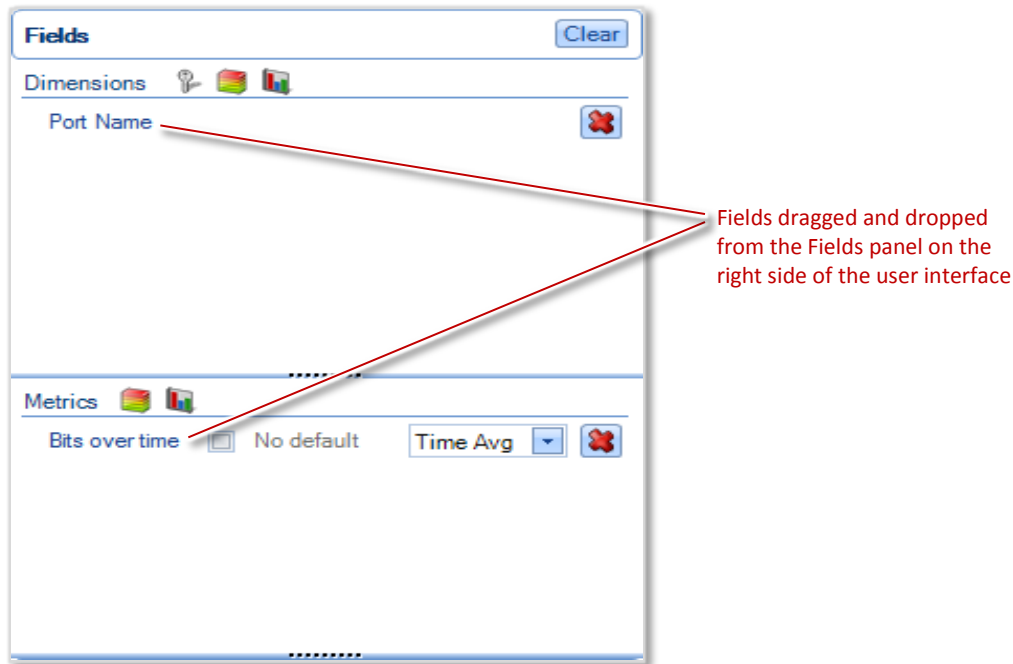
The Chart Types drop-down list in the View Editor lets you select from five types of chart:

- Strip chart
- Conversation ring
- Bar chart
- Pie chart
- Grid



Dimensions and Metrics

Entries in the Dimensions and Metrics panels determine what information is displayed in the chart. You make entries in these panels by dragging fields from the Fields panel.



A **dimension** is a field used to define categories in the data set. For example, a dimension could define:

- the lines or areas in a strip chart
- the source and destination in a conversation ring
- the bars in a bar chart
- the wedges in a pie chart
- the rows in a grid

Any of the different field types can be used as a dimension.

Note: A conversation ring requires two dimensions of the same type, for example, Source IP and Destination IP or Caller Name and Receiver Name.

A **metric** is a value calculated for each packet of the source. A metric can be of the qualitative value or quantitative value field types, but it cannot be of the category field type. You can set the calculation for a qualitative field to **min** or **max**; for a quantitative field you can use any of the calculations: **min**, **max**, **sum**, **average**, or **time average**. These calculations are used to aggregate values from all the packets of a single sample or a time range and to show the result in a chart.

In combination, the dimension and the metric(s) define the data used to populate the chart. Consider an example where you specify a strip chart to plot a dimension of traffic type and a metric of bits. Since a strip chart is a plot against time, the view performs a calculation for each unit of time. In this case the metric is bits with a calculation type of time average; and in each unit of time each packet is analyzed and the number of bits is assigned to the appropriate category. So bits in ARP packets are assigned to the ARP category; bits in DHCP packets are assigned to the DHCP category; and so on. For each unit of time the number of bits in each category is averaged. The view shows each category as a trace on the plot over time, and the result looks like this:

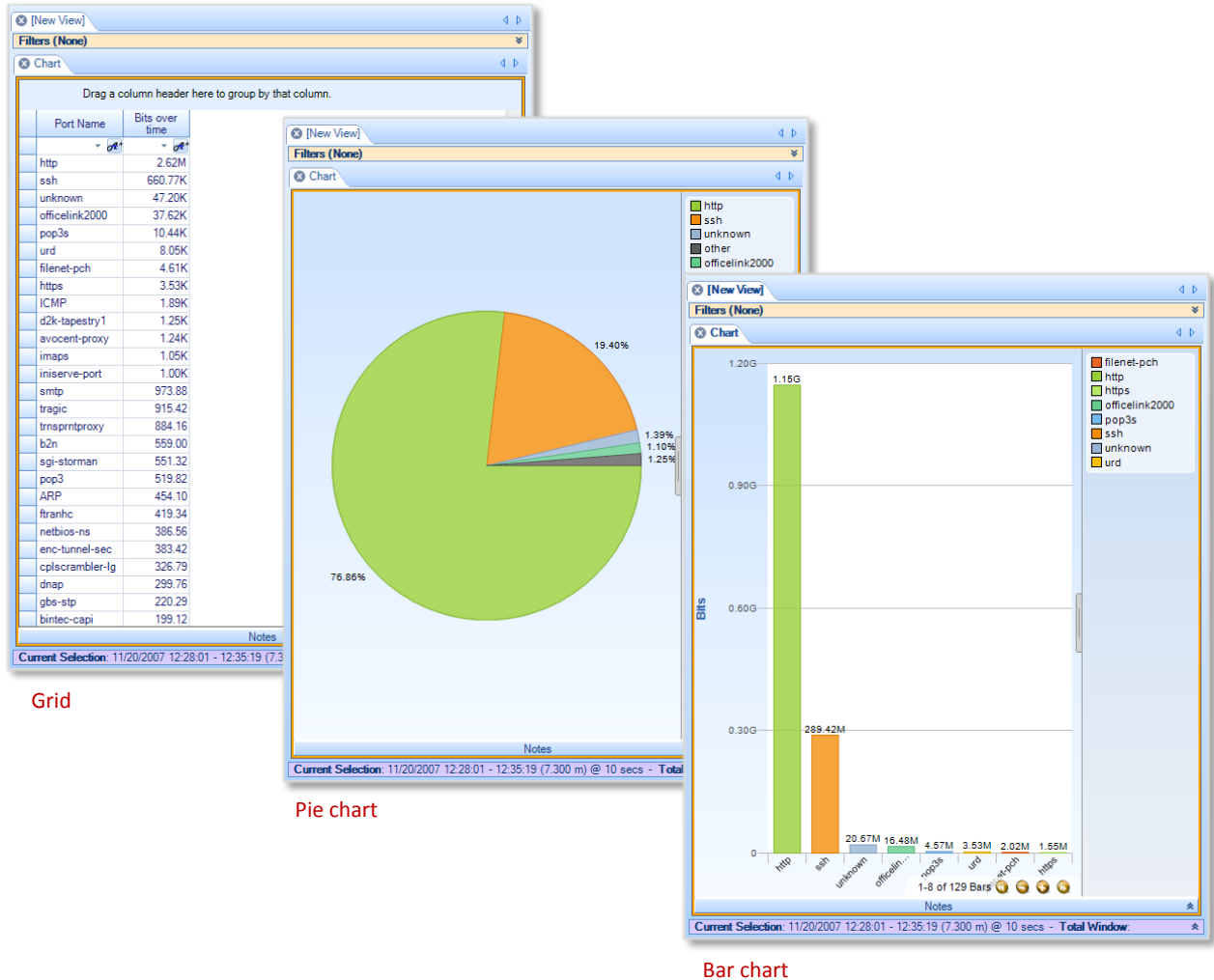
The screenshot shows the 'View Editor' on the left and the 'Chart' view on the right. Red lines point from labels to specific settings in the View Editor:

- Chart type:** Points to the 'Chart' dropdown menu, which is set to 'Strip chart'.
- Dimension field:** Points to the 'Dimensions' section, where 'Port Name' is selected.
- Metric field:** Points to the 'Metrics' section, where 'Bits over time' is selected.
- Calculation type:** Points to the 'Time Avg' dropdown menu in the Metrics section.

The Chart view shows a strip chart with a Y-axis labeled 'BITS/s' ranging from 0 to 4.5M. The X-axis shows time from 12:28:01 to 12:35:19. A legend on the right lists various traffic categories, including ssh, http, pop3s, urd, https, unknown, officelink2000, rmaps, filenet-pch, smtp, iniserve-port, pop3, trnsprntproxy, tragic, enc-tunnel-sec, b2n, sgi-storman, franhc, CMP, and d2k-tapestry1.

Strip chart

You can show the same fields using different chart types. Note that conversation rings, bar charts, pie charts, and grids do not have a time component, so they show the data for each category aggregated over the entire time span of the source (or the range specified by the Time Control). Also, a conversation ring requires two dimensions, so for this example that chart type cannot be used.

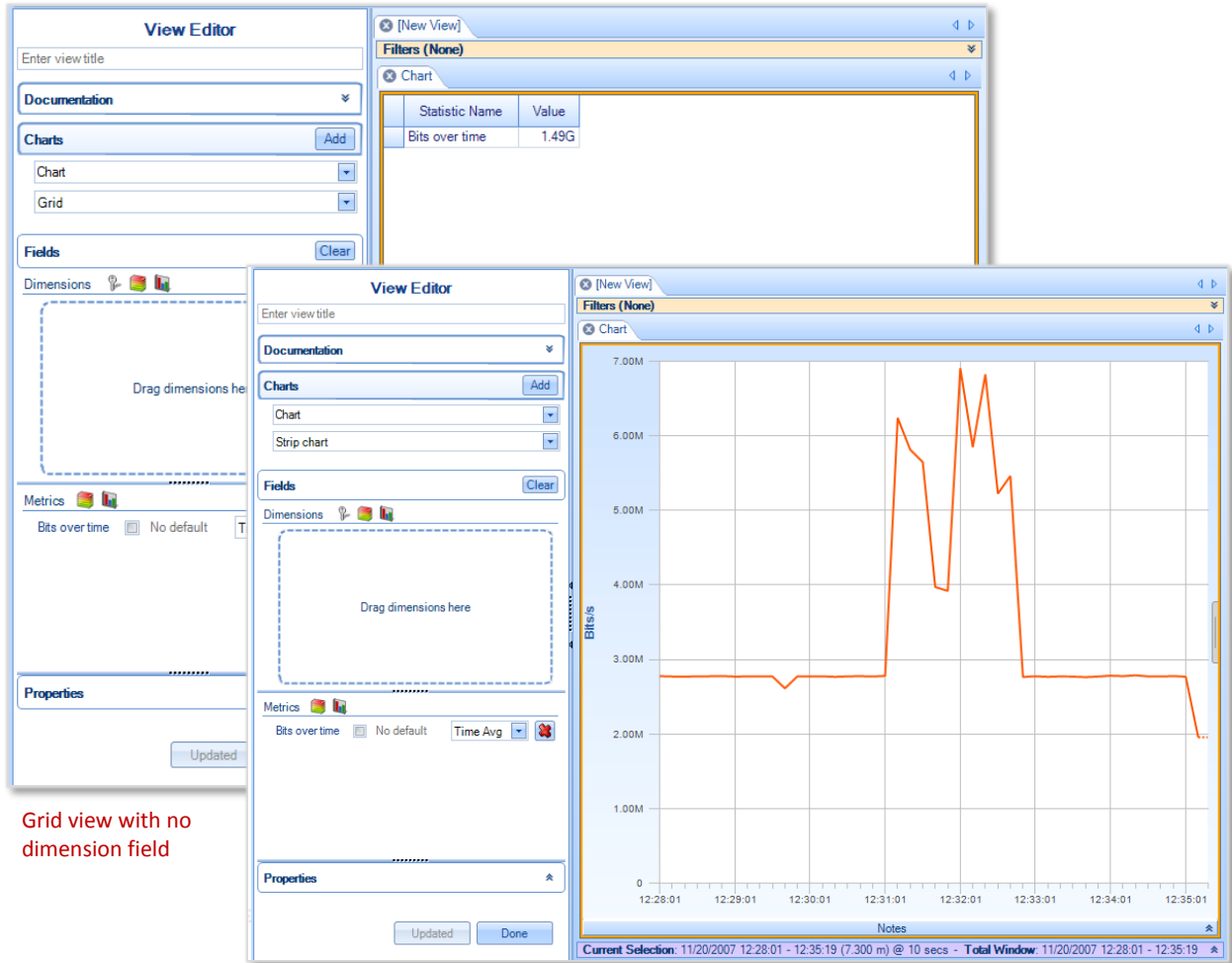


Bar charts and pie charts require a dimension field. (Without categories, bar charts would display a single bar showing 100% of the data, and pie charts would display a single wedge showing 100% of the data. Neither would provide any new insights about the data.)

Bar charts can also use an additional dimension to define a grouped or stacked bar chart.

Note: Conversation rings only support metrics of the same type.

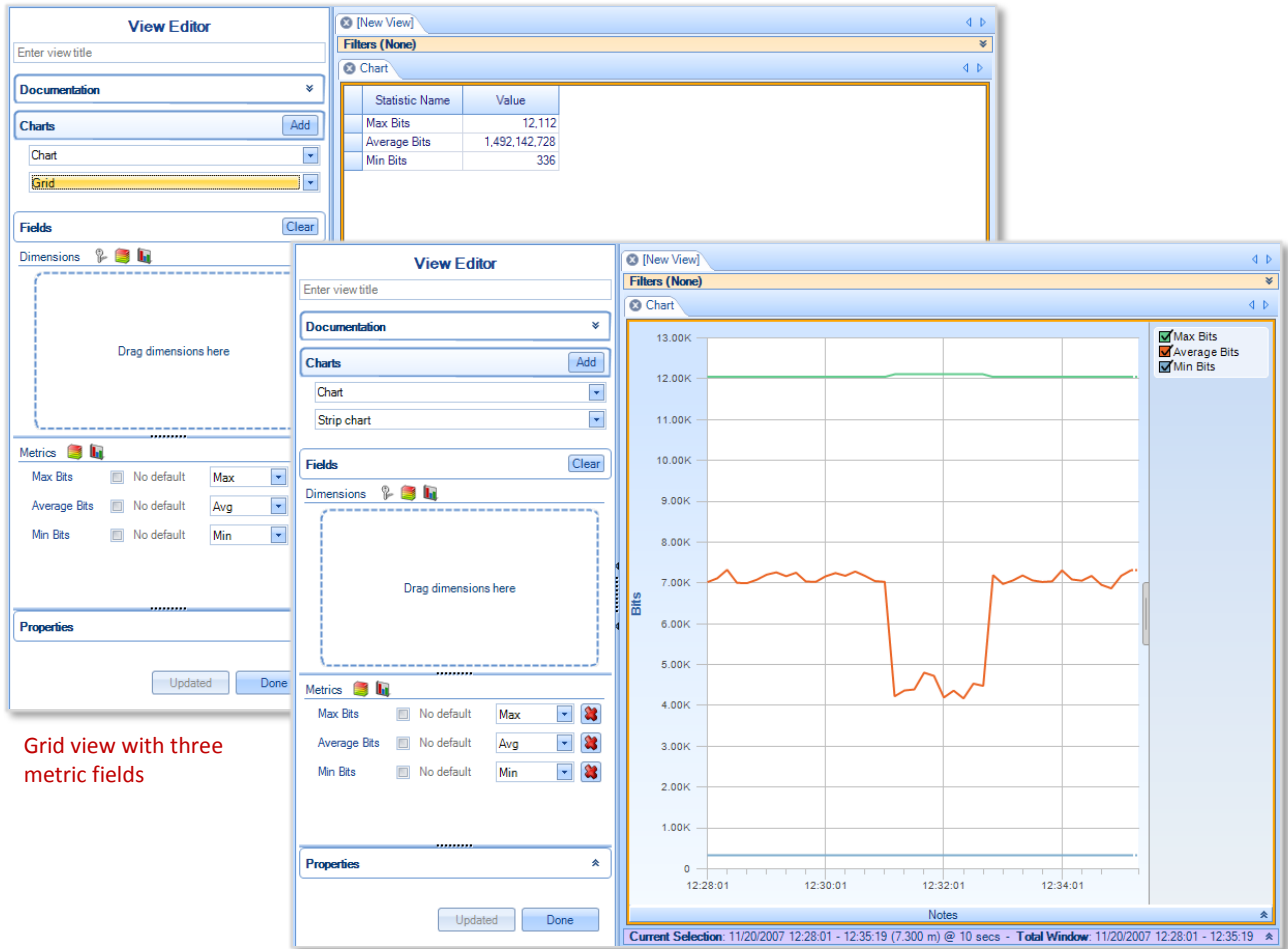
Strip charts and grids can be displayed without specifying a dimension field. In that case—that is, no categories—you see aggregate numbers for all data packets per unit of time (in the case of a strip chart) or for the entire sample interval (in the case of a grid).



Grid view with no dimension field

Strip chart view with no dimension field

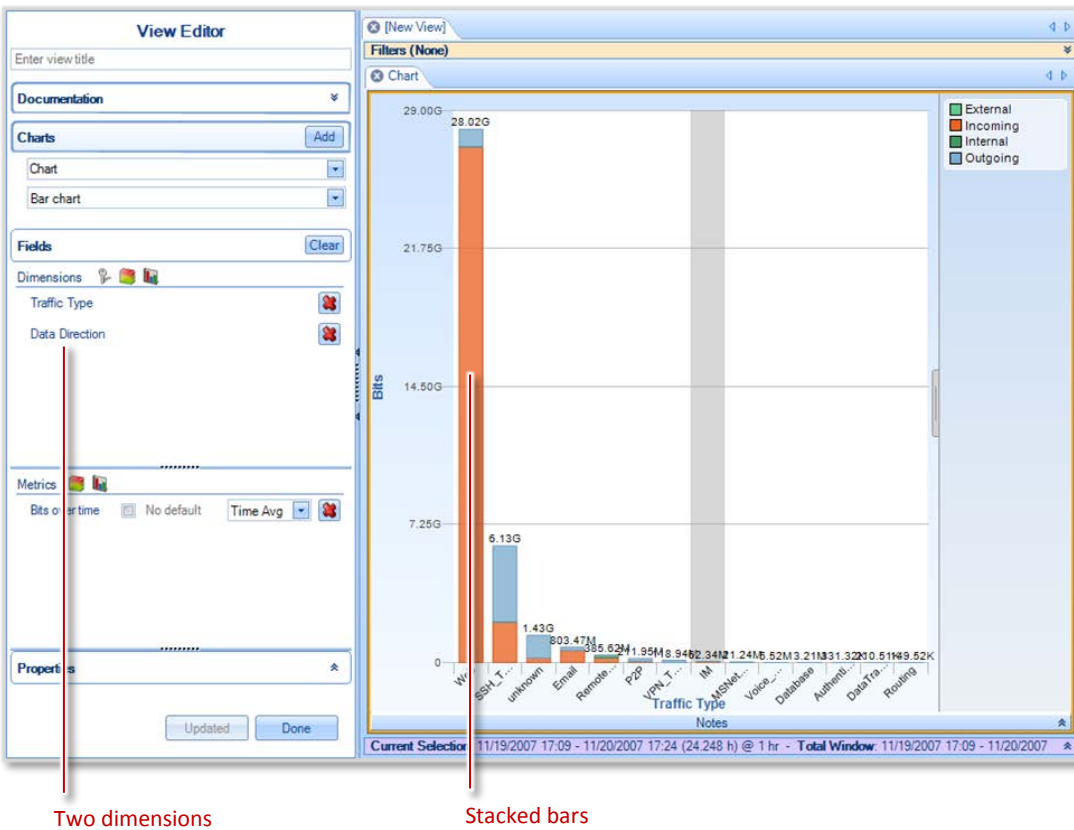
Strip charts, conversation rings and grids can also display multiple metrics. These are displayed as multiple traces on a strip chart, as multiple rows on a grid, or as multiple data types in a conversation ring. In a conversation ring, the metric displayed is selected from the chart's context menu "Data" item. Right click in the chart to open the context menu, choose "Data" and select from the list of metrics displayed.



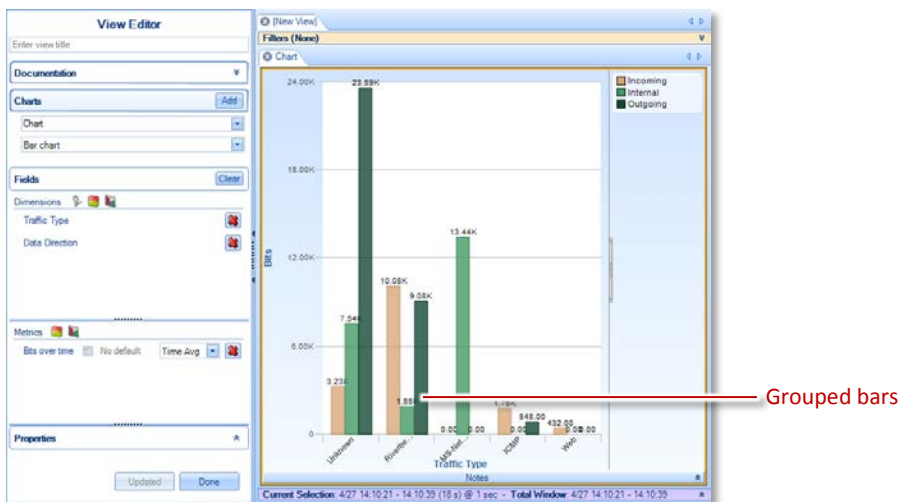
Grid view with three metric fields

Strip chart view with three metric fields

Bar charts can show up to two dimensions. If you have a bar chart with a single dimension and you drag a second field to the Dimensions panel and then update the view, the single bar chart switches to a stacked bar chart.



You can change the chart to a grouped bar chart by selecting the Bar Chart Type property in the Properties panel (described [below](#)) and choosing “Grouped”.



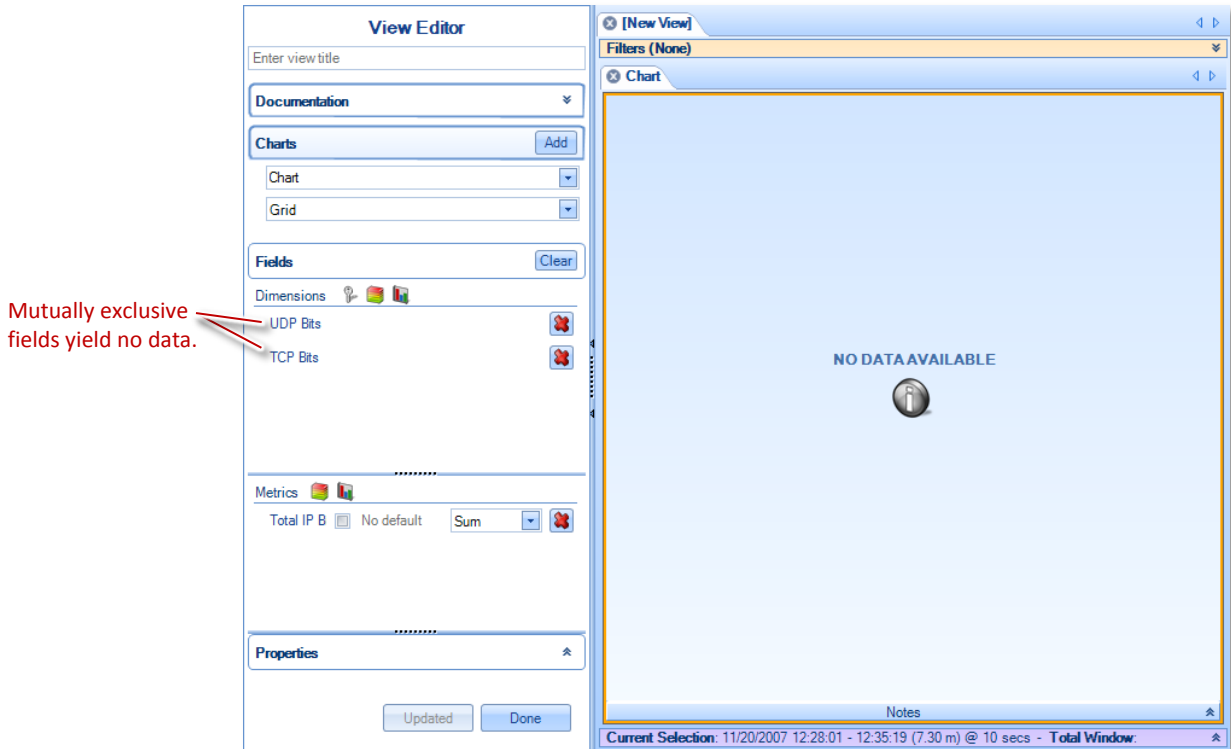
In addition, grid views can display multiple dimensions.

The screenshot shows the 'View Editor' interface on the left and a 'New View' window on the right. The 'View Editor' has sections for Documentation, Charts (with 'Add' button), Fields (with 'Clear' button), Dimensions (containing 'UDP Bits' and 'Length' with red 'X' icons), and Metrics (containing 'Total IP B' with 'No default' and 'Sum' options). The 'New View' window shows a grid with the following data:

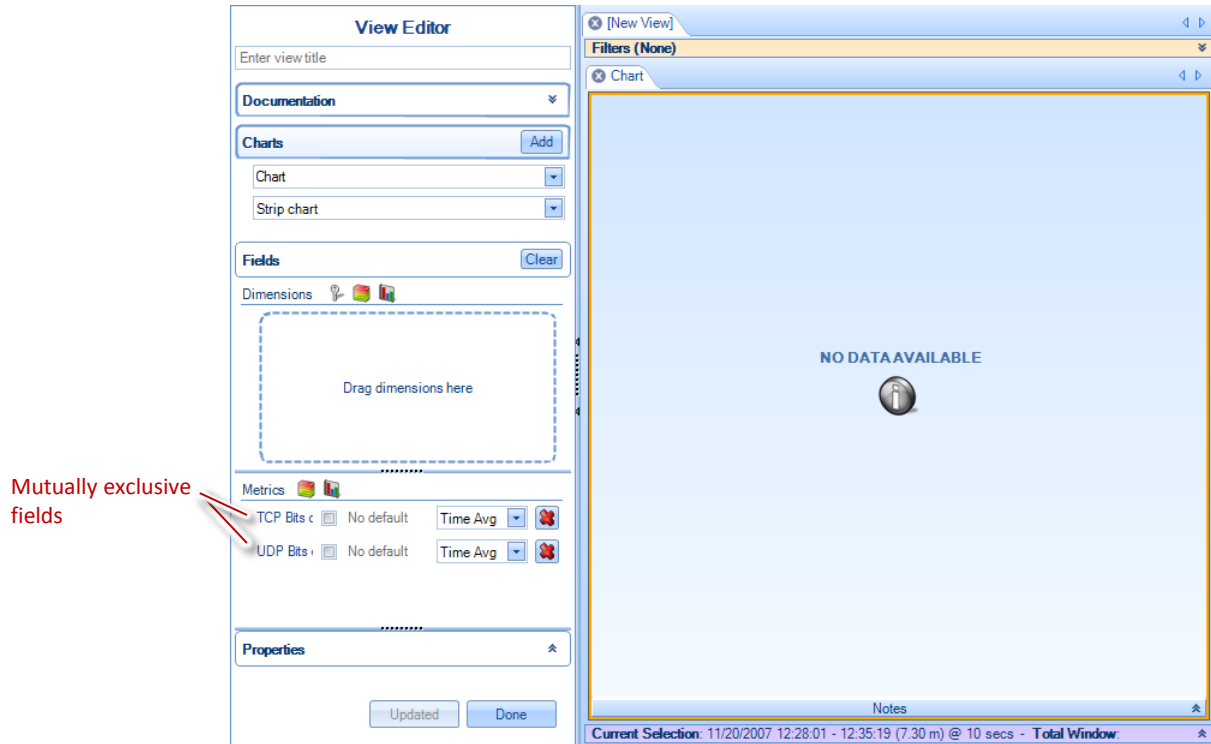
Total IP Bits	UDP Bits	Length
16,056,320	4480	526
1,943,712	544	34
397,056	4512	530
137,632	736	58
100,864	512	30
86,400	480	26
84,672	576	38
80,400	600	41
69,048	504	29
67,744	584	39
61,008	496	28
56,160	520	31
52,416	1248	122
50,840	1240	121
41,096	3736	433
38,400	1280	126
35,520	592	40
35,200	880	76
34,144	3104	354
33,264	616	43
32,240	3224	369
31,936	3992	465
31,824	1224	119
21,640	4520	521

The 'New View' window also includes a 'Filters (None)' dropdown, a 'Chart' section with a 'Drag a column header here to group by that column.' instruction, and a 'Notes' section at the bottom. The status bar at the bottom of the window reads: 'Current Selection: 11/20/2007 12:28:01 - 12:35:19 (7.30 m) @ 10 secs - Total Window.'

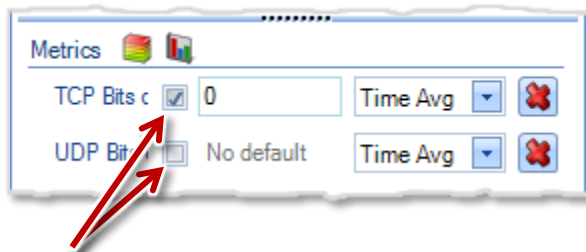
Note that all dimensions have to be computed for a given packet if that packet is to be included in the data set. So, for instance, a view that attempted to use both TCP bits and UDP bits as dimensions would have no data, since TCP and UDP packets are mutually exclusive and no single packet has both TCP and UDP bits.



Metrics behave in a similar way: all metrics must be calculated for a given packet if that packet is to be included in the data set. So, as in the case with dimensions above, a view that attempted to use TCP bits and UDP bits as metrics would display no data, since no packet could have both TCP and UDP bits.

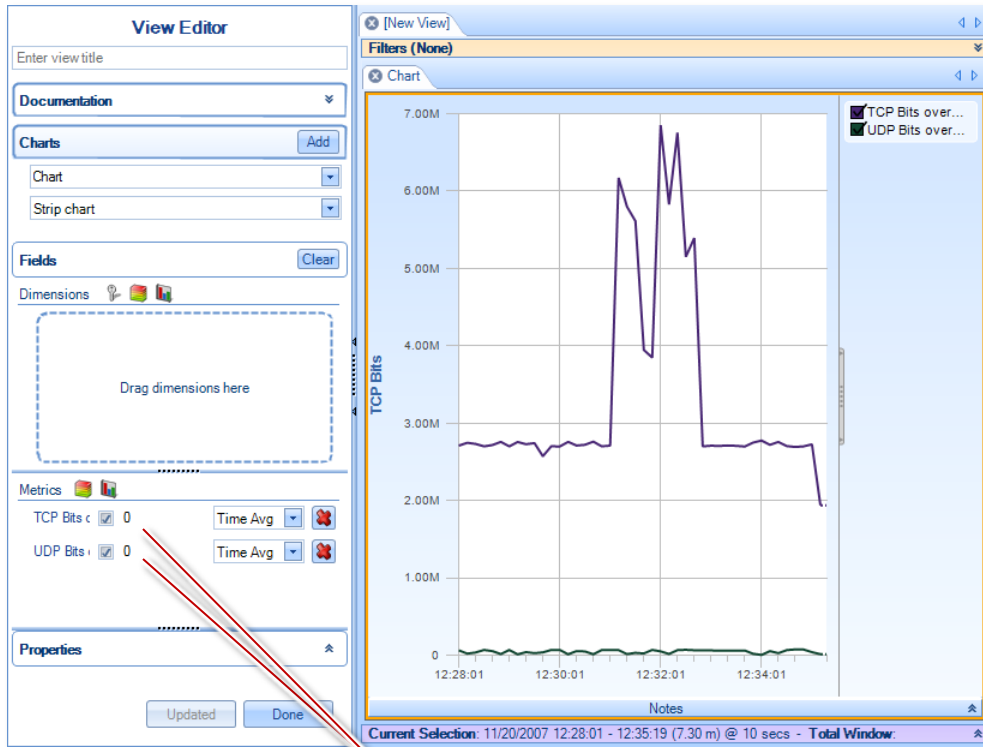


But metrics provide a way around this problem that is not available with dimensions: you can specify a default value for a metric. Just check the box in the line for the field (next to the “No default” legend that is there until you have specified a default value) and specify a default value for that field. That allows a metric to be calculated for the field, which allows the packet to be included in the data set.



Check the boxes and provide default values.

In our example, zero would be a reasonable default value for both TCP bits and UDP bits, since a TCP packet would have zero UDP bits and a UDP packet would have zero TCP bits. By providing default values, the TCP and UDP packets fulfill the requirement that all metrics can be calculated for each packet, so they are included in the data set. The strip chart for our example now looks like this:



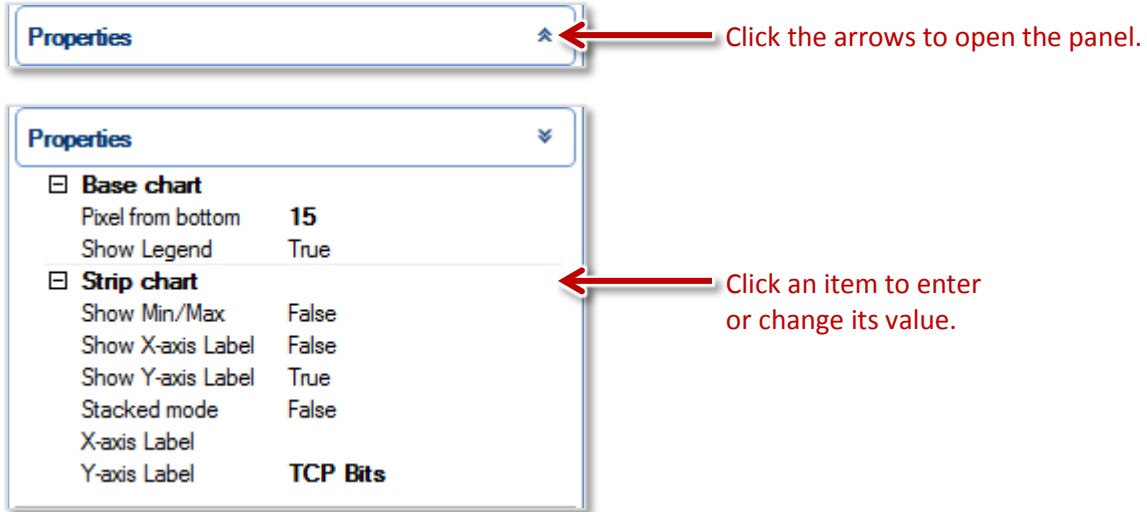
Fields with default values allow calculations for packets where values would otherwise be missing. Including these values in the data set makes it possible to plot the metrics.

Not all combinations of dimensions and metrics will give you useful results. Consider what network information you need, and explore the Fields panel to see what fields you might use to assemble that information. The standard views that are built into Packet Analyzer can provide you with good examples for useful views.

In a conversation ring, some combinations of dimensions or metrics may not be allowed if they are not of the same type.

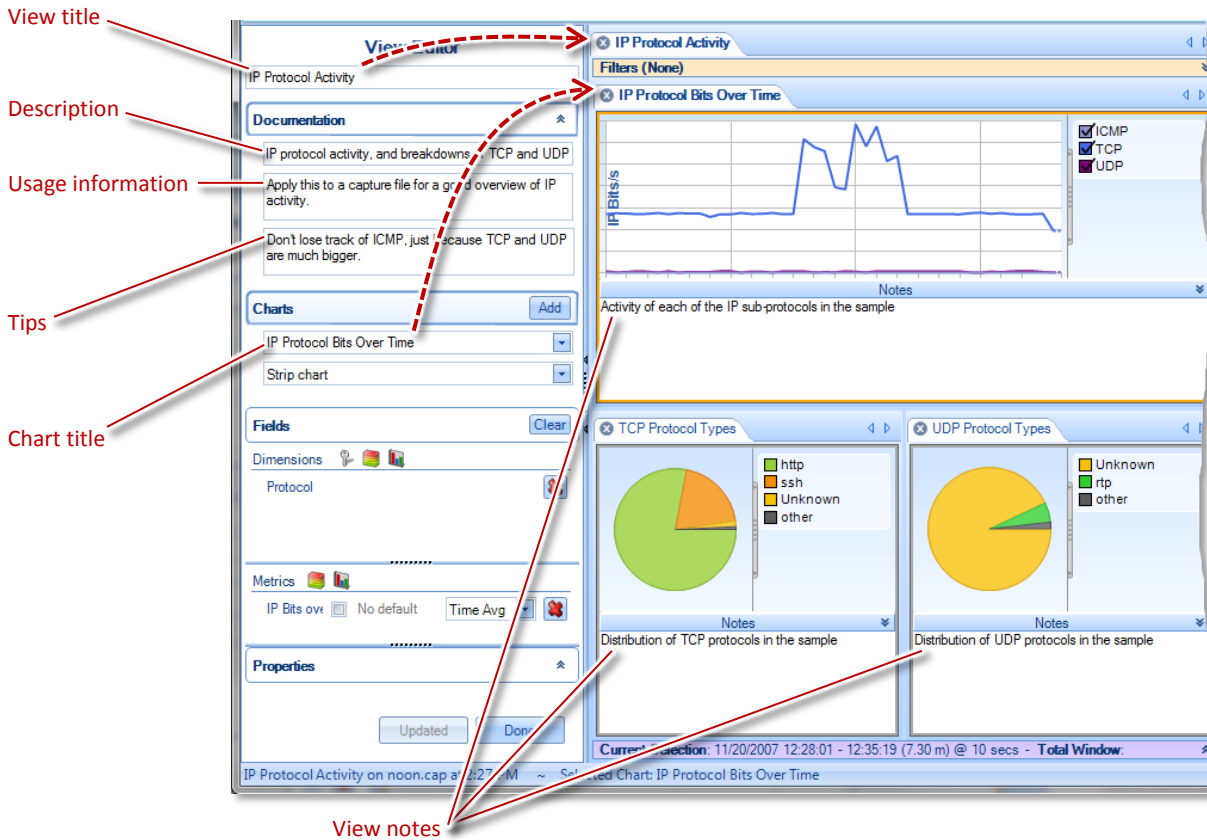
Properties

The Properties panel lets you change the appearance of the view, primarily through labeling. Click the arrows to open the panel, and click the entries in the panel to change the values there or enter new values.



Documentation and Labeling

To label the charts and provide documentation for the view's tooltip, fill in the entries in the Documentation panel. The view title is transferred to the view's tab in the main window, and the chart title is transferred to the selected chart. (The view shown here includes three charts. The chart with the yellow highlight is the active chart.)



When you are applying a view to a source, the documentation and notes also show up in the tooltips that you see when you hover the mouse over one of the view icons in the Views panel. The following diagram shows which items in the View Editor show up in which places in the tooltips.

IP Protocol Activity Live File

Overall IP protocol activity, and breakdowns of TCP and UDP

- 1 Activity of each of the IP sub-protocols in the sample
- 2 Distribution of TCP protocols in the sample
- 3 Distribution of UDP protocols in the sample

Usage Information

Apply this to a capture file for a good overview of IP activity.

Tips

Don't lose track of ICMP, just because TCP and UDP are much bigger.

Sampling Time: Second, Data Retention Time: Day

View Editor

IP Protocol Activity

Documentation

IP protocol activity, and breakdowns of TCP and UDP

Apply this to a capture file for a good overview of IP activity.

Don't lose track of ICMP, just because TCP and UDP are much bigger.

Charts Add

IP Protocol Bits Over Time

Strip chart

Fields Clear

Dimensions +

Protocol +

Metrics +

IP Bits over No default Time Avg

Properties +

Updated Done

IP Protocol Activity

Filters (None)

IP Protocol Bits Over Time

IP Bits/s

ICMP TCP UDP

Notes

Activity of each of the IP sub-protocols in the sample

TCP Protocol Types

http ssh Unknown other

Notes

Distribution of TCP protocols in the sample

UDP Protocol Types

Unknown rtp other

Notes

Distribution of UDP protocols in the sample

Current Selection: 11/20/2007 12:28:01 - 12:35:19 (7.30 m) @ 10 secs - Total Window

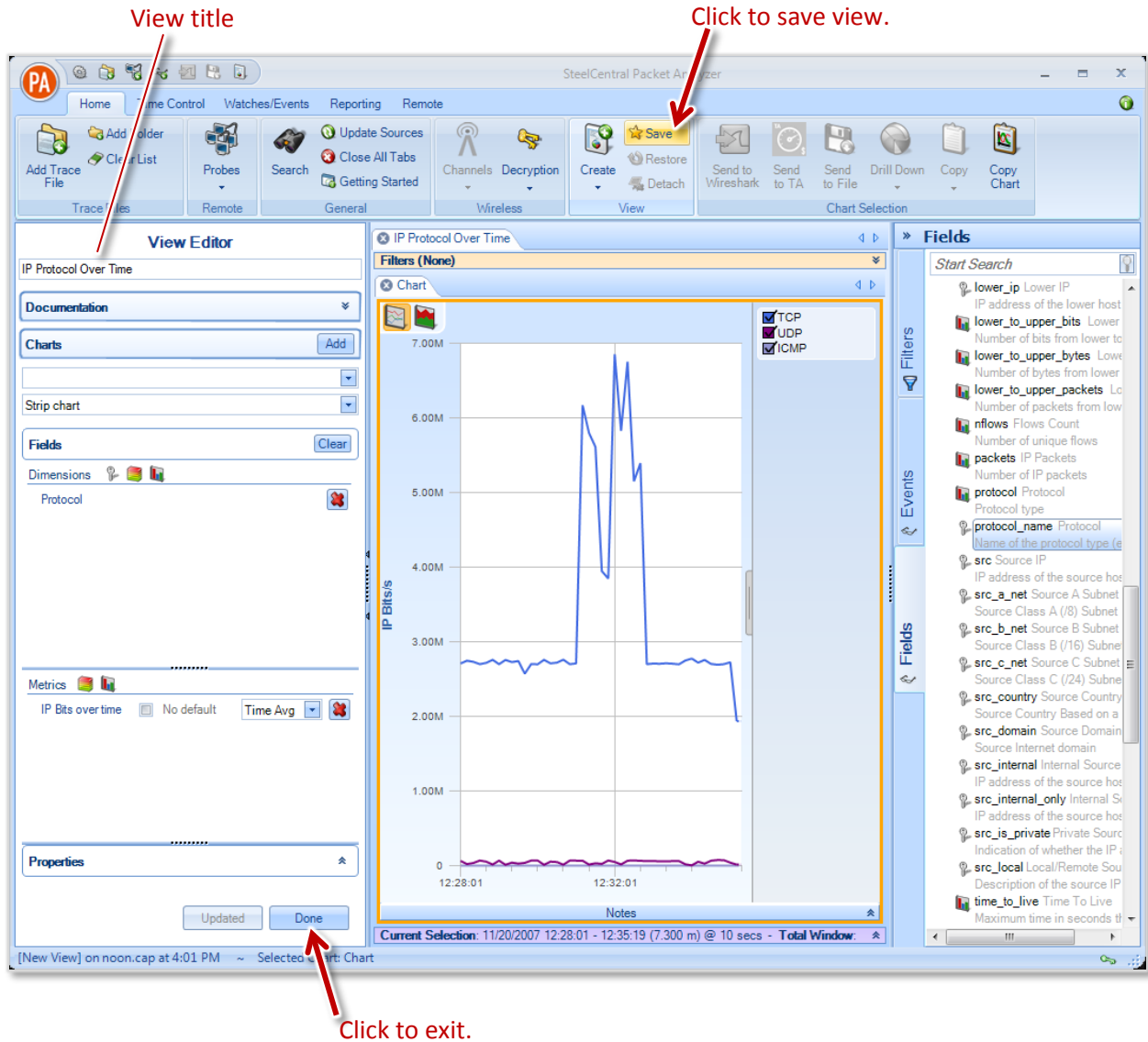
IP Protocol Activity on noon.cap at 2:27 PM ~ Selected Chart: IP Protocol Bits Over Time

Saving a View and Exiting the View Editor

When you have created a view that you want to apply to other capture files, you can save it by clicking the Save button in the View section of the Home tab. The view will be saved in the Custom folder of the Views panel, using the view title as the name of the view.

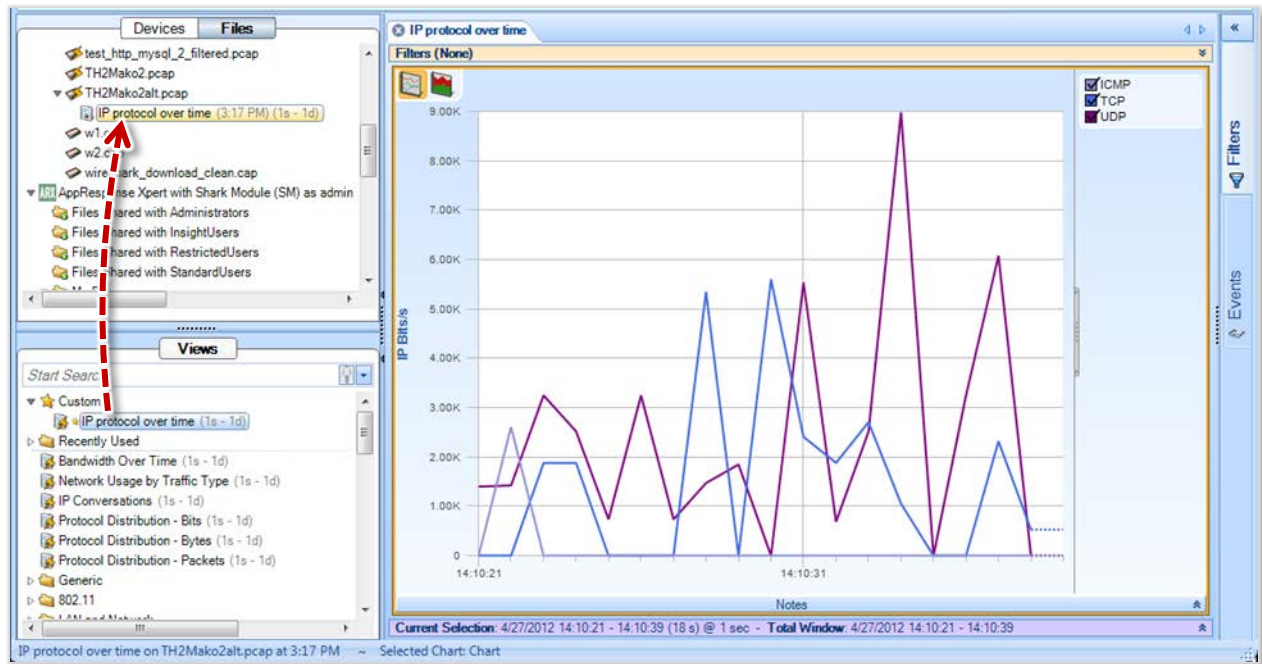
If you exit the View Editor without saving your view, the view will be lost.

Click the Done button at the bottom of the View Editor to exit.



Applying Views

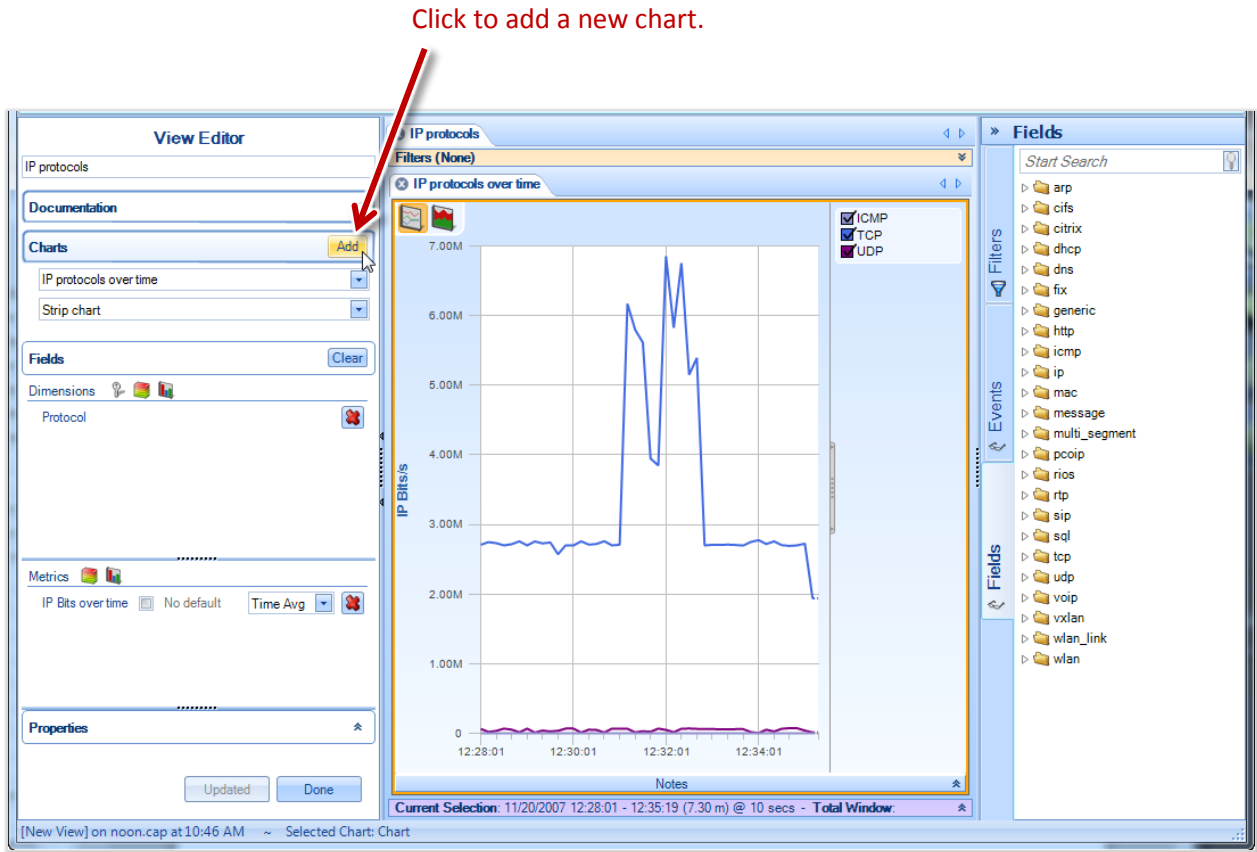
Apply a view that you have created or edited in the View Editor in the same way you apply a standard view that is built into Packet Analyzer: drag the view onto a source in the Devices or Files panel.



Though you can't use the View Editor to *create* a view using a live device—the View Editor operates only on files—you can *apply* a view that you have created in the View Editor to a live device.

Multi-Chart Views

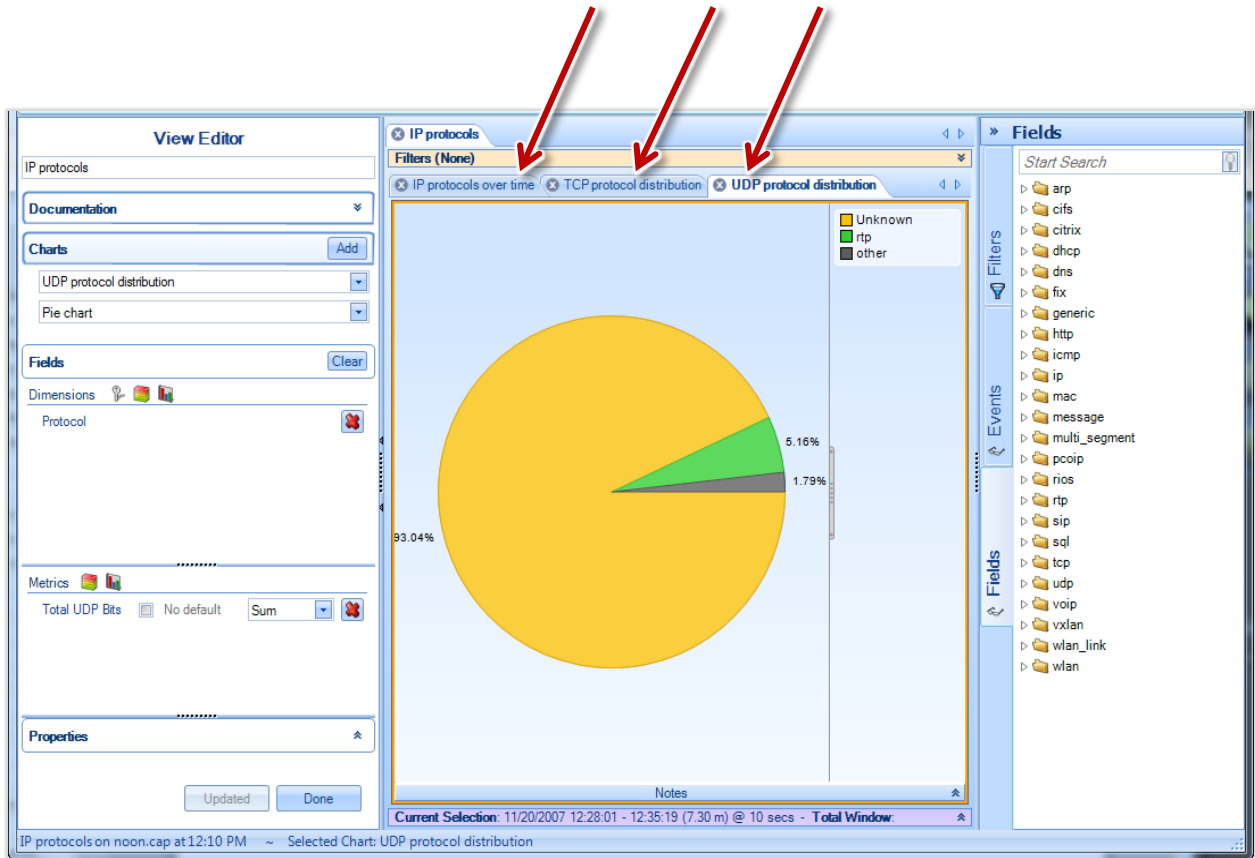
You can build views that contain multiple charts. Add a chart by clicking the Add button in the Charts panel of an existing chart.



A new blank view appears and you can create a new chart by specifying all of its parameters: dimension, metric, chart title, notes, and so on.

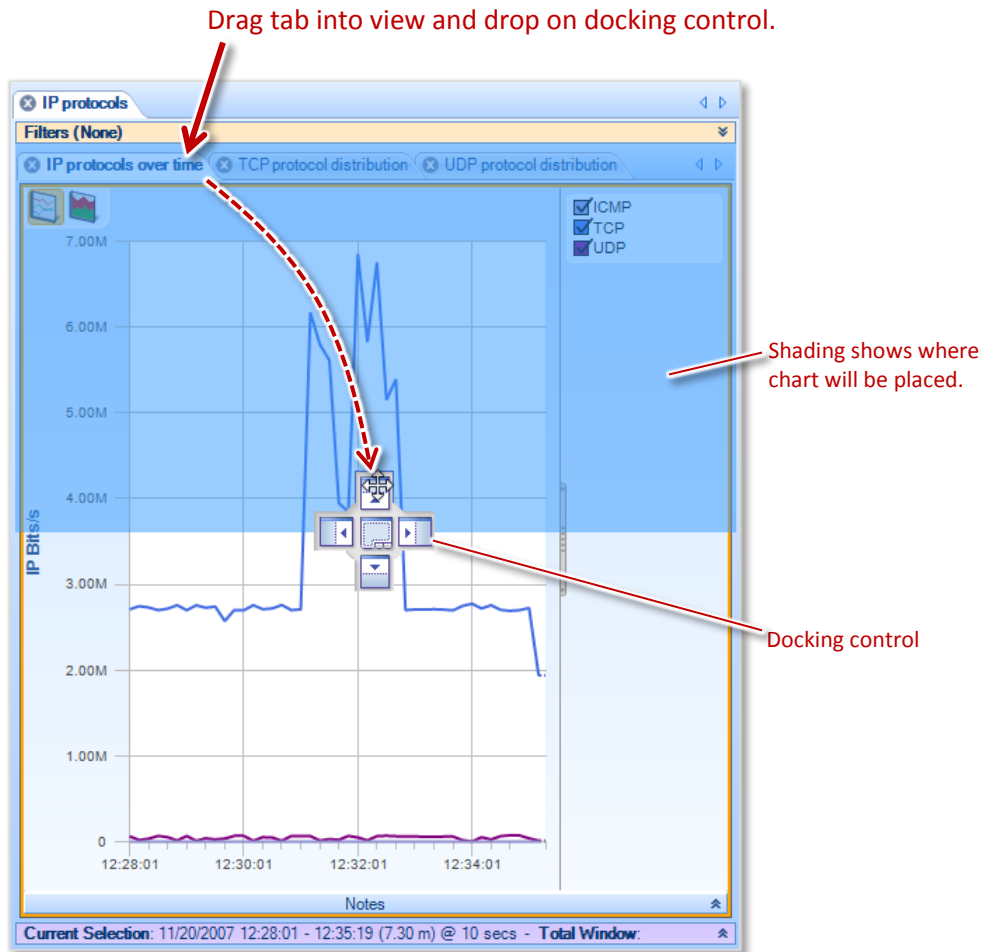
You can keep adding charts to the view until you have all the charts you want. By default, each chart occupies the whole view and you switch between charts by clicking on the tab of the chart you want to see.

Click a tab to switch to a different chart.

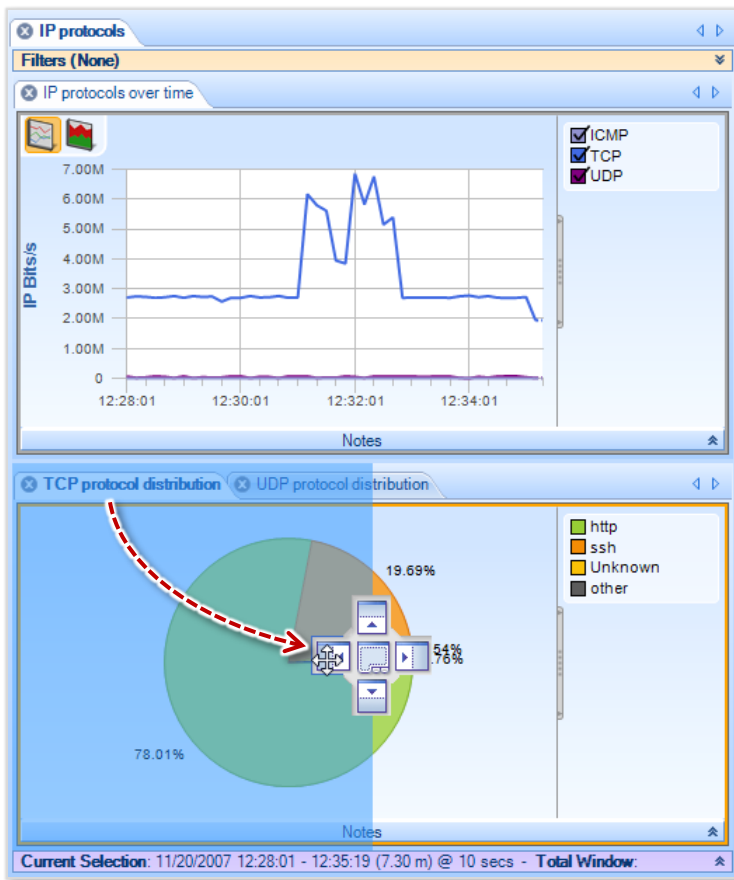


You can rearrange the charts so that you can see all of them at the same time.

For example, assume your view includes a strip chart and two pie charts, and that you want the final view to show the strip chart across the top of the view with the two pie charts side-by-side beneath it. Start by clicking the tab for the strip chart and dragging it toward the center of the view. As you drag the tab, the docking control appears. When you drag the tab over the docking control, the blue shading on the chart shows where the chart will appear in the view.

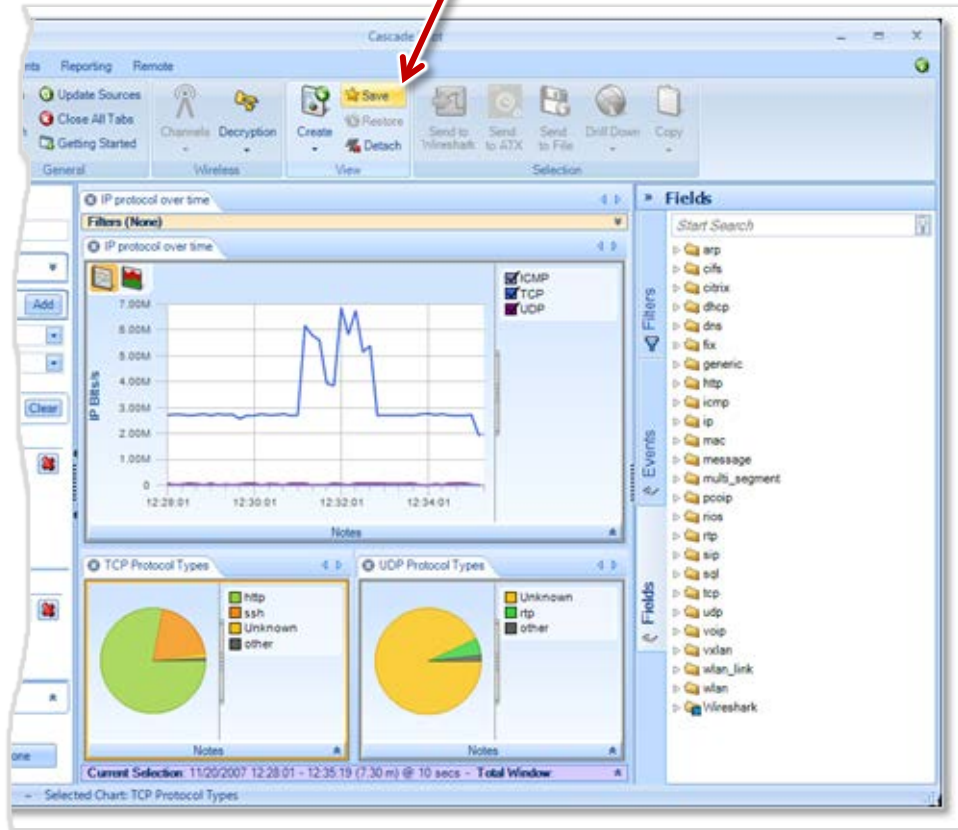


When you have the chart placed where you want it, release the mouse button to drop the tab and rearrange the view. Repeat the process until you have all the charts in the right locations.

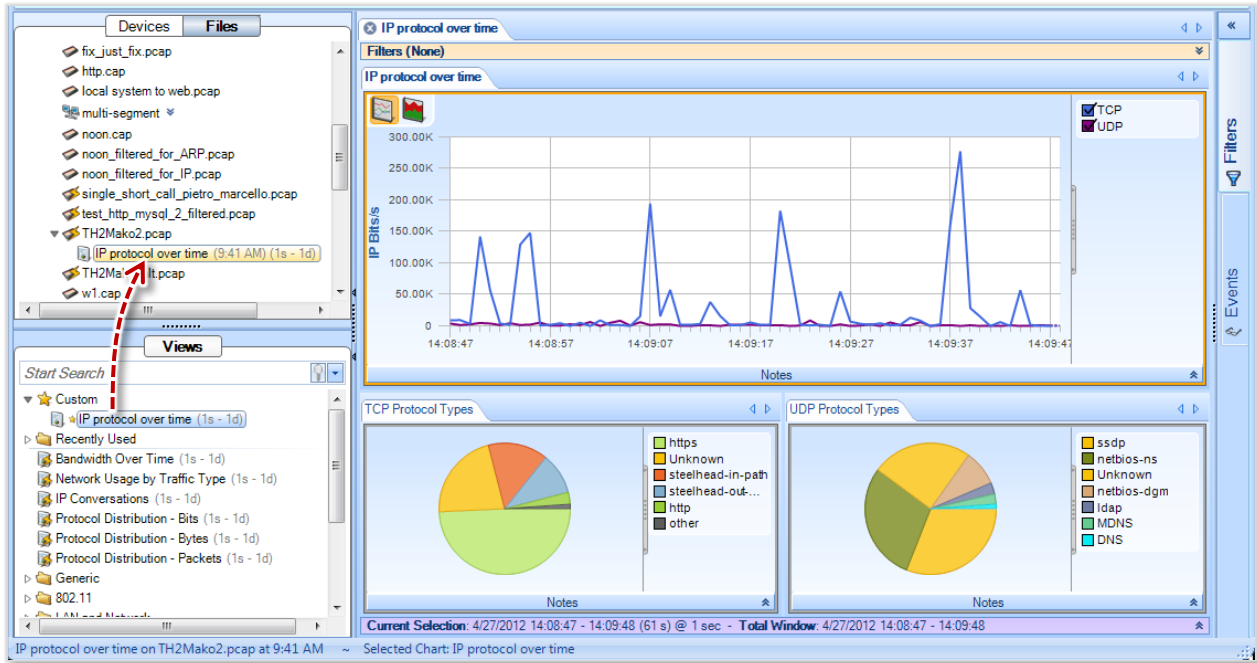


When you have the charts the way you want them, save the view.

Click to save view.



You can then apply the view to any of your devices or files.



Microflow Indexing

Indexing a Trace File

Indexing a trace file can improve the performance of several views by a factor of 100x to 1000x. Creating a Microflow Index does not take much more time than loading a single view, thus it is often more efficient to create an index on a large file and then apply multiple views on the indexed file.

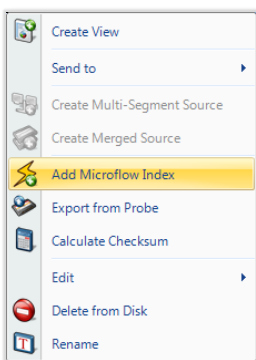
Microflow Indexes can be applied to all types of trace files except Wi-Fi capture files. When an index is successfully created, the indexed file shows a small yellow lightning icon on it. If, for any reason, the index is not completely loaded, a red lightning arrow appears on the top of the trace file icon. 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

A Microflow Index can be applied to a trace file using the *Add Microflow Index* button in the trace file context menu option.

Context Menu

Add Microflow Index



The context menu for a Trace File without index shows:

Add Microflow Index

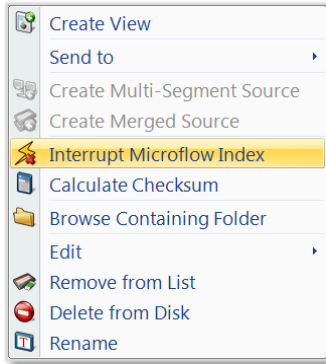
The *Add Microflow Index* menu option creates a Microflow Index on the selected file.

Add Microflow Index context menu



Add Microflow Index

Interrupt Microflow Index



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

Interrupt Indexing

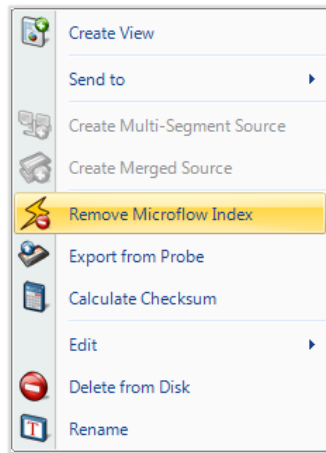
The *Interrupt Microflow Index* menu option interrupts the creation of an Index while it is being created

Interrupt Microflow Index context menu



Interrupt Indexing

Remove Microflow Index



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

Remove Microflow Index

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

Remove Microflow Index context menu



Remove Microflow Index

Index Icons on Trace Files



Index Applied means that the index has been applied successfully and thus many views will be accelerated.

Index Applied

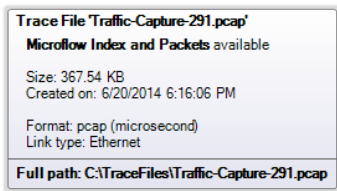


Index Broken means that either the file does not support indexing (e.g. a Wi-Fi file) or the index was interrupted before completion. To show the cause of the broken index, text in gray appears on the right of the trace file containing either:

Index Broken

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

Tooltips



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

Trace File

The name of the file.

Microflow Data and Packets available

Indicates that the index has been applied and both accelerated microflow data and detailed packet data are available for this trace file.

Size

The size of the trace file in kilobytes.

Created on

The date the trace file was created.

Format

The type of trace file.

Link type

The link type of the trace file. This is important because not all views can be applied on all files. In particular, if the Link type is PPI, then the index cannot be created.

Full path

The location of the file.

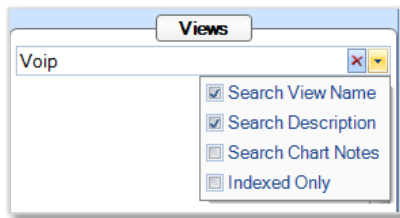
Indexed File Tooltip

Drag and Drop Cursors for Indexed Trace Files



When dragging and dropping a view that supports indexed files, the *Drag and Drop cursor* includes a yellow lightning bolt when dragged over an indexed file to indicate that the index will be used

Search Text Box

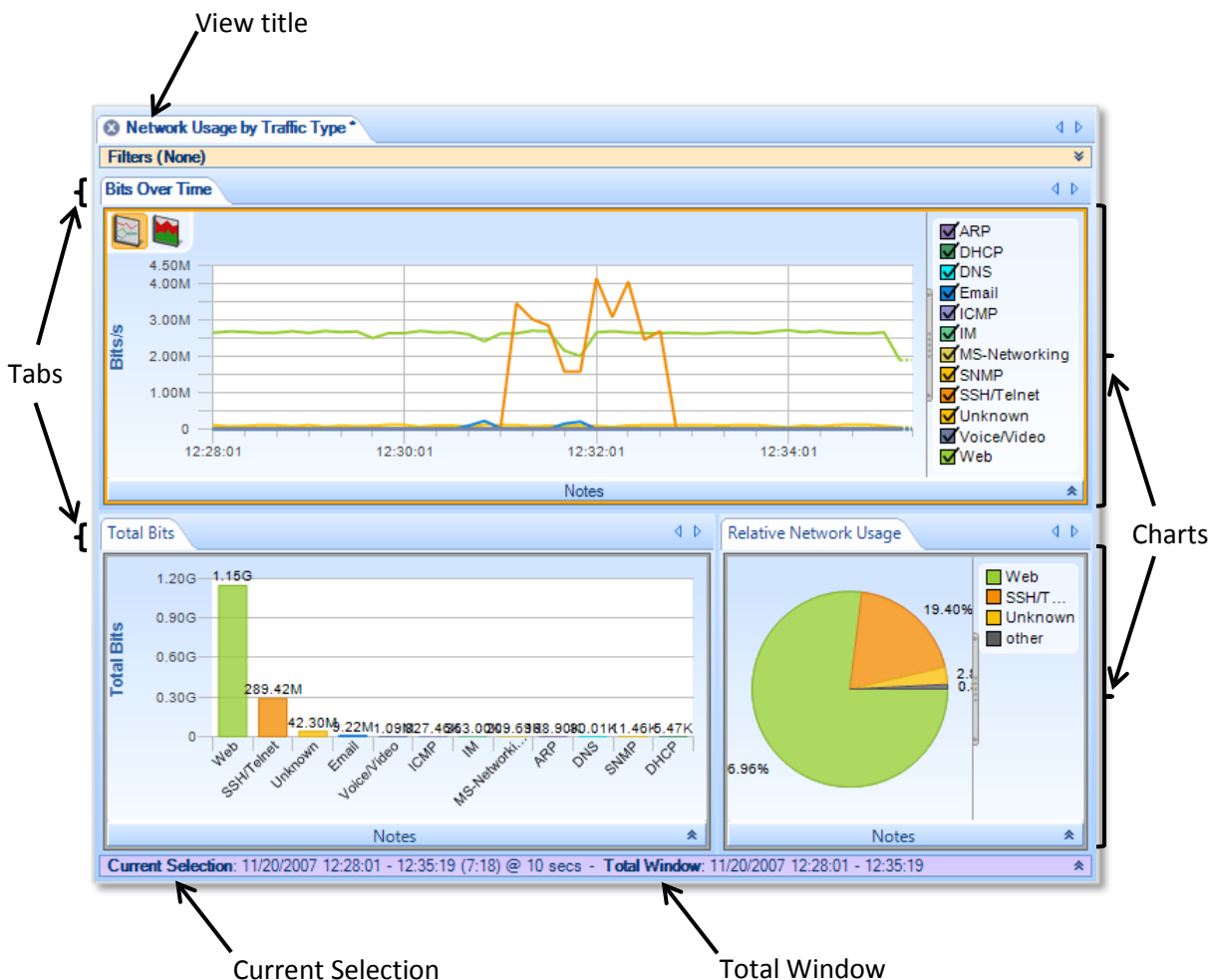


The Search box has an Indexed Only option to include only Views that support indexing.

View Panel Search

Main Workspace

The *Main Workspace* uses tabbed windows that are usually referred to as “views” or the more general term “tabs.” A View consists of a number of Charts – for example, 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.



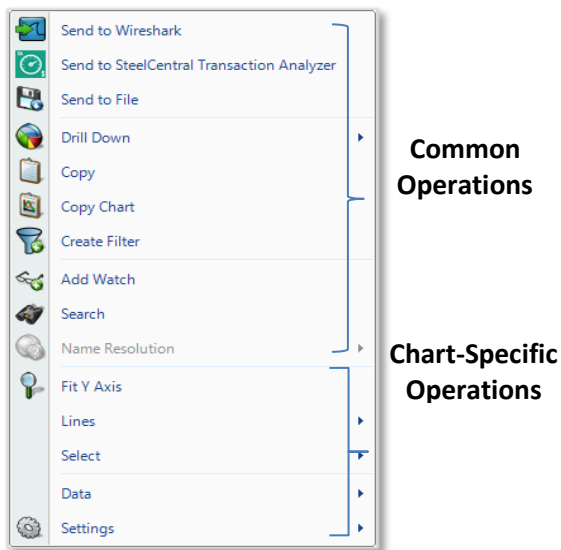
A View in the Main Workspace

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 displays two time intervals: the *Current Selection* interval and the *Total Window* interval.

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

Context Menus



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 for strings within a Chart or Charts
- Add Watch (only for Strip Charts and Bar Charts)
- Chart-Specific Operations
- General Chart and Selection Operations

Chart Context Menu Overview

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



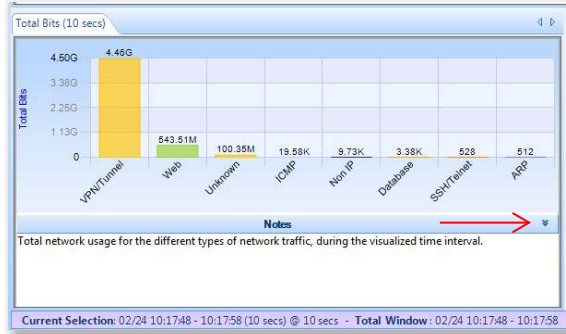
Every chart has a section that can be used to place notes that are included in a generated report and if applicable, saved in a custom view.

For example, in the view on the left, all the note areas are expanded.



View Notes Toggle Button

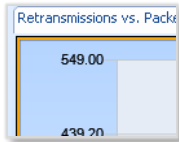
Each chart has a long horizontal bar with a small arrow on the right bottom border.



View With Expanded Notes

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



A chart can be selected by clicking on it, and the currently selected chart can be identified 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.

Chart Selected

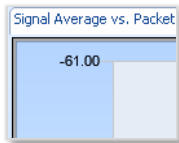
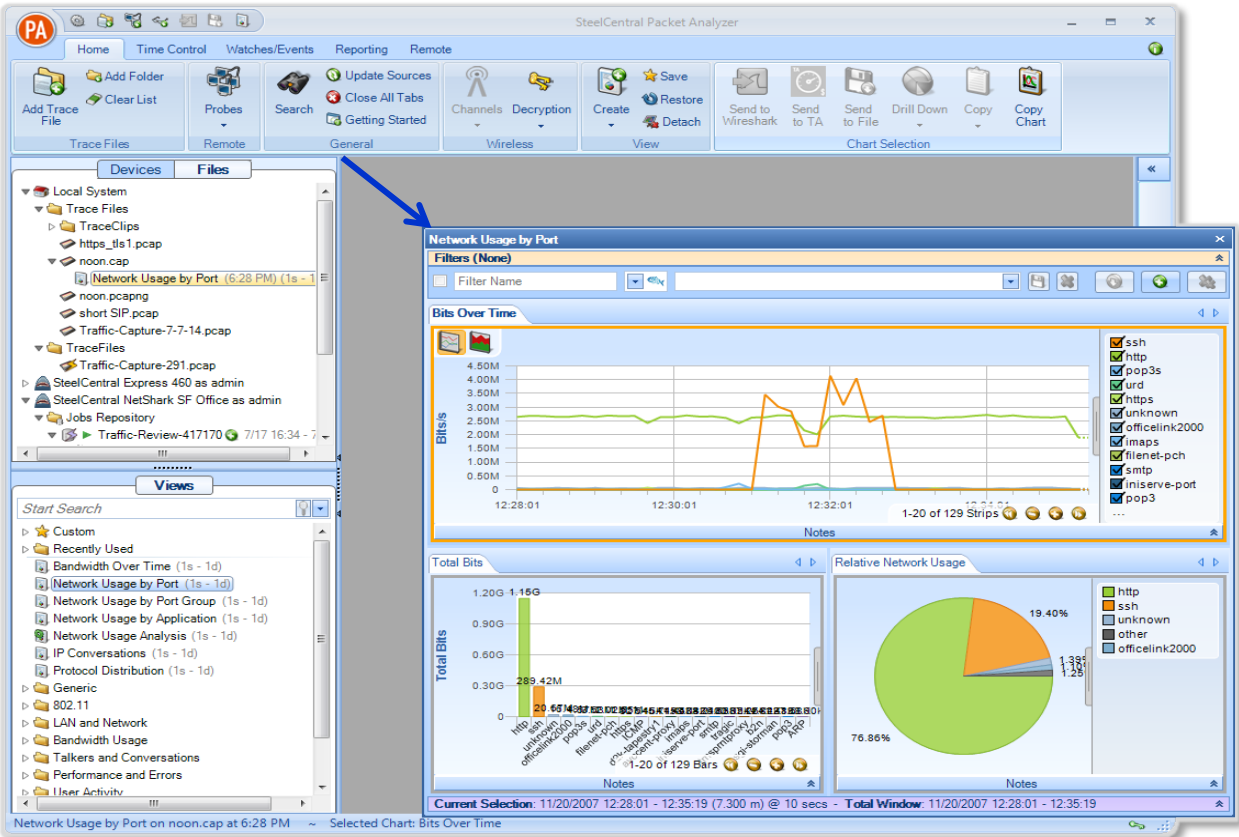


Chart Not Selected

Undocking Views

By default, a view is docked in the main window. You can undock a view so that it occupies a separate floating window. As with other windows, you can resize the window by dragging on the borders, and you can relocate it anywhere on the screen, even on a different monitor.

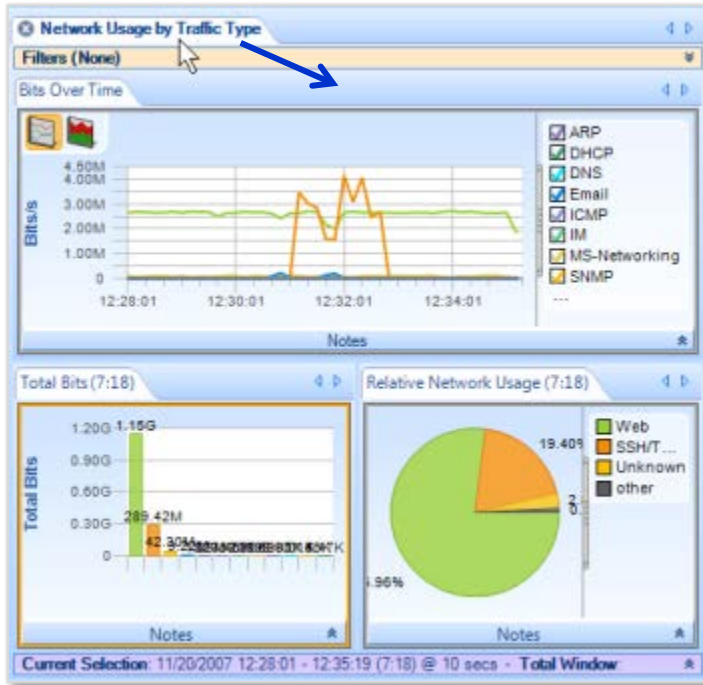


Typical undocked view

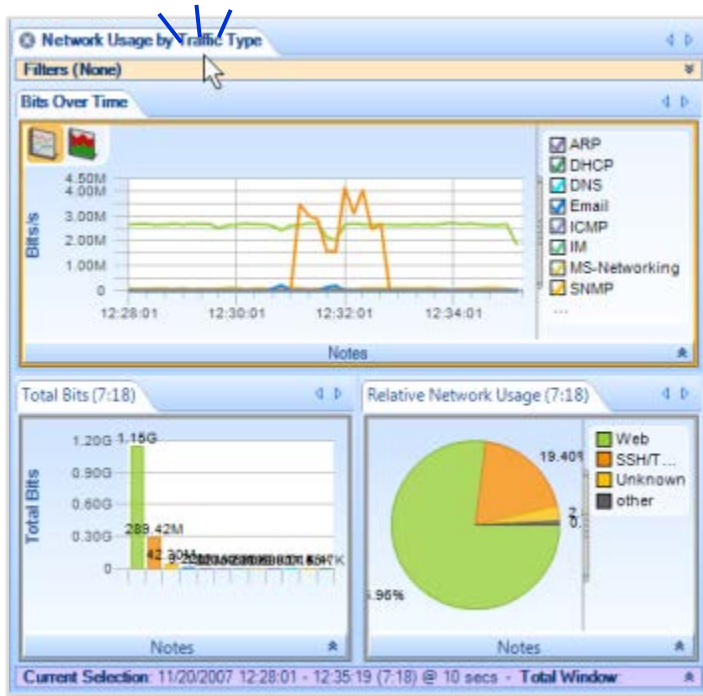
Undocking a View

There are three ways to undock a view:

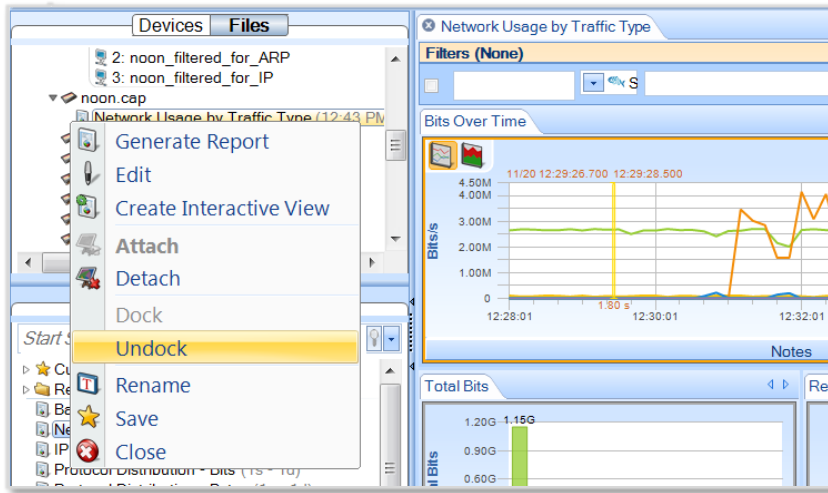
- Drag the view's tab.



- Double-click the view's tab



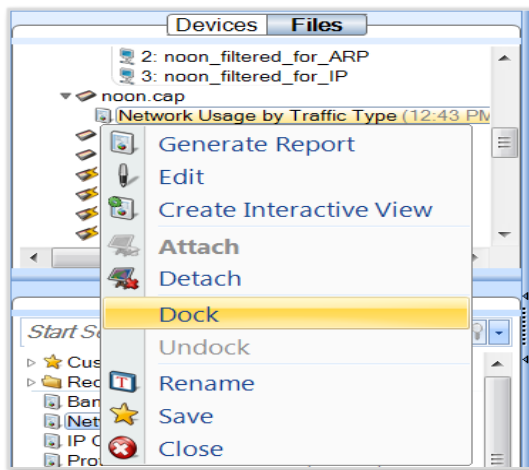
- Right-click the applied view in the Devices/Files panel and select **Undock** from the context menu.



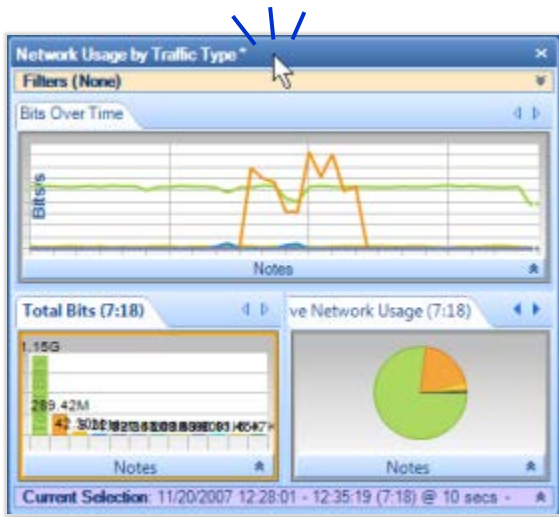
Docking a View

There are three ways to dock an undocked view:

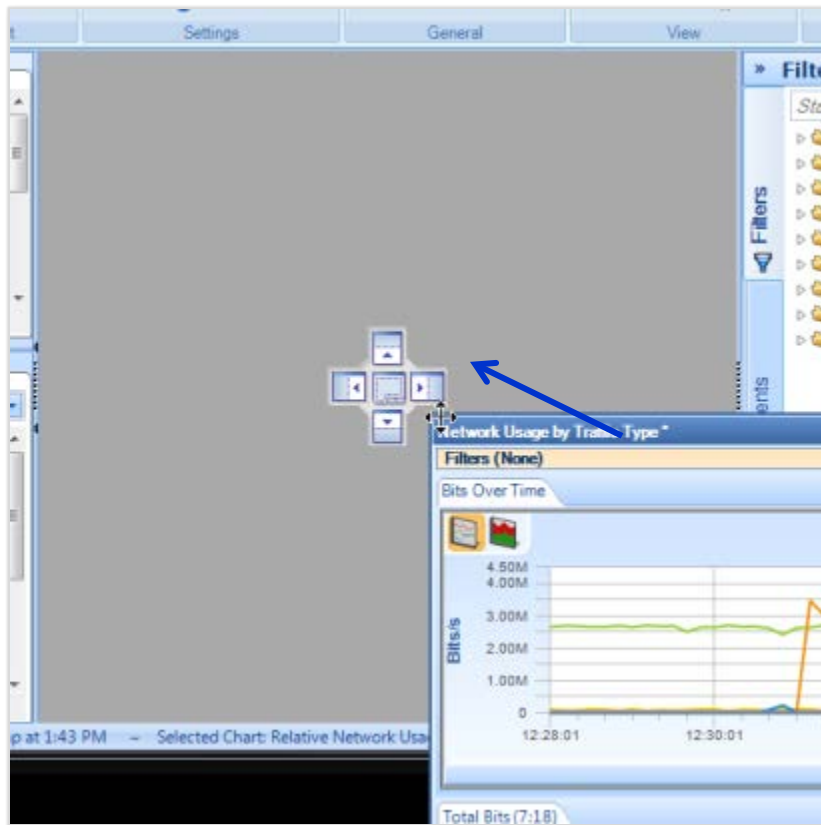
- Right-click the applied view in the Devices/Files panel and select **Dock** from the context menu.



- Double-click the main bar of the floating window.



Drag the floating window onto the Packet Analyzer main window. When the mouse cursor hovers over the docking control, the main window turns blue and you can drop the floating window onto it.



If the main window is empty, the floating window will dock and fill the entire main window. If another view occupies the main window, the result depends on interaction between the mouse cursor and the docking control.



Docking control

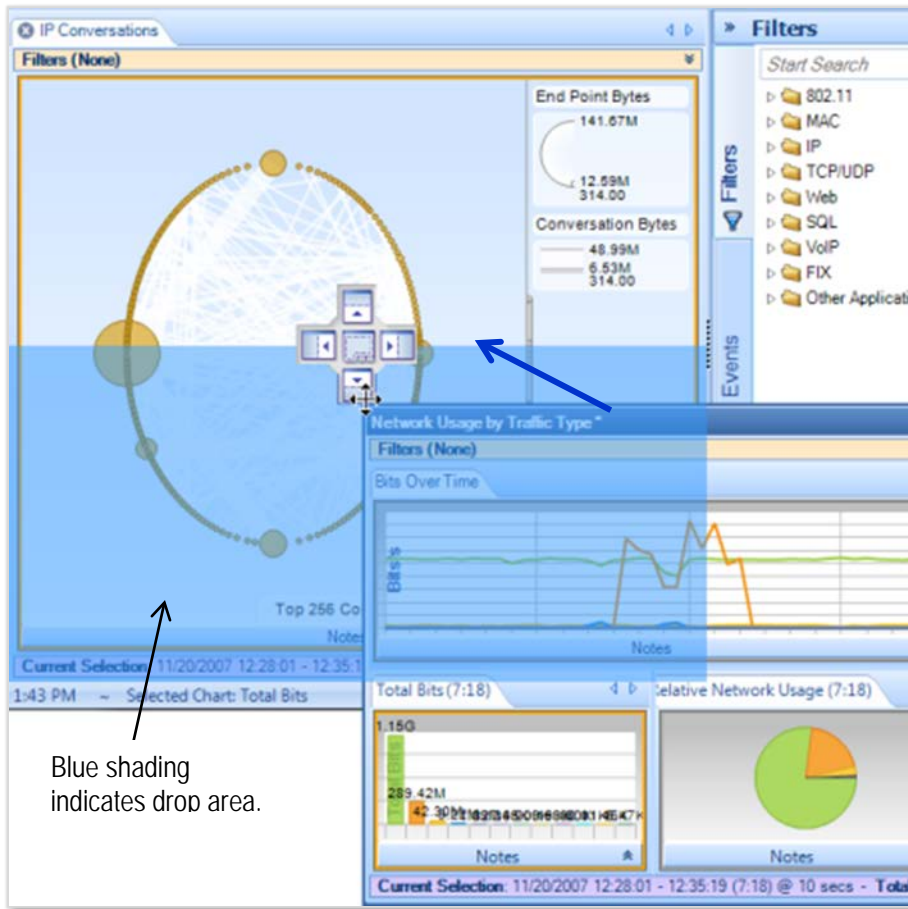
If the mouse cursor hovers over the center icon of the docking control, the entire main window turns blue. When you click the mouse, the floating window drops into the main window and replaces the view that was there. (The previous view is still available. Click its tab to bring it to the front of the main window.)



Docking into the entire main window

If the mouse cursor hovers over one of the outside icons of the docking control, a portion of the main window turns blue. When you click the mouse, the floating window drops into that portion of the main window and shares the main window with the view that was there.

For example, in the illustration below, the mouse cursor is hovering over the bottom icon of the docking control, and the bottom half of the main window is shaded blue.



Docking into a portion of the main window

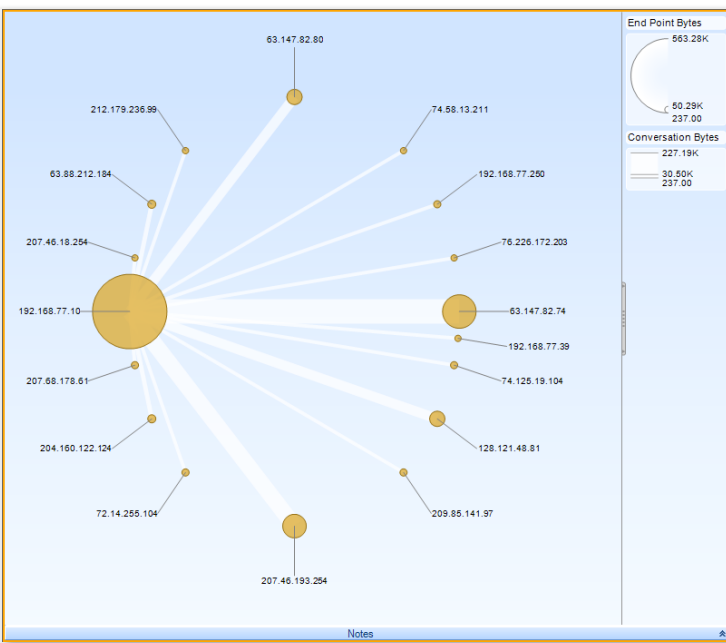
When the mouse cursor is clicked, the floating window drops into the bottom half of the main window.



Conversation Ring

In the *Conversation Ring*, “conversation” endpoints are placed around an ellipse. The Conversation Ring is used for situations in which “stations,” represented by the endpoints, communicate (i.e. have a conversation) with each other. The endpoints are depicted as circles, and 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 the amount of traffic sent to/from the endpoints over the selected time period.

Default



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

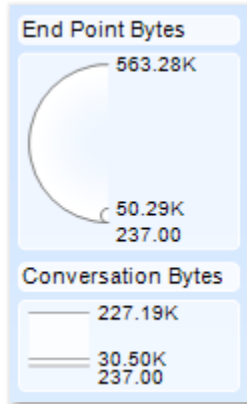
- Show endpoint labels
- Endpoint color
- Name resolution
- Choose metric to display
- Toggle legend visibility

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

- Scroll Wheel
- Hover
- Selection

Conversation Ring

Size Legends



In the upper right corner of the view are two size legends that depict the maximum, average and the minimum traffic in all displayed endpoints and conversations. An example is shown in the figure on the left.

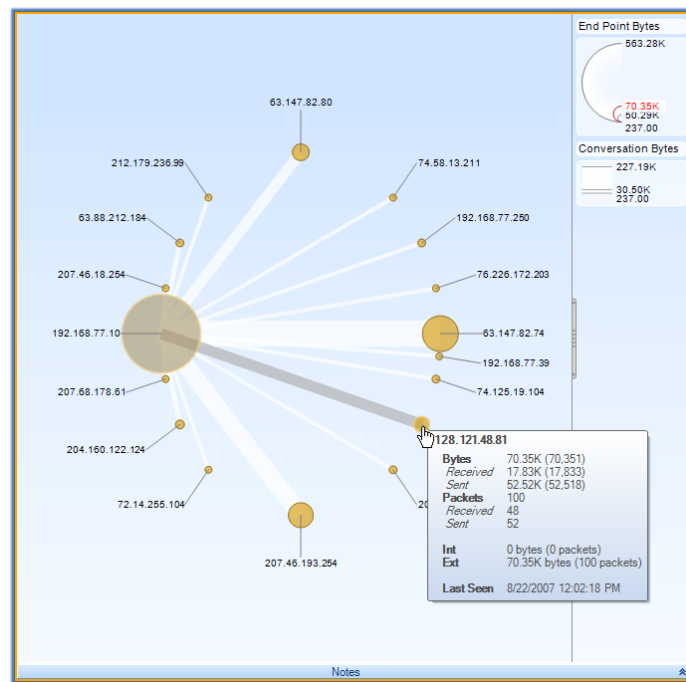
Size Legends in a Conversation Ring

Scroll Wheel

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

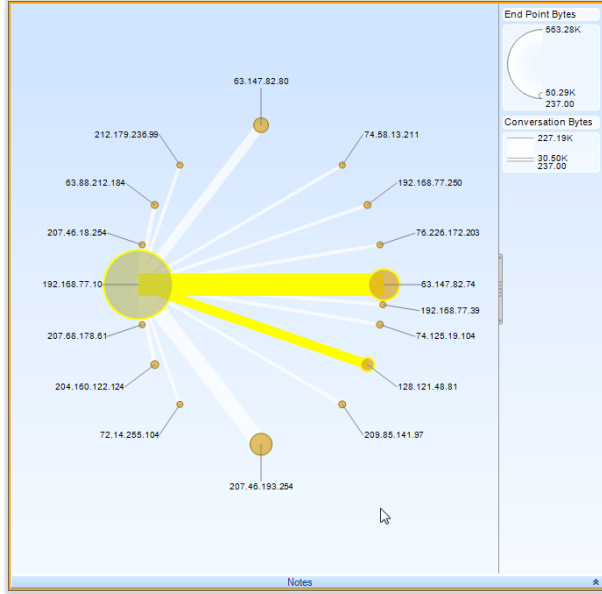
Hover with Tooltip

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 describing the connection or endpoint, and causes the Size Legend to display the values for the endpoint or conversation in red.



Conversation Ring Hover

Selected



Conversation Ring Selection

Clicking on a connection selects the connection and the associated endpoints. Clicking on an endpoint selects all the connections that include the endpoint as well as all the associated endpoints that are on the other side of the connections.

Clicking with Control key pressed is supported for multiple endpoint or connection based selections (which can be mixed).

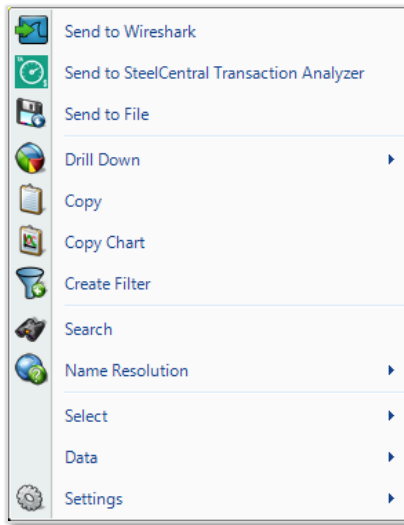
Top Conversations



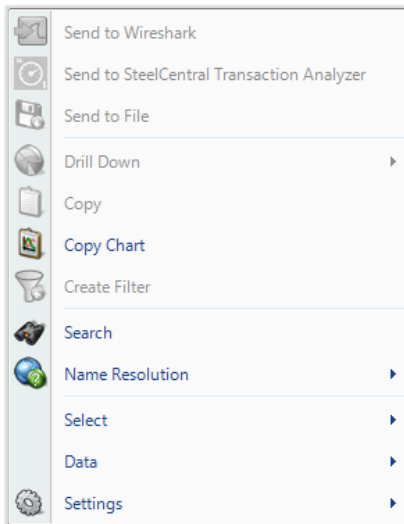
Conversation Ring Top Conversations

When there is not enough space to display all of the conversations clearly in a single ring, Packet Analyzer automatically includes data by relevance. A small label displaying the number of conversations and the percentage of the underlying 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. Endpoint labels can always be shown using the Settings item in the context menu.

Context Menu



Conversation Ring (Selection)



Conversation Ring (No 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 SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected endpoint(s) and connection(s) to Transaction Analyzer 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.

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

The *Copy* menu option copies a table of data values corresponding to the current selection to the clipboard. These are copied in the order that the hosts were discovered in the conversation ring. The only exception to this rule is that the “Last Seen” value is not included in what is copied to the clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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 consists of the labels of the items in a chart which can be selected. For instance, an IP

address, MAC address, or hostname can all be searched. The Search Dialog is described in its own section later on.

Name Resolution

The *Name Resolution* menu option tries to identify unresolved IP addresses, ports, or MAC addresses from all or the selected endpoints and/or conversations. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Select

The *Select* menu option has two 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).

Select All

Selects all the connection(s) and endpoint(s) in the Conversation Ring.

Select Inverse

Inverts the current selection of the endpoint(s) and connection(s).

Data

The *Data* submenu sets what data are displayed from the available metrics.

Settings

The *Settings* submenu option opens up a submenu with three items.

Show Legend

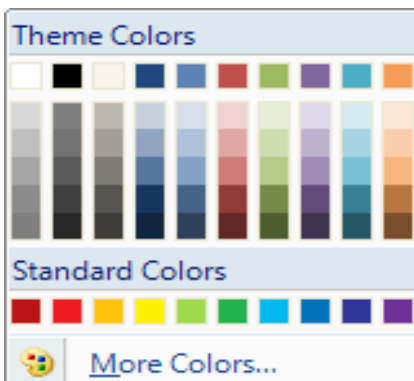
Toggles Legend display

Always Show Labels

Forces all endpoint labels to be shown.

Endpoint Color

Color choices to change the color of the endpoints for the chart.



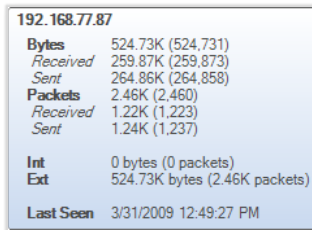
Tooltips

The conversation ring has two kinds of tooltips:

- Connection Based
- Endpoint Based

Tooltips provide information on the metrics used in the conversation ring chart. In the examples given below, the chart metrics are Bytes and Packets. Your tooltips may differ as they will reflect the metrics you used in your conversation ring chart.

Endpoint



192.168.77.87	
Bytes	524.73K (524,731)
Received	259.87K (259,873)
Sent	264.86K (264,858)
Packets	2.46K (2,460)
Received	1.22K (1,223)
Sent	1.24K (1,237)
Int	0 bytes (0 packets)
Ext	524.73K bytes (2.46K packets)
Last Seen	3/31/2009 12:49:27 PM

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.

Bytes

The *Bytes* value refers to the total number of bytes that have been either sent from or received at that endpoint, i.e. the sum of Received and Sent bytes.

Received

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

Sent

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

Packets

The *Packets* value refers to the total number of packets that have been either sent from or received at that endpoint, i.e. the sum of Received and Sent packets

Received

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

Sent

The *Sent* value refers to the total number of packets sent at that endpoint over a given sample period, i.e. the count of

Conversation Ring Endpoint

all packets where the endpoint was the source field in the packet.

Int

Int refers to bytes and packets that are sent from the host to itself (i.e. the IP source is the same as the destination).

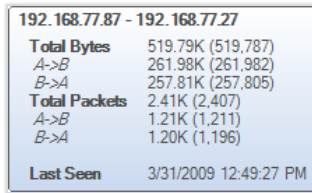
Ext

Ext refers to bytes and packets that are sent to or received from other hosts.

Last Seen

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

Conversation



192.168.77.87 - 192.168.77.27	
Total Bytes	519.79K (519,787)
A->B	261.98K (261,982)
B->A	257.81K (257,805)
Total Packets	2.41K (2,407)
A->B	1.21K (1,211)
B->A	1.20K (1,196)
Last Seen	3/31/2009 12:49:27 PM

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

Address(A)

The *Address(A)* refers to the source address in the first packet for that connection.

Address(B)

The *Address(B)* refers to the destination address in the first packet for that connection.

Total Bytes

The *Total Bytes* value refers to the total number of bytes sent between the source and destination addresses over the given sample period and is the sum of *A->B* and *B->A*.

A->B

The *A->B* value refers to the total number of bytes sent from the source address to the destination address over the view's sample period.

B->A

The *B->A* value refers to the total number of bytes sent from the destination address to the source address over the view's sample period.

TotalPackets

The *TotalPackets* value refers to the total number of packets sent between the source and destination addresses over the given sample period and is the sum of *A->B* and *B->A*.

Conversation Ring Conversation

A->B

The *A->B* value refers to the total number of packets sent from the source address to the destination address over the view's sample period.

B->A

The *B->A* value refers to the total number of packets sent from the destination address to the source address over the view's sample period.

Last Seen

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

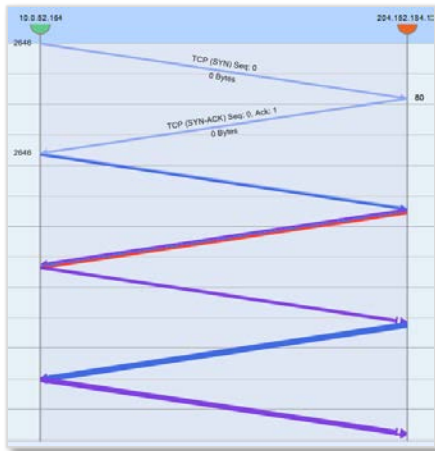
Sequence Diagram

The sequence diagram presents a sequential analysis of transactions and messages between hosts. The chart represents hosts as vertical lines arranged over the X axis, and messages as arrows between the hosts. The vertical axis represents time proceeding downward, which can be either relative (default) or absolute.

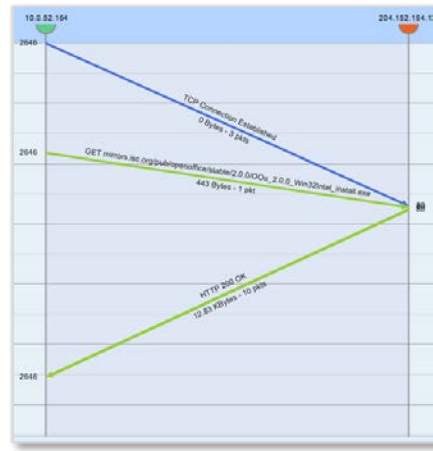
Layers

The chart can display data in one of two layers. The *Transport* layer displays each packet in the trace as a separate message in the sequence diagram. The *Application* layer decodes the packets for supported protocols and displays the protocol-specific messages. The user can toggle between these layers to gain different understandings of the underlying network transaction(s).

For example, the figures below show both the transport layer view and the application layer view for an HTTP download transaction. In the transport layer, separate message arrows show the three way TCP handshake to establish the connection, and then each data and acknowledgement packet in the exchange. In the application layer, on the other hand, only three messages are shown – one to establish the TCP connection, one to represent the HTTP GET request, and one to represent the HTTP response.



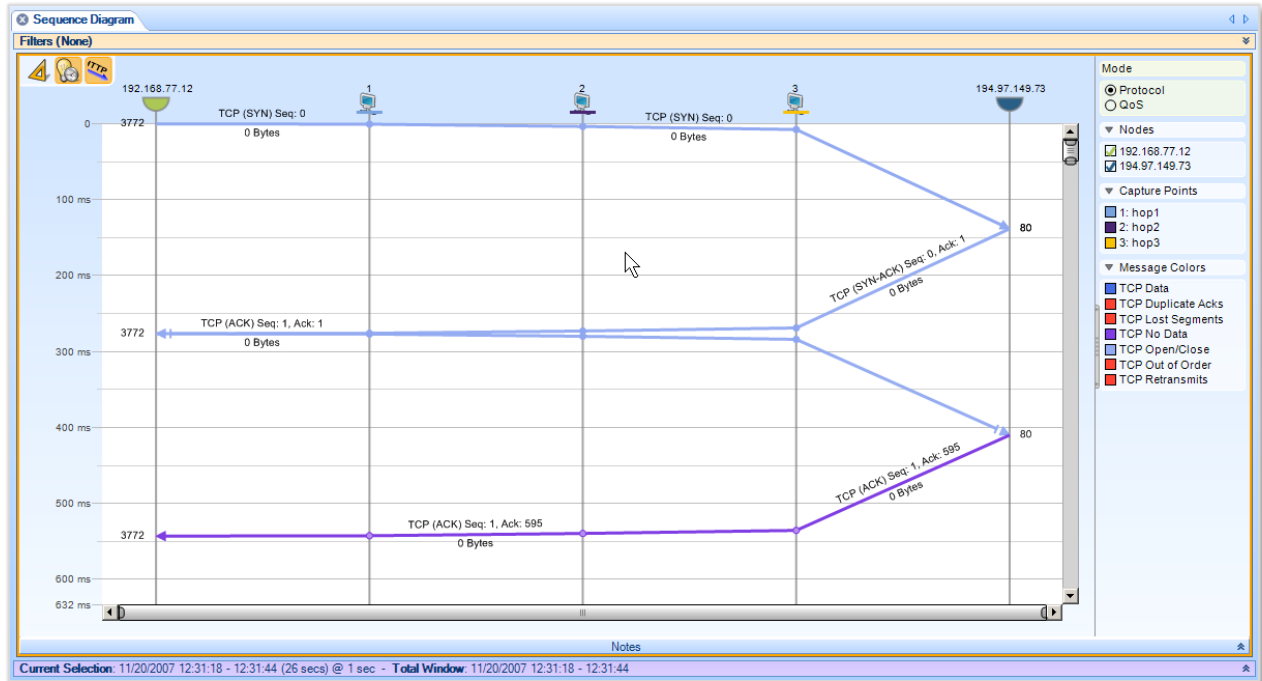
Transport Layer View



Application Layer View

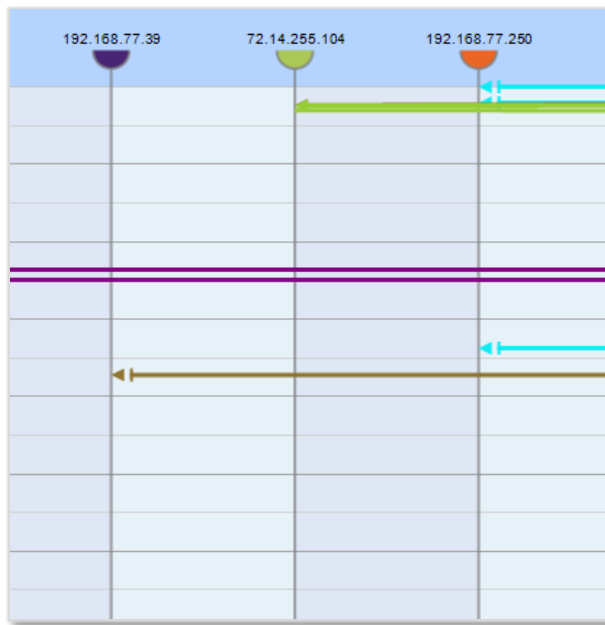
Multi-Segment Sequence Diagram

When a multi-segment sequence diagram view is applied to a multi-segment source, the resulting sequence diagram shows traffic between nodes across multiple segments in a network. In the following diagram, hosts are indicated by half-circles and capture points in the network are indicated by console icons



For additional information on multi-segment analysis, refer to the section on “Multi-Segment Analysis (MSA).”

Node



Sequence Diagram nodes

Nodes are visualized over the X axis and separated by columns of different shades of grey to emphasize the space among them.

A node is represented by three graphic objects:

Head

Half circles with a color for each host. Using the node head, it is possible to select, highlight and drag the node itself;

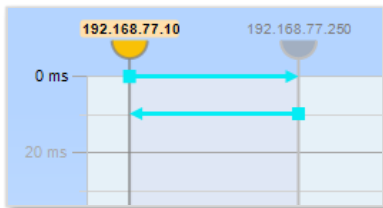
Body

Gray vertical line where messages arrive and leave; the body also allows selecting and highlighting the node itself;

Label

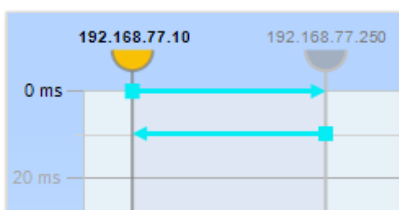
Node name, which is typically the IP address of the host or its resolved DNS name.

The node depiction varies based on selection and highlighting:



Selected node

If a node or message is selected (i.e. clicked), then the label is bolded and is given a background color. The label, head and body of all other nodes are grayed out.



Highlighted node

If a node is highlighted (i.e. by hovering the mouse on it), its label is bolded, and all other nodes are grayed out.



1 Dragged node

When dragging a node, it is represented as a transparent full circle head with no label. The node also stays in its original place until the drag is complete.

Node Layout

The Sequence Diagram has a minimum column width which constrains the total number of nodes that can be shown to ensure they can be displayed properly. When a view is applied, the graph selects a default initial column width, and using the horizontal scroll bar, the user can scroll and zoom to change the set of displayed nodes.

By default, the chart arranges the nodes from left to right based on the timestamp of the first message sent or received by the node. Users can override this ordering by dragging nodes and/or hiding nodes to reduce the number in the display.

Selection

When selecting a node, the selection includes all messages sent or received by the specific host. If multiple nodes are selected (by pressing Control key), the selection includes only messages between the set of selected nodes.

When holding the Shift key and selecting a node, the selection toggles among:

- All messages sent or received by the specific host;
- All messages sent by the selected host;
- All messages received by in the selected host.

Highlight

When highlighting (hovering over) a single node, the chart highlights all messages sent or received by the highlighted host. If multiple selection is enabled (by pressing the Control key) and at least one other node has been selected, the chart highlights only messages between the selected host(s) and the highlighted one.



Hide button

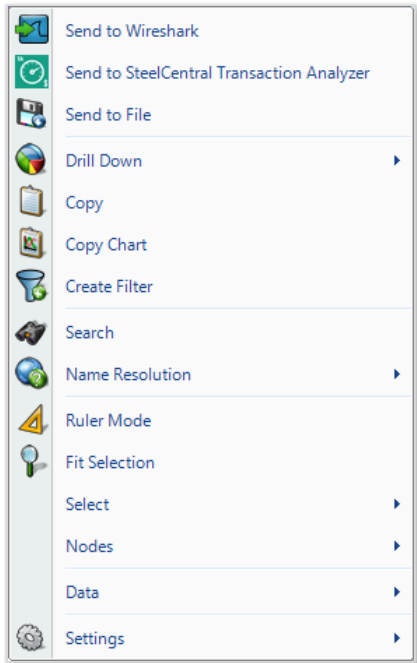
Also, when highlighting a host, the “Hide” button is shown to allow the user to hide the node itself, only if the column width is large enough to display it without overlapping the adjacent nodes.

Drag

As mentioned previously, users can manually arrange the order of the nodes by dragging hosts in different positions.

Additionally, the user can use the selection to define a filter by dragging the selected node(s) over the Filter panel or the Filter Bar. This action creates a Packet Analyzer filter for the selected host(s) and can then be used for additional views.

Context Menu



Node context menu

With one or more nodes selected, the context menu provides the following options:

Send to Wireshark

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

Send to SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected host(s) to Transaction Analyzer for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected host(s) to a user-specified trace file that 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 host(s) and opens a new view tab in the main workspace.

Copy

The *Copy* menu option copies a tabular form of the selected data to the system clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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.

Name Resolution

The *Name Resolution* menu option tries to identify unresolved IP addresses, ports, or MAC addresses from all or the selected nodes. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Ruler Mode

Ruler Mode displays detailed timing information about one or more messages. For more information, see the description of Ruler Mode (below).

Fit selection

The *Fit Selection* menu option arranges the horizontal range to fit the selected nodes.

Select

The *Select* menu option allows user to control which messages are selected based on the set of selected hosts. If only one host is selected, options include selecting all messages From or To the node, all messages From the node or all messages To the node.

If two nodes have been selected, options include Conversation between the selected nodes, all messages From the first node to the second or all messages From the second node to the first.

If more than two nodes are selected, the only option

is Conversation Between Selected Nodes.

Nodes

The *Node* menu provides options to control which nodes are hidden or shown.

Show All

Shows all hidden nodes.

Show Selected Only

Hides all nodes but the selected one(s).

Show All But Selected

Hide the selected nodes and show all others. Note that at least two nodes must be visible at all times.

Inverse

Inverts the hidden node set, by showing all hidden nodes and hiding all visible ones.

Data

Time Hints

Enables the sequence diagram to visually represent the network delay between nodes. For more information, see the description of Time Hints (below).

Absolute Time

Displays the actual time covered by the file.

Relative Time

Displays the time that has elapsed since the beginning time of the file.

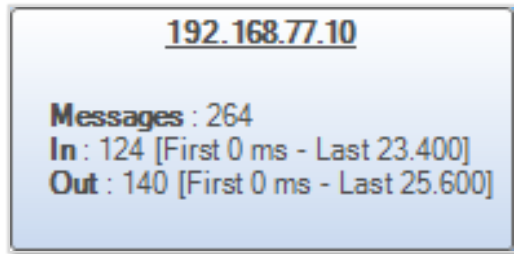
Settings

The Settings menu allows you to set two parameters that affect the sequence diagram display.

Show Legend

Show Labels

Tooltip



Node tooltip

The node tooltip shows data about the node itself.

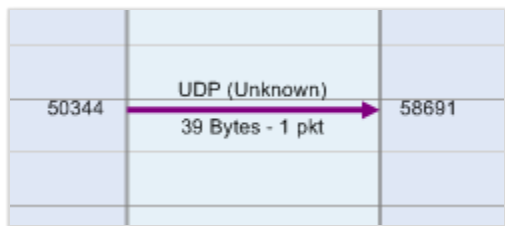
Node label

IP address of the highlighted node.

Messages

Statistics about the number of messages to and from the highlighted node, as well as timing information about the messages.

Message



Sequence message

A message is displayed as an arrow from the source host line to the destination host line.

The arrow itself is graphically composed by:

Shaft

Represents the body of the message as a line between source and destination nodes.

Head

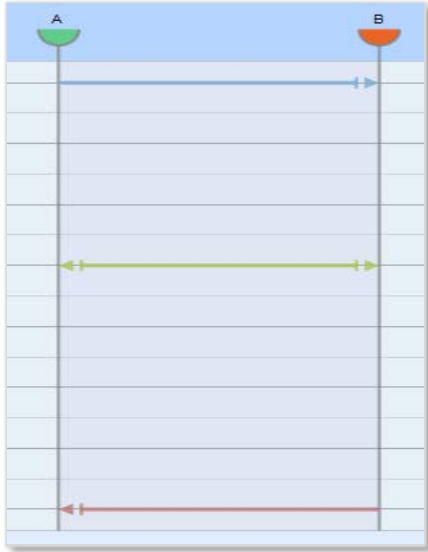
Represents the arrival of the message as a triangle pointing at the destination node.

Tail

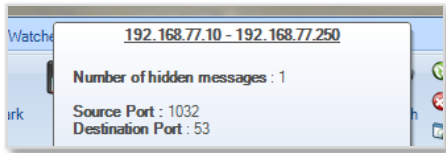
Represents the source of the message as a square at the source node (only in "Ruler Mode").

Labels

Shows text information about the message, including the protocol, packet and byte count, etc.



Filtered messages



Group message tooltip

Compression

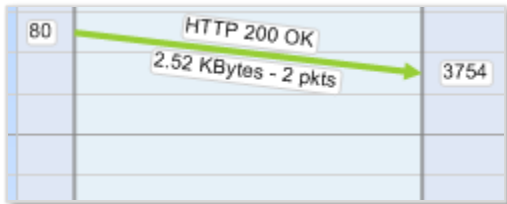
The diagram applies a compression algorithm over the set of messages to maximize performance and clarify the display. The algorithm can both reduce the number of displayed messages and change the message layout.

First, message labels are not displayed if there is not enough room to show them. Second, overlapping messages are combined into a group message. A group message uses a special head and tail to inform the user that it represents more than one message. A highlighted or selected group message does not show Top, Bottom and Main labels.

If all messages in the group have the same orientation, then the arrow is shown in one direction. Otherwise it is shown with head and tail in both directions.

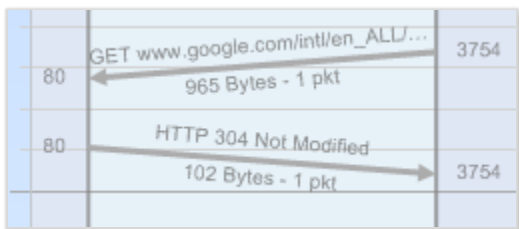
When all messages in a group have the same source and destination ports, then they are shown. Otherwise, they are not. The group message tooltip shows the number of hidden messages.

Message and node status



Highlighted message

If a message is selected or highlighted, it is brought to the foreground, increasing the likelihood that the label will be displayed.



Not focused message

Messages that are not selected or highlighted are greyed out to emphasize the selected ones.

Selection

Selecting one or more messages also selects the nodes that are the source or destination for one or more of the messages.

Highlight

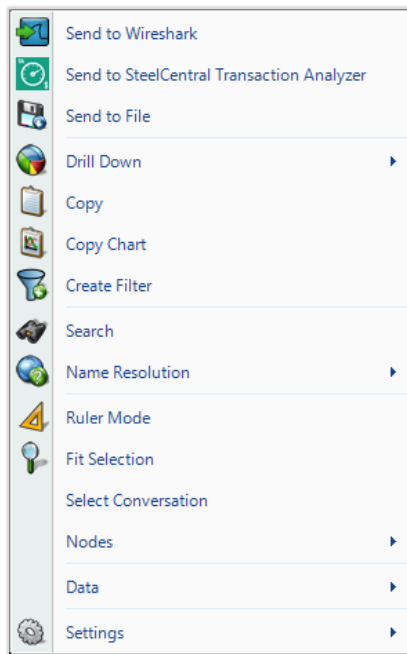
Highlighting a single message causes the chart to highlight the source and destination nodes.

Double click

Double clicking on a message toggles between the layers and zooms the display to fit the message in the time range.

Context Menu

By selecting one or more messages, the following actions can be performed through the context menu.



Message context menu

Send to Wireshark

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

Send to SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected message(s) to Transaction Analyzer for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected message(s) to a user-specified trace file that 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 message(s) and opens a new view tab in the main workspace.

Copy

The *Copy* menu option copies a tabular form of the selected data to the system clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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.

Name Resolution

The Name Resolution menu option tries to identify unresolved IP addresses, ports, or MAC addresses from all or the selected chart elements. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Ruler Mode

Ruler Mode displays detailed timing information about one or more messages. For more information, see the description of Ruler Mode (below).

Fit Selection

The *Fit Selection* menu option sets the horizontal range to fit the source and destination nodes and the vertical range to fit the start and end times of the selected message. If more than one message is selected then the minimum start time and maximum end time are used.

Select Conversation

The *Select Conversation* selects all messages with the same source and destination IP addresses and source and destination ports as the selected message.

Nodes

The *Node* menu provides options to control which nodes are hidden or shown.

Show All

Shows all hidden nodes.

Show Selected Only

Hides all nodes but the selected one(s).

Show All But Selected

Hide the selected nodes and show all others. Note that at least two nodes must be visible at all times.

Inverse

Inverts the hidden node set, by showing all hidden nodes and hiding all visible ones.

Data

Time Hints

Displays detailed timing information about one or more messages. For more information, see the description of Time Hints (below).

Absolute Time

Absolute Time displays the actual time covered by the file.

Relative Time

Relative Time displays the time that has elapsed since the beginning time of the file.

Settings

The Settings menu allows you to set two parameters that affect the sequence diagram display.

Show Legend

Show Labels

Tooltip

192.168.77.111 => 195.210.230.46	
(This message hides 3 messages)	
Source Port	54226
Destination Port	40282
Packet Description	UDP (Unknown)
Transfer Info	34 Bytes - 1 pkt
Start	3:28.658003 (11/20/2007 12:31:30.377745)
End	3:28.658003 (12:31:30.377745)
Range	0

Message tooltip

The message tooltip shows information about the message itself

Tooltip header

Comprises the source and destination IP addresses.

Tooltip body

Displays the port numbers, a description of the message, and its sizing information.

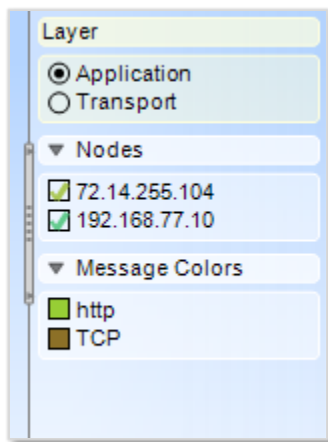
Tooltip footer

Shows statistics about the start and end time in both absolute and relative terms.

Legend area

The Legend area always occupies the right side of the chart. It contains a set of legends that show information about the displayed diagram and enable interaction with the chart. The legend can be resized by dragging the handle, or collapsed and expanded by double clicking the handle.

The legend area contains the following legends:



Sequence legend area

Layer

Shows the currently selected layer and enables switching between layers.

Nodes

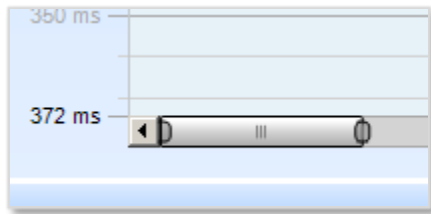
Checkbox list of nodes in the current sequence diagram. Enables selecting one or more hosts, highlighting a single host and hiding or showing a host by clicking the label icon.

Message Colors

List of colors used by messages in the current sequence layers and their meaning. Clicking on a color highlights all messages having the highlighted color.

Both the Message Colors and the Nodes legends can be expanded or collapsed by clicking the header.

Scroll bar



Scroll bar

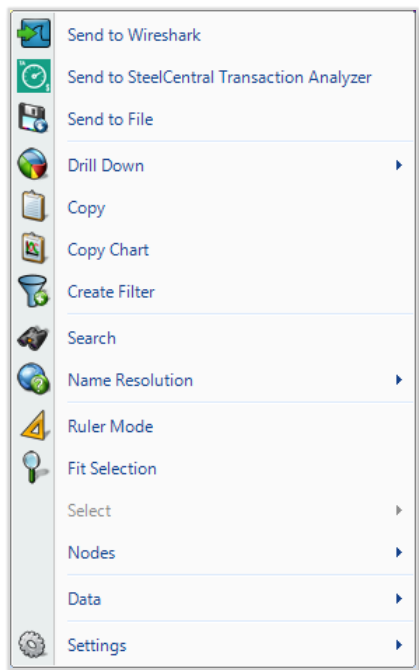
Scroll bars enable interaction with both the X and Y axis. In addition to panning left and right and up and down by dragging the scroll thumb, you can expand or contract the view by dragging the ends of the thumb.

Time Filter

By selecting a vertical region, the user selects a time range. All messages starting within the time range are displayed as selected.

Context Menu

In the time selection area is possible to perform the following actions:



Time Filter Context Menu

Send to Wireshark

The *Send to Wireshark* menu option sends all the traffic within the selected time range to Wireshark.

Send to SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends all the traffic within the selected time range to Transaction Analyzer for analysis.

Send to File

The *Send to File* menu option sends all the traffic within the selected time range to a user-specified trace file that 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 time range and opens a new view tab in the main workspace.

Copy

The *Copy to Clipboard* menu option copies a tabular form of the data within the selected time range to the system clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

Create Filter

The *Create Filter* menu option creates a time filter based on the current time selection.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Name Resolution

The Name Resolution menu option tries to identify unresolved IP addresses from all or the selected chart elements. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Ruler Mode

Ruler Mode displays detailed timing information about one or more messages. For more information, see the description of Ruler Mode (below).

Fit Selection

The *Fit Selection* menu option arranges the horizontal range to fit the selected nodes.

Select

Not applicable.

Nodes

The *Node* menu provides options to control which nodes are hidden or shown.

Show All

Shows all hidden nodes.

Show Selected Only

Hides all nodes but the selected one(s).

Show All But Selected

Hide the selected nodes and show all others. Note that at least two nodes must be visible at all times.

Inverse

Inverts the hidden node set, by showing all hidden nodes and hiding all visible ones.

Data

Time Hints

Enables the sequence diagram to visually represent the network delay between nodes. For more information, see the description of Time Hints (below).

Absolute Time

Displays the actual time covered by the file.

Relative Time

Displays the time that has elapsed since the beginning time of the file.

Settings

The Settings menu allows you to set two parameters that affect the sequence diagram display.

Show Legend

Show Labels

Double Click

Double click expands the current time range to reflect the time filter range.

Dragging

The time selection can be used to create a time filter by dragging it on the Filter panel or the Filter Bar. Also, dragging the time selection onto a different Sequence Diagram or Strip Chart highlights the messages in the other chart that fall within the selected time range.

A time selection can be removed by clicking on the area outside the hosts grid or, after a double-click, by clicking over the area itself.

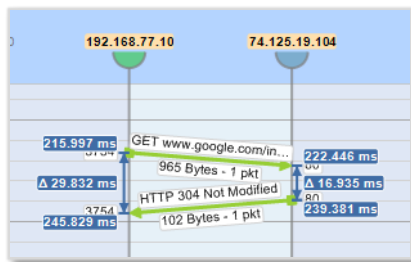
Ruler Mode

Ruler mode displays detailed timing information about one or more messages. It is activated by clicking the mode icon.



Ruler Mode Icon

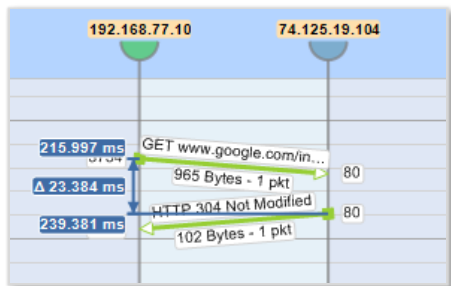
The system shows timing information in two modes:



Node ruler mode

Node Mode

When a message is selected or a time range is created, the diagram shows the start time, end time and delta value between the first and the last message in the range.



Global ruler mode

Message Mode

When a first message terminator (head or tail) is clicked, followed a second terminator, the system shows the timing of the two messages as well as the interval between them.

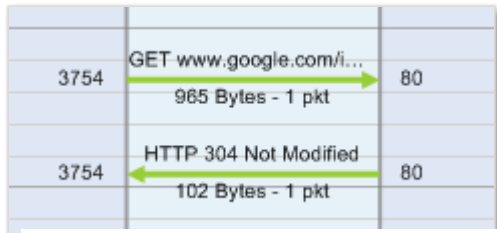
If a **third terminator** is selected, the initial selection is retained, and the system updates to show the timing information between the first message terminator and the newly clicked one. Selecting another message or clicking in the background will clear the original selection.

Time Hints

Time hints enable the sequence diagram to visually represent the network delay between nodes. The feature is activated or deactivated using the icon in the upper-left corner of the chart.

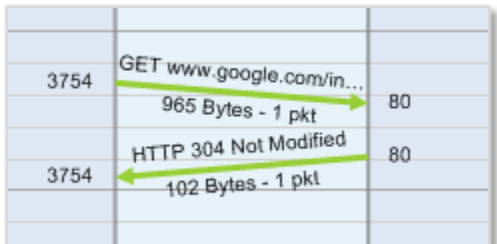


Time Hints Icon



Time without hints

When time hints are disabled, all messages are shown as horizontal lines, where the Y axis value represents the message timestamp as recorded in the trace file.



Time with hints

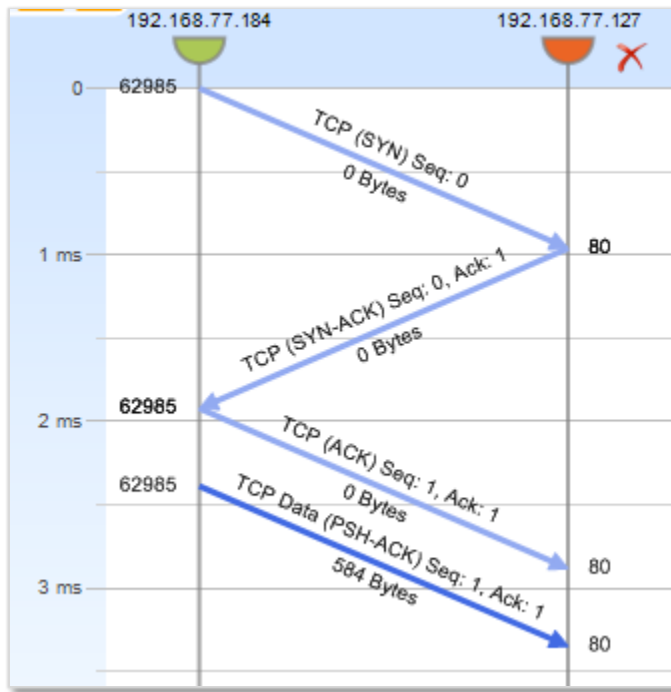
When time hints are enabled, the network delay is inferred from the TCP calculations, and the message lines are drawn with a slope that illustrates the network delay.

Message Labels

Message labels show information about the message: protocol, byte count, and so on. The feature is activated or deactivated using the icon in the upper-left corner of the chart.



Message Label Icon



Typical message labels

Strip Chart

The Strip Chart displays quantitative data with respect to time.

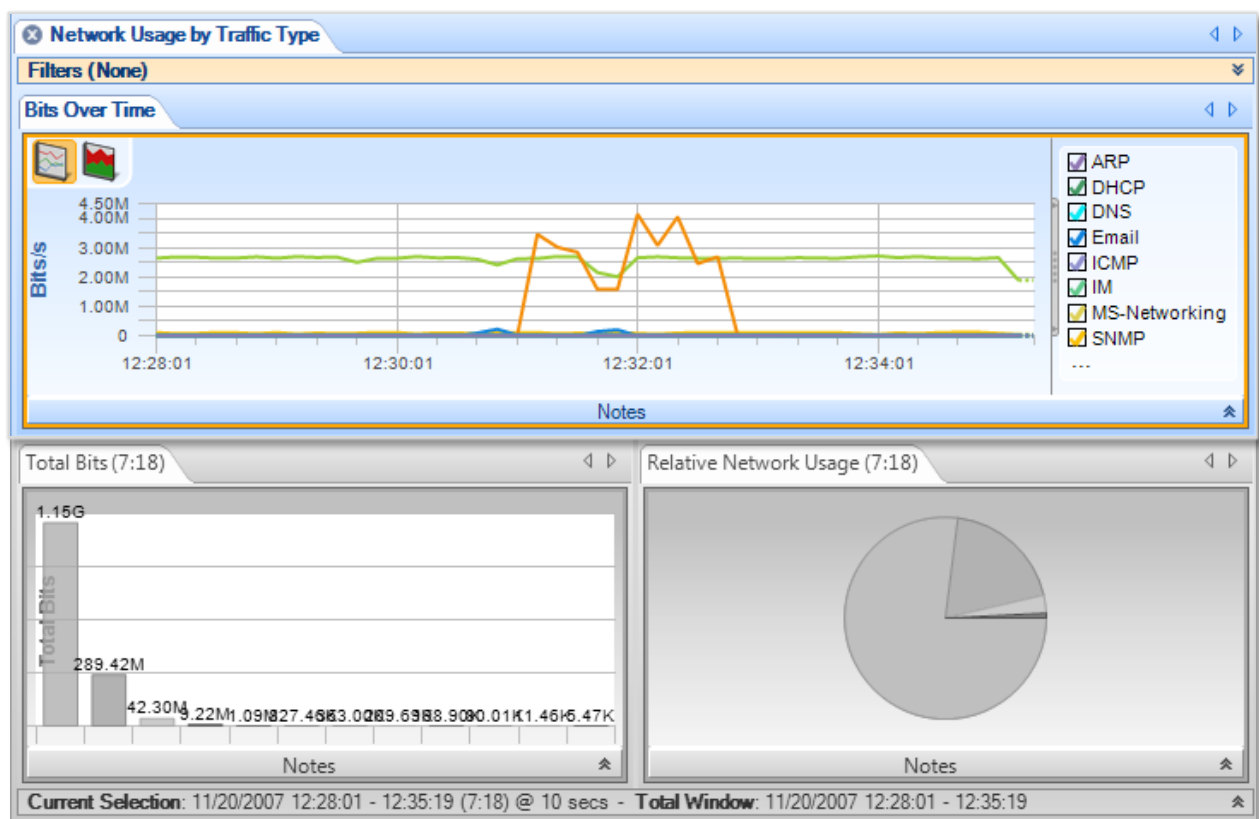
Diagram

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:



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 above shows 3 charts, namely a strip chart, a bar chart, and a pie chart. This section discusses 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 shows the total duration of the source trace file or, for a live source, the total duration of the capture or the Data Retention Time, whichever is smaller.

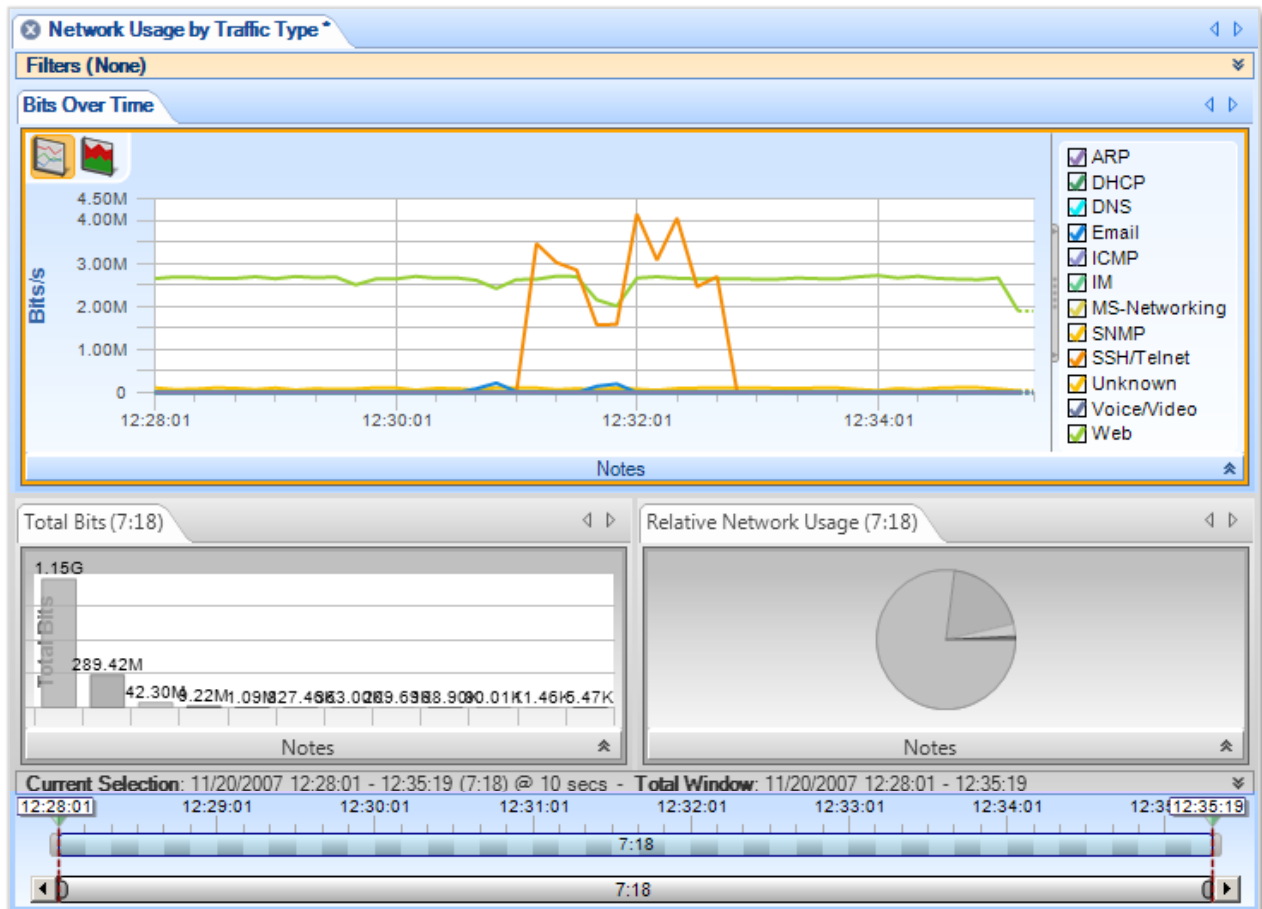


Figure 44. Strip Chart with Horizontal Zoom

Figure 44 shows the strip chart “zoomed” horizontally using the Selection bar in the Time Window. The Time Control Ribbon can also be used to set the duration and location of the Current Selection. The minimum and maximum values in the Current Selection are displayed (unless they are obvious from the context).

The Selection Bar (upper bar) controls the portion of the data (trace file or live capture) that is displayed in the charts. Move the triangular markers above the ends of the Selection Bar to trim the time interval that is displayed.

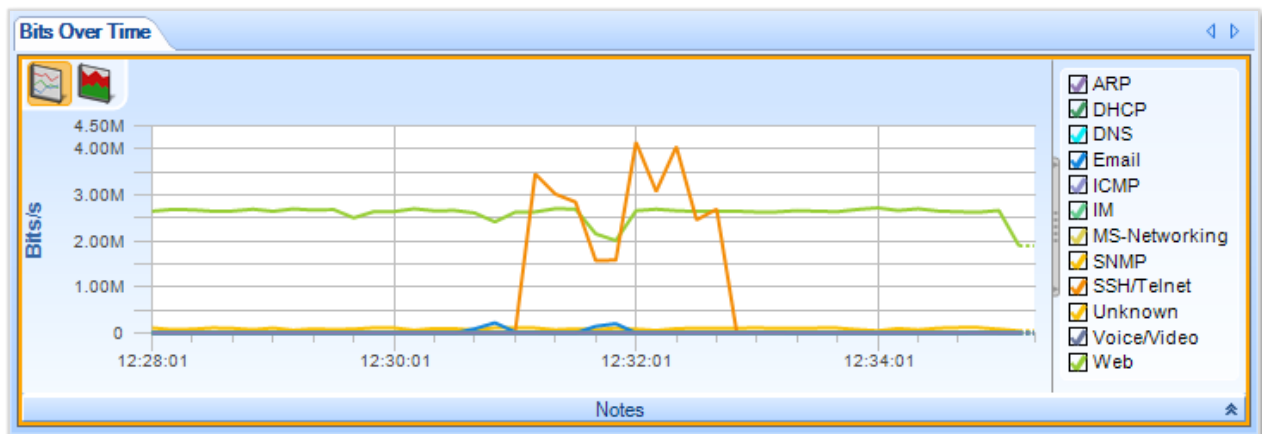
The Time Scroll Bar (lower bar) controls the resolution of the upper bar. As you bring the ends of the bar in toward the center, the time scale in the upper bar expands, allowing you to make finer selections of time intervals using the upper bar.

Along with the “Sampling Time” and “Data Retention Time” options as previously described, the Strip Chart can be customized using the chart context menu:

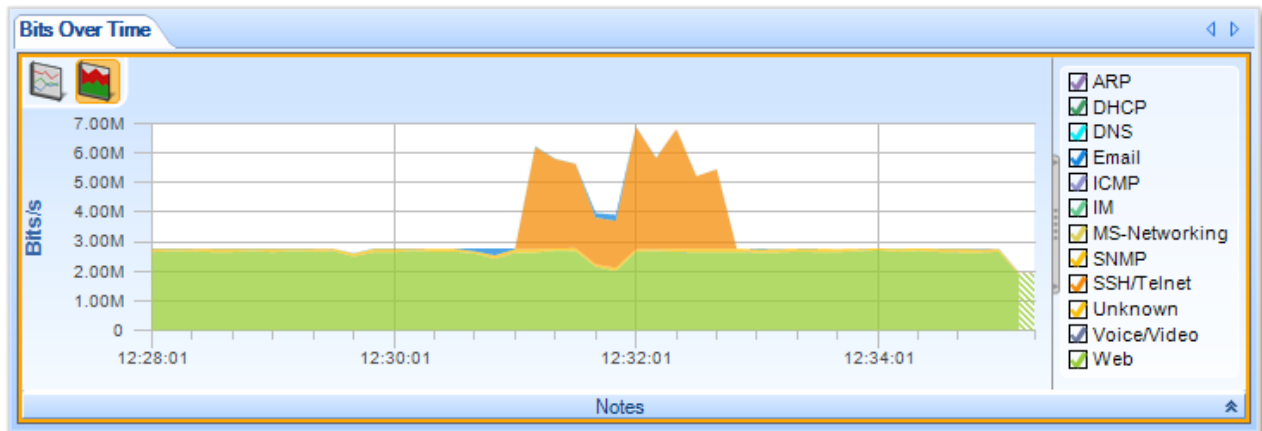
- Toggling display mode (line chart or stacked area chart)
- Selecting data sources to be displayed
- Changing the stacking order (stacked area mode only)
- Toggle legend visibility
- Displaying Min and Max values
- Rescaling Y Axis

Display Modes

There are two display modes for strip charts: normal (line) mode and stacked area mode. Normal mode is the default.



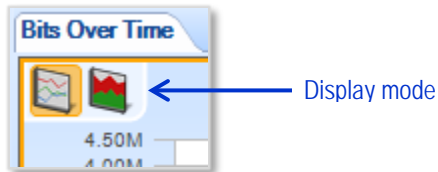
Normal strip chart



Stacked area strip chart

In the normal (line) chart, each data point's value at a given time is plotted relative to zero. In the stacked area chart, each data point's value at a given time is plotted relative to the value of the data in the layer below.

To switch from one mode to the other, click one of the display mode buttons in the upper left corner of the strip chart:

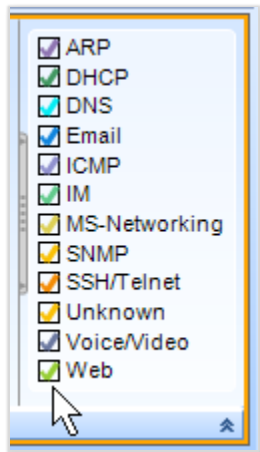


Alternatively, you can choose the display mode from the context menu (described below).

To display a strip chart in stacked area mode by default, set the view to stacked area mode and save it as a custom view. (Click the Save button in the View section of the Home tab.) When you drag the custom view onto your data of interest, the strip chart displays in stacked area mode.

Data Display

You can show or hide lines or areas of data by checking or unchecking the boxes in the legend area to the right of the data area.



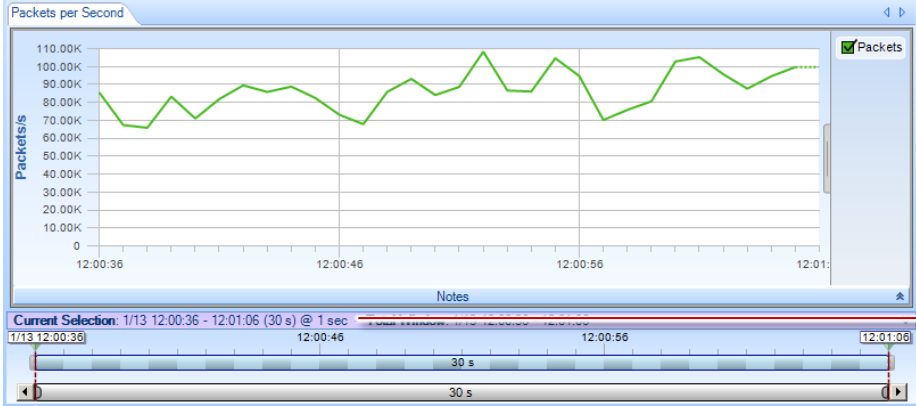
Stacking Order

You can change the stacking order of areas in a stacked area chart by dragging the labels up or down in the legend area to the right of the data area.

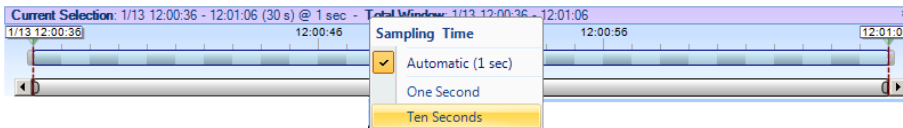


Custom sampling interval

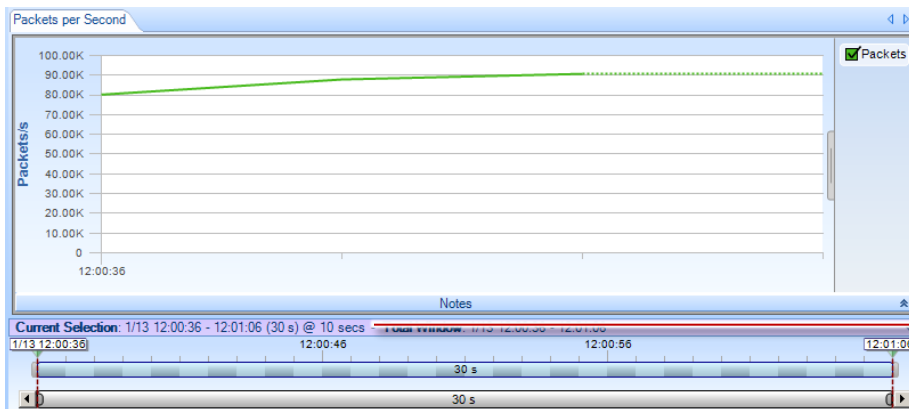
By default, the sampling interval for a strip chart is calculated automatically by Packet Analyzer.



A context menu in the time control bar shows the current sampling interval and allows you to select a different one. The allowed sampling intervals are calculated based on display considerations.



The strip chart is recalculated using the new sampling interval.



Manually selected
sampling interval

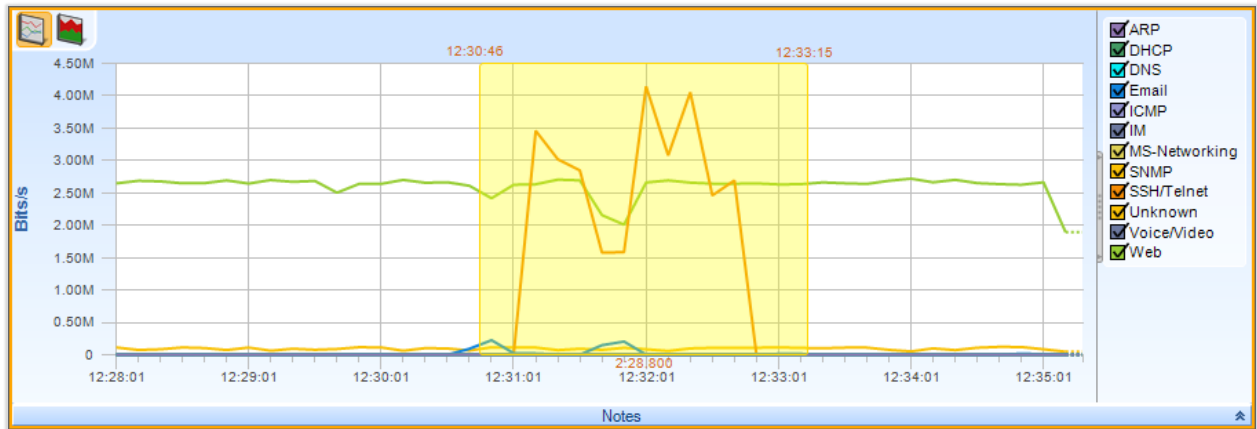
Selection

The Strip Chart supports two types of selection:

- Time-based
- Line- or area-based

Time-Based Selection

A *Time-Based Selection* can be applied to any Strip Chart and is performed by clicking and dragging the mouse over a time period. An example result is shown below:

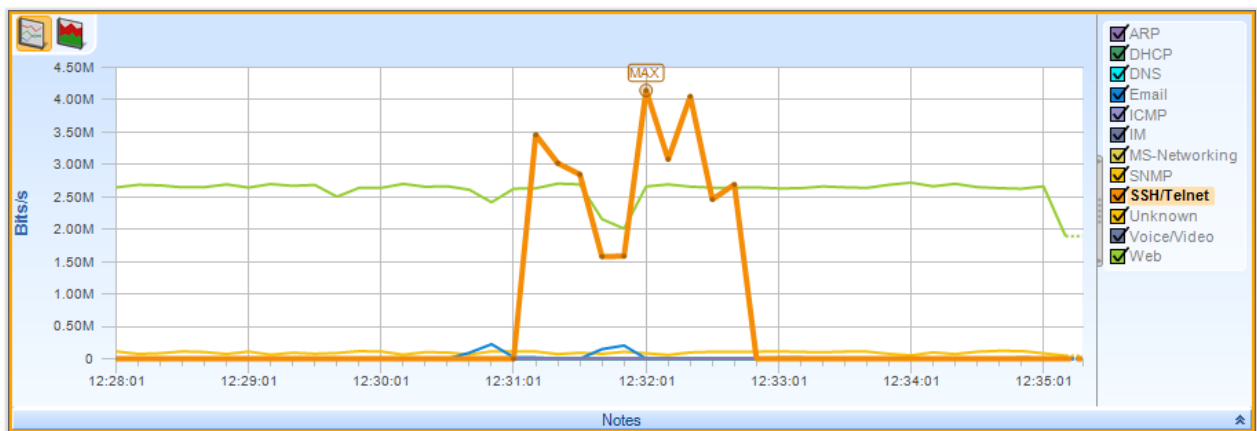


Strip Chart Selection (Time)

Note that multiple selection cannot be performed using time-based selection.

Line- or Area-Based Selection

A *Line- or Area-Based Selection* can be applied to Strip Charts where more than one metric is being displayed, for example in the case of multiple protocols over time:

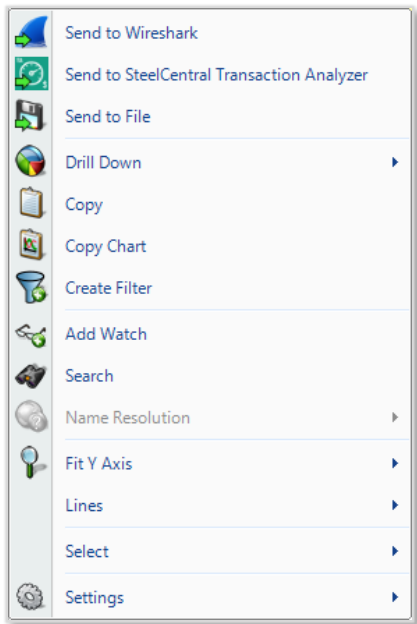


Strip Chart Selection (Element)

Individual lines or areas are selected by clicking either on the line or area itself, or on its representation in the legend. Multiple lines or areas can be selected by clicking with the Control key pressed.

Context Menu

The context menu for a strip chart has the following options:



**Context menu
(selection)**

Send to Wireshark

Sends traffic from the selected time slice or lines/areas to Wireshark for analysis.

Send to SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected time slice or lines/areas to Transaction Analyzer for analysis.

Send to File

Sends traffic from the selected time slice or lines/areas to a user-specified trace file that will appear, after completion, in the Files panel, for immediate analysis.

Drill Down

Applies the user-specified view to the selected time slice or lines/areas and opens a new view tab in the main workspace.

Copy

Copies a tabular form of the selected data to the system clipboard.

Copy Chart

The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

Create Filter

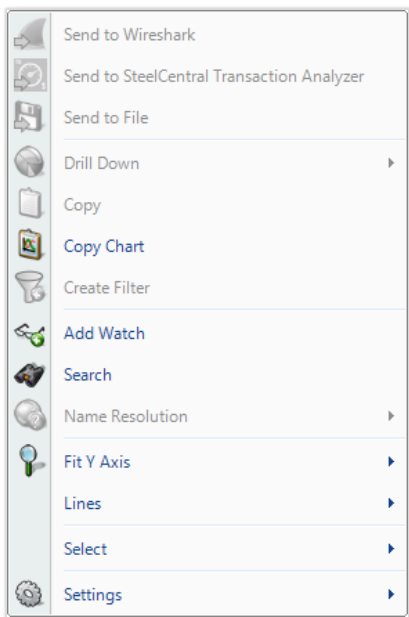
Creates a filter based on the current selection and adds the filter to the Filter List.

Add watch

Opens 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.

Search

Opens a search dialog window that can be used to find data in the charts.



**Context menu
(no selection)**

Name Resolution

The Name Resolution menu option tries to identify the port name, IP address, or MAC address of all or the selected elements in the strip chart. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Fit Y Axis

Scales the vertical height of the strip chart to fit within the chart. Default is Fit All.

Fit All

Y Axis is fit to the currently available strips.

Fit Selected Only

Y axis is fit to the selected strips. Strips must be selected before this choice is available.

Lines

The *Lines* submenu allows you to choose what lines are displayed.

Show All

Shows all hidden lines.

Show Selected Only

Hides all lines but the selected one(s).

Show All But Selected

Hide the selected line(s) and show all others. Note that at least two lines must be visible at all times.

Inverse

Inverts the hidden line set, by showing all hidden lines and hiding all visible ones.

Select

Brings up two submenu options:

Select All

Selects all lines or areas.

Select Inverse

Selects all lines or areas that are not currently selected (and deselects those that are currently selected).

Settings

Brings up three submenu options:

Show Legend

Shows the legend area to the right of the strip chart, indicating which data sets correspond to which lines or areas.

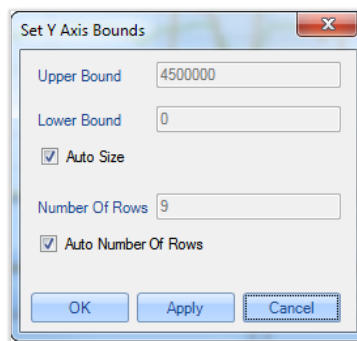
Show Min/ Max

Shows a minimum point and a maximum point for each data set on the chart:



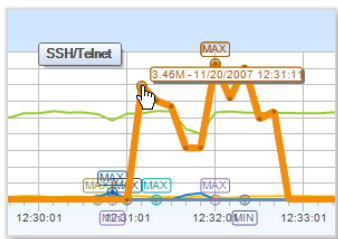
Setup Y Axis

Brings up the dialog for setting up the Y axis. You can set the upper and lower bounds of the Y axis, or choose Auto Size to let Packet Analyzer choose the bounds automatically. And you can specify the number of increments displayed on the Y axis, or choose Auto Number of Rows to let Packet Analyzer choose the number of rows automatically.



Tooltips

The tooltips for the Strip Chart show the full quantitative value of a specific sample point of the element in the data area. Hover your mouse over a sample point to see its value.



Bar Chart

This chart 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

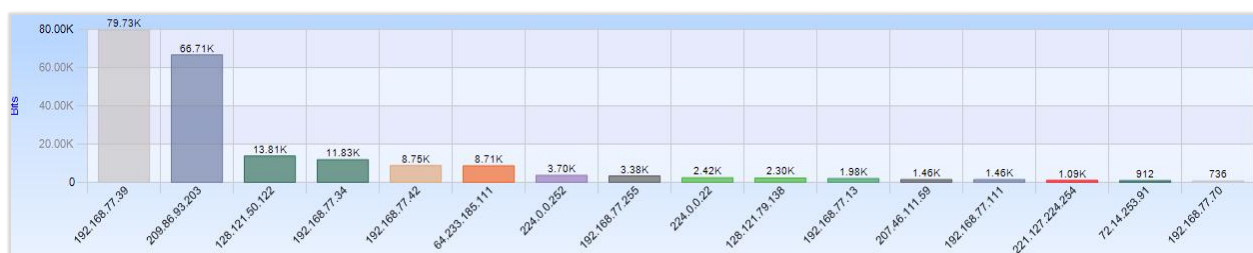
Single Bar Charts are the most basic form of Bar Charts. Each column is a single valued bar. The colors of the bars match the labels in the legend.

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

- Reorder Bars
- Toggle legend visibility
- Toggle label visibility above individual bars
- Select value or percentage as label

Default

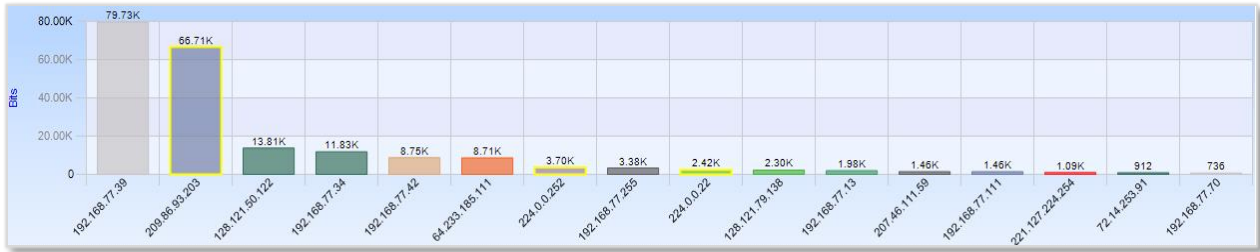
This is an example of the default view for a Single Bar Chart:



Single Bar Chart

Selection

A bar in a Single Bar Chart is selected by clicking on the bar itself, its column, or its representation in the legend. Clicking with the Control key pressed is supported for multiple selection.



Bar Chart Multiple Selection

Stacked Bar Chart

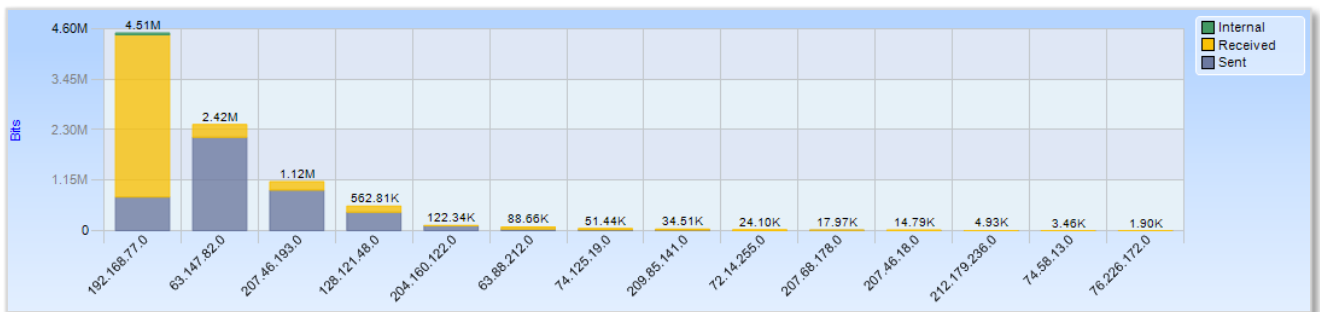
A *Stacked Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into predetermined constituents. These constituent components can be selected and analyzed individually or collectively.

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

- Sort Bars
- 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:



Stacked Bar Chart

Selection

A bar in a Stacked Bar Chart is selected by clicking on the bar itself, its column, or its representation in the legend. Clicking with the Control key pressed is supported for multiple selection.

Grouped Bar Chart

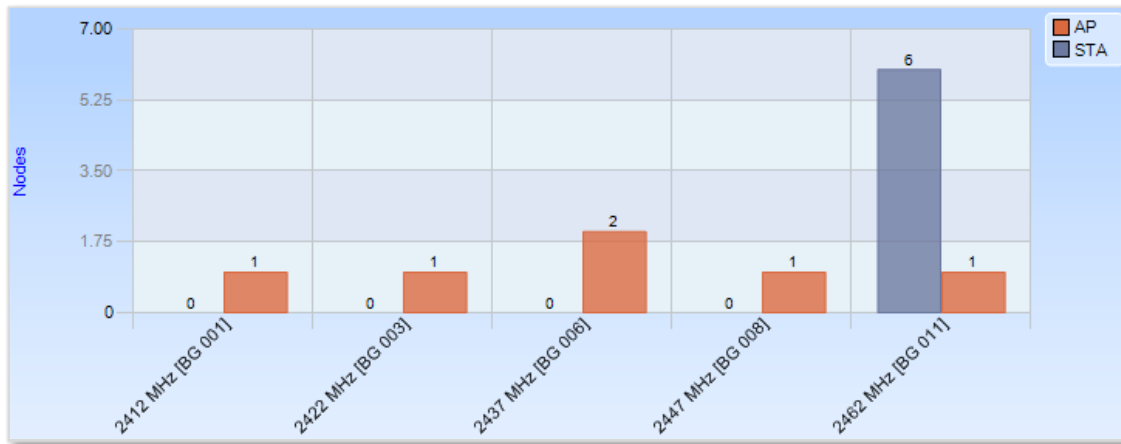
A *Grouped Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into two or more sub columns.

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

- Sort Bars
- Toggle legend visibility
- Toggle 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:



Grouped Bar Chart

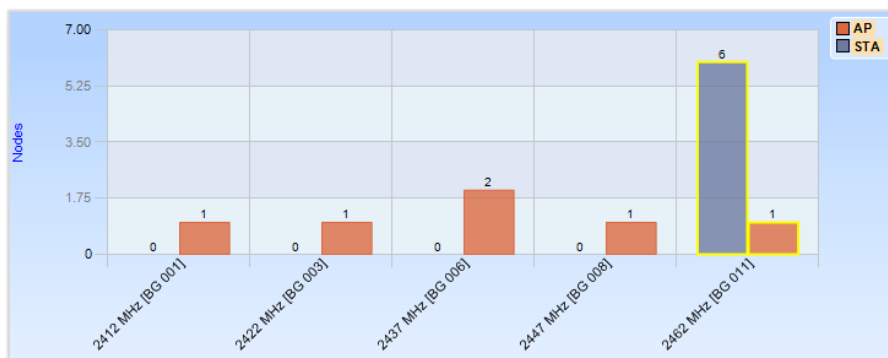
Selection

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

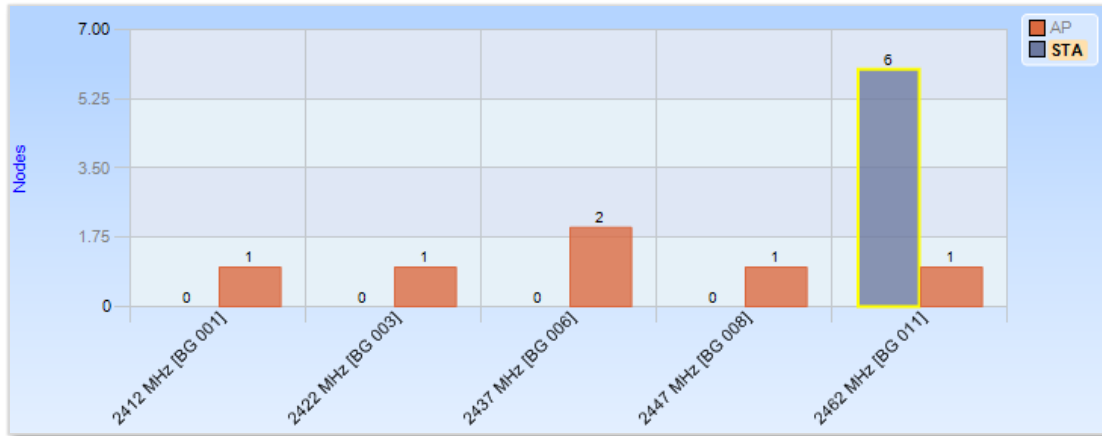
A *column based* selection selects all data corresponding to the column. This method of selection is achieved by selecting the area around the bar with respect to the desired column inside the chart, but not the bar itself.



Grouped Bar Chart Selection (Column)

Component Instance

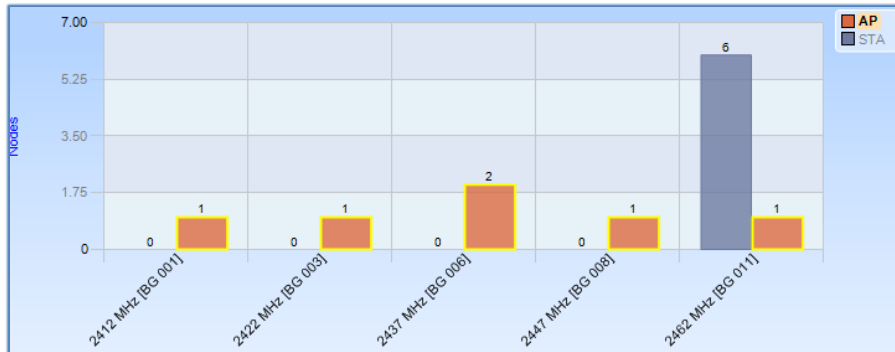
A *component instance based* selection selects a subset of the data in a particular column. This method of selection is achieved by clicking on the component.



Grouped Bar Chart Selection (Component Instance)

Component

A *component based* selection selects data in all columns for a particular component subset. This method of selection is achieved by clicking on the representation of the component in the legend.



Grouped Bar Chart Selection (Component)

Navigation Through Data



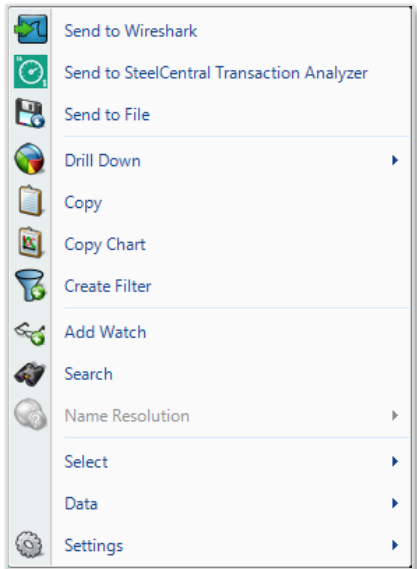
Bar chart Top Bars

When there is not enough space to display clearly all the bars in a single chart, the system automatically ranks and displays data by relevance, based on the selected sorting option.

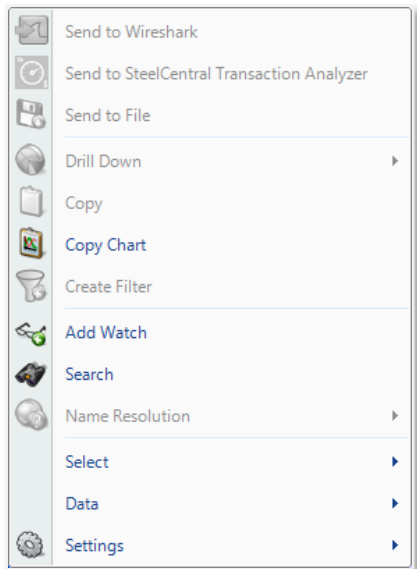
By default, the columns are sorted from high to low (usually by value). A small label displaying the total number of bars and the current interval is shown at the bottom of the view. One can navigate through data using the four buttons in the label. + and - buttons increase or decrease the length of 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.



Bar Chart (Selection)



Bar Chart (No Selection)

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 SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the selected bar(s) or component(s) to Transaction Analyzer 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 that 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

The *Copy* menu option copies a tabular form of the selected data to the system clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

Create Filter

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

Add Watch

The *Add Watch* menu option opens 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).

Search

The *Search* menu option opens a search dialog window to find data in the charts.

Name Resolution

The Name Resolution menu option tries to identify

unresolved IP addresses, ports, or MAC addresses from all or the selected bars. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Select

The *Select* menu option provides the option to select the bar(s) and component(s) of the Bar Chart.

Select All

Selects all bars in the chart.

Select Inverse

Deselects the currently selected bar(S) and selects all other bars.

Data

The *Data* menu option provides choices for how chart data is displayed and sorted.

Percentage

Sorts the bars numerically by their percentage of the total traffic.

Value

Sorts the bars numerically by their quantitative values.

Default

Reverts to the original sorting order.

Sort By Label

Sorts the bars alphabetically by their labeled column names.

Sort By Value

Sorts the bars numerically by their quantitative values.

Descending

Sorts the bars sequentially from left to right, either by name or value, as specified by the first group.

Ascending

Sorts the bars sequentially from right to left, either by name or value, as specified in the first group.

Show Previous/Next Bars

When there are more bars than will fit in the display area, selecting this option displays a Previous bar and/or a Next bar. These bars show cumulative totals for all bars that come before and/or after the bars displayed in the current view.

Settings

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

Show Legend

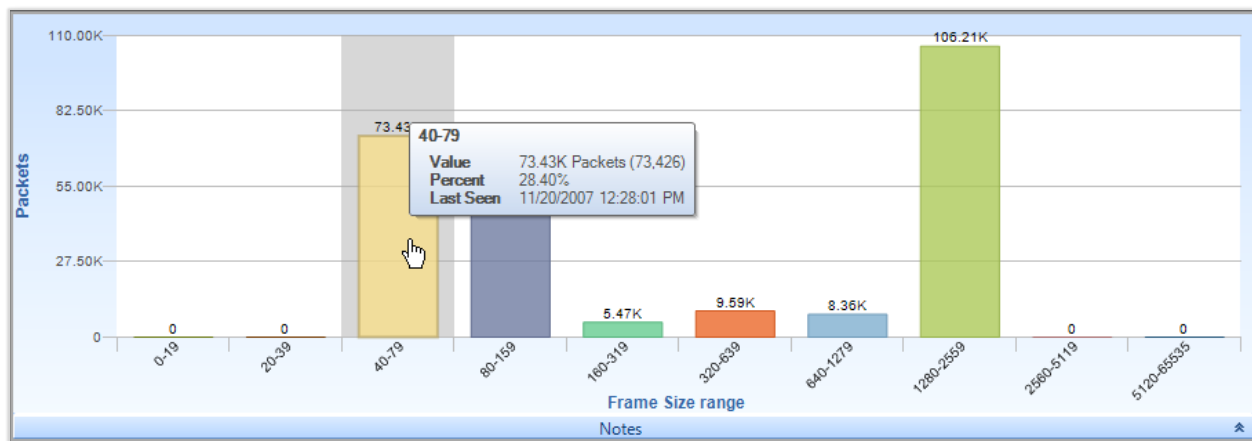
Toggles off or on the Bar Chart legend.

Show Labels

Toggles off or on the labels on each bar on a Bar Chart.

Tooltips

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



Scatter Plot

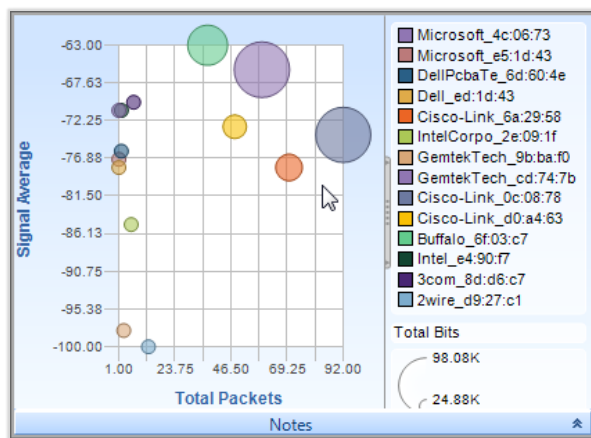
The *Scatter Plot* is a versatile and flexible chart that can display complex relationships between values using three dimensions:

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

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

Scatter Plots are most useful when there is expected to be a correlation between metrics, such as the total number of packets and the total bytes sent out by a host. For example, if the Y Axis is “Packet Count” and the X Axis is “Byte Count,” then there is typically a diagonal line of points from the origin to the top right. An anomaly would then be visually evident if this relationship did not hold for certain situations.

Default

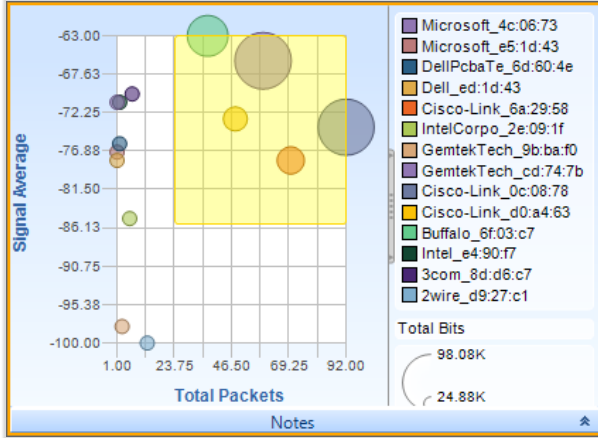


Scatter Plot

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

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

Selection

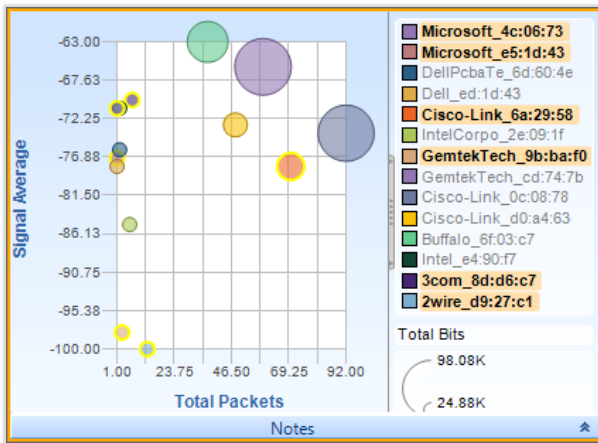


Selection in a Scatter Plot is done by one of four ways:

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

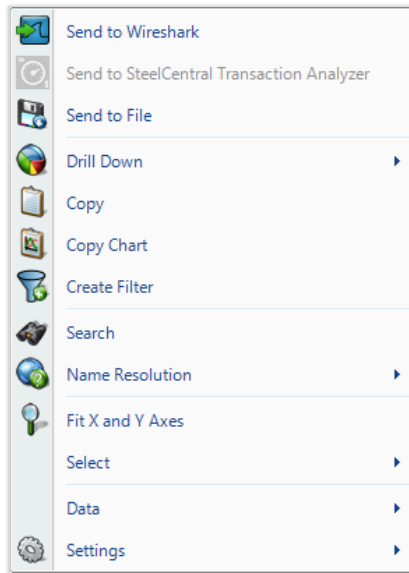
Clicking with the Control key pressed for multiple selection is supported for point based and legend based selection.

Scatter Plot with Draw Box



Scatter Plot with Multiple Selections

Context Menu



Scatter Plot (Selection)

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 SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected point(s) to Transaction Analyzer 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 that 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

The *Copy* menu option copies a tabular form of the selected data to the system clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

Create Filter

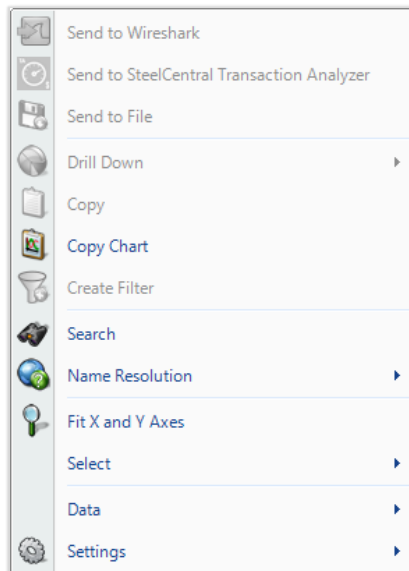
The *Create Filter* menu option creates a filter based on the current selection within the scatter plot and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Name Resolution

The *Name Resolution* 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 fields are not automatically resolved (see the Name Resolution submenu available in the Home Ribbon). Default is from Settings menu.



Scatter Plot (No Selection)

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

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 all values fit within the chart.

Select

The *Select* menu option has two submenu options.

Select All

Selects all the point(s) in the Scatter Plot.

Select Inverse

Inverts the selection of point(s).

Data

The *Data* menu option provides choices for how chart data is displayed and sorted.

X Axis

Presents all possible choices for the metric of the X-Axis. Some charts may only have one option, while others may have multiple; for instance, "Bits/s" versus "Bytes/s" or "Packets/s."

Y Axis

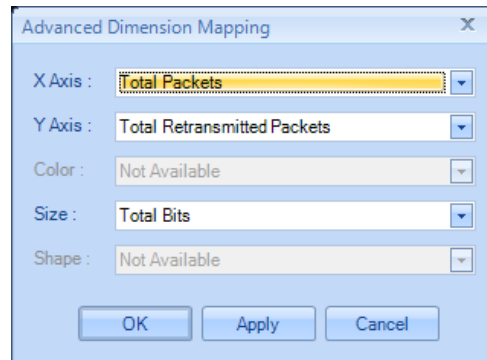
Presents all possible choices for the metric of the Y-Axis. Some charts may only have one option, while others may have multiple; for instance, "Bits/s" versus "Bytes/s" or "Packets/s."

Size

The dot size of the points can be enabled and associated with a metric or disabled by selecting "Nothing."

Advanced

Opens up a separate dialog box where drop-down lists provide options for a chart's format.



Settings

The *Settings* menu option provides choices on how a chart is displayed.

Show Legend

Toggles off or on the Scatter Plot legend.

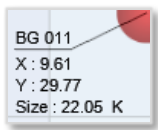
Show Labels

Toggles off and on the point labels, which can otherwise be viewed via a tooltip.

Autosize

Toggles off and on whether the area will automatically resize based on maximum values.

Tooltips



Scatter Plot

A tooltip is shown 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.

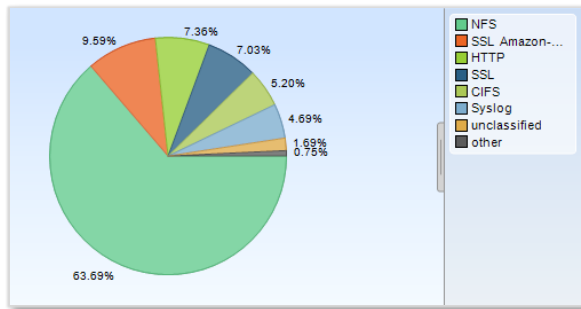
Size

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



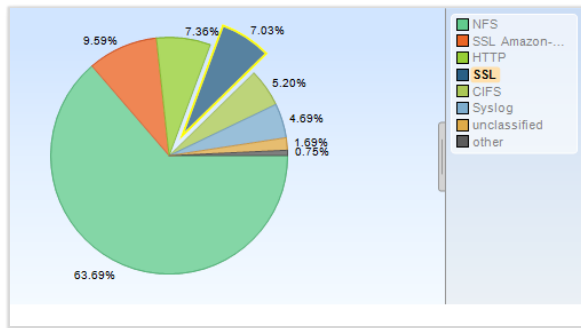
Pie Chart

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

- 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.

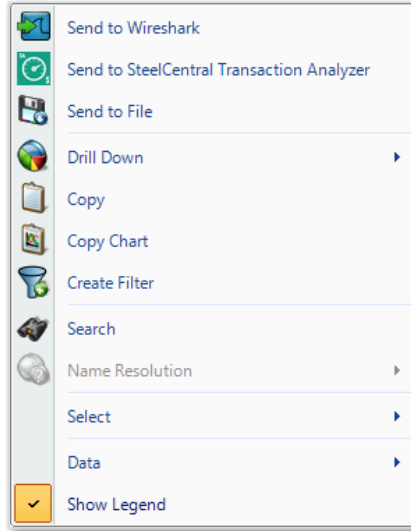
Selection



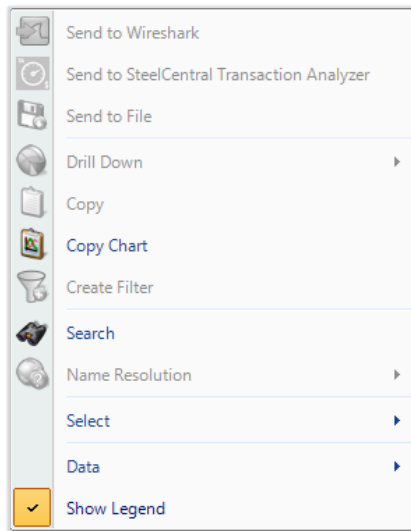
Pie Chart Selection

Selection in a Pie Chart is done either by clicking on a slice in the Pie Chart or on its representation in the legend. Clicking with the Control key pressed for multiple selections is supported.

Context Menu



Pie Chart (Selection)



Pie Chart (No Selection)

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 SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected slice(s) to Transaction Analyzer 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 that 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

The *Copy* menu option copies a tabular form of the data to the system clipboard.

Copy Chart

The *Copy Chart* menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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.

Name Resolution

The *Name Resolution* menu option resolves, when applicable, the Port Name, IP Address, or MAC Address of the slice(s) in the Pie Chart. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Select

The *Select* menu option has two submenu options.

Select All

Selects all slices in the pie chart.

Select Inverse

Deselects the currently selected slice(s) and selects all others.

Data

The *Data* menu option provides choices on how data are displayed in the chart.

Percentage

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

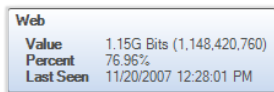
Value

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

Show Legend

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

Tooltips



Web	
Value	1.15G Bits (1,148,420,760)
Percent	76.96%
Last Seen	11/20/2007 12:28:01 PM

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.

Pie Chart Tooltip

Data Grid

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

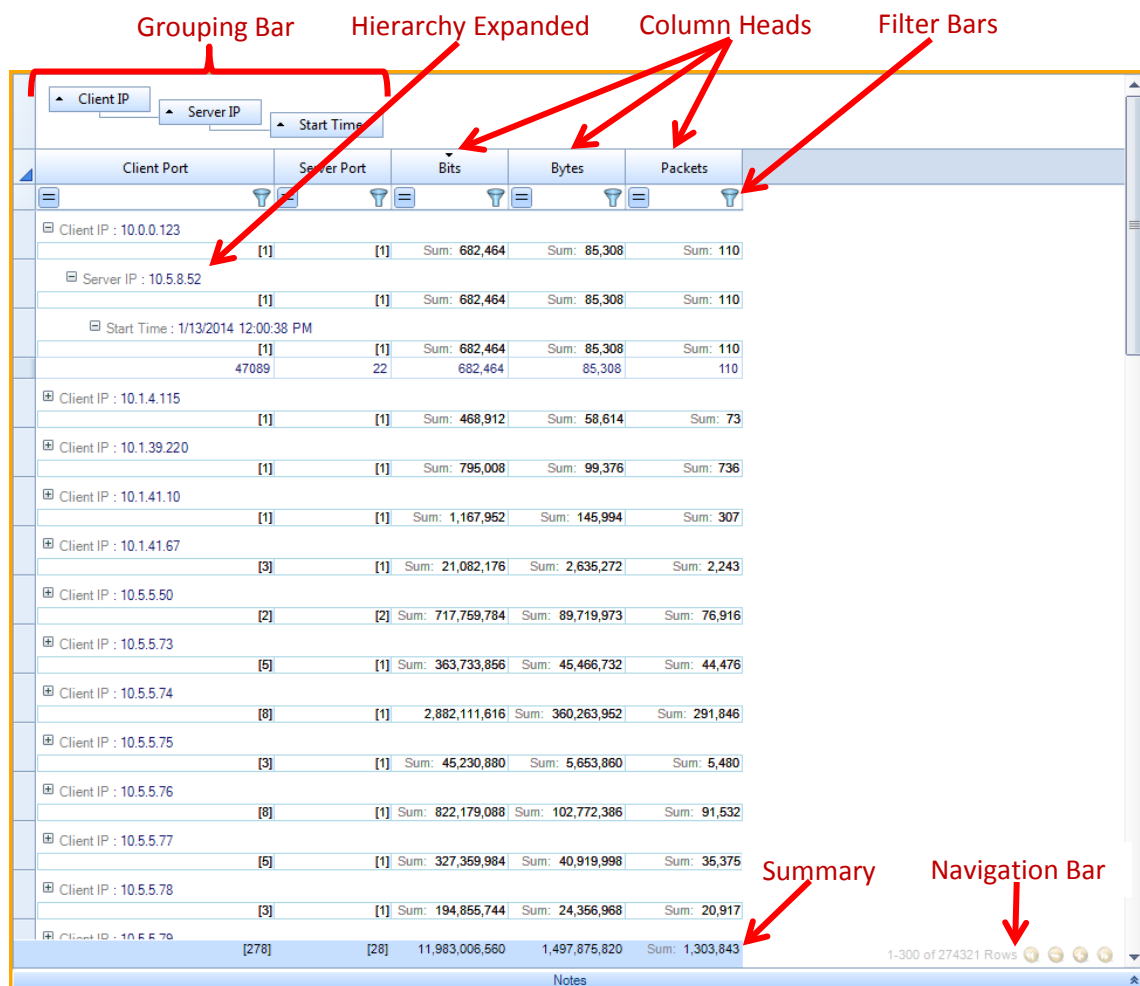
The columns can be:

- Rearranged in any order
- Resized
- Hidden and shown

The rows can be:

- Filtered
- Sorted by one or multiple columns simultaneously
- Hierarchically grouped
- Summarized by selection, group, or the entire table.

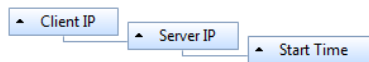
The figure below shows an example grid with a number of features enabled and some grid components identified.



Grid

Grouping Bar

The elements of the *Grouping Bar*, called groups, determine the row hierarchy. In the above example, columns in the view Performance and Errors>TCP>Connections and Requests> TCP Traffic Details by Connection have been dragged into the Grouping Bar to group the TCP traffic connections and metrics. The root level contains the Client IP. Each Client IP can be expanded to show the Server IP, which can in turn be expanded to show the Start Time.



Grid Grouping Bar

Each element of the Grouping Bar also has a triangle before each group that specifies the sorting order of that level of the hierarchy. The order can be toggled by clicking on the group itself.

Additionally, grouping can be changed by dragging group headers into a different order, and groups can be removed from the hierarchy by dragging them back to the grid.

The data grid rows organized in a multi-tiered tree using the grouping bar can be fully expanded and collapsed using the context menu. The “+/-” box next to a grid row can also be used to expand a group.

Column Headers

Column Headers refers to columns which can be shown or not shown using the Columns item in the right-click context menu. Column headers dragged to the top of the chart group rows in the hierarchy specified in the Grouping Bar. Grouped rows appear under the left-most column header.

Sorting

One or more column headers can be used to sort table rows. Clicking a column head sorts the rows by that column. An arrow appears above the column name indicating it is being used to sort the rows and the type of sort, ascending or descending, being performed. Click a column to change the type of sort done. Sort rows using additional columns by shift-clicking columns in the desired sort order. The sort type can be changed by shift-clicking on the column.

Grid data is sorted as follows:

- Text fields – alphabetically
- IP addresses – numerically by each address component, left to right.
- Numbers – numerically
- Time – by time value

Note: Sorting is done on the displayed value of the cell in each row of a column. The precision of a value may be higher than that of the displayed value, resulting in cells in some rows appearing to be the same when they are in fact different.

When using groups, sorting on a grouped column sorts the groups; sorting on a non-grouped column sorts the rows within each group.

Filter Bars

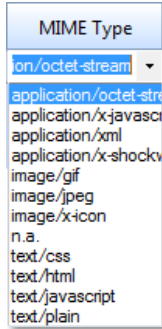
A Data Grid *Filter Bar* enables the filtering of data rows by a column. A filter is made up of two elements :

- A value
- An operator

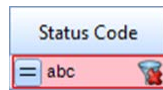
Click in a column's filter bar to enter a filter. Hold down the shift key and click in a column's filter bar to enter additional filters.

Values

A filter value can be entered in the filter bar or selected from a list of the column's contents by clicking the funnel icon on the right side of the filter bar. Here is an example of selecting a value from a MIME Type column. The drop down list contains all MIME types present in the grid rows.



Filter value list



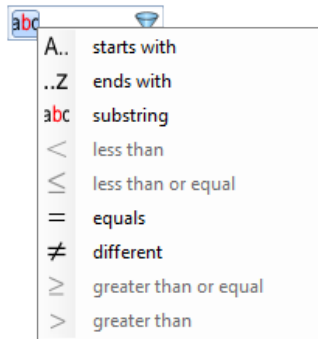
Invalid Filter value

Entered values are evaluated as the same value type as the column's values. For example, in a column of time values, the entries "2m" or "120s" are evaluated to the same value. Invalid entries, for example, text entered in a numeric column, are highlighted in red as shown in the figure above. All filtering is done on the displayed values, so different values can be displayed as the same and will be filtered as the same value. Note: Only rows can be selected in a grid table, not cells, so you cannot cut-and-paste the value in a cell for use in a filter. However, a cell's value can be selected from the drop down list displayed when you click the funnel icon in a column's filter bar.

When a filter is applied, a red X appears over the funnel icon. Click the X to remove the filter.

Client Port	Server Port	Bits	Bytes	Packets
Client IP : 10.5.5.74	[1]	Sum: 2,112,901,536	Sum: 264,112,692	Sum: 204,091
Client IP : 10.5.5.79	[1]	Sum: 2,214,835,872	Sum: 276,854,484	Sum: 192,466
Client IP : 10.5.42.61	[1]	Sum: 1,160,729,056	Sum: 145,091,132	Sum: 142,396
	[3]	Sum: 5,488,466,464	Sum: 686,058,308	Sum: 538,953

Operators

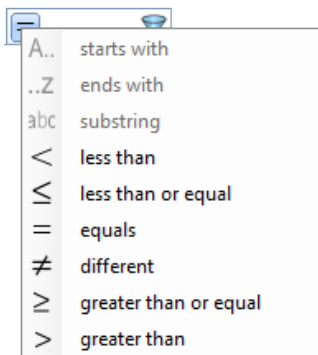


For strings or IP addresses

A filter *Operator* is selected by clicking the icon on the left side of a column's Filter Bar. A drop down list opens that lists the operators available based on the type of content in the column (strings, IP addresses, numbers or time values). After an operator is selected, rows not satisfying the filter are hidden.

A filter bar has a default operator based on the type of content in the column. If you enter a value without selecting an operator, the default operator is used:

- Substring for text or IP addresses
- = for numbers or time values



For numbers or time values

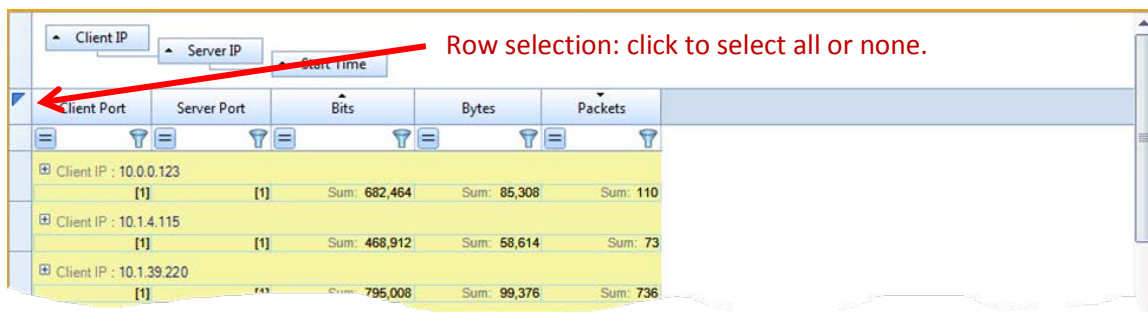
Further filters can be applied. The funnel now only lists the values from the rows that are not filtered out.

Operators Drop Down

Once a value and an operator are specified, the filter is enabled.

Selection

Select all or select none can be performed by clicking the cell at the left end of the column header row. The icon changes when the cell is clicked to indicate whether all or none of the rows will be selected.



Any combination of rows or groups can be selected although selecting rows when the parent group is already selected does not change the meaning of the selection. All of the standard Windows selection shortcut keys, for example, Control-A, can be used. All of the standard Windows selection shortcut keys, for example, Control-A, can be used.

The context menu provides options on how selected content can be used.

Summaries

A table summary appears at the bottom of each table, providing item counts for unique values in a dimension column and calculated values for a metric column. The type of value calculated is set in the view and can be changed using the view editor. Right-click the view applied to the traffic source and click the Edit item. Set the type of calculation you want under Metrics. Below is the example grid we have been using as shown in the View Editor:

The screenshot shows the View Editor interface for 'TCP Traffic Details by Connection'. The 'Metrics' section is expanded, showing a dropdown menu with 'Sum' selected. A red arrow points from this 'Sum' option to the 'Sum' column in the 'TCP Connection Summary' table. The table displays data for various Client IP, Server IP, and Start Time groups, with summary rows at the bottom of each group.

Client IP	Server IP	Start Time	Client Port	Server Port	Bits	Bytes	Packets
Client IP : 10.5.5.78			[3]	[1]	Sum: 194,855,744	Sum: 24,356,968	Sum: 20,917
Server IP : 10.5.51.54			[1]	[1]	Sum: 50,808,240	Sum: 6,351,030	Sum: 6,613
Start Time : 1/13/2014 12:00:36 PM			[1]	[1]	Sum: 50,808,240	Sum: 6,351,030	Sum: 6,613
	1008	2049			50,808,240	6,351,030	6,613
Server IP : 10.5.51.56			[1]	[1]	Sum: 48,323,808	Sum: 6,040,476	Sum: 6,233
Start Time : 1/13/2014 12:00:37 PM			[1]	[1]	Sum: 48,323,808	Sum: 6,040,476	Sum: 6,233
	719	2049			48,323,808	6,040,476	6,233
Server IP : 10.5.51.75			[1]	[1]	Sum: 95,723,696	Sum: 11,965,462	Sum: 8,071
Start Time : 1/13/2014 12:00:37 PM			[1]	[1]	Sum: 95,723,696	Sum: 11,965,462	Sum: 8,071
	739	2049			95,723,696	11,965,462	8,071
Client IP : 10.5.5.79			[1]	[1]	Sum: 2,214,835,872	Sum: 276,854,484	Sum: 192,466
Client IP : 10.5.5.88			[1]	[1]	Sum: 1,823,728	Sum: 227,966	Sum: 335
Client IP : 10.5.5.126			[1]	[1]	Sum: 1,485,648	Sum: 185,706	Sum: 204
Client IP : 10.5.14.69			[1]	[1]	Sum: 11,110,608	Sum: 1,388,826	Sum: 1,448
Client IP : 10.5.14.81			[1]	[1]	Sum: 496,422,024	Sum: 62,052,753	Sum: 59,833
[278]	[28]				Sum: 11,983,006,560	Sum: 1,497,875,820	Sum: 1,303,843

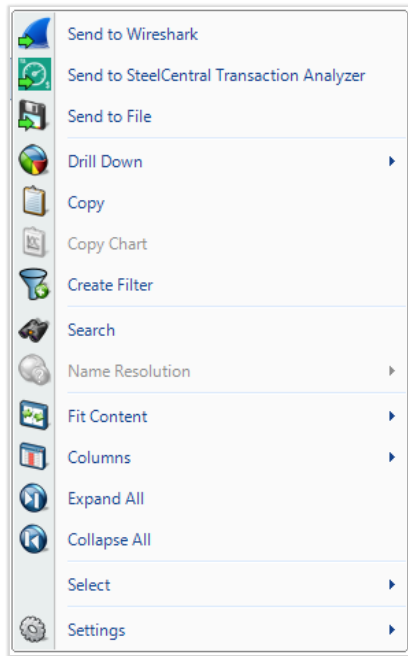
If no rows or groups are selected, the summary table includes all table rows and groups. If specific rows or groups are selected, the summary only includes the selected items. Selected rows that appear in a selected group are not double counted.

A group summary is provided for each group. A grid with three groups, such as our example, will have a summary shown for each group. Our example includes a summary for Client IP. A summary for Server IP, and a summary for Start Time, as shown above.

Note: If a grid has 300 or more rows, a navigation pane appears in the lower right corner of the screen. The table summary includes the rows indicated by the navigation pane, which could be less than the number of rows in the entire table.

To save a view with customized summary calculations, click Save in the View section of the Home ribbon. A new name must be used as standard views cannot be overwritten.

Context Menu



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) and group(s) to Wireshark for analysis.

Send to SteelCentral Transaction Analyzer

The *Send to SteelCentral Transaction Analyzer* menu option sends the traffic from the selected row(s) and group(s) to SteelCentral Transaction Analyzer for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected row(s) and group(s) to a user-specified trace file that 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 group(s) and opens a new view tab in the main workspace.

Copy

The *Copy* menu option copies a tabular form of the selected row(s) and group(s) to the system clipboard.

Copy Chart

The *Copy Chart* menu option is always disabled for the grid and is included in the context menu in order to be consistent with the other charts.

Create Filter

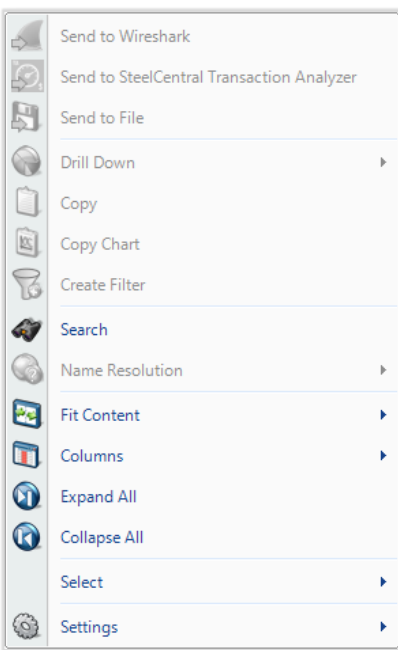
The *Create Filter* menu option creates a filter based on the current selection within the Grid and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find and select data in the chart. Note: Remove all groups from a grid table before using Search.

Name Resolution

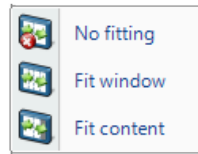
The *Name Resolution* menu option is always disabled for the grid and is included in the context menu in order to be consistent with the other charts.



Grid (No Selection)

Fit Content

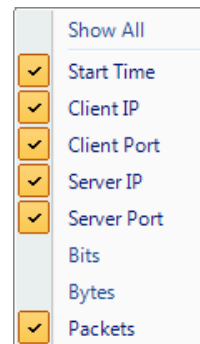
The *Fit Content* menu provides options for resizing the table columns.



- *No fitting* - The same default width is given to each column. Column widths can be manually adjusted.
- *Fit Window* - Column widths are adjusted so they use the entire horizontal space. Each column is given the same width. Column widths can be manually adjusted.
- *Fit content* - Column widths are adjusted based on the column content. Column widths cannot be manually adjusted.

Columns

The *Columns* menu option expands to a submenu that is used to show and hide columns in the grid. A menu shows a check box for each column. Toggling the various options will either show or hide the corresponding columns. A checkbox is also provided to show all items in a single click. Grouped columns visibility cannot be changed.



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.

Select

The *Select* menu option has two submenu options. *Select All*

The Select All menu option selects all visible rows and groups in the grid.

Select Inverse

The current selection in the grid is inverted.

Settings

The *Settings* menu option provides specific settings for the chart.

Show Filter Bar

Shows or hides the filter bar on the Data Grid Chart.

Show Grouping Bar

Shows or hides the Grouping Bar on the Data Grid Chart.

Channels Button

A Packet Analyzer provides 802.11 wireless analyses on live traffic using the Riverbed® AirPcap adapters for wireless interfaces.

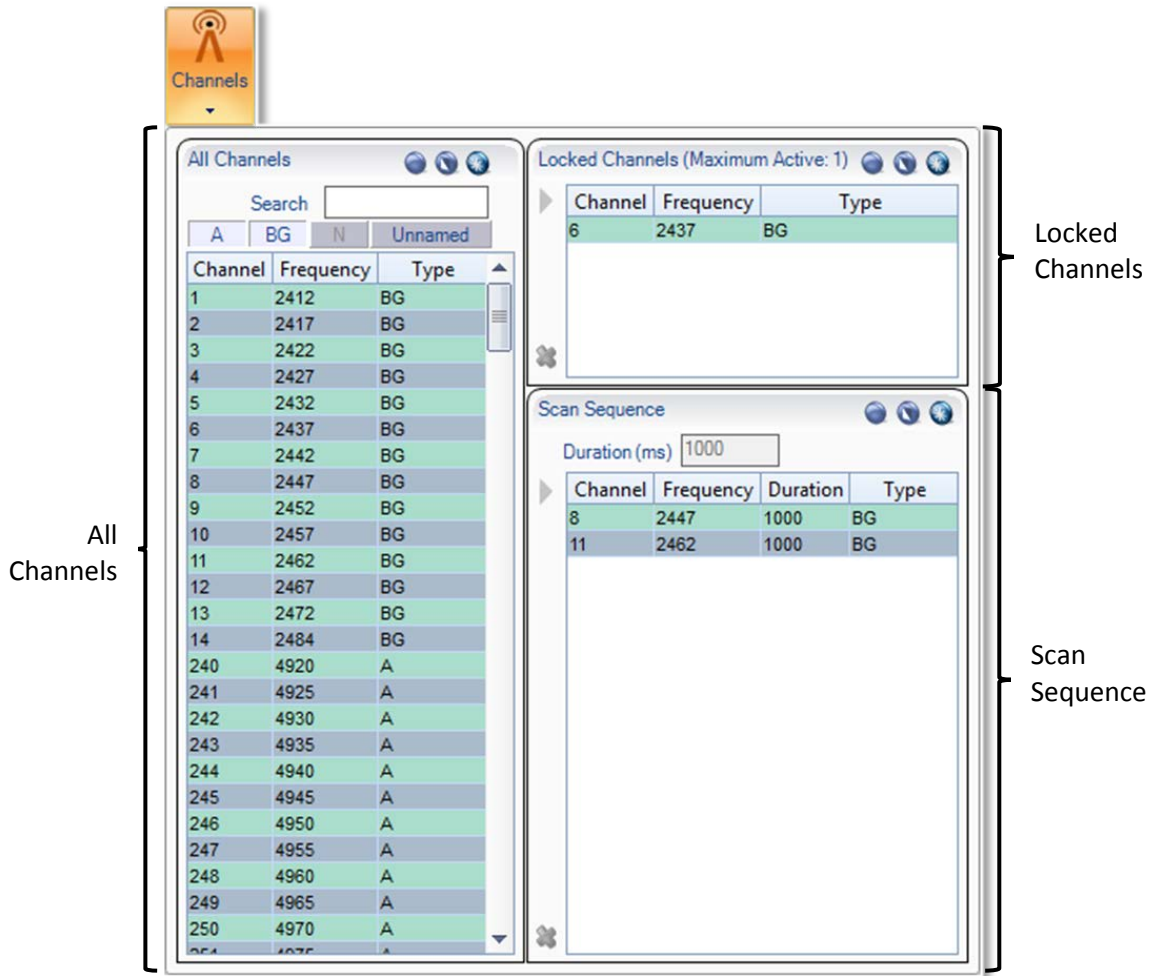


Figure 46 Wireless Interface in Sources Panel

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 46). The AirPcap adapters are aggregated into a single capture device for convenience in dealing with hopping or scan sequences, where the adapters are sequenced through multiple channels using the Channel Management Panel.

Note: Although it is possible to use different types of AirPcap adapters at the same time, in some cases there may be conflicts in the capabilities available on different adapters.

The Channels button in the Home Ribbon brings up the Channel Management Panel. The Channel Management Panel selects which channels to capture for a particular time interval. The Channel Management Panel is available in the Home Ribbon and is shown below.



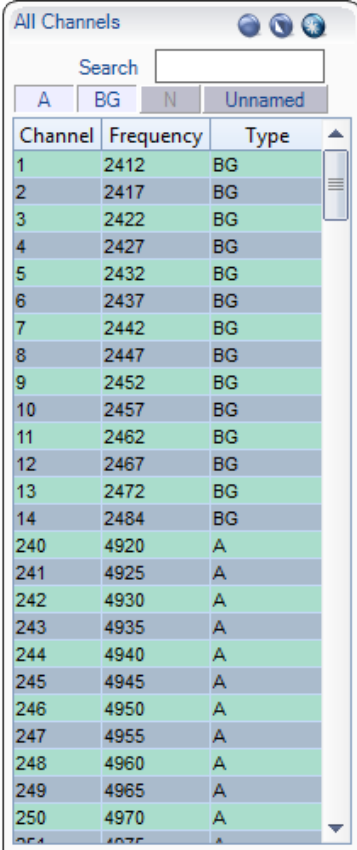
Channel Management Panel

Note: To close the Channel Management Panel, click the Channels button again or click 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

All Channels



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
250	4970	A

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 specific 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 2.437 GHz center frequency will capture BG frames. At 5.260 GHz, the AirPcap Ex adapter will capture A frames.

The AirPcap Nx adapter at 2.437 GHz center frequency and 20 MHz bandwidth will capture BG, A, and N frames. At 5.260 GHz center frequency and 40 MHz bandwidth (NHigh), the AirPcap Nx adapter will capture A, N, and NHigh frames.

Channel Names

Channels are generally identified by a number and a frequency band. For example, channel 13 in the 2.4 GHz band corresponds to center frequency 2.472 GHz. 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.
- Four 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 are visually broken up.
- Selection control buttons.

This view enables a traditional flat list of channels that can be quickly navigated and selected without concern for the complexities of the standards.

However, 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 one N adapter and one BG adapter, then only the N adapter can scan the 2.4 GHz 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
250	4970	A

Channel List

The Channel List is a scrollable 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. Not all available frequencies have a canonical name.

Frequency

The actual center frequency of the row in MHz.

Type

The type of Channel; one of the following: BG, A, N, NHigh, NLow.

Selection Controls



Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.



Invert Selection

The *Select Inverse* button reverses the channel list selection(s).



Select All Channels

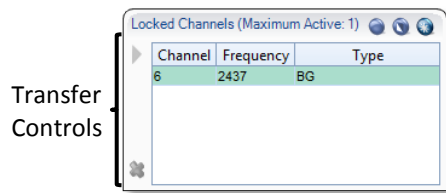
The *Select All* button selects all of the channel(s) in the channel list.

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



Locked Channels

The *Locked Channels* is a list of channels that are used to assign a wireless adapter dedicated to a channel. It contains four 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 Packet Analyzer. 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



Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.



Invert Selection

The *Select Inverse* button reverses the channel list selection(s).



Select All Channels

The *Select All* button selects all channel(s) in the channel list.

Transfer Controls



Transfer Channels

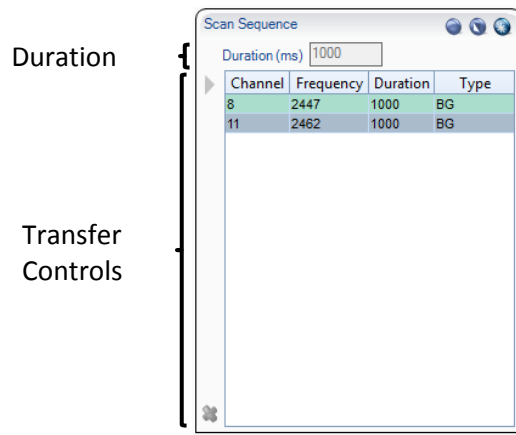
The *Right Arrow* button adds the selected channel(s) to the locked list. If the selected channel was in the Scan Sequence List, it is removed from that list.



The *Remove* button removes the selected channel(s) from the lock list. The lock list can be empty.

Remove Channels

Scan Sequence



The *Scan Sequence* is a list of channels that the wireless adapter(s) will listen on occasionally. It contains four elements:

- Duration
- Selection controls
- Transfer controls
- Channel list

The following is saved in the global configuration file:

- Scan sequence elements
- Duration for each element

Scan Sequence

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 to have only one type of AirPcap adapter in the system, for example, either all AirPcap Ex adapters or all AirPcap Nx adapters. Having both AirPcap Ex and AirPcap Classic/Tx adapters works well in the 2.4 GHz band, but not in the 5 GHz band.

Duration

Duration (ms)

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.

Channel Duration

Selection Controls



The *Select None* button deselects all channel(s) in the channel list, if applicable.

Select No Channels



**Invert
Selection**

The *Select Inverse* button reverses the channel list selection(s).



**Select All
Channels**

The *Select All* button selects all channel(s) in the channel list.

Transfer Controls



**Transfer
Channels**

The *Right Arrow* button adds the selected channel(s) to the scan sequence list. If the selected channel was in the locked list, it is removed from that list. Durations of previous, deleted channel(s) are not saved if they are retransferred. Channels are removed from the Locked Channels section when they are transferred.



**Remove
Channels**

The *Remove* button removes the selected channel(s) from the scan list. The scan list can be empty.

Scan Sequence

The *Scan Sequence* is a frequently updated color-coded list of scanned channels. The scan sequence is updated a few times per 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 channel will be scanned before moving on to the next. Each channel can have a different duration value.

Decryption

Packet Analyzer 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. Note that an exported configuration file will contain the decryption keys so care should be taken.

Wireless Decryption Keys Manager



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

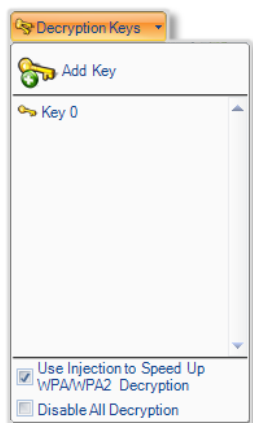
The *Use Injection to Speed Up WPA/WPA2 Decryption* check box, described below in the section entitled “WPA related packet injection” is only enabled if all plugged in AirPcap adapters are Ex. Please note that there are a number of important considerations when using this feature, as discussed below.

Disable All Decryption

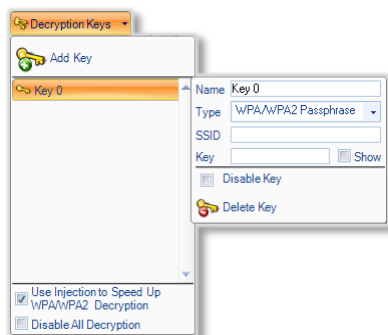
The *Disable All Decryption* check box is used to completely turn off decryption. This may decrease the time required to process a packet if trying to mitigate packet loss on an extremely busy network. It can also be used to confirm that a network is encrypted.

Note: *To close the Wireless Decryption Keys Manager, click the button again or click somewhere outside of the submenu. All changes take place immediately hence there is no need for confirmation buttons.*

Adding a Key



Decryption Keys with Key



Decryption Keys with Key (Detail)

To add a key, click on the *Add Key* button. The submenu will change to show a scrollable list with one decryption key, and as many decryption keys can be added as desired. Note that there is no need to associate a particular decryption key with a trace file or wireless adapter, as the appropriate decryption key will be automatically matched with its specific context.

After a decryption key has been added, its parameters need to be set by clicking on the 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, as it is what will appear as the name in the key gallery, but does not affect 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 will map 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.

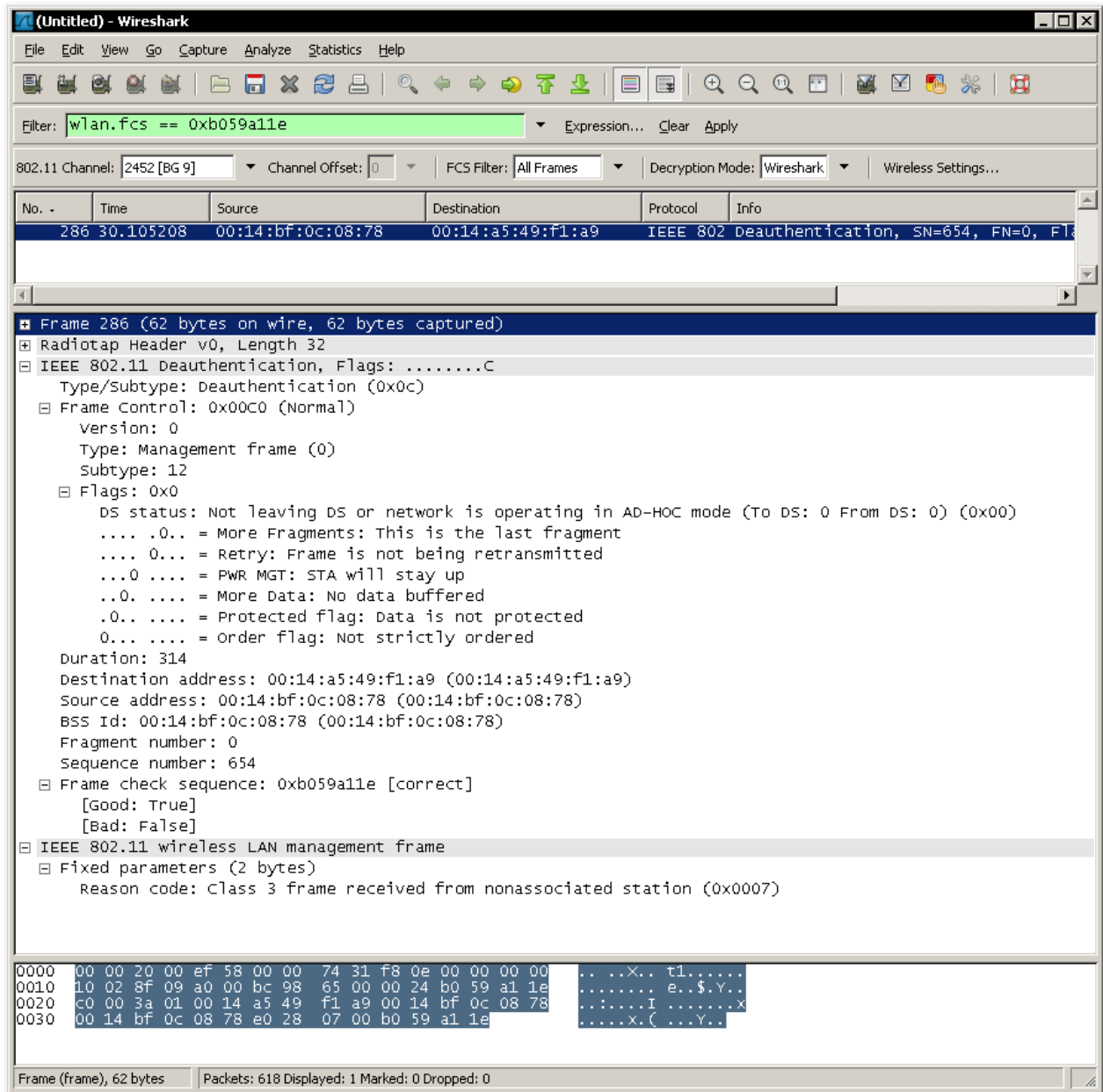
In order to successfully decrypt WPA traffic then, even with a valid decryption key, the setup of this link needs to be captured. However, because stations may not authenticate for hours or possibly longer, in order to view traffic without waiting a long time, the hosts need to re-associate with their 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:



Wireshark analyzing a Packet Analyzer generated Deauthentication frame

Drill Down

Drill Down enables data to be analyzed at various levels of detail by iteratively applying views to visually selected subsets of the data.

How to

A Drill Down can be done in three ways:

- Make a selection in a chart and click the Drill Down button in the Chart Selection section of the Home Ribbon.
- Right-click a selection in any chart and select Drill Down from the context menu.
- Drag a view from the Views Panel over a selection in a chart.

Every chart has a means of selecting data subsets to enable a drill down operation.

The following operating rules apply to drill down operations:

- If you can create a filter using a selected item, you also can drill down on the selected item.
- Drill down is not available for a time selection in a view applied to a live source.
- Drill down is chart specific. Drill down may be available in some charts in a view, but not others.

Examples

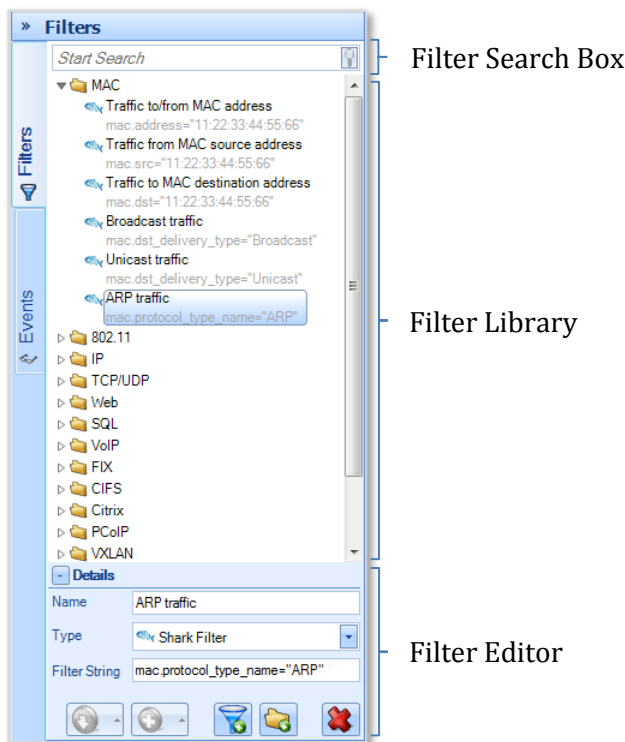
For examples of Drill Down sequences and operations, please refer to the tutorial videos. Click Getting Started in the General section of the Home Ribbon

Filtering

Packet Analyzer offers several ways to apply user-defined filters on large data sets to help focus the analysis the data of interest.

Filter panel

The Filter panel, located on the right side of the Packet Analyzer user interface in the tabbed navigation panel, displays and organizes the set of filters. The panel is composed of three elements.



Filter panel

Filter Search Box

The Filter Search Box is used to locate specific filters among the list. The search will match any filter that has the search string in either the filter name or the filter string.

Filter Library

The *Filter Library* displays the collection of pre-packaged and user customized filters. Filters can be selected, edited, moved, added and removed through the buttons on the bottom of the library, or through the context menu.

Filter Editor

The *Filter Editor* section has three elements:

Name

The name of the filter to be modified.

Type

The language the filter is to be written in. There are four languages available:

- NetShark Filter
- BPF¹
- Wireshark Display Filter ²
- Time Interval

Filter String

The code for the filter associated with the description as specified above.

Apply



The *Apply* button is used to apply selected filters to the current view. It provides the user with a list of options that can be used in applying the selected filter based on the operator. This set matches that of Wireshark's context menu for filters:

<i>Selected</i>	}	Selected filters are applied in place of applied filter of the same type.
<i>Not Selected</i>		
<i>... and selected</i>	}	Selected filters are applied to the currently applied filter of the same type and the new filter value depends on the chosen operator.
<i>... and not selected</i>		
<i>... or selected</i>		
<i>... or not selected</i>		

If more than one filter is selected, filters of the same type are aggregated using OR, while filters of different types are aggregated using AND.

Prepare



The *Prepare* button sets up the selected filters for editing in the Filter Bar (described below) without applying them. See the *Apply* button for options.

¹ BPF was published in USENIX 93 and can be seen here: <http://www.tcpdump.org/papers/bpf-usenix93.pdf>

² See <http://www.wireshark.org/docs/dfref/>

Edit



The *Edit* button moves focus to the Filter Editor at the bottom of the Filter panel to edit the selected filter. If no view is currently applied, the same behavior is performed by pressing the Enter key.

Delete



The *Delete* button removes the selected filters from the collection after prompting the user for confirmation. The same behavior is performed by pressing the Del key.

Duplicate



The *Duplicate* button creates a copy of the selected filter. The new copy has the same filter type and value as the original, but has a unique name, constructed by appending a counter to the original name.

Move to Top

The *Move to Top* button moves the selected filter to the top of the hierarchy level in which the filter is located, to give it more visibility.

New Filter/Folder



The *New Filter* button creates a new filter and adds it to the collection. If clicked from the context menu or in the Filter Editor when something is selected, the behavior is similar to *Duplicate* button (except for the name). Otherwise a new default BPF filter is created.



The *New Folder* button creates a new empty folder as subfolder of the selected one. If none is selected a new folder is added to the root level.

Sort



The *Sort* button sorts the collection elements based on one of the following options: Default (order defined in the Packet Analyzer configuration file), Name or Type.

Reset Filters



The *Reset Filters* button restores the factory-defined filter list. If the configuration file was imported from an older version of Packet Analyzer (formerly Cascade Pilot), there is an option to merge the filters defined by the new version into the factory list.

Drag & Drop

Filters can be easily dragged in and out of the panel to create, organize or apply filters.



Dragging and dropping filters

Inside Filter panel

- Within the Filter panel itself, filters can be dragged around to change their position inside their folder, or to move them from one folder to another. If the Control key is held during drag, a copy is performed instead of a move.
- Folders cannot be copied or moved. It is only possible to change their position by dragging them within the same hierarchy level.

From Filter panel

- Filters can be dragged over an unapplied standard view in the Views panel, creating a filtered view in the Custom Views folder. If a filter is dragged onto a custom view, that view is modified to add the filter.
- Filters can be dragged onto the Filter Bar or onto an applied view chart, which will apply the view to the open view. Multiple selection is supported:
 - Two or more filters of the *same type* will be applied as a single filter item in the Filter Bar in OR.
 - Two or more filters of *different type* will be set on as many filter items in the Filter Bar as the number of different filter types in the multiple selection. Filters of the same type are in OR, otherwise in AND
- When a filter is dragged onto the filter bar and a previous one of the same type is already set, the new one replaces the old one. A new filter can be applied using OR or AND with the previous one by holding, respectively, Control and Alt keys while dropping.
- A time filter can be dragged over the master controller to apply it. It can be dragged over a Strip Chart or Sequence Diagram to perform a time selection or over the Filter Bar to apply it to the view.

To Filter panel

- Any filter can be dragged from the Filter Bar onto the filter panel to create a new item in the list. Also, time filters can be created by dragging a time selection from the Strip Chart, Sequence Diagram or Master Controller onto the Filter panel.

Shortcuts

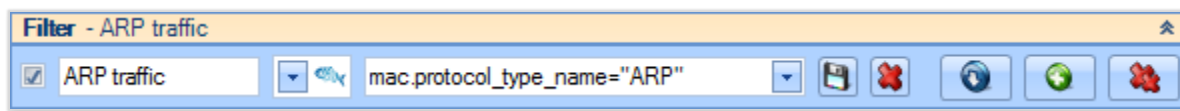
Some of the operations can be performed by keyboard shortcuts:

- **Double-Click / Enter:**
 - **Folder list item:** expands the folder in the Filter panel to show its name and moves focus to it.
 - **Filter list item**
 - If no view is applied, expands the Filter panel editor showing the filter details and moves focus to the editor.
 - If a view is applied, adds the filter to the view and updates it instantly.
- **F2:** expands Filter Editor details and gives focus to it.
- **F3:** gives focus to search box.
- **Del:** removes selected item.
- Typing a filter name performs a search and first occurrence is selected.

Filter Bar

The Filter Bar is a visual component on the top of an open view that shows the currently applied filters and/or the filters being edited. It is the Packet Analyzer equivalent of Wireshark's "display

filter input” and provides the user with a graphical interface to disable, edit, save, remove and apply filters. Whenever a filter is applied or modified, the view is updated to show the new filtered data.



Filter bar

The bar displays the filter parameters and a check box on the left shows if a filter item is currently applied to the view. Checking or unchecking that item performs an instant view update.

Save



The *Save* button saves the filter, adding it to the root folder in the Filter panel.

Delete



The *Delete* button removes the applied filter and updates the view. If the filter isn't applied, all the fields are simply cleared.

Apply



The *Apply* button applies the filter changes and updates the view. This behavior can also be performed by pressing the Enter key.

Prepare



The *Prepare* button creates a new empty row and adds it to the filter bar so that a new filter can be edited and applied.

Delete All

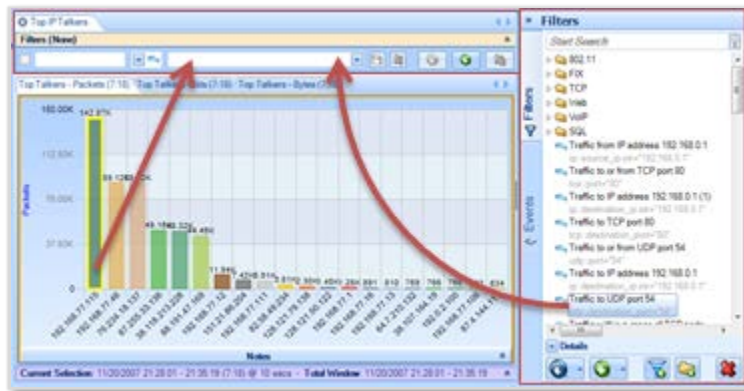


The *Delete All* button removes all the filters from the Filter Bar and updates the view accordingly.

Note: It is NOT possible to have two or more filter rows with the same filter type because each filter item specifies one and only filter type. Different types are defined on different rows and are combined using AND.

Drag & Drop behavior

Filters in the Filter panel can interact with the Filter Bar through Drag & Drop or by means of the context menu.



Filter panel - Filter bar interaction

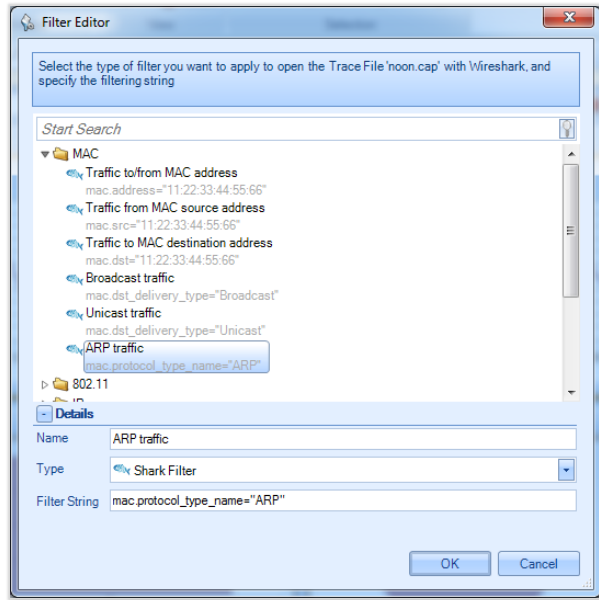
As mentioned above, any filter can be dragged over the Filter Bar to instantly apply it. See the previous section for a description of the various options for applying filters using drag & drop.

Shortcuts

Some operations can be performed using keyboard shortcuts:

- **Enter:** Apply the filter, if modified.
- **Control+Z:** Undo changes in the filter value combo box in order to show the history of the applied filters.
- **Control+Y:** Redo changes in the filter value combo box.

Filter Dialog

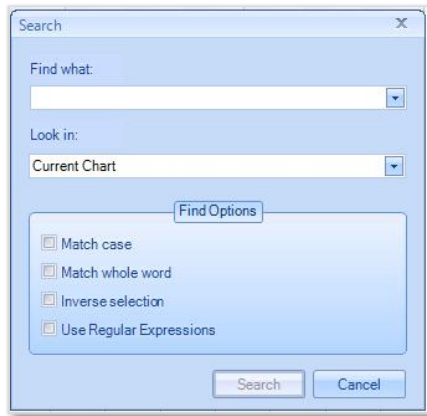


Filter Dialog

The *Filter Dialog* appears every time an operation with a filter is requested; for example, after selecting any option to send traffic with a filter either to file or to Wireshark.

The Filter Dialog implements the same graphical interface shown in the Filter panel, but it is not possible to apply filters, drag them out of the control, delete or reset them.

Search Dialog



Search Dialog

The *Search* dialog can be activated either by clicking on the binocular icon labeled Search in the Home Ribbon or by context clicking on a chart and choosing the “Search” option. There are two search features:

- 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, identified with an orange border.

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 with a tab 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 for alphabetic characters [A-Z].

Match whole word

By default, search looks for substrings. For example, if a hostname is “www.riverbed.com” and “river” is searched, then “www.riverbed.com” would still be matched. When *Match whole word* is checked, then only entering the full “www.riverbed.com” string will match.

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

Packet Analyzer supports POSIX regular expressions for advanced searching, which are well documented elsewhere. The basic syntax includes:

- ^** 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

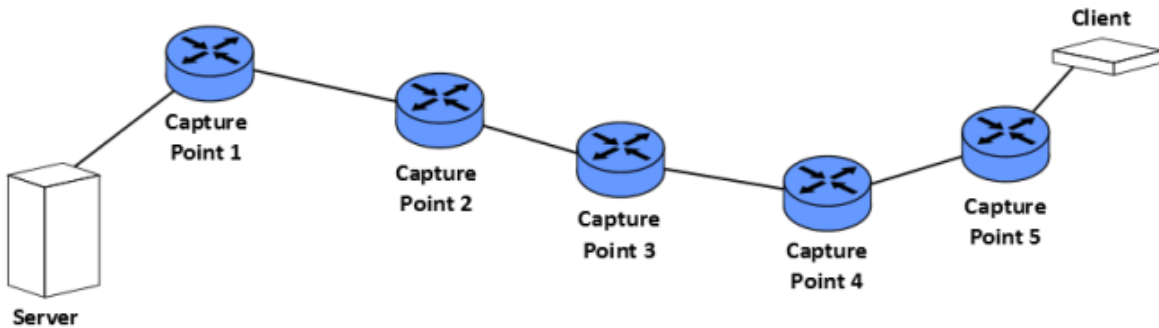
All local IPv4 networks

The IPv4 address ranges 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:

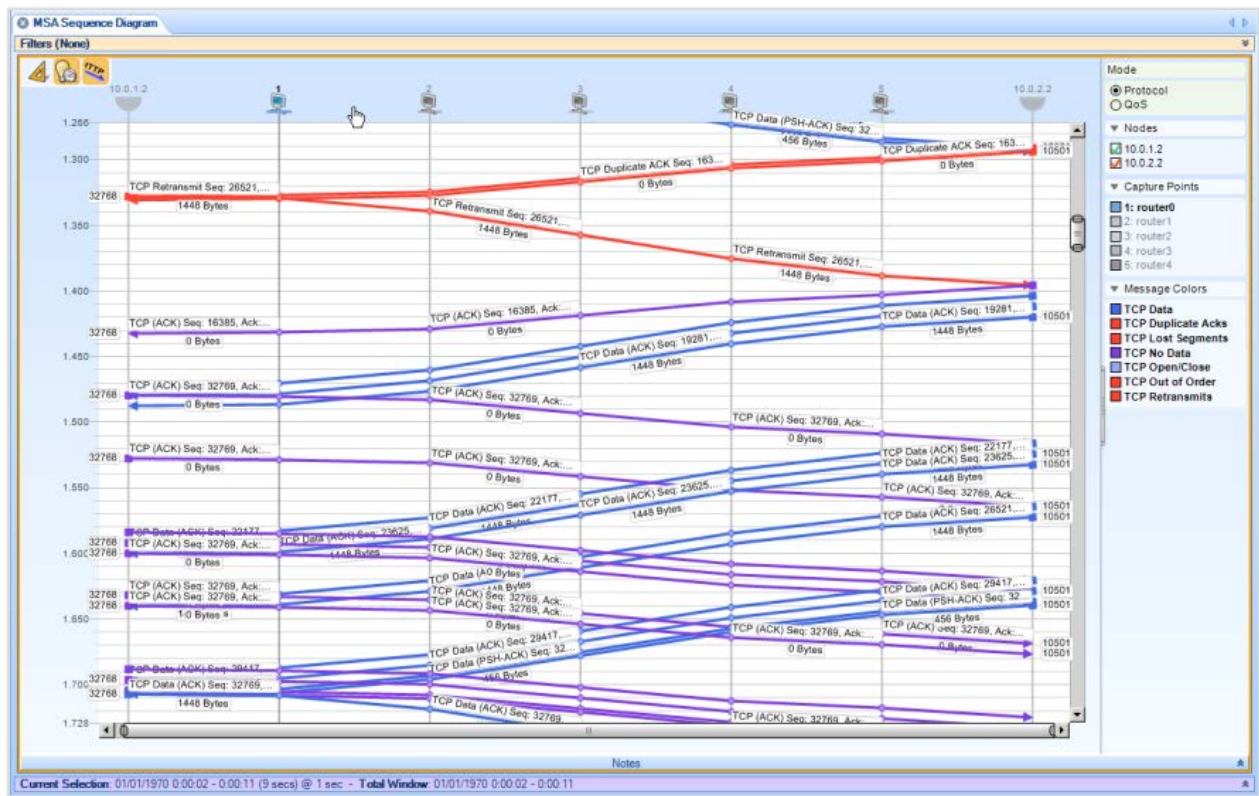
```
^(192\.168|10\.|172\.16)
```

Multi-Segment Analysis (MSA)

Multi-segment analysis (MSA), added in version 9.5, allows you to combine traffic data captured over the same time period from different locations on the network so you can view and analyze the traffic flows.



Typical network path using multiple segments between hosts



Typical multi-segment sequence diagram showing traffic flows through capture points between hosts

General approach

Review timestamp settings at the packet source

Accurate timestamps at the packet source and capture points are critical when performing multi-segment analysis. Inaccurate timestamps are very difficult to adjust automatically or manually, and frequently result in a failed MSA view.

Do the following to minimize timestamp issues when doing MSA analysis:

- If possible, use hardware taps to provide timestamps. Such devices can coordinate timestamps across network locations and help ensure accurate timestamps.
- Use NTP or other highly-accurate time references. Be sure that all capture devices reference the same time source.
- When using a hardware tap, make sure that your NetShark specifies the correct tap type when configuring the capture interface on the NetShark.

If your multi-segment source name indicates a problem “Some invalid timestamps found” follow the steps under “Adjust time skews (if necessary)” to correct the problem. If your attempt to correct the problem fails, you need to check your timestamps and create new capture files.

Assemble the data

Put all your source data in one place. Packet Analyzer requires that all of the source capture files or trace clips that you use be in one location—either on a single NetShark or on the computer that runs Packet Analyzer.

All the data processing for multi-segment analysis occurs locally on the NetShark or Packet Analyzer local system where the data sources are stored. If that processing takes place on a NetShark, only the results are sent across the network for Packet Analyzer to display.

Use small source files. If your capture files are large and you know that the time interval of interest is small, use trace clips that cover that interval. When sending files across the network to a central location, smaller files use less network bandwidth.

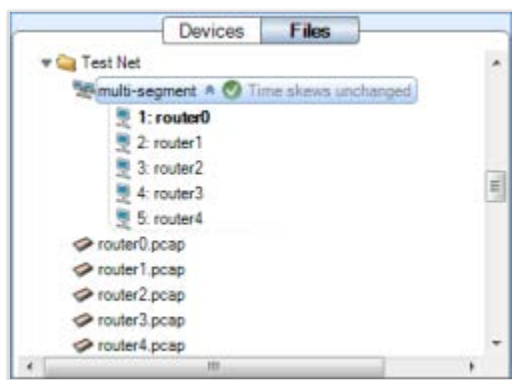
You may be able to use high-level views, even if not multi-segment views (such as network usage by traffic type) to narrow down the interval of interest. Then you can drill down with multi-segment views.

Make a multi-segment source

1. In the Files section of the Sources panel, select two or more sources that you will combine into a multi-segment source. (Use a click and multiple control-clicks, or a click and a shift-click.)
2. Right-click one of the sources to bring up a context menu. Click Create Multi-Segment Source.

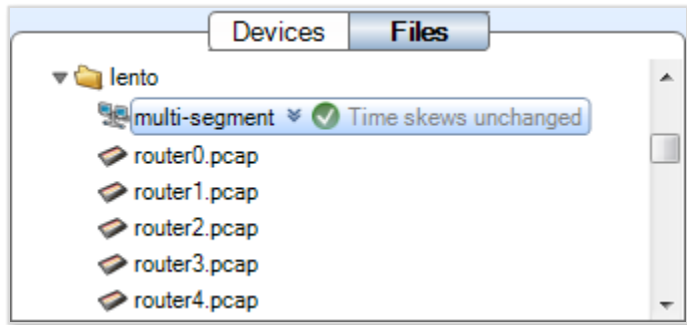


Packet Analyzer builds a multi-segment source and lists it in the Files panel. One of the segments is designated as the primary segment and shown in bold type. The primary segment is generally used when a single-segment view is applied to the multi-segment source.

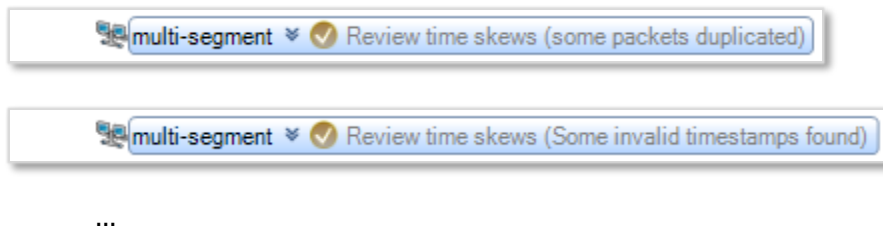


Adjust time skews (if necessary)

Packet Analyzer automatically adjusts the time skews between capture points, so in most cases you won't need to do anything. If the adjustment succeeds, the Files panel shows the multi-segment source with a green check-mark icon.

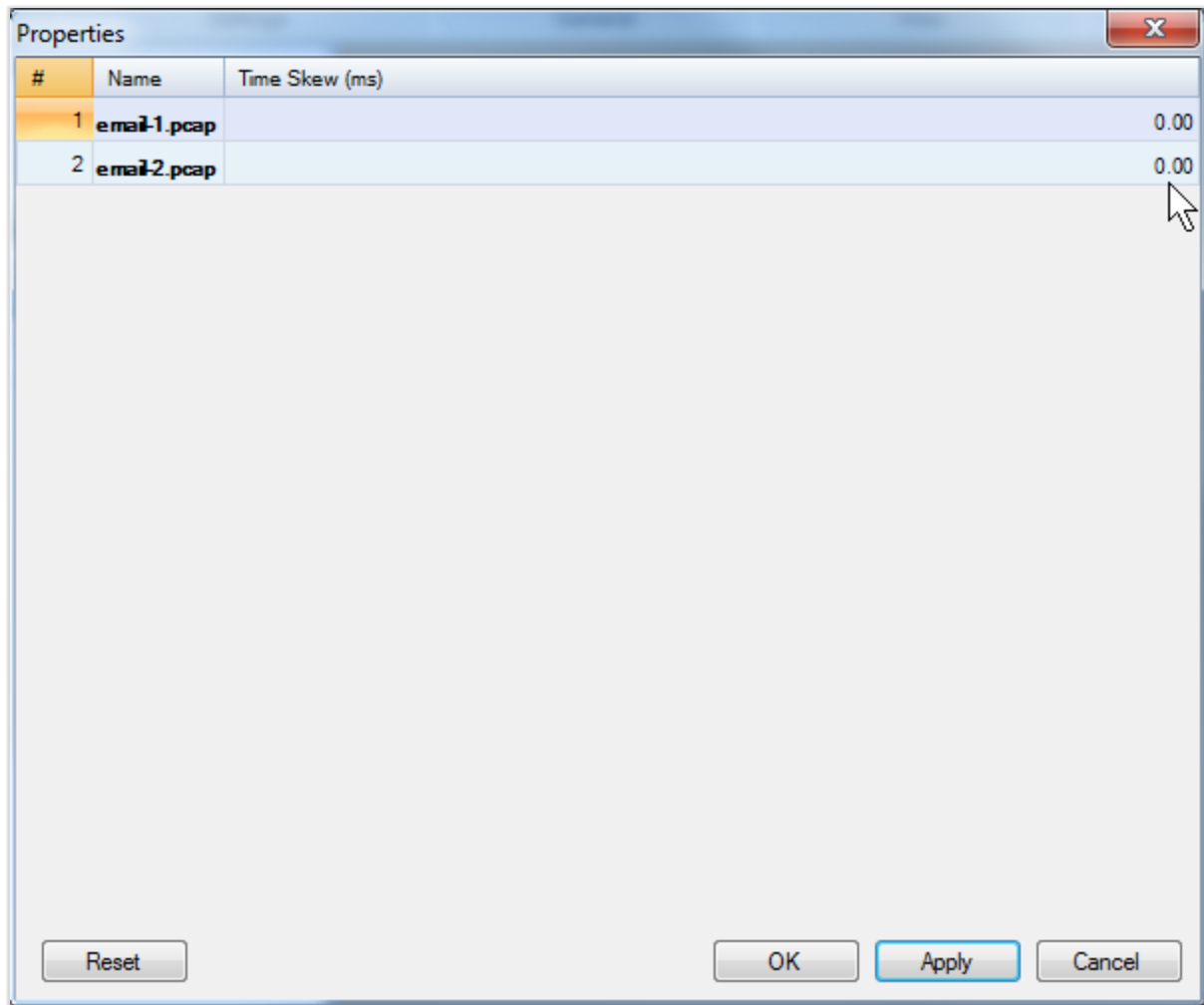


If the adjustment fails, the check-mark icon is yellow and has a brief explanation of why it failed.



You can run the time skew adjustment by right-clicking the multi-segment file and selecting Estimate Time Skews from the context menu that appears. The initial time skew estimate made when the multi-segment file is first created samples 1000 packets. When you right-click and select Estimate Time Skews the computation uses all the packets in the sample. This should be somewhat more accurate, though it may take more time to compute.

You can enter your own time skew values by right-clicking the multi-segment file and selecting Properties. The individual source files are listed, and each one has a time skew value that you can adjust manually.



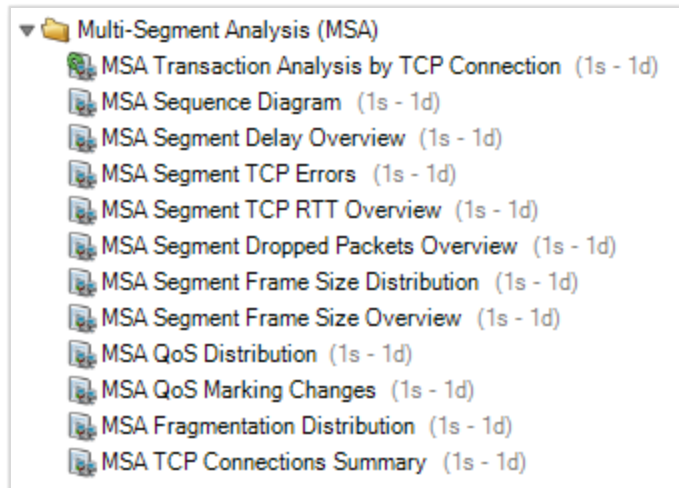
You may find it difficult to arrive at time skew values that improve on the automatic adjustments made by Packet Analyzer. As an alternative, make sure that the timing values that go into your source data are as accurate as they can be:

- The NetShark software (version 9.5 and later) supports taps that can add more accurate timestamps to packets. Hardware tap vendors can also ensure that captures taken at different locations can be coordinated by GPS or CDMA signals. Make sure that you specify the correct tap type when configuring the NIC interfaces on your NetShark.
- Use NTP or better time sources as your time reference, and make sure that all of your capture devices are referenced to the same source.

When timestamping is perfectly synchronized among NetShark appliances capturing trace files for multi-segment analysis, you should expect the time skew to equal 0.

Apply views

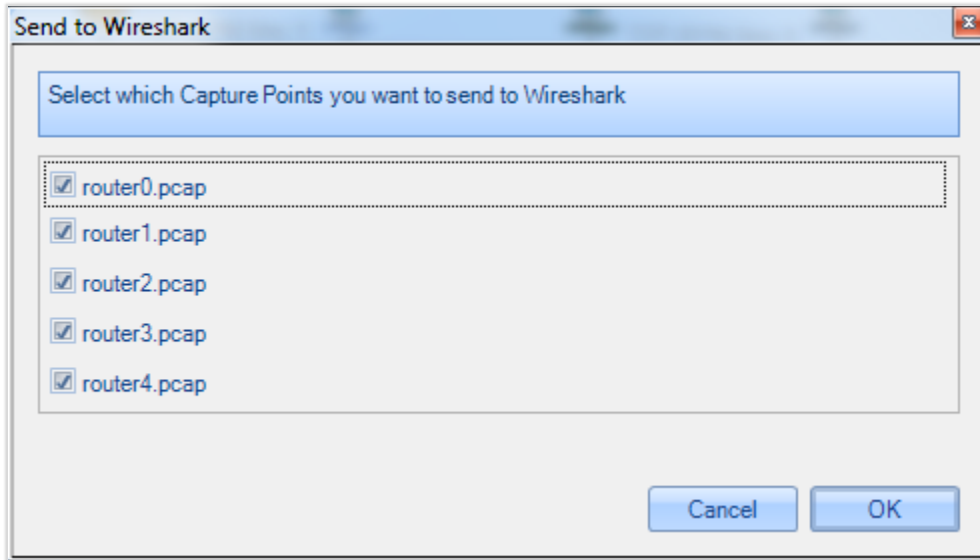
There are several views designed specifically for multi-segment analysis. You can easily find them by using the Search box (at the top of the Views panel) to search for “segment” or “MSA”.



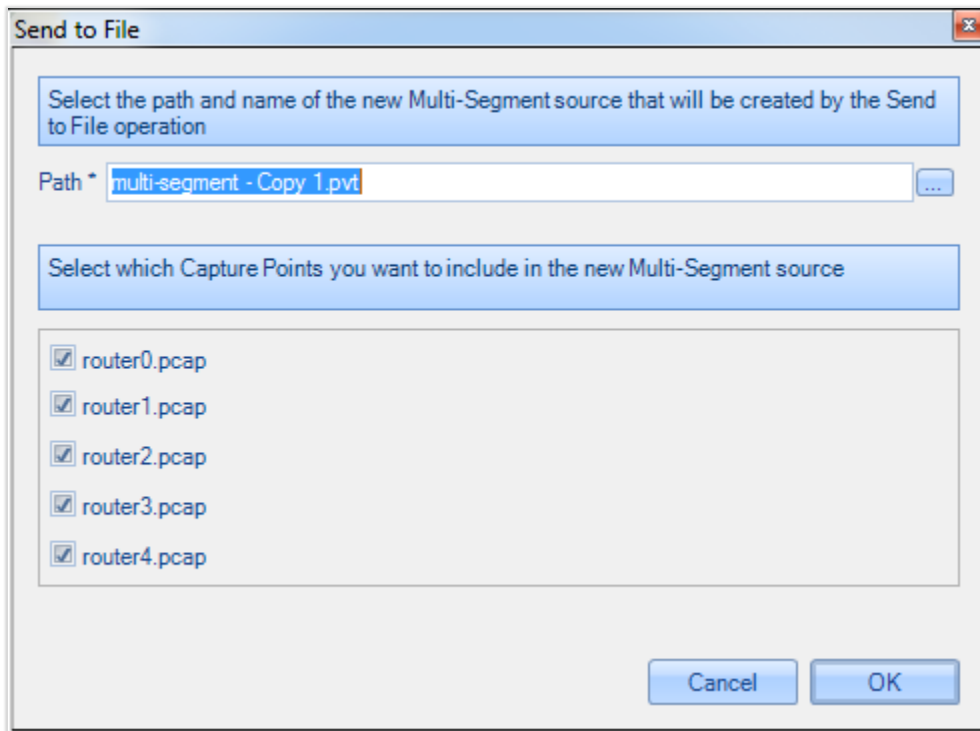
Once you have applied a view you can select an area of interest and drill down (apply additional views). But note that:

- You can't apply a multi-segment view to a normal (single-segment) trace file.
- If you apply a single-segment view to a multi-segment file, the view uses one trace. But if you drill down further with a multi-segment view, it uses all of the traces of the multi-segment file.
- When you can see all capture points in a multi-segment view, if you drill down further you can choose which capture points to include.

If you right-click a selection in a multi-segment view and choose “Send to Wireshark” from the context menu, a pop-up dialog lets you choose which capture points to use. For each capture point you choose, the packets in the selection are sent to a separate instance of Wireshark.



If you right-click a selection in a multi-segment view and choose “Send to File” from the context menu, a pop-up dialog lets you choose which capture points to use as sources for the new multi-segment file that corresponds to the selection.

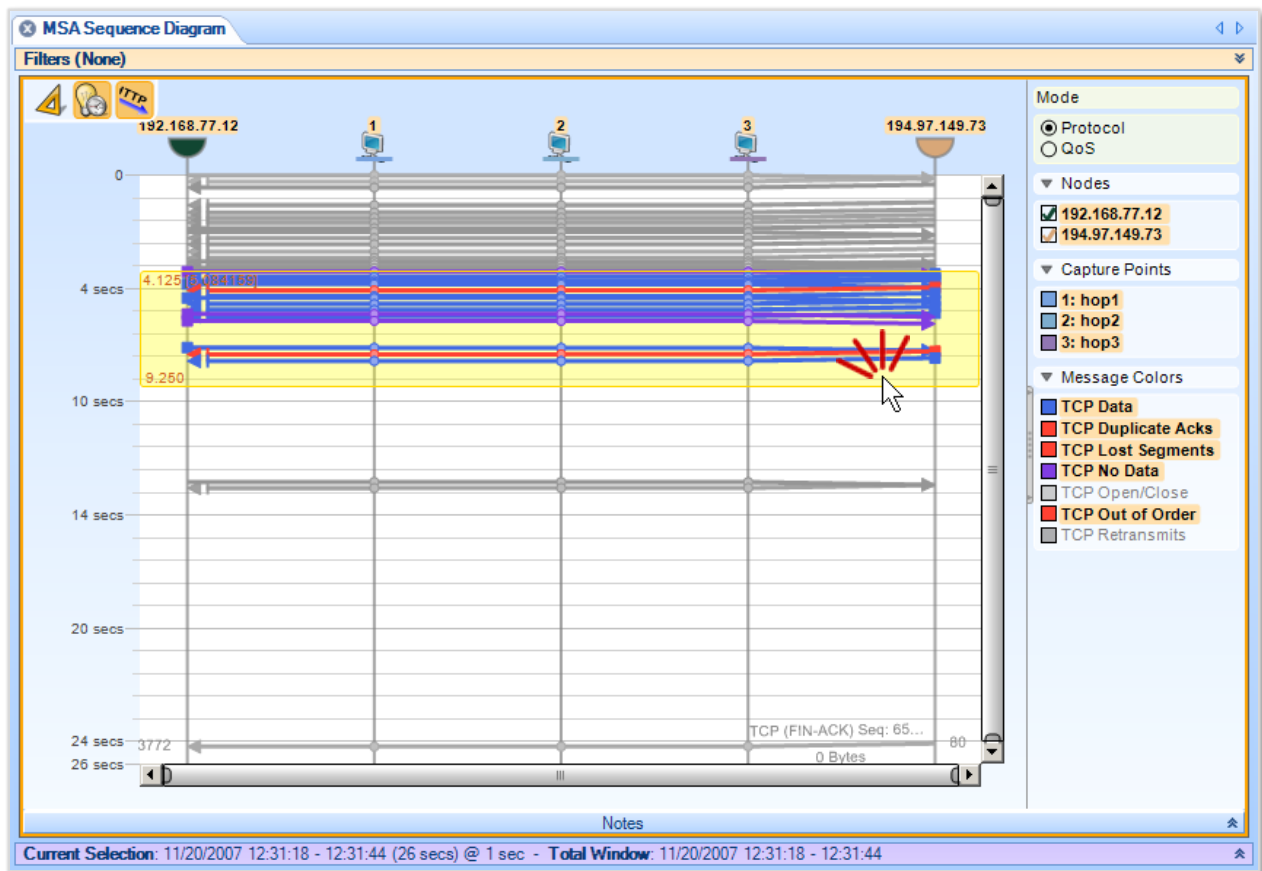


Navigating a multi-segment sequence diagram

There are several different ways to view the information in a sequence diagram. Choose the combination that works best for you.

Select and zoom

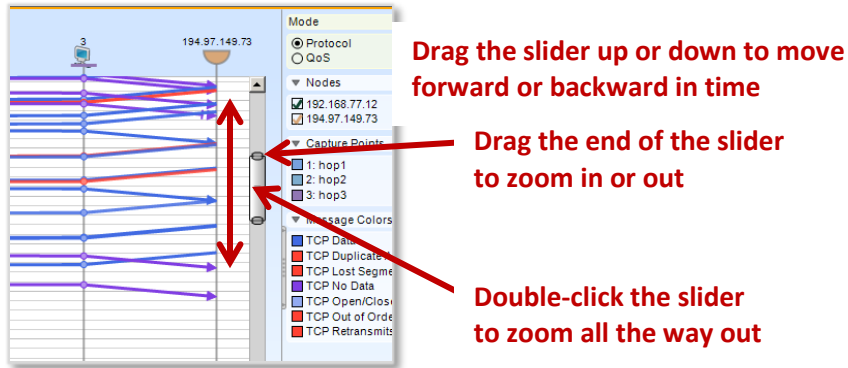
- Click and drag in the view to select a time interval to examine more closely. Then double-click the selection to zoom in.



- To deselect, click anywhere inside the main window.

Use the slider

- Drag the time slider up or down to move backward or forward in time.
- Drag the end of the slider in or out to zoom in or out.
- Double-click the middle of the slider to view the full time interval (unzoomed).

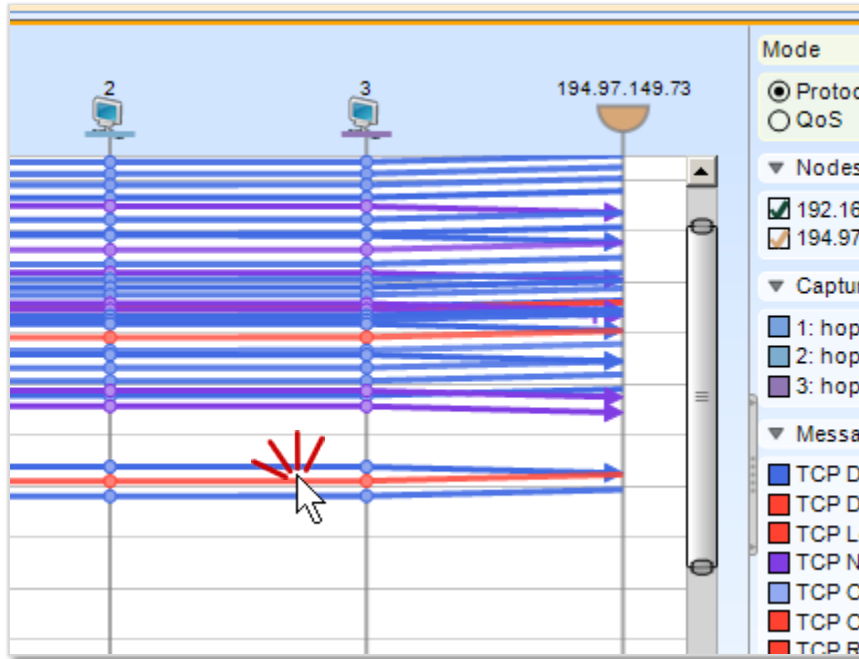


Use the mouse wheel or the up- and down-arrow keys

Click anywhere inside the main window. Then:

- Hold down the CTRL key and scroll—using the mouse wheel or the up- and down-arrow keys— to zoom in or out. Zooming is centered on the cursor. (That is, the area around the cursor stays in place while the rest of the window moves in or out.)
- Release the CTRL key and scroll to move forward or backward along the time line.

With a little practice, you will find that you can navigate the sequence diagram very quickly by scrolling and alternately holding or releasing the CTRL key.

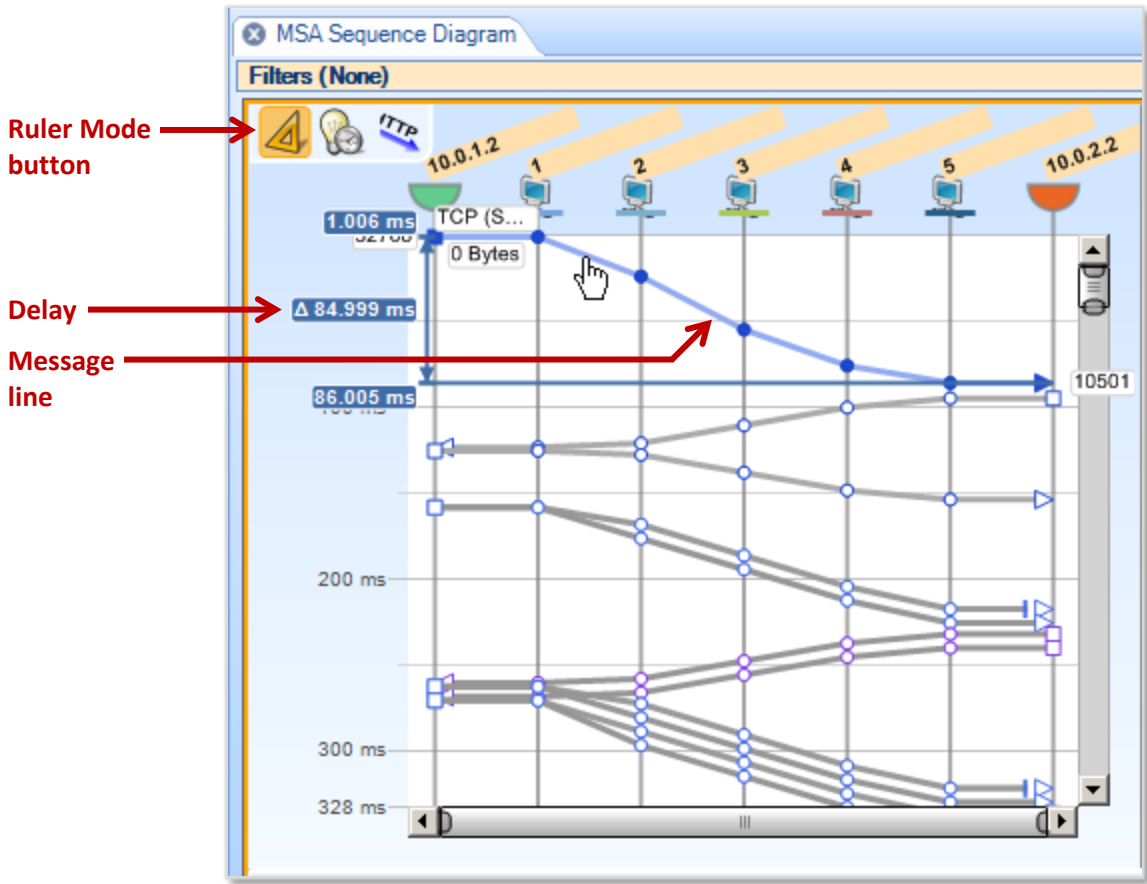


Scroll to move along the time line, using the mouse wheel or the up- and down-arrow keys

CTRL+scroll to zoom in and out

View delays and round-trip times

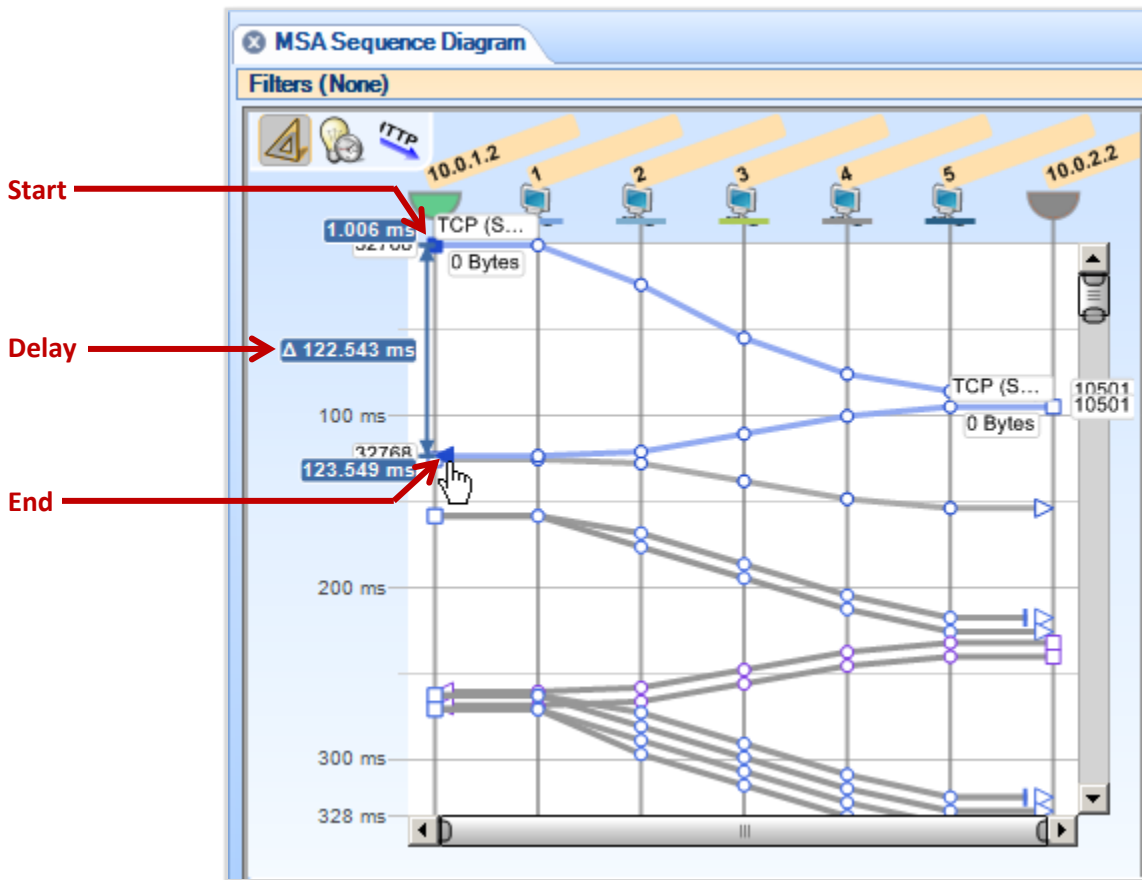
Click the Ruler Mode button to enter ruler mode. Then click a message line to see the delay for that message (the time it takes to go from the source node to the destination node). Note that the timing for capture points is precise, but that timing for end points is estimated.



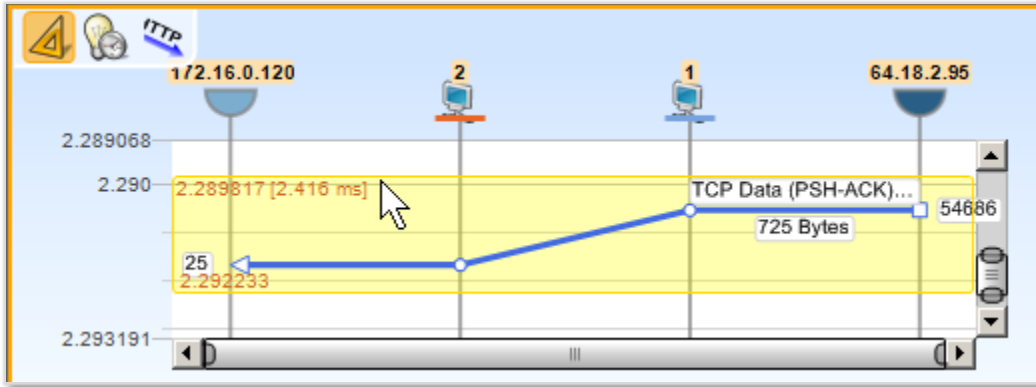
Or click a start point and an end point to see the time difference between any two time points on the sequence diagram.

- Square dots represent the source of a message.
- ▷ Triangular dots represent the destination of a message.
- Circular dots represent capture points along the path of a message through the network.

Unselected points are open; when you click a point, it fills with the color of the message line.

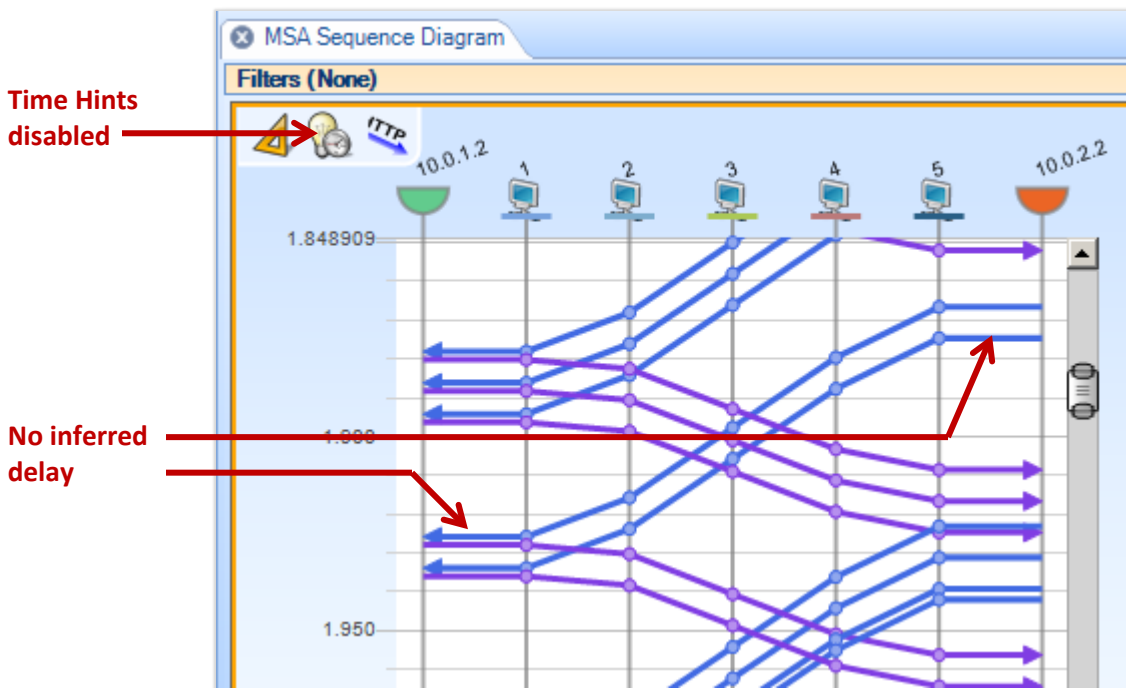


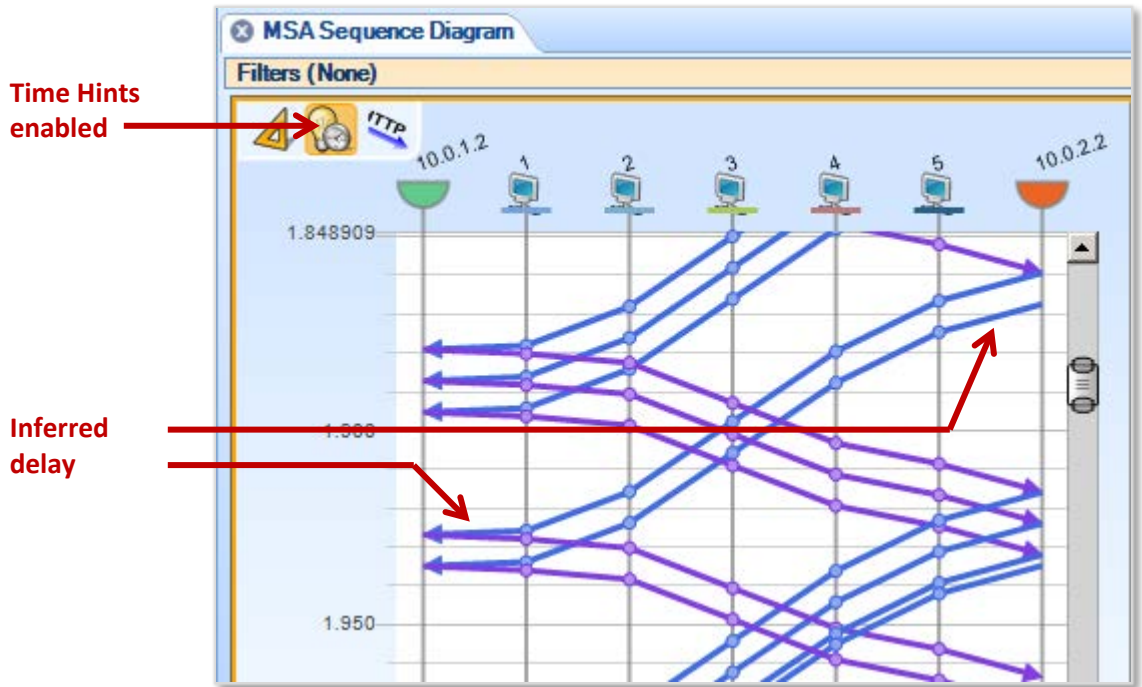
Ruler mode also shows the time span covered by a selection.



Estimate network delays

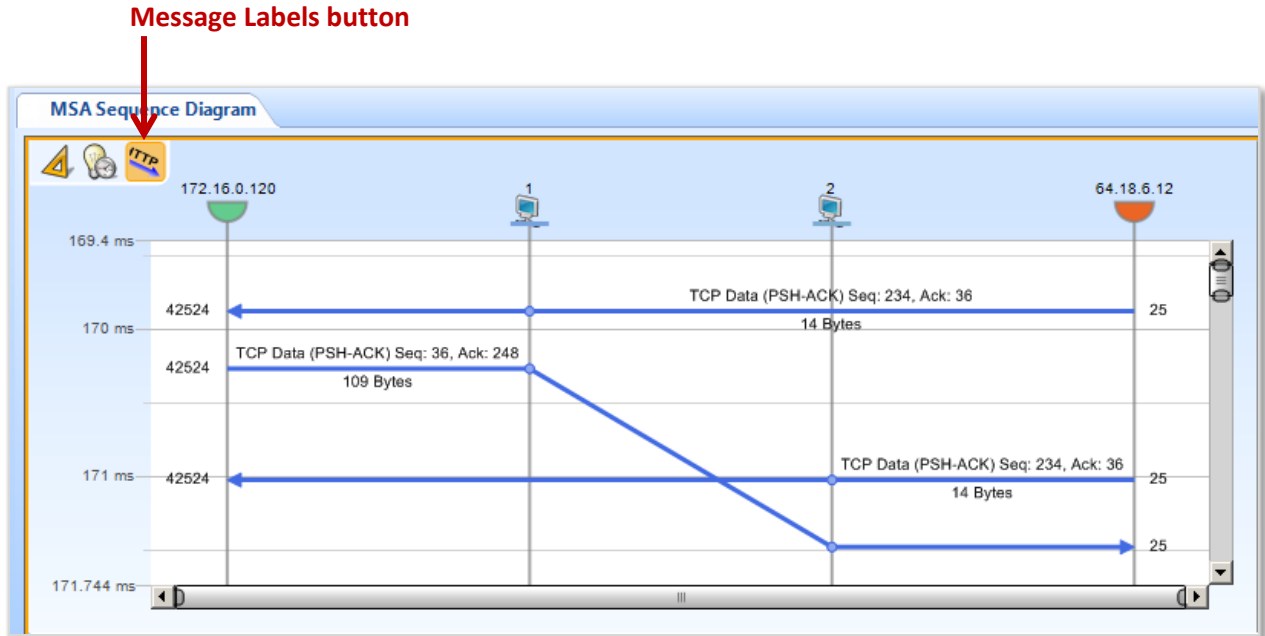
Click the Time Hints button to generate an estimate of network delays. The delays are inferred from the capture data and show up as sloped, rather than flat, timelines between the hosts and their nearest capture points.





Label message lines

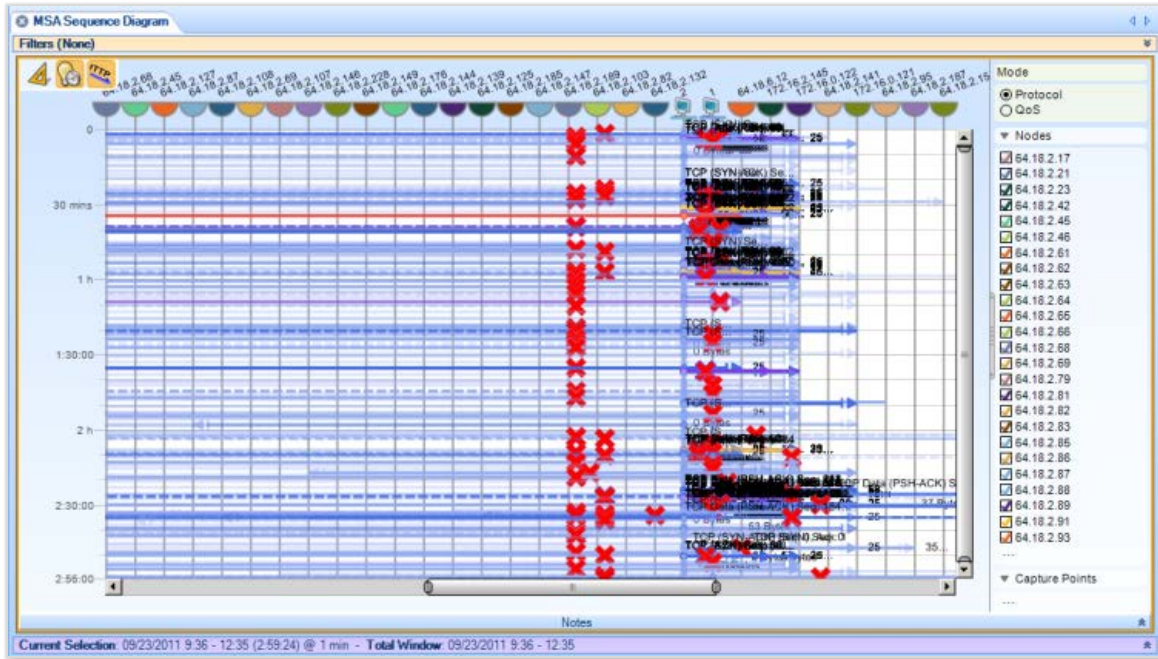
Click the Message Labels button to label the message lines with protocol information, byte counts, and so on.



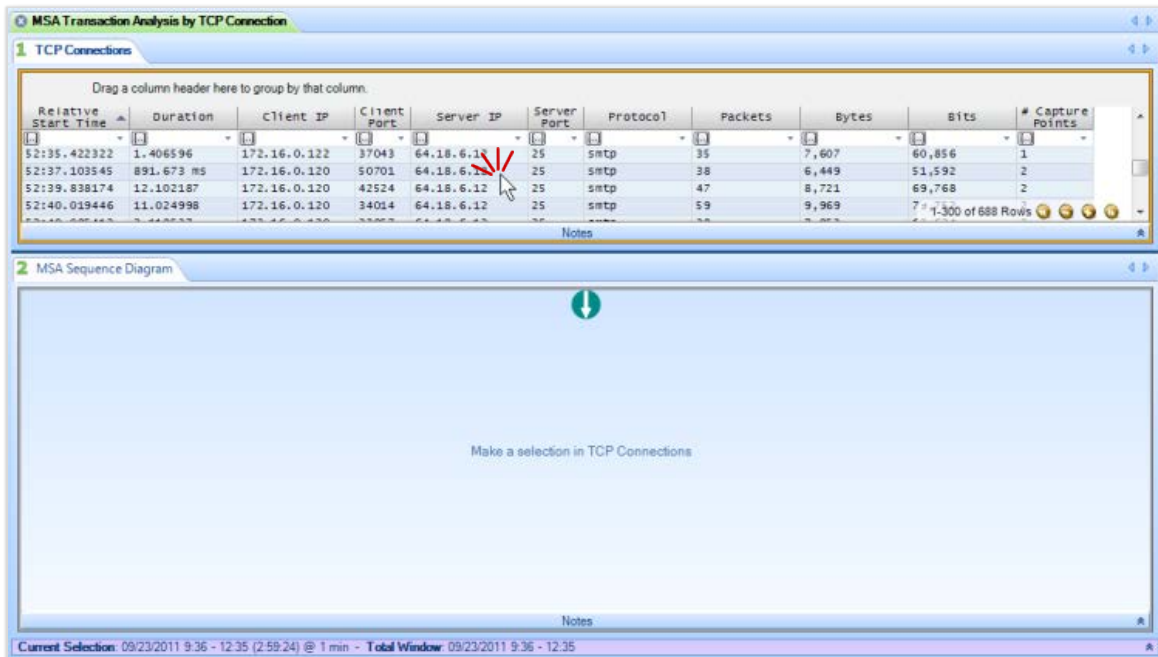
Simplify a sequence diagram

Sequence diagrams can get complicated. They are best used on small traces, or after drilling down from a larger data set.

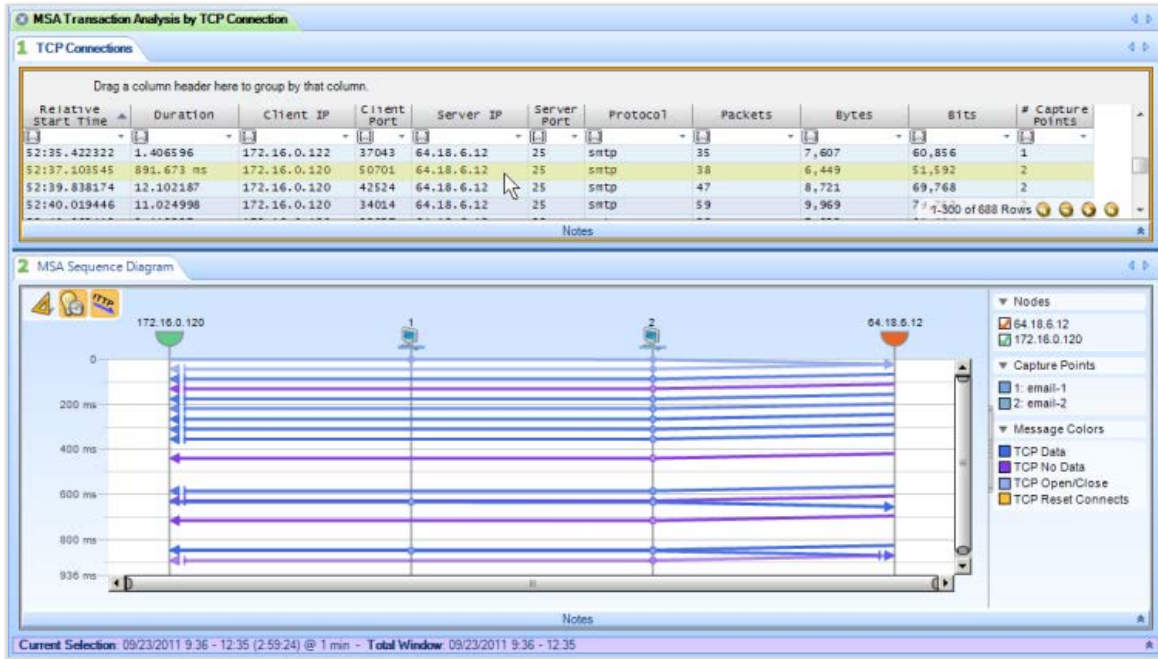
You may be able to simplify a sequence diagram if you know the TCP connections. For example, here is a somewhat complicated sequence diagram created by the MSA Sequence Diagram view.



If you know the TCP connection you want to see, you can apply the MSA Transaction Analysis by TCP Connection view to the same data. Choose the connection you want from the data grid...

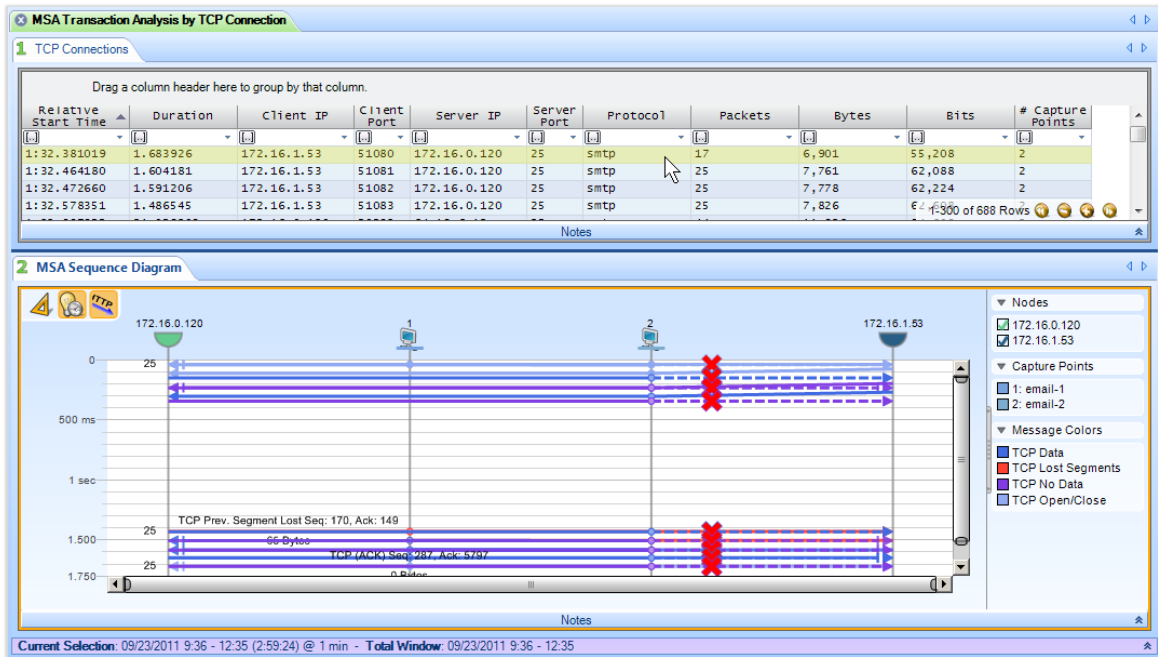


...and a simplified sequence diagram, showing only that TCP connection, is displayed in the lower window.



You can then zoom in more easily and continue your analysis.

If you are trying to track down a problem but don't know the TCP connection, you can quickly select successive TCP connections from the data grid until a troublesome-looking one appears.

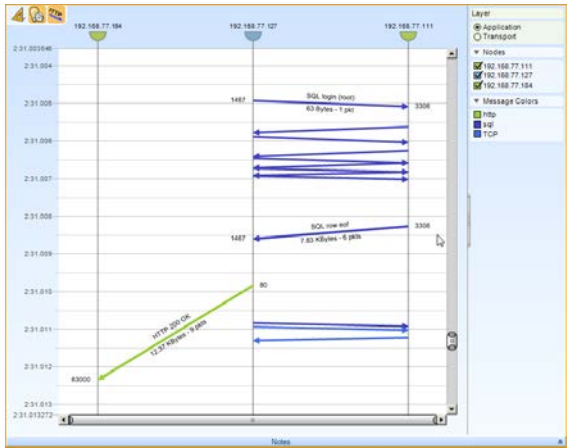


Then you can zoom in, drill down, and diagnose the problem.

Security Disclosures

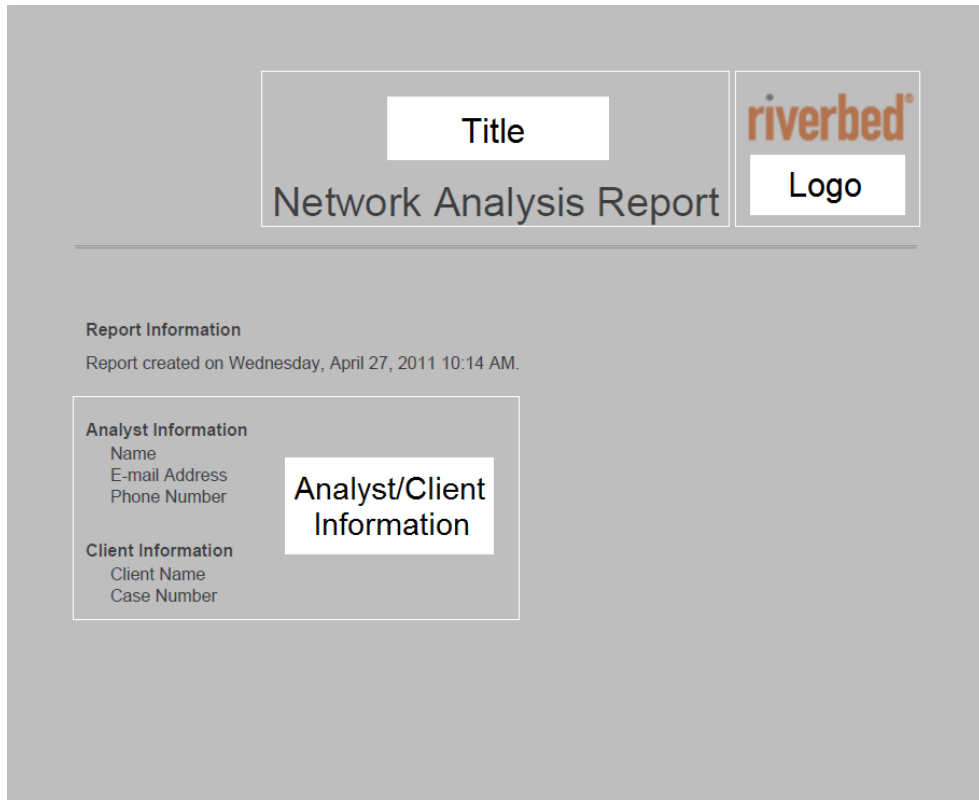
Please carefully read the following important disclosures.

- Unlike Wireshark, once a valid decryption key is defined, all relevant subsequent traffic is automatically decrypted, and, if saved, will be stored decrypted to disk.
- Regardless of whether decryption keys are shown or hidden, they are stored on disk in plain text. Exporting a configuration file will export the plain text decryption keys that have been entered.

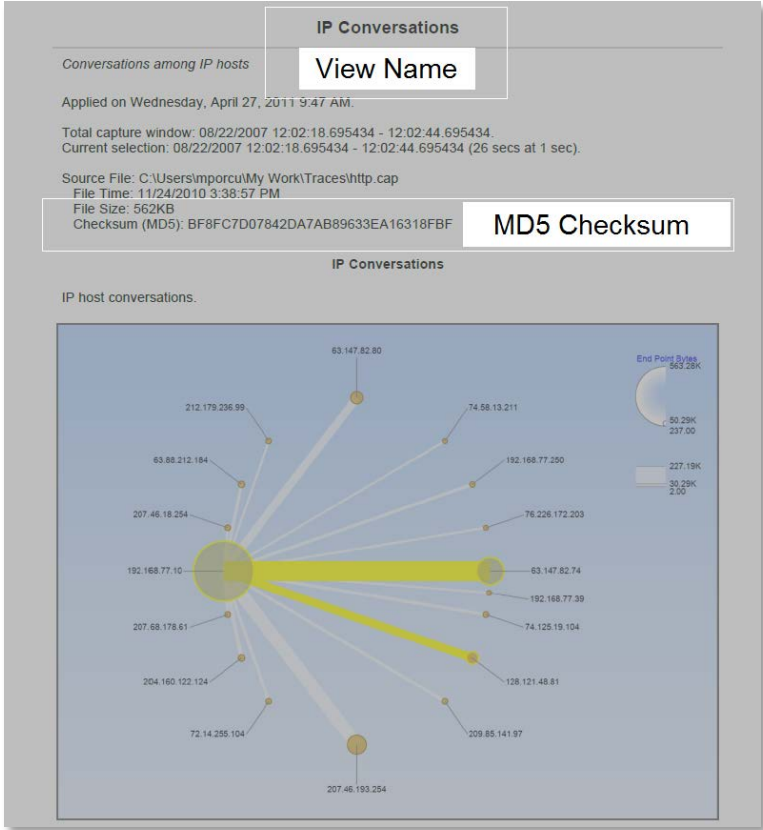


Sequence

Appendix B Report Example Breakdown



Report layout



IP Conversations layout

IP Conversations Discovery

Conversations among IP hosts shown in a table.

Applied on Wednesday, April 27, 2011 11:11 AM.

Total capture window: 08/22/2007 12:02:18.695434 - 12:02:44.695434.
 Current selection: 08/22/2007 12:02:18.695434 - 12:02:44.695434 (26 secs at 1 sec).

Source File: C:\Users\mporc\My Work\Traces\http.cap
 File Time: 11/24/2010 3:38:57 PM
 File Size: 562KB
 Checksum (MD5): BF8FC7D07842DA7AB89633EA16318FBF

IP Conversations

A grid containing the amount of bits, bytes & traffic.

Data as Table

Data										
Address A	Address B	Bytes	Bits	Packets	Bytes A->B	Bytes B->A	Bits A->B	Bits B->A	Packets A->B	Packets B->A
63.147.82.74	192.168.77.10	227,185	1,817,480	284	196,176	31,009	1,569,408	248,072	156	128
192.168.77.10	207.46.193.254	139,648	1,117,184	164	23,920	115,728	191,360	925,824	76	88
63.147.82.80	192.168.77.10	75,387	603,096	87	70,106	5,281	560,848	42,248	50	37
128.121.48.81	192.168.77.10	70,351	562,808	100	52,518	17,833	420,144	142,664	52	48
192.168.77.10	204.160.122.124	15,293	122,344	21	1,294	13,999	10,352	111,992	9	12
63.88.212.184	192.168.77.10	11,082	88,656	38	4,308	6,774	34,464	54,192	16	22
74.125.19.104	192.168.77.10	6,430	51,440	14	3,116	3,314	24,928	26,512	6	8
192.168.77.10	192.168.77.250	4,931	39,448	24	922	4,009	7,376	32,072	12	12
192.168.77.10	209.85.141.97	4,314	34,512	15	1,914	2,400	15,312	19,200	7	8
72.14.255.104	192.168.77.10	3,013	24,104	11	784	2,229	6,272	17,832	5	6
192.168.77.10	207.68.178.61	2,246	17,968	6	1,090	1,156	8,720	9,248	4	2

IP Conversations Discovery
 Report created on Wednesday, April 27, 2011 11:11 AM

Page 3/4

IP Conversations Discovery layout

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com