



VIAssist 2.6 User Guide

December 14, 2011

Revision History

Date	Revision	Paragraphs Affected	Description
1/11/2011	2.4	All	User manual for VIAssist 2.4
11/8/2011	2.6	All	User manual updated for VIAssist 2.6. Heavy revisions to every section. New sections added.

Table of Contents

1	About.....	4
2	System Overview	5
2.1	Client Architecture	5
2.2	Visual Query Builder	6
2.3	Smart Aggregator	6
2.4	Report Designer.....	6
2.5	Limitations.....	7
3	User Guide	8
3.1	Opening Data Sources	8
3.1.1	Opening Remote (Server) Data Sources	8
3.1.2	Opening Embedded Data Sources	9
3.2	Using the Visual Query Builder	12
3.2.1	Selecting Data	13
3.2.2	Limiting Data	16
3.2.3	Default Criteria.....	21
3.2.4	Additional Features.....	25
3.3	Using the Smart Aggregator	26
3.3.1	Configuration	27
3.3.2	Aggregation Report.....	29
3.4	Visualizing Data Sources.....	32
3.4.1	Using Multiple Monitors	33
3.4.2	How to Detect and Verify Anomalies.....	39
3.4.3	Viewing Temporal Data.....	45
3.5	Interacting with Visualizations	46
3.5.1	Using Filter Widgets.....	46
3.5.2	Filtering Data.....	49
3.5.3	Highlighting Data.....	52
3.5.4	Collaboration Tools	57
3.5.5	Context Menus.....	67
3.5.6	Manipulating the Data Sheet	71
3.5.7	Arranging Views	75
3.5.8	Drilling Into Data	81
3.6	Using the Report Designer	84
3.6.1	Create a Report	84
3.6.2	Save a Report	86
3.6.3	Report Templates.....	87
3.7	Options	88

3.7.1	General.....	89
3.7.2	Data Coloring	92
3.7.3	Visualization Appearance.....	96
3.7.4	Data Tools	97

1 About

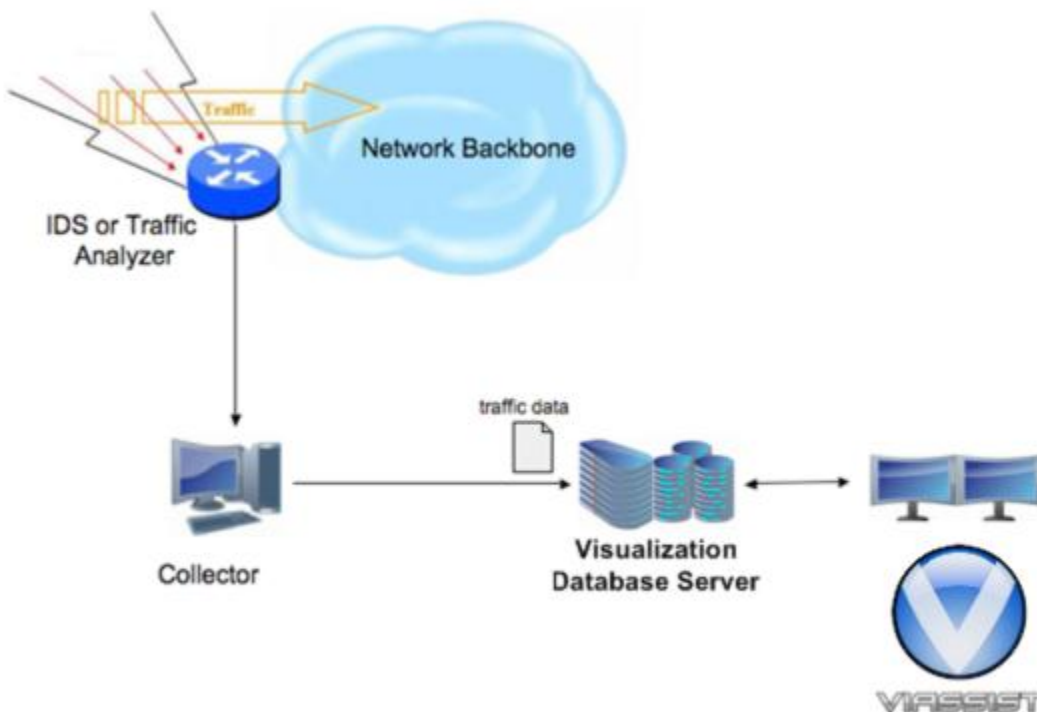
The purpose of VIAssist is to provide cyber-security analysts with a fully-functional visualization tool that supports analysts in pursuing their goals and objectives. VIAssist is the result of years of effort working with analysts and performing a cognitive task analysis of their work habits, needs, and repetitive tasks. Months spent working with analysts in operational environments led to the creation of not just another visualization tool, but to VIAssist - a visualization framework.

VIAssist brings numerous commercial visualization tools together in a collaborative interactive interface. Designed around the analyst-user, VIAssist integrates these commercial tools under a multi-monitor interface that is designed to support global situational awareness and incident handling.

All VIAssist components visualize data from the same dataset. As the user manipulates the data from within VIAssist, changes and highlights are reflected simultaneously in each of the integrated tools. Supporting this collaborative integration, VIAssist provides data pre-processing to filter and collate information prior to presentation. The combination of pre-processing, multiple views from differing visual tools, and a fully user-controlled framework make VIAssist a powerful ally for cyber-security analysts.

2 System Overview

Accessing, viewing, and analyzing network traffic information is easy with VIAssist and requires minimal setup. Network devices gather network information from an Intrusion Detection System (IDS), Intrusion Protection System, Traffic Analyzer, or a network sniffing device. This network traffic information is exported from a Collector's database and imported into the VIAssist Visualization Database Server. VIAssist can then visualize the data from the database.



2.1 Client Architecture

The VIAssist client is written in C#, utilizing Microsoft's .NET framework, and mixing in C++ ActiveX controls for some visualizations. Data types, data labels, and data values are represented by a robust XML data model that VIAssist uses to populate data from a data repository. Fetched data is kept in memory to increase the speed of rendering and interacting with visualizations by reducing database transaction requests. All data in local memory is shared by the VIAssist components.

VIAssist components are configurable; after an initial integration effort, new components can be used within the VIAssist framework. Components that have already been integrated can be used optionally.

VIAssist uses a workspace model for managing its components. A workspace can be populated with any type and number of components which can be saved together as a workspace. The workspace can then be reused with existing or new data sources instead of requiring the user to reconfigure their environment every time they want to analyze data.

2.2 Visual Query Builder

VIAssist's Visual Query Builder is an easy to use, powerful interface used to concentrate the investigation of data into a subset of the dataset to be viewed in the workspace. Creating expressions with the Visual Query Builder is similar to the *where* clause of an SQL statement but does not require any knowledge of SQL.

Making query building quick and easy without having to learn a textual syntax decrease's the time it takes for an analyst to investigate data.

To learn more about the Visual Query Builder, [please see the "Using the Visual Query Builder" section](#).

2.3 Smart Aggregator

Massive datasets present a tricky problem when it comes to rendering and interacting with visualizations. Visualizations need to be high performing and high quality to not impact the time it takes for an analyst to investigate data. The Smart Aggregator was created to make visualizing massive datasets more intelligent by aggregating data into smaller datasets containing clusters of data that have the same value. Intelligent aggregation of data can greatly reduce the volume of data while maximizing the relevant information displayed in visualizations.

To learn more about the Smart Aggregator, [please see the "Using the Smart Aggregator" section](#).

2.4 Report Designer

Collaboration with other analysts and presenting the results of analysis is an important part of the investigation process. Co-workers, managers, and managing operations want to see the results of an analysis investigation. The VIAssist Report Designer fills this role by making it simple to create visual reports of an analysis. A report is created in a familiar slide fashion and supports text annotations, drawings, and other typical presentation options as well as making it easy to include visualizations and components from within VIAssist to show the data.

Reports created with VIAssist's Report Designer can be saved in a VIAssist specific format, or as a PowerPoint presentation or PDF file for sharing with others.

The Report Designer also supports Report Templates, which make it easy to recreate a report with updated data information.

To learn more about the Report Designer, [please see the "Using the Report Designer" section](#).

2.5 Limitations

VIAssist is a pseudo real-time network data analyzer. VIAssist is not an intrusion detection system or a network sniffer. VIAssist displays data that was exported from a database that contains real-time information from an IDS or Traffic Analyzer.

The display time of large datasets grows with the volume of data that is retrieved from a data source. Display times can be reduced by making use of the Smart Aggregator to aggregate large datasets into smaller, more manageable clustered datasets, and by making use of the Visual Query Builder to limit the data fetched to a more applicable, precise subset of the data.

To learn more about the Smart Aggregator, [please see the "Using the Smart Aggregator" section](#).

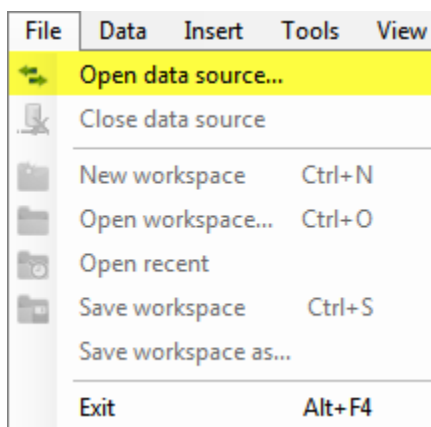
To learn more about the Visual Query Builder, [please see the "Using the Visual Query Builder" section](#).

3 User Guide

3.1 Opening Data Sources

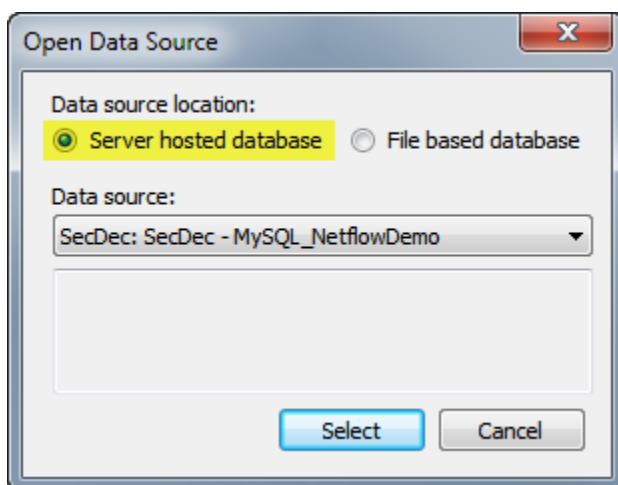
VIAssist supports two general forms of data sources: remote and embedded. Remote data sources are databases hosted on a server. Embedded data sources are kept on the local machine and are created from a data file.

To open a data source, open the File menu and select the Open Data Source option:

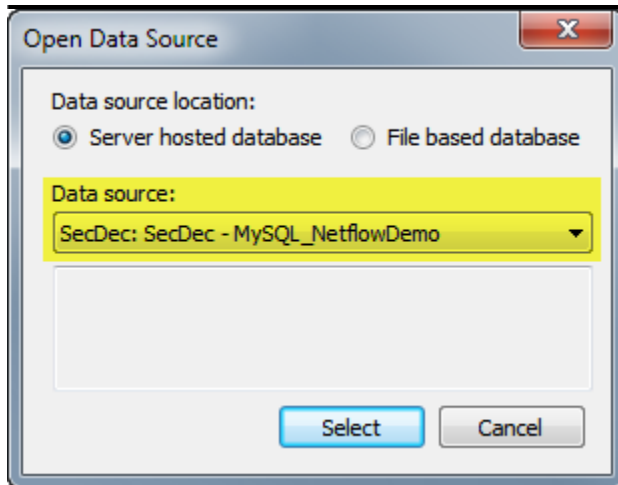


3.1.1 Opening Remote (Server) Data Sources

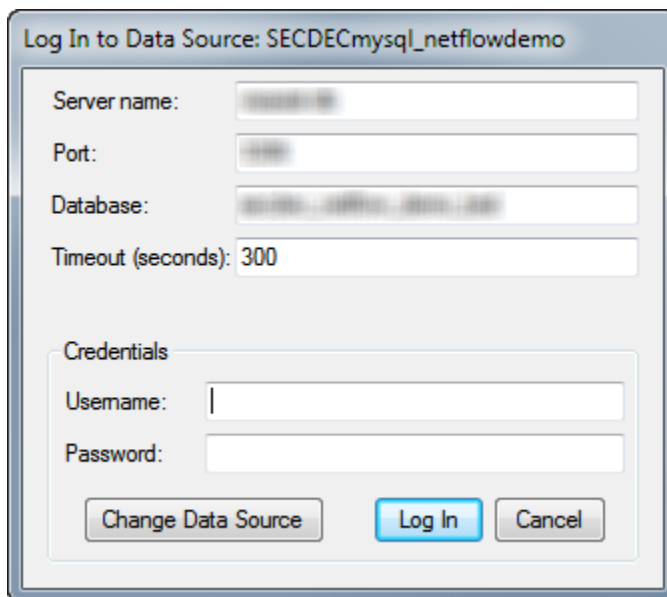
To open a data source from a remote server location, select the Server hosted database option:



The data source drop down box will populate with all potential data sources that are server hosted:



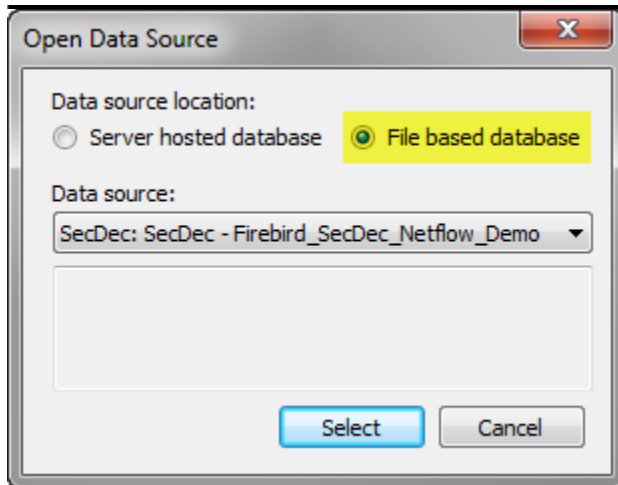
Select the appropriate data source from the drop down box and then press the Select button in order to log in to the data source. Different types of databases require different sorts of credential and option information. The login dialog that is displayed will reflect all required options to login to a specific type of database. As an example, a MySQL login dialog looks like this:



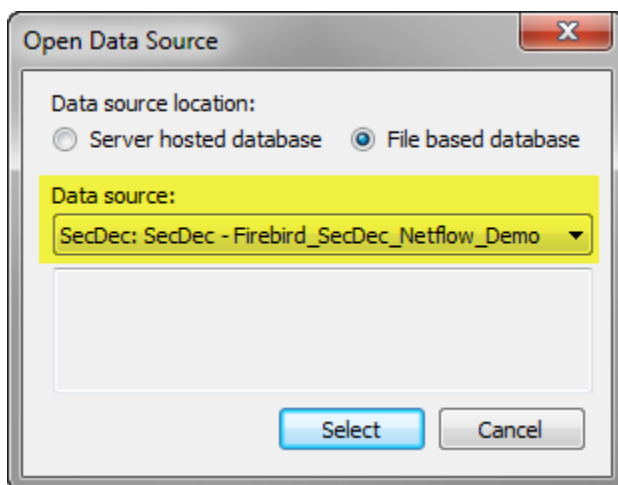
Other login dialogs will be similar but with different requirements.

3.1.2 Opening Embedded Data Sources

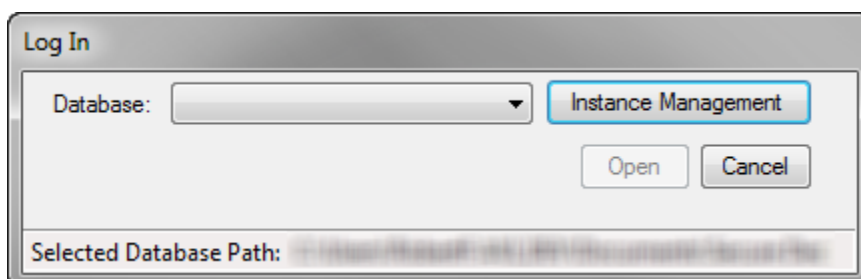
To use an embedded data source, select the File based database option:



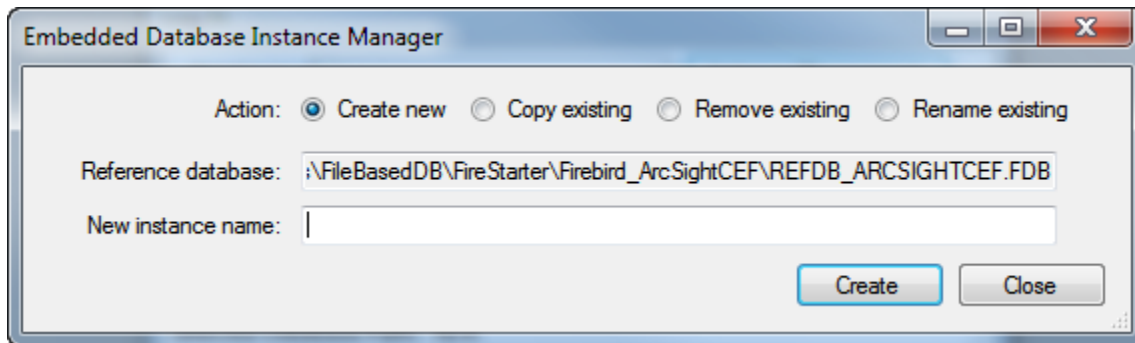
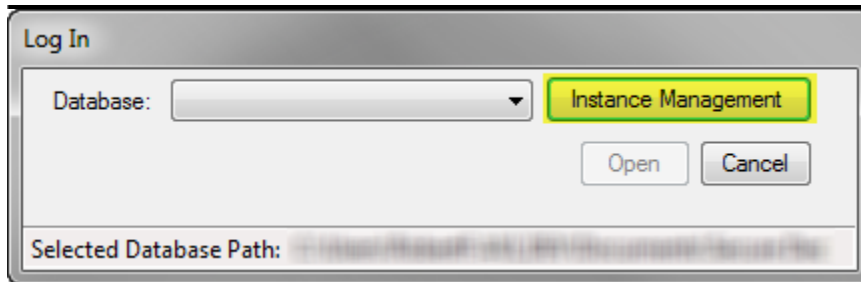
The data source drop down will populate with potential embedded data sources:



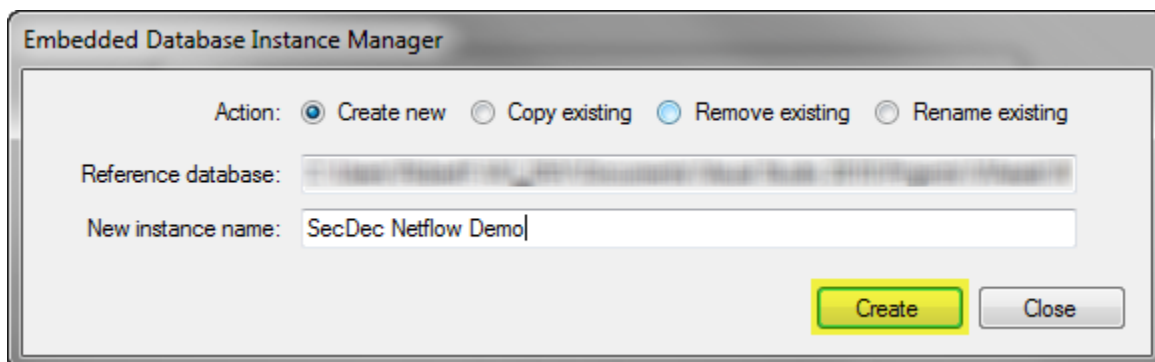
Select the appropriate data source from the drop down box and then press the Select button in order to create the embedded database or to open an existing embedded database:



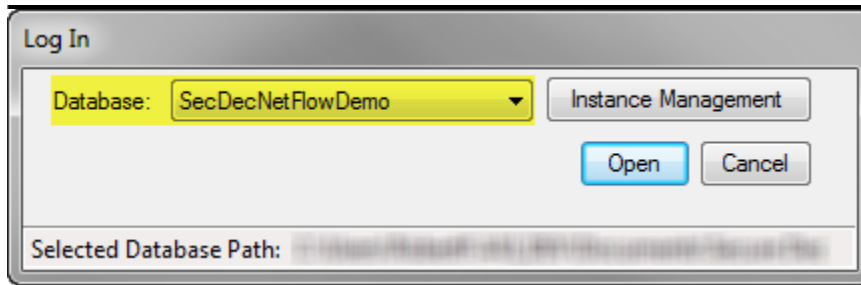
If no database is available from the database drop down, a new embedded database needs to be created through the instance management. Click the Instance Management button to open the Instance Management dialog:



Several options exist for instance management. To create a new embedded database, keep the default Create new option selected. A reference database file is needed to import data into the new embedded database. This file is automatically selected by VIAssist based on the initial data source that was selected. Simply enter a new instance name and click the create button:



Once the new embedded database has been created, it will appear in the database drop down of the login dialog:

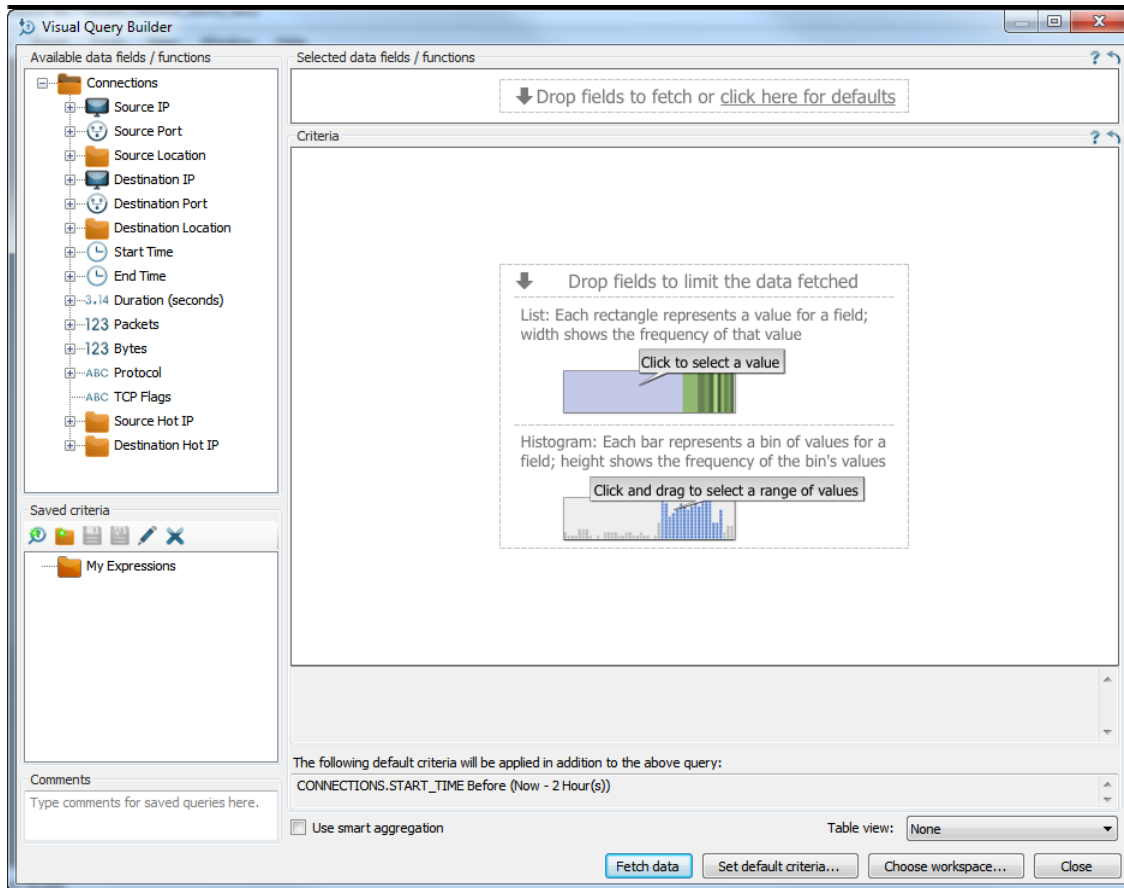


Select the appropriate database and click on the open button to open and use this data source. In the future, this database will be available from the start until it is deleted.

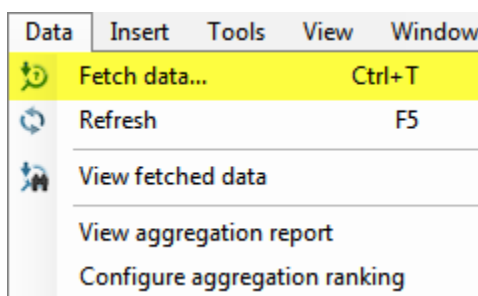
3.2 Using the Visual Query Builder

VIAssist's Visual Query Builder is an easy to use, powerful interface used to concentrate the investigation of data into a subset of the dataset to be viewed in the workspace. Creating expressions with the Visual Query Builder is similar to the *where* clause of an SQL statement but does not require any knowledge of SQL.

Expressions created by the Visual Query Builder can be saved for future use and modification; expressions along with related notes are available to all users of the VIAssist client.

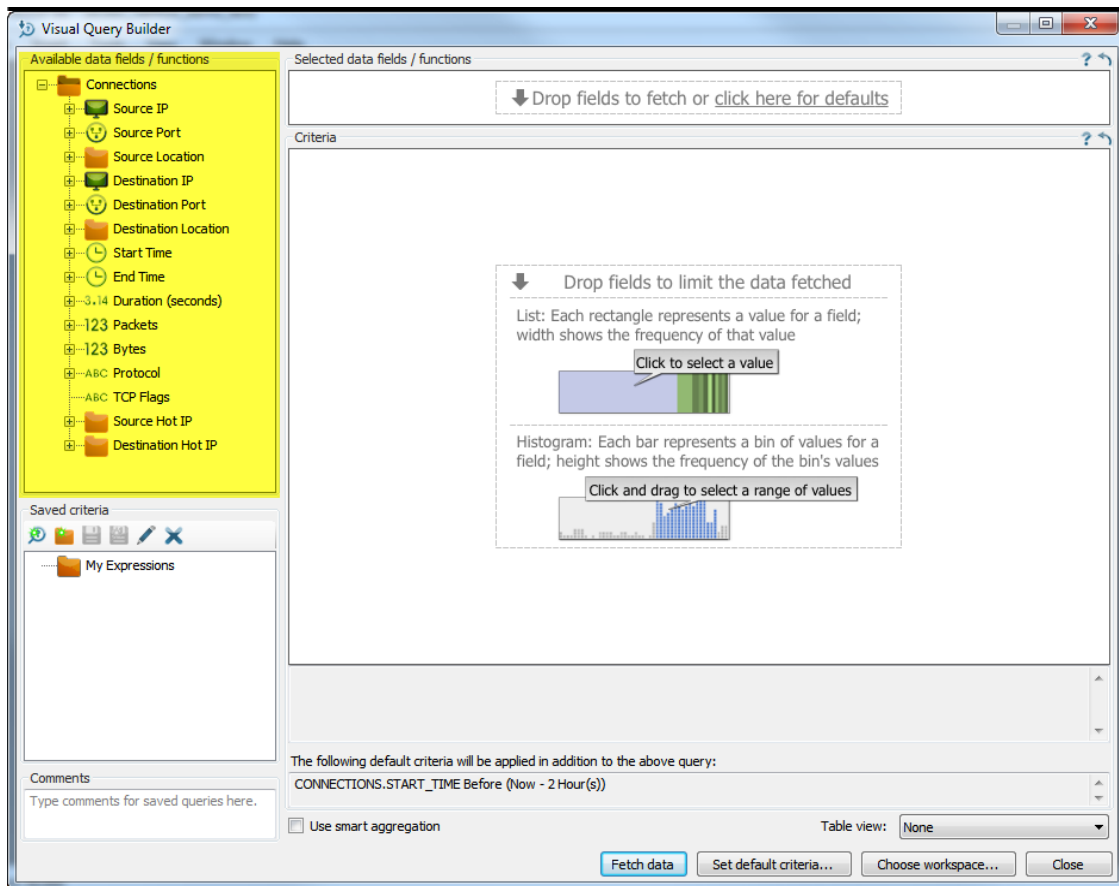


To access the Visual Query Builder, first [open a data source](#), and then open Data menu and select the Fetch Data option:

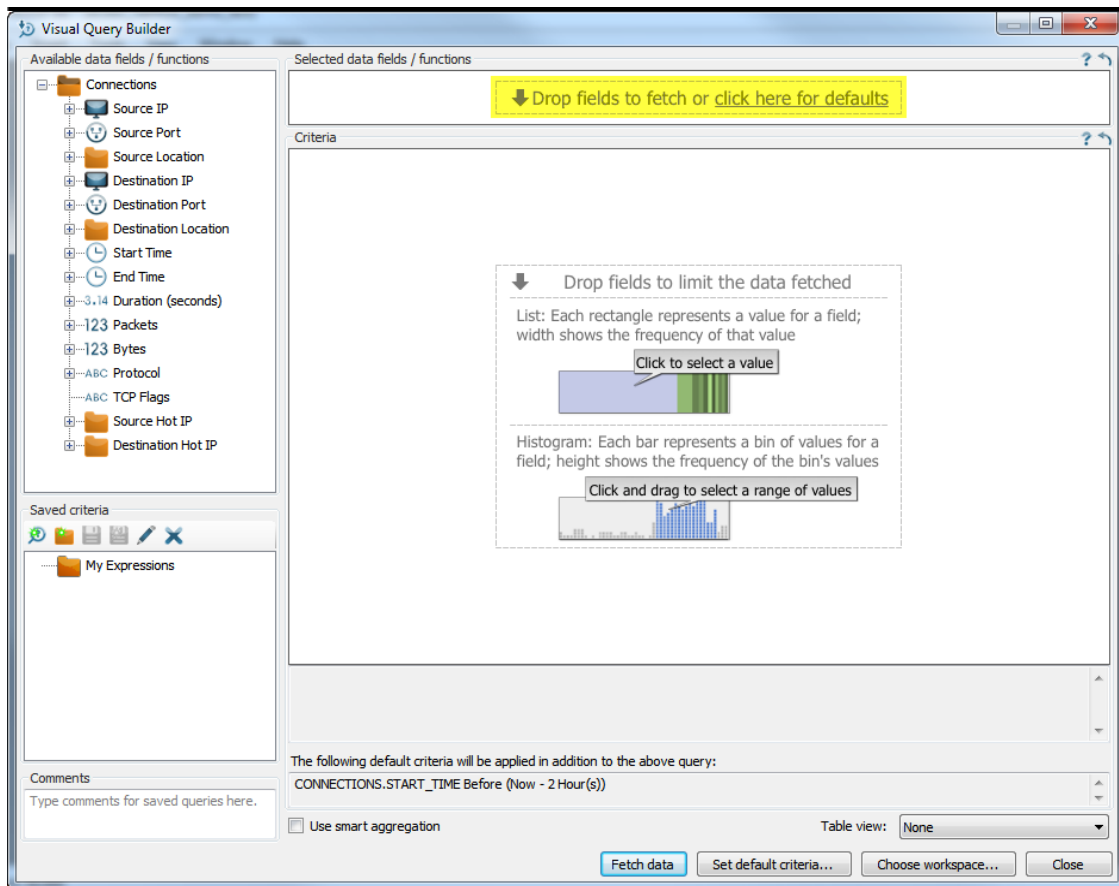


3.2.1 Selecting Data

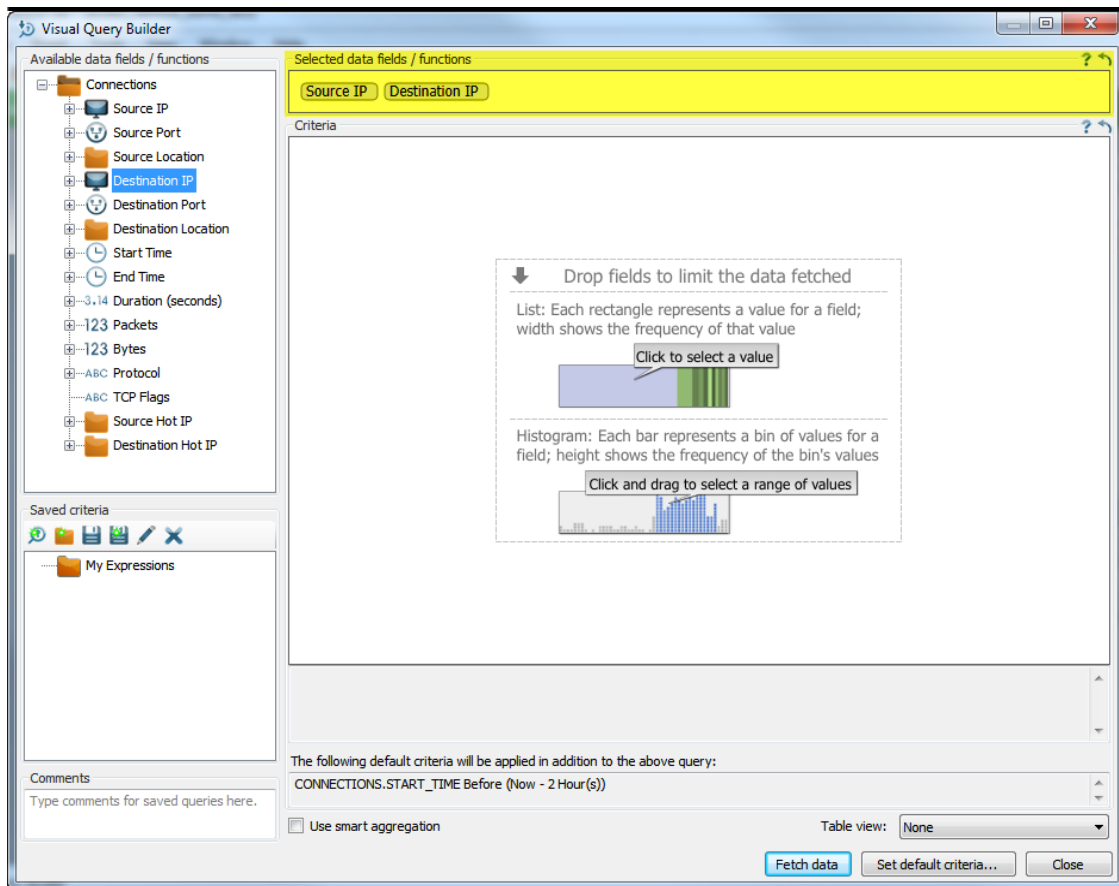
The Visual Query Builder contains a list of all available data fields that can be used for building queries. Entries can be expanded to provide further granularity if applicable.



Default fields can be added by clicking in the Selected data fields / function section when no fields have yet been added.



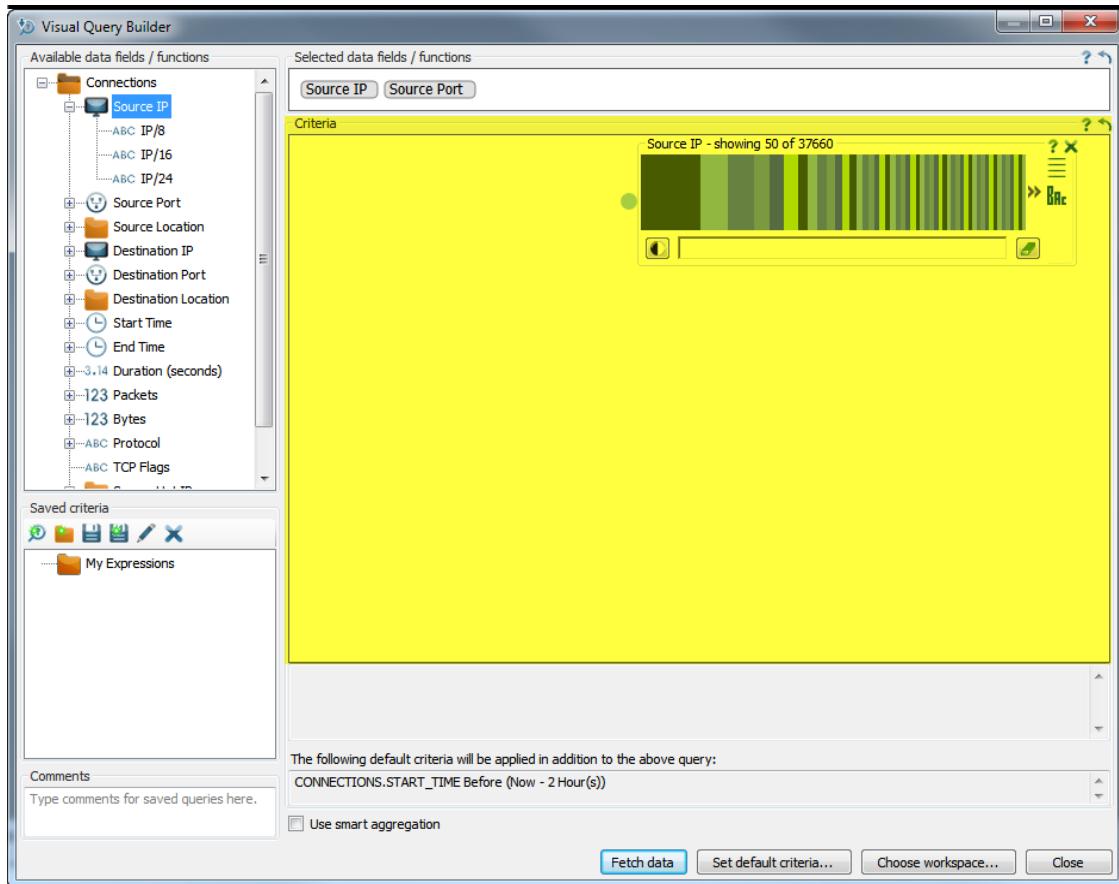
Fields can be selected and then dragged with the mouse to the Selected data fields / functions section to indicate the data for those fields should be fetched.



When the Fetch Data button is pressed, all data related to those fields present in the Selected data fields / functions section will be fetched. The data fetched can be further limited by criteria. To see more information about limiting data, [please see the "Limiting Data" section](#).

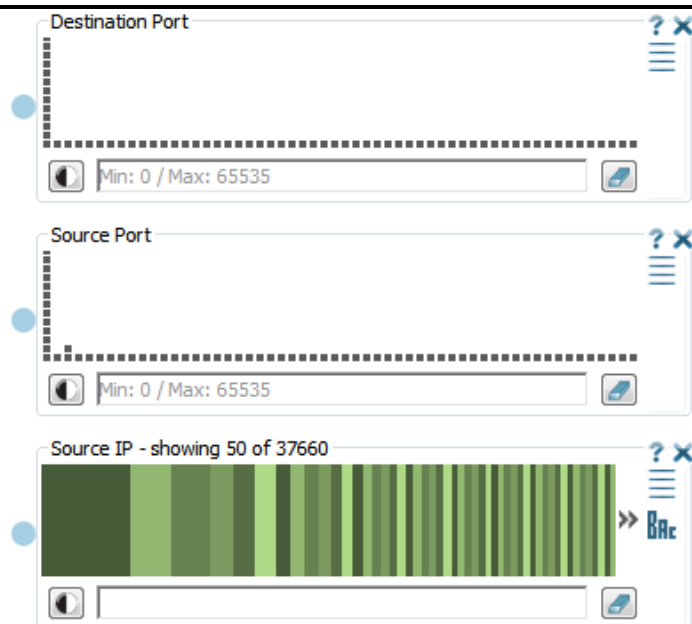
3.2.2 Limiting Data

The Visual Query Builder can be used to limit the data that VIAssist fetches by building a query expression. To begin building an expression, select and drag a field from the Available data fields / functions to the Criteria section of the Visual Query Builder. Alternately, simply double-click a field to automatically place it in the Criteria section.

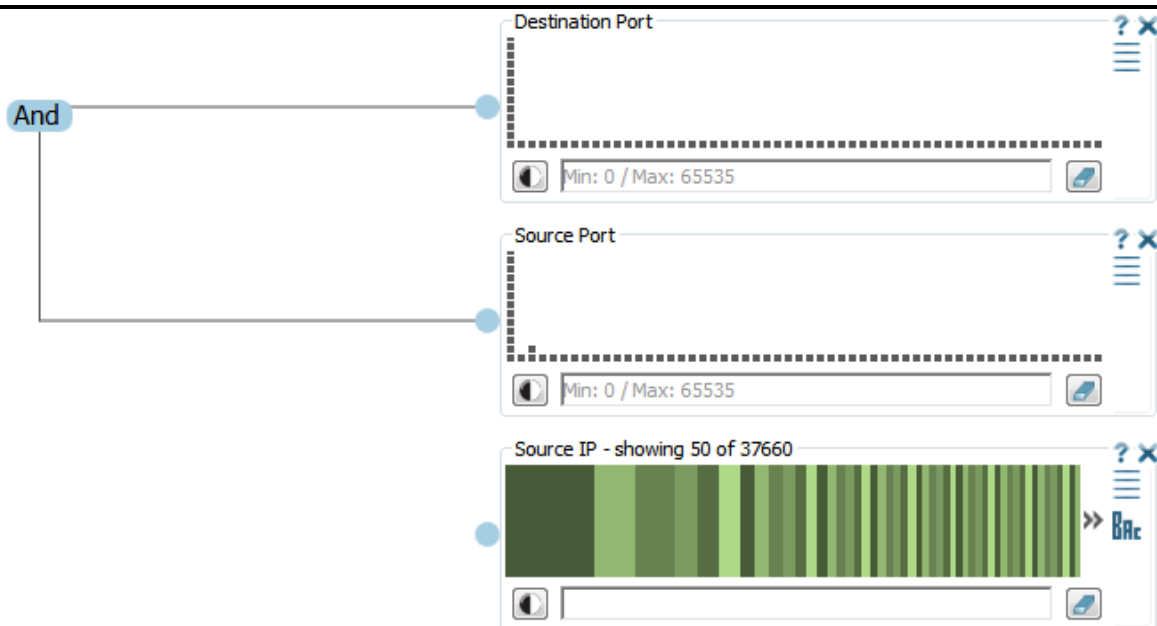


Adding a field to the Criteria section creates a filter where specific values of that field can be specified. To learn more about using filters, [please see the "Using Filter Widgets" section](#).

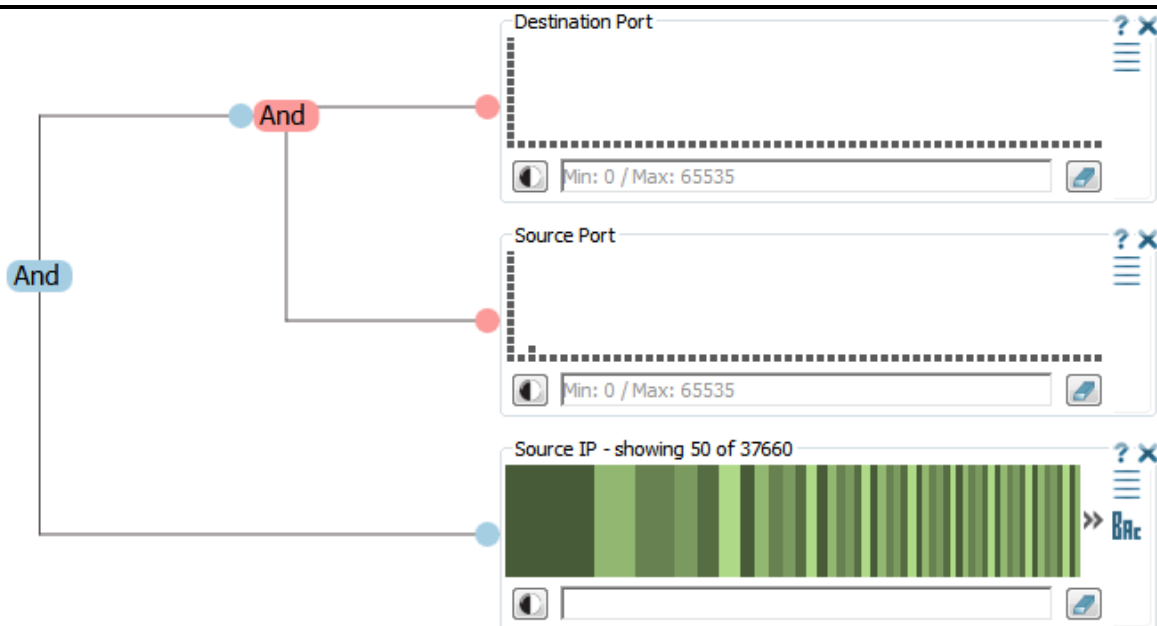
Multiple fields can be added to the Criteria section to build powerful expressions. For example, start with the Source IP, Source Port, and Destination Port fields:



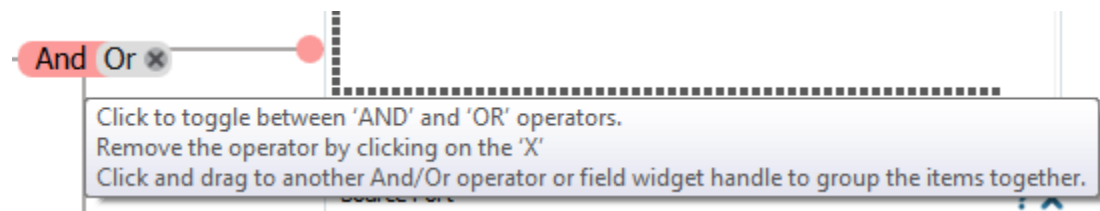
To build an expression with the three criteria fields, use the left mouse button to click and drag from one of the blue dots next to a filter to another blue dot next to a different filters:



Filters and operators can also be directly connected by using the left mouse button to click and drag from an operator to a blue dot next to a filter, or vice versa:



Two operators are available: And and Or. The And operator is used by default. To use the Or operator, hover over the operator that needs to be changed and then click. This will switch the operator from an And to an Or, and vice versa:

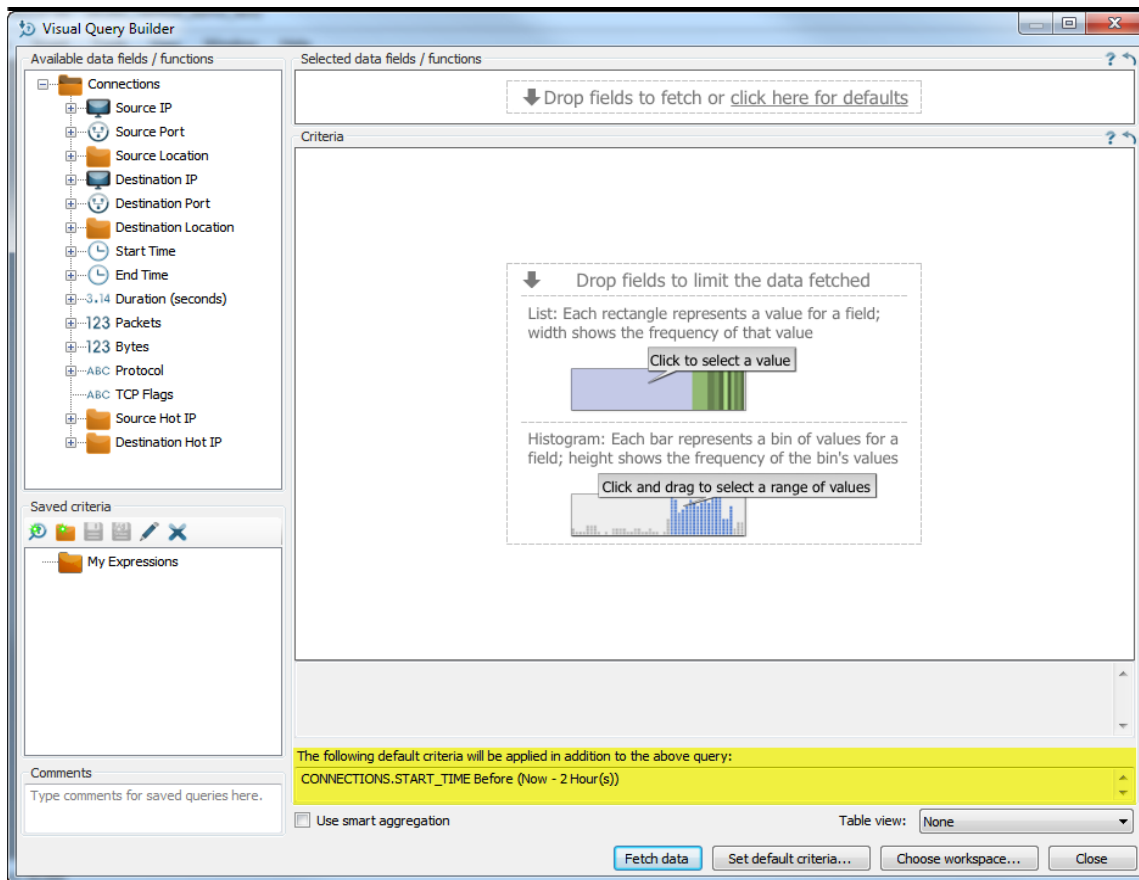




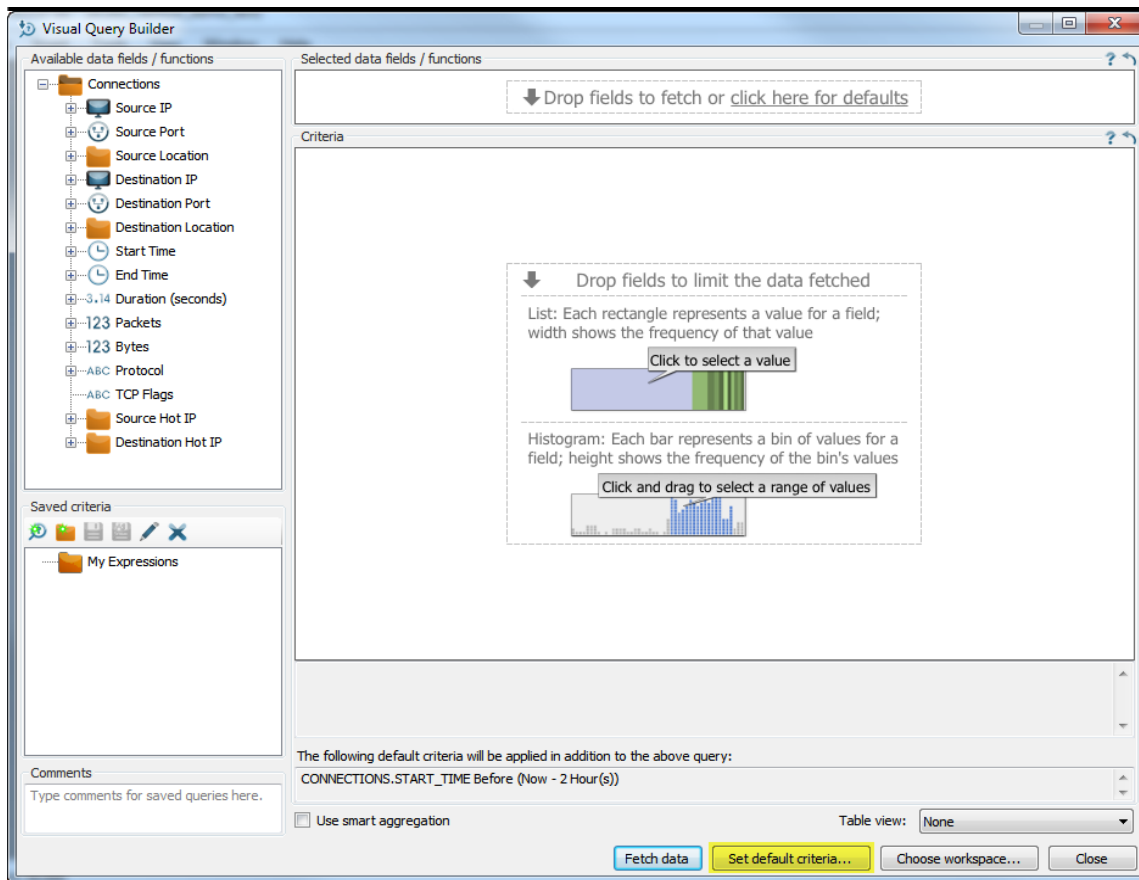
Data can also be limited by Default Criteria. To view more information about Default Criteria, [please see the "Default Criteria" section](#).

3.2.3 Default Criteria

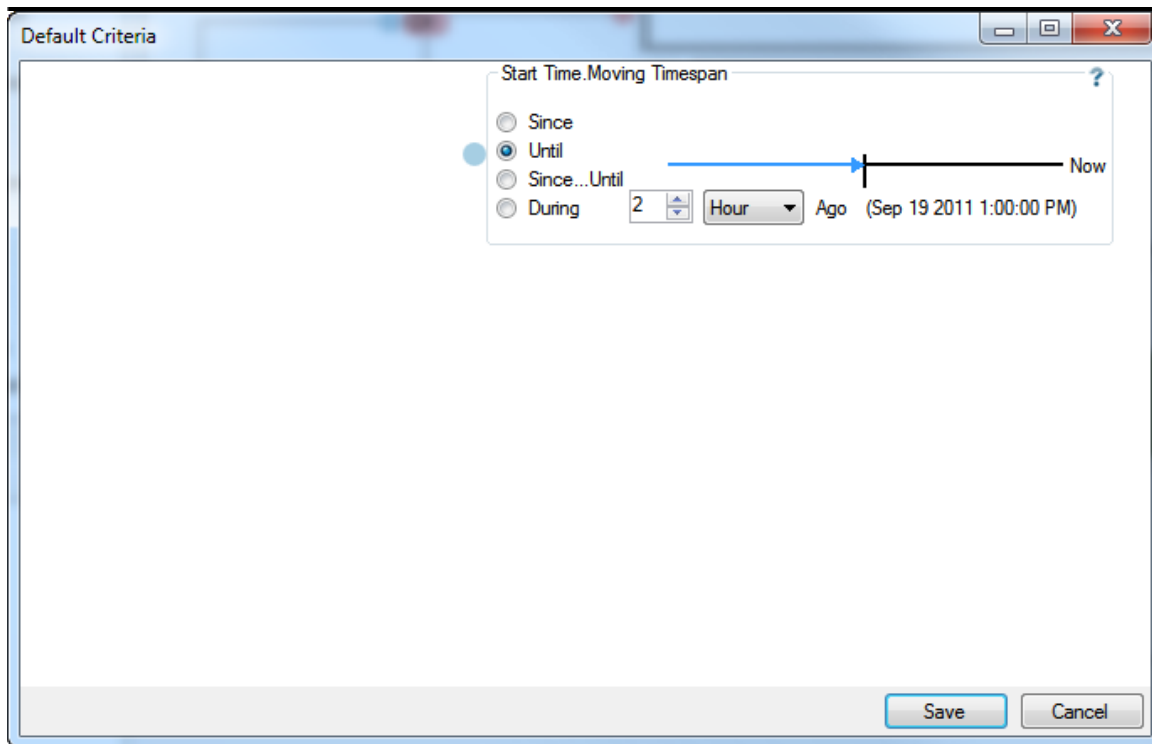
The Visual Query Builder may have Default Criteria present. Default Criteria is pre-defined, data limiting criteria that is configured for a specific customer as part of the initial VIAssist deployment. Default Criteria is automatically included as part of any query created with the Visual Query Builder.



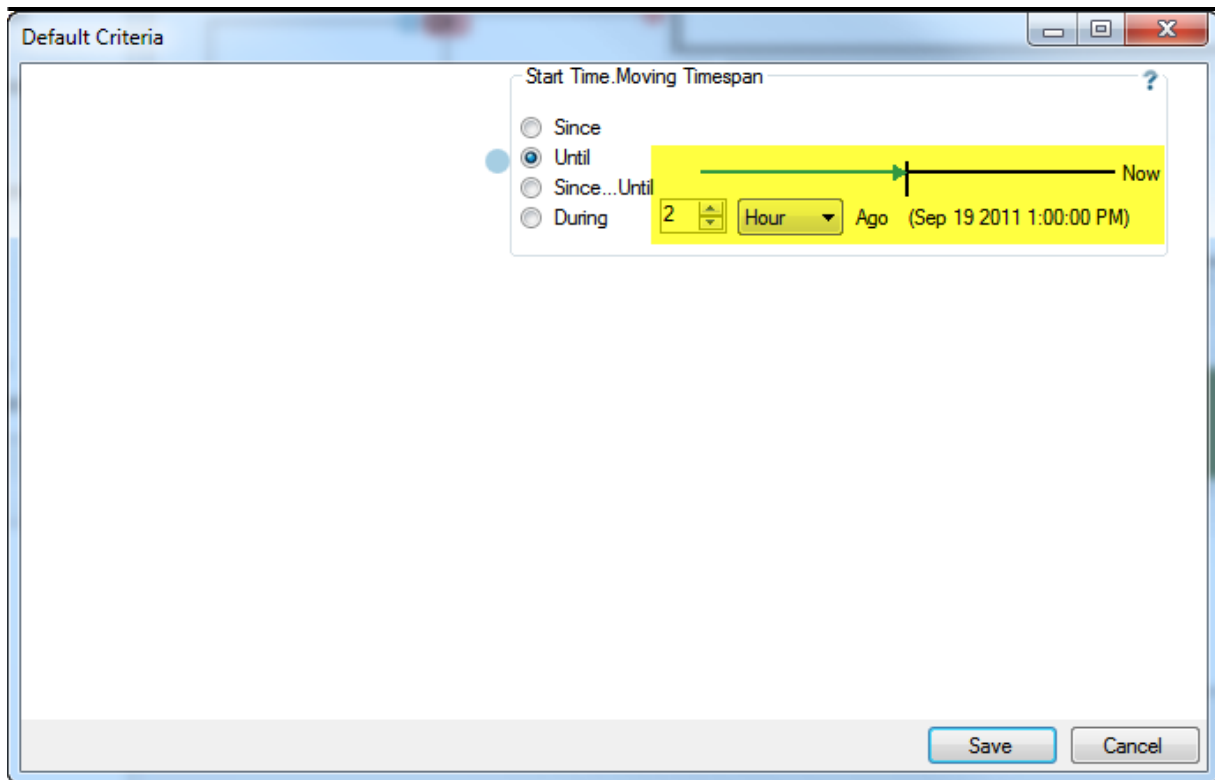
The Default Criteria can be modified through the Default Criteria form which is accessed by clicking the Set Default Criteria button:



Multiple fields for default criteria may be present and make use of the same And/Or expression building as the normal criteria section of the Visual Query Builder. In this example, only one field is used for default criteria:



This example uses a time based default criteria and has options to refine the time span. Select a time frame option and then set the actual time amount. The graph and time amount settings relate to the time span option selected:



The initial expression is set so that data up until two hours ago is fetched. This can easily be modified to fetch data since two hours ago, or a specific time frame using the Since . . . Until option. The analyst has control over what the default criteria should be so that the data fetched is relevant.

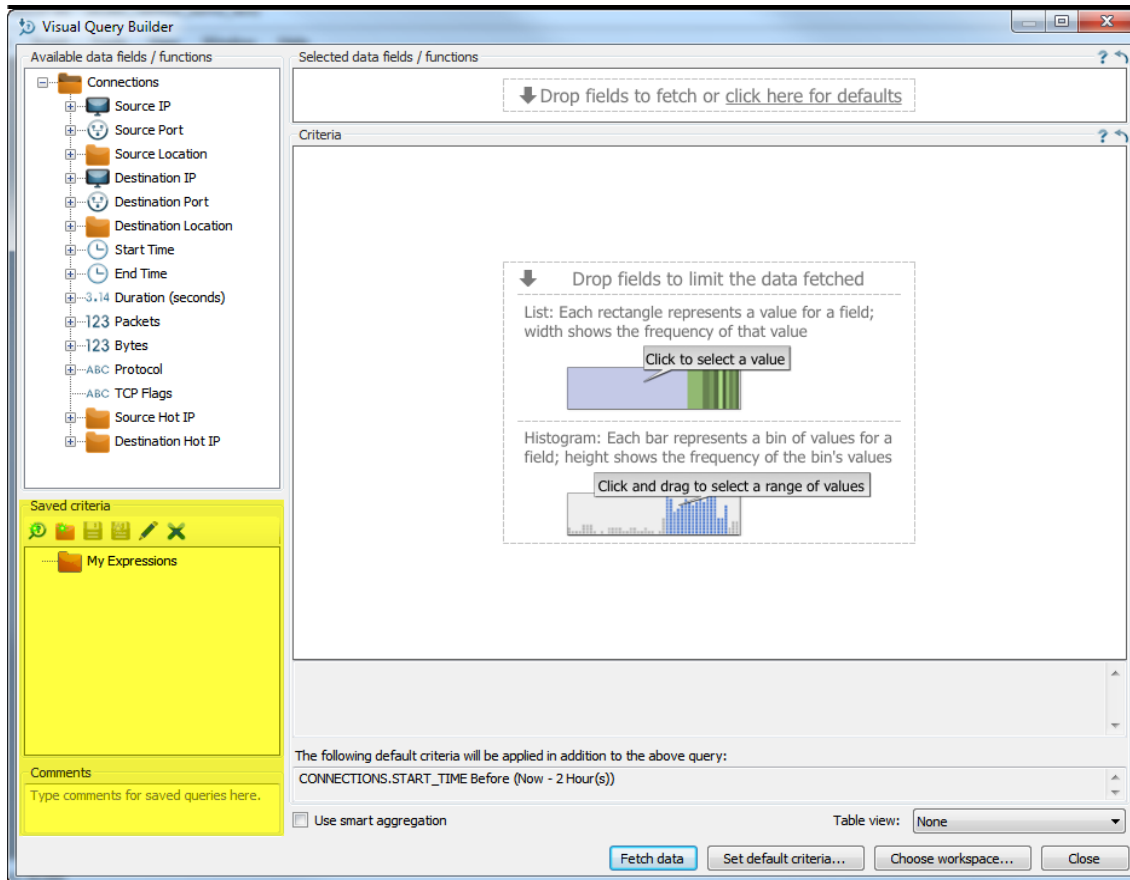
3.2.4 Additional Features

The Visual Query Builder offers to additional features: saving queries and using the Smart Aggregator. For more information about using the Smart Aggregator, [please see the "Using the Smart Aggregator" section](#).

3.2.4.1 Saving Query Criteria

Any query created with the Visual Query Builder can be saved for reuse and modification later. Comments can also be added to the query to give more information about what the query means. Saved queries and their comments are available to all analysts using VIAssist to facilitate collaboration efforts.

To save, view, or modify queries, use the Saved criteria section of the Visual Query Builder:



3.3 Using the Smart Aggregator

VIAssist's Smart Aggregator increases performance for visualizations by aggregating data. The aggregation of data is based on a Byte Cost per data row, an estimation of total number of bytes requested by a query. Two pieces of data factor into the Byte Cost:

- The cardinality - the unique count of values - of every field in the query, and
- The total number of rows the query would return.

The Byte Cost of a query is compared to a configurable maximum threshold value; if the Byte Cost is higher than the threshold, a series of steps is taken to aggregate high cardinality columns.

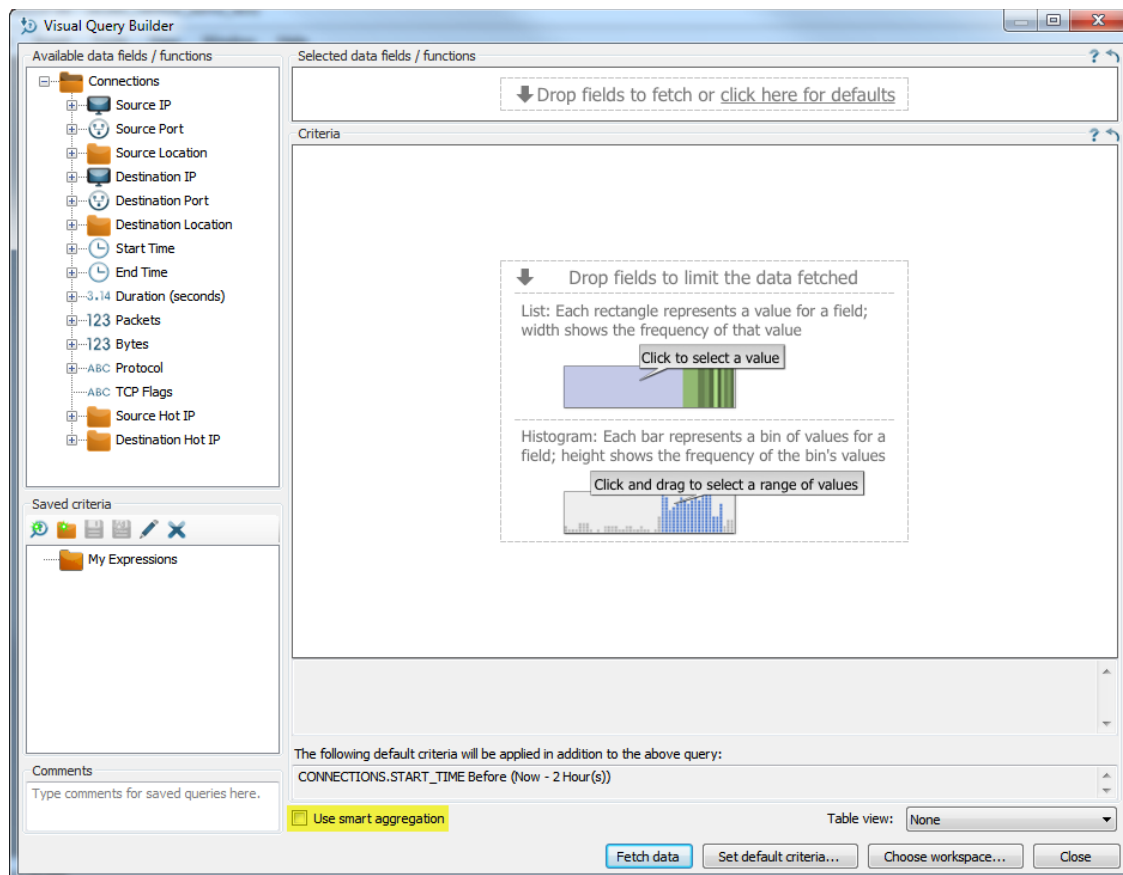
1. The cardinality ratio of a field is computed, and if the ratio is greater than the configurable maximum threshold, aggregation occurs. The cardinality ratio is computed by dividing the field's cardinality by the row count.
2. An improvement ratio is calculated to determine the level of aggregation needed. The improvement ratio is calculated by Byte Cost divided by the Maximum Threshold

configured, and then a level of aggregation is decided: LOW, MEDIUM, HIGH, or SINGLE_ROW. The level of aggregation determines the extent of the aggregation that will be performed on the field.

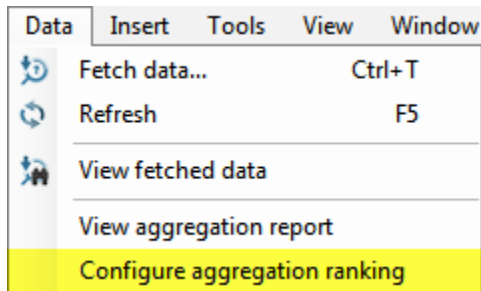
3. An estimated Byte Cost determined by the difference between the original Byte Cost and a new Byte Cost based on the aggregation. The estimated Byte Cost is compared to the configured maximum threshold to determine if more aggregation is needed. If more aggregation is needed, new fields are chosen from a user configurable list of fields and step two is repeated until an acceptable Byte Cost is found.
4. Steps one through three are repeated until a Byte Cost is found that falls below the configured maximum threshold.

3.3.1 Configuration

The Smart Aggregator can be enabled on the [Visual Query Builder](#) form by checking the Use Smart Aggregation checkbox. Field rankings must be present for aggregation to take place; an informational message box will open if no field rankings are present.



Field rankings can be configured by accessing the Aggregation Ranking form. To open the Aggregation Ranking form, open the Data menu and select the Configure aggregation ranking option.



The Aggregation Ranking window is used to rank database fields and calculations that can be applied to those fields. The top half of the form is used for ranking the database fields. The bottom half of the form is used for ranking field calculations.

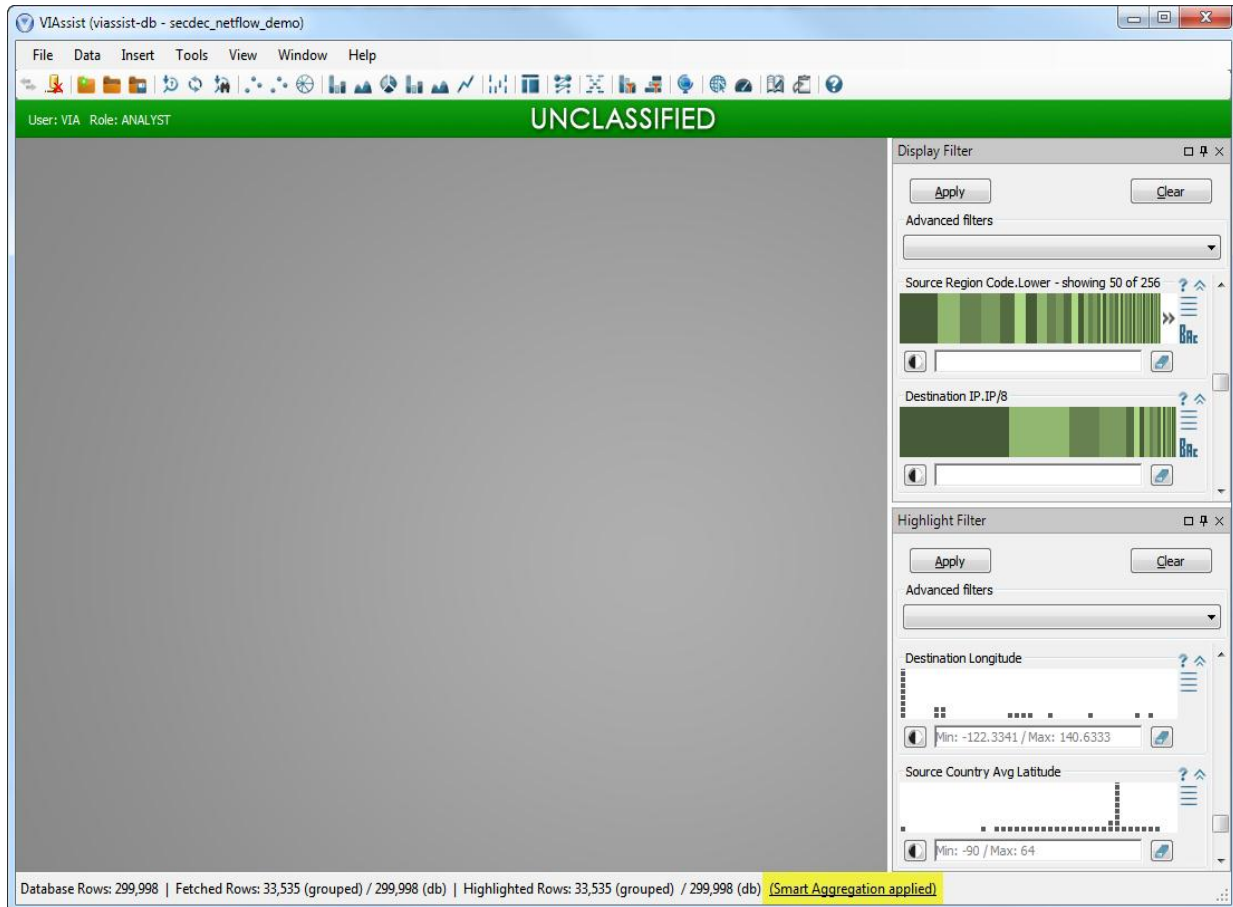
To rank fields, select a field in the list and use the up and down arrows to reorganize the fields based on how important they are.

Each field has calculations that can be applied to it. Calculations determine the extend of aggregation for a database field. For example, Source IP may be truncated to the first, second, or third octet. To rank calculations, select a database field in the top half of the form to display the calculations that can apply to the field. Then use the up and down arrows to reorganize the available calculations.

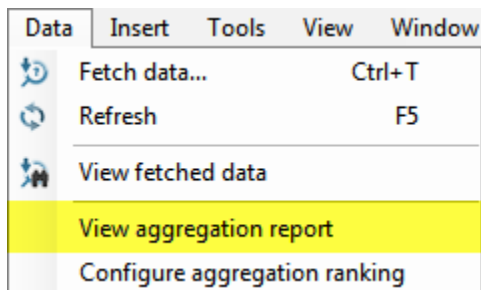
3.3.2 Aggregation Report

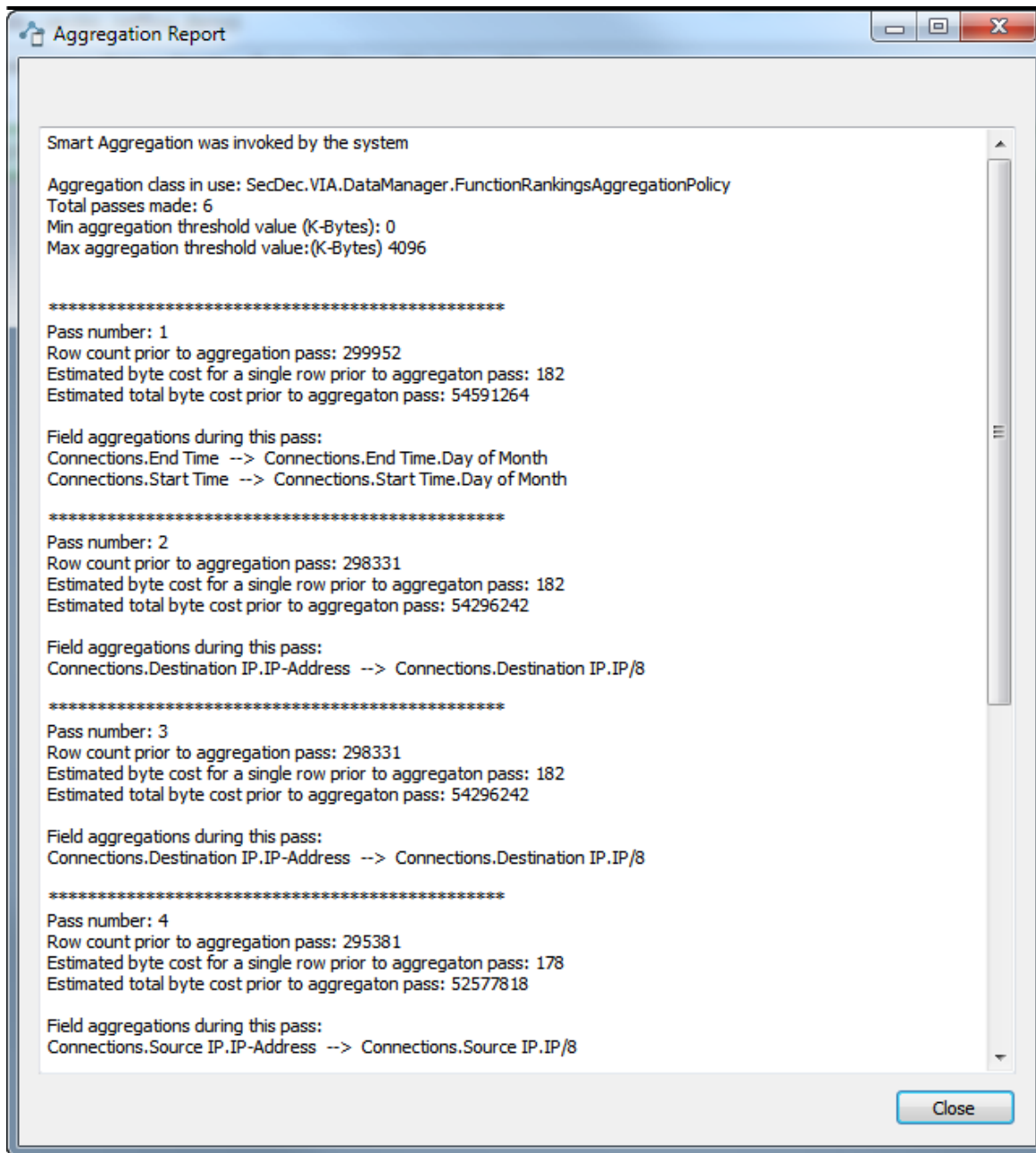
When the Smart Aggregator is used for fetching data, VIAssist will create a report summarizing relevant information about the aggregation process that was used by the Smart Aggregator.

There are two ways to view the aggregation report. When VIAssist is done aggregating data, a link to the Aggregation Report is placed in the status bar. Clicking this link will open the report:



The Aggregation Report can also be accessed from the Data menu and selecting the View aggregation report option:





The top portion of the Smart Aggregator Report tells which aggregation class was used, the total number of times the data was passed through the Smart Aggregator, and the minimum and maximum aggregation threshold values.

Smart Aggregation was invoked by the system

Aggregation class in use: SecDec.VIA.DataManager.FunctionRankingsAggregationPolicy
Total passes made: 6
Min aggregation threshold value (K-Bytes): 0
Max aggregation threshold value:(K-Bytes) 4096

The remained of the Smart Aggregator Report details information about each pass that was taken by the Smart Aggregator. Each section for each pass shows the row count prior to the aggregation, the estimated byte cost, the total byte cost, and the database field values that were aggregated.

```
*****
Pass number: 1
Row count prior to aggregation pass: 299952
Estimated byte cost for a single row prior to aggregaton pass: 182
Estimated total byte cost prior to aggregaton pass: 54591264

Field aggregations during this pass:
Connections.End Time --> Connections.End Time.Day of Month
Connections.Start Time --> Connections.Start Time.Day of Month

*****
Pass number: 2
Row count prior to aggregation pass: 298331
Estimated byte cost for a single row prior to aggregaton pass: 182
Estimated total byte cost prior to aggregaton pass: 54296242

Field aggregations during this pass:
Connections.Destination IP.IP-Address --> Connections.Destination IP.IP/8

*****
Pass number: 3
Row count prior to aggregation pass: 298331
Estimated byte cost for a single row prior to aggregaton pass: 182
Estimated total byte cost prior to aggregaton pass: 54296242

Field aggregations during this pass:
Connections.Destination IP.IP-Address --> Connections.Destination IP.IP/8

*****
Pass number: 4
Row count prior to aggregation pass: 295381
Estimated byte cost for a single row prior to aggregaton pass: 178
Estimated total byte cost prior to aggregaton pass: 52577818

Field aggregations during this pass:
Connections.Source IP.IP-Address --> Connections.Source IP.IP/8
```

3.4 Visualizing Data Sources

VIAssist is a robust visualization system that provides distinct visualization tools for analyzing massive datasets. Visualizations can present either summary or detail information; the choice of which visualization(s) to use can be tailored to each task. The combination of visualizations

chosen give multiple and coordinated views of the data, revealing patterns, trends, anomalies, and associations within the data that would otherwise be difficult or time consuming to expose.

Many visualization utilities are available in VIAssist; this variety gives an analyst flexibility to choose the most appropriate visualization(s) for their task. Visualizations can be easily configured, as described in the ["Configuring VIAssist Components"](#) section. Data elements have many interactions available for highlighting, filtering, calculations, and other manipulations, which are described in more detail in the ["Interacting with Visualizations"](#) section.

The sections that follow show how to get the most out of VIAssist visualizations by:

1. Utilizing summary and detail coordinated views;
2. Focusing on subsets of data;
3. Visualizing few, low cardinality data elements;
4. Relying on visualization cluster counts.

3.4.1 Using Multiple Monitors

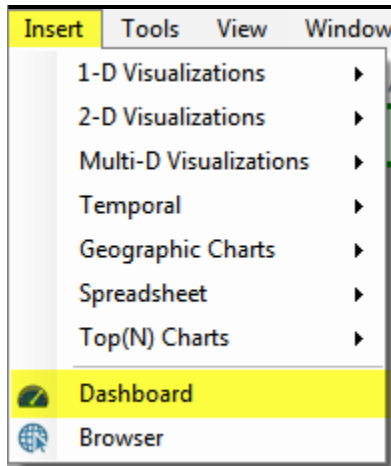
VIAssist has a flexible windowing and visualization system that lets an analyst maximize the use of their screen real estate. When multiple monitors are present a mix of summary visualizations (or views) and detailed information can be spread across the different monitors, keeping all relevant information ready at a glance. Similarly, both summary and detail visualizations can be docked directly in the VIAssist workspace when only a single monitor is present.

A multi-monitor approach to presenting information allows easy consumption of summarization data in conjunction with event-specific details. This approach of summary and details creates a simple process for detecting extreme data points or other outliers that may be associated with a critical asset while providing the capability to do much deeper analysis.

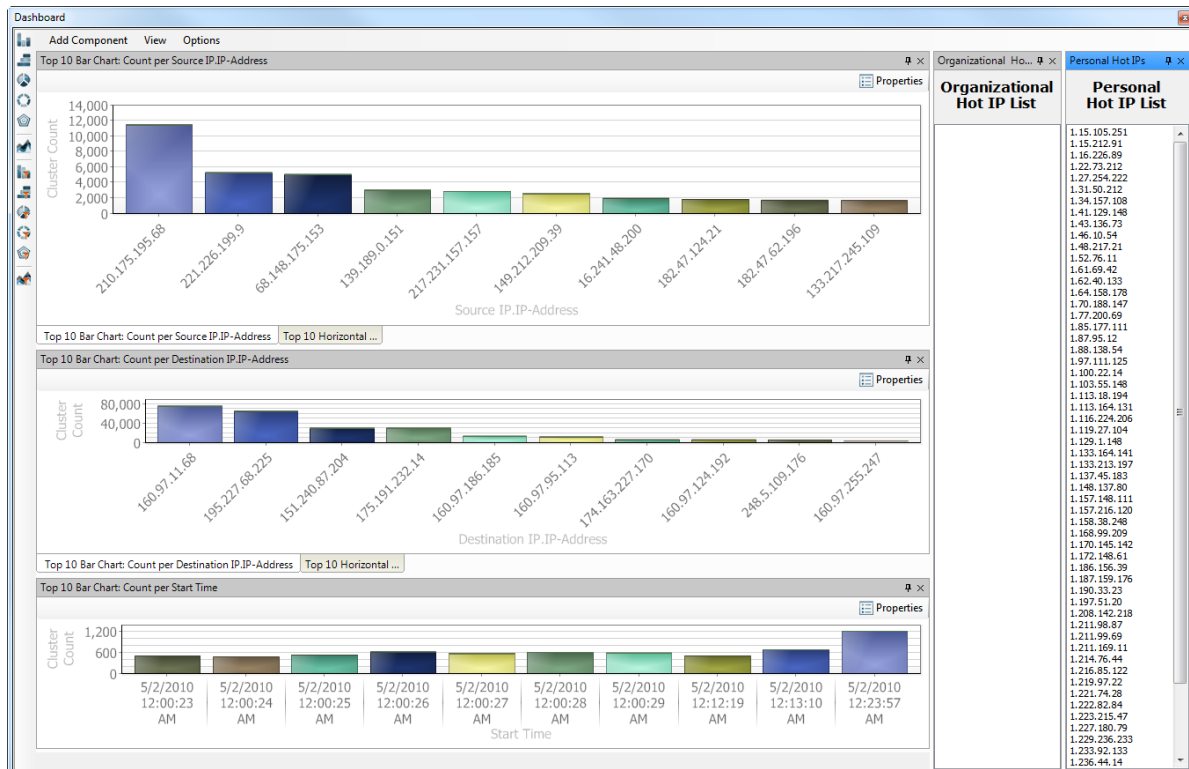
3.4.1.1 Example: Dashboard

A VIAssist Dashboard can quickly summarize connection data by using the Dashboard's Top 10 Lists functionality. When appropriate connection related data is available, the Dashboard will automatically display information related to the Top 10 matches that have the largest number of transaction or connection records in the data repository.

Insert a Dashboard into the VIAssist workspace by selecting the Dashboard option from the Insert menu.



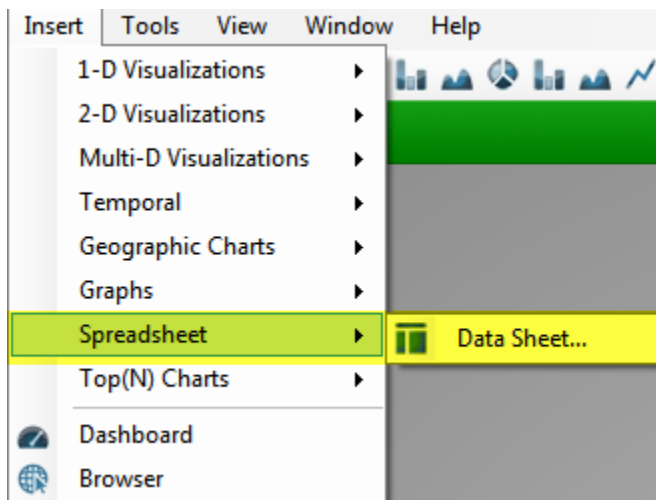
The default Dashboard will appear in its own floating window that can be positioned anywhere on any monitor or docked in the main application. A basic usage is to position the Dashboard on a free monitor so that the information displayed will remain visible while doing other analysis within the main VIAssist application. Once data has been [fetched](#), the Dashboard displays will update with relevant information.



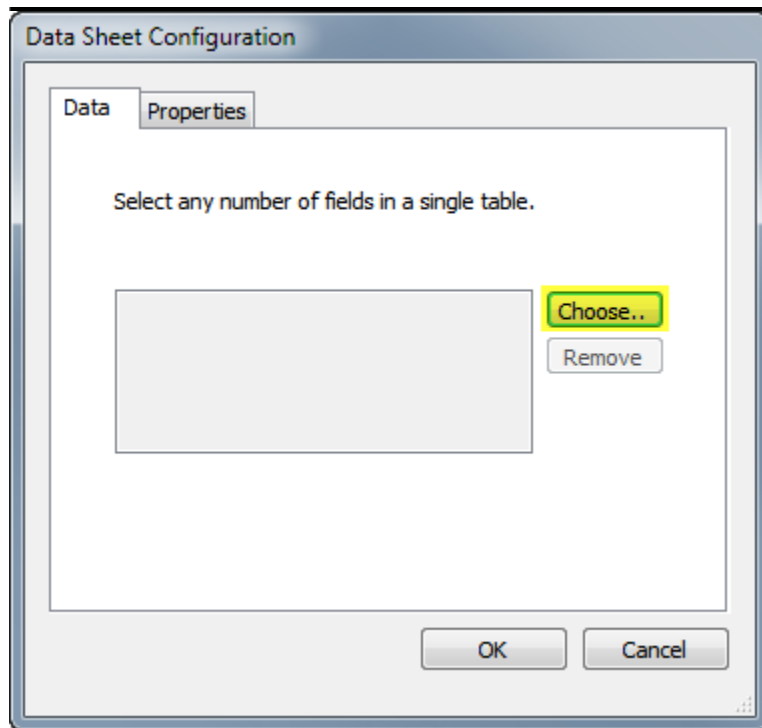
3.4.1.2 Example: Data Sheet

VIAssist has many visualization tools to choose from; each can operate in its own floating window or docked to the main application. In this example, a Data Sheet will be used to display detailed information in its own window for use on a separate monitor.

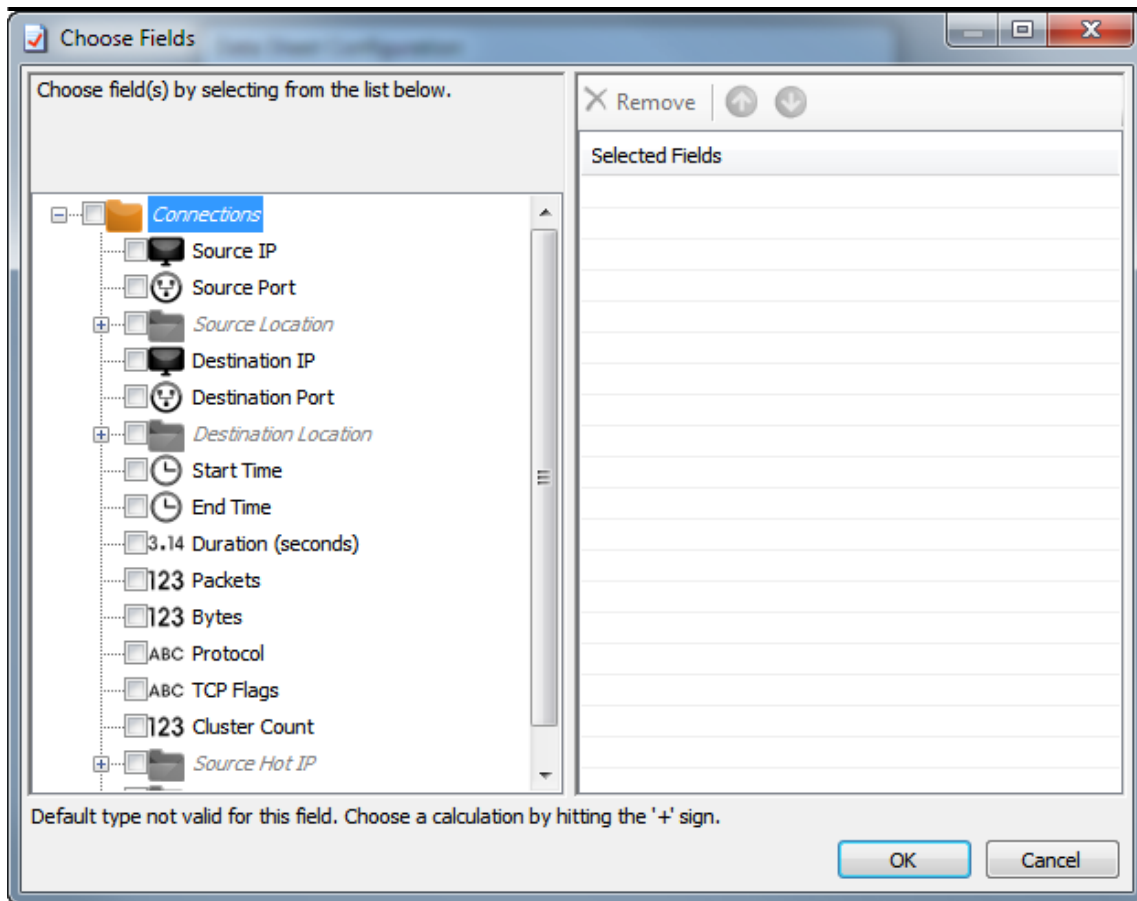
Insert a Data Sheet into the VIAssist workspace by selecting the Data Sheet option from the Spreadsheet sub-menu in the Insert menu.



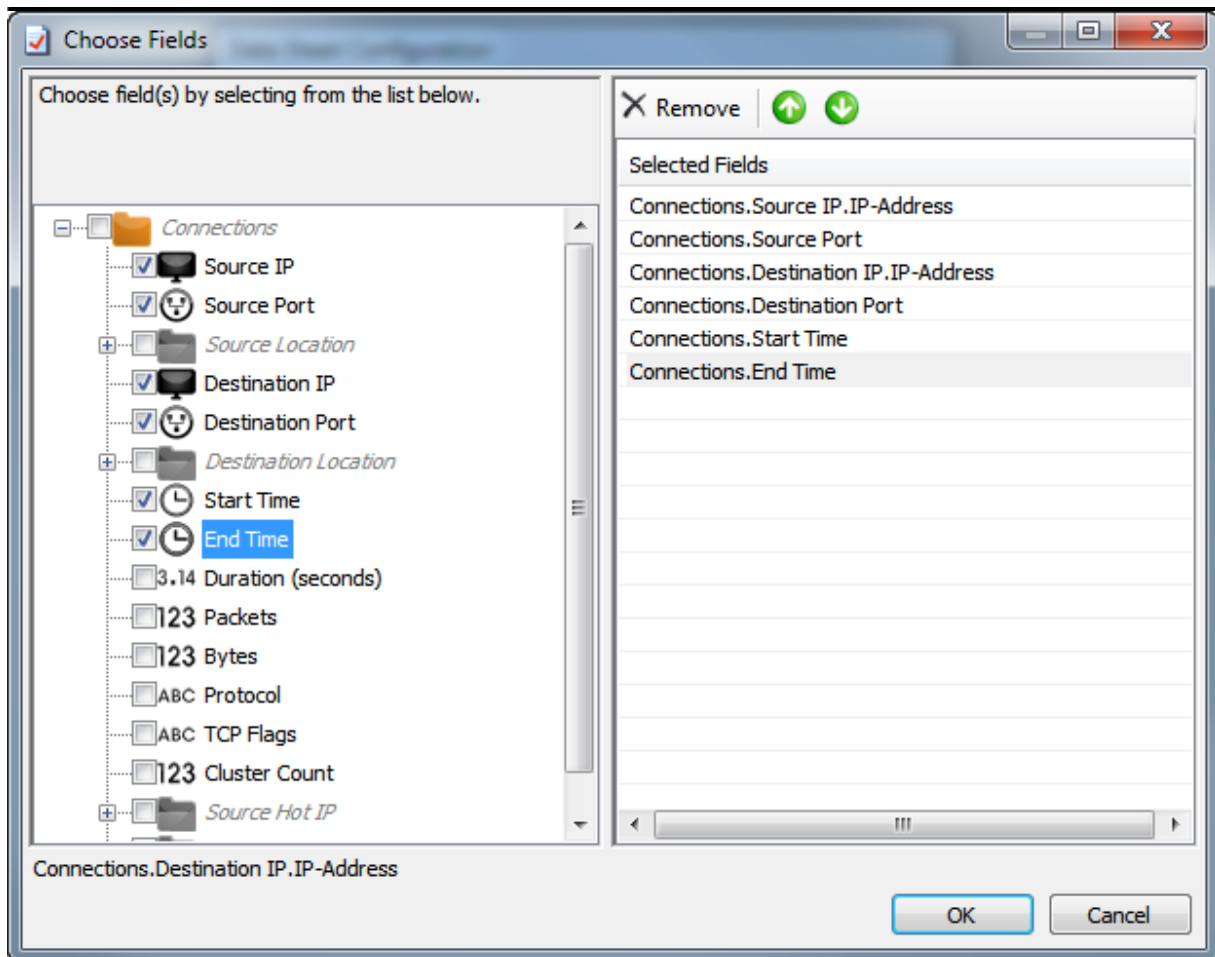
Selecting the Data Sheet will prompt for more information about what data should be displayed. Press the "Choose . . ." button to select which fields of information should be displayed.



This will open a form for choosing the fields that should be displayed in the Data Sheet.



This example will use the Source IP, Source Port, Destination IP, Destination Port, Start Time, and End Time fields as the data driving the Data Sheet. Selecting these fields will populate the "Choose Fields" form:



Accepting these configuration steps for the Data Sheet will open a new Data Sheet view. This view can be arranged like all other windows: it can be docked, it can be floating, or it can be placed on a separate monitor.

Source_IP-Address	Destination_IP-Address	Source_Port	Destination_Port	Start_Time	End_Time	Duration_(seconds)
1.100.22.14	160.97.11.68	53	5296	5/2/2010 12:15:48 AM	5/2/2010 12:15:48 AM	0
1.100.22.14	248.5.109.176	53	7426	5/2/2010 12:25:40 AM	5/2/2010 12:25:40 AM	0
1.100.22.14	248.5.109.176	53	58480	5/2/2010 12:07:36 AM	5/2/2010 12:07:36 AM	0
1.103.55.148	175.191.232.14	53	1388	5/2/2010 12:07:19 AM	5/2/2010 12:07:19 AM	0
1.103.55.148	175.191.232.14	53	21058	5/2/2010 12:07:19 AM	5/2/2010 12:07:19 AM	0
1.103.55.148	175.191.232.14	53	64483	5/2/2010 12:07:20 AM	5/2/2010 12:07:20 AM	0
1.113.164.131	175.191.232.14	53	4007	5/2/2010 12:07:19 AM	5/2/2010 12:07:19 AM	0
1.113.164.131	175.191.232.14	53	9745	5/2/2010 12:07:39 AM	5/2/2010 12:07:39 AM	0
1.113.164.131	175.191.232.14	53	12789	5/2/2010 12:07:19 AM	5/2/2010 12:07:19 AM	0
1.113.164.131	175.191.232.14	53	12910	5/2/2010 12:07:19 AM	5/2/2010 12:07:19 AM	0
1.113.18.194	160.97.11.68	53	27658	5/2/2010 12:10:24 AM	5/2/2010 12:10:24 AM	0
1.113.18.194	160.97.11.68	53	27960	5/2/2010 12:10:24 AM	5/2/2010 12:10:24 AM	0
1.113.18.194	160.97.11.68	53	30152	5/2/2010 12:10:24 AM	5/2/2010 12:10:24 AM	0
1.113.18.194	160.97.11.68	53	39271	5/2/2010 12:10:24 AM	5/2/2010 12:10:24 AM	0
1.116.224.206	160.97.11.68	53	15477	5/2/2010 12:09:49 AM	5/2/2010 12:09:49 AM	0
1.116.224.206	160.97.11.68	53	16316	5/2/2010 12:09:49 AM	5/2/2010 12:09:49 AM	0
1.116.224.206	160.97.11.68	53	19319	5/2/2010 12:09:49 AM	5/2/2010 12:09:49 AM	0
1.116.224.206	160.97.11.68	53	40063	5/2/2010 12:09:49 AM	5/2/2010 12:09:49 AM	0
1.116.224.206	160.97.11.68	53	44377	5/2/2010 12:09:49 AM	5/2/2010 12:09:49 AM	0
1.116.224.206	160.97.11.68	53	47028	5/2/2010 12:09:49 AM	5/2/2010 12:09:49 AM	0
1.119.27.104	160.97.11.68	53	3728	5/2/2010 12:11:03 AM	5/2/2010 12:11:03 AM	0
1.119.27.104	160.97.11.68	53	7676	5/2/2010 12:11:03 AM	5/2/2010 12:11:03 AM	0
1.119.27.104	160.97.11.68	53	17478	5/2/2010 12:11:03 AM	5/2/2010 12:11:03 AM	0
1.119.27.104	160.97.11.68	53	26464	5/2/2010 12:07:20 AM	5/2/2010 12:07:20 AM	0
1.119.27.104	160.97.11.68	53	41503	5/2/2010 12:11:03 AM	5/2/2010 12:11:03 AM	0
1.119.27.104	160.97.11.68	53	43525	5/2/2010 12:11:03 AM	5/2/2010 12:11:03 AM	0
1.119.27.104	160.97.11.68	53	45417	5/2/2010 12:11:03 AM	5/2/2010 12:11:03 AM	0
1.119.27.104	160.97.205.86	53	54294	5/2/2010 12:08:09 AM	5/2/2010 12:08:09 AM	0
1.119.27.104	175.191.232.14	53	6921	5/2/2010 12:00:36 AM	5/2/2010 12:00:36 AM	0
1.119.27.104	175.191.232.14	53	12155	5/2/2010 12:24:40 AM	5/2/2010 12:24:40 AM	0
1.119.27.104	175.191.232.14	53	41562	5/2/2010 12:24:40 AM	5/2/2010 12:24:40 AM	0

3.4.1.3 View Coordination

Using multiple monitors to display summary and detail information is a very powerful way to look at data. With the amount of data displayed across many views, it could be easy to become lost in the data. VIAssist implements many features to make interacting with all views and visualizations easier, which becomes even more important as more monitors are utilized. Please see the ["Interacting with Visualization"](#) section for more information on how VIAssist makes using views easier, especially the ["Highlighting Data"](#) section which helps coordinate multi-view information.

3.4.2 How to Detect and Verify Anomalies

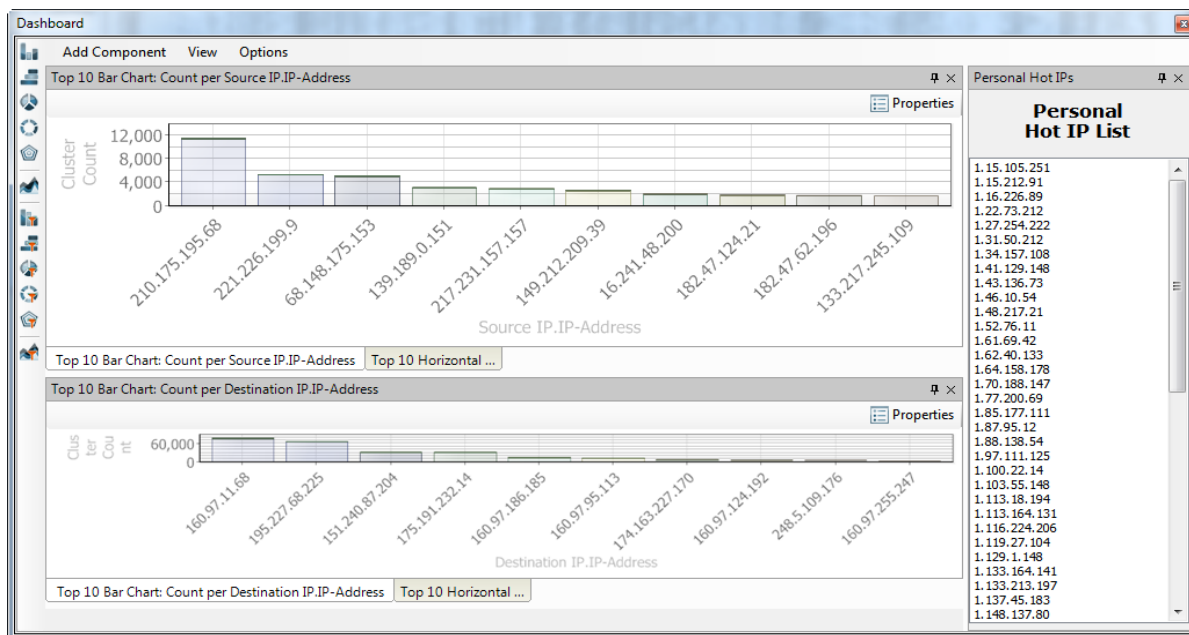
Anomalous data is usually difficult to identify because anomalies are outliers that deviate from regular patterns. This situation is exacerbated by having to pick the correct resolution of data for a visualization: displaying a large number of data elements may reduce the resolution of the visualization making it hard to find an anomaly, while displaying too few number of data elements may eliminate the anomalous data from inspection all together. A useful method to

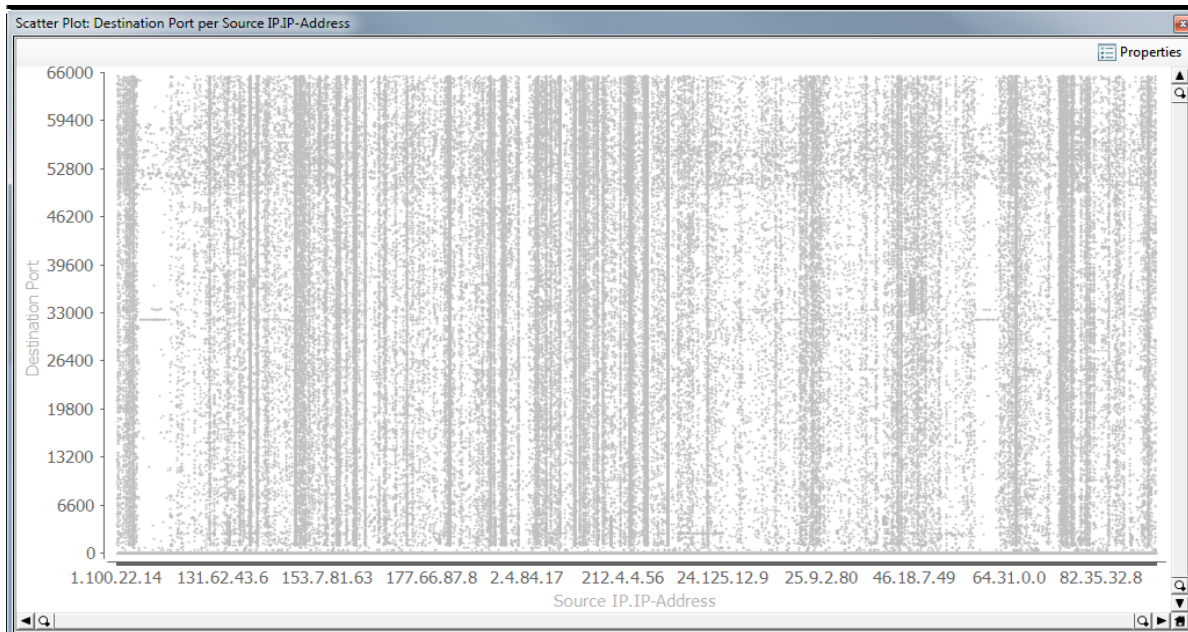
uncover anomalies is to use VIAssist to visualize a small number of low cardinality data elements.

This process is explained in the port scanning example below.

3.4.2.1 Example: Port Scanning

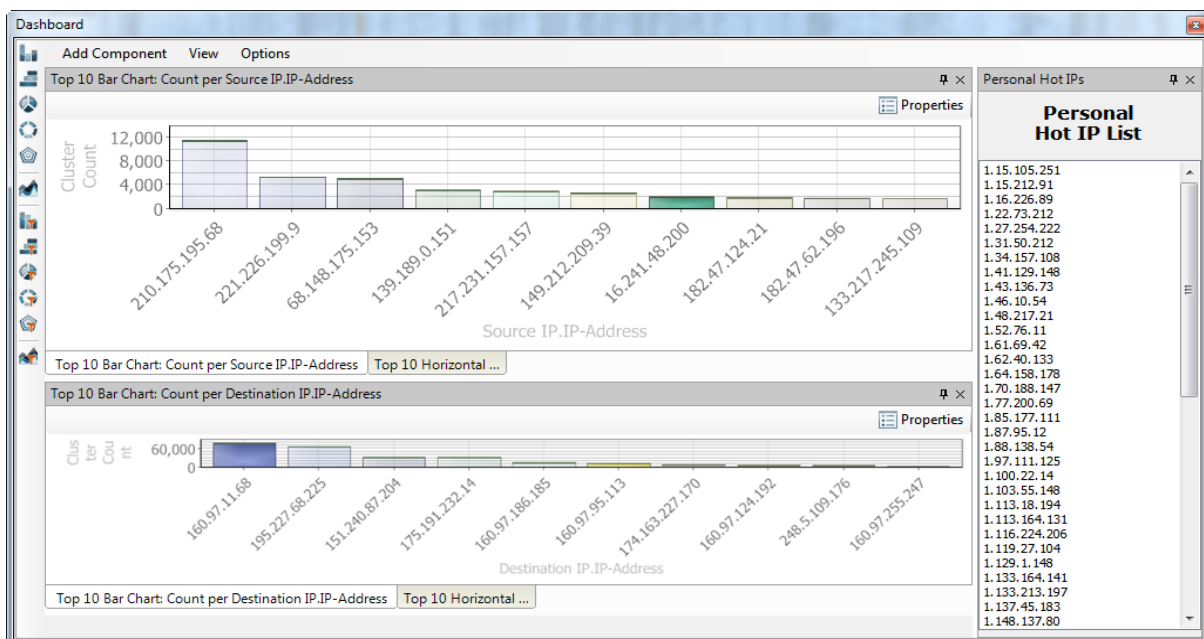
A Dashboard and a Scatter Plot are created using data that contains Source IPs and Destination Ports. The Dashboard is automatically populated with Top 10 information; the Scatter Plot is configured to use the Source IP as its X-axis and Destination Port as its Y-axis.

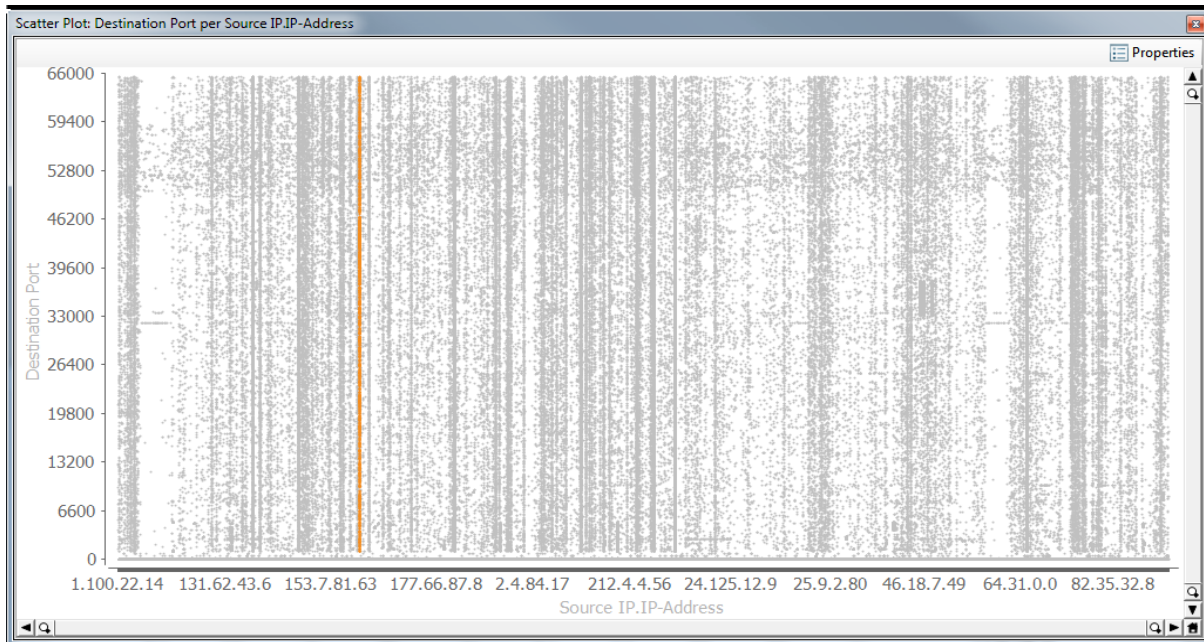




It quickly becomes evident that there is a lot of data to be consumed. The Scatter Plot has so much data that it may be difficult to notice potential anomalies. Vertical bands of points form in many places, which could indicate port scans. The Dashboard's display of the Top 10 Source IPs will serve as a useful starting point to gain more detailed information.

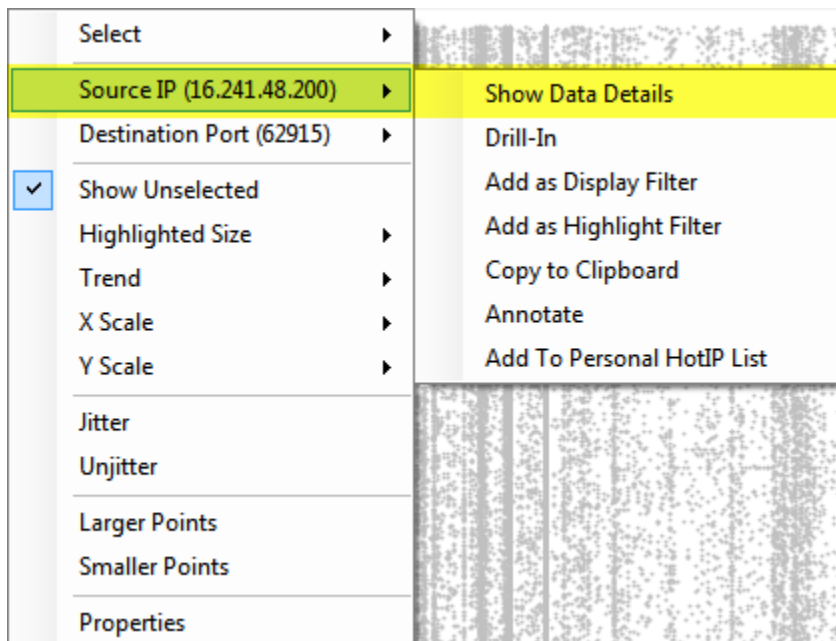
Selecting one of the Top 10 Source IPs highlights it in the Scatter Plot:



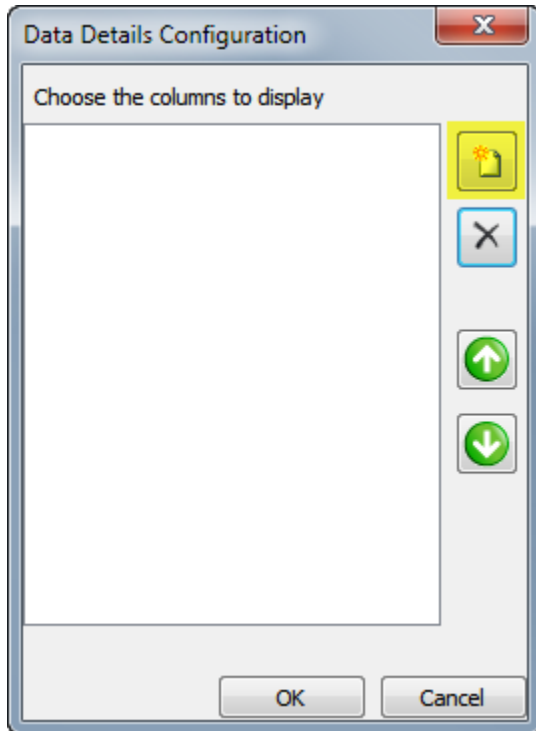


The vertical band highlighted in the Scatter Plot is a clear indication of a port scan, with almost every port available being touched. More information about this series of events is gathered by viewing the Data Details. Viewing the Data Details is available from both the Dashboard and the Scatter Plot. Right-clicking in either the Scatter Plot or on a bar in one of the Dashboard views will open a context menu.

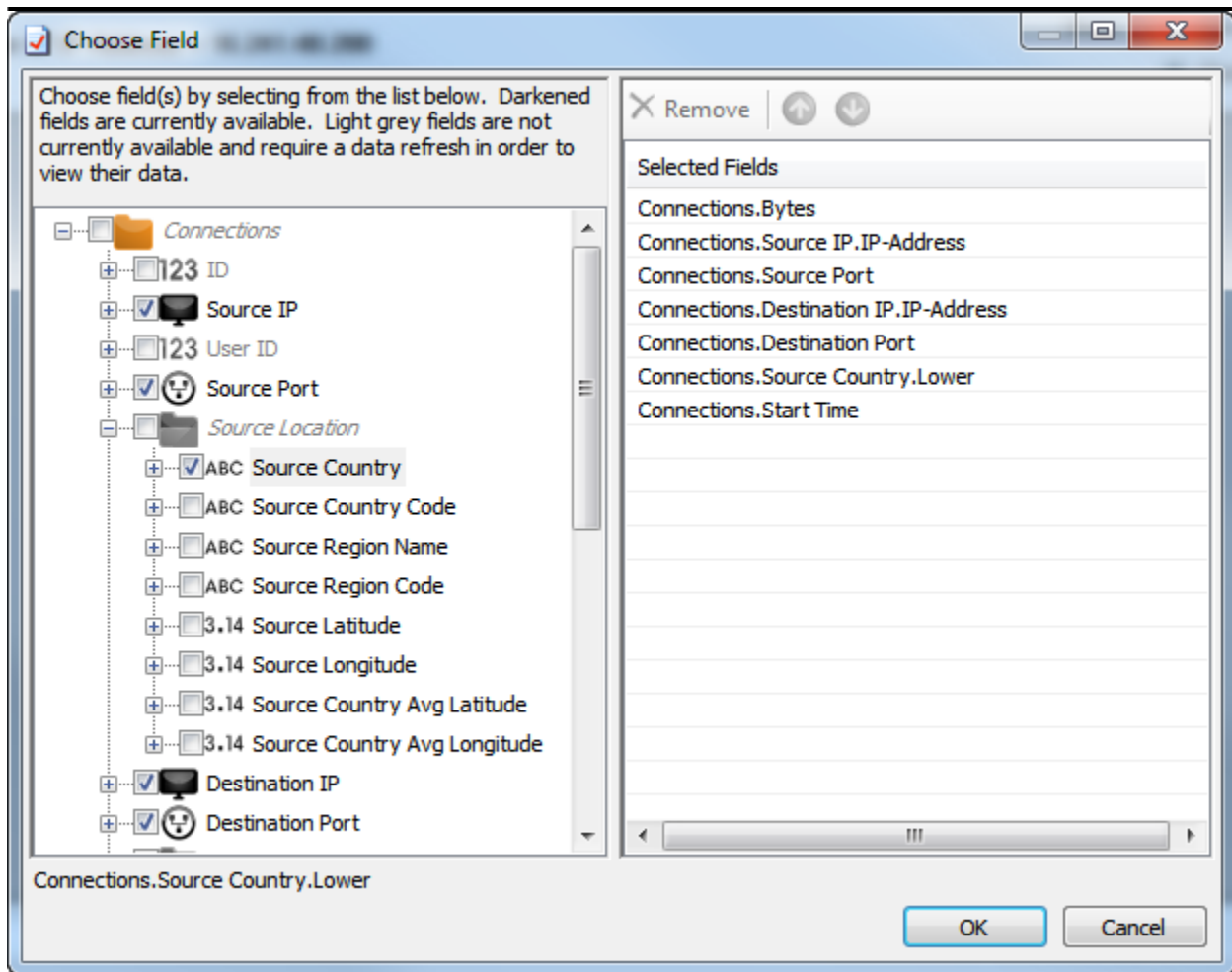
View the Data Details by selecting the "Show Data Details" option in the "Source IP" sub-menu.



The Data Details view can display any relevant data based on chosen fields. When the Data Details view opens, it first prompts for the fields of data that are to be displayed.



Selecting the "choose fields" button opens the Field Chooser form. For this example, the Bytes, Source IP, Source Port, Destination IP, Destination Port, Source Country, and Start Time fields are chosen for data:



Accepting this configuration will populate the Data Details view:

Data Details

Viewing details for: **Source IP.IP-Address = 16.241.48.200**

Show: ☐ Row ID ☒ Cluster Count [Configure](#)

	Bytes	Source IP.IP-Address	Source Port	Destination IP.IP-Address	Destination Port	Source Country.Lower	Start Time	Cluster Count
	129	16.241.48.200	53	160.97.95.113	40141	italy	5/2/2010 12:22:41 AM	1
	129	16.241.48.200	53	160.97.95.113	40159	italy	5/2/2010 12:22:43 AM	1
	129	16.241.48.200	53	160.97.95.113	40161	italy	5/2/2010 12:22:43 AM	1
	129	16.241.48.200	53	160.97.95.113	40213	italy	5/2/2010 12:22:46 AM	1
	129	16.241.48.200	53	160.97.95.113	40238	italy	5/2/2010 12:22:47 AM	1
	129	16.241.48.200	53	160.97.95.113	40248	italy	5/2/2010 12:22:48 AM	1
	129	16.241.48.200	53	160.97.95.113	40632	italy	5/2/2010 12:23:05 AM	1
	129	16.241.48.200	53	160.97.95.113	41005	italy	5/2/2010 12:23:19 AM	1
	129	16.241.48.200	53	160.97.95.113	41128	italy	5/2/2010 12:23:26 AM	1
	129	16.241.48.200	53	160.97.95.113	41134	italy	5/2/2010 12:23:26 AM	1
	129	16.241.48.200	53	160.97.95.113	41136	italy	5/2/2010 12:23:26 AM	1
	129	16.241.48.200	53	160.97.95.113	41144	italy	5/2/2010 12:23:27 AM	1
	129	16.241.48.200	53	160.97.95.113	41156	italy	5/2/2010 12:23:28 AM	1
	129	16.241.48.200	53	160.97.95.113	41198	italy	5/2/2010 12:23:30 AM	1
	129	16.241.48.200	53	160.97.95.113	41203	italy	5/2/2010 12:23:30 AM	1
	129	16.241.48.200	53	160.97.95.113	41215	italy	5/2/2010 12:23:31 AM	1
	129	16.241.48.200	53	160.97.95.113	41257	italy	5/2/2010 12:23:35 AM	1

Find: [Previous](#) [Next](#)

[Export to CSV](#) Rows: 1929

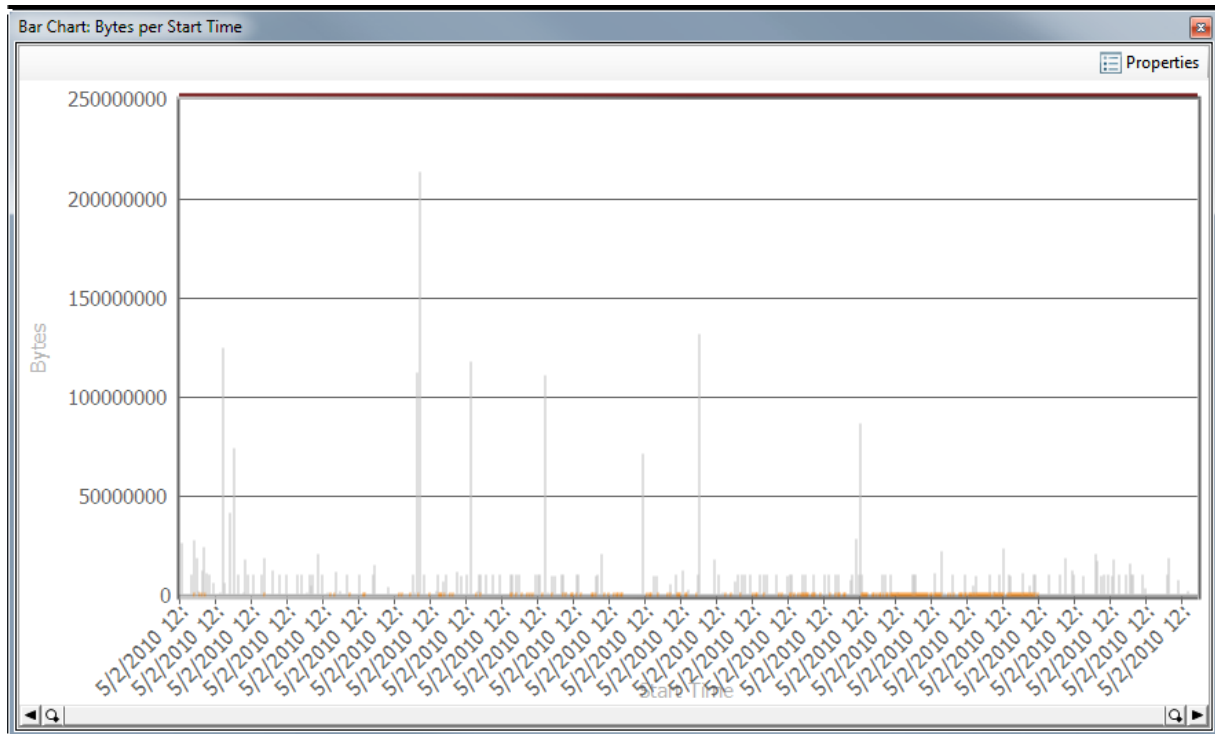
The Data Details view reveals that the port scans took place on 05/02/2010 between 12:00 a.m. and 12:30 a.m. The scan originated from Source Port 53, and maybe more interesting, the scan originated in Italy.

3.4.3 Viewing Temporal Data

VIAssist components can be easily configured to visualize temporal data. Time based data is both simple and powerful, providing information that can be used to detect or predict attacks to a network.

Many visualizations within VIAssist easily support temporal data. The Bar Chart is one of many that provide direct viewing within VIAssist.

The Port Scanning example in the ["How to Detect and Verify Anomalies"](#) section showed how to find information about a port scan using the Dashboard as a starting place. Another method of detecting unwanted network activity is to use simple temporal data. A Bar Chart that plots the X-Axis as Start Time and Y-Axis as Bytes reveals a very suspicious, excessive number of bytes:



A large spike occurs on 05/02/2010. This information corresponds to the port scan that occurred at the same time in the example scenario. The Bar Chart reveals several other large spikes, each potentially needing investigation.

3.5 Interacting with Visualizations

VIAssist visualization components support a number of interactions between each other and with the user. Control over visualizations is supported through context menus, filtering and highlighting, data fetching, and through direct selection of data points. The following sections detail how to:

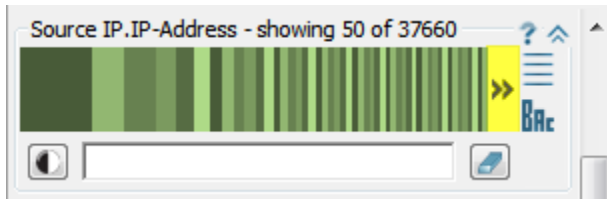
1. Filter data;
2. Highlight data;
3. How to use the collaboration tools;
4. What tools are available through context menus;
5. How to use the Data Sheet; and
6. How to arrange views.

3.5.1 Using Filter Widgets

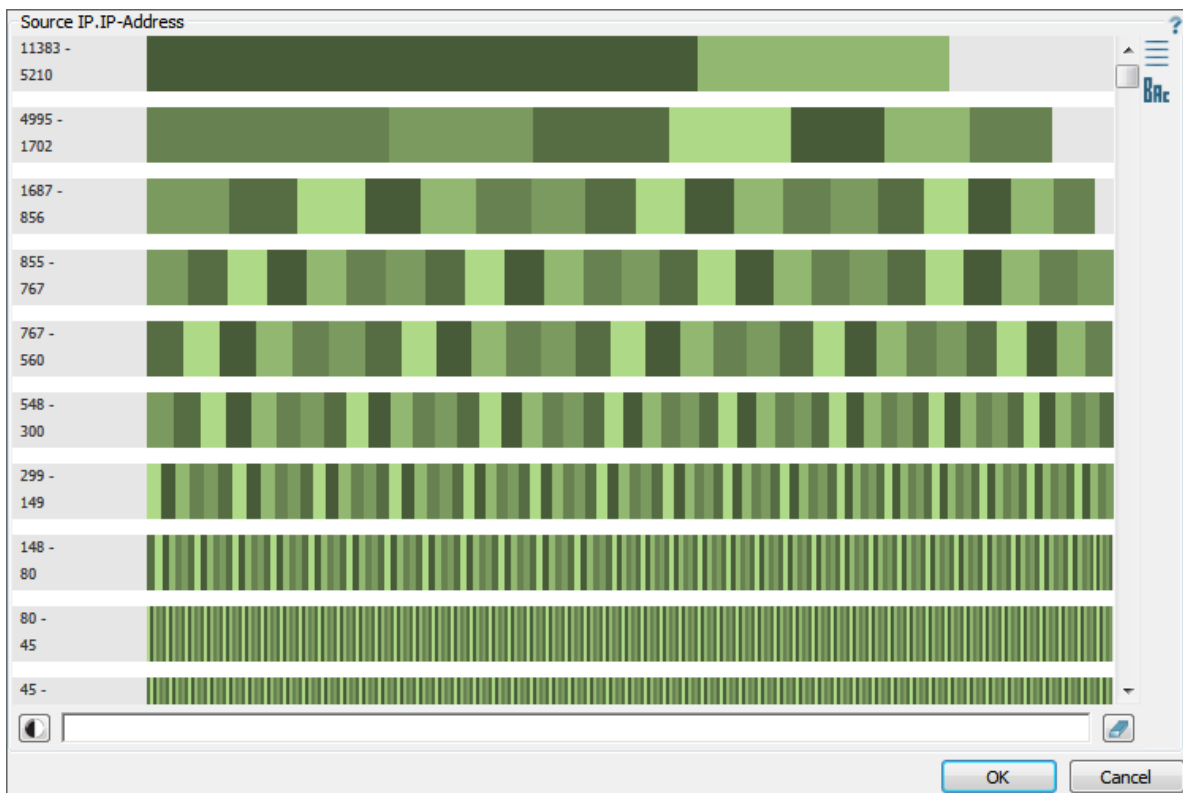
The operation of each type of filter is very similar, with only a couple of differences. The filter views are interactive, so mousing over items, clicking, ctrl+clicking, shift+clicking, ctrl+dragging,

and shift+dragging are all supported operations for selecting the filter criteria. The Linear Map filter supports deselection of individual items by ctrl+clicking an already selected item; the Histogram filter does not support this operation.

A Linear Map filter cannot always display all available data at once. If there is too much information to display in the normal Linear Map area, an arrow item will be available on the right hand side of the Linear Map:



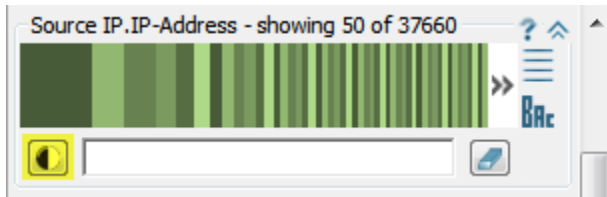
Clicking this item will open an expanded version of the Linear Map where all items are made available for selection:



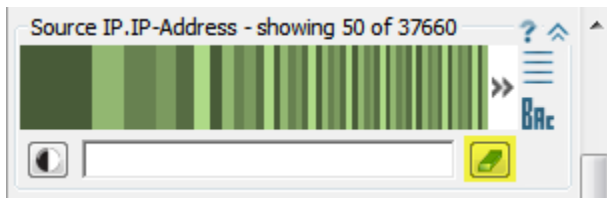
The Histogram filter does not have this functionality as a Histogram, by definition, can display all of its backing data.

All filter widgets contain a set of common functionality.

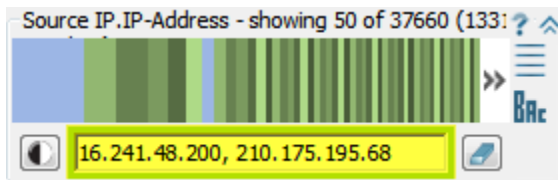
A filter's criteria can be inverted:



or cleared:

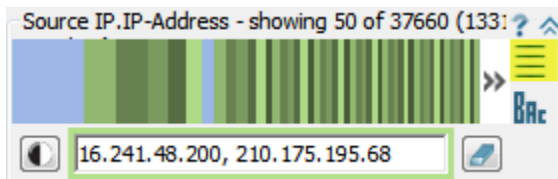


When a filter has active criteria, the textual version of that criteria can be seen below the visualization:

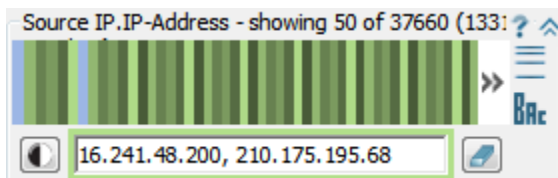


This textual criteria can be manually edited if the exact filter criteria is already known. This can sometimes save time if there are too many items to visually look through.

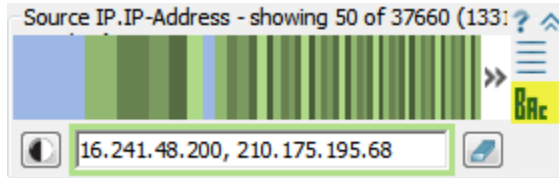
The scale used for the filter views can be toggled between a linear scale and a logarithmic scale.



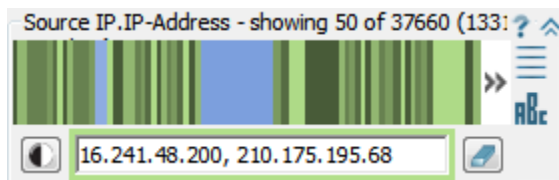
Toggling this option results in:



Similarly, the sorting of the items in the view can be toggled between frequency sorting and alphabetic sorting.

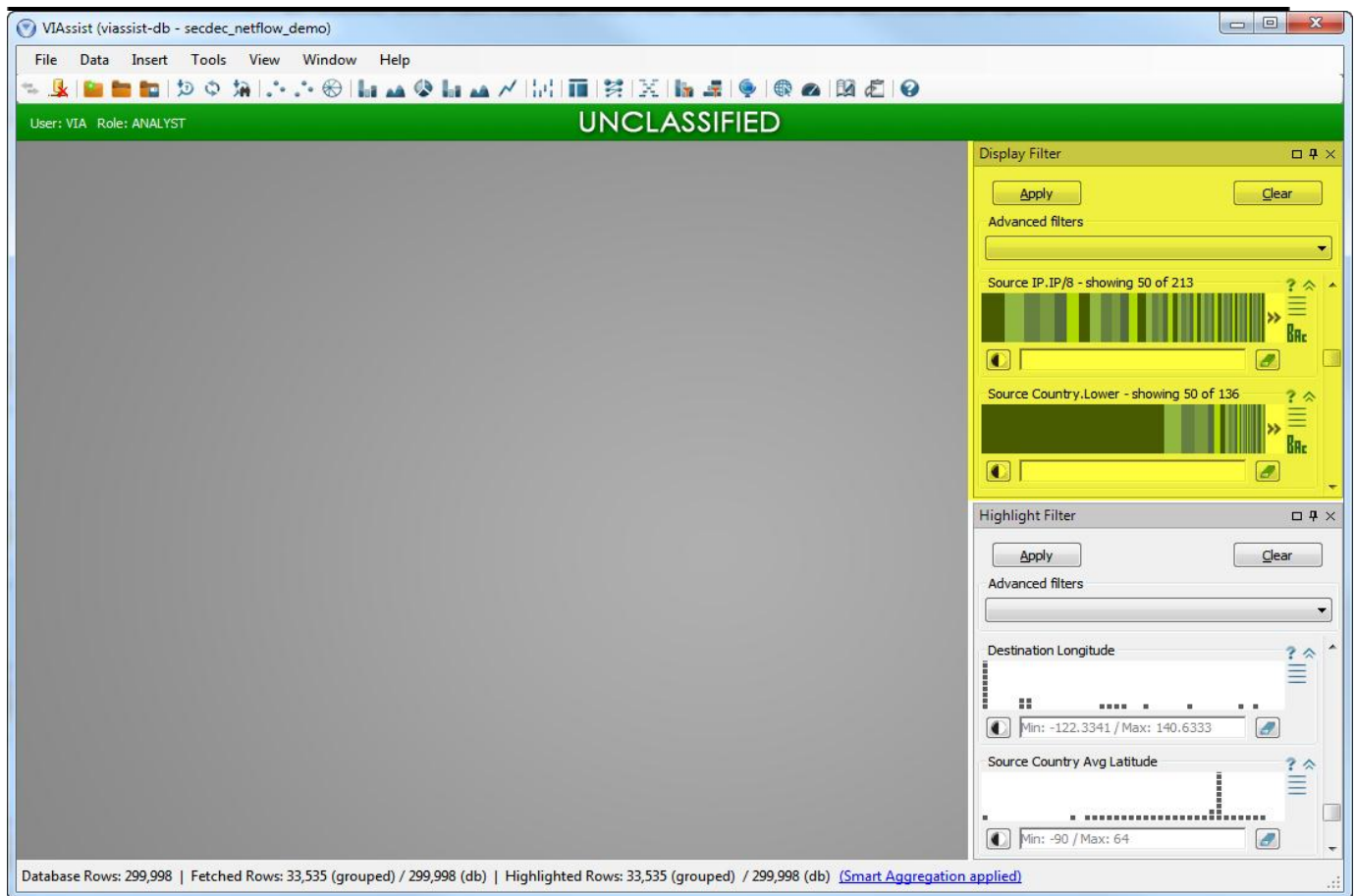


Toggling this option results in:



3.5.2 Filtering Data

It is often necessary to look at only a subset of data. VIAssist supports two methods of filtering data to a particular subset. The first way of filtering data is by using the ["Visual Query Builder"](#), which is detailed in its own section. The second way of filtering data is by using VIAssist's Display Filters. Display Filters will be available once a data source has been loaded. By default, a Display Filters panel will appear on the right side of the window:



The Display Filters panel contains a scrollable list of individual filters; each filter corresponds to a particular field that was selected when loading the data source. There are two types of Display Filters: the Linear Map and the Histogram. The type of filter that is chosen for a field depends on the type of that field. If the field is numeric data, a Histogram filter will be created; otherwise, a Linear Map filter will be chosen.

These filters are fully interactive. Individual elements within the view can be selected with typical mouse operations, including single select through mouse clicks and multi-select through mouse drags.

Filters are applied as a group after all filter criteria has been selected. As an example, a Parabox view is created that displays Source IP, Source Port, Destination IP, and Destination Port. The data is not yet filtered and creates a very cluttered view:

Parabox: Source IP,IP-Address, Source Port, Destination IP,IP-Address, Destination Port

Source_IP,IP-Address	Source_Port	Destination_IP,IP-Address	Destination_Port
1.100.22.14	65535	160.97.11.68	65535
111.255.84.27		191.236.118.167	
132.247.213.136		191.236.28.0	
144.165.133.114		135.221.146.202	
151.27.72.203		135.221.29.175	
161.231.210.195		139.202.142.209	
172.227.26.246		139.202.47.163	
184.14.228.227		144.5.153.24	
195.81.84.12		144.5.242.34	
20.234.166.134	38916	163.175.105.163	
206.234.118.124		163.175.186.12	
216.114.225.71		163.175.33.251	38982
226.186.77.87		173.135.113.32	
24.71.121.129		173.135.209.159	
246.213.119.250		173.135.75.87	
250.124.212.26		174.163.177.102	
26.94.149.28		174.163.54.179	
46.171.140.151		175.191.184.76	
56.65.193.228		175.191.83.41	
64.213.73.10		112.170.115.202	
75.132.30.203		163.175.57.103	
82.203.229.128	30895	242.4.25.176	13675

Filter criteria can be established to greatly reduce the visual clutter of this view. Setting a filter on the Source IP and Source Ports and then Applying those filters...

Display Filter

Apply Clear

Advanced filters

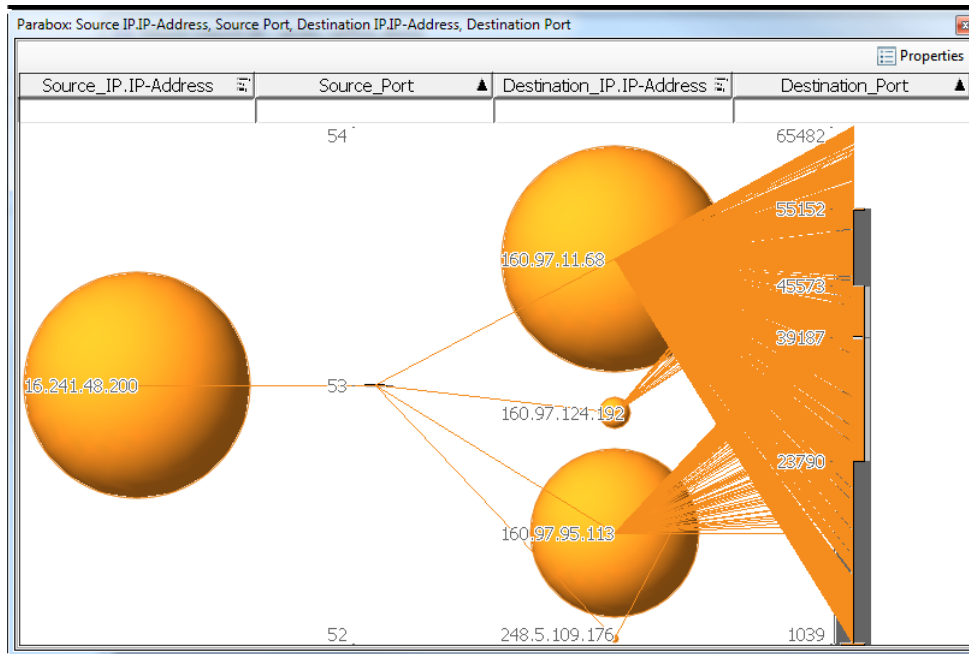
Source IP,IP-Address - showing 50 of 37660 (133)

16.241.48.200, 210.175.195.68

Source Port (130914 matches)

0-1599

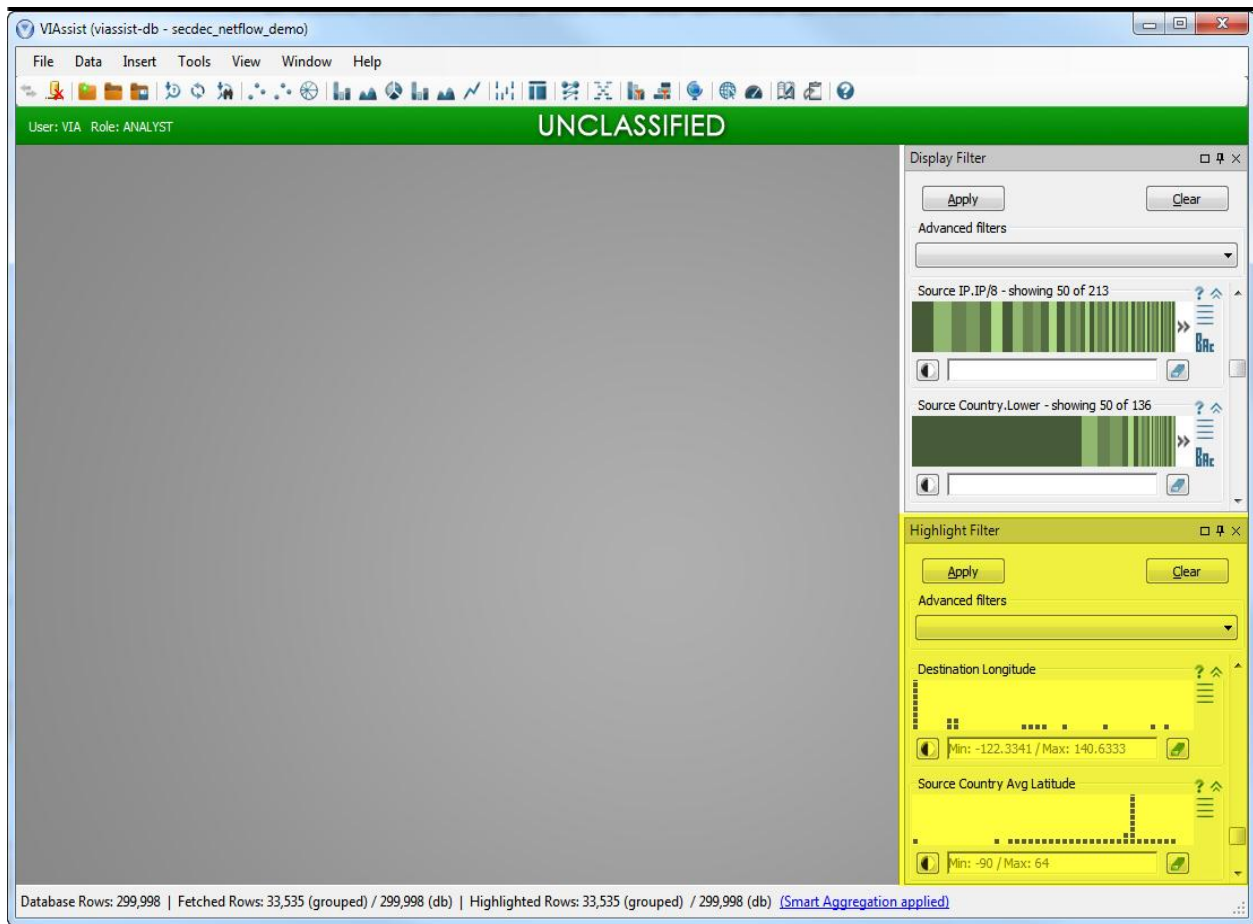
... results in a much more usable presentation of data:



3.5.3 Highlighting Data

Different views can give different insight into the data being analyzed, and sometimes it is necessary to find the same data elements across the different views. Doing this manually can be an arduous process, so VIAssist makes finding the same data elements in different views as easy as possible. VIAssist can highlight the same data element across all views.

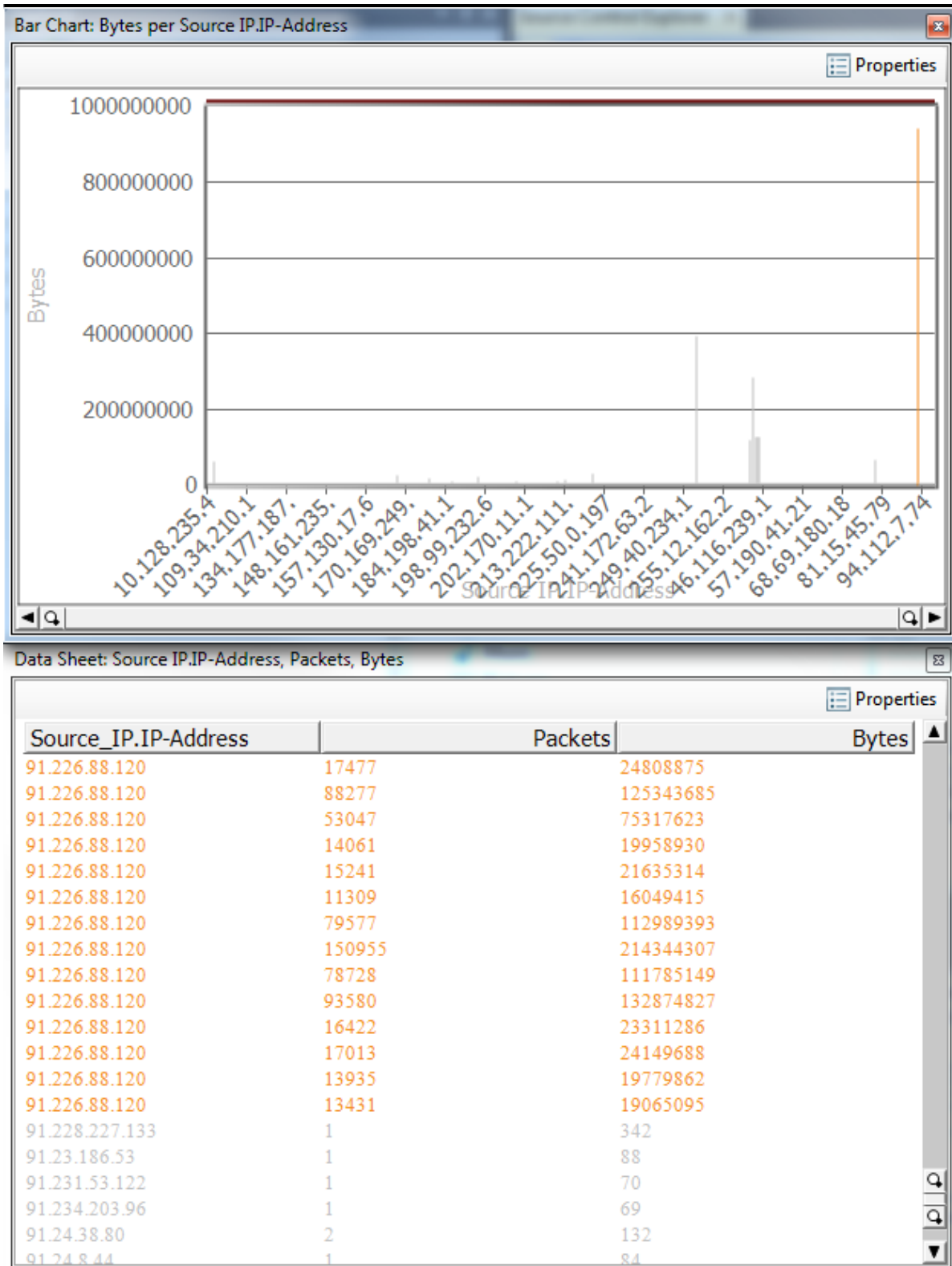
There are two main ways to highlight data in multiple views. The first is by specifying Highlight Filters in the Highlight Filter pane.



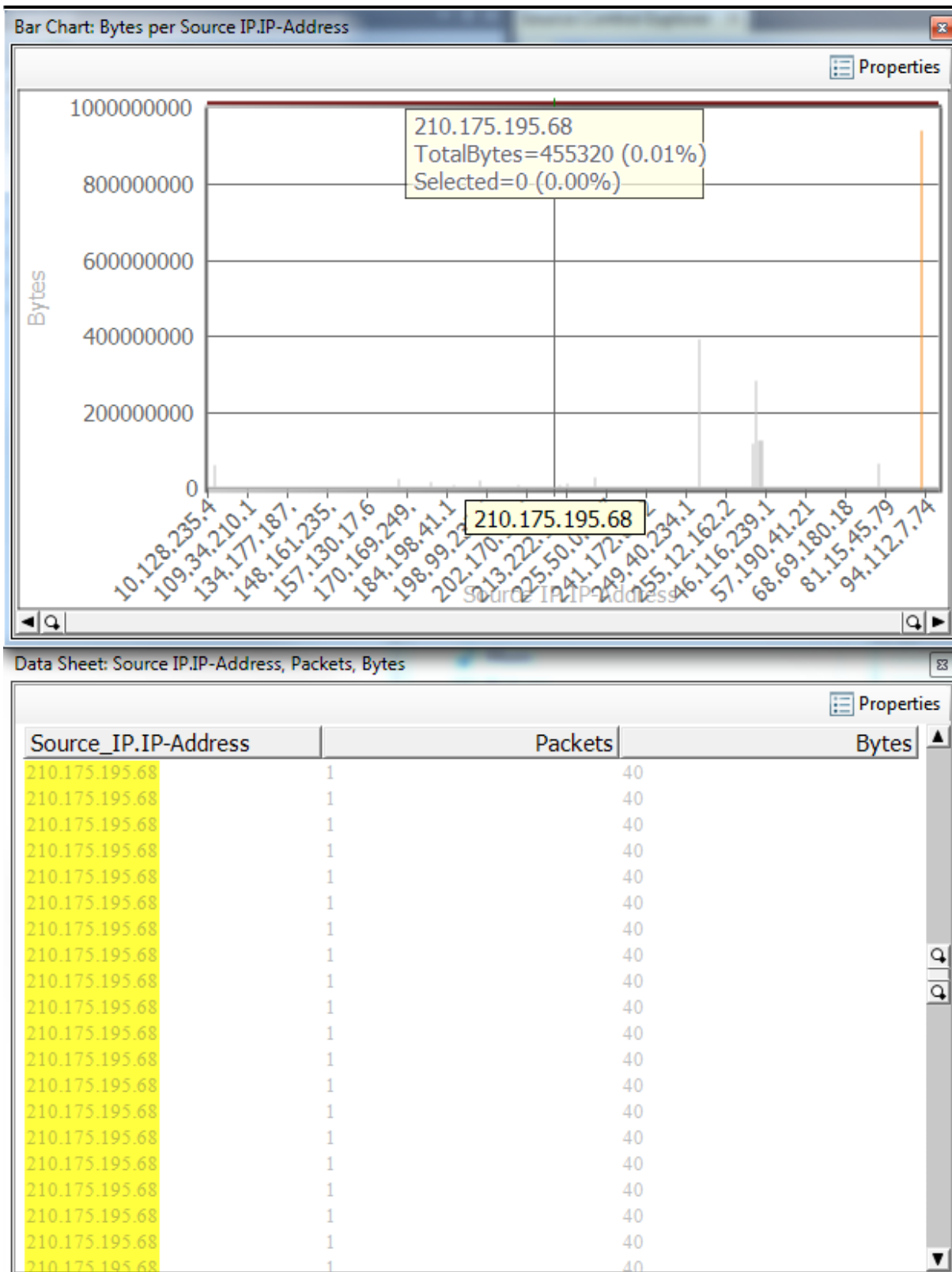
The use of the Highlight Filter pane to highlight data is virtually identical to the use of the Display Filter pane to filter data. The difference is that filtering data effects what data is displayed in visualizations. Highlighting data does not remove any data - it just makes it easier to spot interesting data within otherwise busy views. To learn more about using filter widgets, [please see the "Using Filter Widgets" section](#).

Another way of highlighting data across views is by interacting with data in any single view. To main highlight functionality are present when interacting with a view: selecting and hovering.

Selecting data elements in one view will also select, and highlight, them in all other views. In this example, the data element for Source IP 92.226.88.120 has been selected in the Bar Chart, colored orange. The Data Sheet subsequently updates with selections for the same Source IP, also colored orange.



Some views support displaying information when a data element is hovered over, such as displaying a tooltip. When an item is hovered over in one view, the hover displays for that same item in different views are triggered. Using the same example, hovering over a Source IP in the Data Sheet triggers the hover display in the Bar Chart:



3.5.4 Collaboration Tools

VIAssist supports the collaboration of multiple analysts through three primary means:

1. Personal and Organizational Hot IP Lists;
2. E-Diary journal entries; and
3. Annotations on specific field and data elements.

Each collaboration tool within VIAssist targets a specific use. Hot IPs are used to bring quick awareness to the data about known critical network resources or suspected attackers. Journal entries allow users to keep track of their analysis process and share with others when it is beneficial to do so. Annotations give analysts fine grained power of documenting fields and specific data that warranted attention.

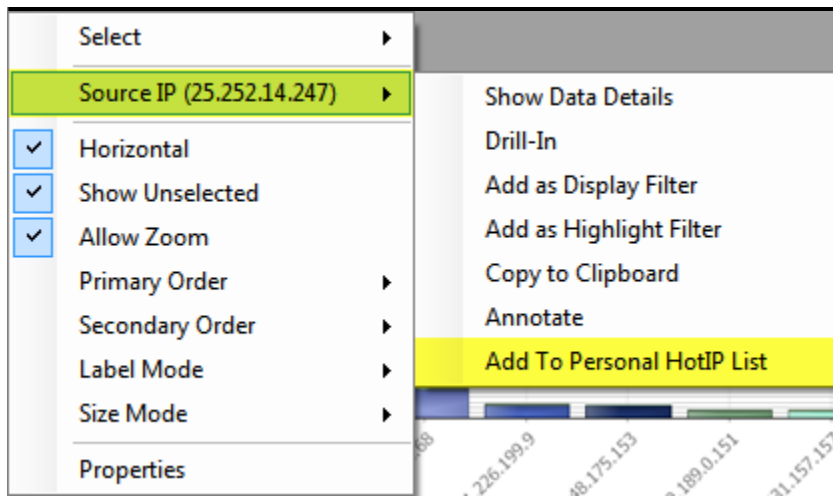
3.5.4.1 Hot IP Lists

Hot IPs provide a quick and convenient way to keep track of critical network assets or suspected attackers. Critical network asset IPs are placed into the Organizational Hot IP list. IPs discovered to belong to potential attackers are placed in an analyst's Personal Hot IP list. Hot IP lists are shared across all analysts. When one analyst adds a Personal Hot IP of a suspected attacker, all analysts will be able to see that Hot IP if it is present in the data. Likewise, an IP belonging to an Organizational Hot IP will be seen if the IP is present in the data.

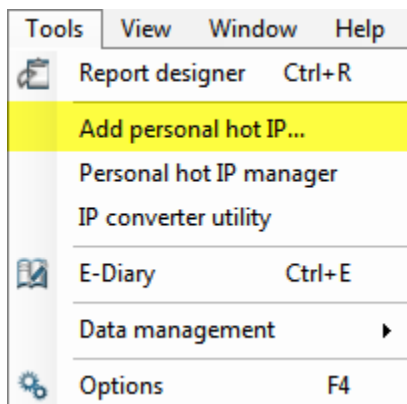
Organization Hot IPs are manually added to the database. Organizational Hot IPs are generally static.

Personal Hot IPs, on the other hand, are the result of analysis work and may change often. The Personal Hot IP list can be modified in several ways.

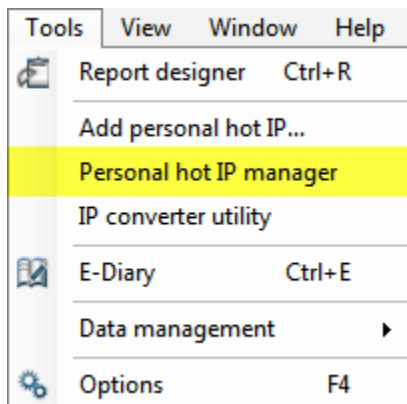
To add a new Hot IP from a visualization, right-click the visualization to open the context menu. Select the related field menu and select the Add To Personal HotIP List option.



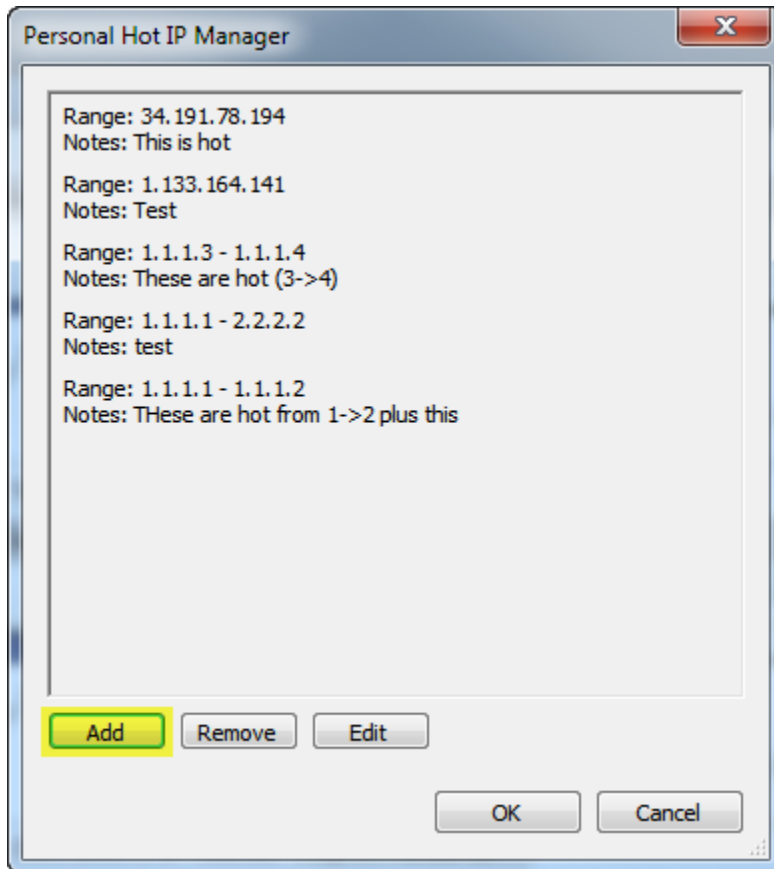
To add a new Hot IP at any time, open the Tools menu and select the Add Personal Hot IP option.



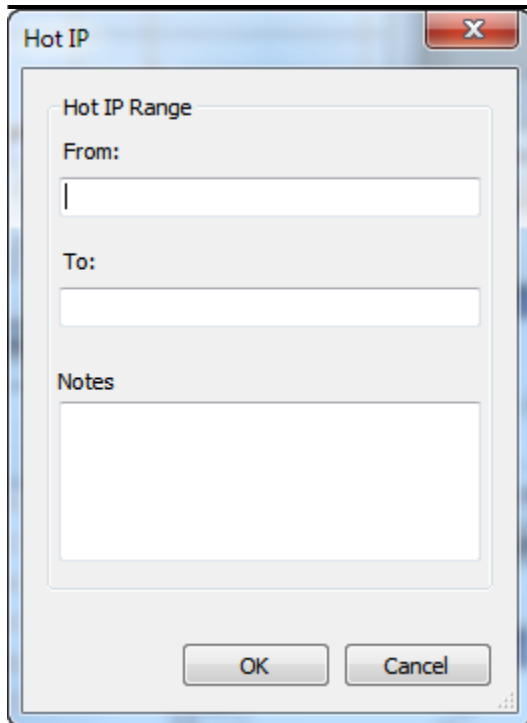
The Personal Hot IP Manager can also be used to add a Personal Hot IP. Access the Personal Hot IP Manager by opening the tools menu and selecting the Personal Hot IP Manager option.



The Personal Hot IP Manager will open and show all existing Personal Hot IPs and provide options for adding, removing, and modifying Hot IPs. Press the Add button to add a new Personal Hot IP:



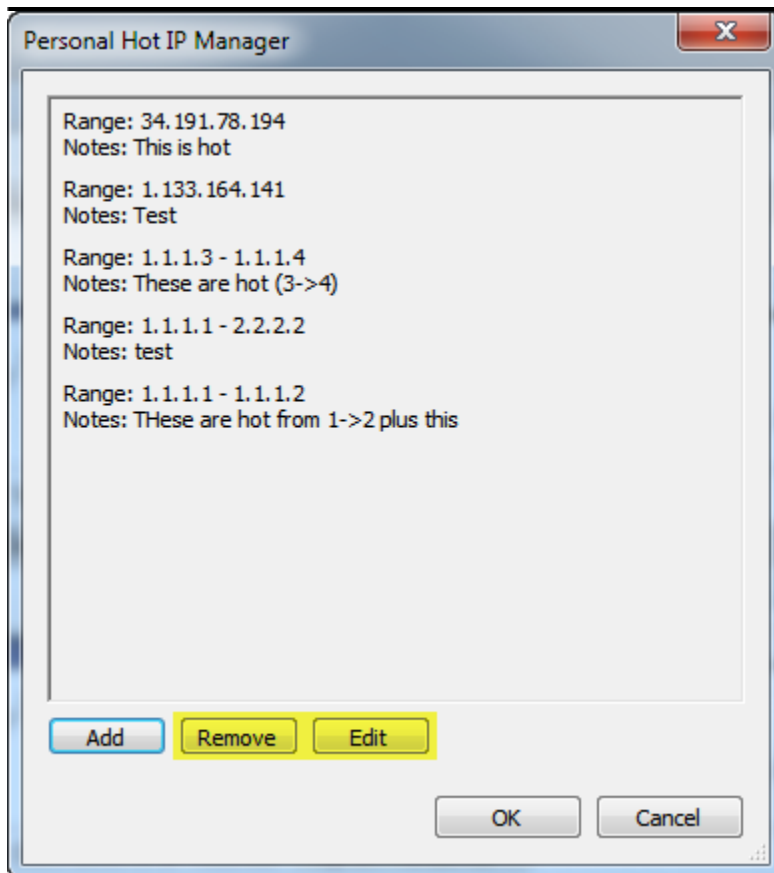
These three methods of adding a new Personal Hot IP will open the Hot IP form. The first method used within a visualization we automatically populate the from and to ranges for the Hot IP, although that range can still be modified if desired. The other two methods simply open a blank Hot IP form.

A screenshot of a Windows-style dialog box titled "Hot IP". The dialog box has a standard title bar with a close button (X). Inside, there is a section labeled "Hot IP Range" containing two text input fields: "From:" and "To:". Below these fields is a larger text area labeled "Notes". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

The Hot IP range starts at some IP and ends at some other IP. For example, 1.1.1.1 to 2.2.2.2 describes a valid IP range. Setting the from and to range to the same IP will simply make a Hot IP with a range of that single IP address.

Notes can optionally be added to describe why this IP is considered a Hot IP. This is useful when collaborating with other analysts who may not have been present at the time of discovery.

The Personal Hot IP Manager provides easy access to the Personal Hot IPs that a particular user has created. Adding a new Personal Hot IP using the Personal Hot IP Manager was already shown. Existing Personal Hot IPs can also be removed or modified using the Personal Hot IP Manager.

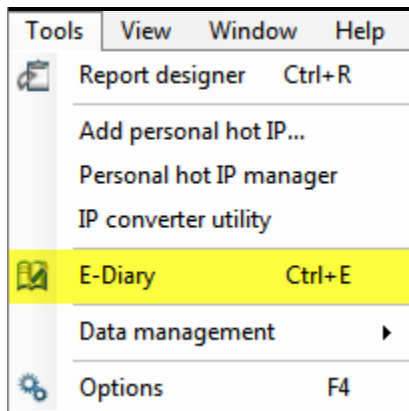


Care should be given to removing or editing existing Hot IPs in a collaborative environment. Others may have found them useful in their own analysis but have not yet added them to their own Personal Hot IPs yet.

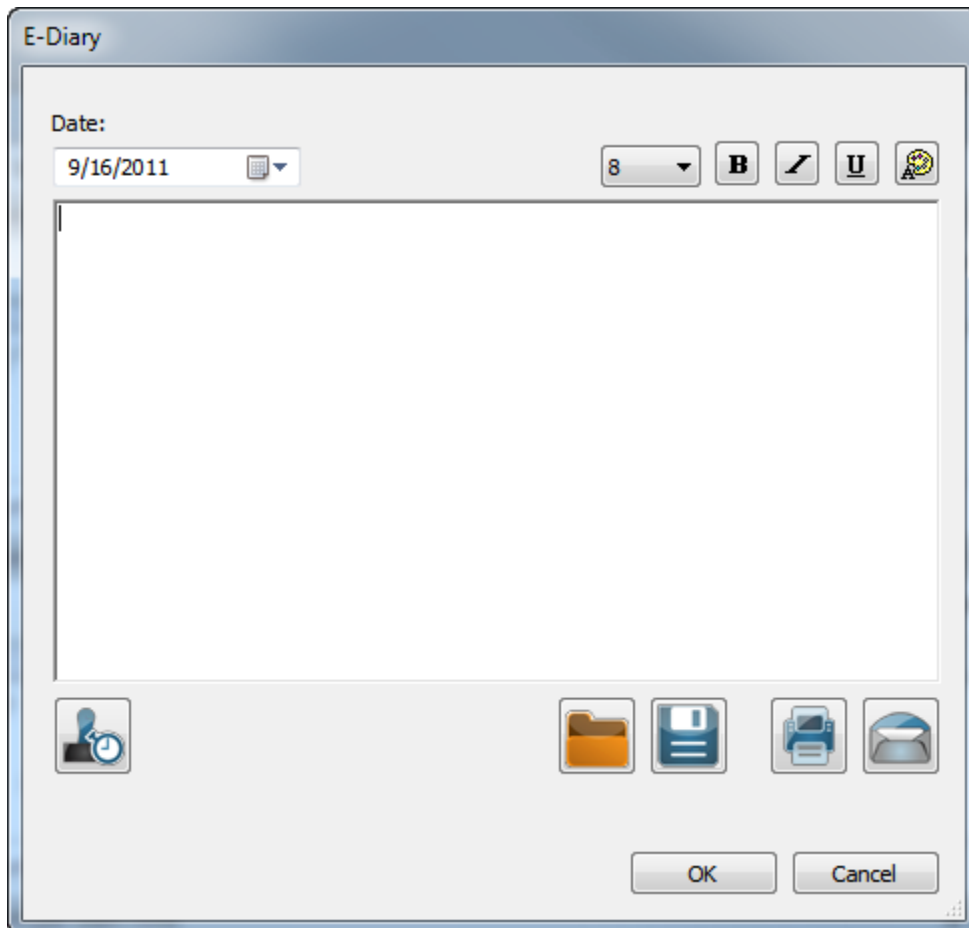
3.5.4.2 E-Diary

The E-Diary provides a quick and easy way for an analyst to store journal entries about analysis work. These journal entries are private and per user, although the E-Diary does provide options for sharing if the need arises.

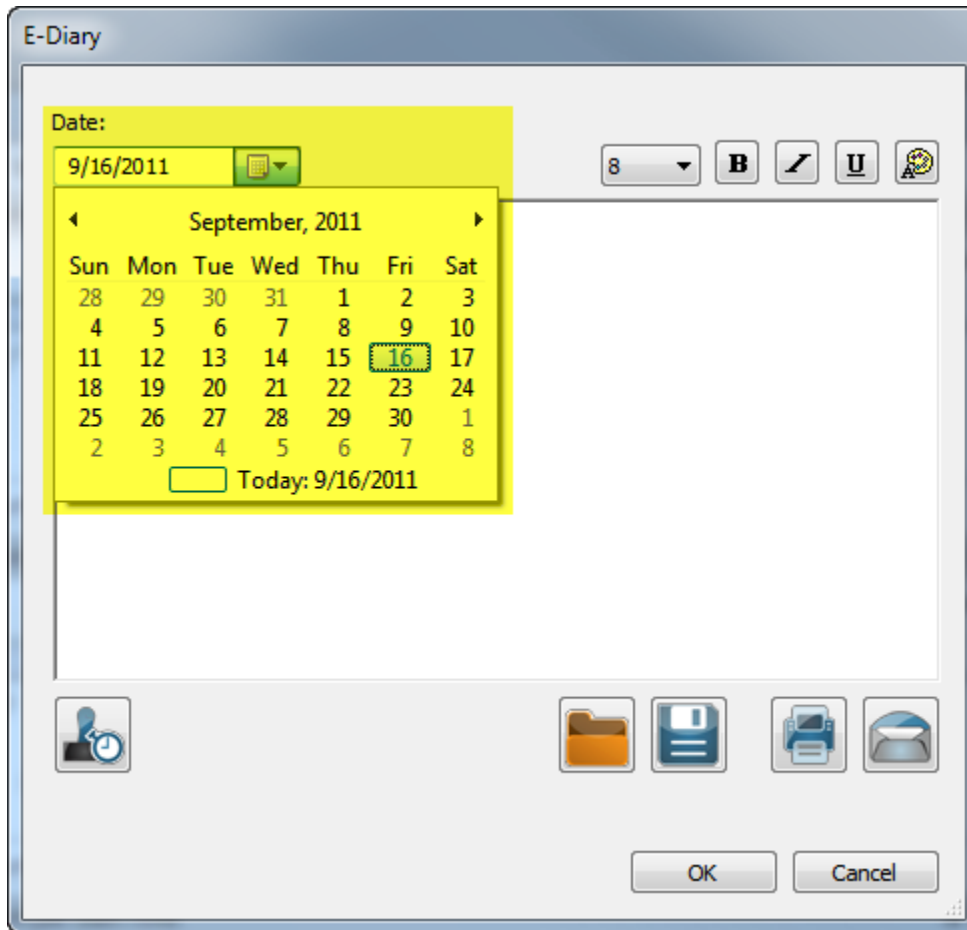
To access the E-Diary, use the hotkey combination "Ctrl+E" or open the Tools menu and select the E-Diary option.



Selecting the E-Diary option will open the E-Diary user interface where new journal entries can be added, or existing journal entries can be viewed or modified.

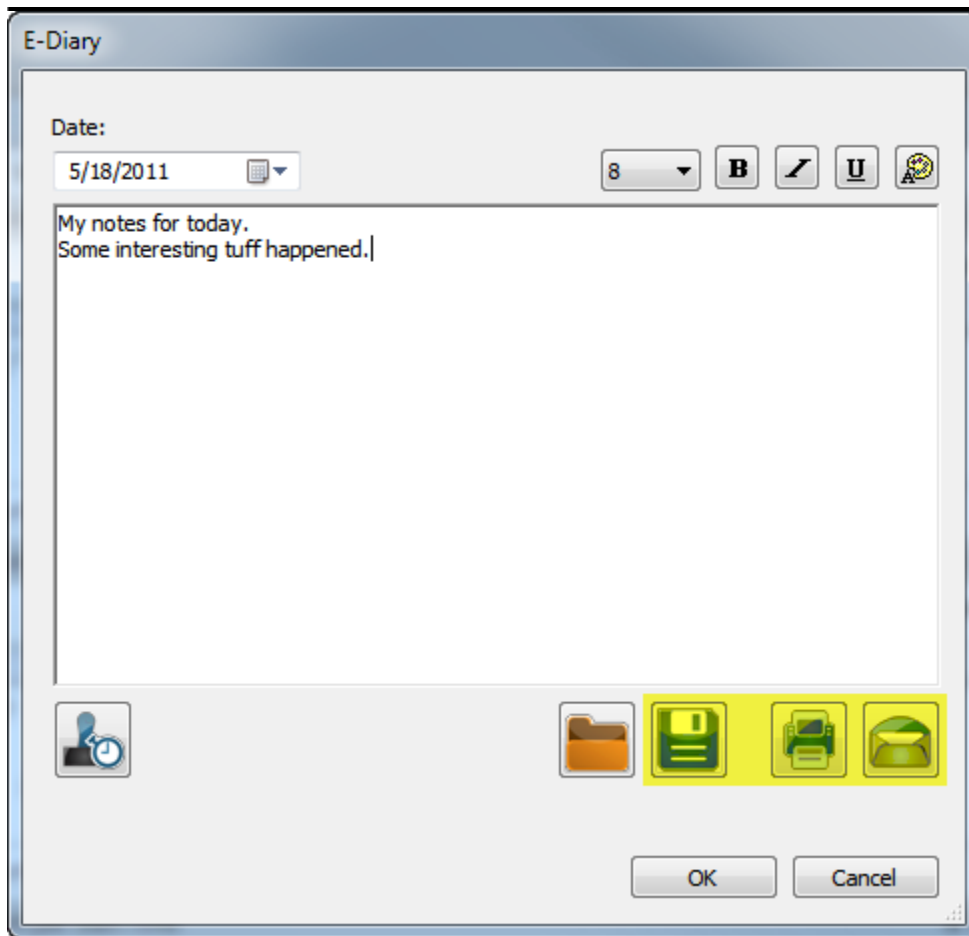


By default, the E-Diary user interface is set for the current day and all journal entry modifications will pertain to that day. It is very simple to select different days, though. The date can be selected with a simple calendar pop-out:



Select a different day to add journal entries for that day, or to view and edit existing entries.

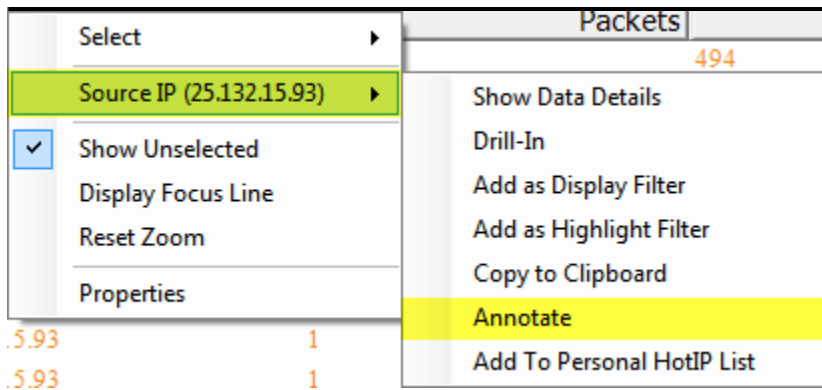
The E-Diary is private to the user by default, but supports three different sharing options: save the journal entry to a file, print the journal entry, or email the journal entry:



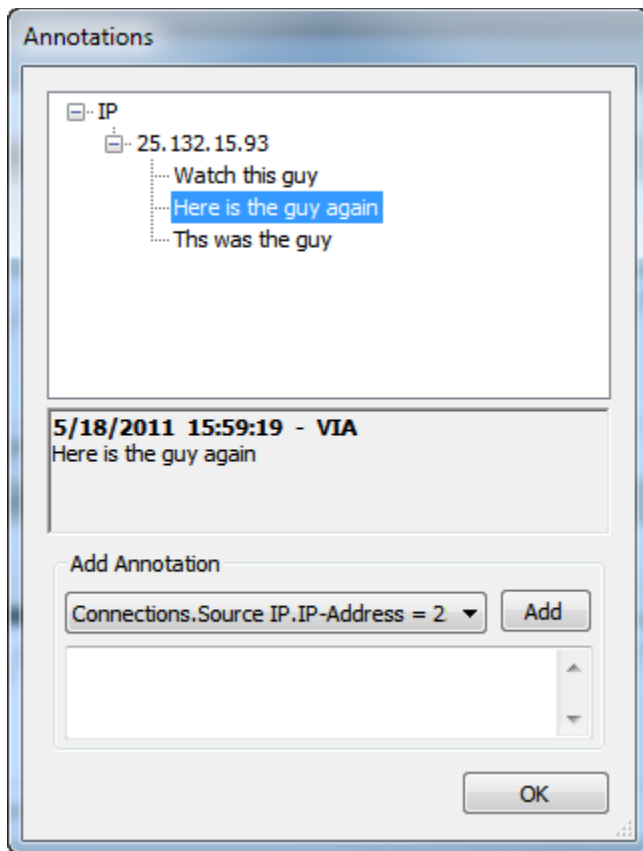
3.5.4.3 Annotations

Annotations are a great way of sharing information between users about particular data values. Annotations are not only available to the different users of VIAssist, but also span data sources. For instance, adding an annotation about a particular IP address would likely be relevant regardless of the data source where the IP address resides.

Annotations can be added to any data element. Access the Annotate option by right-clicking inside of a view to open the context menu. Select the field related sub-menu and then select the Annotate option.

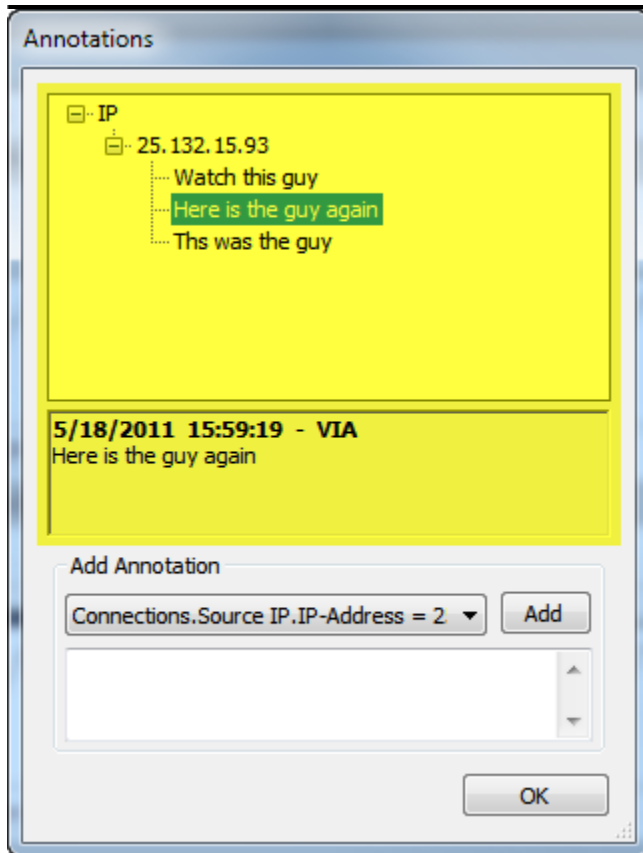


Selecting the Annotate option will open the Annotations user interface where existing annotations can be viewed and new annotations can be added.

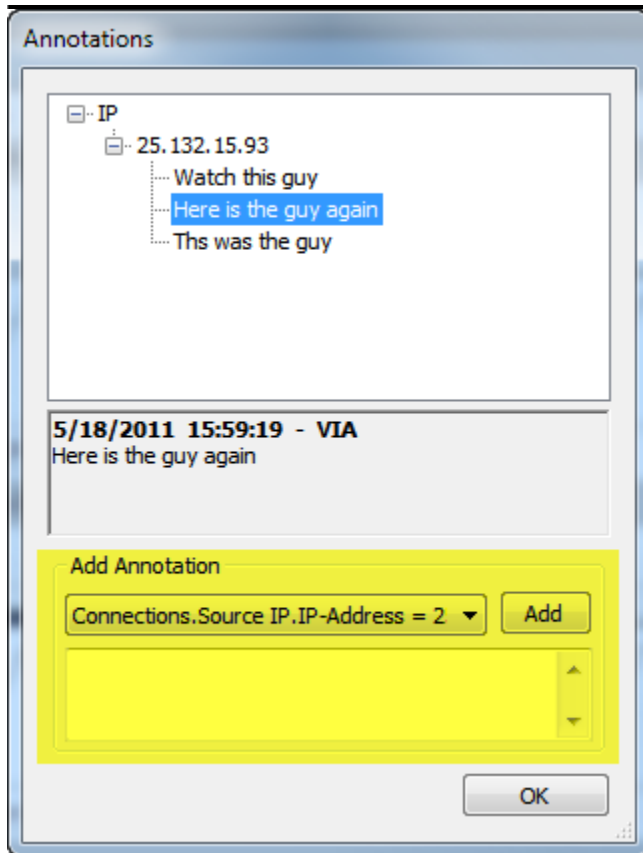


The Annotations user interface is divided into two sections for viewing and adding annotations. The top half of the user interface is devoted to viewing existing annotations while the bottom half of the user interface is for adding new annotations.

Use the tree list navigation in the top half of the interface to view existing annotations:



To add an annotation, use the drop down box in the bottom half of the user interface to select the field and value information that needs annotating. Add any needed comments to the text box beneath the drop down box. For example, comments could include date and time with a short description. Clicking the "Add" button will add the annotation for others to see.

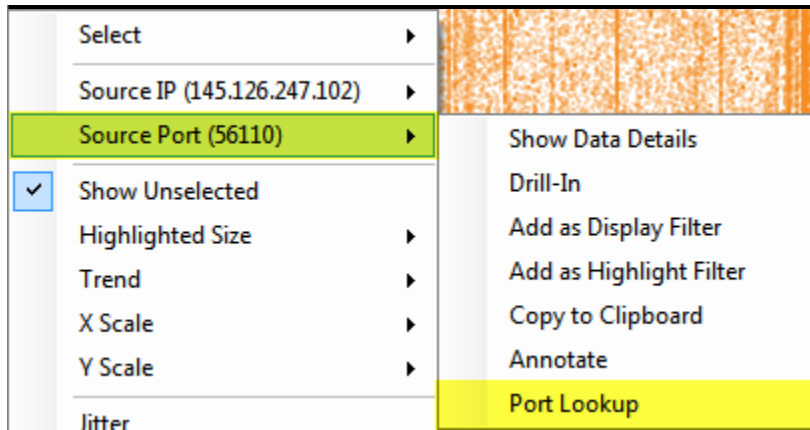


3.5.5 Context Menus

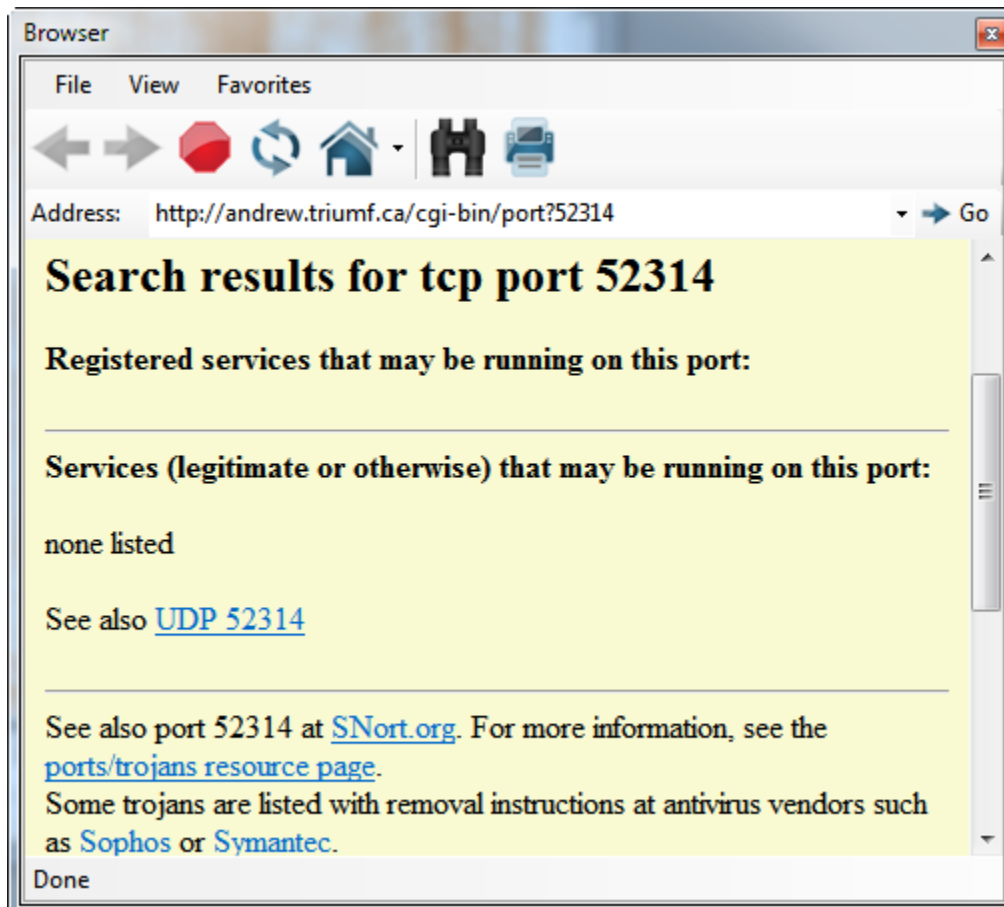
Every visualization in VIAssist supports a right-click context menu. Right-clicking on the visualization will open a context menu with options relevant to the visualization or to the data element that was clicked. Many context menu items are optional and configurable and may not always be applicable. The following sections will cover the most common context menu options.

3.5.5.1 Port Lookup

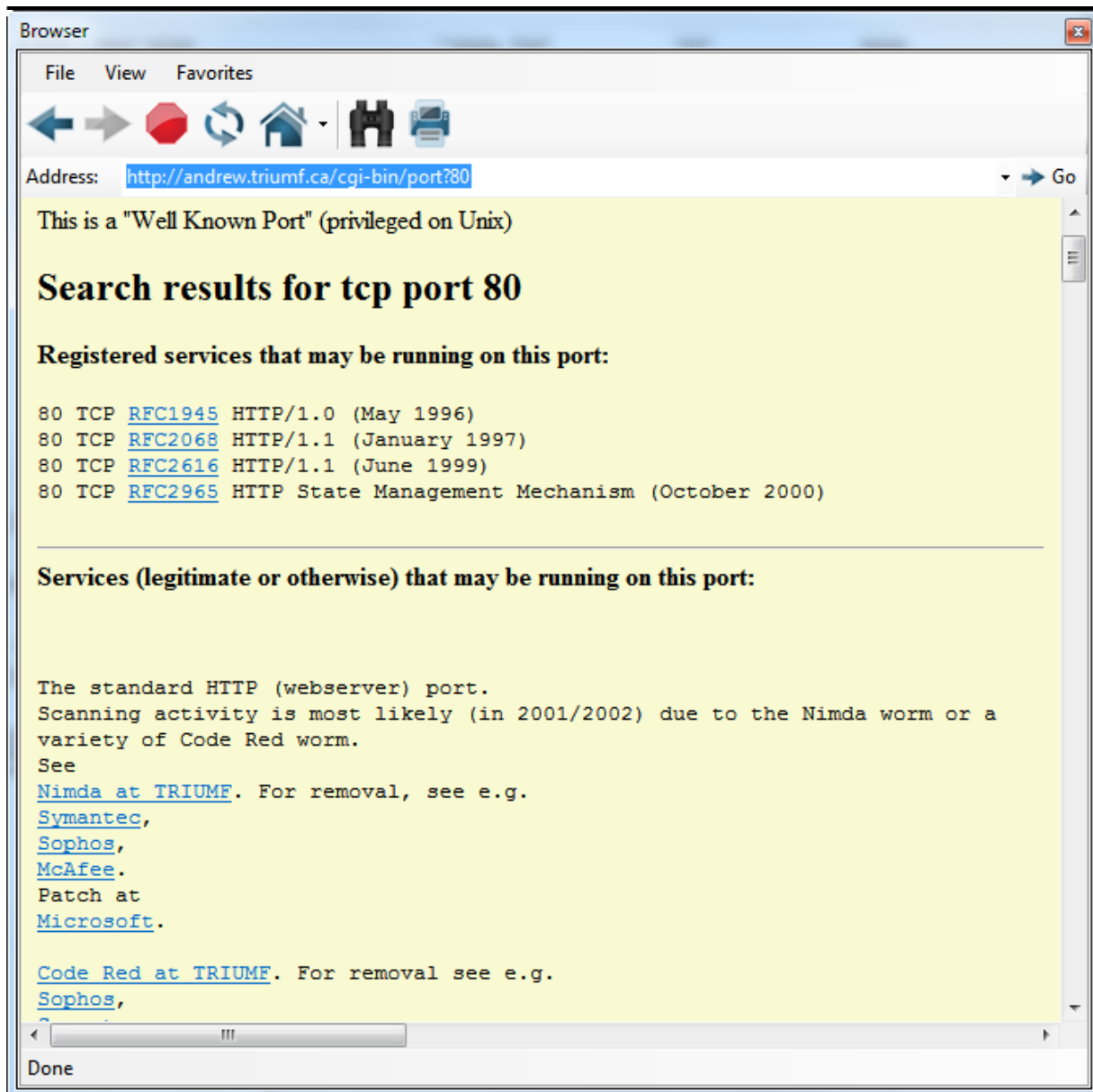
When a visualization uses port related data, the Port Lookup option will be available from the context menu for the port related data element. To access the Port Lookup, open the context menu by right-clicking on a visualization data element, select the appropriate field sub-menu, then select the Port Lookup option:



The Port Lookup option will open a Browser window to display a list of search results related to the port number of the data element:

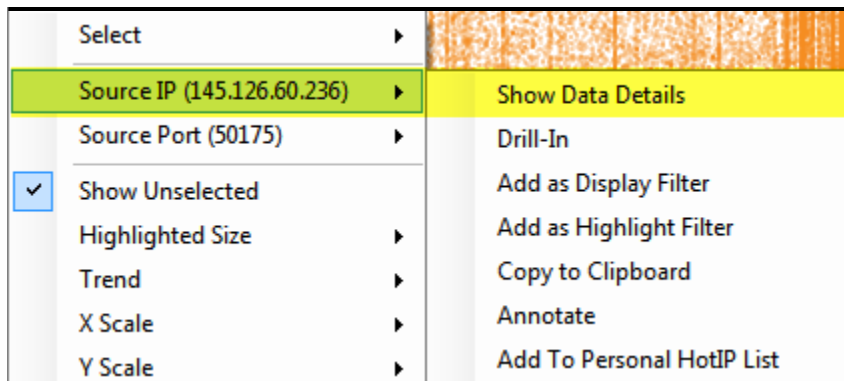


There is a wide range of ports, and not all have known, legitimate uses, such as the port in this example. Other ports, such as port 80 for HTTP, will show their usage. Usage listed will contain both legitimate uses and attack uses:



3.5.5.2 Data Details

A Data Details view is available from all VIAssist visualization views. To access the Data Details view, open the context menu for a data element and select the Show Data Details option:



The Data Details view displays raw data in a table format. The fields of data that can be displayed are configured when opening the Data Details view.

Data Details

Viewing details for: **Source IP.IP-Address = 145.126.46.39**

Show: ☐ Row ID ☒ Cluster Count [Configure](#)

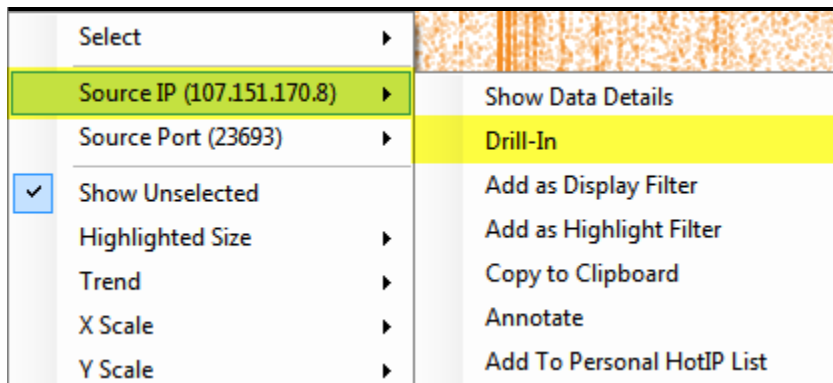
	Bytes	Source IP.IP-Address	Source Port	Destination IP.IP-Address	Destination Port	Source Country.Lower	Start Time	Cluster Count
▶	58	145.126.46.39	59770	160.97.11.68	53	united states	5/2/2010 12:09:...	1
	62	145.126.46.39	10336	195.227.68.225	53	united states	5/2/2010 12:10:...	1
	62	145.126.46.39	44910	175.191.232.14	53	united states	5/2/2010 12:10:...	1
	124	145.126.46.39	32437	151.240.87.204	53	united states	5/2/2010 12:10:...	1
	138	145.126.46.39	18020	160.97.249.29	53	united states	5/2/2010 12:06:...	1

Find: [Previous](#) [Next](#)

[Export to CSV](#) Rows: 5

3.5.5.3 Drill-In

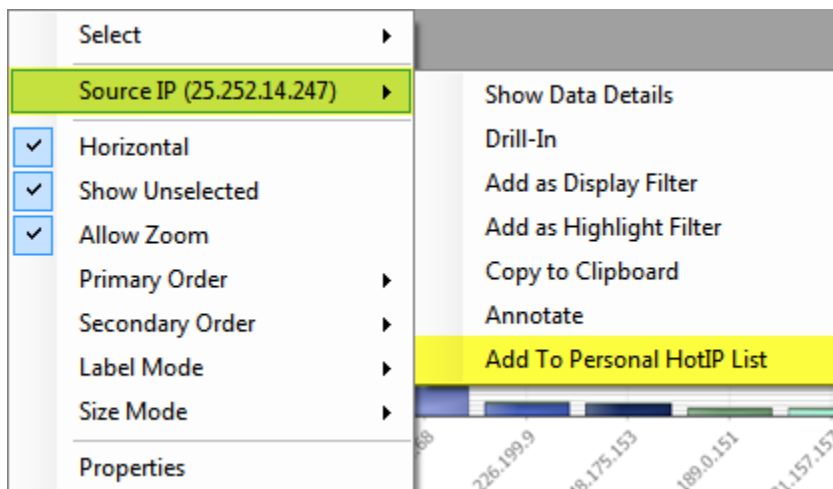
Drilling into a visualization is available from the right-click context menu. Drilling into a visualization focuses the visualization around a particular data element, which helps reduce the noise of too much information. To access the Drill-In capability, open the context menu, select the appropriate field related sub-menu, and select the Drill-In option:



For more information on drilling into data, [please see the "Drilling Into Data" section](#).

3.5.5.4 Personal Hot IP List

When a visualization view uses IPs as data, the Add To Personal HotIP List context menu option will be available. To access this option, open the right-click context menu for a data element, select the appropriate field related sub-menu, and select the Add To Personal HotIP List option:



For more information on using Personal Hot IP Lists, [please see the "Hot IP Lists" section](#).

3.5.6 Manipulating the Data Sheet

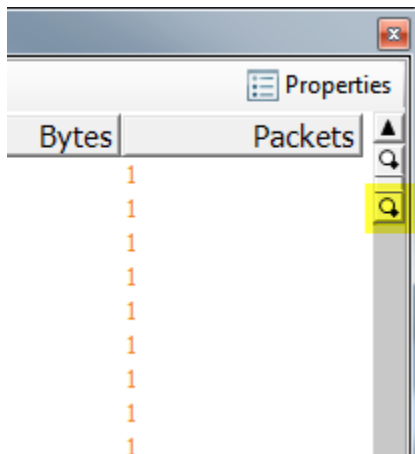
The Data Sheet view is an effective way to view lots of raw data. It is organized much like a typical spreadsheet with columns and rows of data. Each column of a Data Sheet corresponds to a field of data in the data repository. Each row contains all of the values for each of the columns.

Two representations of the data are available in the Data Sheet: textual and graphical. The Data Sheet will default to displaying a textual version of the data:

Data Sheet: Source IP,IP-Address, Source Port, Destination IP,IP-Address, Destination Port, Cluster Count, Bytes, Packets

Source_IP,IP-...	Source_Port	Destination_I...	Destination_P...	Cluster_Count	Bytes	Packets
1.100.22.14	53	160.97.11.68	5296	1	176	1
1.100.22.14	53	248.5.109.176	7426	1	142	1
1.100.22.14	53	248.5.109.176	58480	1	164	1
1.103.55.148	53	175.191.232.14	1388	1	120	1
1.103.55.148	53	175.191.232.14	21058	1	148	1
1.103.55.148	53	175.191.232.14	64483	1	175	1
1.113.164.131	53	175.191.232.14	4007	1	193	1
1.113.164.131	53	175.191.232.14	9745	1	172	1
1.113.164.131	53	175.191.232.14	12789	1	128	1
1.113.164.131	53	175.191.232.14	12910	1	148	1
1.113.18.194	53	160.97.11.68	27658	1	145	1
1.113.18.194	53	160.97.11.68	27960	1	145	1
1.113.18.194	53	160.97.11.68	30152	1	145	1
1.113.18.194	53	160.97.11.68	39271	1	145	1
1.116.224.206	53	160.97.11.68	15477	1	119	1
1.116.224.206	53	160.97.11.68	16316	1	123	1
1.116.224.206	53	160.97.11.68	19319	1	204	1
1.116.224.206	53	160.97.11.68	40063	1	123	1
1.116.224.206	53	160.97.11.68	44377	1	204	1
1.116.224.206	53	160.97.11.68	47028	1	204	1
1.119.27.104	53	160.97.11.68	3728	1	258	1
1.119.27.104	53	160.97.11.68	7676	1	258	1
1.119.27.104	53	160.97.11.68	17478	1	258	1
1.119.27.104	53	160.97.11.68	26464	1	218	1

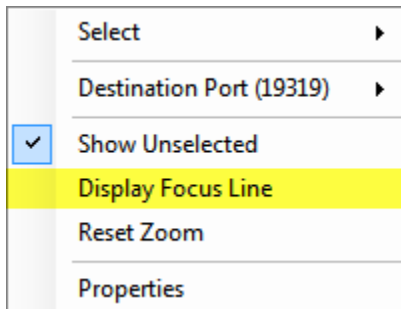
While the textual version of the Data Sheet can be useful, the graphical version can facilitate visual searches of data easier, such as when the data is numeric based. To change the Data Sheet to graphical mode, click the zoom button on the scrollbar:



The Data Sheet will now update all fields of information to a graphical representation. Numeric values are represented as horizontal bars with a proportional length to the maximum value of the column. Category and date values are represented as blips positioned based on the relative category value or position in time.



While in the Data Sheet's graphical mode it is still common to want the text version of specific data. The Data Sheet has an optional Focus Line that will display the textual representation of the data element that is hovered over with the mouse cursor. To enable the Focus Line, right-click anywhere on the Data Sheet visualization to open the context menu and select the Display Focus Line option.



The Focus Line appears directly below the column headers and will update based on which data row is hovered.

Data Sheet: Source IP,IP-Address, Source Port, Destination IP,IP-Address, Destination Port, Cluster Count, Bytes, Packets

Source_IP,IP-...	Source_Port	Destination_I...	Destination_P...	Cluster_Count	Bytes	Packets
1.116.224.206	53	160.97.11.68	19319	1	204	1

Each column can be sorted ascending or descending. Sorting capability can make searching through the data much easier by establishing a desired ordering of the data. To sort a column, click on the column header of the column to be sorted. An up or down arrow will now show in the column header indicating the sorting direction.

Take for example the case of wanting to find high data activity. By using the graphical representation of the Data Sheet and by sorting the Bytes column descending, it becomes very easy to fine high data activity.

Data Sheet: Source IP,IP-Address, Source Port, Destination IP,IP-Address, Destination Port, Cluster Count, Bytes, Packets

Source_IP,IP-...	Source_Port	Destination_I...	Destination_P...	Cluster_Count	Bytes ▼	Packets
------------------	-------------	------------------	------------------	---------------	---------	---------

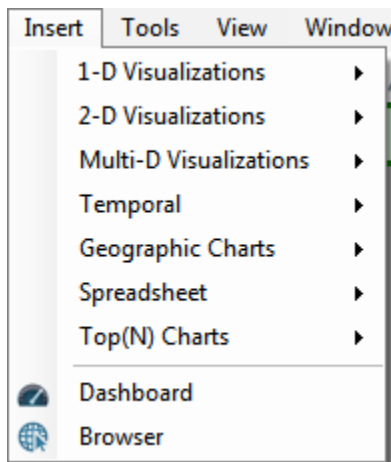
It's easy to spot where the high activity has taken place. Further, by having the Data Sheet in graphical representation mode and by sorting descending on Bytes, it's easy to spot this as suspect activity because it is an outlier. For most of the data rows, there is no activity or very low activity, indicating that the high spike is unusual and should be examined.

3.5.7 Arranging Views

When a large number of visualizations are inserted into the VIAssist workspace, it could become cluttered very quickly and difficult to manage. However, VIAssist offers a lot of flexibility in window management, making it simpler to arrange windows to best suit the user's needs.

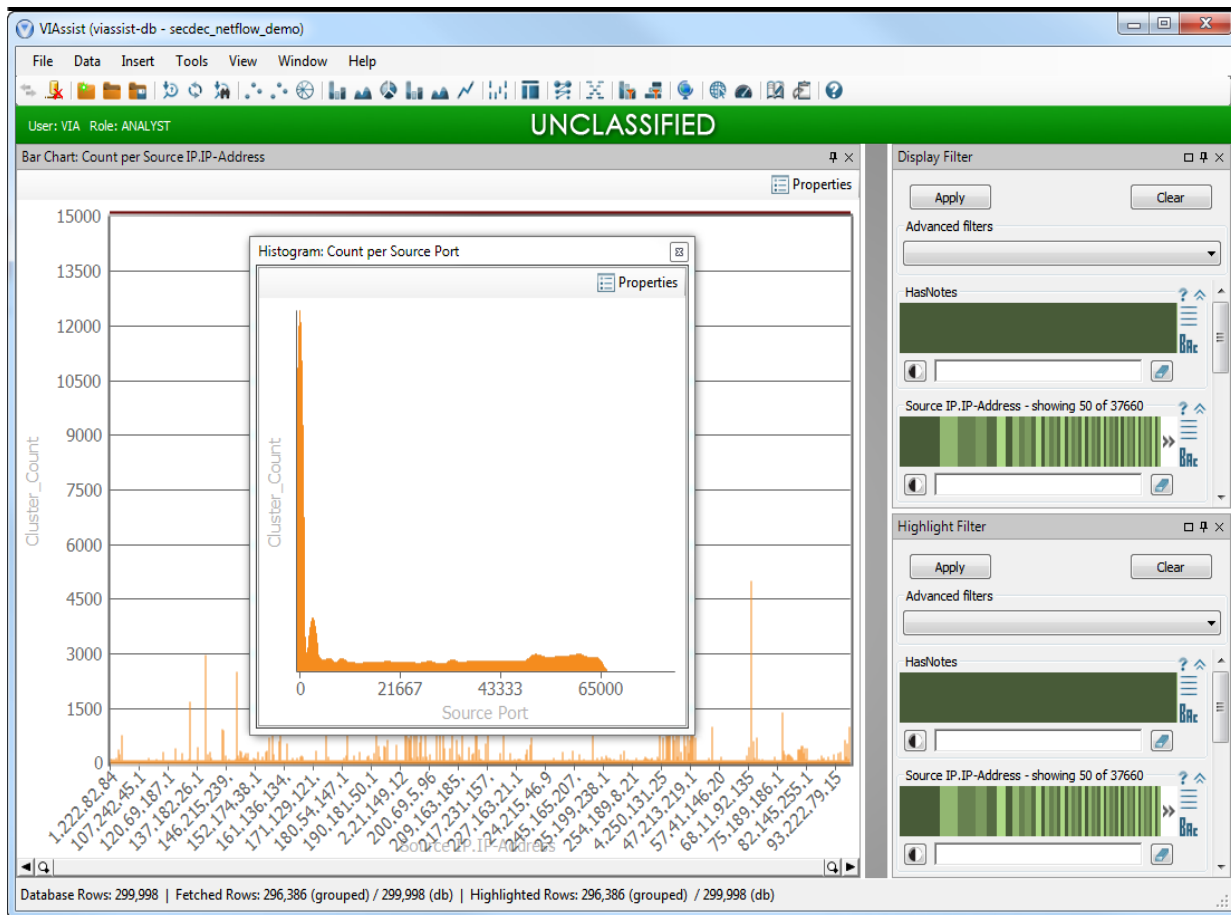
3.5.7.1 Inserting Views

Upon startup VIAssist has a blank workspace. The workspace becomes populated by inserting new views and visualizations as windows. When new views are inserted into VIAssist they are inserted as floating windows. To insert new views and visualizations, open the Insert menu and select one of the many options available for views and visualizations:



3.5.7.2 Managing Floating Views

Views as floating windows offers many possibilities for sizing and arrangement. A floating window functions similarly to most other windows: they can be resized and moved around, even to other monitors. The Histogram visualization is contained in a floating window in this example:

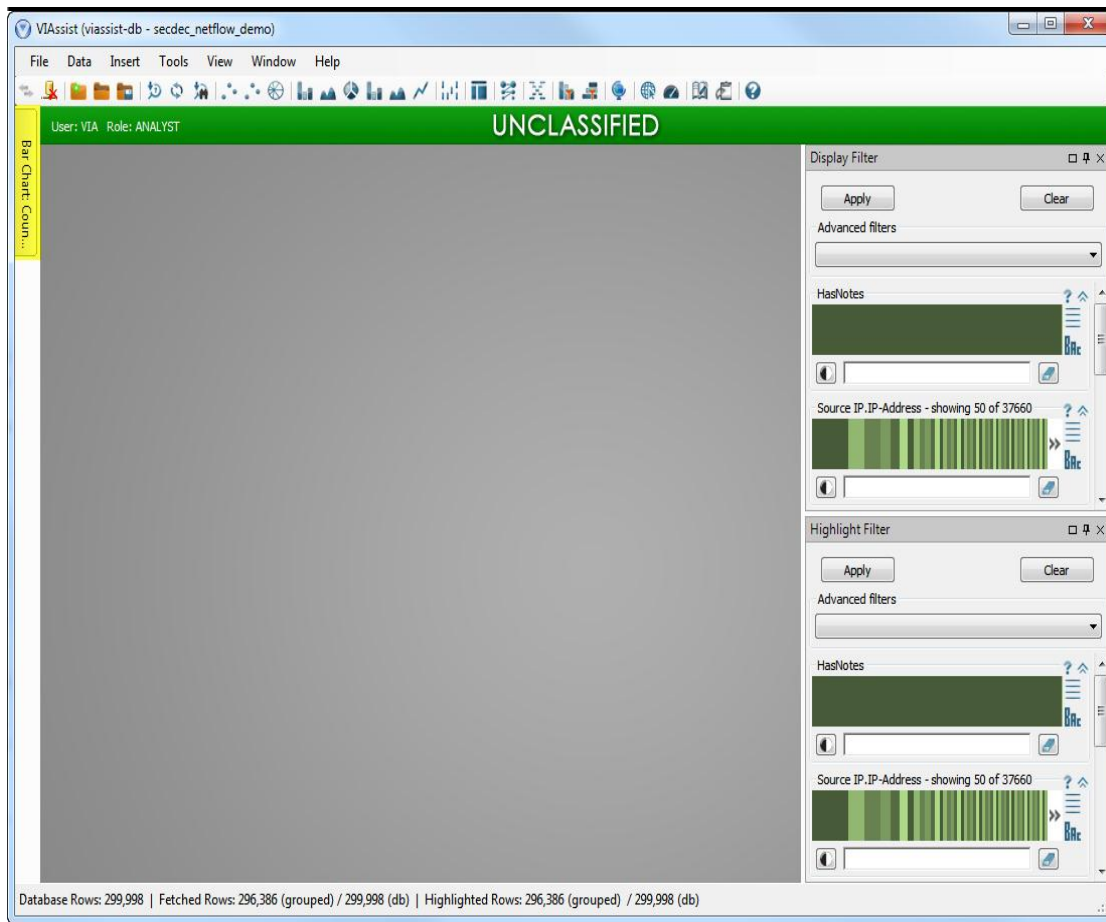


Most windows within VIAssist can be made to be floating windows at any time. There are two main ways of accomplishing this:

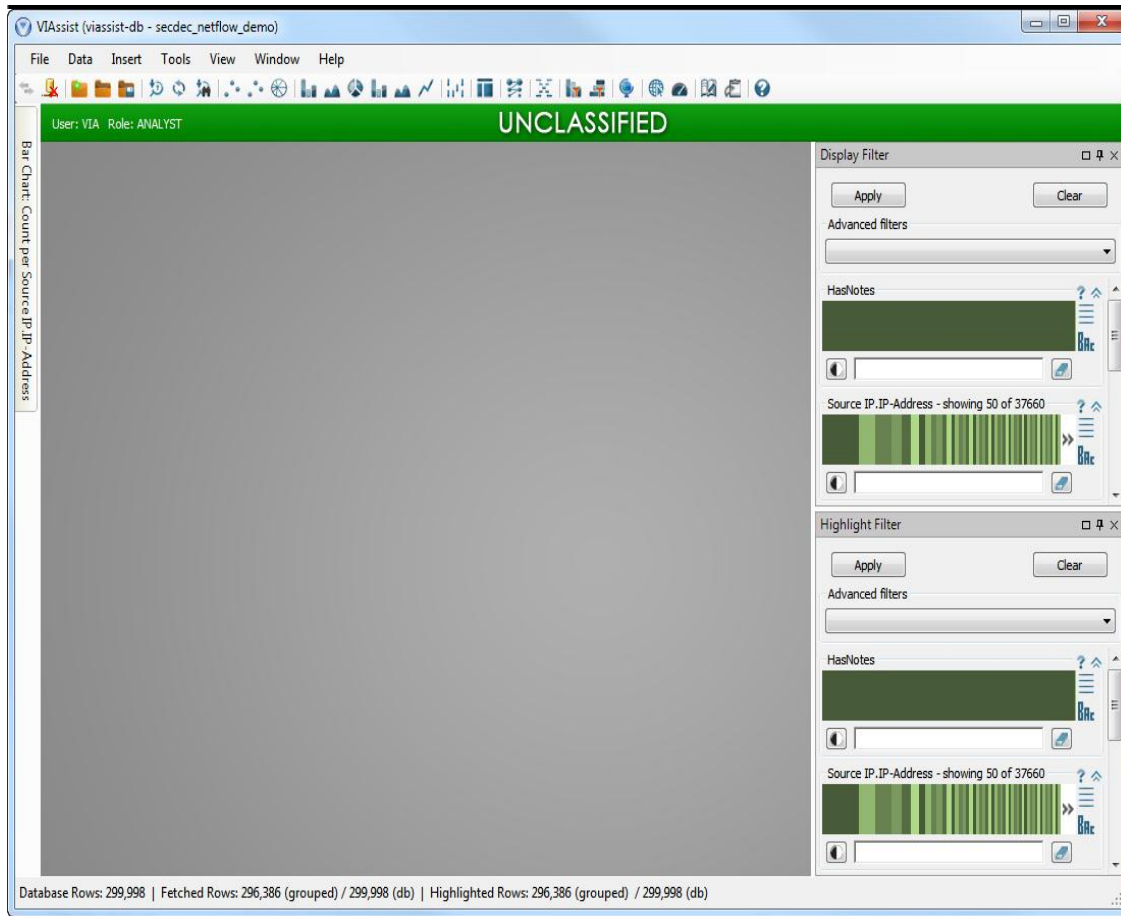
1. Double-click the title bar of a non-floating window. This will change it into a floating window.
2. Click and drag the title bar of a non-floating window. This will change it into a floating window and immediately allow placement to a new location.

3.5.7.3 Pinning and Unpinning

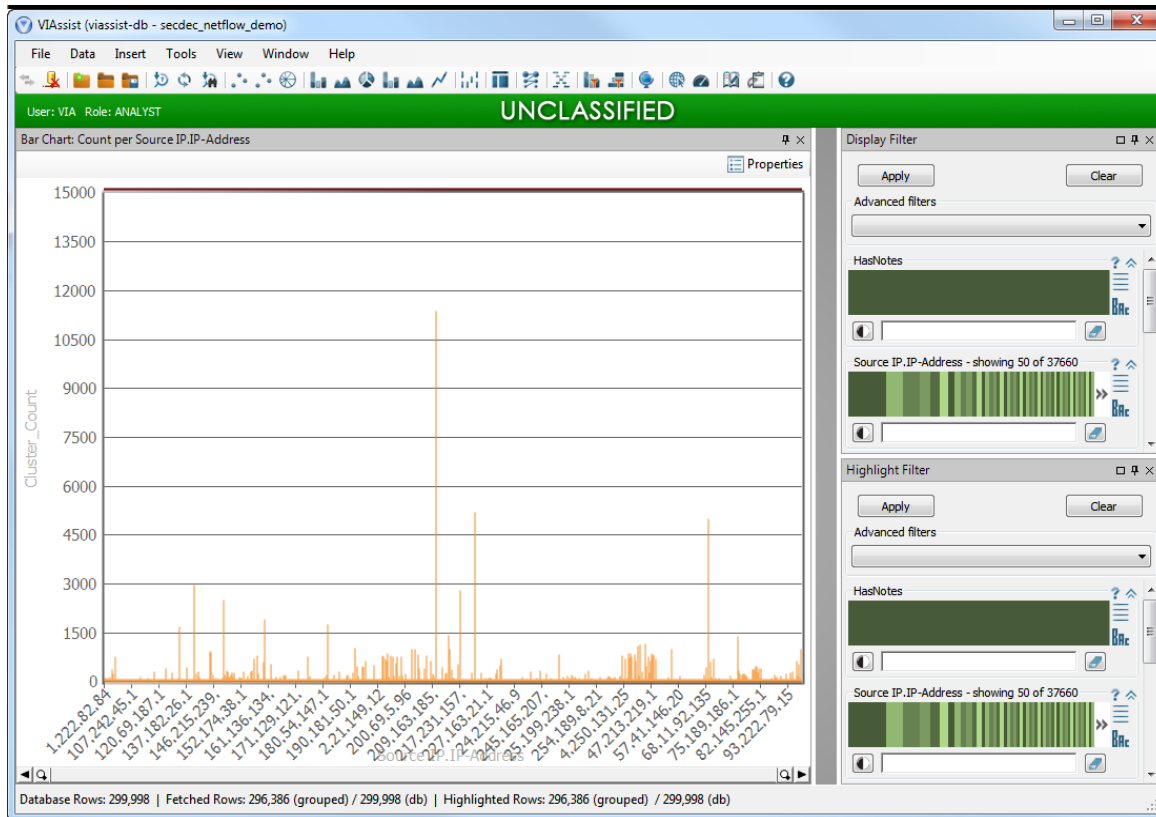
The pinning functionality of VIAssist's window management is useful for keeping views open that don't necessarily always need to be visible. Pinning windows is only available to non-floating windows and is accessed by clicking the pin icon that is next to the close button of a window. Pinning a window will cause the window to auto-hide into a window bar along the left or right side of the screen when the window does not have focus.



Accessing a pinned window will expand it so that the contents can be viewed:

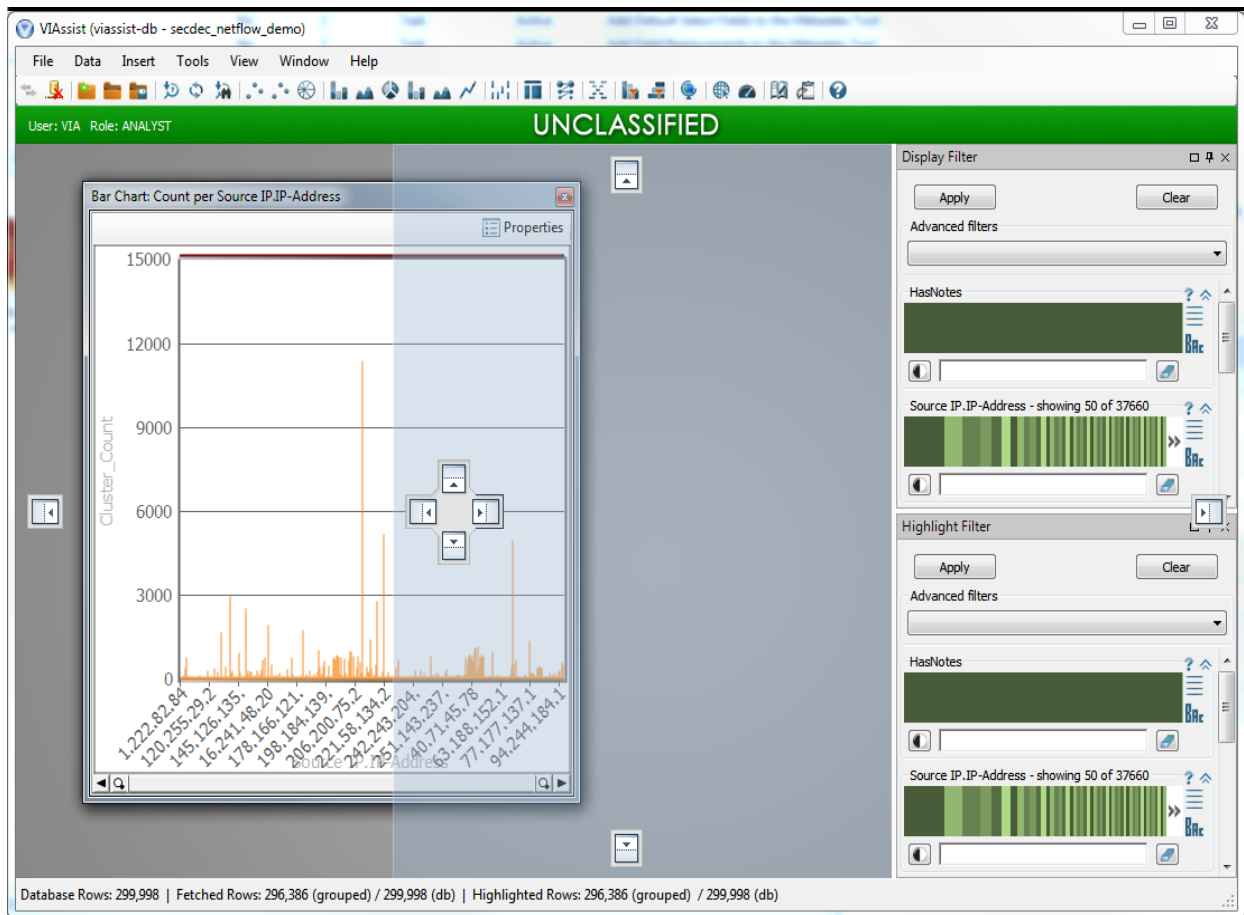


Unpinning a window reverses this so that a window will no longer auto-hide; it will always be visible. Simple click the pin icon that is next to the close button of a window to unpin it.

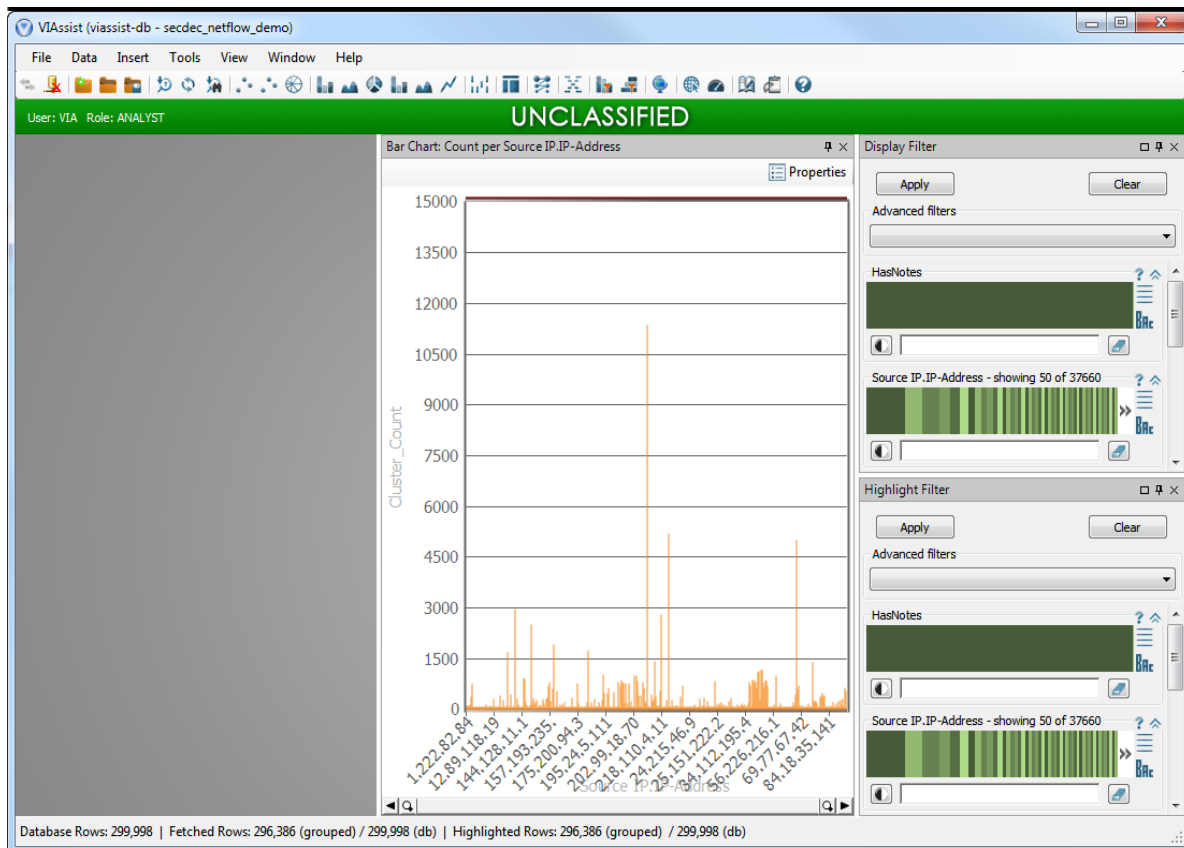


3.5.7.4 Docking Windows

Floating views can be docked to the main application workspace. To access the docking mode of VIAssist, click and drag a window's title bar. Docking guides will appear inside of the main application workspace indicating where the window can be docked. While still dragging the window, move the mouse over one of the docking guides to see how the window will be docked within the application.



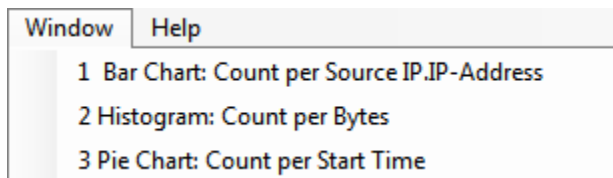
When a suitable docking position is found, simply release the mouse button to make the window dock.



Docking windows is not permanent and can be done as many times as desired.

3.5.7.5 Window Menu

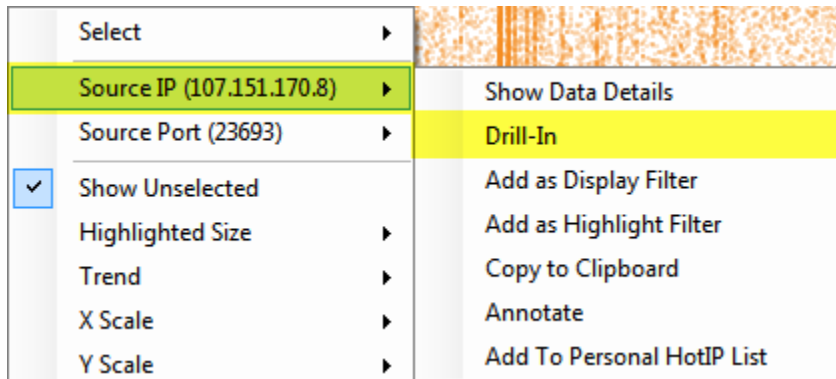
The window menu keeps a list of all open windows within VIAssist. While the window management of VIAssist makes it simple to create powerful arrangements, sometimes a list is the easiest thing to use to find windows. Clicking any of the windows listed in the Window menu will show or hide that window. An example of the window menu populated with a list of windows:



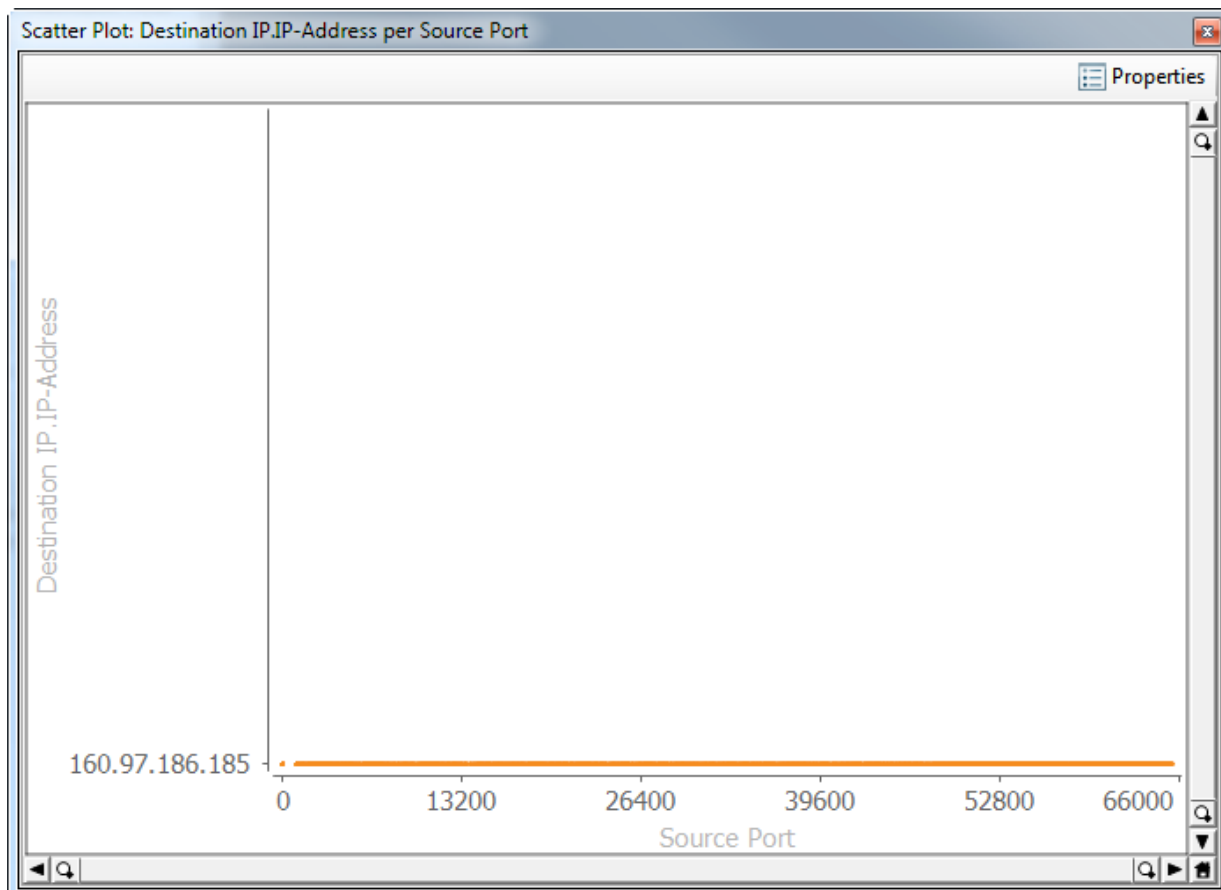
3.5.8 Drilling Into Data

Drilling into data is an easy way to distill a visualization to a subset of the data being displayed. Visualizations can then be focused on the data of interest instead of being polluted with all

fetches data that may not be relevant 100% of the time during an investigation. To drill into data, open the right-click context menu for a data element in a visualization and select the Drill-In option:

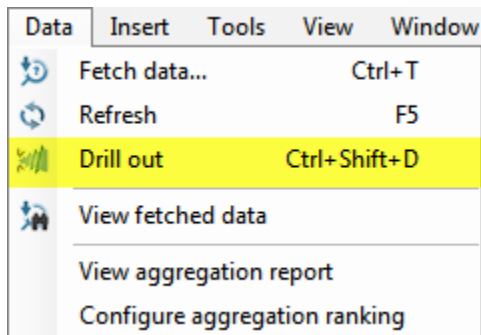


Using the Drill-In option will update the view to focus around the drilled-in data element:

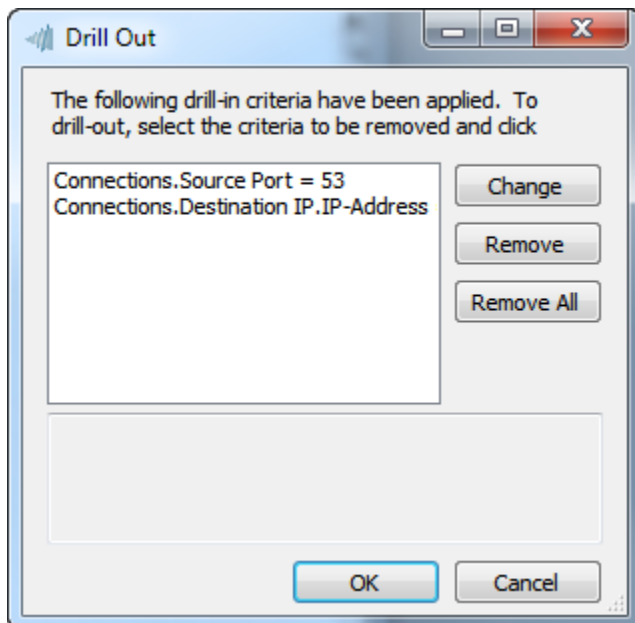


Drilling into data wraps an automatic query. When a drill-in event occurs, a query is established to fetch data related to the data element. The query is then executed and updated data is fetched and redisplayed in the visualizations.

To return to a drilled-out state, open the Data menu and select the Drill Out option. Note that the Drill Out option is only available if a Drill-In has been performed:



Drilling in can be done multiple times without drilling out in between. This creates a stack of drill-in queries that represent how to get to the current drilled in state. When drilling out, if there is more than one drill-in query in the stack, a dialog will open to show the current stack of drill-in queries.



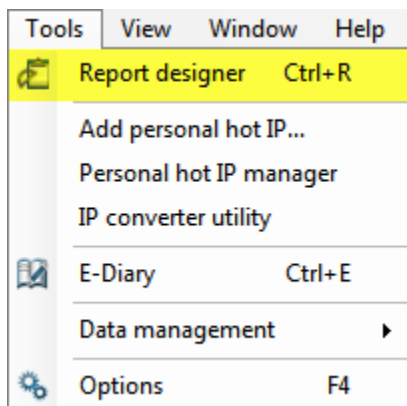
Instead of automatically drilling out all the way, this dialog gives fine grained control over how the drill out should occur. Drill-in queries can be modified or removed to change the drilled in state.

3.6 Using the Report Designer

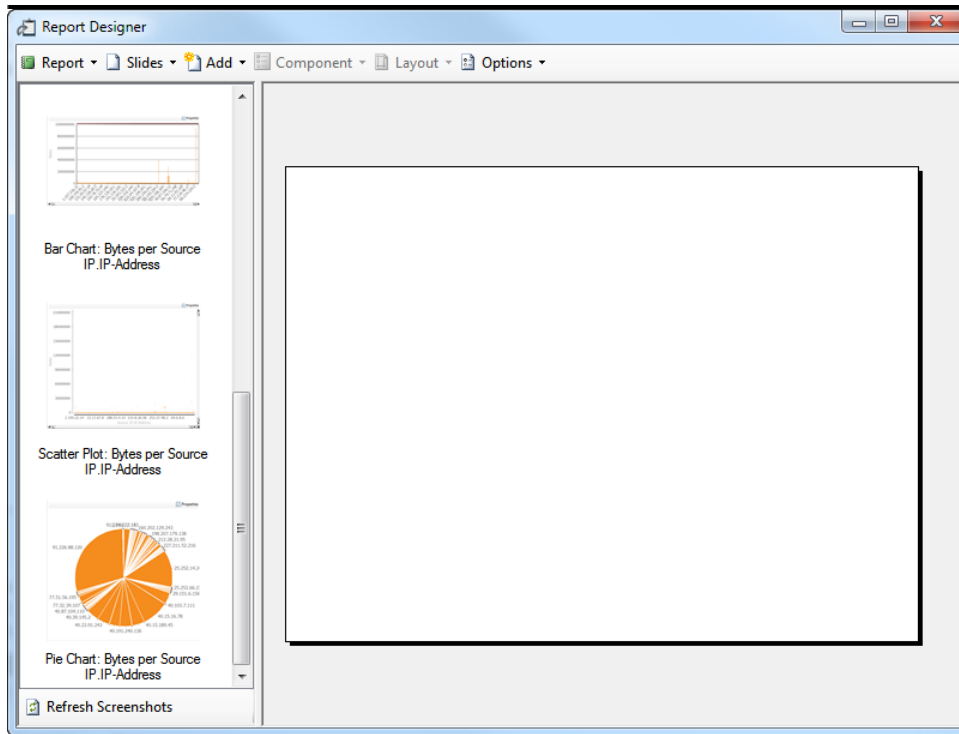
VIAssist's Report Designer is a simple way of enabling collaboration by making it easy to share analysis findings. The Report Designer makes it easy to share charts, graphs, and other annotations in a familiar slide oriented fashion. Reports can be exported as PowerPoint presentations or as PDF files. For analysis reports that may need updating frequently to present current analysis findings, the Report Designer supports Report Templates which make saving the layout and general data of a report easy, automatically handling the updating of the charts within the report.

3.6.1 Create a Report

Before creating a report, the VIAssist workspace should contain one or more visualization components. A new report can be created through the Report Designer. To access the Report Designer, use the hotkey combination Ctrl+R or open the Tools menu and select the Report Designer option.

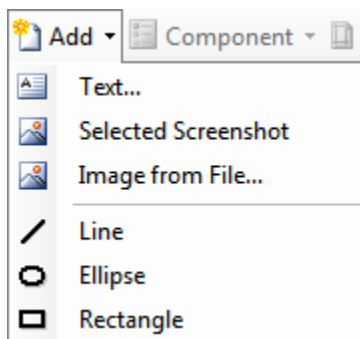


The way the Report Designer opens depends on the number of monitors that are available. If a single monitor is available, the Report Designer will open as any other window. If multiple monitors are available, the Report Designer will open on a second monitor.



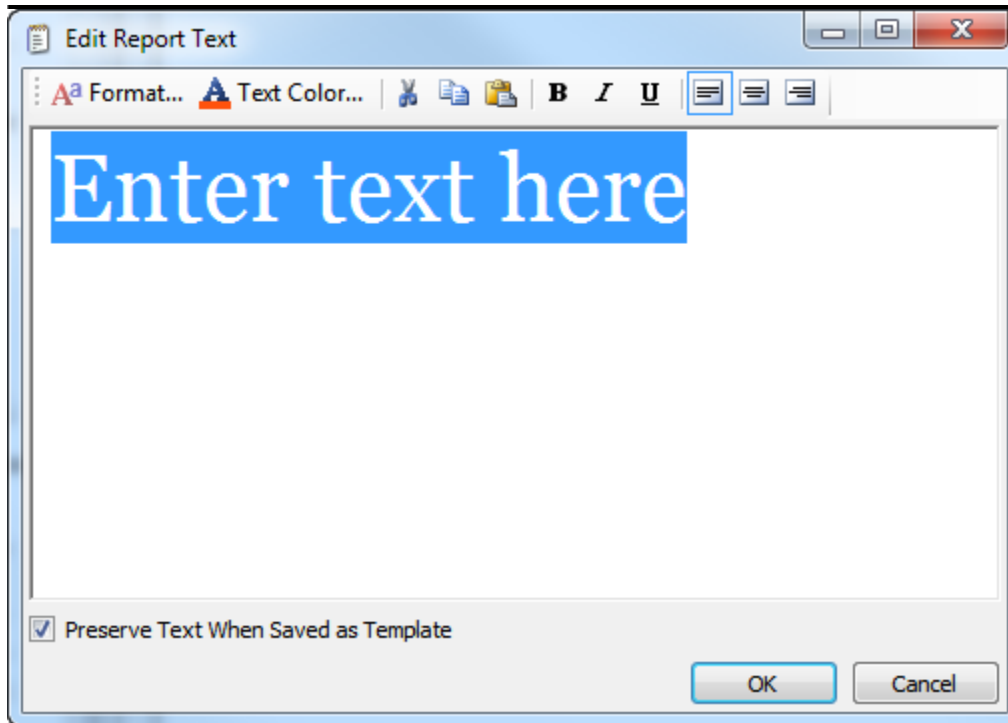
The Report Designer is divided into two main sections. The left side holds contains a visual list of all the visualizations and panels in the VIAssist workspace. If the VIAssist workspace is empty when the Report Designer is opened or if no data has been fetched, blank graphics will appear in the list instead.

The Report Designer supports most of the familiar and common functionality for creating slides: slide backgrounds, textual annotations, images, and drawing shapes. All of these options can be accessed from the Add menu and selecting the appropriate option:



Images added to a slide of the report can be resized as needed to fit the space.

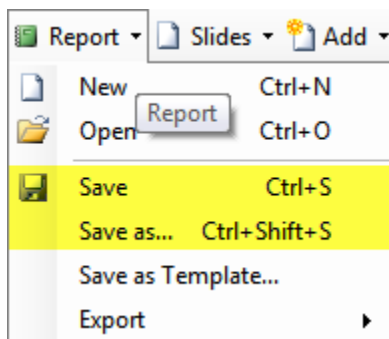
Text added to a slide is of a rich format that allows the most common functionality: font, color, style, and alignment. The text area itself can also be resized on the slide.



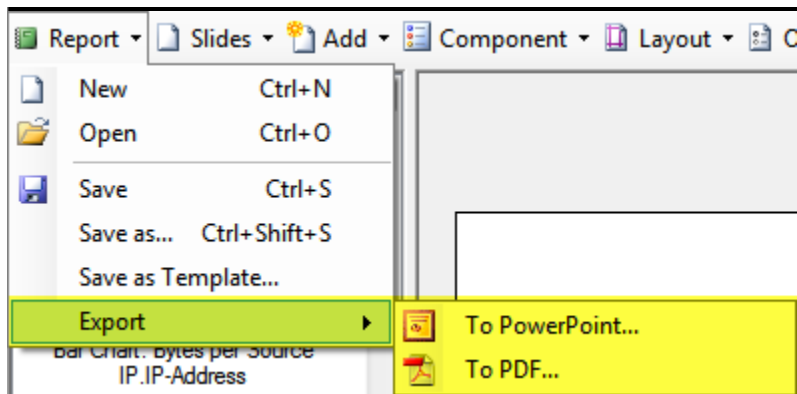
3.6.2 Save a Report

A report created with VIAssist's Report Designer can be saved in several formats.

Reports can be saved in VIAssist's VRP format to preserve all annotations and data used to create the report. To save the report as a VRP file, use either the Save or Save as . . . options in the Report menu:



Reports created with VIAssist's Report Designer can also be exported as other common formats. VIAssist currently supports exporting reports as PowerPoint presentations and PDF files. To export a VIAssist report as one of these common formats, select the appropriate export option from the Export sub-menu in the Report menu:

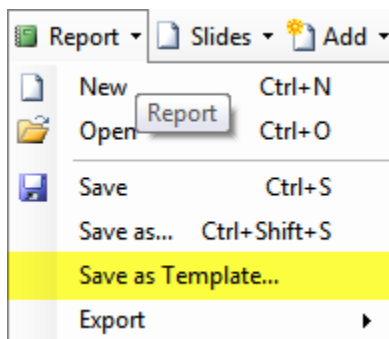


The Report Designer can also be used to create Report Templates. For more information using and saving Report Templates, [please see the "Report Templates" section](#).

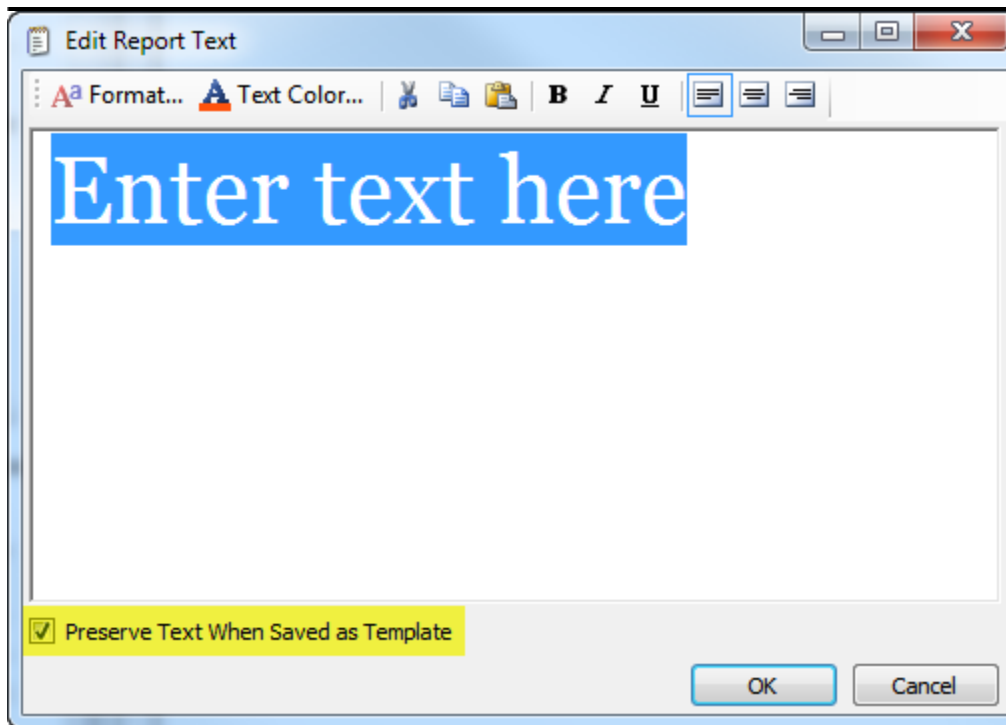
3.6.3 Report Templates

Report Templates are a simple way of creating a standard report that will update with new data. A Report Template is created in the same way as normal reports. For more information on creating reports, [please see the "Create a Report" section](#).

To save the report as a Report Template, select the Save as Template . . . option from the Report menu:



When saving a Report Template, be aware that text annotations are only saved if the Preserve Text When Saved as Template checkbox is checked when adding the text annotation:

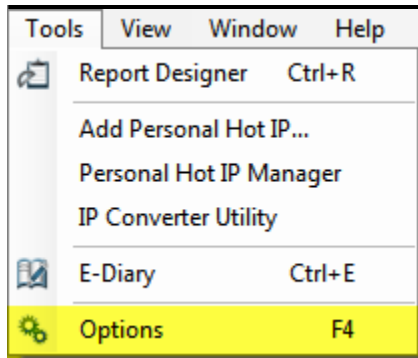


When a Report Template is loaded into VIAssist, the visualization views are automatically updated with the current data in the workspace. All shape objects are restored to their original positions. Any text that was set to preserve when saved in the template will also be restored.

3.7 Options

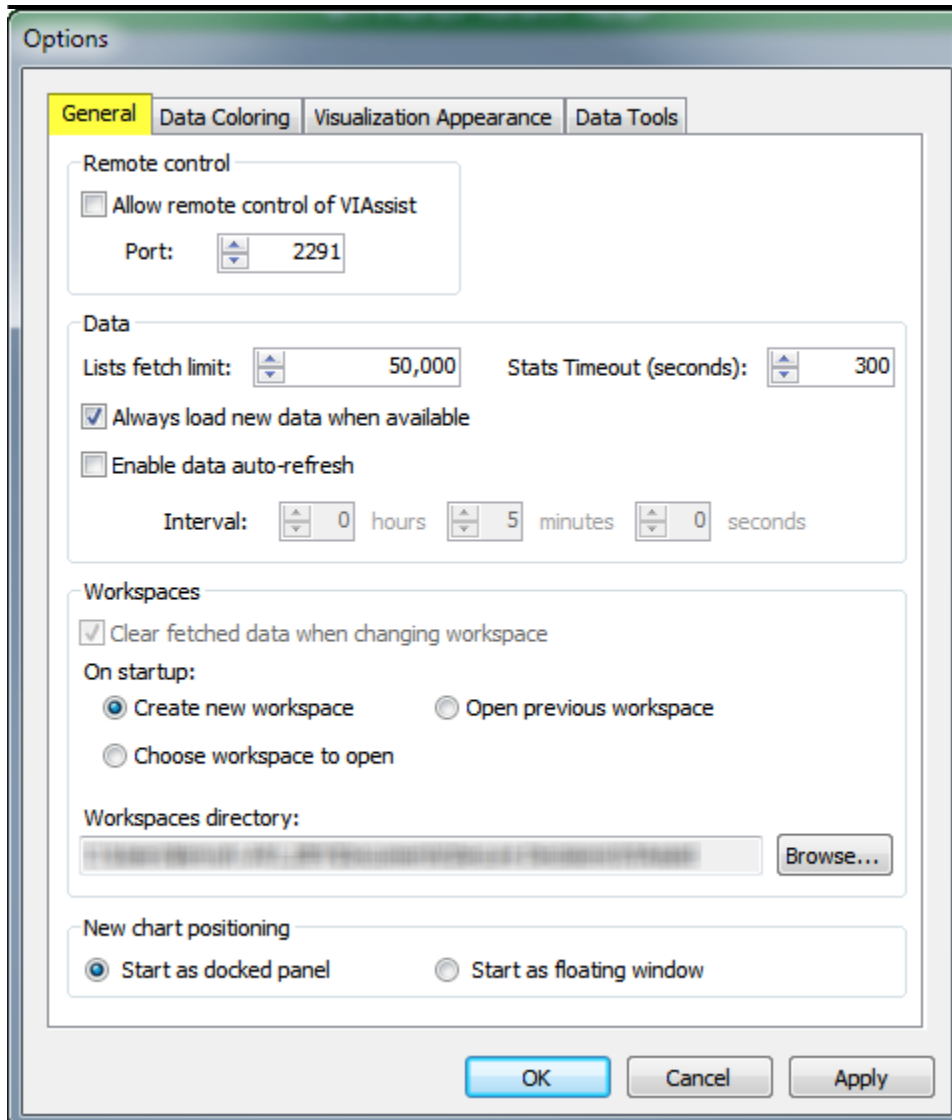
VIAssist exposes a number of configuration elements through its Options screen. The options that can be configured range from how VIAssist handles data fetching and workspace management, to visualization appearance and data coloring, as well as exposing certain data tool configurations.

To access the Options configuration of VIAssist, open the Tools menu and select the Options option:



3.7.1 General

View and edit VIAssist General options by accessing the General tab of the Options screen:



3.7.1.1 Data

The Data configuration options can be used to improve performance by limiting thresholds, to increase accuracy by ensuring latest data, or to automate routine data updates.

Select the Always load new data when available checkbox to force VIAssist to always load the latest available data when fetching:

Data

Lists fetch limit: Stats Timeout (seconds):

☒ Always load new data when available

☐ Enable data auto-refresh

Interval: hours minutes seconds

A useful function of VIAssist is to automate the retrieval of new data. This can be enabled by checking the Enable data auto-refresh checkbox:

Data

Lists fetch limit: Stats Timeout (seconds):

☒ Always load new data when available

☐ Enable data auto-refresh

Interval: hours minutes seconds

When this checkbox is enabled, an interval can be set that specifies how frequently VIAssist should auto-refresh data:

Data

Lists fetch limit: Stats Timeout (seconds):

☒ Always load new data when available

☒ Enable data auto-refresh

Interval: hours minutes seconds

3.7.1.2 Workspaces

VIAssist has several options for workspace configuration. On startup, VIAssist can do one of three different operations for workspace management:

Workspaces

☒ Clear fetched data when changing workspace

On startup:

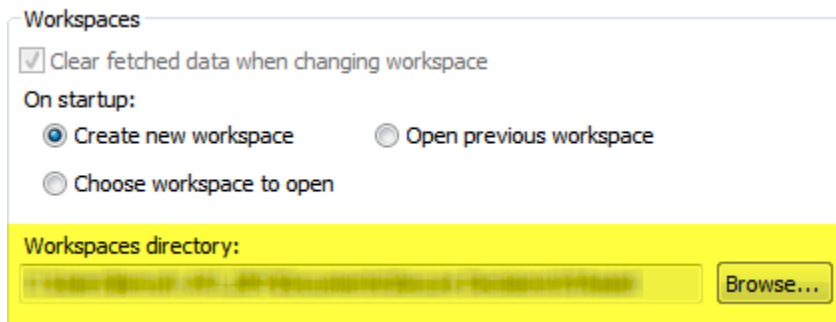
☒ Create new workspace ☐ Open previous workspace

☐ Choose workspace to open

Workspaces directory:

On startup, VIAssist can create a new workspace, open the previously used workspace, or prompt the user to open a workspace. Choose the option that best suits the typical workflow.

Workspaces are stored on disk in a user configurable location. By default, the workspaces are stored in the user's documents directory. The location to store workspaces can be changed by browsing for a new location:



The first option under the workspaces section, Clear fetched data when changing workspace, is not currently user configurable and is disabled.

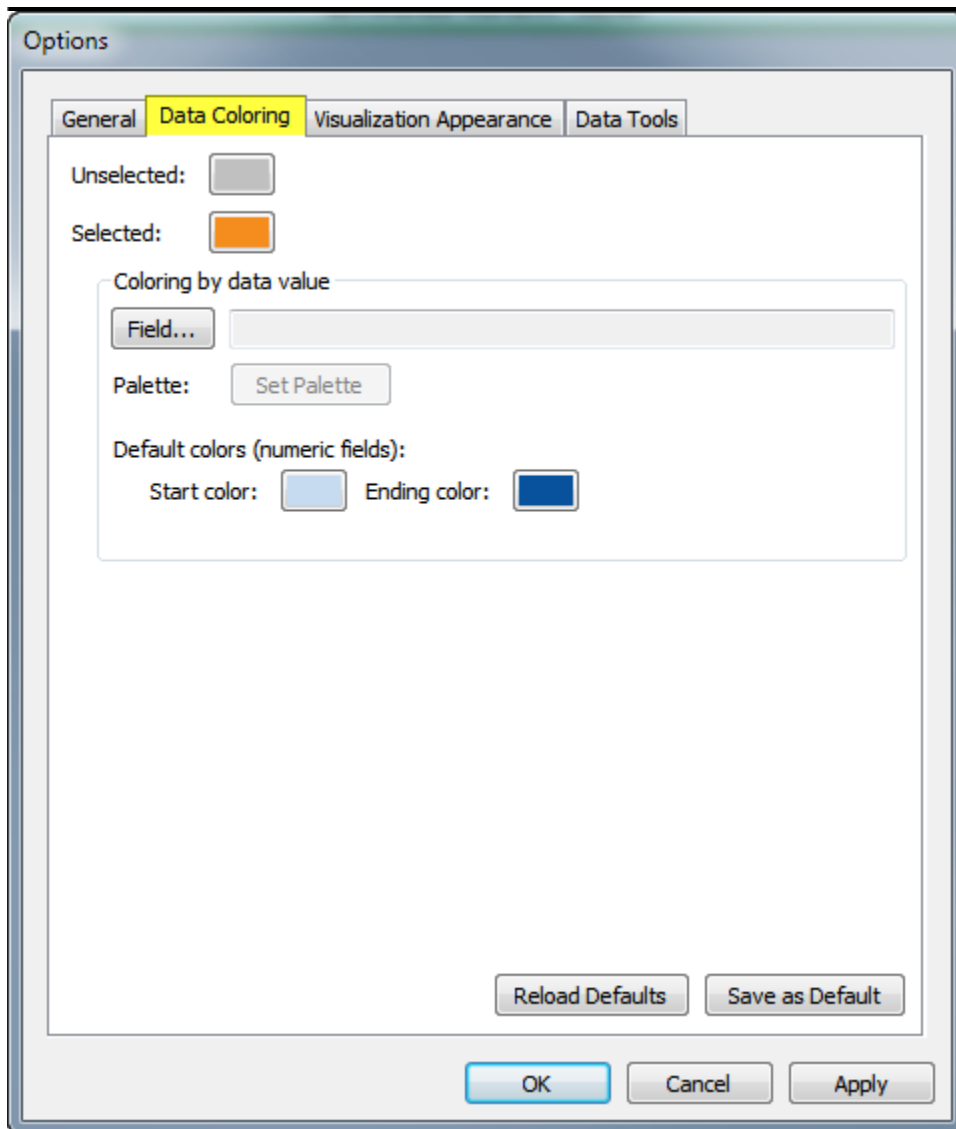
3.7.1.3 View Positioning

VIAssist offers two modes of opening new views: one mode will open a new view as a floating window that can be moved around, even to other monitors, and resized; the other mode opens view as automatically docked in the main VIAssist workspace. Select the mode based on the preferred workflow for introducing new views.



3.7.2 Data Coloring

View and edit VIAssist's Data Coloring options by accessing the Data Coloring tab of the options screen:



The two most basic data coloring options are the selected and unselected colors. These colors will be used when no other colors are specified.

Sometimes attention should be drawn to certain values of a field. The Coloring by data value section can be used to color a field by the ranges of values within that field. This makes it easier to spot specific data elements of interest:

Coloring by data value

Field...

Palette:

Default colors (numeric fields):

Start color: Ending color:

When a field is chosen, the Set Palette button can be used. Click the Set Palette button to access the Color Mapping form:

Color Mapping

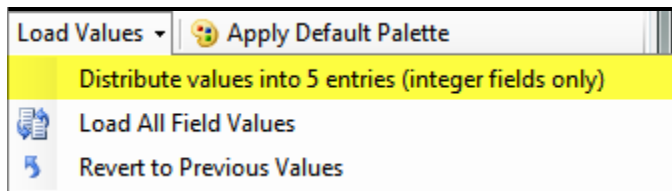
Field for coloring:

Color mappings

	Values	Color
▶	0 - 13106	<input type="color" value="#add8e6"/>
	13107 - 26213	<input type="color" value="#add8e6"/>
	26214 - 39320	<input type="color" value="#add8e6"/>
	39321 - 52427	<input type="color" value="#ffff00"/>
	52428 - 65535	<input type="color" value="#ff0000"/>
*		

Default color:

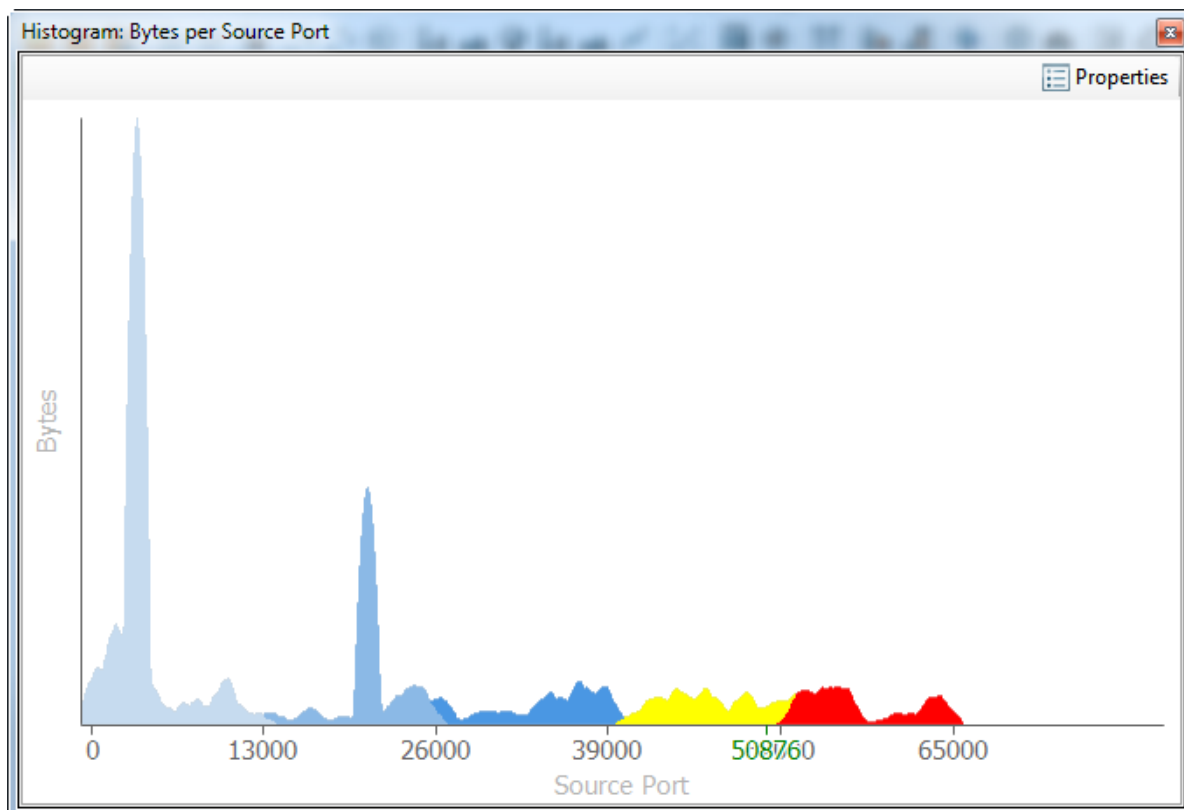
Range entries can be entered manually, but VIAssist can also automatically create five ranges that are evenly divided among the values. To let VIAssist create five ranges automatically, open the Load Values menu and select the Distribute Values into 5 entries option:



This automatic calculation can only be done on fields that can be represented numerically. Other field types will need to be distributed manually.

Once values or ranges of values are set, a color for each value or range of values can be selected. In this example, the Source Port field is being used and yellow and red are used to draw attention to the top end of the port values.

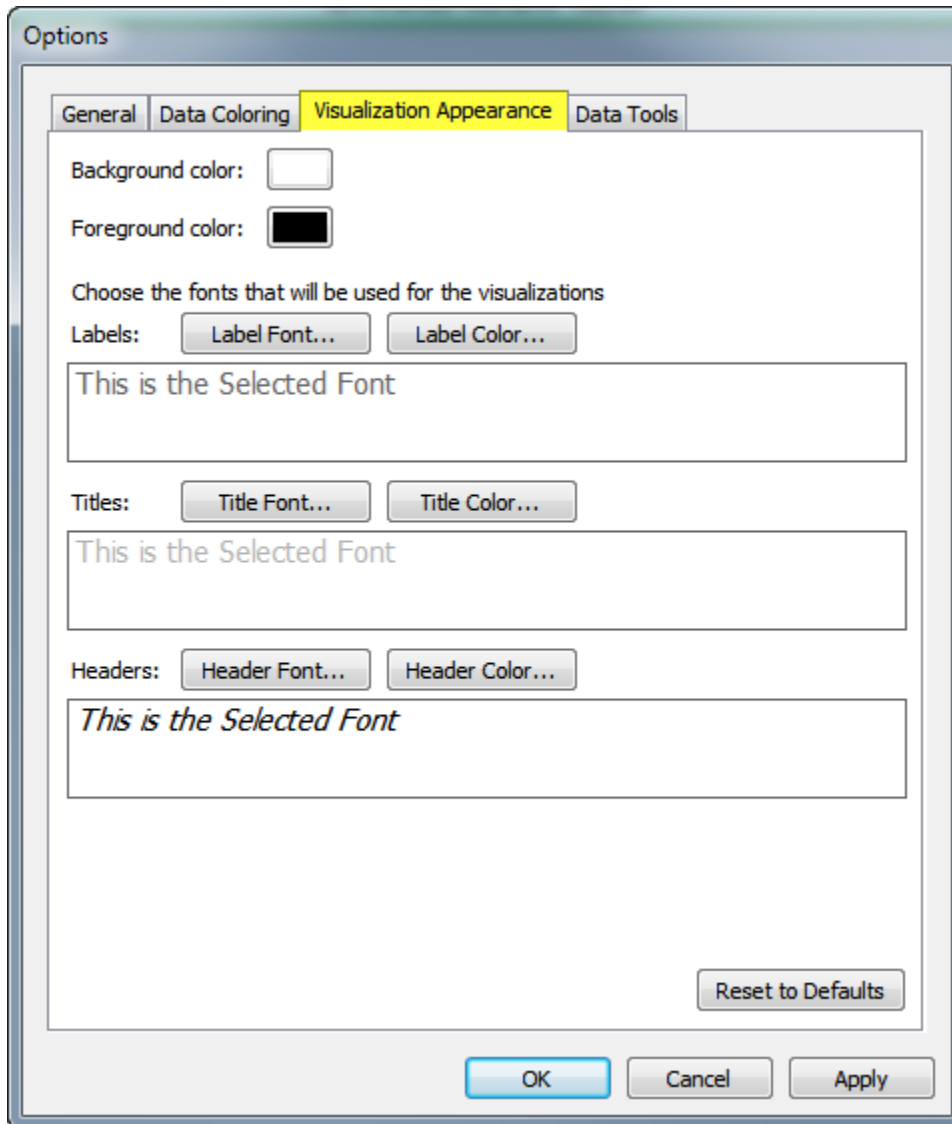
When a visualization uses the Source Port field, the visualization will use these colors instead of the default selected or unselected colors:



This technique of data coloring makes it easy to spot values of interest. In this case, it is easy to see that there is not as much byte activity in the yellow and red ports as the lighter blues.

3.7.3 Visualization Appearance

View and edit VIAssist's Visualization Appearance options by accessing the Visualization Appearance tab of the options screen:

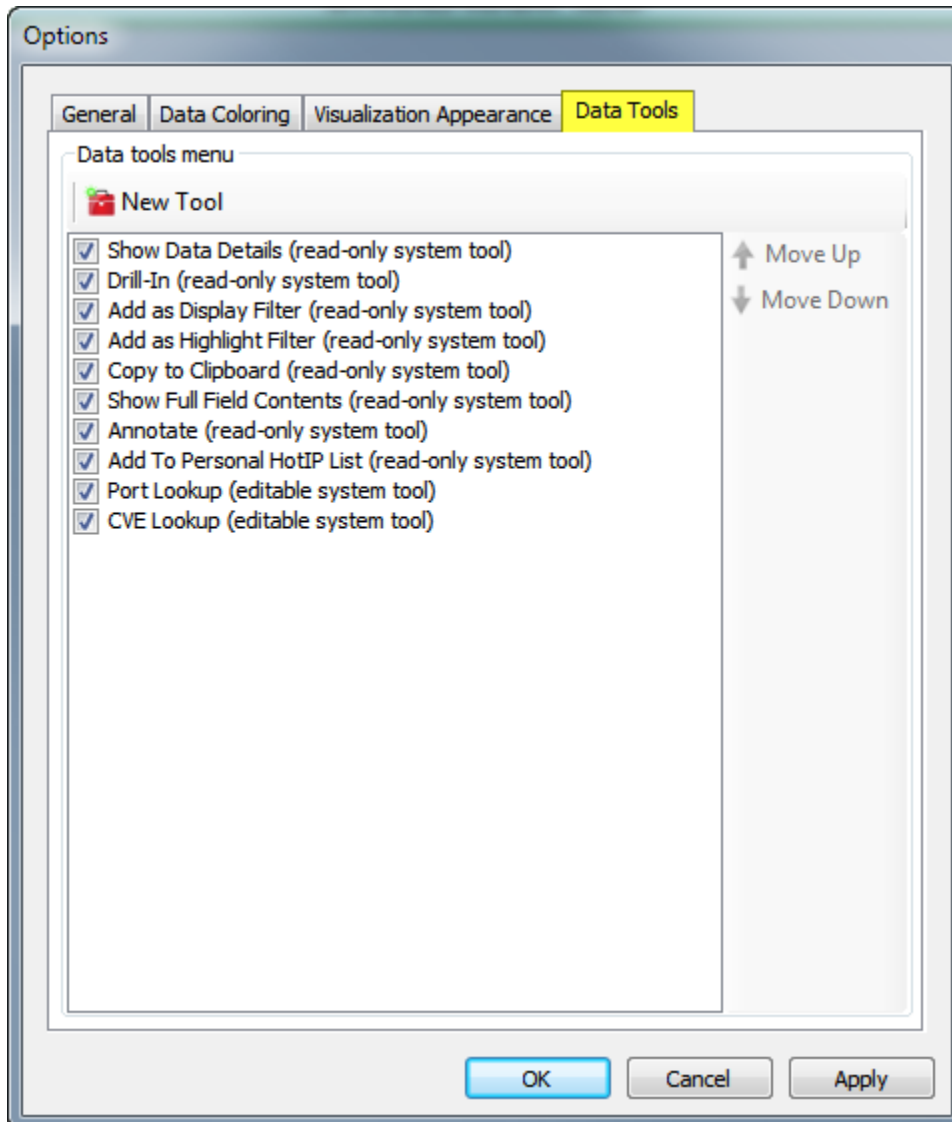


The Visualization Appearance options controls the basic appearance of visualizations, but not the appearance of data elements. The background and foreground colors of the visualization canvas can be specified, as well as the fonts used for labels, titles, and headers. Previews of colors and fonts are shown for each.

To learn how to set the appearance of data elements, [please see the "Data Coloring" section](#) .

3.7.4 Data Tools

View and edit VIAssist's Data Tools options by accessing the Data Tools tab of the options screen:



The Data Tools configuration determines which data tools are available and which order they appear. Data tools are normally available through the right-click context menu of visualizations.

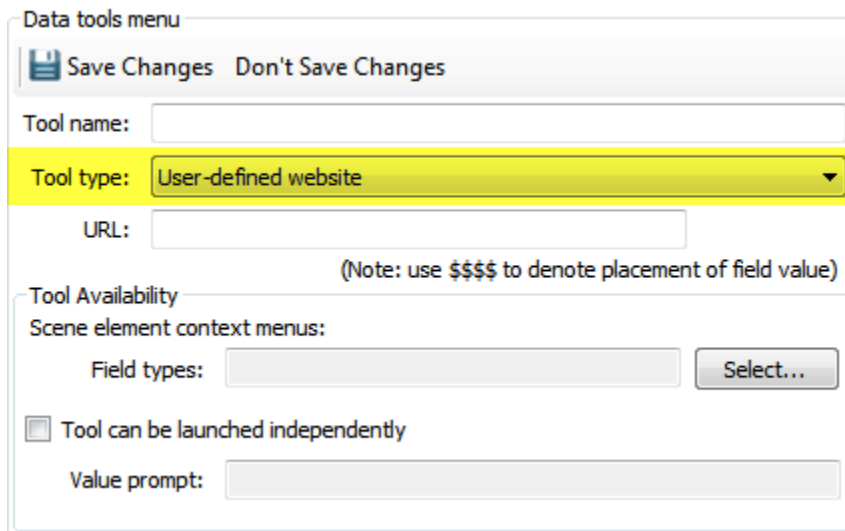
To enable or disable data tools, simply check or uncheck the checkbox next to the data tools.

To change the order the data tools appear, select individual data tools and press the Move Up or Move Down button to change its position in the list.


Some data tools can be edited, although most default tools are not editable. However, new data tools can be added and edited at any time.

VIAssist supports two types of user created data tools: web based and executable. Each is configured very similarly, with the main difference being how to specify the tool location and the field query parameter.

The tool type drop down box controls which type of data tool will be created and the options present on the data tool creation form:



Data tools menu

 Save Changes Don't Save Changes

Tool name:

Tool type: **User-defined website** ▼

URL:

(Note: use \$\$\$\$ to denote placement of field value)

Tool Availability

Scene element context menus:

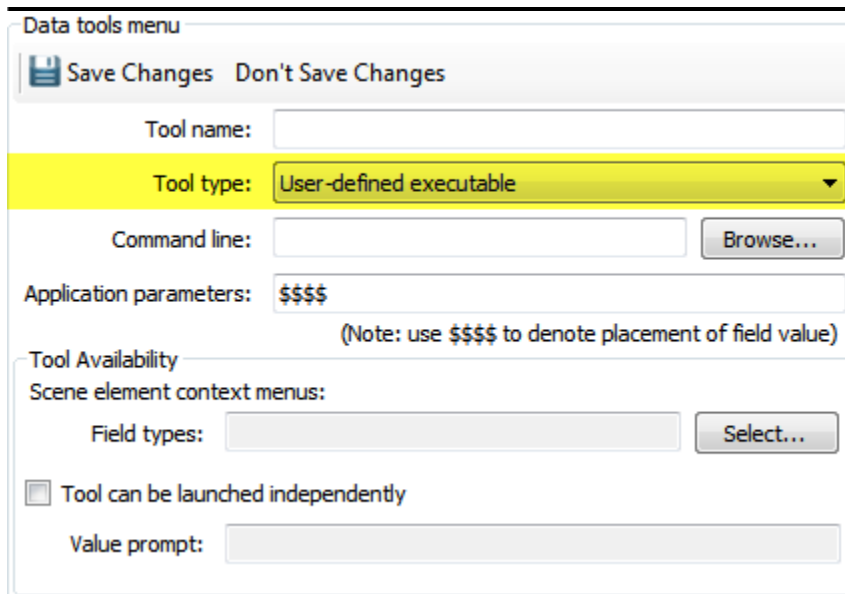
Field types:

☐ Tool can be launched independently

Value prompt:

Notice for a tool type of User-defined website that a URL field is present, which indicate the URL that VIAssist will use for the data tool. The URL needs to accept a parameter, which will be indicated by \$\$\$\$.

A tool type of User-defined executable changes the form:

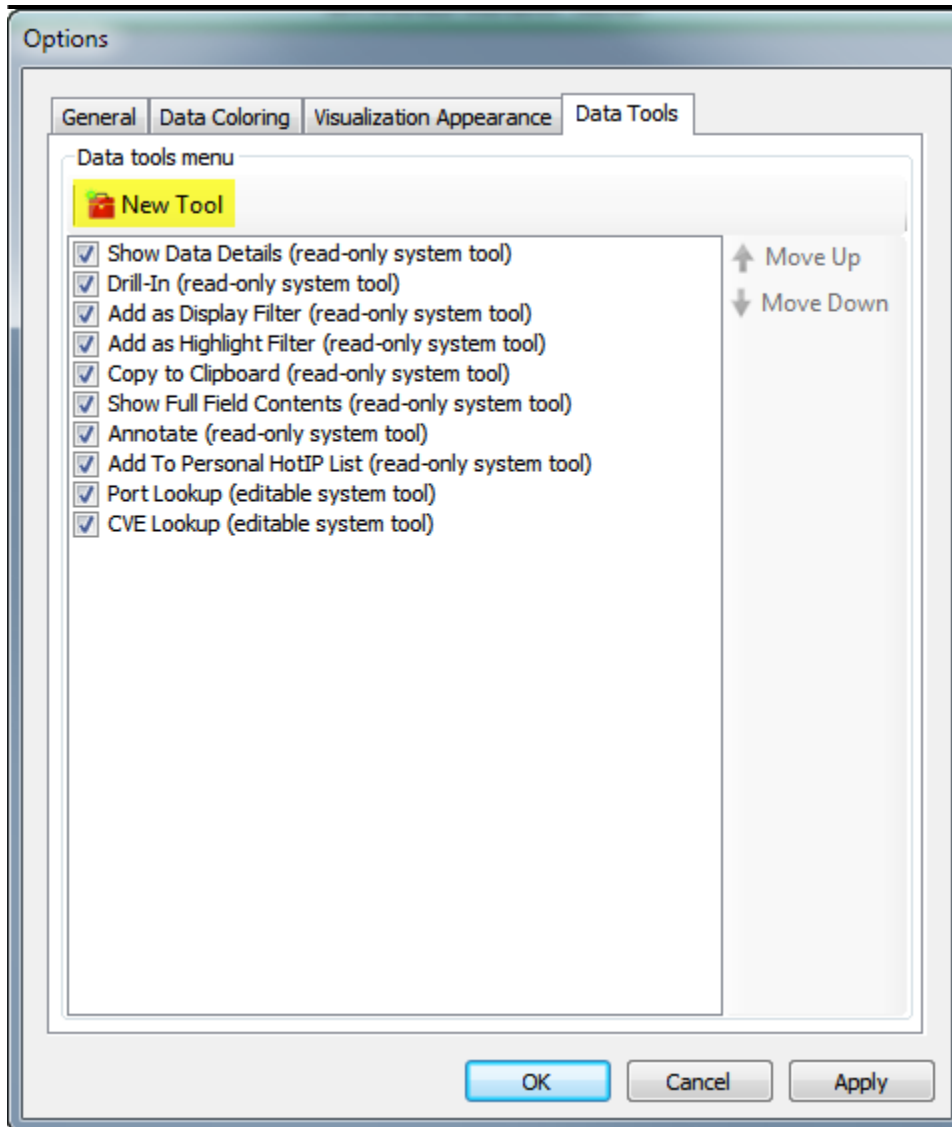
A screenshot of a web form titled "Data tools menu". At the top, there are two buttons: "Save Changes" (with a floppy disk icon) and "Don't Save Changes". Below these are several input fields: "Tool name:" followed by a text box; "Tool type:" followed by a dropdown menu currently showing "User-defined executable"; "Command line:" followed by a text box and a "Browse..." button; "Application parameters:" followed by a text box containing "\$\$\$\$" and a note "(Note: use \$\$\$\$ to denote placement of field value)"; "Tool Availability" section with "Scene element context menus:" followed by "Field types:" and a text box, and a "Select..." button; a checkbox labeled "Tool can be launched independently"; and a "Value prompt:" followed by a text box.

Instead of a URL, a command line path is needed. Browse to the location of the executable that will be used. Also notice that a new application parameters field is present. Enter the application parameters in this box, using \$\$\$\$ to represent where the field value belongs. Often, the default application parameter will suffice.

3.7.4.1 Example: Adding a Google Data Tool


As an example, a simple Google data tool will be created. This data tool will simply issue a search term to Google and display the results in a browser. All field types will be applicable.

To create a new data tool, press the New Tool button:



Ensure that a User-defined website tool type is selected:

Data tools menu

 Save Changes Don't Save Changes

Tool name:

Tool type: **User-defined website** ▼

URL:

(Note: use \$\$\$\$ to denote placement of field value)

Tool Availability

Scene element context menus:

Field types:

☐ Tool can be launched independently

Value prompt:

Google's basic URL searching is specified by the URL <http://www.google.com/search?q=> with a value following the equals sign. The value will be populated by a field value from VIAssist and is indicated by \$\$\$\$:

Tool name:

Tool type: **User-defined website** ▼

URL:

(Note: use \$\$\$\$ to denote placement of field value)

Data tool are only applicable to certain fields, so a data tool must be told which fields it applies to in order for it to work. Because this tool is simply searching Google which can accept any input that can be represented as a string, all fields are selected as applicable to this data tool:

Tool Availability

Scene element context menus:

Field types:

☐ Tool can be launched independently

Value prompt:

All of the information for the Google data tool is now populated. Save the new Google data tool to be able to use it within VIAssist:

Options

General Data Coloring Visualization Appearance Data Tools

Data tools menu

Save Changes Don't Save Changes

Tool name: Google

Tool type: User-defined website

URL: [http://www.google.com/search?q=\\$\\$\\$\\$](http://www.google.com/search?q=$$$$)

(Note: use \$\$\$\$ to denote placement of field value)

Tool Availability

Scene element context menus:

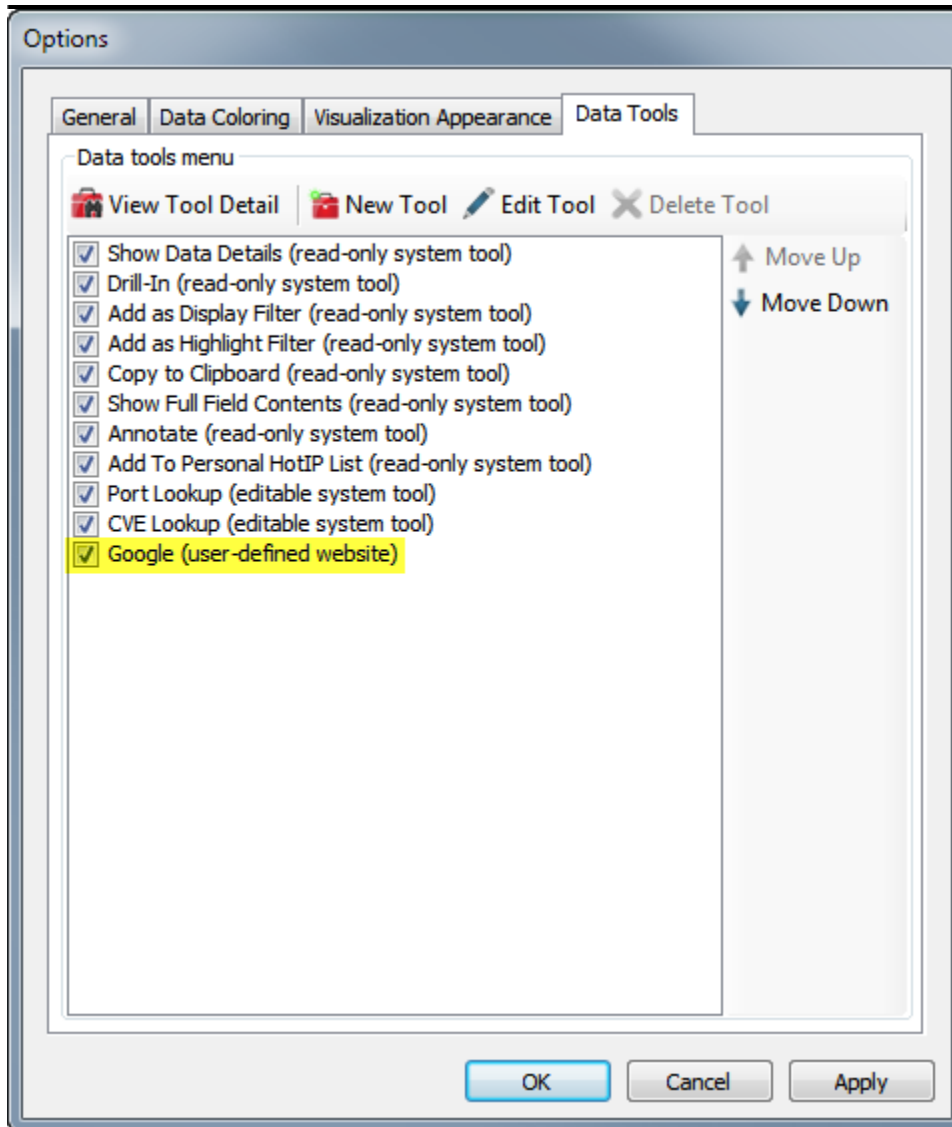
Field types: Text, Integer, Unsigned Integer, Date, Time, I **Select...**

☐ Tool can be launched independently

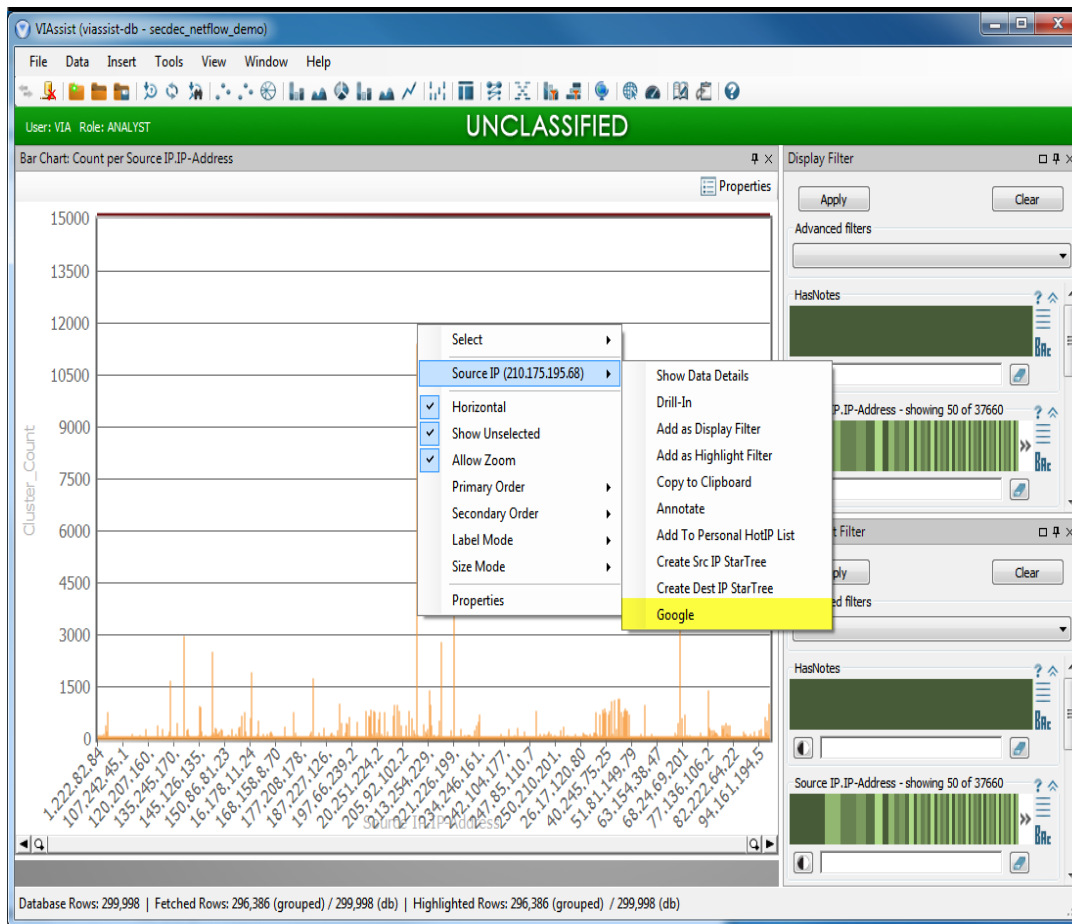
Value prompt:

OK Cancel Apply

The Google data tool is now present in the list of data tools under the Data Tools options screen:



The Google data tool is now present from any supported visualization data element:



which will open a Browser to display the result of the Google data tool query:

