UNCLASSIFIED

Federal Bureau of Investigation

FANTOM Reference Guide

Framework for the Analysis & Navigation of Transient Object Maps

To install FBI FANTOM on UNet, double-click the BigFix icon in the taskbar tray and accept the installation offer. FANTOM and the documentation is added to the Start menu.

3/10/16
FBI FANTOM Version 3.1.3

UNCLASSIFIED

For information, training, feedback or support, contact [redacted] at: [redacted]

Federal Bureau of Investigation

Notices

Document Release Date: March 2016.

Document Change History

Version	Date	Chapters	Reason for Change
4.8	01/31/13	All	Update to match new User's Guide template and FANTOM 3.0 changes
4.9	03/04/2013	Ch 9, 11; Ap B	Change Link to Edge
5.0	04/25/2013	All	Update to match FANTOM 3.0.5 software
5.1	08/08/13	All	Update to match FANTOM 3.0.6 software
5.2	11/14/13	All	Update to match FANTOM 3.0.7 software
5.3	02/10/14	All	Update to match FANTOM 3.0.8 software
5.4	04/23/14	All	Update to match FANTOM 3.0.9 software
5.5	11/10/14	All	Update to match FANTOM 3.1 software
5.6	12/10/14	Chapter 10	Update to match FANTOM 3.1 software
5.7	03/23/15	All	Update to match FANTOM 3.1.1 software
5.8	06/02/15	Chapter 12	Update CSV Importer to add new edge attributes
5.9	09/09/15	All	Update to match FANTOM 3.1.2 software
6.0	12/21/15	All	Update to match FANTOM 3.1.3 software

FBI FANTOM Version 3.1.3
FANTOM User's Guide and Quick Reference Cards (QRCs) Version 6.0 - March 10, 2016

Getting Started

(U) Welcome to FANTOM! This guide offers task-oriented instructions to help you quickly start using the FANTOM software. It focuses on time-saving features and tasks that you are likely to use while performing analysis.

(U) This chapter provides an overview of the application, explains how to obtain a FANTOM deployment kit, lists requirements, discusses how to make feature requests, describes typographical conventions used in this guide, shows you how to start and exit FANTOM, and explains how to choose a graphic user interface (GUI) look and feel.

What is FANTOM?

(U) The FANTOM application was created by the FBI to help analysts more quickly understand and exploit large and complex network data sets.

(U) FANTOM is based on the concept of *visual analytics*—that the combination of intuitive and responsive visuals, coupled with powerful analytics will allow analysts to identify interesting patterns from large amounts of data. The goal of FANTOM is to present complex information in a simple manner, allowing analysts to "shorten the time to insight" on investigations or intelligence matters that involve data sets that are too complex for most applications.

(U) The Advanced Visualization Team uses a high-end workstation to run the FANTOM software for intensive analysis work. The FBI also may be able to provide the software to approved organizations (see "Requirements.")

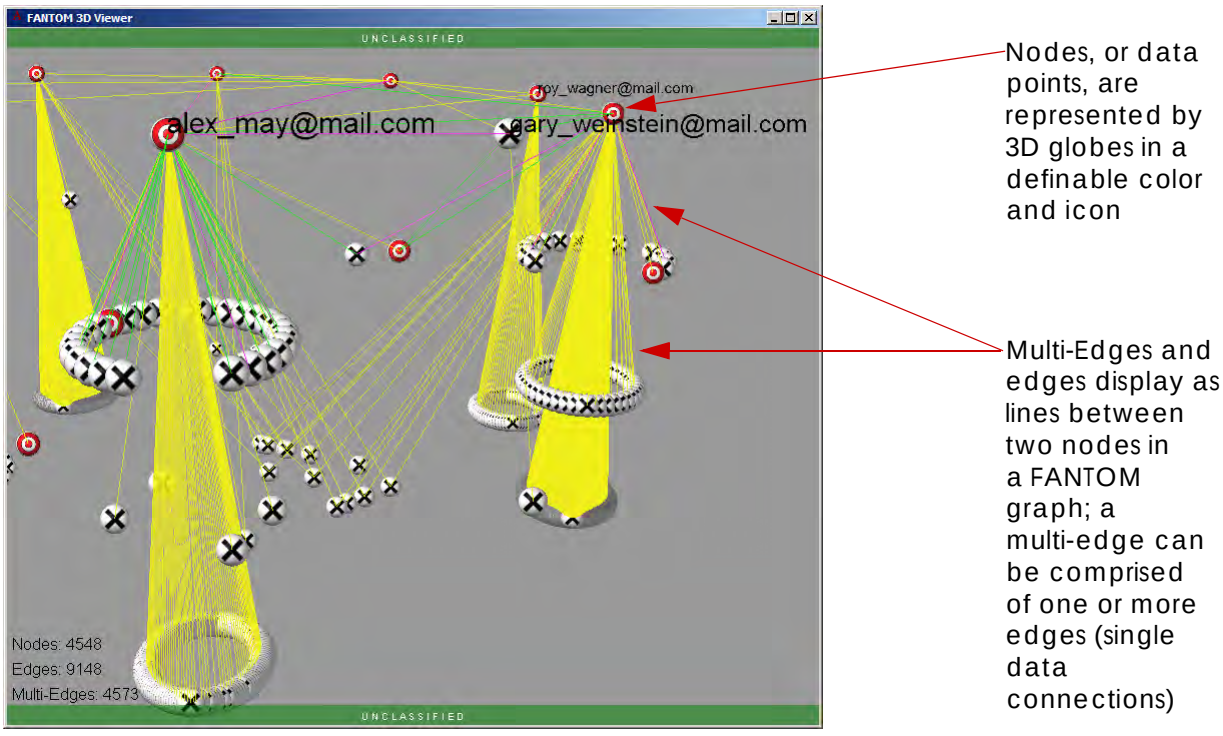
What is Visual Analysis?

(U) Visual Analysis is the science of analytical reasoning facilitated by interactive visual interfaces. It is a unique blend of human computer interaction, analytical reasoning, cognitive science, high-performance

computing, and computer graphics. It lets you expose meaningful patterns and identify hidden relationships in any structured data set.

(U) As developed and implemented by the FBI Advanced Visualization team, FANTOM encompasses a custom suite of internally developed and extensible visual analysis software. FANTOM software presents information on state-of-the-art visual displays and uses powerful algorithms to support personnel who must dissect and analyze immense amounts of information. It is targeted at analyzing relational data sets including, but not limited to financial transactions, IP traffic, communications logs or any type of data that has a point-to-point connection.

Figure 1-1: (U) FANTOM reveals patterns in data connections



Requirements

(U) You can use a workstation to run FANTOM if it meets the following minimum requirements:

- (U) For a 32-bit operating system, such as Microsoft Windows XP, we recommend 2 gigabytes (GB) random access memory (RAM)

  or:

  (U) For a 64-bit operating system, such as Microsoft Windows 7.0 or Apple Macintosh OS X v10.6 Snow Leopard, we recommend a minimum of 4 GB RAM

Note: If you want to work with the 3D Viewer window, you cannot use VMware with FANTOM 3.0.

- (U) Application usage: approximately 60 MB of hard disk storage
- (U) Java JRE 1.6.37 or later

Example of Memory Allocation

(U) The number of rows that can be ingested is determined by the amount of memory that is available to the application. As an example:

- (U) for 1 GB of memory, you can ingest about 100,000 rows of data;
- (U) for 32 GB of memory, you can ingest about 10 million rows of data.

Feature Requests and Scalability

(U) FANTOM is a system that evolves based on user needs. It was created internally by the FBI, so it better addresses investigative user needs and concerns. The Advanced Visualization team encourages you to provide feedback regarding new features or functions that you believe would make FANTOM a more helpful and potent application.

(U) Send feedback to the Advanced Visualization team through your established contacts.

Typographical Conventions

(U) This guide uses the following typographical conventions:

- (U) GUI objects that you manipulate, such as options in dialog boxes, commands on menus, and buttons are shown in bold. Examples: **File** > **Import** command, **Node Icon Size** text box, or **Save** button.
- (U) Submenus and commands are separated from the menus where they reside using greater than symbols (>). Examples: **File** > **Import**.
- (U) Characters you type are shown in the `Courier New` font.
- (U) Keyboard keys that you press are highlighted using SMALL CAPS. Multiple keys that you press at the same time are indicated with a plus sign (+) that you do not press. Examples: SHIFT+drag to draw a selection rectangle around nodes to select or ALT+drag to move the selected nodes.
- (U) Placeholders are shown in *italics* surrounded with less than and greater than symbols. Examples: <*user name*> and <*password*>.

Starting FANTOM

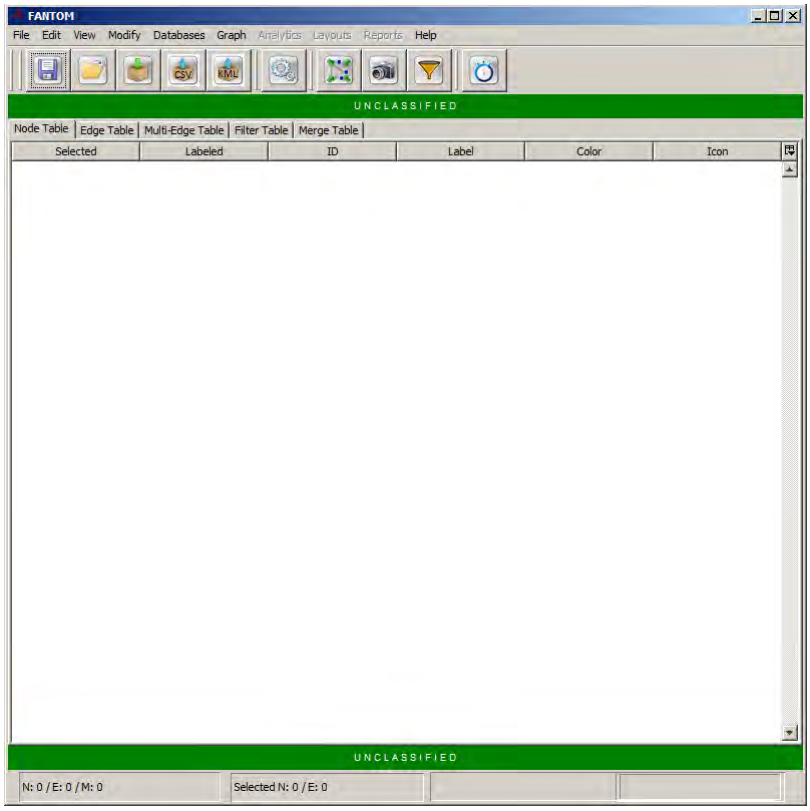
(U) To start FANTOM:

1. (U) Click the **FANTOM.bat** file in the folder where the application has been installed.

Figure 1-2: (U) FANTOM.bat icon

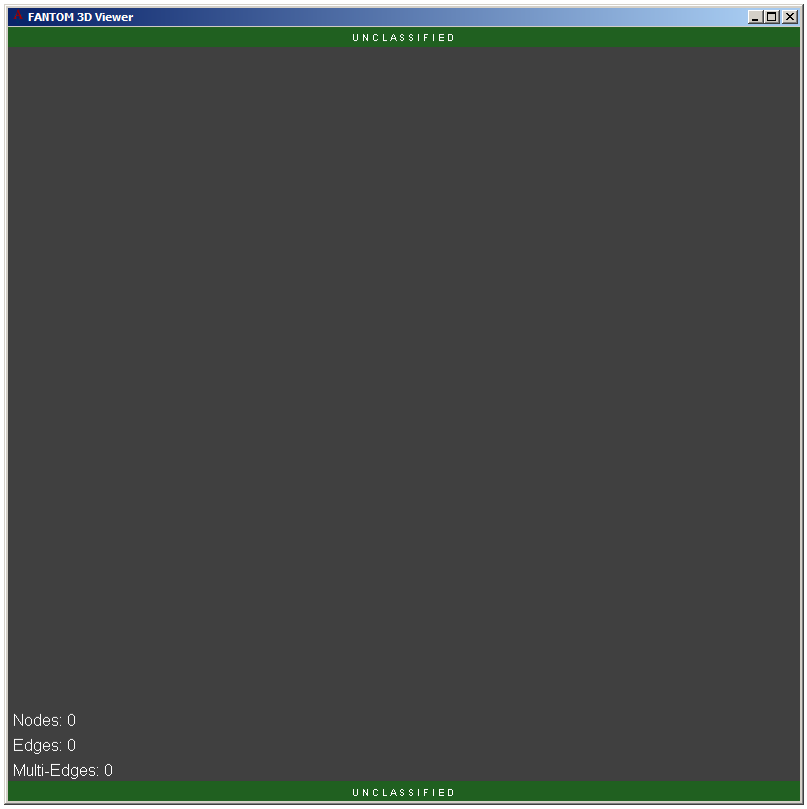
(U) The FANTOM Controller window displays (Figure 1-3).

Figure 1-3: (U) FANTOM Controller



2. (U) Choose the **View** > **3D Viewer** command to open the 3D Viewer window (Figure 1-4).

Figure 1-4: (U) FANTOM 3D Viewer window



Getting Help

(U) FANTOM offers a Help menu with the following commands:

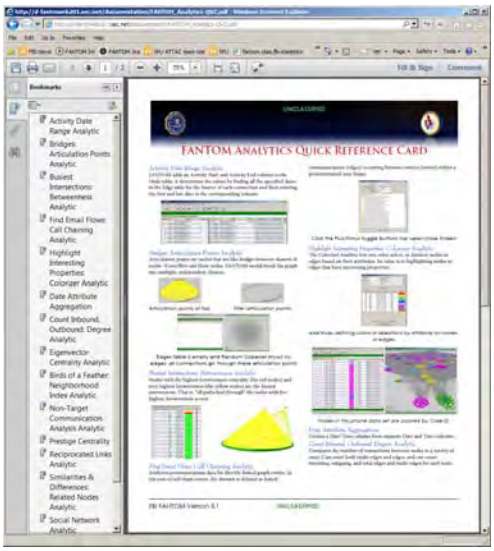
- (U) Analytics – The *FANTOM Layouts Quick Reference Card* PDF file displays. This document is also provided after the end of this user's guide (see FANTOM Analytics Quick Reference Card).
- (U) Contact Info – The FANTOM Contact information displays.
- (U) Hot Keys – The *FANTOM Quick Reference Card* displays. This document is also provided after the end of this user's guide (FANTOM Hot Keys Quick Reference Card).
- (U) Layouts – The *FANTOM Analytics Quick Reference Card* PDF file displays. This document is also provided after the end of this user's guide (see FANTOM Layouts Quick Reference Card).
- (U) Release Notes – The *FANTOM Release Notes* describe the updates in the current version of the software.
- (U) Reports – The *FANTOM Reports Quick Reference Card* PDF file displays. This document is also provided after the end of this user's guide (see FANTOM Reports Quick Reference Card).

- (U) About – The FANTOM User's Guide displays.
- (U) About – The About dialog box displays, showing you all services with the version and description.

Analytics

(U) To go to the Analytics Quick Reference Card PDF, choose **Help** > **Analytics**.

Figure 1-5: (U) Analytics Quick Reference Card (PDF file)



Contact Info

(U) To view the contact information, choose **Help** > **Contact Info**.

Figure 1-6: Contact Information

Hot Keys

(U) To go to the FANTOM Hot Keys page, choose **Help** > **Hot Keys**.

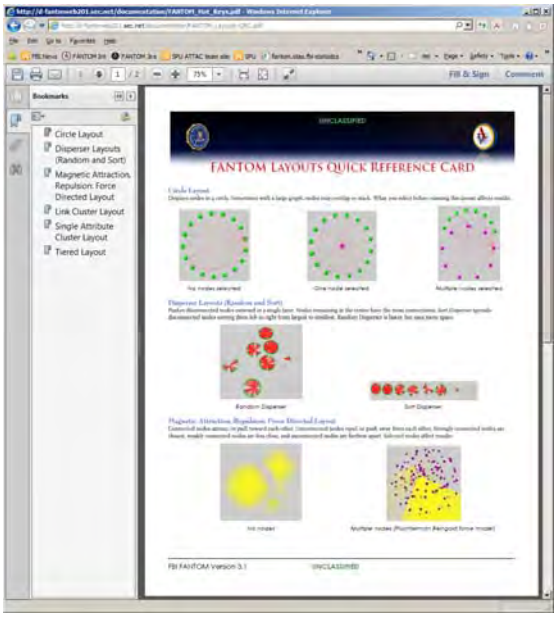
(U) The FANTOM Hot Keys page displays.

Figure 1-7: (U) FANTOM Hot Keys

Layouts

(U) To go to the Layouts Quick Reference Card PDF, choose **Help** > **Layouts**.

Figure 1-8: (U) Layout Quick Reference Card (PDF file)

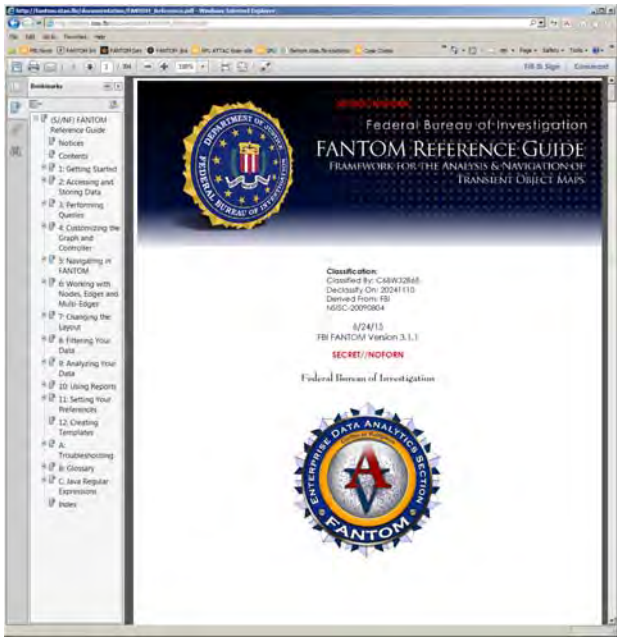


Reference

(U) To go to the *FANTOM Reference Guide*, choose **Help** > **Reference**.

(U) The guide displays in an Adobe Acrobat Reader or Preview window (Figure 1-9).

Figure 1-9: (U) FANTOM Reference Guide example

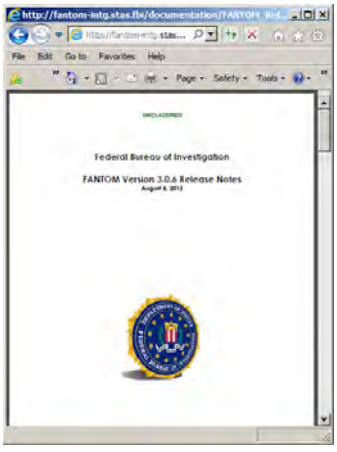


Release Notes

(U) To go to the FANTOM Release Notes, choose **Help** > **Release Notes**.

(U) The notes display in an Adobe Acrobat Reader or Preview window (Figure 1-10).

Figure 1-10: (U) FANTOM Release Notes

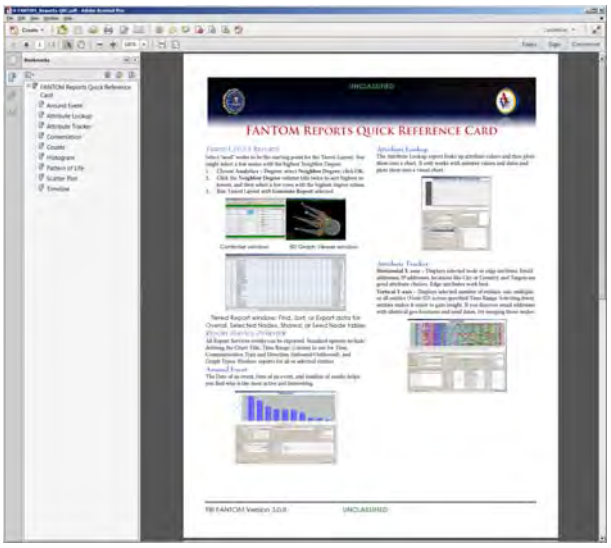


Reports

(U) To go to the *FANTOM Reports Quick Reference Card*, choose **Help** > **Reports**.

(U) The card displays in an Adobe Acrobat Reader or Preview window.

Figure 1-11: (U) FANTOM Reports Quick Reference Card example



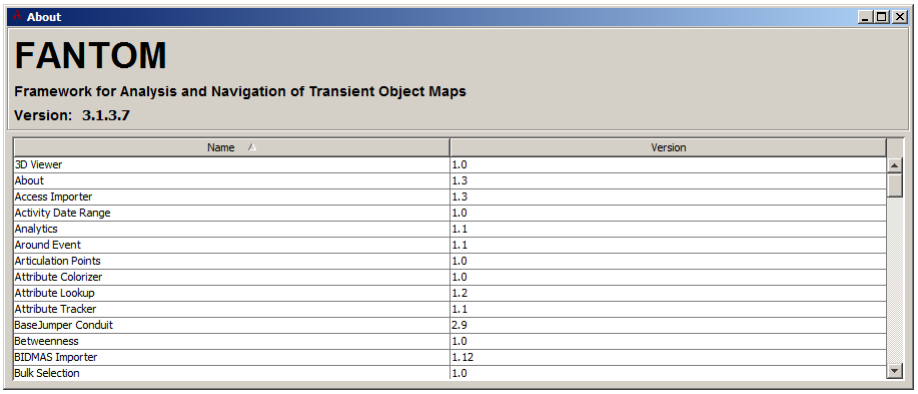
About

(U) FANTOM provides version numbers for not only the application itself, but also for the individual services available to you within FANTOM.

(U) To go to the About FANTOM message box, choose **Help** > **About**.

(U) The About FANTOM message box displays.

Figure 1-12: (U) About FANTOM



Exiting FANTOM

(U) In FANTOM, your data is temporarily stored in random access memory (RAM). You should save FANTOM work sessions so you can return to the data later (see "Saving a FANTOM Session.") You can also export FANTOM data to a CSV (comma separated value) file that can be opened with many applications, such as Microsoft Excel (see "Exporting FANTOM Data to a Delimited File.")

(U) To exit FANTOM, choose **File** > **Exit**.

Accessing and Storing Data

(U) This chapter explains:

Note: (U) FANTOM 2.8.1 and later requires you to specify classification information when you import data. FANTOM adds this

classification as the first row of data if you export it later. If you do not supply a classification, you cannot continue to access the data.

Note: (U) When you import or export data, FANTOM initially opens the `C:\Users\<username>` directory; after you browse to a different location and open or save a file, FANTOM remembers this location and returns you to it the next time you import or export data.

Importing Data into FANTOM

(U) You can import data into FANTOM in the following ways:

- (U) **Microsoft Access Database** – Import Microsoft Access database files in the .accdb and .mdb file formats.
- (U) **Delimited File** – The Delimited File import command is a powerful feature. A *delimited file* is a text file where each line represents an edge of the graph (possibly including attributes of the edge and the nodes). FANTOM recognizes delimited files in one of the following text-based file formats:
  - (U) **CSV (comma separated value)** – A standard format for table data that you might create using word processors, spreadsheets, or database export capabilities. Microsoft Excel can save files as .csv, which is a delimited file, so you can think of a delimited file as an Excel spreadsheet saved as .csv.
  - (U) **DSV (delimiter separated value)** – A file format that uses separator characters such as commas, tabs, or colons.
  - (U) **LOG** – IIS log files and other Internet traffic logs with comma delimited data may use a .log file extension. FANTOM recognizes these .log files when you drag and drop them into a FANTOM window.
  - (U) **TXT (text)** – Plain text file.

  (U) Each line in a delimited file is divided into fields by a delimiter character (usually a comma). The fields represent nodes and attributes. Usually we think of the fields as "columns" since every line will have the same number of fields.

  (U) **BIDMAS** (**.csv**, **.dat**) – The Bureau Investigative Document Management and Analysis System (BIDMAS) is a database application accessible on UNet where FBI investigators can review and share information with other partners (DOJ, SEC, and FDIC) and Law Enforcement entities. After you export data from BIDMAS in either .dat or .csv format, you can import that data file into FANTOM without needing to define import settings.

- (U) **Microsoft Excel (.xls, .xlsx)** – Microsoft Excel Spreadsheet file.
- (U) **GraphML** – The GraphML import command lets you import graphs saved in GraphML (Graph Markup Language) exchange file format. You can also use it to import .XML files.
- **(**U) **IVML** – This format was added because a FANTOM customer needed it. For more information about IVML files, you can go to the following public Internet link:

  `http://citeseerx.ist.psu.edu/viewdoc/summmary?doi=10.1.1.84.5400`

- (U) **Legacy Session** – The Legacy Session import command lets you import .fsaz sessions saved with FANTOM 2.8.5 or earlier.
- (U) **PCAP** (Packet Capture Data) – PCAP files (.pca, .pcap, and .pcp files) are created by network analyzer software, such as Wireshark.
- (U) **Research** (**.xls**, .xlsx) – The Research import file type lets you import Open Research-exported Excel files (XLS or XLSX) into FANTOM. It lets you import these files without needing to define import settings.
- (U) **Session** – FANTOM 3.0 and later saves session files with the file extension of .session.

Import Tips

- (U) You can drag and drop multiple files of the same type onto the FANTOM Controller or 3D Viewer window to begin the Import process.
- (U) If you perform multiple imports with the same column titles, the last value imported will display if the values are different. If you want both columns, rename one of the column titles so they are unique.
- (U) Nodes (Source and Destination) are case sensitive.
- (U) You can edit a template, but the columns must stay in the same position. If you want to rearrange columns, create a new template.

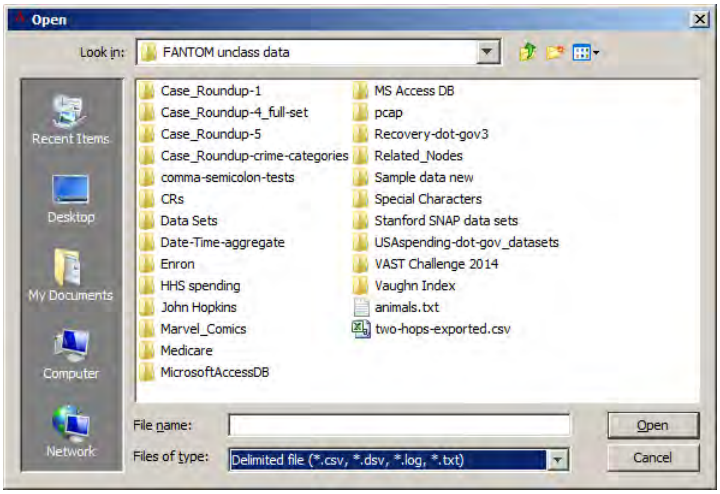
Importing Microsoft Access Databases

(U) To import Microsoft Access database data:

1. (U) Choose **File** > **File Importer** or click the **Import** tool button ( ).

   (U) A standard Open dialog box displays.

Figure 2-1: (U) Import dialog box



2. (U) Choose **Microsoft Access Database** from the **Files of type** menu.

   (U) FANTOM hides all files except those of the file type you selected.

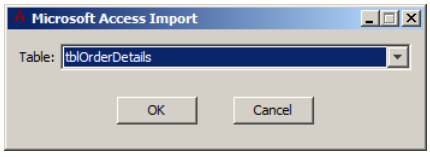
3. (U) Select a file and click the **Open** button.

Tip: (U) You can press SHIFT+CLICK to select a contiguous range of files, or CTRL+CLICK (Windows) or COMMAND+CLICK (Macintosh) to select multiple noncontiguous (or unadjacent) files.

(U) FANTOM opens the database in the background.

(U) The Microsoft Access Import dialog box displays, listing the available tables.

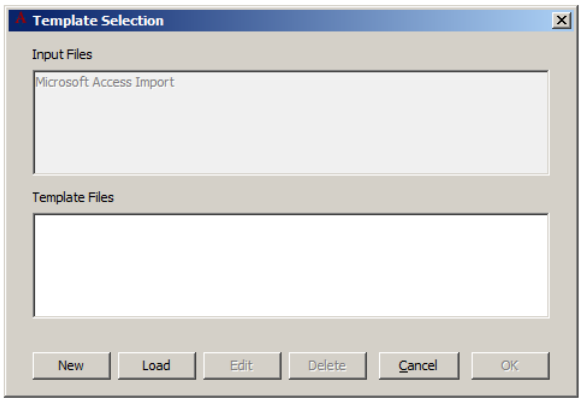
Figure 2-2: (U) Microsoft Access Import dialog box



4. (U) Select a table from the menu and click **OK**.

   (U) The Template Selection dialog box displays (Figure 2-3).

Figure 2-3: (U) Template Selection dialog box



5. (U) Do one of the following:

   - (U) Click the **New** button if there is not yet a template for the database you are importing.

     (U) FANTOM displays a Save dialog box where you can provide a filename for the new template and then define template settings. See Chapter 12, "Creating Import Templates."

   - (U) Click the **Load** button if a template file exists for the file you are importing.

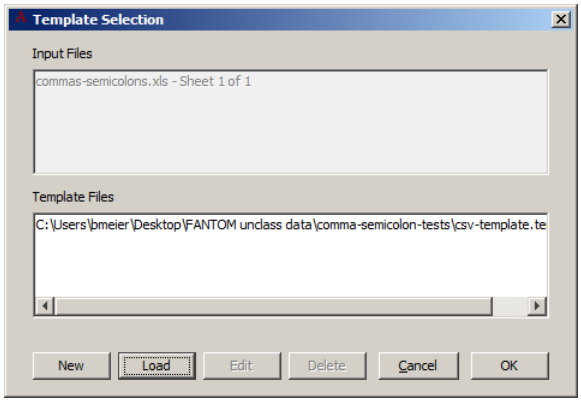
     (U) FANTOM displays an Open dialog box where you can select an existing template. After you select a template file and click **Open**, FANTOM adds the full path to the **Template Files** text box.

Note: (U) You can select the file in the **Template Files** list at the bottom of the dialog box if you need to edit or delete the selected template.

6. (U) Click **OK** in the Template Selection dialog box.

   (U) The Access Importer dialog box redisplays.

Figure 2-4: (U) Access Importer dialog box



7. (U) Click **OK**.

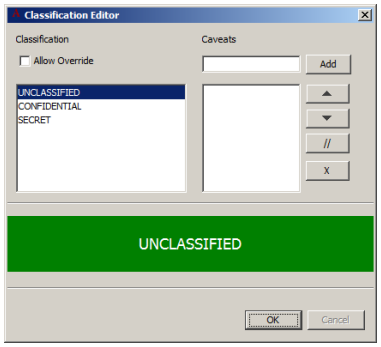
   (U) The Access Importer dialog box redisplays.

8. (U) Do one of the following:

   - (U) Click **Import More Files** to select more data files to import.
   - (U) Select a file in the **Files to import** list and click **Delete** to remove that source from your import list.
   - (U) Click **Process Access Import** to begin importing data.

   (U) FANTOM imports the data and when it's ready to display the data set, it first displays the Classification Editor dialog box.

Figure 2-5: (U) Classification Editor dialog box



   (U) You must choose a Classification level before you can continue.

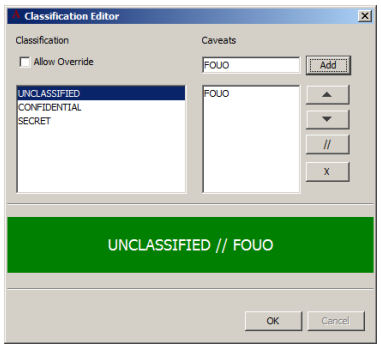
9. (U) Select Classification options and then click **OK**.

   (U) Your options include:

   - (U) **Allow Override** – Select this check box if you want to be able to change the classification from higher to lower after importing the data. For example, if the data set is currently set at Confidential (from another import), the Classification Editor dialog box disables Unclassified unless you select the Allow Override check box. You can always change from lower to higher (Unclassified to Confidential) regardless of whether this check box is selected.
   - (U) **Caveats** – Type a caveat in the **Caveat** text box and click the **Add** button.

     (U) FANTOM adds the caveat text after the classification, separated with double slash marks (//).

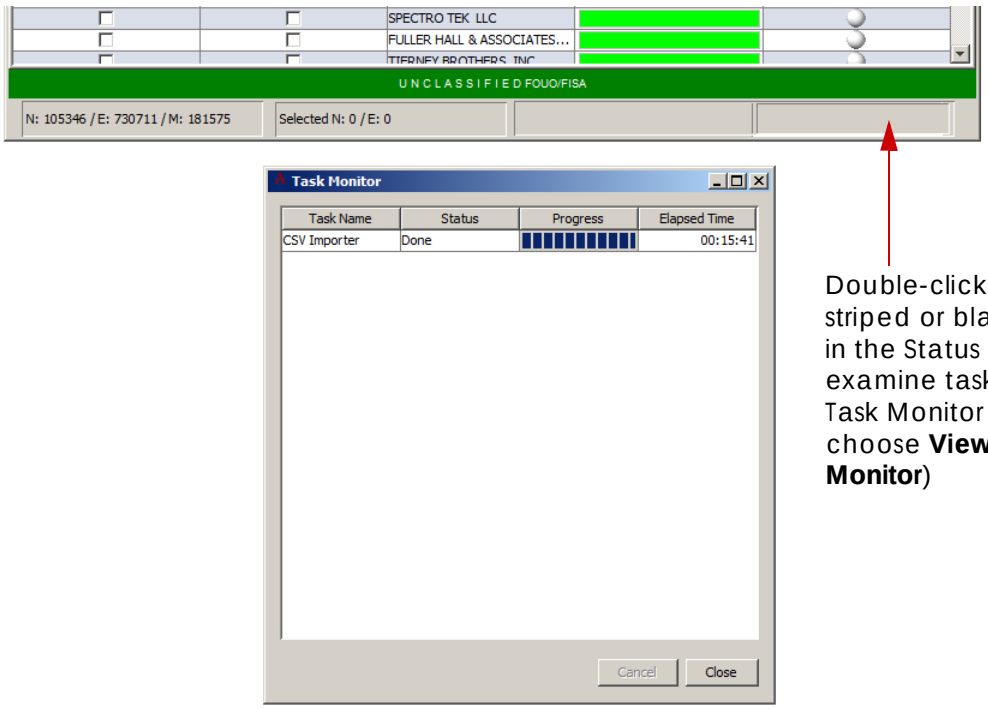
Figure 2-6: (U) FANTOM adds caveats after the classification separated by double slash marks



(U) If the file you are importing is large, a blue-striped Status bar displays at the bottom right of the Controller window while the data is imported (Figure 2-16). You can double-click the Status bar or blank tray to examine the Task Monitor dialog box. This dialog box provides you with details about the progress of tasks. FANTOM also lets you choose the **View** > **Task Monitor** command to examine the Tasks dialog box.

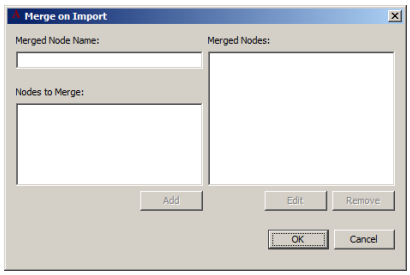
Note: (U) If FANTOM discovers duplicates, it displays an error message to let you know. See "Duplicates Error Message" on page A-6..

Figure 2-7: (U) Double-click the blue-striped or blank tray in the Status bar to examine Task information



(U) FANTOM displays the Merge on Import dialog box if the **Show Merge Dialog** option is selected in the **Edit** > **Preferences** > **General Importer** dialog box.

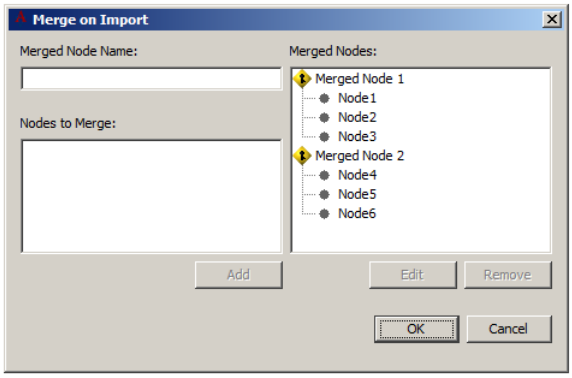
Figure 2-8: (U) Merge on Import dialog box



10. Do one of the following:

- Click **OK** or **Cancel** if you have no nodes to merge at this time.
- Specify any groups of nodes that you want to identify as merged nodes by typing a unique name in the **Merged Node Name** text box, typing or pasting the list of nodes into the **Nodes to Merge** text box and clicking the **Add** button. FANTOM adds the node to the **Merged Nodes** list. Repeat this process to add more Merged Nodes if needed. Click **OK** when you finish.

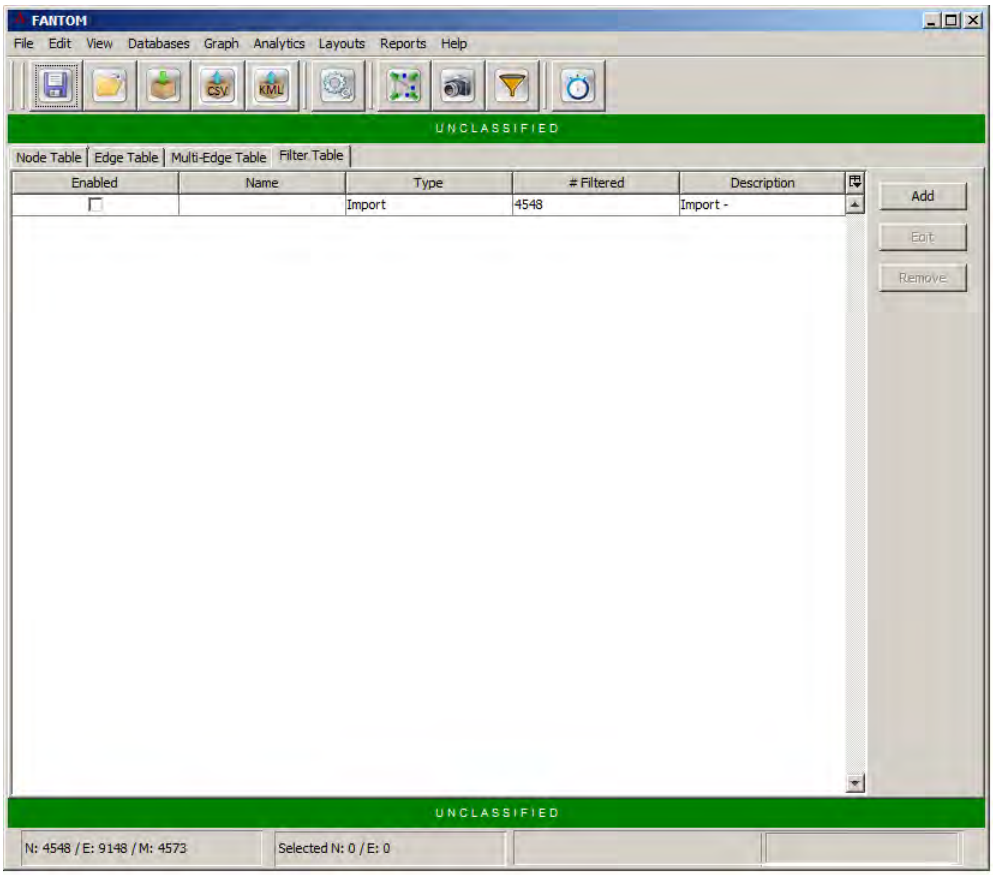
Figure 2-9: (U) Merged Nodes added



(U) The data displays in the FANTOM windows.

Note: (U) When you import data, FANTOM creates a default filter for the full data set identified by the data set's filename. The filter is initially disabled. To hide the entire data set, click the Filter tab and select the **Enabled** check box for that filter entry in the list.

Figure 2-10: (U) Default filter for imported data set



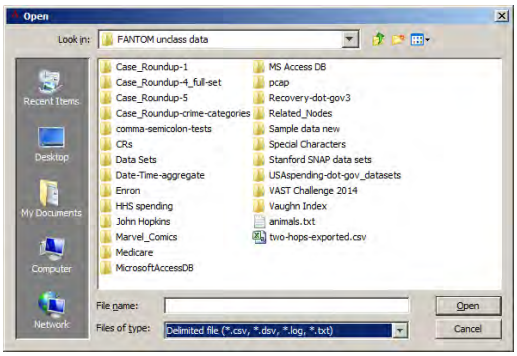
Importing Delimited Data

(U) To import delimited data:

1. (U) Choose **File** > **File Importer** or click the **Import** tool button ( ).

   (U) A standard Open dialog box displays (Figure 2-11).

   Figure 2-11: (U) Import dialog box



2. (U) Choose **Delimited file** from the **Files of type** menu.

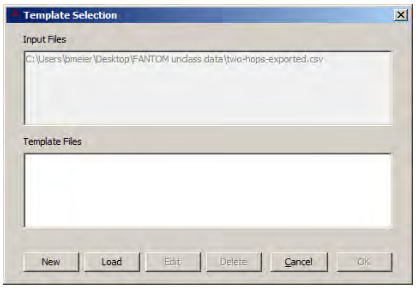
(U) FANTOM hides all files except those of the file type you selected.

3. (U) Select a file and click the **Open** button.

Tip: (U) You can press SHIFT+CLICK to select a contiguous range of files, or CTRL+CLICK (Windows) or COMMAND+CLICK (Macintosh) to select multiple noncontiguous (or unadjacent) files.

(U) The Template Selection dialog box displays (Figure 2-12).

Figure 2-12: (U) Template Selection dialog box



4. (U) Do one of the following:

- (U) Click the **New** button if there is not yet a template for the file you are importing.

  (U) FANTOM displays a Save dialog box where you can provide a filename for the new template and then define template settings. See Chapter 12, "Creating Import Templates."

- (U) Click the **Load** button if a template file exists for the file you are importing.

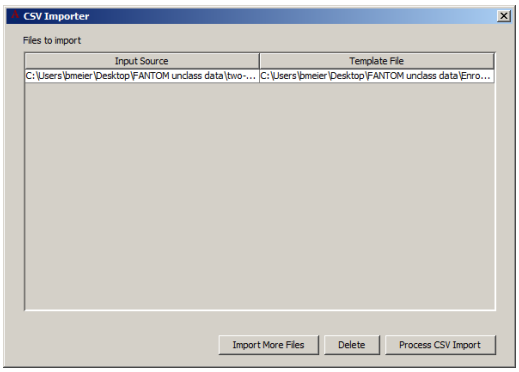
  (U) FANTOM displays an Open dialog box where you can select an existing template. After you select a template file and click **Open**, FANTOM adds the full path to the Template Files text box.

Note: (U) You can select the file in the **Template Files** list at the bottom of the dialog box if you need to edit or delete the selected template.

5. (U) Click **OK** in the Template Selection dialog box.

(U) The CSV Importer dialog box redisplays (Figure 2-13).

Figure 2-13: (U) CSV Importer

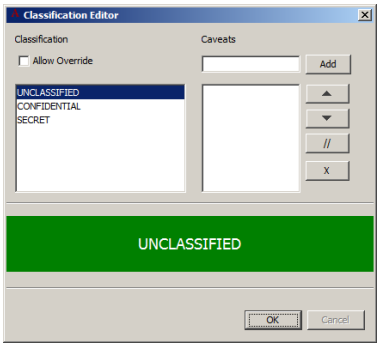


6. (U) Do one of the following:

   - (U) Click **Import More Files** to select more data files to import.
   - (U) Select a file in the **Files to import** list and click **Delete** to remove that source from your import list.
   - (U) Click **Process CSV Import** to begin importing data.

   (U) FANTOM imports the data and when it's ready to display the data set, it first displays the Classification Editor dialog box.

Figure 2-14: (U) Classification Editor dialog box



   (U) You must choose a Classification level before you can continue.

7. (U) Select Classification options and then click **OK**.

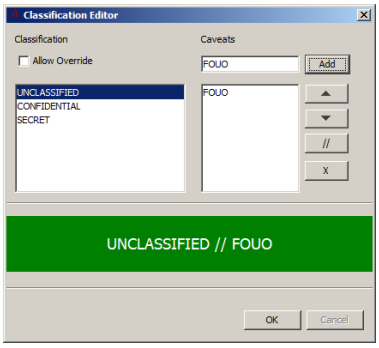
   (U) Your options include:

   - (U) **Allow Override** – Select this check box if you want to be able to change the classification from higher to lower after importing the data. For example, if the data set is currently set at Confidential (from another import), the Classification Editor dialog box disables Unclassified unless you select the Allow Override check box. You can always change from lower to higher (Unclassified to Confidential) regardless of whether this check box is selected.

- (U) **Caveats** – Type a caveat in the **Caveat** text box and click the **Add** button.

  (U) FANTOM adds the caveat text after the classification, separated with double slash marks (//).

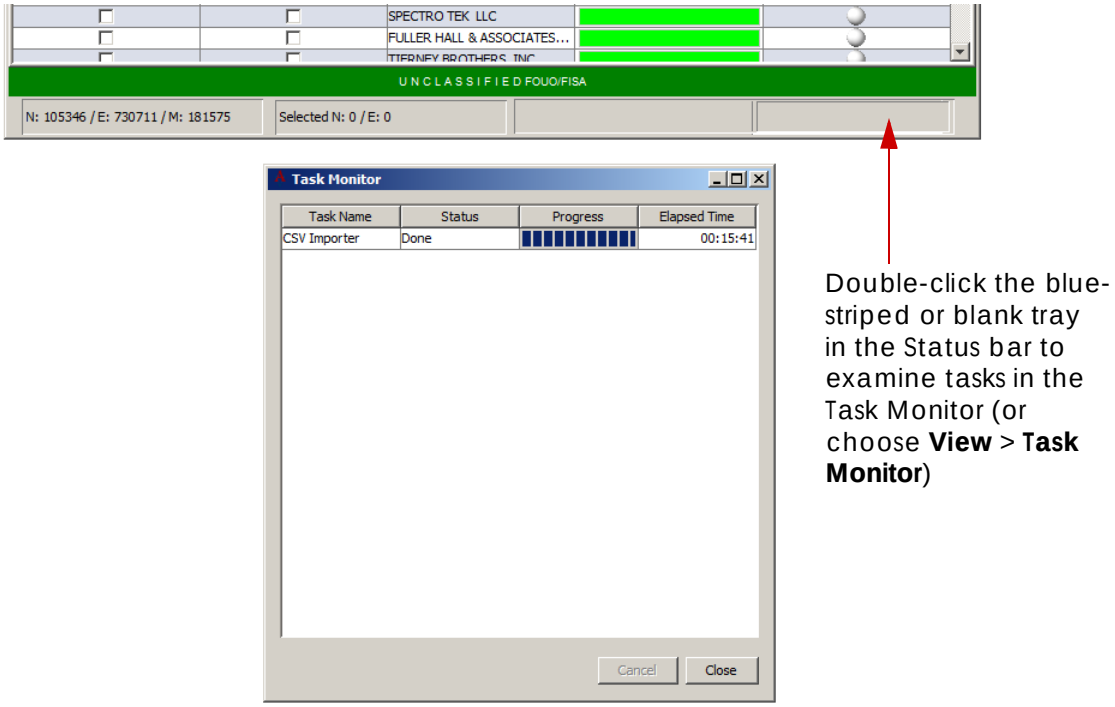
Figure 2-15: (U) FANTOM adds caveats after the classification separated by double slash marks



(U) If the file you are importing is large, a blue-striped Status bar displays at the bottom right of the Controller window while the data is imported (Figure 2-16). You can double-click the Status bar or blank tray to examine the Task Monitor dialog box. This dialog box provides you with details about the progress of tasks. FANTOM also lets you choose the **View** > **Task Monitor** command to examine the Tasks dialog box.

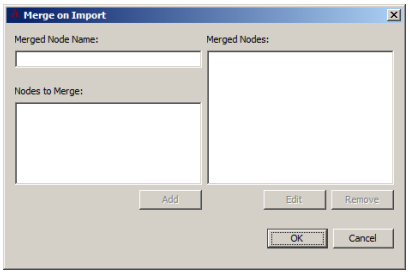
Note: (U) If FANTOM discovers duplicates, it displays an error message to let you know. See "Duplicates Error Message" on page A-6..

Figure 2-16: (U) Double-click the blue-striped or blank tray in the Status bar to examine Task information



(U) FANTOM displays the Merge on Import dialog box.

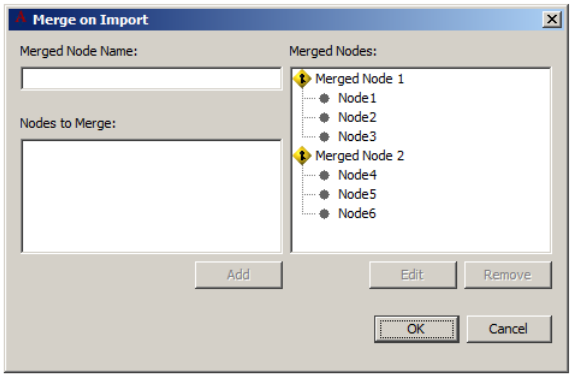
Figure 2-17: (U) Merge on Import dialog box



8. (U) Do one of the following:

   - (U) Click **OK** or **Cancel** if you have no nodes to merge at this time.
   - (U) Specify any groups of nodes that you want to identify as merged nodes by typing a unique name in the **Merged Node Name** text box, typing or pasting the list of nodes into the **Nodes to Merge** text box and clicking the **Add** button. FANTOM adds the node to the **Merged Nodes** list. Repeat this process to add more Merged Nodes if needed. Click **OK** when you finish.

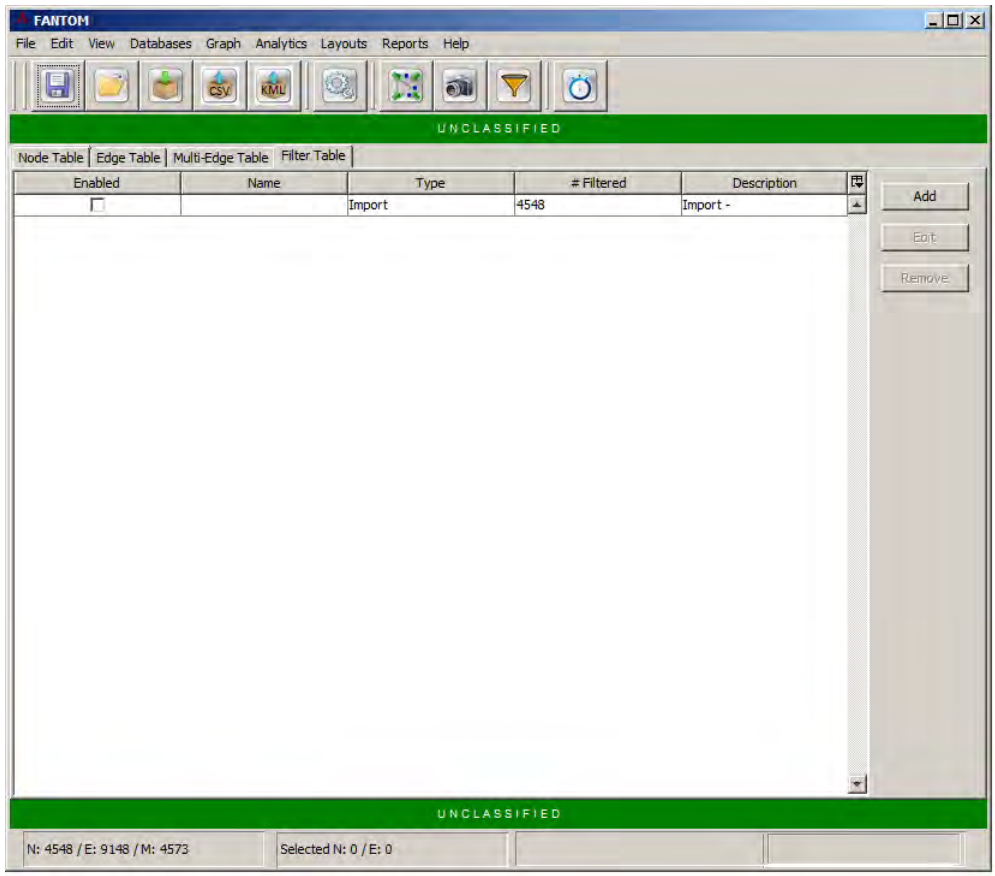
Figure 2-18: (U) Merged Nodes added



(U) The data displays in the FANTOM windows.

Note: (U) When you import data, FANTOM creates a default filter for the full data set identified by the data set's filename. The filter is initially disabled. To hide the entire data set, click the Filter tab and select the **Enabled** check box for that filter entry in the list.

Figure 2-19: (U) Default filter for imported data set



Importing Microsoft Excel Data

(U) FANTOM lets you import Excel spreadsheet files in either .xls or .xlsx format. If the file has multiple sheets, FANTOM lets you specify the Source, Destination, and columns to add for each sheet, one after another.

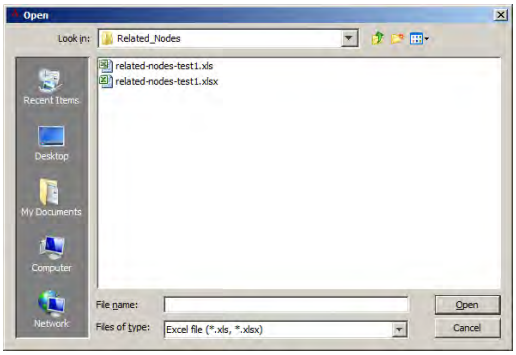
(U) FANTOM also lets you indicate that your Excel file was exported from Open Research by selecting that type of file when opening the file.

To import an Excel file:

1. (U) Choose **File** > **File Importer** or click the **Import** tool button ( ).

   (U) A standard Open dialog box displays.

Figure 2-20: (U) Import dialog box



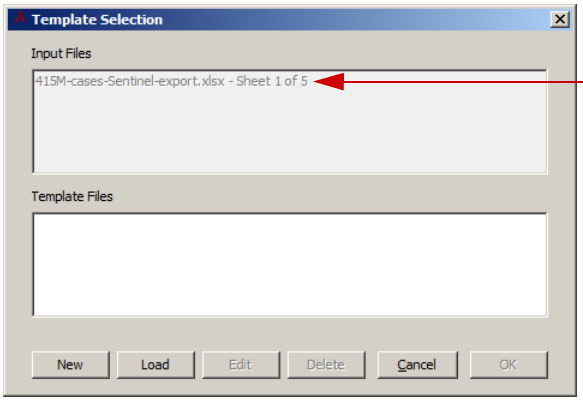
2. (U) Choose **Excel file** from the **Files of type** menu.

   (U) FANTOM hides all files except those of the file type you selected.

3. (U) Select a file and click the **Open** button.

   (U) FANTOM displays the Template Selection dialog box (Figure 2-21).

Figure 2-21: (U) Template Selection dialog box with multiple sheet Excel input file



This **Input File** status indicator shows you which of the sheets in the input file you are currently working with; the indicator increments to the next sheet number once you finish defining a new or loading an existing FANTOM template

4. (U) Do one of the following:

   - (U) Click **New** to save a new template for this spreadsheet .
   - (U) Click **Load** to use an existing template.

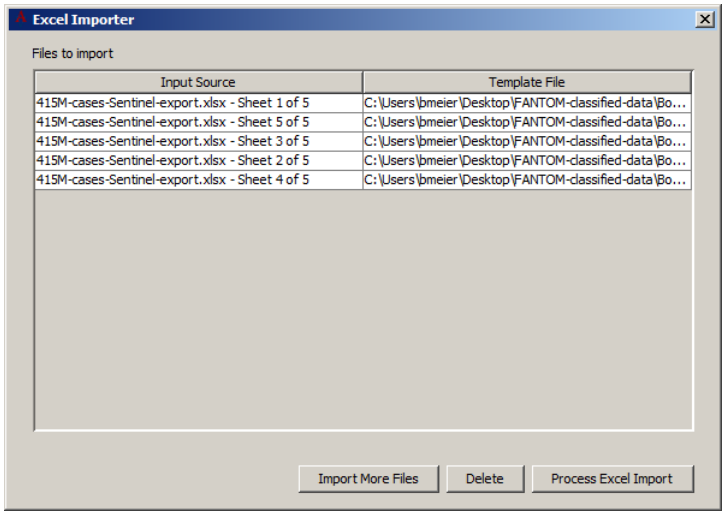
5. (U) Select the template file in the bottom Template Files section at the bottom of this dialog box.

   (U) The Input Files <***filename***> **Sheet # of #** indicator increments to the next sheet in the Excel spreadsheet so you can define the columns to use as a Source and Destination.

6. (U) Repeat step 4 and step 5 until you finish creating or loading an import template for the last sheet.

   (U) The Excel Importer dialog box displays.

Figure 2-22: (U) Excel Importer dialog box



7. (U) Click the **Process Excel Import** button.

   (U) FANTOM imports the information based on the template definitions.

   (U) It displays the Classification dialog box to let you specify the proper markings for this data set.

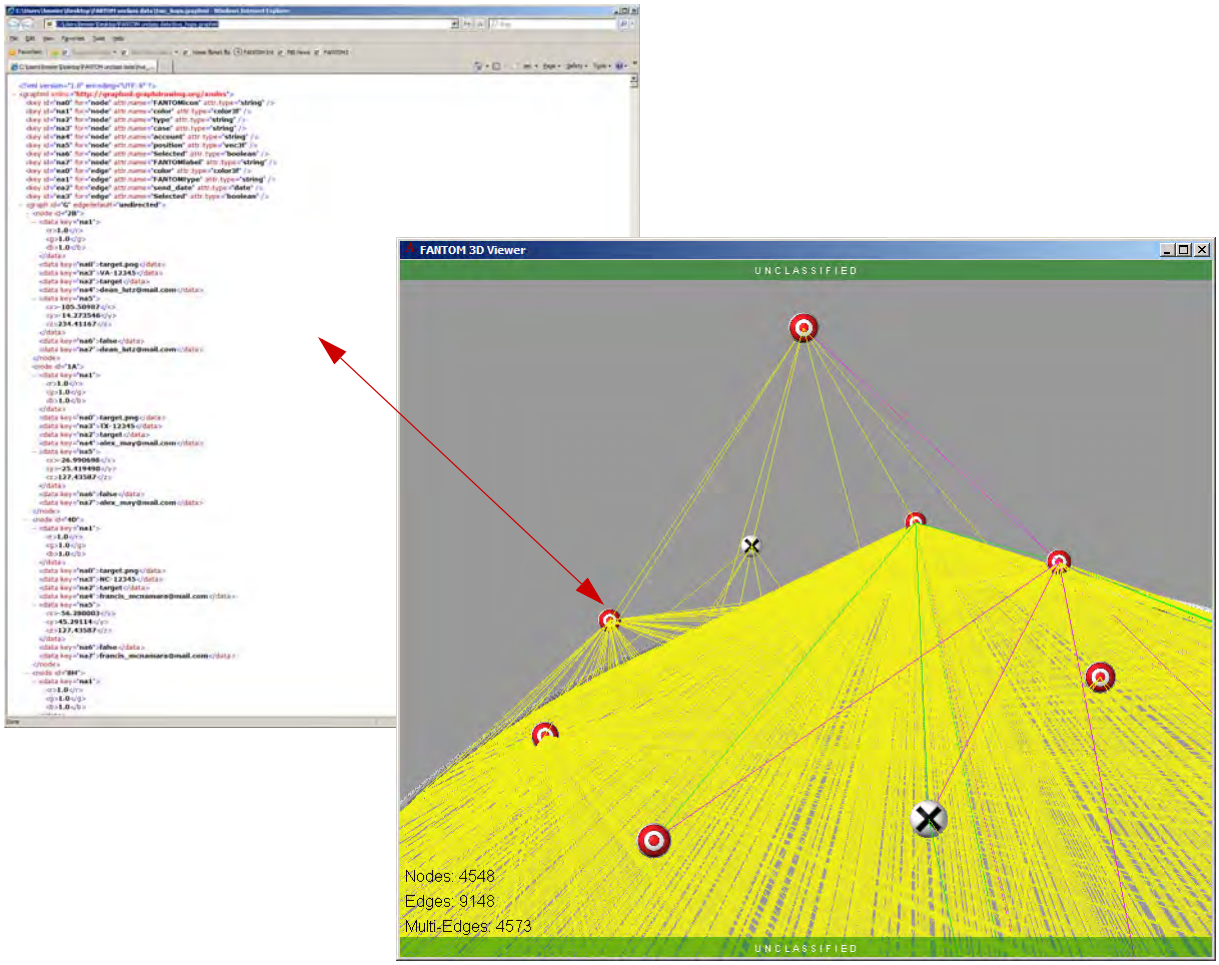
8. (U) Select the proper classification markings for this data set and click **OK**.

   (U) FANTOM displays the imported information in the Controller and Graph Viewer windows.

Importing GraphML Data

(U) GraphML is an XML-based file format used for graphs. In Figure 2-23, you can see an example of a GraphML file, which defines a graph created in FANTOM.

Figure 2-23: (U) Example of the text contents of a GraphML file



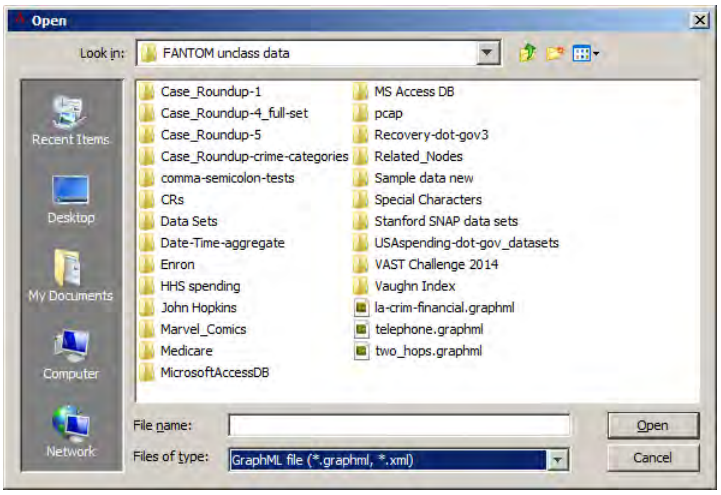
(U) **To import GraphML data:**

1. (U) Choose **File** > **File Importer** or click the **Import** tool button ( ).

   (U) A standard File Import dialog box displays.

2. (U) Select the **GraphML** file type (Figure 2-24).

Figure 2-24: (U) File Import dialog box



3. (U) Select one or more GraphML files or a folder that contains one or more GraphML files.

   (U) You can use SHIFT+CLICK to select a contiguous range of files or COMMAND+CLICK to select multiple files that are not adjacent.

4. (U) Click the **Open** button.

   (U) The imported GraphML files display in the FANTOM Controller and 3D Viewer windows.

Note: (U) When you import a data set, FANTOM creates a default filter for it identified by each data set's filename. The filter is initially disabled. To hide the entire data set, click the **Filter** tab and select the **Enabled** check box for that filter entry in the list.

Importing PCAP Data

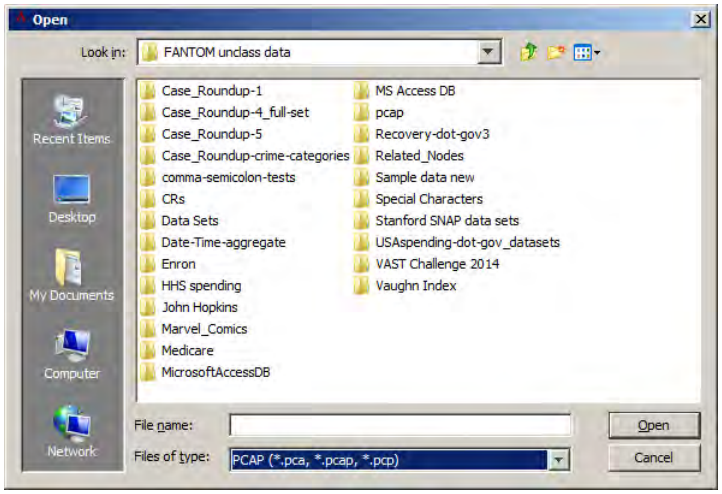
(U) You can import PCAP (Packet Capture Data) data into FANTOM for analysis. The PCAP data format is used by network monitoring and packet sniffing software, such as Wireshark. These applications let you analyze network traffic data.

(U) **To import PCAP data:**

1. (U) Choose the **File** > **File Importer** command or click the **Import** tool button ( ).

   (U) A standard Import dialog box displays.

   Figure 2-25: (U) File Import dialog box



2. (U) Select the PCAP file format.

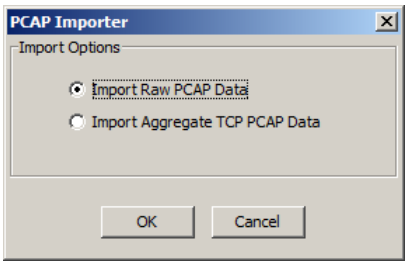
3. (U) Browse to the location where your PCAP files are stored, and select one or more of them or a folder that contains one or more PCAP files.

   (U) You can use SHIFT+CLICK to select a contiguous range of files or COMMAND+CLICK to select multiple files that are not all adjacent.

4. (U) Click the **Open** button.

   (U) The PCAP Importer dialog box displays (Figure 2-26).

Figure 2-26: (U) PCAP Importer dialog box



5. (U) Select the Import Options:

   - (U) **Import Raw PCAP Data** – Select this radio button and FANTOM maps each IP packet to a FANTOM record. Each packet in the PCAP file is treated as an edge. For example, if someone is downloading a file, there could be thousands or millions of packets (edges) for that one connection.
   - (U) **Import Aggregate TCP PCAP Data** – Select this radio button and FANTOM maps each unique TCP session to a FANTOM record. Each unique TCP session (technically from the SYN to the FIN packets) is considered one edge. The total TCP session is aggregated into a single edge. In the scenario of downloading a single file, this would (most likely) show up as a single edge. If the connection is interrupted, it may still split TCP sessions though.

6. (U) Click **OK**.

7. (U) Wait for the import to complete.

   (U) FANTOM displays the Classification Editor dialog box.

   (U) Select the classification, add any caveats, and decide whether to allow override of the classification after the data set has been imported into FANTOM.

8. (U) Click **OK**.

   (U) FANTOM displays the packet capture information for the first file in the Controller window table and displays the information visually in the Graph window.

9. (U) Repeat step 7 and step 8 for each PCAP data set you are importing.

   (U) If no classification has been selected, you cannot continue.

Note: (U) When you import a data set, FANTOM creates a default filter for it identified by the data set's filename. The filter is initially disabled. To hide the entire data set, click the Filter tab and select the Enabled check box for that filter entry in the list.

Importing Email Data

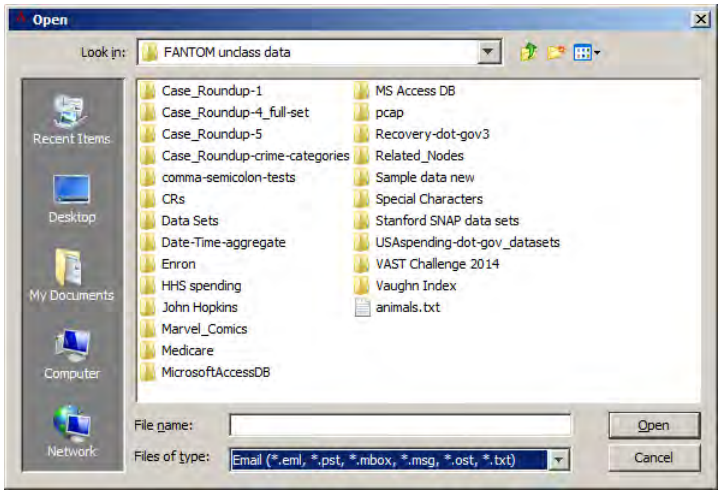
(U) FANTOM lets you import Multipurpose Internet Mail Extensions (MIME) email data formats including Microsoft Outlook .pst, .MBOX, and .eml.

To import Email data:

1. (U) Choose **File** > **File Importer**.

   (U) FANTOM displays a standard Open dialog box.

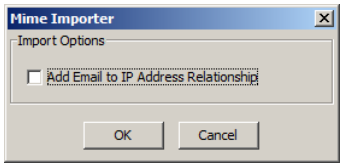
   Figure 2-27: (U) Import Open dialog box



2. (U) Select **Email (*.eml, *.pst, *.mbox, *.ost, *.txt)** from the **File name** menu.

   (U) The Mime Importer dialog box displays.

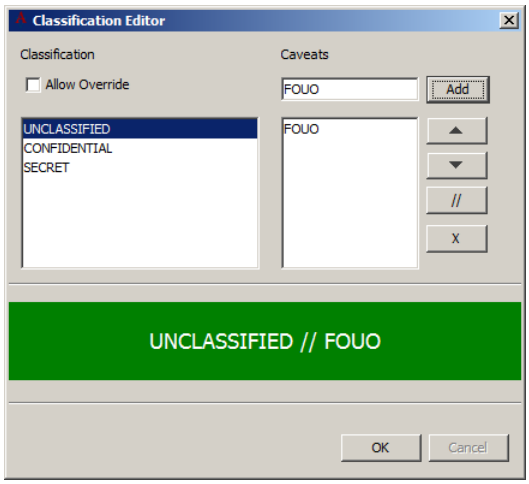
   Figure 2-28: (U) Mime Importer dialog box



3. (U) Select or deselect the **Add Email to IP Address Relationship** check box and click **OK**.

   (U) The Classification Editor dialog box displays (Figure 2-29).

Figure 2-29: (U) Classification Editor dialog box



4. (U) Select the classification level, add any caveats, and specify whether to **Allow Override** of this classification in this data set later.

5. (U) Click **OK**.

   (U) FANTOM displays the email data set in the Controller and 3D Viewer windows.

Dragging and Dropping Files into FANTOM

(U) FANTOM lets you drag and drop files into either the Controller or 3D Viewer windows to indicate you want to open them. The following table shows the way FANTOM responds when you do this.

Table 2-1: (U) Dragging and Dropping Files into FANTOM

File Format	FANTOM Response
Delimited (csv, dsv, log, txt)	Displays the Choose Importer dialog box. After you select the type of import (CSV or Email), FANTOM displays the Template Selection dialog box where you can create a new or select an existing FANTOM template
Excel (xls, xlsx)	Displays the Choose Importer dialog box. After you select the type of import (Excel or Research for Open Research), FANTOM displays the Template Selection dialog box where you can create a new or select an existing FANTOM template
GraphML	Displays the Classification Editor where you can specify the classification for your data. Then, FANTOM opens the GraphML or XML file
Legacy Session File	Directly opens a FANTOM 2.8.5 or earlier session file
Email (eml, pst, mbox, msg, ost, txt)	Displays the Mime Importer dialog box where you can select or deselect the **Add Email to IP Address Relationship** option

File Format	FANTOM Response
PCAP	Displays the PCAP Importer dialog box where you can select either the **Import Raw PCAP Data** or **Import Aggregate TCP PCAP Data** option
Session File	Directly opens a FANTOM 3.0 or later session file

Saving FANTOM Data

(U) FANTOM lets you save your work in the following ways:

- (U) **File** > **CSV Exporter** – Saves all of the data from the tables but does not save the appearance of the graph in CSV format. See "Exporting FANTOM Data to a Delimited File."
- (U) **File** > **Session File - Save** saves the graph and table data, plus it saves the view position on the graph, and the filters. See "Saving a FANTOM Session."
- (U) Highlight data in any FANTOM table, press CTRL+C to copy, go to a spreadsheet or word processor window and press CTRL+V to paste.

Exporting FANTOM Data to a Delimited File

(U) The CSV Exporter produces a comma-separated value file that spreadsheet programs such as Excel can import. The content merges the Node Table and the Edge table. FANTOM can import the resulting file with the Delimited file importer. However, the graph layout and other things related to the display form will be lost.

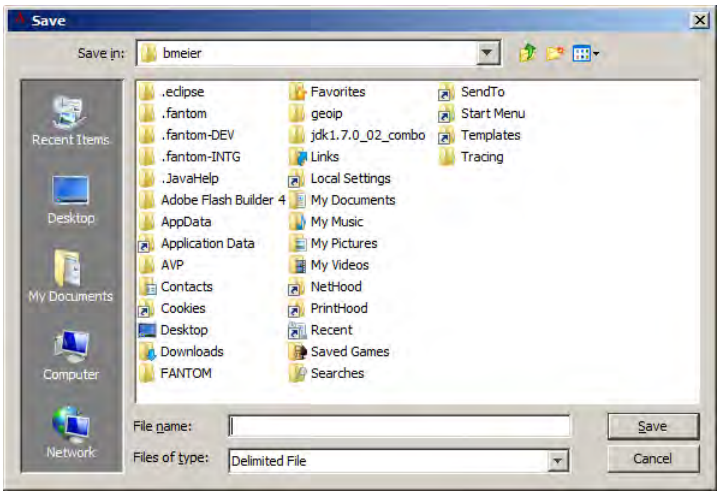
Note: (U) Exported CSV files are not intended for re-import into FANTOM. It has no mechanism for saving filters or filtered information. If you want to save everything, including currently filtered data, be sure to turn off any enabled filters first. Saving a session is the best way for you to save everything including filters, node icons, and so on. CSV files that you have exported from FANTOM *can be imported*, but it requires the template creation process described above. Saving a session is simpler and saves everything.

(U) **To export FANTOM data:**

1. (U) Choose **File** > **CSV Exporter** or click the **CSV Exporter** tool button ( ).

   (U) A standard Save dialog box displays (Figure 2-30).

Figure 2-30: (U) Save dialog box



2. (U) Specify the filename to use in the **File name** text box, or accept the default, and then click **Save**.

Caution: (U) If filters are enabled, the CSV Exporter exports only the *filtered graph* and not the *full graph* data set. If you want to save all the data, either disable the filters or use **Save Session**.

Saving a FANTOM Session

(U) When you save a session, FANTOM saves the current state of your FANTOM session including the graph, tables, filters, view (or camera) position, the results of analytics in the tables, including the colors of nodes, position of nodes, viewpoint position, and results of filtering.

(U) The selection and labeling of nodes is saved, as are the sizes of windows and the formatting of tables (where you can deselect columns for display and change the displayed width of columns).

Table 2-2: (U) Evolution of FANTOM Session Files

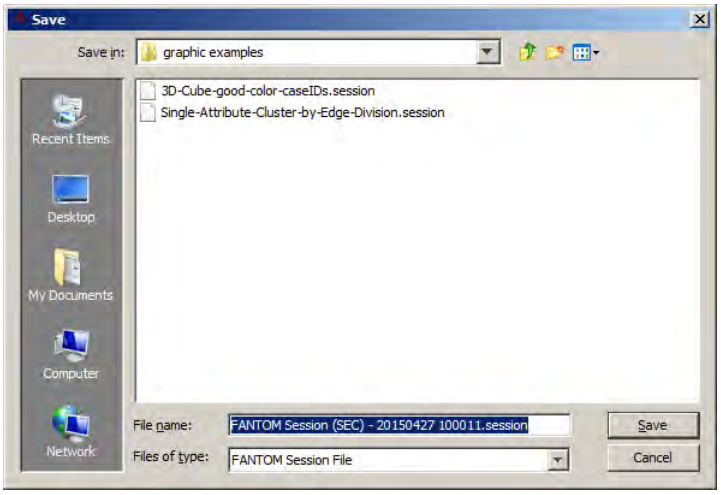
FANTOM Session File	Active in FANTOM Version	Description
*.fsa and a related .fsa folder	FANTOM version 2.7.4 or earlier	A FANTOM *.fsa file held the filters, camera views, and similar characteristics. Each .fsa file should have a companion fsa folder, which FANTOM placed in the same location as the .fsa file. The fsa folder contains resources like node icon graphic files and a .graphml file. The .graphml file contains the actual graph. To open a FANTOM .fsa file in FANTOM 3.0 or later, open the .fsa folder and drag the *.graphml file to the Controller or 3D Viewer windows. FANTOM 3.0 does not currently support conversion of the .fsa file, so you will need to recreate any filters.
*fsaz	FANTOM 2.8.0 to 2.8.5	A FANTOM *.fsaz session file is a compressed file that contains the FANTOM fsa file and its associated resources. FANTOM 3.0 can open *.fsaz files.
*.session	FANTOM 3.0 and later	FANTOM 3.0 introduces the .session file format for its session files.

(U) To save a FANTOM session:

1. (U) Choose **File** > **Session File - Save** or click the **Save Session** tool button ().

   (U) A standard Save dialog box displays (Figure 2-31).

Figure 2-31: (U) Save dialog box



2. (U) Accept the default filename, or change the filename (the portion left of the **.session** file extension) in the **Save As** text box to something meaningful to you.

Note: (U) Keep the **.session** file extension intact or completely remove it; otherwise, FANTOM cannot correctly save your session. FANTOM version 2.8.5 or earlier saved sessions using the *.fsaz file extension. You can drag and drop these files into FANTOM 3.0 to open them and then resave a new session in the new file format.

3. (U) Click **Save**.

Saving a Screenshot of Your Graph

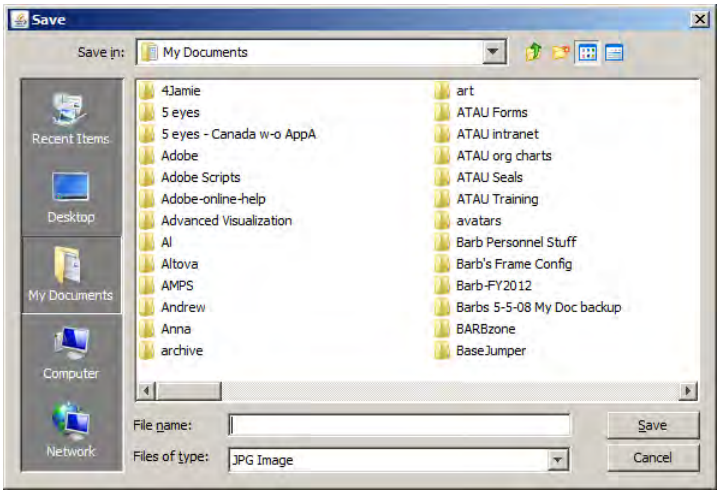
(U) FANTOM offers a command to let you save a screenshot of the graph you are viewing in the FANTOM Graph Viewer window.

(U) To save a screenshot of your graph:

1. (U) Choose the **Graph** > **Save Screenshot** command.

   (U) A standard Save dialog box displays (Figure 2-32).

Figure 2-32: (U) Save dialog box



2. (U) Accept the default filename, or change it to something that reminds you of the screenshot's contents.

3. (U) Select type of file and then click the **Save** button.

   (U) The available file types are:

   - (U) **JPG Image** – JPG is short for JPEG (Joint Photographic Experts Group). This compressed, LOSSY image file type was defined jointly by the ISO and ITU-T. LOSSY image compression means some quality may be lost.
   - (U) **PNG Image (*.png)** – PNG (Portable Network Graphics) is a compressed bitmap image file format widely used on the Internet and intranets. Like BMP, you can open, view, or edit these compressed bitmap image files using Microsoft Paint. PNG was approved by the Worldwide Web Consortium as a patent and license-free replacement for the GIF file format.
   - (U) **Bitmap Image (*.bmp)** – BMP is the standard uncompresse3d bitmap image file format used with Microsoft Windows-based computers. You can open, view, or edit these bitmap image files using Microsoft Paint (click **Start** > **Programs** > **Accessories** > **Paint**) or other graphics applications if they are available to you. If you ZIP a BMP image, the ZIP form of compression will noticeably reduce the document's file size.

Table 2-3: (U) Image file sizes at 2560 x 1581 pixels

Image File Type	2560 x 1581 Pixel Image File Size
JPG	209 KB
PNG	227 KB
BMP as saved by FANTOM	11.5 MB
BMP Zipped	263 KB

Copying and Pasting Table Data into an External File

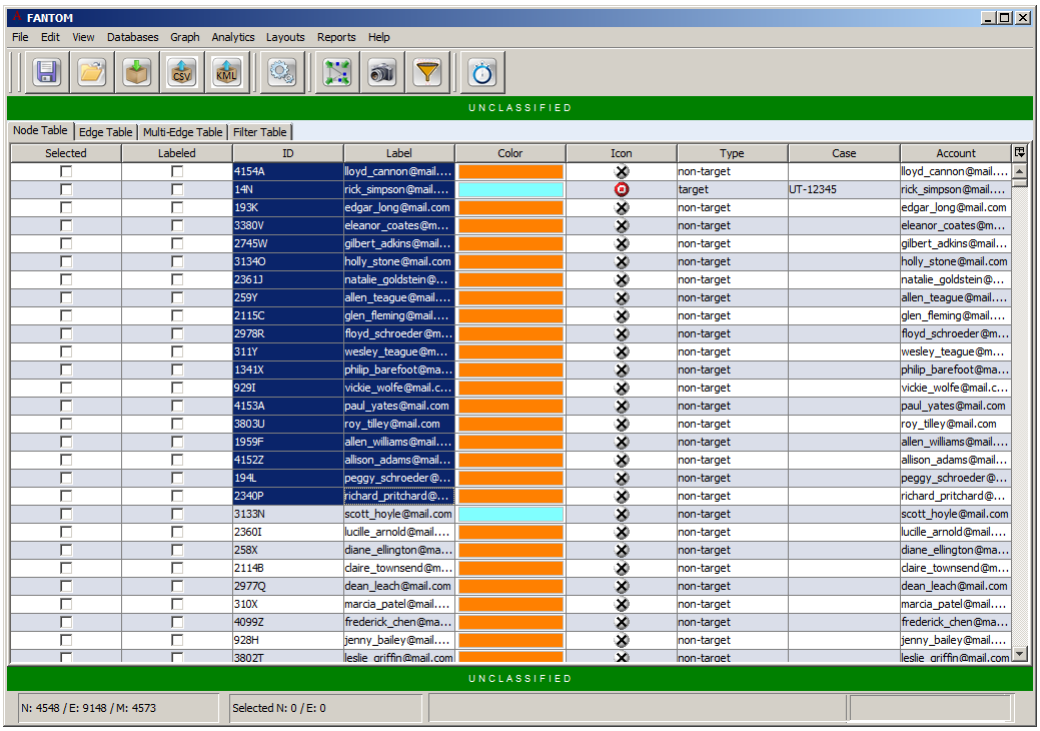
(U) FANTOM lets you copy and paste data from the Controller table into an open document file, such as a word processing or spreadsheet document.

(U) To copy data into another application:

1. (U) Drag up or down and left or right to highlight one or more rows and columns of data in the FANTOM Controller window's table.

   (U) FANTOM changes highlighted table cells to navy blue with reversed text in white (Figure 2-33).

Figure 2-33: (U) Highlighting data in the Controller window



2. (U) Choose the **Copy** command by pressing the CTRL+C keys.
3. (U) Open another application's document and place the cursor where you want to paste the FANTOM data.
4. (U) Choose the **Edit** > **Paste** command (or press CTRL+V).

Exporting FANTOM Data to a Google Earth KML File

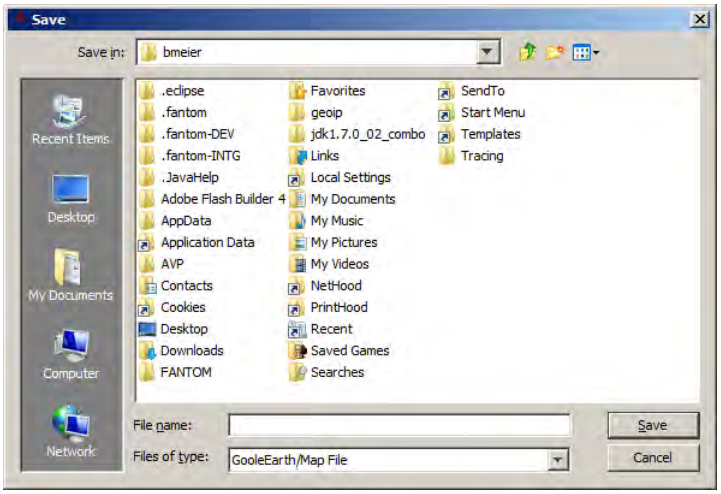
(U) If your data set includes IP addresses, you can use the GeoIP Local command to obtain the longitude and latitude plus other selected information. Once you have the Longitude and Latitude, you can use the KML Exporter command to create a .KML file which can be dragged and dropped into Google Earth to see the geographical location of the IP addresses.

To export FANTOM data to a Google Earth .KML file:

1. (U) Verify that your IP data set has latitude and longitude columns, or use the **Databases** > **GeoIP Local** command to obtain these values.
2. (U) Choose **File** > **KML Exporter (GoogleEarth)** or click the KML tool button ( ).

   (U) FANTOM displays a standard Save dialog box.

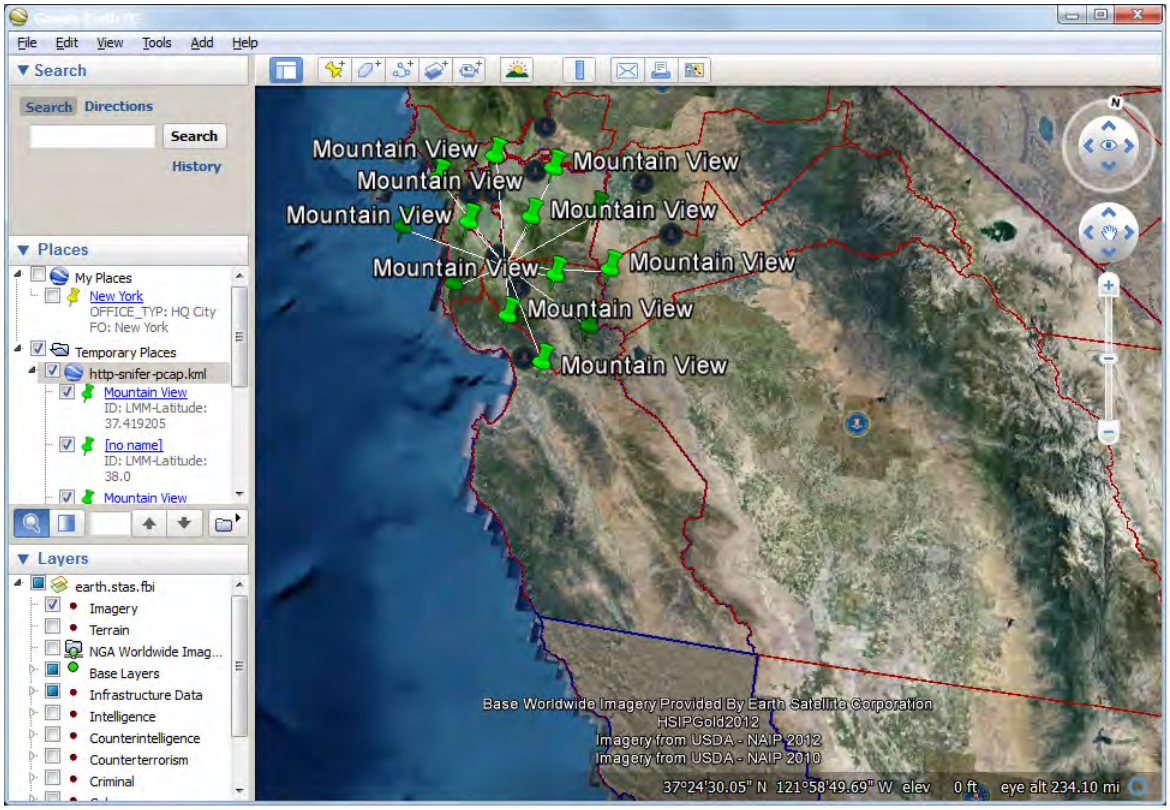
Figure 2-34: (U) Save dialog box



3. (U) Type a filename and click **Save**.
4. (U) Start Google Earth and then drag/drop the .kml file into the open Google Earth window.

   (U) Google Earth places the placemarks into the Places pane's Temporary Places folder (Figure 2-35).

Figure 2-35: (U) Example of Google Earth with exported FANTOM data



Opening a FANTOM Session

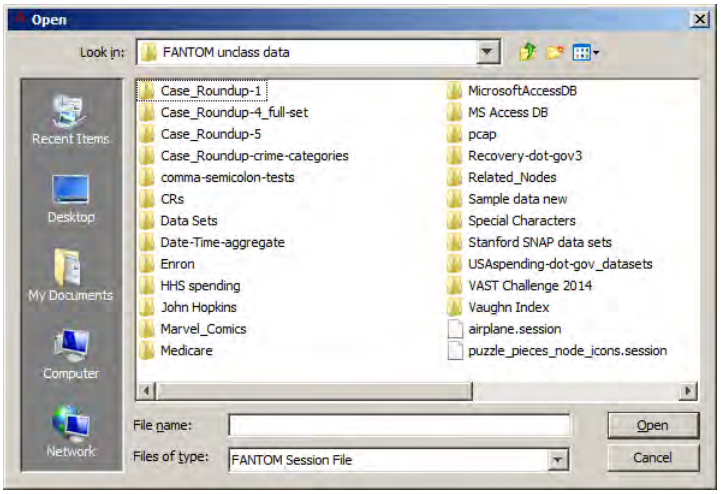
(U) After you save a FANTOM session, you can reopen it to resume your work. FANTOM can open either the original FANTOM session file format (*.fsa) or the current compressed FANTOM session file format (*.fsaz).

(U) To open a FANTOM session:

1. (U) Choose **File** > **Session File - Open** or click the **Open Session** tool button ( ).

   (U) A standard Open dialog box displays (Figure 2-36).

Figure 2-36: (U) Open dialog box



2. (U) Select a session file with a **.session** file extension and click **Open**.

Querying a Database

(U) FANTOM lets you connect to an Oracle, MySQL, PostgresSQL, or SQL Server database to access the data it contains using the **Databases** > **Database Importer** command.

Note: (U) You can open multiple data sets in FANTOM using the **Import** and **Databases** commands to cross-correlate point-to-point connections across these data sets. The only limit to the amount of data you can access is how much RAM is available on the computer where you are running FANTOM.

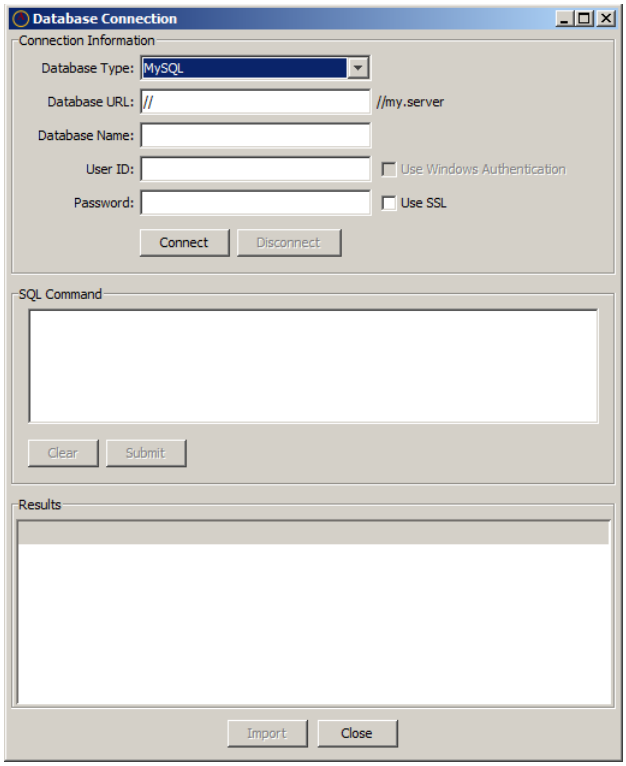
(U) This section explains how you can query a database that has an existing *template*, which the Advanced Visualization Team has probably created for you. In FANTOM, *templates* specify what data to use and how it should be presented.

(U) **To access a database:**

1. (U) Choose **Databases** > **Database Importer**.

   (U) The Database Connection dialog box displays (Figure 2-37).

Figure 2-37: (U) Database Connection dialog box

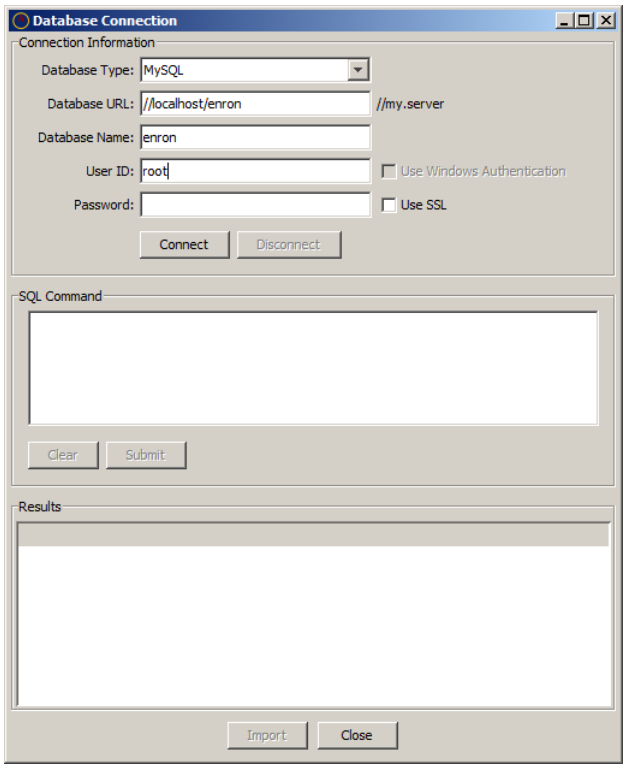


2. (U) Specify the following database connection information, and then click the **Connect** button:

   - (U) **Database Type** – Choose **MySQL**, **Oracle**, **PostgreSQL** or **SQL Server**.
   - (U) **Database URL** – Type the name of the database in the following format:
     - (U) **Oracle** – `@<server_name>:<port_number>`
     - (U) **MySQL** – `//<server_name>`
     - (U) **PostgreSQL** – *`//<server name>/<host:port>/`*
     - (U) **SQL Server** – `//<server_name>:<port_number>`
   - (U) **Database Name** – Enter the name for this database in this text box.
   - (U) **User ID** and **Password** – Supply your database user name and password.
   - (U) **Use Windows Authentication** – This check box is only available when you choose **SQL Server**. It uses your current logged in user credentials to authenticate you (disables the **User ID** and **Password** fields).

- (U) **Use SSL** – This check box is only available for PostgreSQL and MySQL database types. You should use it if the database requires a Secure Socket Layer (SSL) connection to authenticate.

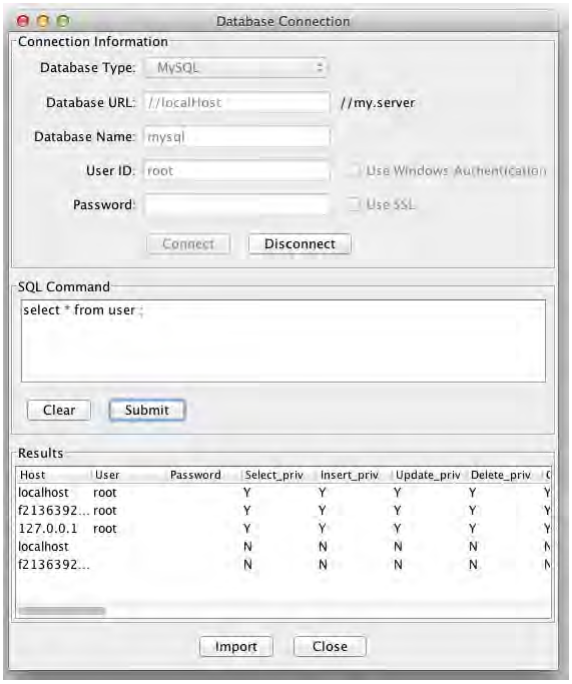
Figure 2-38: (U) Example of a database connection established



3. (U) Type a **SELECT** command in the **SQL Command** text box that defines the information to retrieve from the database (see example in Figure 2-39).

4. (U) Click the **Submit** button.

Figure 2-39: (U) Example of submitted SELECT command

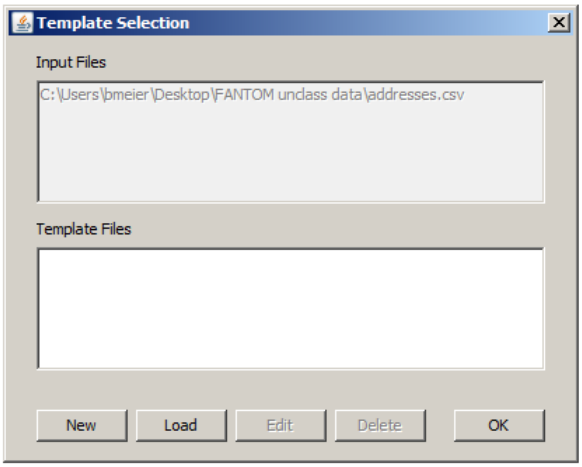


(U) Data that matches the SELECT command you typed displays in the Results table.

5. (U) Click the **Import** button.

   (U) The Template Selection dialog box displays.

Figure 2-40: (U) Template Selection dialog box



6. (U) Do one of the following:

   - (U) Click the **New** button if there is not yet a template for the file you are importing.

(U) FANTOM displays a Save dialog box where you can provide a filename for the new template and then define template settings. See Chapter 12, "Creating Import Templates."

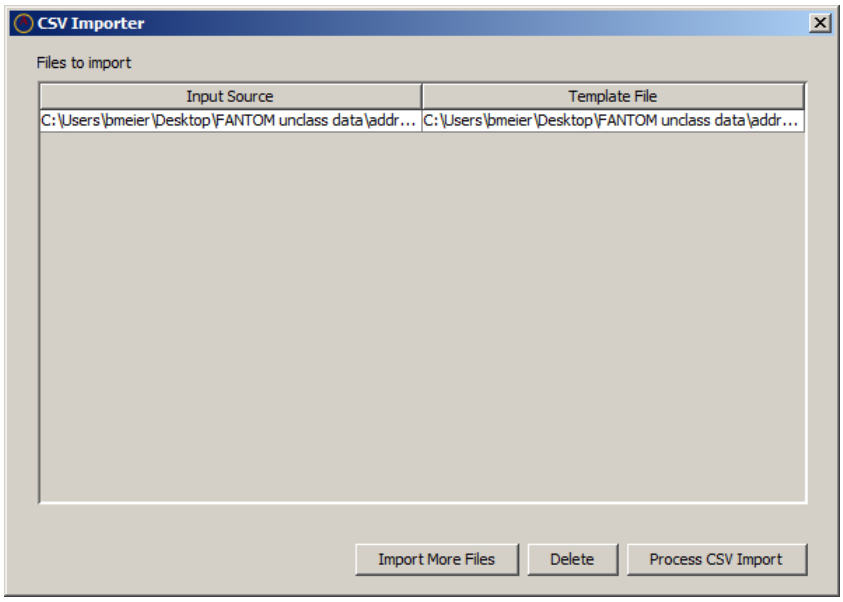
- (U) Click the **Load** button if a template file exists for the file you are importing.

  (U) FANTOM displays an Open dialog box where you can select an existing template. After you select a template file and click Open, FANTOM adds the full path to the Template Files text box.

7. (U) Click **OK** in the Template Selection dialog box.

   (U) The CSV Importer dialog box displays.

Figure 2-41: (U) CSV Importer

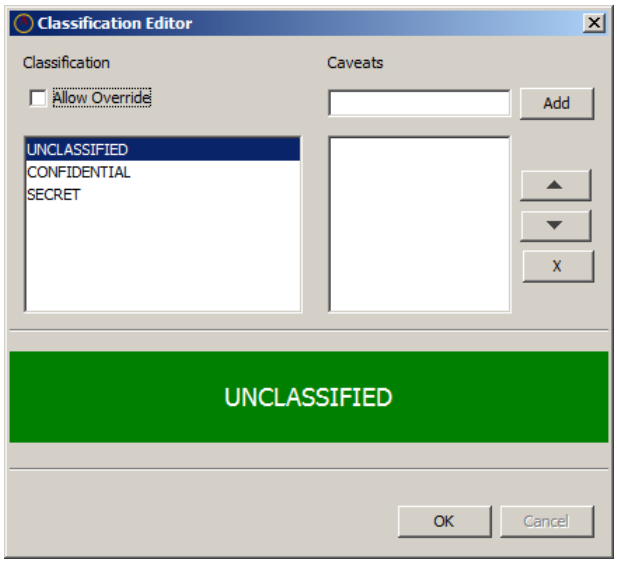


8. (U) Do one of the following:

   - (U) Click **Import More Files** to select more data files to import.
   - (U) Select a file in the **Files to import** list and click **Delete** to remove that source from your import list.
   - (U) Click **Process CSV Import** to begin importing data.

   (U) The Classification Editor dialog box displays (Figure 2-14).

Figure 2-42: (U) Classification Editor dialog box



(U) You must choose a Classification level before you can continue.

9. (U) Select Classification options and then click **OK**.

   (U) The data displays in the FANTOM Controller and 3D Viewer windows.

Finding Text in the Controller Window

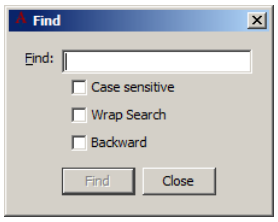
(U) In FANTOM, you can find text in the Controller window.

(U) To find text:

1. (U) Click any cell in the Node, Edge, Multi-Edge, or Filter tables.
2. (U) Press CTRL+F.

   (U) The Find dialog box displays (Figure 2-43).

Figure 2-43: (U) Find dialog box



3. (U) Type the text to find and select any of the options:

   - (U) **Case Sensitive** to require a match by upper or lower case for a search string to be found.

- (U) **Wrap Search** to continue the search from the top or bottom of the table once one end or the other is reached.
- (U) **Backward** search to change the direction of the search.

4. (U) Click the **Find** button repeatedly to go from one result to the next.

Performing Queries

(U) This chapter contains step-by-step procedures for:

- (U) Querying a Database
- (U) Getting GeoIP Information with GeoIP Local

Querying a Database

(U) FANTOM lets you connect to an Oracle, MySQL, PostgresSQL, SQL Server, or SQLite database to access the data it contains using the **Databases** > **Database Importer** command.

Note: (U) You can open multiple data sets in FANTOM using the **Import** and **Databases** commands to cross-correlate point-to-point connections across these data sets. The only limit to the amount of data you can access is how much RAM is available on the computer where you are running FANTOM.

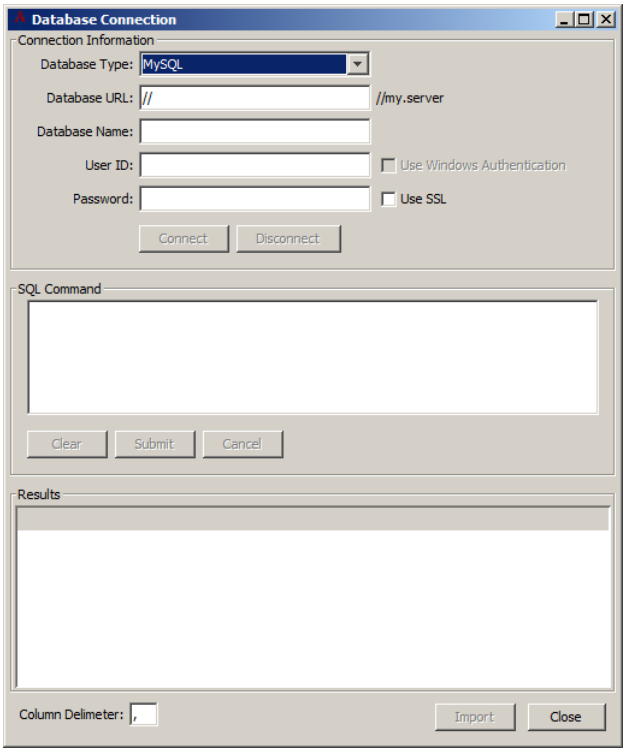
(U) This section explains how you can query a database that has an existing *template*, which the Advanced Visualization Team has probably created for you. In FANTOM, *templates* specify what data to use and how it should be presented.

(U) **To access a database:**

1. (U) Choose **Databases** > **Database Importer**.

   (U) The Database Connection dialog box displays (Figure 3-1).

Figure 3-1: (U) Database Connection dialog box



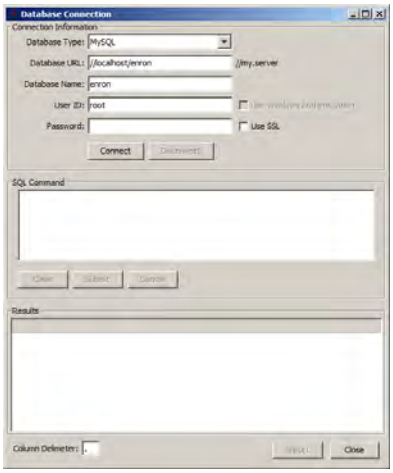
2. (U) Specify the following database connection information, and then click the **Connect** button:

   - (U) **Database Type** – Choose **MySQL**, **Oracle**, **PostgreSQL**, **SQL Server**, or **SQLite**.
   - (U) **Database URL** – Type the name of the database in the following format:
     - (U) **Oracle** – `@<server_name>:<port_number>`
     - (U) **MySQL** – `//<server_name>`
     - (U) **PostgreSQL** – *`//<server name>/<host:port>/`*
     - (U) **SQL Server** – `//<server_name>:<port_number>`
     - (U) **SQLite** – *`<standard path to database location>`*
   - (U) **Database Name** – Enter the name for this database in this text box.
   - (U) **User ID** and **Password** – Supply your database user name and password.
   - (U) **Use Windows Authentication** – This check box is only available when you choose **SQL Server**. It uses your current

logged in user credentials to authenticate you (disables the **User ID** and **Password** fields).

- (U) **Use SSL** – This check box is only available for PostgreSQL and MySQL database types. You should use it if the database requires a Secure Socket Layer (SSL) connection to authenticate.

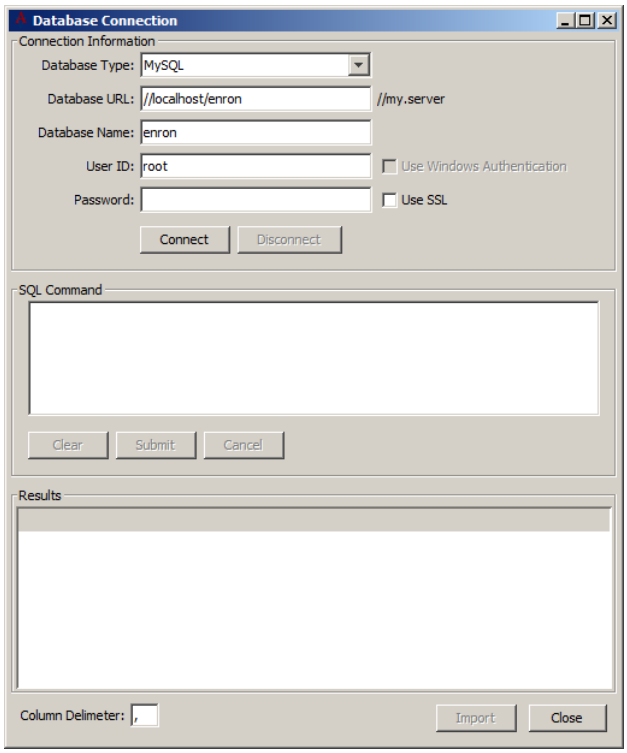
Figure 3-2: (U) Example of a database connection established



3. (U) Type a **SELECT** command in the **SQL Command** text box that defines the information to retrieve from the database (see example in Figure 3-3).

4. (U) Click the **Import** button.

Figure 3-3: (U) Example of submitted SELECT command

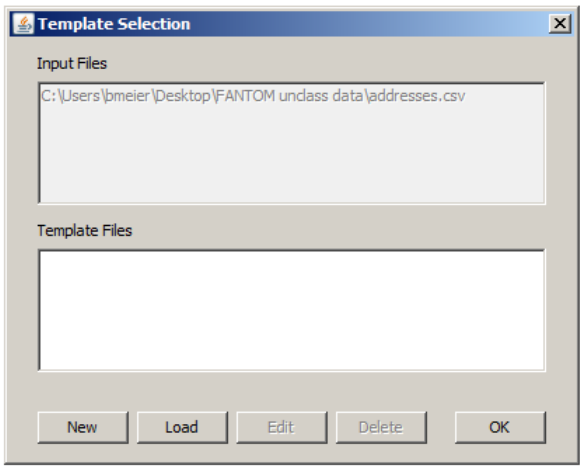


(U) Data that matches the SELECT command you typed displays in the Results table.

5. (U) Click the **Import** button.

(U) The Template Selection dialog box displays.

Figure 3-4: (U) Template Selection dialog box



6. (U) Do one of the following:

   - (U) Click the **New** button if there is not yet a template for the file you are importing.

     (U) FANTOM displays a Save dialog box where you can provide a filename for the new template and then define template settings. See Chapter 12, "Creating Import Templates."

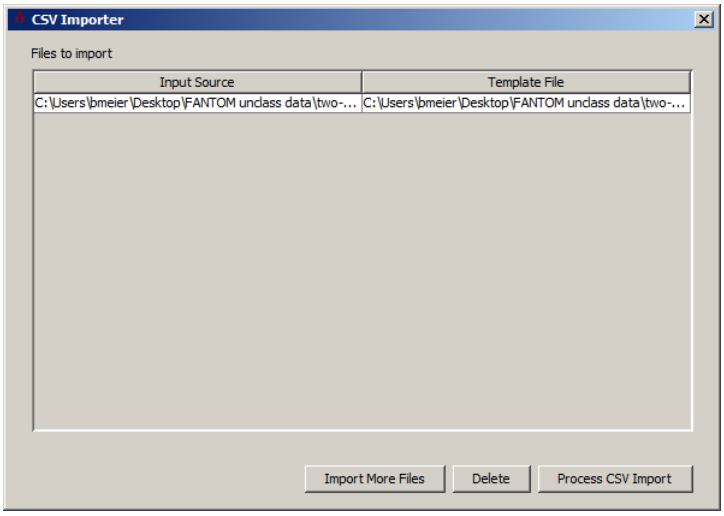
   - (U) Click the **Load** button if a template file exists for the file you are importing.

     (U) FANTOM displays an Open dialog box where you can select an existing template. After you select a template file and click Open, FANTOM adds the full path to the Template Files text box.

7. (U) Click **OK** in the Template Selection dialog box.

   (U) The CSV Importer dialog box displays.

Figure 3-5: (U) CSV Importer

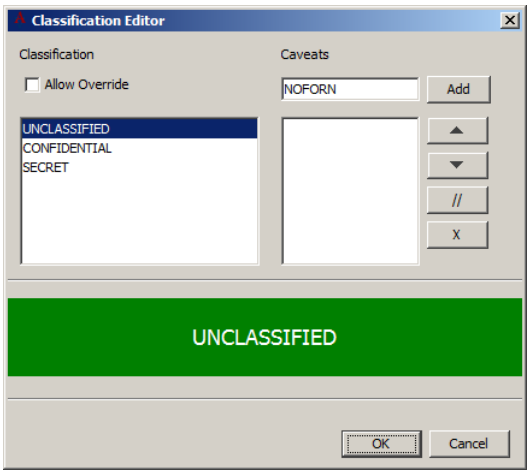


8. (U) Do one of the following:

   - (U) Click **Import More Files** to select more data files to import.
   - (U) Select a file in the **Files to import** list and click **Delete** to remove that source from your import list.
   - (U) Click **Process CSV Import** to begin importing data.

   (U) The Classification Editor dialog box displays.

Figure 3-6: (U) Classification Editor dialog box



(U) You must choose a Classification level before you can continue.

9. (U) Select Classification options and then click **OK**.

   (U) The data displays in the FANTOM Controller and 3D Viewer windows.

Getting GeoIP Information with GeoIP Local

(U) FANTOM provides a GeoIP Local service that uses the Max Mind geographic data set. You need to obtain a license from the corporation at:

http://www.maxmind.com

(U) Periodically, the Max Mind data must be updated. It includes the following files: GeoIPCity.dat, GeoIPDomain.dat, GeoIPISP.dat, GeoIPOrg.dat, and GeoIPSpeed.dat.

(U) FANTOM provides GeoIP Local preferences to show you information about these files. It also lists the version of the GeoIP Local Analytic in the **Help** > **About** message box (see "About" on page 1-9).

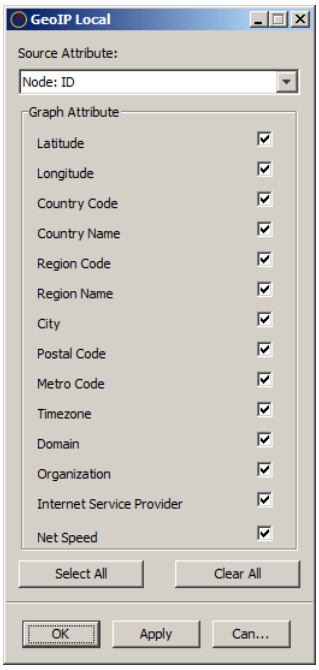
(U) If the MaxMind GeoIP files are not found at the location specified in your GeoIP Local Analytic Preferences, FANTOM displays a message to let you know when you choose this analytic. You can view or change the path by choosing **Edit** > **Preferences** and choosing **GeoIP Local**. You can obtain the MaxMind files and copy them to the default, or another, location specified in preferences.

To get GeoIP information about IP addresses in your data set:

1. (U) Choose **Databases** > **GeoIP Local**.

   (U) The GeoIP Local dialog box displays (Figure 3-7) if the MaxMind files are found at the location specified in GeoIP Local preferences.

Figure 3-7: (U) GeoIP Local dialog box

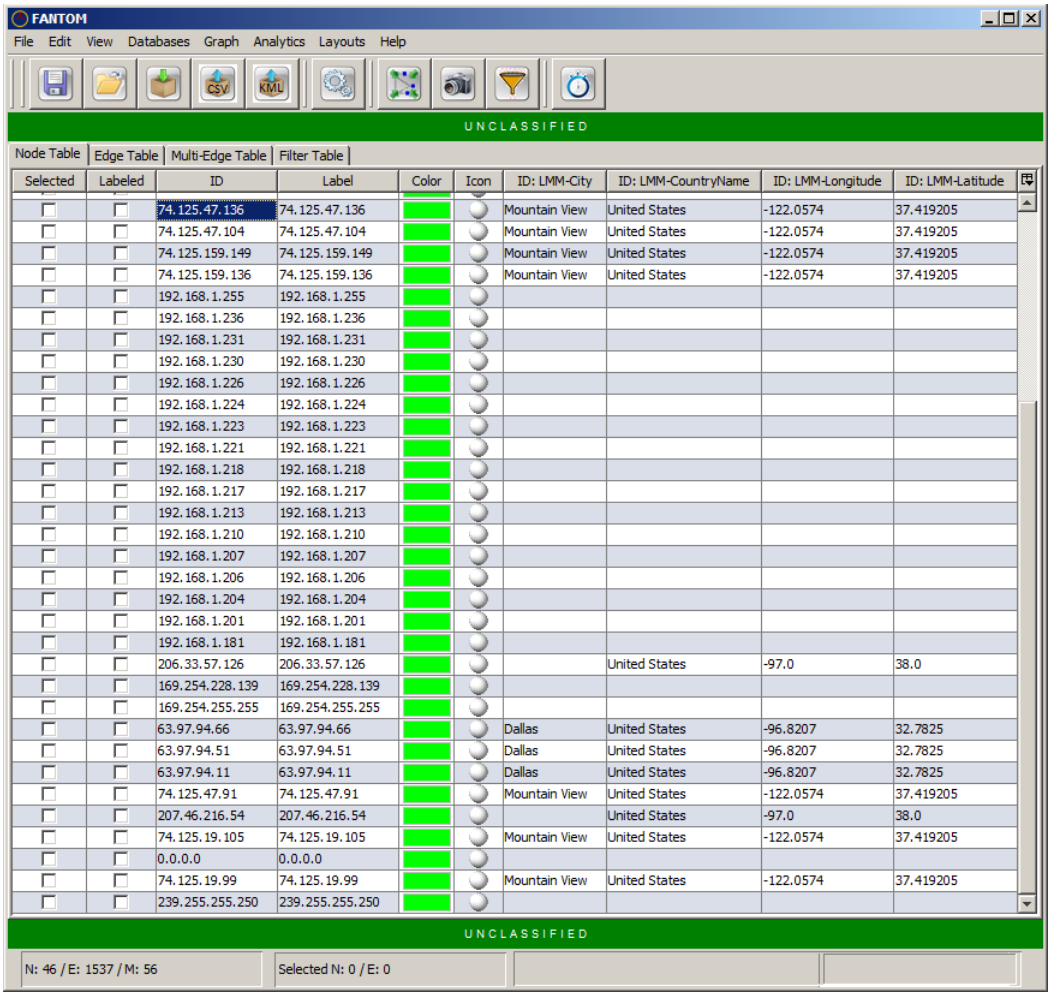


2. (U) Select the node in the **Source Attribute** menu and **Graph Attributes** to use, and then click **OK**.

3. (U) FANTOM adds columns matching the selected Graph Attributes to the table in the Controller window (Figure 3-8).

Note: (U) If the check boxes are dimmed, verify the path to the MaxMind data is correct in the GeoIP Local Analytic preferences component. Choose **Edit** > **Preferences**, select **GeoIP Local** from the **Plug-in** menu. You can expand the dialog box to more easily read or change the path by dragging the bottom right corner of the dialog box.

Figure 3-8: (U) GeoIP results example with GeoIP values added to Node Table; the GeoIP Local columns are each prefaced with LMM-



Customizing the Graph and Controller

(U) FANTOM offers several ways to customize the appearance of information in the Controller and 3D Viewer windows.

(U) After you access data, the Controller window displays information about that data in tables in the Node Table, Edge Table, and Multi-Edge Table tabs. The same information is shown graphically in the 3D Viewer window.

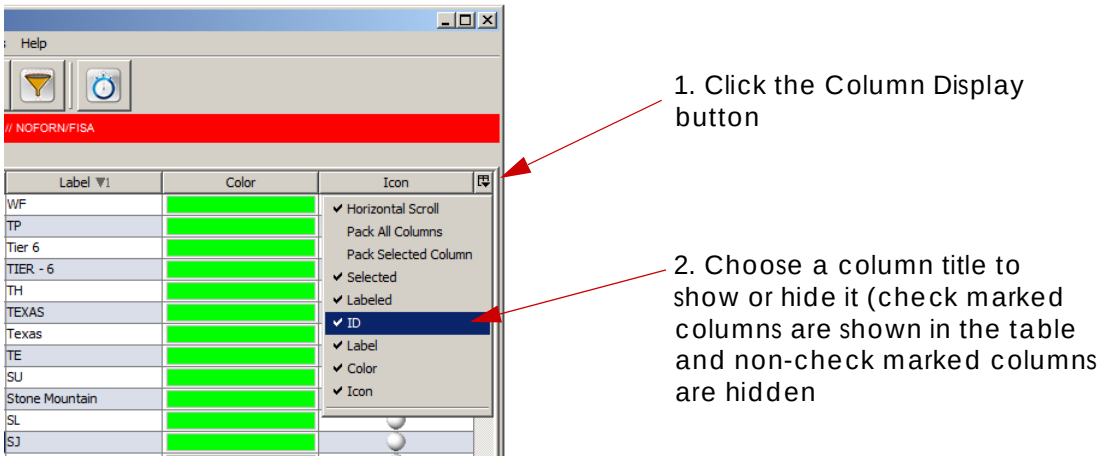
(U) This chapter explains the following options:

- (U) Showing and Hiding Columns
- (U) Resizing Columns
- (U) Sorting Columns
- (U) Setting and Clearing Colors
- (U) Labeling a Node
- (U) Configuring Labels
- (U) Clearing Graph Information

Showing and Hiding Columns

(U) To show or hide a column, right-click the **Column Display** button ( ) and choose a column name from the list. Columns with check marks will be hidden when you choose them; columns without check marks will be shown when you choose them.

Figure 4-1: (U) Column display button and menu

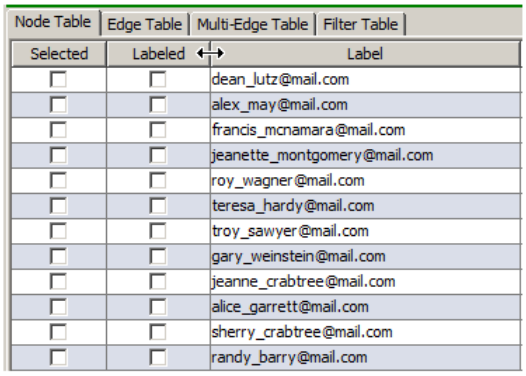


Resizing Columns

(U) To change the width of columns in the Controller table, do one of the following:

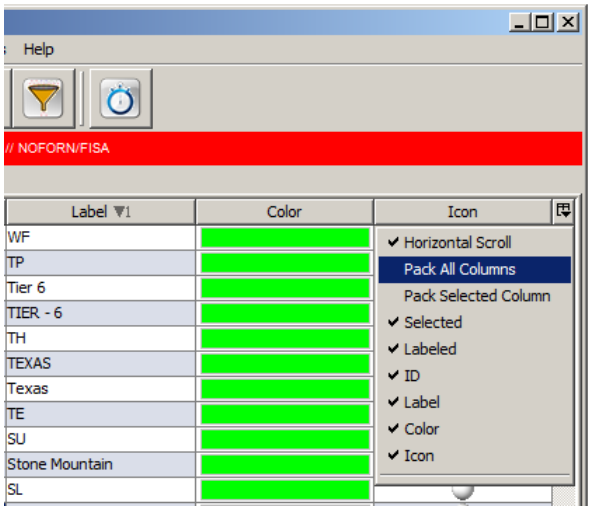
- (U) Point at a vertical bar between two column titles; when the Arrow pointer changes to the Resize pointer ( ), drag the vertical bar left or right to resize the two columns that share this border.

Figure 4-2: (U) Drag a vertical bar to resize the two columns that share this border



- (U) Click the **Column Display** button ( ) and choose the **Pack All Columns** command (Figure 4-3). FANTOM makes each column slightly wider than the widest entry in that column.

Figure 4-3: (U) Pack All Columns command



Sorting Columns

(U) FANTOM lets you sort multiple columns in the Controller window's Node Table, Edge Table or Multi-Edge Table.

(U) To sort multiple columns:

1. (U) Click a column title until the sort order you prefer is indicated.

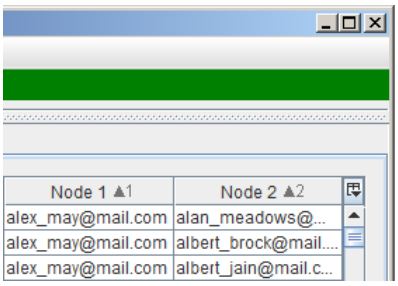
   (U) The sort indicator toggles between the following three settings:

   - (U) Ascending sort order ▲1
   - (U) Descending sort order ▼1
   - (U) Unsorted

2. (U) Hold down the SHIFT key while selecting another column title.

(U) FANTOM displays another sort indicator (▲2) incremented by one from the previous sort column. It toggles between ascending, descending, and unsorted.

Figure 4-4: (U) Example of multiple column sorting

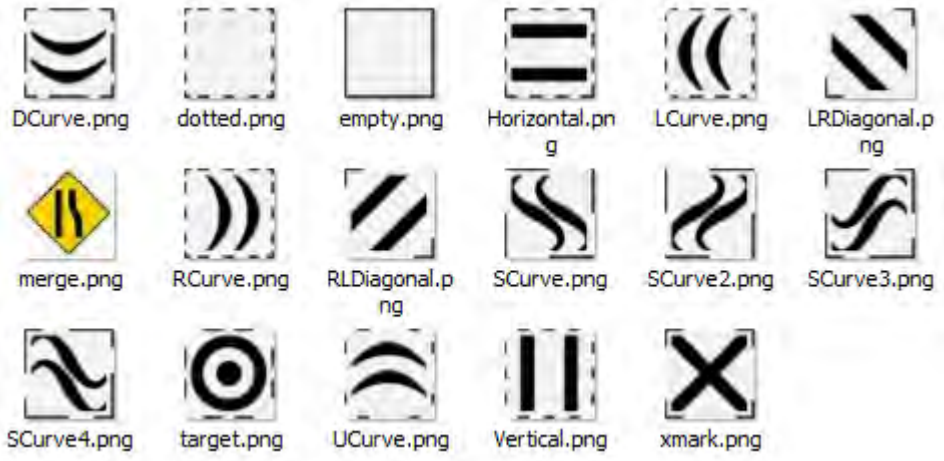


Setting a Node's Icon in the Controller

(U) FANTOM version 2.8.0 and earlier provided a collection of node icons designed to help you easily distinguish them when working with massive data sets where nodes in the Graph Viewer window are very small or overlapping.

Figure 4-5: (U) FANTOM node icons – main categories

Figure 4-6: (U) Original FANTOM node icons



(U) FANTOM version 2.8.1 and later offers greater flexibility by providing more node icon collections, such as targets, social media, FBI Most Wanted Terrorists, financial, people, case IDs, alias, and so on.

Figure 4-7: (U) Case ID node icons

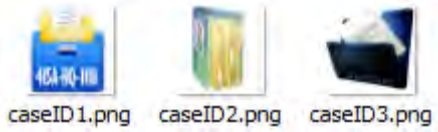


Figure 4-8: (U) FBI Most Wanted Terrorist node icons (from FBI public internet site)

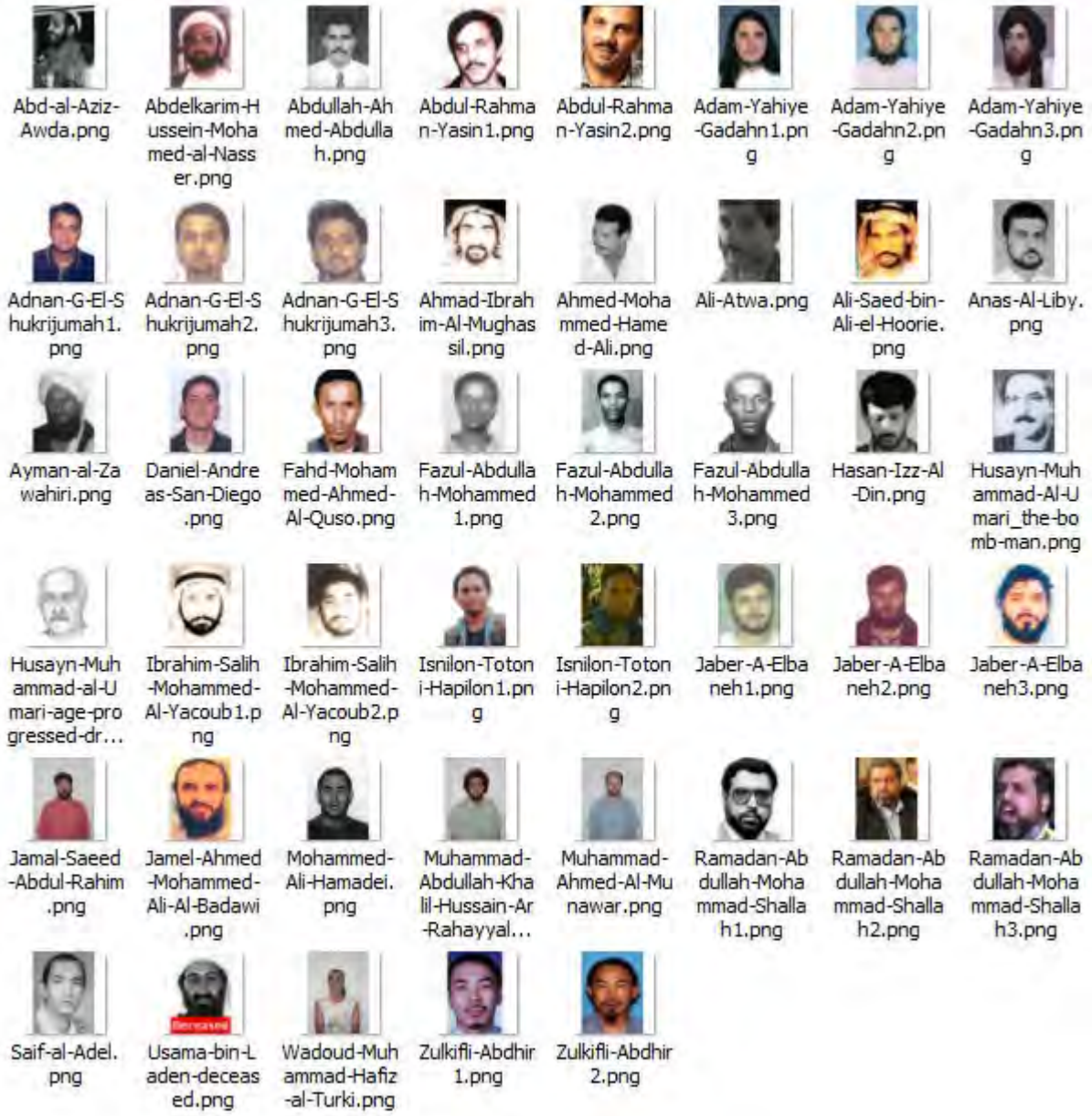
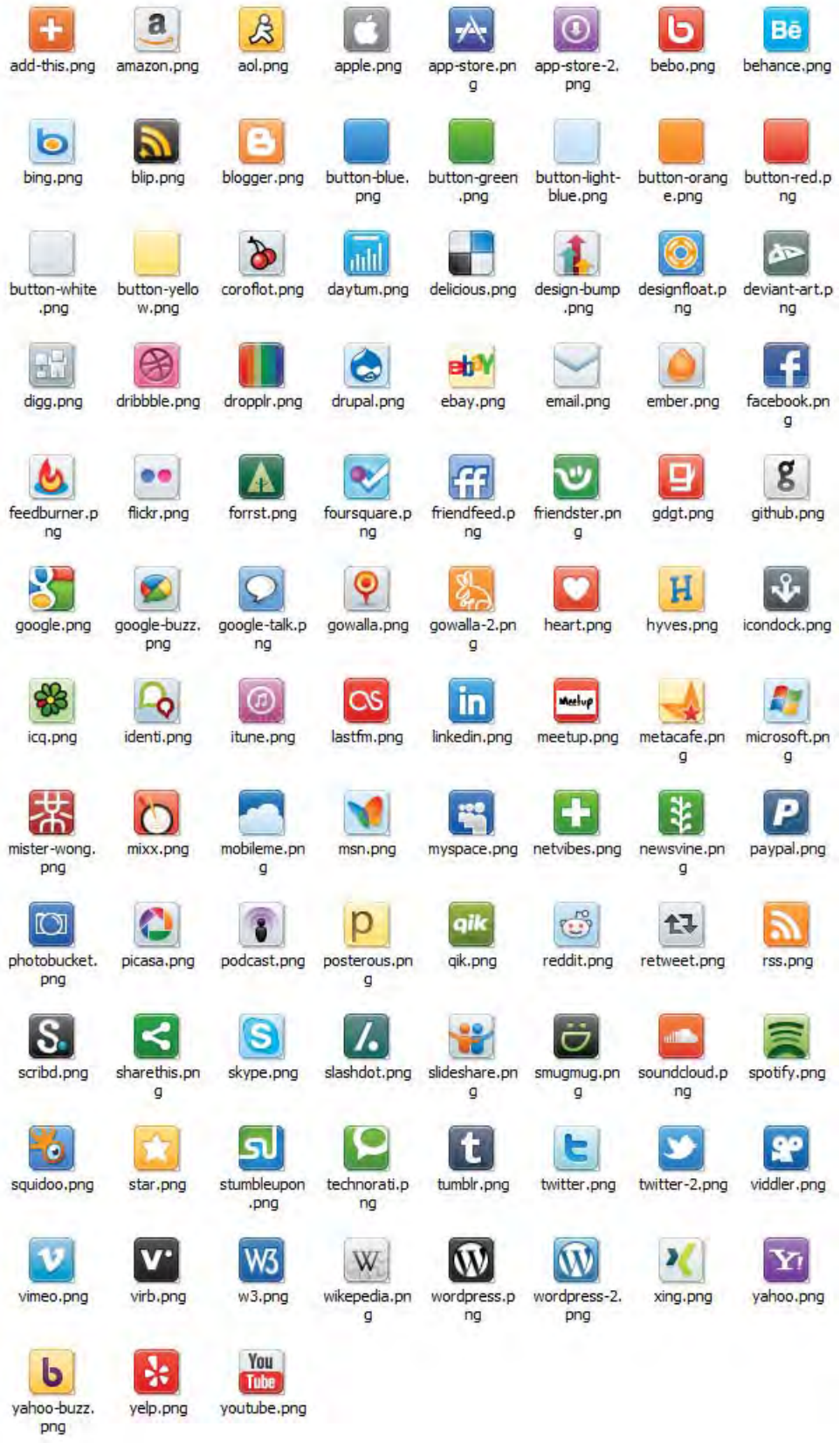


Figure 4-9: (U) Social Media node icons



(U) You can also select other PNG file images to use as node icons. If you obtain your own .png images, resize, crop, or trim them—use the Windows Paint application to do this—so they have one of the following dimensions (in pixels):

- 64 x 64
- 32 x 32

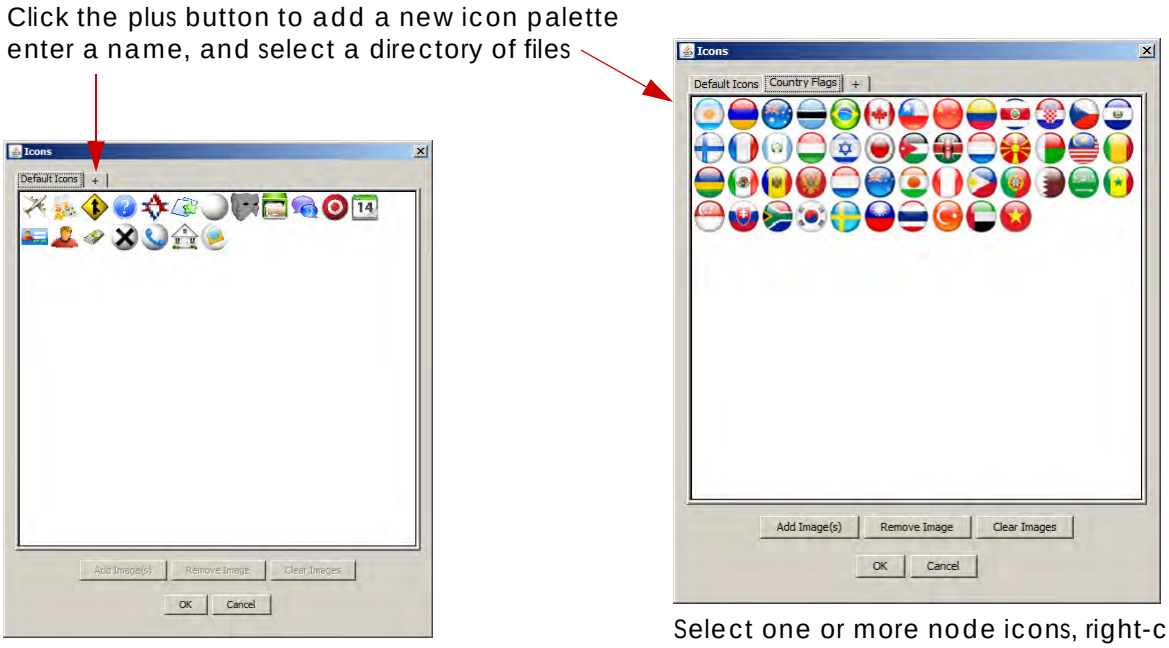
Note: (U) Be careful about the image size of png files you use as node icons. The larger the file size, the longer it takes for FANTOM to repaint the images in its Controller table and Graph Viewer.

(U) To select a node icon:

1. (U) Go to the Nodes tab in the Controller window and select one or more rows.
2. (U) Do one of the following:
   - (U) Double-click a node icon or icon placeholder ( ).
   - (U) Right-click an icon or icon placeholder and choose **Set Icon**.

   (U) The Select a Node Icon dialog box displays (Figure 4-5).

Figure 4-10: (U) Select a Node Icon dialog box



Double-click one node's Icon box and the simple Select A Node Icon dialog box displays; your selection changes only the node icon you double-clicked

Select one or more node icons, right-click and choose **Set Icon** and the expanded select A Node Icon dialog box displays; your selection changes the node icons for all the node icons highlighted in the node table

3. (U) Locate and select a node icon image (a .png file).

4. (U) (*Expanded dialog box only*) Select whether the icon should apply to the highlighted rows or to rows based on an exact **Value** you specify for an **Attribute Name** in the Node Attributes Filter section.

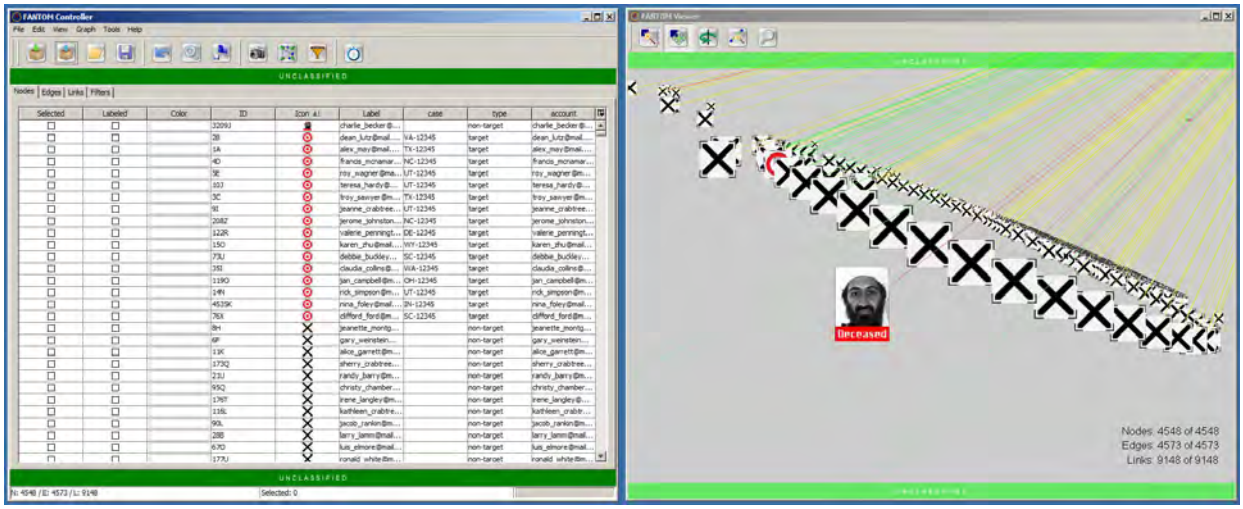
5. (U) Click **OK**.

   (U) FANTOM does one of the following:

   - ((U) Adds the icon to the icon box you double-clicked.
   - (U) Adds the icon to the selected node icons.
   - (U) Adds the icon to nodes that meet the criteria you specified.

   (U) FANTOM also applies the node icon to the corresponding nodes in the Graph Viewer window.

Figure 4-11: (U) Example of a terrorist target node icon applied



Setting and Clearing Colors

(U) You can set a node and edge color for one or more of the selected objects to help you more easily identify them in a graph. Multi-edges are colored based on the colors of the edges that comprise them. FANTOM also lets you clear colors.

Note: The colors you select for edges automatically color the corresponding multi-edges. If you set different colors for one multi-edge, the multi-edge changes to the first manually set color. If you change the color for all edges in a multi-edge, FANTOM changes the multi-edge to the new color.

Table 4-1: (U) Ways to Color Nodes, Edges, and Multi-Edges

What to Color	Command	Color Selection Method
Nodes or Edges	Double-click a **Color** box in corresponding table	Color palette selection
Nodes or Edges	Source to Destination Path Analytic	Optionally sets Node color and Edge color to the color you select (red is the default)
Edges	Colorizer Analytic	Color by rule
Edges	Link Cluster Layout	Color Edges check box colors by cluster
Edges	Attribute Colorizer	Color by cluster attribute
Nodes	Articulation Points Analytic	Colors nodes red that are articulation points
Nodes	Betweenness Analytic	Colors nodes by betweenness level: red - highest; yellow - near highest; green - all other nodes
Nodes	Colorizer Analytic	Color by rule
Nodes	Choose **Graph** > **Clear Node Colors**. See Clearing Node Colors.	Clears all node colors
Nodes	Reciprocated Links Analytic	**Highlight Nodes** check box sets Color to red for nodes with reciprocated links
Nodes	Tiered Layout	Colors nodes by Tier level and unrelated

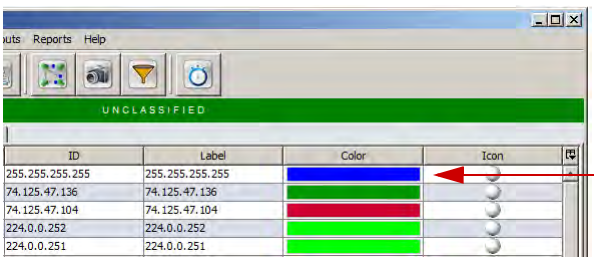
Setting Node Colors

(U) To set the color of one or more nodes:

1. Do one of the following:

   - (U) Double-click the **Color** swatch of a node in the Controller window and go ahead to Figure 4-14.

Figure 4-12: (U) Color swatches in Node Table



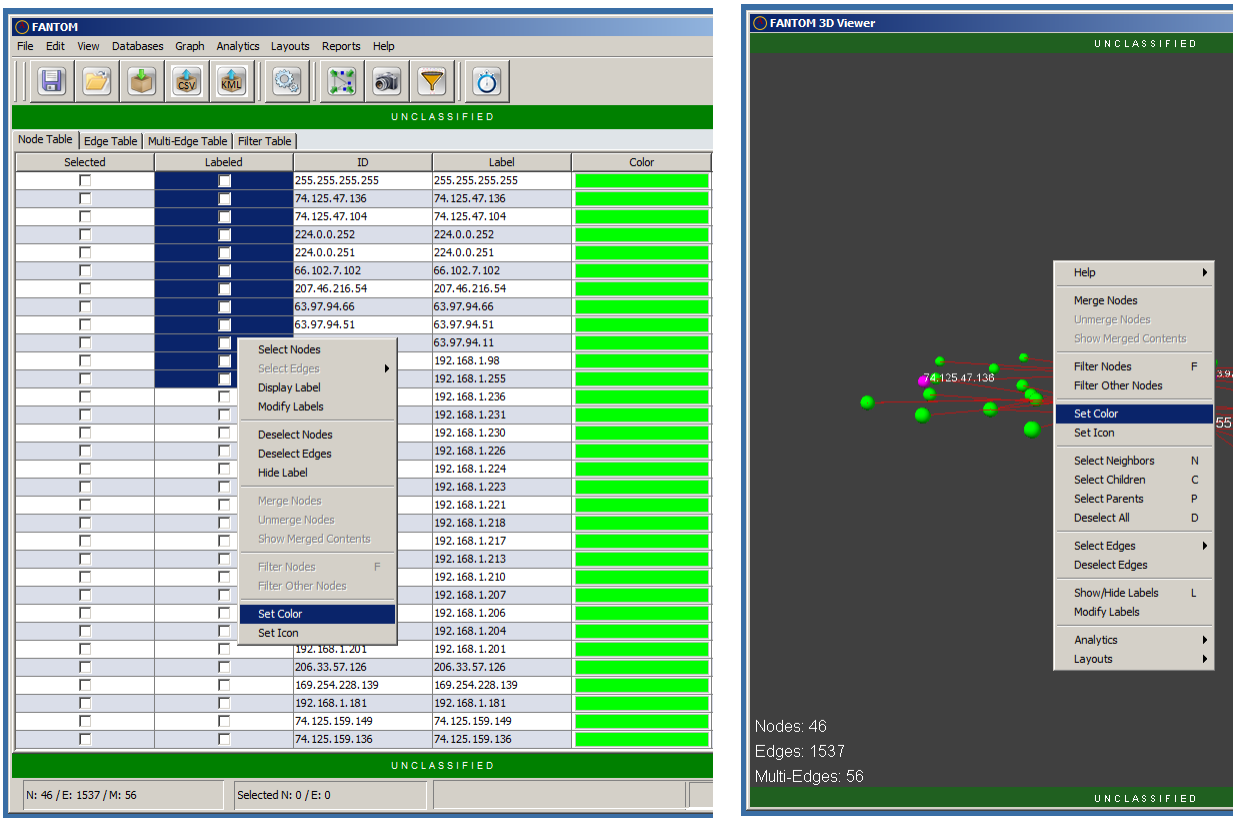
Each node has a Color swatch that you can set; this color is applied to the node in the 3D Viewer table and is visible if the node is deselected

Or:

- (U) Select one or more nodes or highlight rows in any column of the Node Table to identify the nodes whose color you want to set.

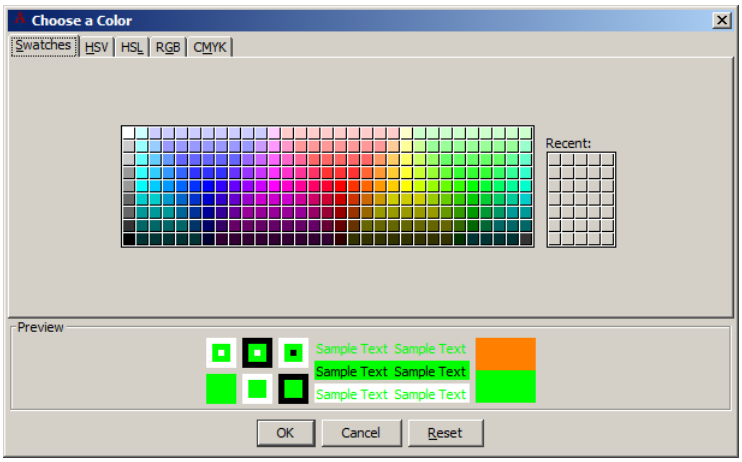
2. (U) Right-click in either window and choose **Set Color**.

Figure 4-13: (U) Right-click to display the shortcut menu



(U) The Choose a Color dialog box displays (Figure 4-14).

Figure 4-14: (U) Choose a Color dialog box – Swatches pane



3. (U) Select a color from any of the color model tabs (**Swatches**, **HSV**, **HSL**, **RGB**, or **CMYK**).

   (U) In addition to the Swatches pane, FANTOM provides the HSV (Hue, Saturation, Value), HSL (Hue, Saturation, Lightness) (Figure 4-15) RGB (Red, Green, Blue) (Figure 4-17), and CMYK (Cyan, Magenta, Yellow, Black) tabs if you prefer setting the node color using one of these color selector options.

Figure 4-15: (U) Choose a Color dialog box – HSV tab

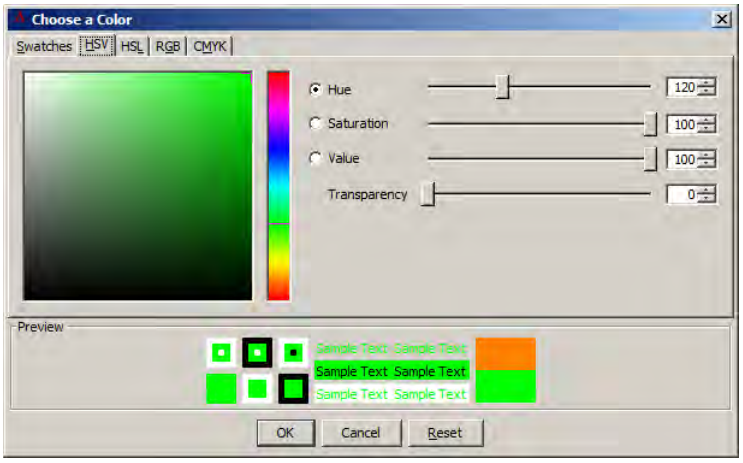


Figure 4-16: (U) Choose a Color dialog box – HSL tab

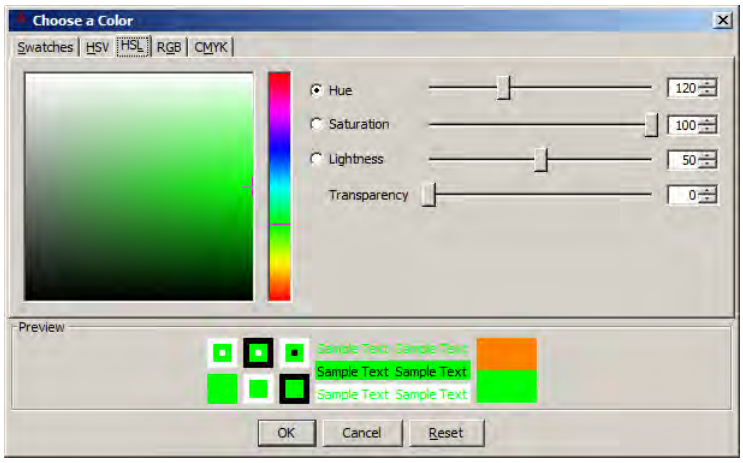


Figure 4-17: (U) Choose a Color dialog box – RGB tab

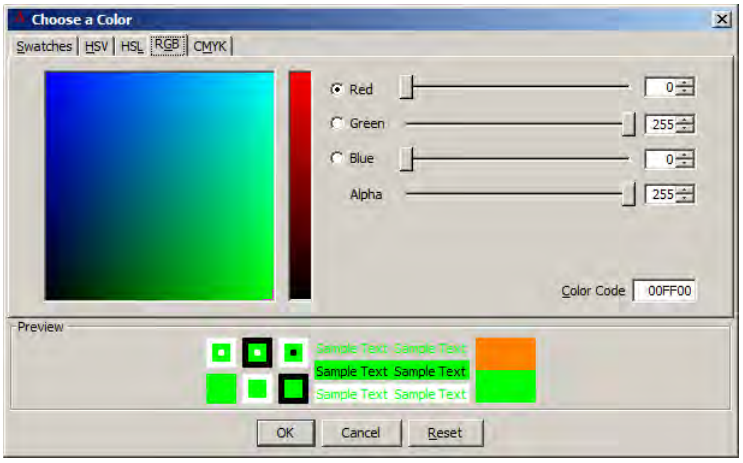
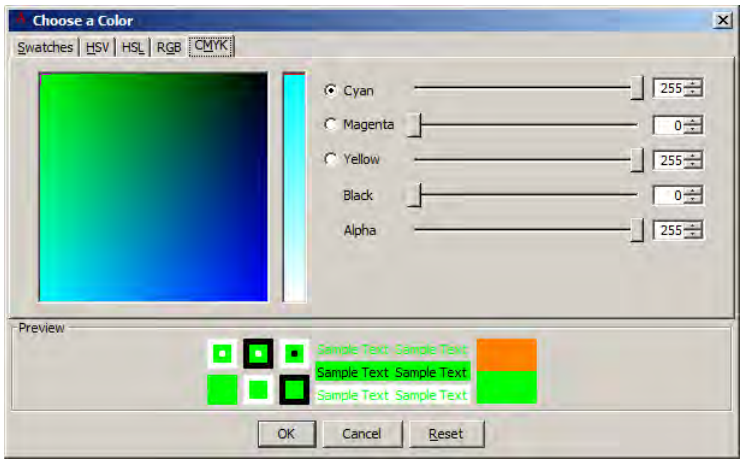


Figure 4-18: (U) Choose a Color dialog box – CMYK tab

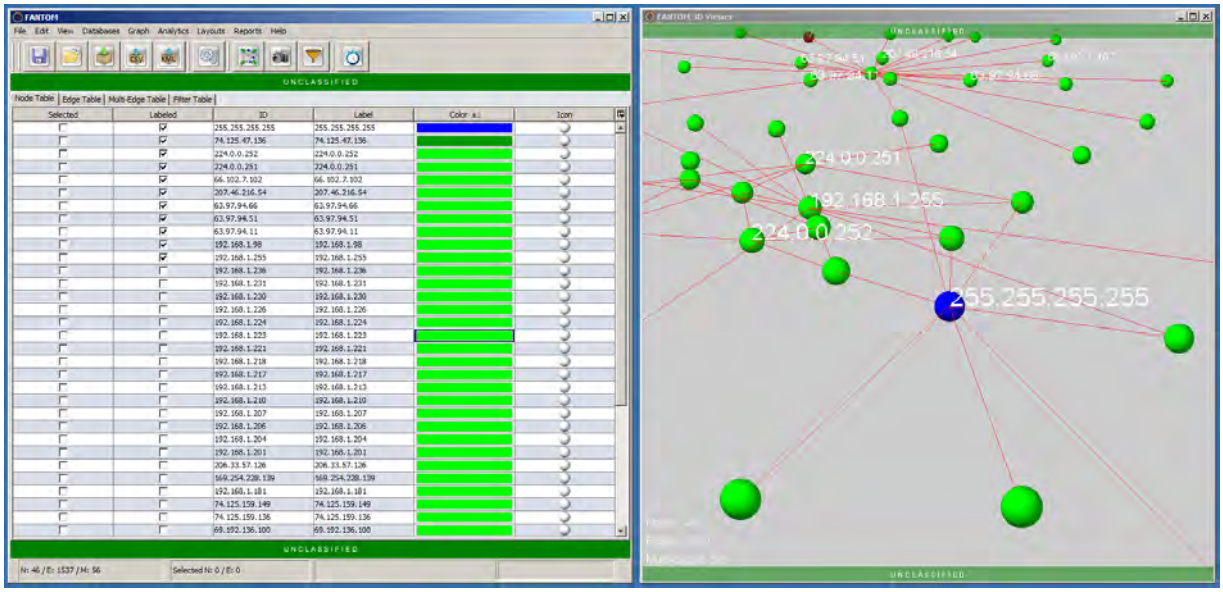


4. (U) Click **OK**.

   (U) FANTOM adds the color you selected to the **Color** swatch of each highlighted or selected node. It also applies the color to node icons in the 3D Viewer window.

5. (U) Deselect any selected nodes to reveal the color you set.

Figure 4-19: (U) Example of a colored node



Clearing Node Colors

To clear node colors, choose **Graph** > **Clear Node Colors**.

Labeling a Node

(U) The fastest way to show the label for a node is to select the **Labeled** check box for that node in the Node Table. You can also show labels for multiple nodes.

Note: You can edit the text of a node's Label. See "Editing a Node Label" on page 6-19.

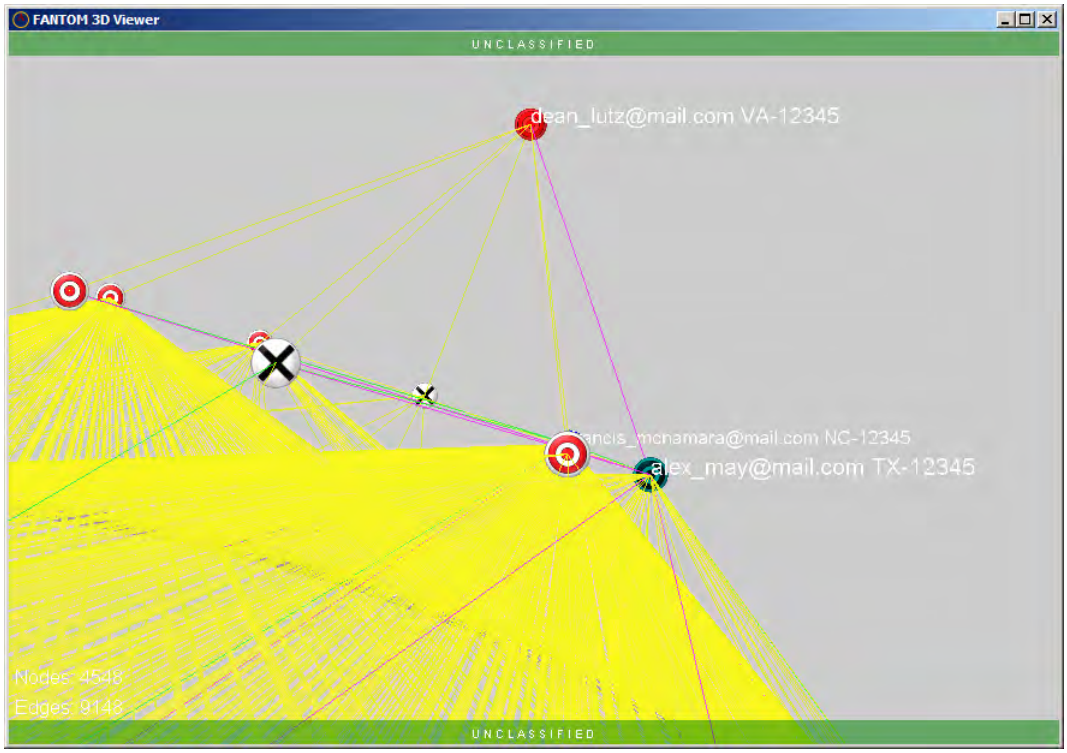
(U) To show labels for multiple nodes:

1. (U) Select one or more nodes or highlight rows in any column of the Node Table to identify the nodes whose labels you want to show in the 3D Viewer window.

2. (U) Right-click in either window and choose **Display Label** (Controller window) or **Show/Hide Labels** (3D Viewer window).

   (U) FANTOM places the node's Label by the node in the graph, as shown in Figure 4-20.

Figure 4-20: (U) Show node labels



Configuring Labels

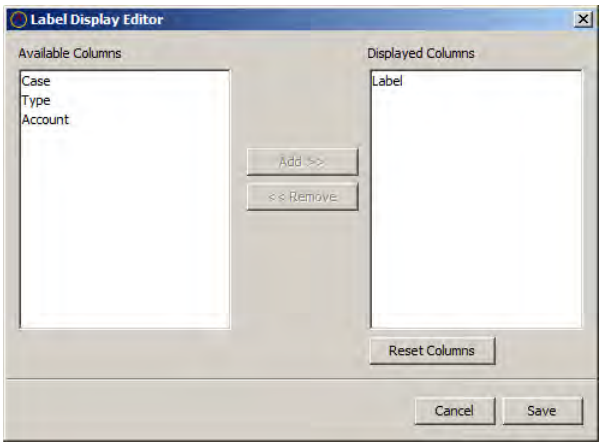
(U) FANTOM lets you define which Node Table column values should display in node labels in the 3D Viewer window.

(U) **To configure labels:**

1. (U) Right-click anywhere in the 3D Viewer window to display the shortcut menu.
2. (U) Choose the **Modify Labels** command.

   (U) The Configure Labels dialog box displays.

Figure 4-21: (U) Configure Labels dialog box



3. (U) Do any combination of the following:

   - (U) Select one or more of the titles in the **Available Columns** list and click the **Add >>** button.
   - (U) Select one or more of the titles in the **Displayed Columns** list and click the **<< Remove** button.
   - (U) Click the **Reset Columns** button to only display the Label value.

Note: (U) To rearrange columns displayed in labels, you can remove all the columns and then add them in the order you want them to display. To do this, click the Displayed Columns list, select all (press CTRL+A), and then click **<< Remove** to move them to the **Available Columns** list. Then, add the column titles in the order you prefer.

4. (U) Click **Save** when you finish.

   (U) FANTOM changes the label format to include the columns of data you selected.

Clearing Graph Information

(U) To clear the graph choose **Graph** > **Clear Graph** and click **Clear Graph**.

Navigating in FANTOM

(U) FANTOM offers several ways to move around in the Controller and 3D Viewer windows.

(U) After you access data, the Controller window displays information about that data in tables in the Node Table, Edge Table, and Multi-Edge Table tabs. The same information is shown graphically in the 3D Viewer window.

(U) This chapter explains the following navigation options:

- (U) Zooming the Camera In and Out
- (U) Rotating the Graph
- (U) Resetting the Graph View
- (U) Centering on the Graph
- (U) Zooming In and Out on Graphs in Report Windows

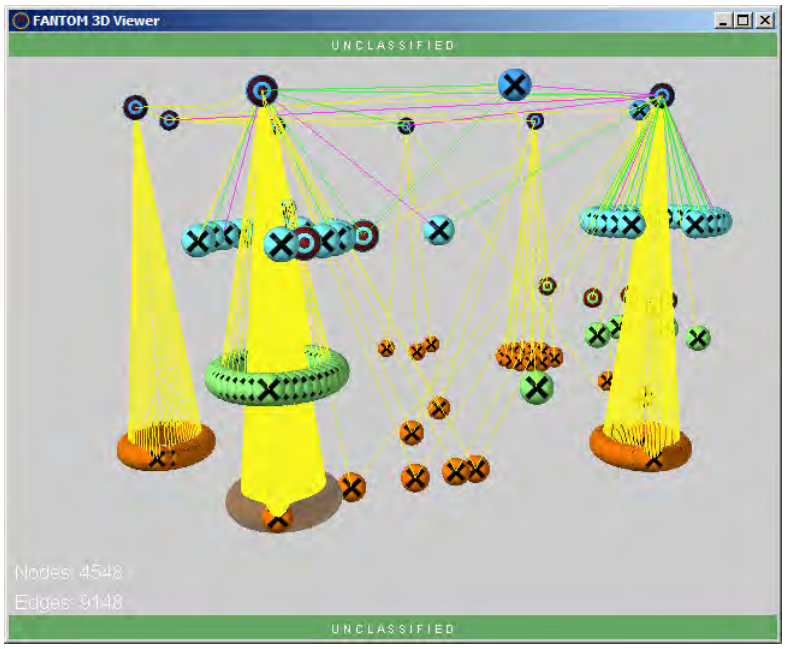
Zooming the Camera In and Out

(U) To zoom the camera in, scroll the small middle mouse button forward.

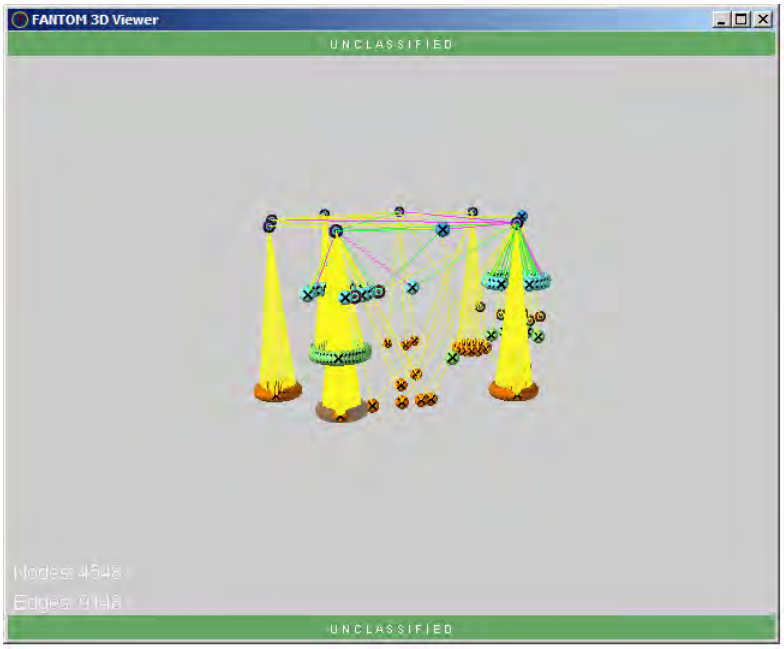
(U) To zoom the camera out, scroll the middle mouse button back.

(U) Press the ALT key while scrolling the middle mouse button forward or back to zoom in or out on the selected nodes in the 3D Graph Viewer window.

Figure 5-1: (U) Zooming the Camera in and out



Zoom In (scroll forward)



Zoom Out (scroll back)

Changing the Graph Orientation

(U) In FANTOM, you can rotate the graph in three dimensions (3D) turning it 360-degrees in the 3D Viewer window. You can also reset the orientation.

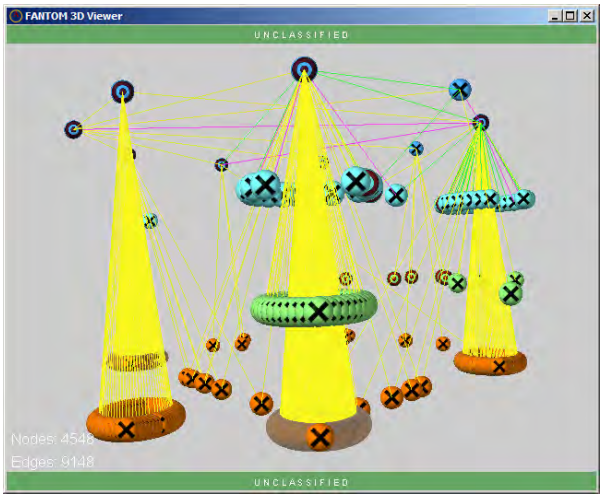
Rotating the Graph

(U) To rotate the graph, hold down the middle mouse scroll wheel and then drag the mouse in any direction.

Resetting the Graph View

(U) To reset the Graph View to its original position, click the **Reset Graph View** tool button ( ) (or choose **View** > **Reset Graph View)**.

Figure 5-2: (U) Resetting the Graph View example



Starting position after rotating results of Tiered Layout

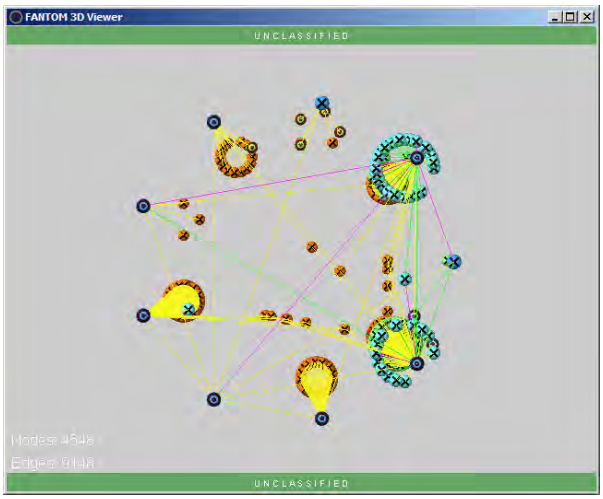
Reset the Graph View moves to the original orientation while retaining the layout

Centering on the Graph

(U) To center on the graph, click the **Center on Graph** tool button ( ) (or choose **Graph** > **Center on Graph**).

Figure 5-3: (U) Centering on the graph

Starting position after resetting the Graph View



Center on Graph puts the graph in the center of the window

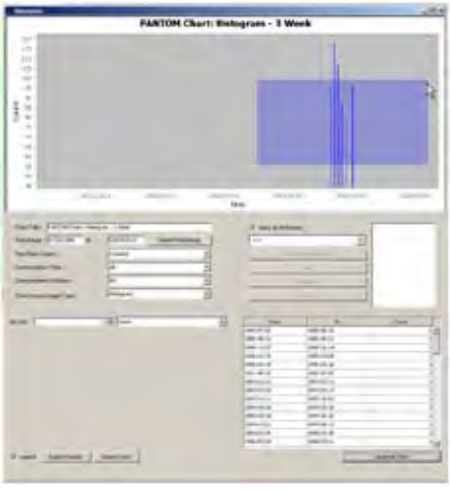
Zooming In and Out on Graphs in Report Windows

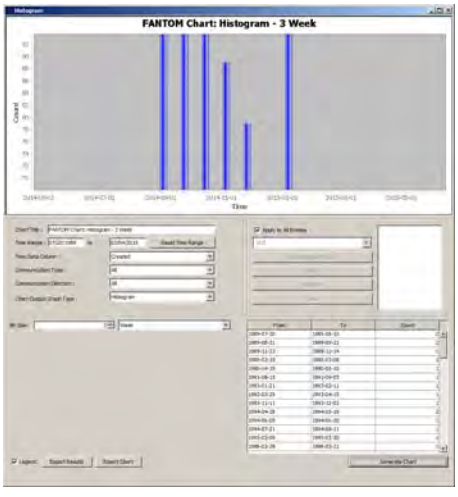
(U) While working with a Report, you can zoom in or out on the graph at the top of the dialog box.

(U) To zoom in, drag right across the graph.

(U) To zoom out, drag left across the graph.

Figure 5-4: Zooming in and out





Working with Nodes, Edges and Multi-Edges

(U) FANTOM lets you work with nodes, edges, and multi-edges as explained in the following topics:

Selecting Nodes

(U) You can select nodes in the following ways:

- (U) Selecting Individual Nodes in the Controller Window
- (U) Selecting Multiple Nodes in the Controller Window
- (U) Selecting Nodes by Relationship

Selecting Individual Nodes in the Controller Window

(U) You can easily select individual nodes in the Controller window.

(U) To select individual nodes in the Controller window:

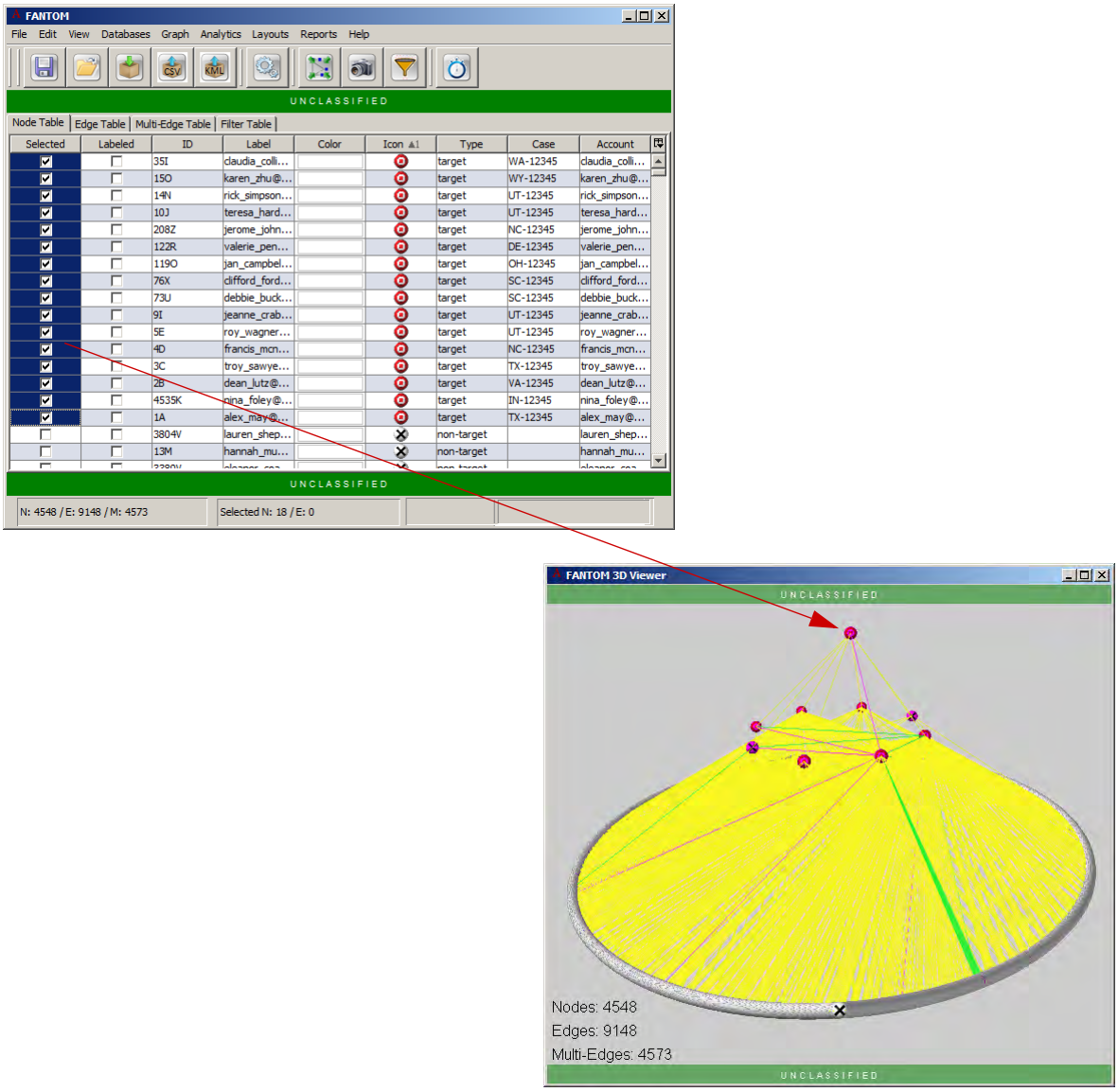
1. (U) Select the Controller window and make sure the Node Table tab is active.
2. (U) Click the **Selected** check box (▣) beside a node to select it.

   (U) FANTOM fills the **Selected** check box with a smaller black box and places a red selection rectangle around the node in the 3D Viewer window (Figure 6-1).

   (U) Selecting nodes in the Controller window works best when you want to select nodes based on attributes that are not easily seen in the graph—such as when you want to select a node by name in a large graph.

Tip: (U) You can sort the Node Table by clicking any of the column titles. This can make it easier to locate particular nodes in large tables.

Figure 6-1: (U) Selecting nodes in a graph



Selecting Multiple Nodes in the Controller Window

(U) In some cases, selecting multiple nodes may be easier using the Controller window table. After you select entries in the Node, Edge, or Multi-Edge tables in the Controller window, you can **Copy** the information. Then, **Paste** it from the Clipboard into another application, such as a spreadsheet or word processing document.

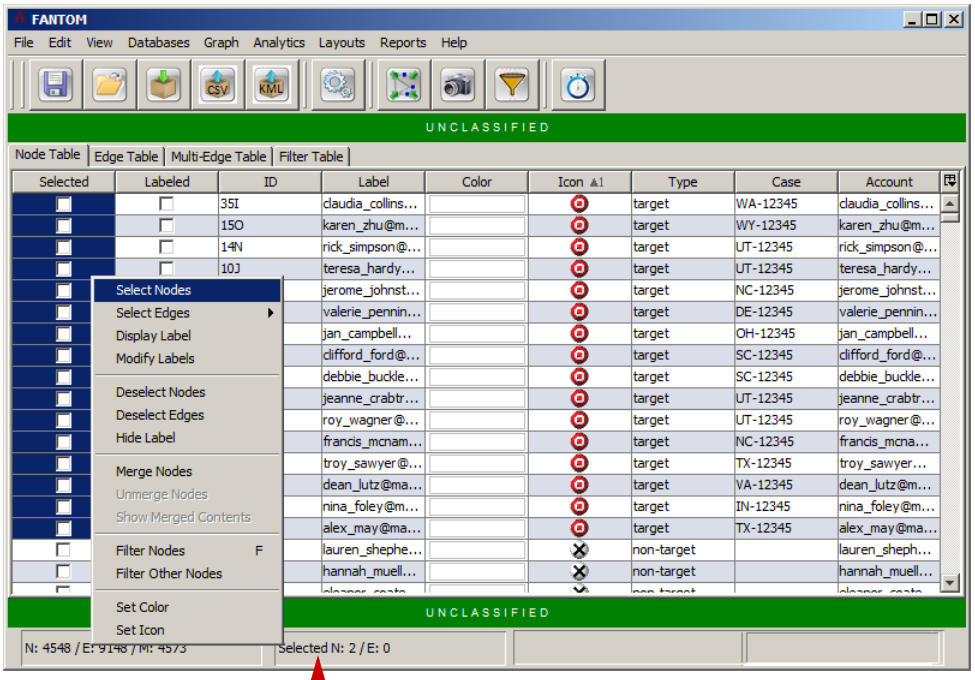
(U) To select multiple nodes in the Controller window:

1. (U) Click the Controller window to bring it to the front, if necessary, and verify that the **Nodes** tab is at the front.

2. (U) Do one of the following:

   - (U) Click the **Selected** check box beside a node to fill it with a check mark.
   - (U) Drag a selection rectangle around one or more rows to select, right-click the mouse button, and choose the **Select** command.

Figure 6-2: (U) Selecting multiple nodes in the Controller window



FANTOM displays the total number of currently selected items in the status bar near the bottom of the window

Selecting Nodes by Relationship

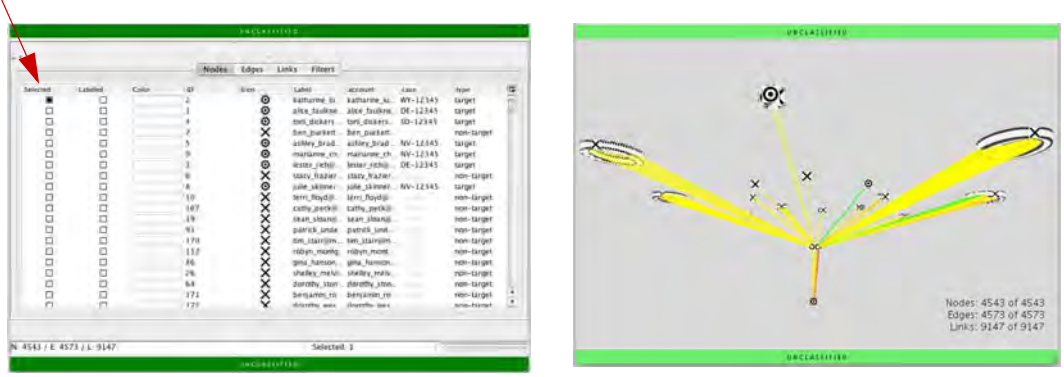
(U) FANTOM lets you select nodes based on their relationship to the currently selected nodes: parents, children, or neighbor nodes.

Selecting the Parents of Selected Nodes

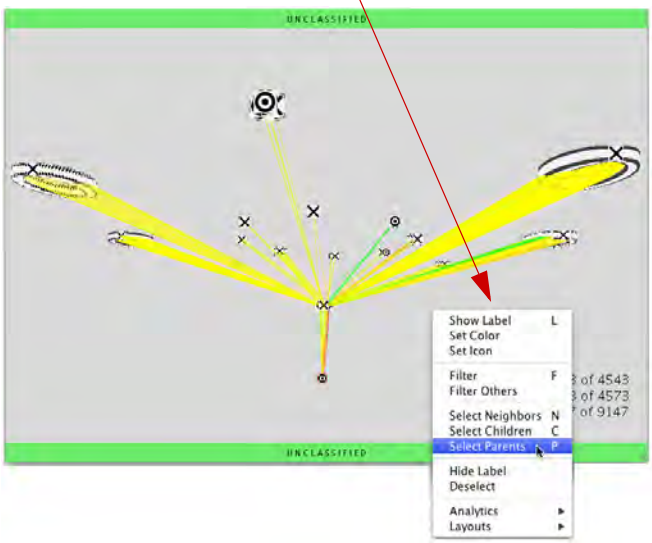
(U) Press the P key to select parents of selected nodes. A *parent* is a node at the remote end of an in-directed connection from a given node. For example, if the graph represents communications, a parent of node A, is one that sends a communication to node A.

Figure 6-3: (U) Example of selecting Parent nodes of the currently selected nodes

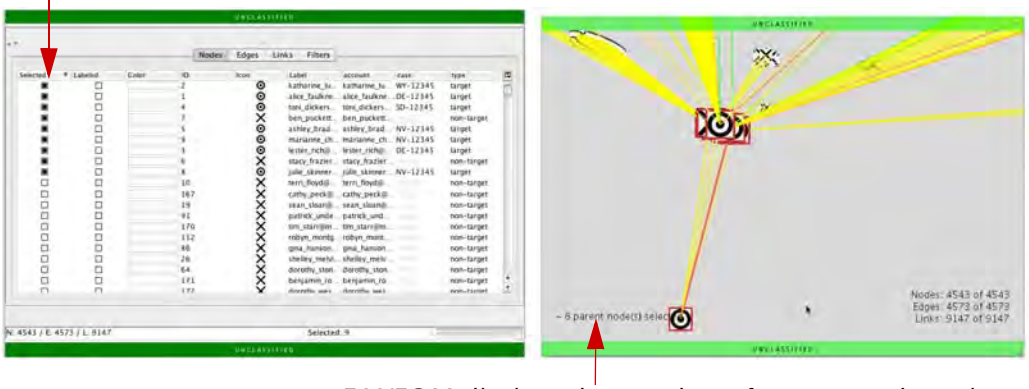
1. Select one or more nodes in the Controller window



2. Click anywhere in the background of the 3D Viewer window to make it active, and then press the P key (or right-click and choose **Select Parents**)



3. Click the **Selected** column title twice to bring all the selected nodes to the top of the list



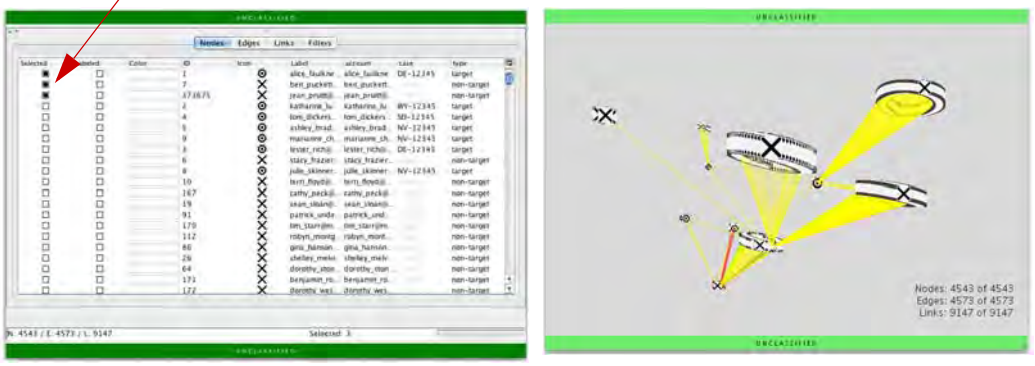
FANTOM displays the number of parent nodes selected

Selecting the Children of Selected Nodes

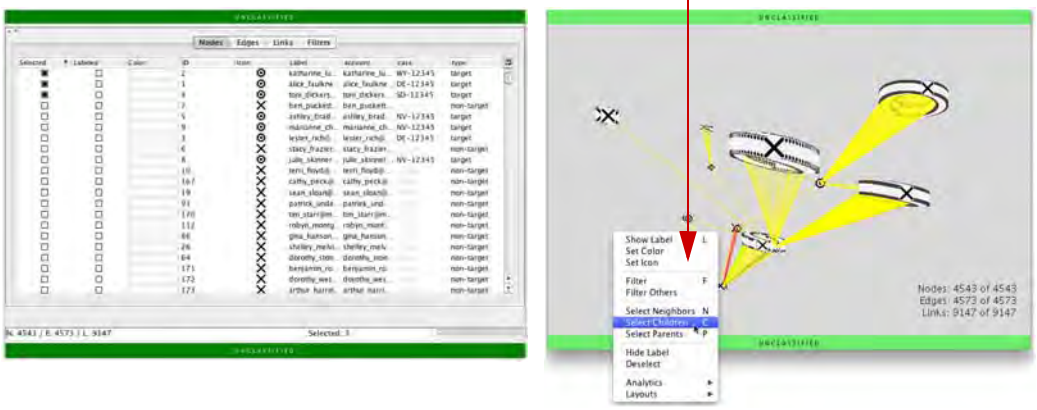
(U) Press the C key to select children of selected nodes. A *child* is a node at the remote end of an out-directed connection from a given node. For example, if the graph represents communications, then a child node of node A, is one that receives a communication from node A. Parent and child are inverse relations, so if A is a parent of B, then B is a child of A.

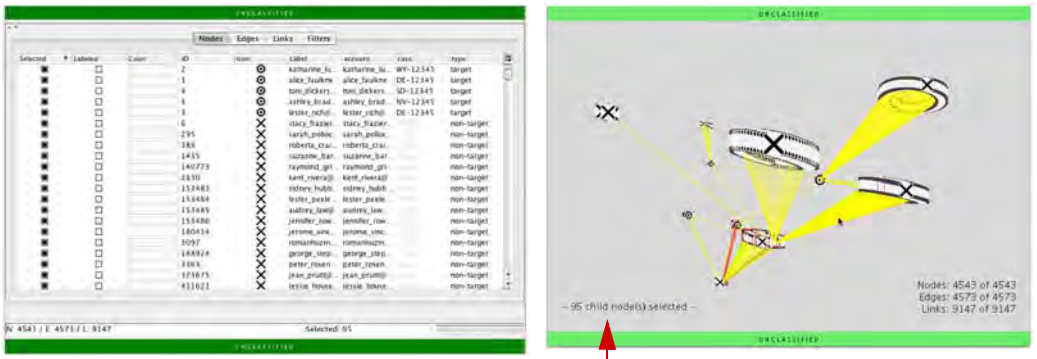
Figure 6-4: (U) Selecting Children nodes of the currently selected nodes

1. Select one or more nodes in the Controller window



2. Click anywhere in the background of the 3D Viewer window to make it active, and then press the C key (or right-click and choose **Select Children**)





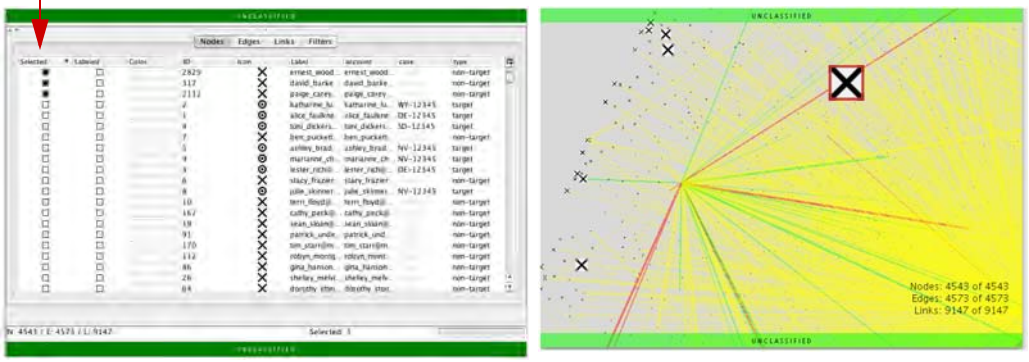
FANTOM displays the number of children nodes selected

Selecting the Neighbors of Selected Nodes

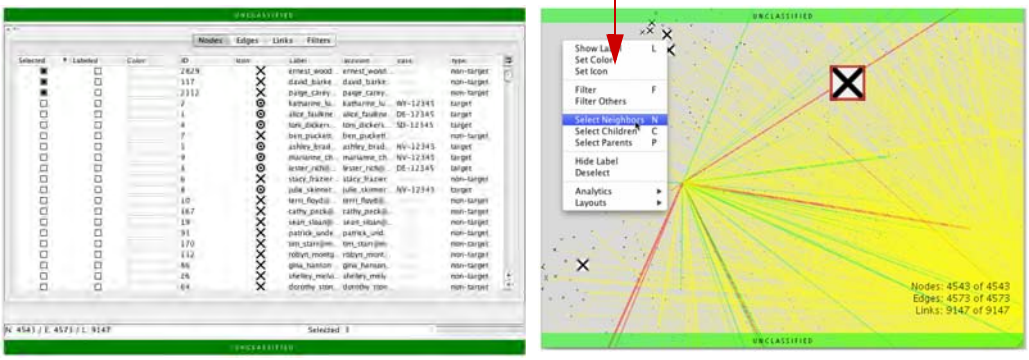
(U) Press the N key to select neighbors of the selected nodes. A *neighbor* is any connecting node, including parents and children.

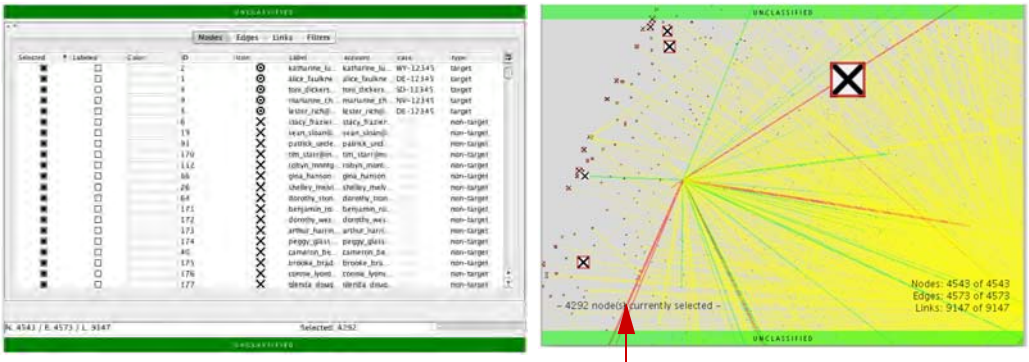
Figure 6-5: (U) Selecting Neighbor nodes of the currently selected nodes

1. Select one or more nodes in the Controller window



2. Click anywhere in the background of the 3D Viewer window to make it active, and then press the N key (or right-click and choose **Select Neighbors**)





FANTOM displays the total number of selected nodes

Selecting Only One Data Set's Nodes

(U) You can import multiple data sets while working with FANTOM. You may want to separate these data sets as you import one after another so it is easier to select or move all the nodes in one data set without affecting others.

(U) To select only one data set's nodes:

1. (U) Import the first data set.
2. (U) Click anywhere in the background of the 3D Viewer window.
3. (U) Zoom out until you can see all the nodes in the data set, if needed.
4. (U) Hold down the SHIFT key while dragging a selection rectangle around the nodes you want to select.
5. (U) Hold down the ALT key while dragging all the selected nodes away from the center of the 3D Viewer window.
6. (U) Import the next data set.
7. (U) Repeat steps 2 through 6 as you open more data sets, moving the data set nodes to different locations.

Selecting Nodes from a Bulk List

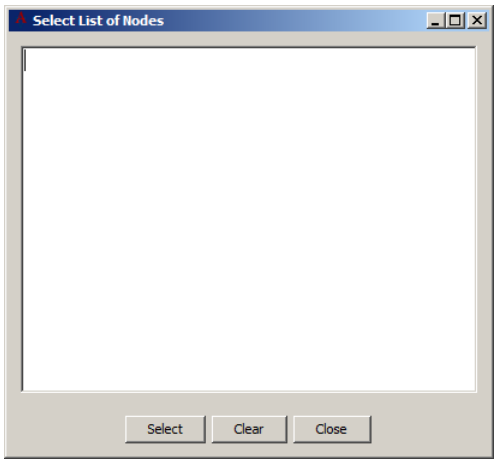
(U) FANTOM offers a Bulk Selection command where you can paste a list of email addresses (which must be found in the **Label** column of the Controller table), and then select the corresponding nodes in an active data set.

(U) To select nodes in FANTOM from a bulk list:

1. (U) Select a list of email addresses in an external file and copy them to the clipboard.
2. (U) Start FANTOM and import a data set or open a session.
3. (U) Choose the **Edit** > **Bulk Selection** command.

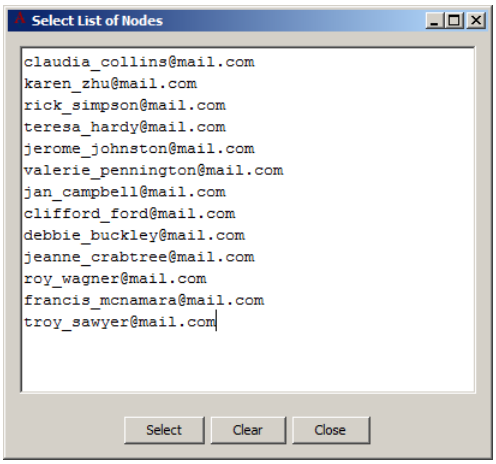
   (U) The Select List of Nodes dialog box displays (Figure 6-6).

Figure 6-6: (U) Select List of Nodes dialog box



4. (U) Click inside the large text box so the cursor displays.
5. (U) Paste (CTRL+V) the data from the clipboard.

Figure 6-7: (U) Example of pasted data in the Select Nodes dialog box



6. (U) Click **Select**.

   (U) FANTOM selects all nodes with a label matching one of the values you supplied.

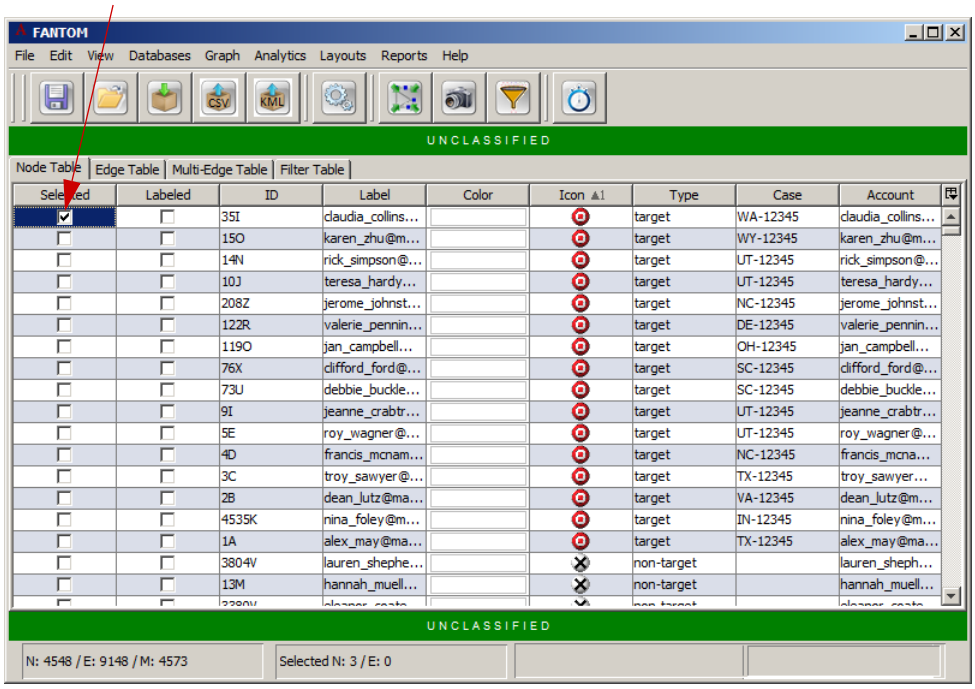
Deselecting Nodes

(U) To deselect one node:

1. (U) Click the Controller window to bring it to the front.
2. (U) Click the **Selected** check box in the row of the node you want to deselect (Figure 6-8).

(U) The **Selected** check box toggles between selecting and deselecting the related node.

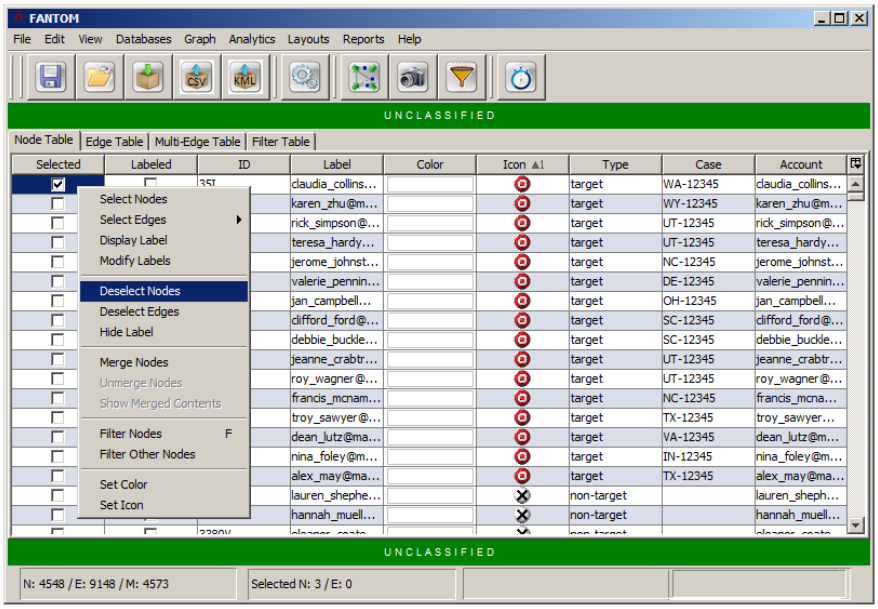
Figure 6-8: (U) Selected check box in the Controller window



(U) To deselect multiple nodes in the Controller window:

1. (U) Click the Controller window to bring it to the front.
2. (U) Drag up or down to highlight one or more selected nodes that you want to deselect.
3. (U) Right-click the mouse button and choose **Deselect Nodes** (Figure 6-9).

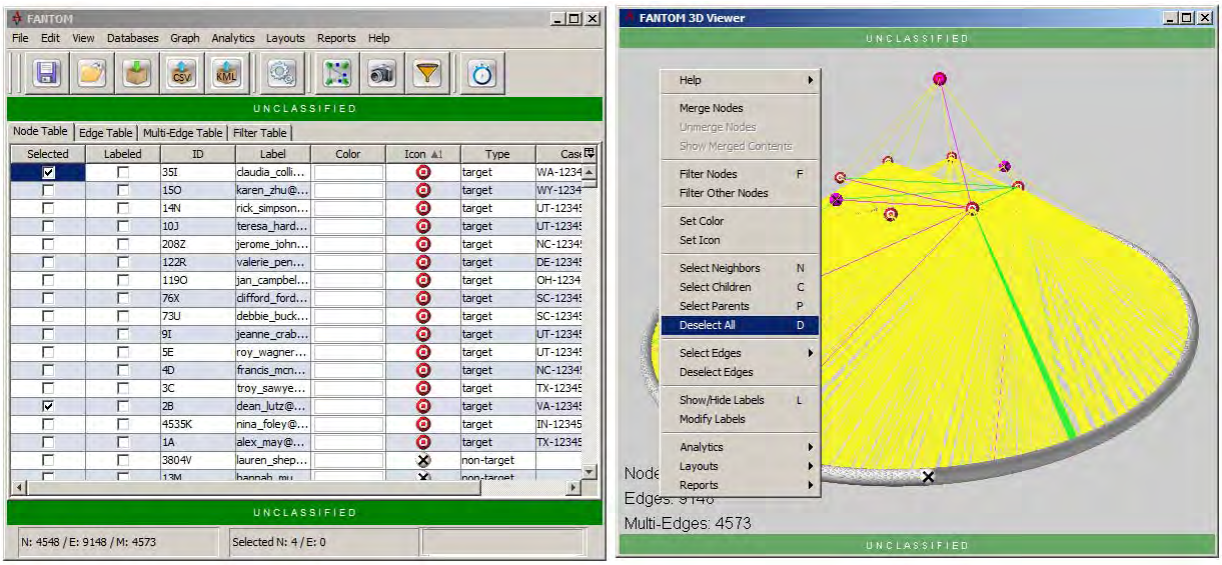
Figure 6-9: (U) Deselecting nodes in the Controller window



(U) To deselect all nodes in the 3D Viewer window:

1. (U) Click the 3D Viewer window to bring it to the front.
2. (U) Drag a selection rectangle around the red node icons that you want to deselect.
3. (U) Do one of the following:
   - (U) Press the D key.
   - (U) Right-click the mouse button and choose **Deselect All**.

Figure 6-10: (U) Deselecting nodes in the 3D Graph Viewer window



Selecting Edges or Multi-Edges

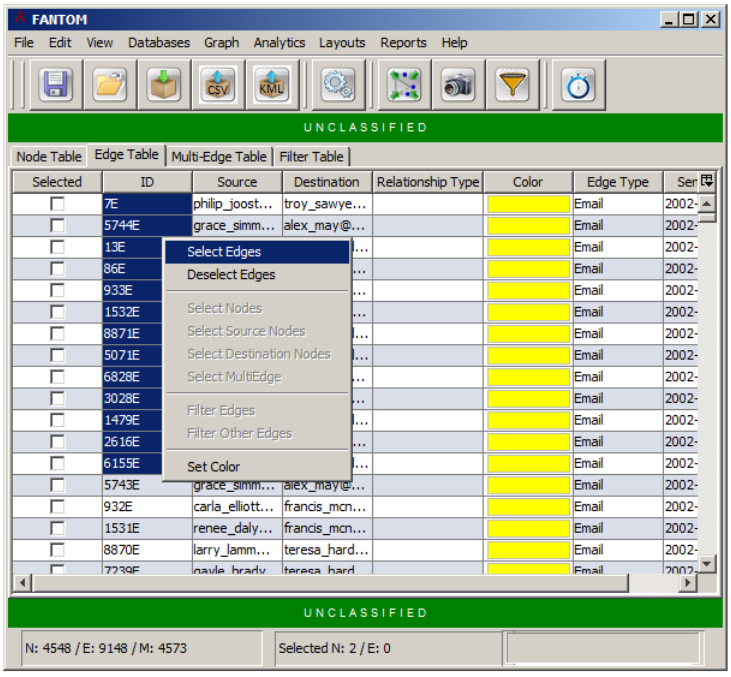
(U) You can select edges or multi-edges in the Controller window table.

(U) To select edges or multi-edges in the Controller window:

1. (U) Click the **Edge Table** or **Multi-Edge Table** tab to bring it to the front.
2. (U) Do one of the following:
   - (U) Click the **Selected** check box beside the edge or multi-edge.

     (U) FANTOM fills the check box with a smaller black box.
   - (U) Drag a selection rectangle around one or more rows to select, right-click the mouse button, and choose the **Select Edges** command (Figure 6-11).

Figure 6-11: (U) Selecting Edges or Multi-Edges in the Controller table

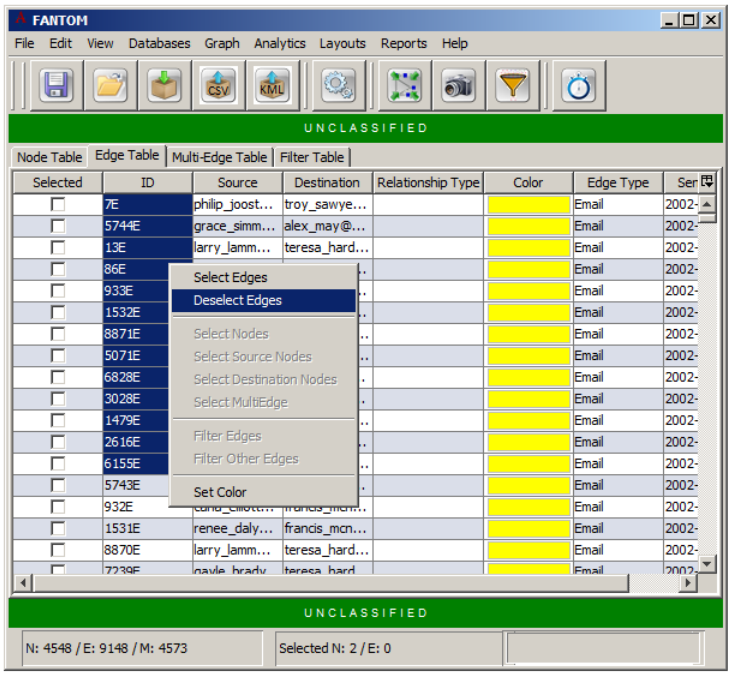


Deselecting Edges or Multi-Edges in the Controller window

(U) To deselect edges or multi-edges in the Controller window:

1. (U) Click the **Edge Table** or **Multi-Edge Table** tab to bring it to the front.
2. (U) Do one of the following:
   - (U) Click the **Selected** check box beside a selected edge or multi-edge row.
   - (U) Drag a selection rectangle around one or more rows to select, right-click the mouse button, and choose the **Deselect Edges** command (Figure 6-12).

Figure 6-12: (U) Deselecting Edges or Multi-Edges in the Controller table

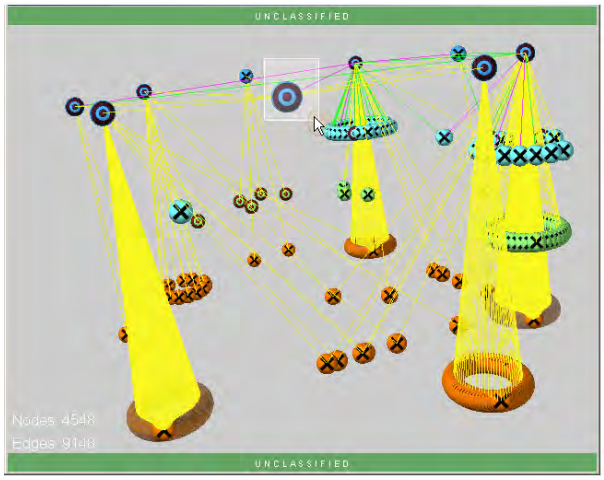


Moving Nodes in a Graph

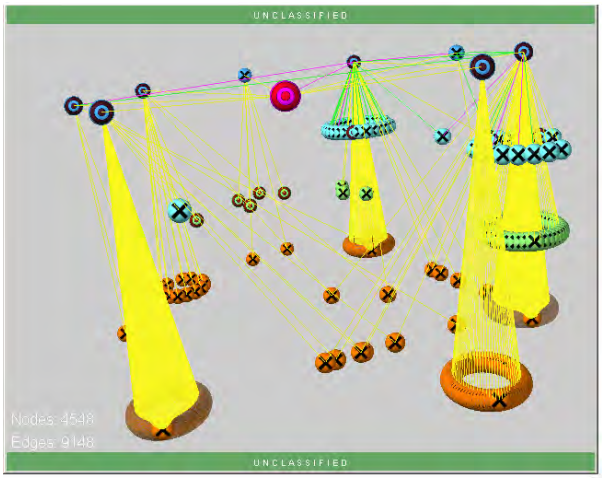
(U) To move nodes in a graph:

1. (U) Hold down the SHIFT key while dragging a selection rectangle to select one or more nodes.
2. (U) Hold down the CTRL key while dragging to move the selected nodes outward until the connections become clear.

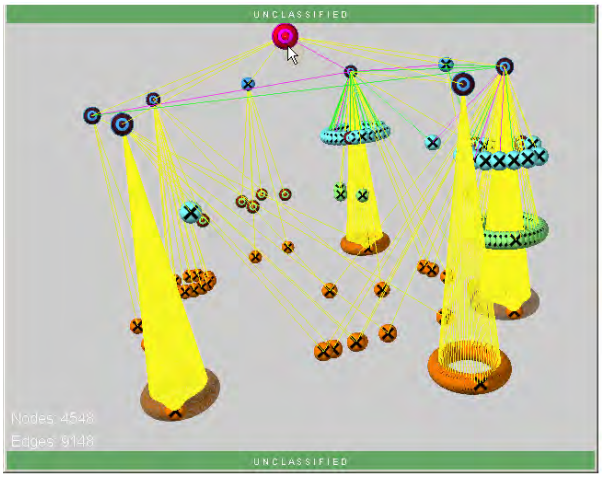
Figure 6-13: (U) Moving nodes in the 3D Viewer window



Hold down the SHIFT key while dragging to enclose nodes in a selection rectangle



When you release the mouse button, FANTOM highlights the nodes with the current Selected Node Color

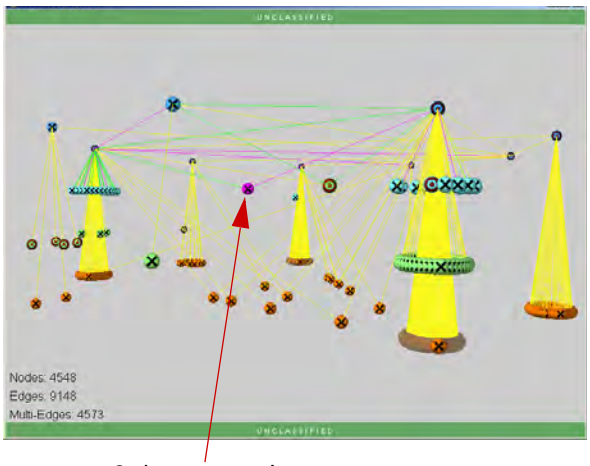


Hold down the CTRL key while dragging to move the selected nodes elsewhere

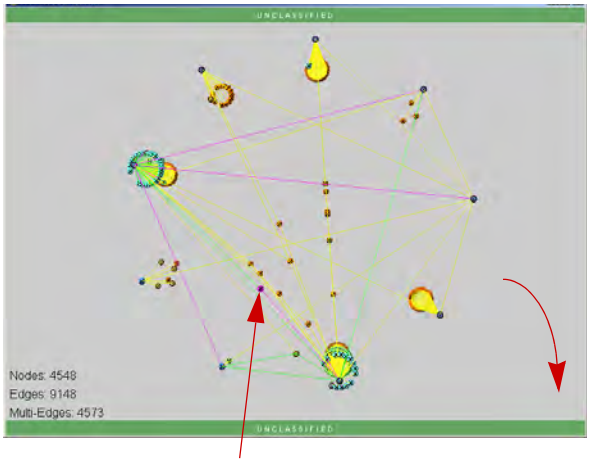
Moving Nodes Across 3D Space

(U) While working with a graph, you may want to move one or more nodes across 3D space. For example, you might want to drag nodes closer to the foreground while leaving all the other nodes in place. The simplest way to do this is to rotate the graph to the "top" or "bottom;" drag the selected nodes up, down, left, or right; and then rotate the graph back to the side.

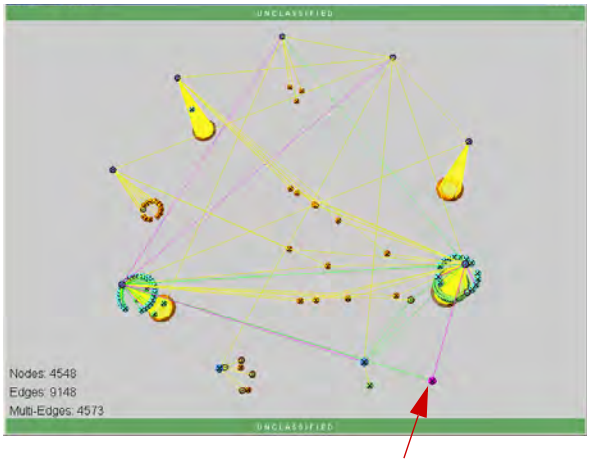
Figure 6-14: (U) Moving nodes in 3D space in the 3D Viewer window



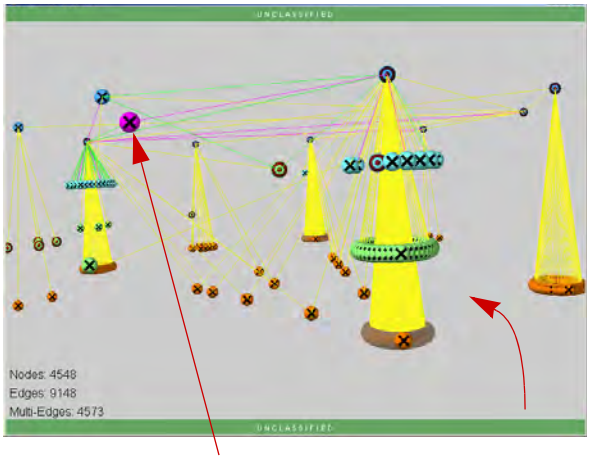
Select a node that you want to move forward or backward in 3D space



Rotate the graph 90 degrees to view the top or bottom



Hold down the CTRL key and drag the selected node up, down, left, or right



Rotate the graph back 90 degrees

Merging Nodes

(U) You can specify nodes to merge at the end of the import or conduit query process or select nodes to merge at any time. FANTOM also lets you nest one merged node within another merged node.

Tip: (U) After you merge selected nodes, save the session.

Note: (U) Even if you subsequently filter all the nodes in a merged node, the merged node itself still displays. You can see this effect by merging nodes and then going to the Filter table and selecting the default filter created when you import a data set.

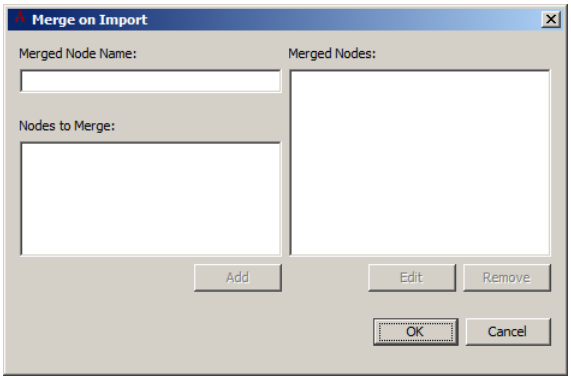
Merging Nodes During a Query or Import

(U) **To merge on query or import:**

1. (U) Verify that the Merge dialog box will display during a query or import:
   a. Choose **Edit** > **Preferences Manager**.
   b. Choose the **General Importer** plug-in.
   c. Verify that the **Show Merge Dialog** check box is selected.
2. (U) Perform the query or import.

   (U) After you complete settings in the Classification dialog box and click **OK**, FANTOM displays the Merge on Import dialog box.

   Figure 6-15: (U) Merge on Import dialog box



3. (U) Type a name for the node in the **Merged Node Name** text box.
4. (U) Type or paste a list of nodes in the **Nodes to Merge** text box and click the **Add** button.
5. (U) Repeat step 4 if desired until you have specified all the nodes to merge.

6. (U) Click **OK**.

   (U) FANTOM displays the information in the Controller and 3D Graph Viewer windows. Merged nodes are easy to identify in FANTOM tables and graph because they use a traffic merge icon).

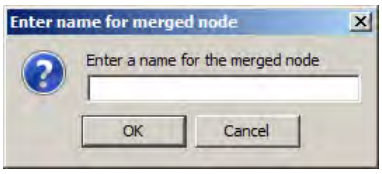
Merging Nodes in a Graph

(U) **To merge selected nodes in a graph:**

1. (U) Select nodes you want to group.
2. (U) Right-click in the 3D Viewer and choose the **Merge Nodes** command.

   (U) The Enter a Name for Merged Node dialog box displays.

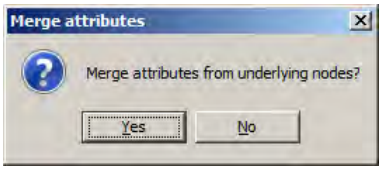
Figure 6-16: (U) Enter a Name for Merged Node dialog box



3. (U) Enter a name for the merged node and click **OK**.

   (U) FANTOM displays the Merge Attributes dialog box.

Figure 6-17: (U) Merge Attributes dialog box

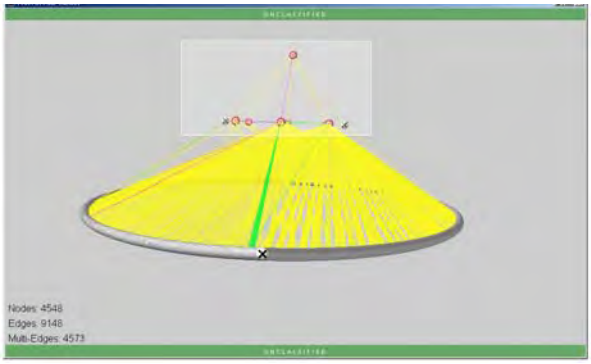


4. (U) Do one of the following:

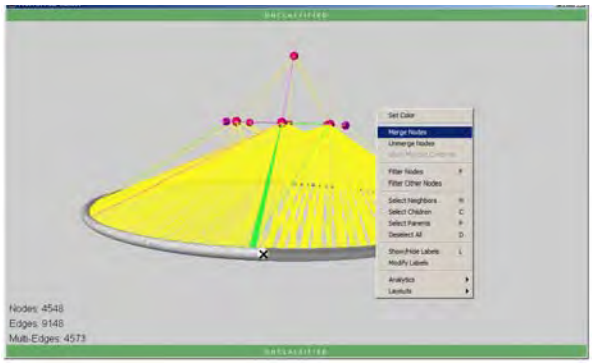
   - (U) Click **Yes** to cause FANTOM to combine all attributes with comma or semicolon separator characters in the Node Table columns while the selected nodes are merged.
   - (U) Click **No** to cause FANTOM not to combine all attributes in the Node Table columns.

   (U) Unless you have sorted the Node Table by the Icon column, FANTOM moves the merged node to the bottom of the Node Table.

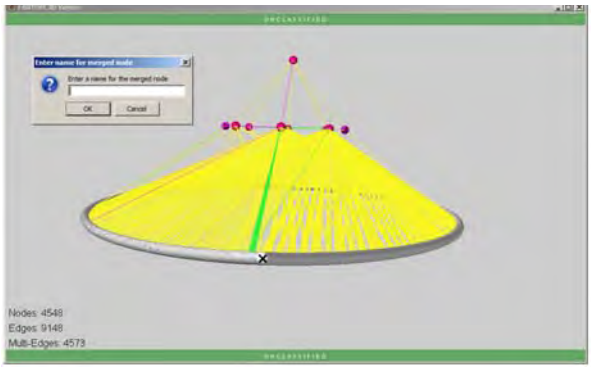
Figure 6-18: (U) Grouping nodes in the 3D Viewer window



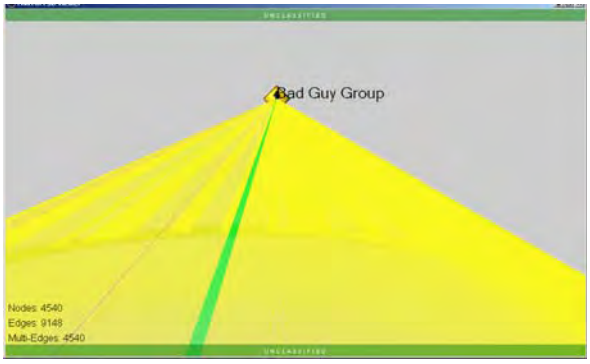
Press the SHIFT key and drag a selection rectangle around nodes to merge



Right-click the background of the 3D Viewer window and choose **Merge Nodes**



Type a name for the merged node



FANTOM displays the new group node with a Merged Node node icon ( )

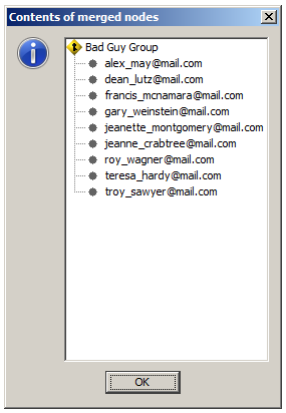
Viewing the Contents of a Merged Node

(U) To view the contents of a merged node:

1. (U) Select a merged node.
2. (U) Right-click the 3D Viewer window background and choose the **Show Merged Contents** command.

   (U) FANTOM displays the Contents of merged nodes dialog box (Figure 6-19).

Figure 6-19: (U) Contents of merged nodes dialog box



3. (U) Click **OK** when you finish viewing the list.

Tip: (U) You can click to select a name in the list, SHIFT+click to select a range, or press CTRL+A to select all, and then press CTRL+C to copy the list to the Clipboard. From there, you can paste it into a word processing, spreadsheet, or other document.

Unmerge a Merged Node

(U) **To unmerge a merged node:**

1. (U) Select a merged node.
2. (U) Right-click the background of the 3D Graph Viewer window and then choose the **Unmerge Nodes** command.

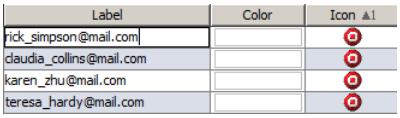
Editing a Node Label

(U) The **Label** column text in the Node Table is editable.

(U) **To edit a node label:**

1. (U) Double-click a Label value to edit that text.
2. (U) Use any of the standard text editing methods:
   - (U) Drag to select text to cut, copy, or delete.
   - (U) Click anywhere in the text string and begin typing.

Figure 6-20: (U) Double-click a Label value in the Node Table to edit it



Changing the Layout

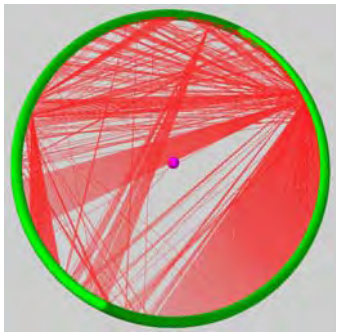
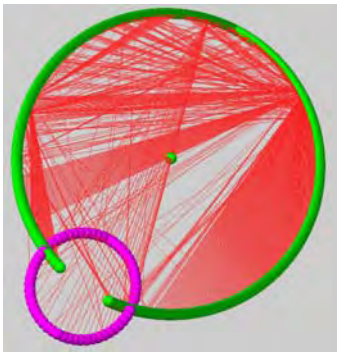
(U) FANTOM offers Layout commands that let you change the arrangement of nodes and edges in a graph in the 3D Viewer window. Layouts can help you see otherwise hidden relationships in the point-to-point connections.

- (U) Circle Layout
- (U) Disperser Layout
- (U) Flow of Values Layout
- (U) Force Directed Layout
- (U) Link Cluster Layout
- (U) Tiered Layout

Circle Layout

(U) The Circle Layout command displays the graph with nodes arranged in a circle, with connected nodes laid on top of one another. What you select before choosing the Circle Layout command determines what this FANTOM command does:

Table 1: (U) How selections affect the Circle Layout results (Enron.session)

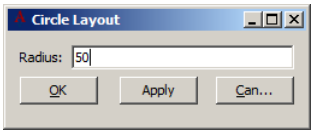
If you select:	FANTOM does this:	The results look like this:
No nodes or all nodes	Places all nodes in a circle of the radius you specify, stacking nodes if necessary	
One node	Moves all the other nodes into a circle of the size you specify around the single selected node	
More than one node	Creates a circle layout of the selected nodes, leaving unselected nodes alone	

(U) To run the Circle layout:

1. (U) Choose **Layouts** > **Circle**.

   (U) The Circle Layout dialog box displays (Figure 7-1).

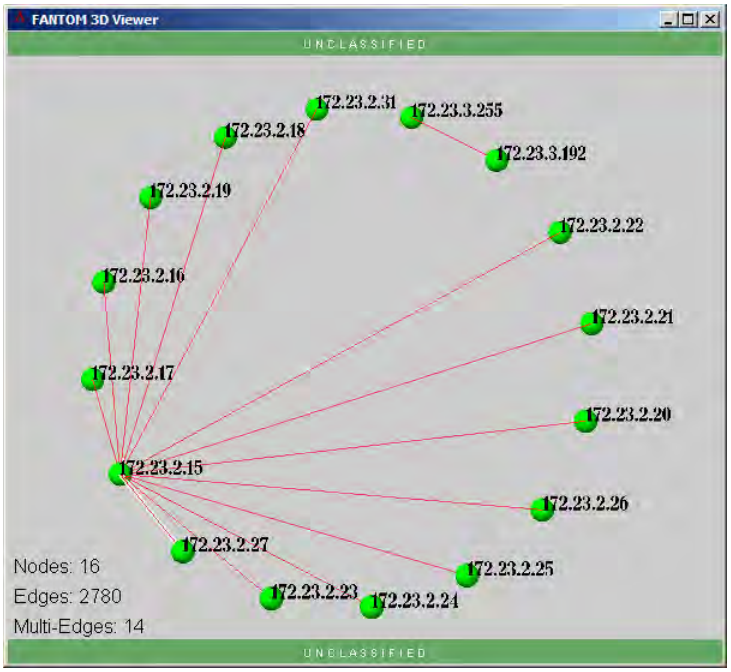
Figure 7-1: (U) Circle Layout dialog box



2. (U) Specify the **Radius** of the circle and click **Apply** or **OK**.

   (U) If you might want to adjust the circle size, click **Apply** to leave the dialog box open.

Figure 7-2: (U) Circle Layout with no selected nodes (Ether-S-IO-traffic_01.session)



Disperser Layout

(U) The Disperser command pushes outward disconnected nodes in the graph in a single layer. So the ones that remain in the center have the most connections. It is useful in order to fully expand the graph to more clearly show its separate components, if any exist. *Components* in a graph are separate groups of connected nodes.

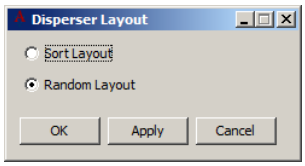
Note: (U) The Disperser Layout command works the same regardless of whether you select no, one, or multiple nodes before choosing the command.

(U) To run the Disperser layout:

1. (U) Choose **Layouts** > **Disperser**.

(U) The Disperser Layout dialog box displays (Figure 7-3).

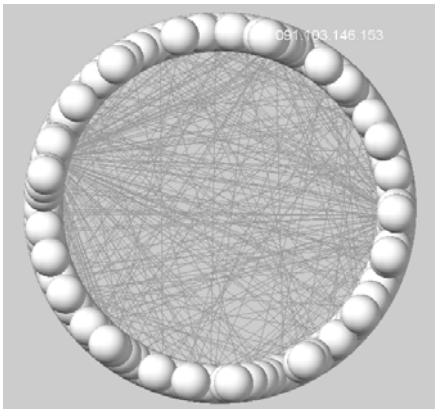
Figure 7-3: (U) Disperser dialog box



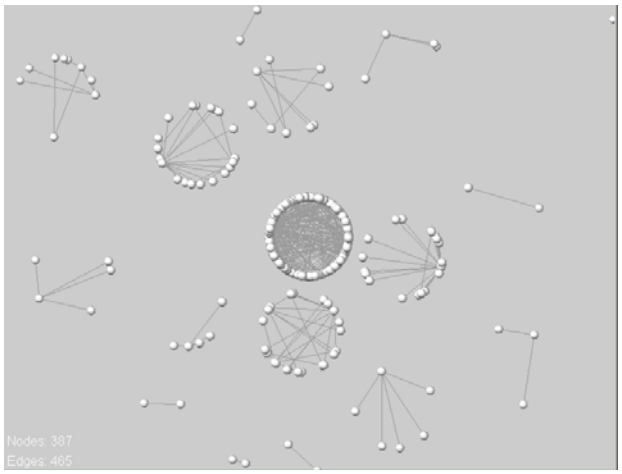
2. (U) Select **Sort Layout** or **Random Layout** and then click **Apply** or **OK**.

   - (U) **Random Disperser Layout** – In a Circular layout, connected nodes are laid on top of one another. In the Disperser's Random layout, FANTOM pulls apart these different components so you can see where the node connections exist more easily.

Figure 7-4: (U) Random Disperser Layout (animals.graphml)



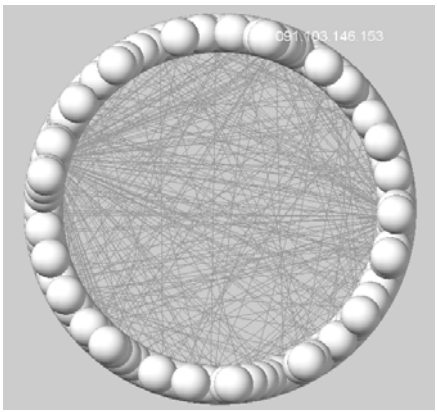
Circular Layout example



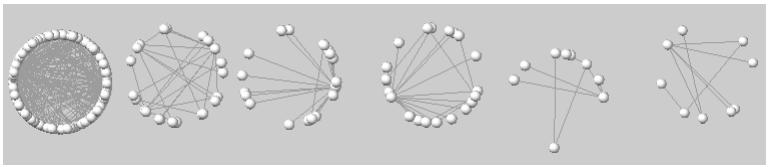
Random Disperser example

   - (U) **Sort Disperser Layout** – Similar to a Random layout, the **Sort Disperser Layout** command spreads out the disconnected components of the graph but it sorts them left to right from largest to smallest. This analytic is usually faster than a Random layout, but a Random layout takes up less space on the screen.

Figure 7-5: (U) Sorted Disperser (animals.graphml)



Circular Layout example



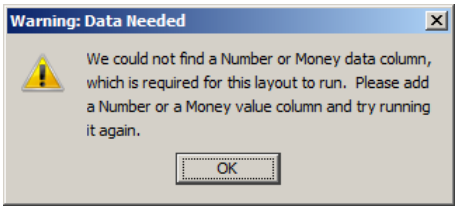
Sort Disperser example

Flow of Values Layout

(U) The Flow of Values layout is a cross between the Force Directed Layout and the Tiered Layout. For a selected node, parent nodes will appear above the selected node and the distance between selected node and parent node is based on the cumulative amount of funds transferred from parent to target.

The selected node has all child nodes appearing below it. Similar to the parent nodes, the distance from the children to the selected node is determined based upon the cumulative amount of funds transferred.

Tip: To run the Flow of Values Layout command, your data set must contain a column defined with the **Currency** or **Number** type during import into FANTOM (see Chapter 12, "Creating Import Templates"). If FANTOM does not find either type of column, it displays a warning message to let you know.

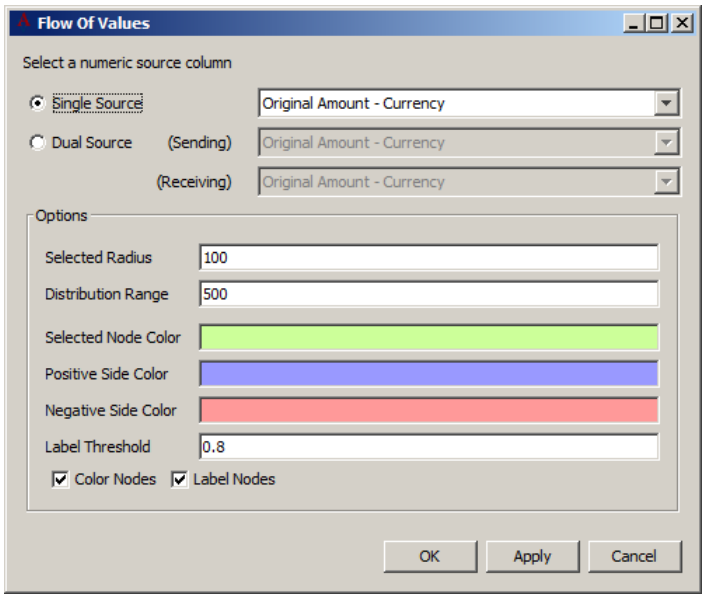


(U) To run the Flow of Values layout:

1. (U) Select one or more nodes.
2. (U) Choose **Layouts** > **Flow of Values**.

   (U) The Flow of Values dialog box displays (Figure 7-6).

Figure 7-6: (U) Flow of Values dialog box



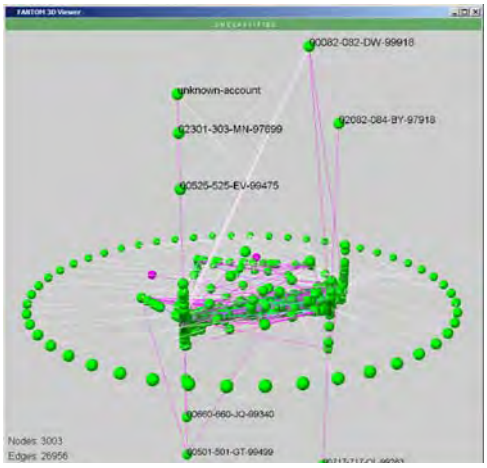
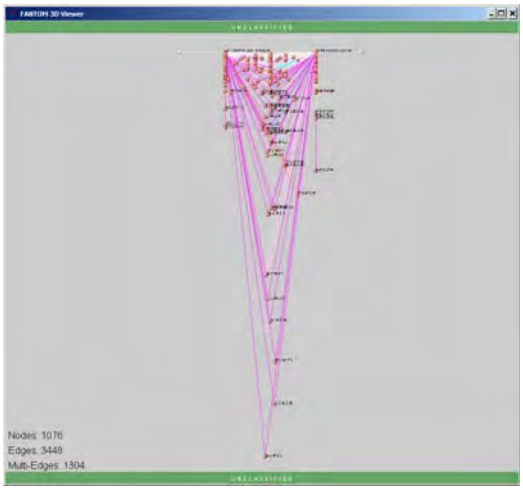
3. Select the **Single Source** or **Dual Source** radio button and then select the appropriate column titles at the right of the radio button you selected.

4. Accept the default options or change them to better suit the visual presentation of the Flow of Values layout in the Graph Viewer window. Your options are:

   - **Selected Radius** – The radius of the circle of nodes in the layout.
   - **Distribution Range** – The height of the nodes in the layout.
   - **Selected Node Color** – The nodes you selected before running this layout.
   - **Positive Side Color** – The nodes at the top of the layout who gained the most money or number.
   - **Negative Side Color** – The nodes at the bottom of the layout who lost the most money or number (the victims).
   - **Label Threshold** – The percentage of the total sums of the takers (at the top) and the givers (at the bottom) whose labels FANTOM should display as part of running the Flow of Values layout.
   - **Color Nodes** – While this check box is selected, FANTOM applies the colors selected in this dialog box to nodes. White nodes are not connected to the selected (or seed) nodes.
   - **Label Nodes** – While this check box is selected, FANTOM displays labels at the defined **Label Threshold**.

5. Click **Apply** or **OK** to run this layout.

Table 2: (U) How selections affect the Flow of Value Layout results (Currency.session)

Select:	When	The results look like this:
Single Source	All your transaction amounts are in the same column (bank-example.csv, bank-example.session, bank-example.template)	
Dual Source	Your credit and debit amounts are two separate columns	

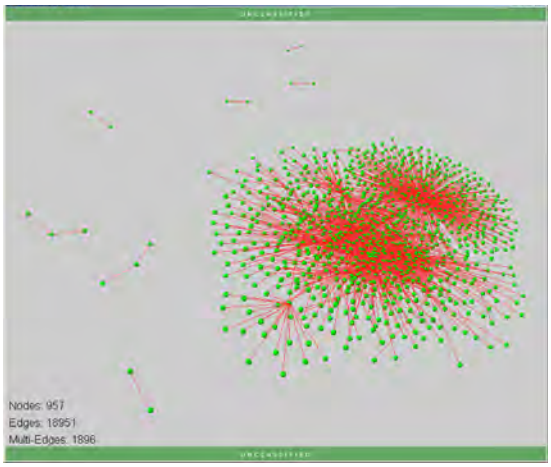
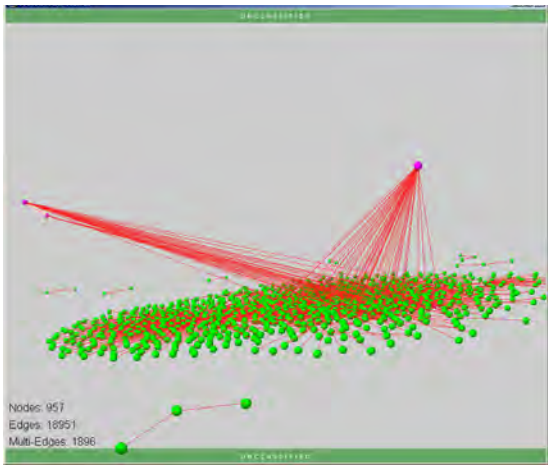
Force Directed Layout

(U) The Force Directed Layout command positions the nodes of the graph using an approach inspired by physics. In this model, nodes that are connected *attract*, or *pull*, toward each other, as if the nodes had opposite magnetic polarity. The nodes that are not connected *repel* (as if they had the same magnetic polarity).

(U) The more strongly connected two nodes are, the more they attract each other. The effect is that nodes that are strongly connected will be close together in the 3D Viewer window. Nodes that are weakly connected will be less close. Nodes that are not connected are farthest apart.

(U) What you select before choosing the Force Directed Layout command also determines what this FANTOM command does:

Table 3: (U) How selections affect the Force Directed Layout results (Enron.session)

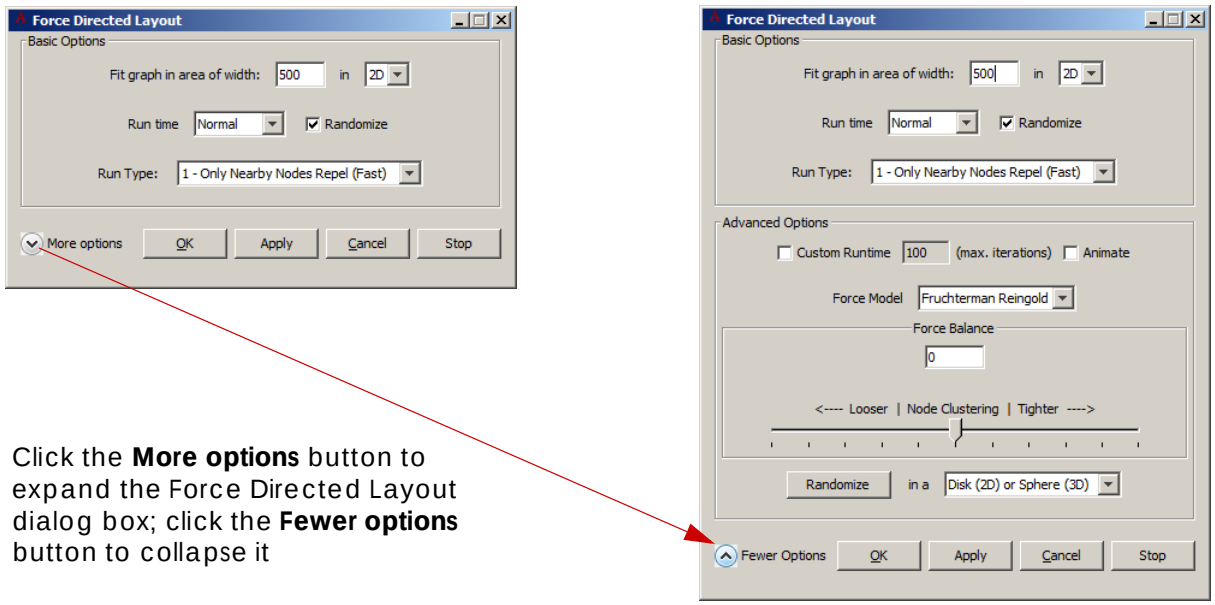
If you select:	FANTOM does this:	The results look like this:
No nodes and 2D	Applies the Force Directed layout to all nodes in the graph	
More than one node and 3D	Applies the Force Directed layout to the selected nodes in the graph **Note:** You can select one node, but it will have nothing to interact with. If you have Randomize selected, the node will move when you run Force Directed layout.	

(U) To run Force Directed layout:

1. (U) Choose **Layouts** > **Force Directed**.

   (U) The Force Directed Layout dialog box displays (Figure 7-7).

Figure 7-7: (U) Force Directed Layout dialog box with More Options shown



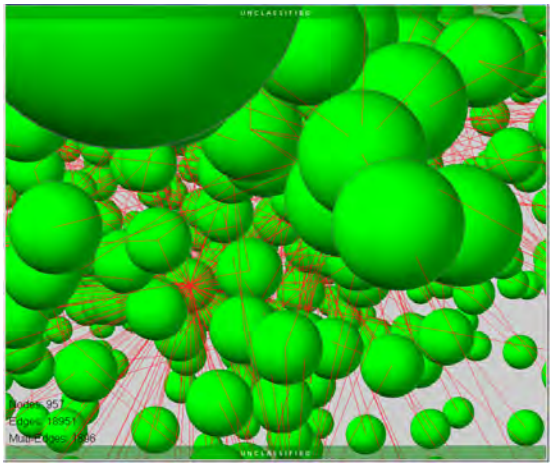
2. (U) Select the following Basic or Advanced options and then click **Apply** or **OK**:

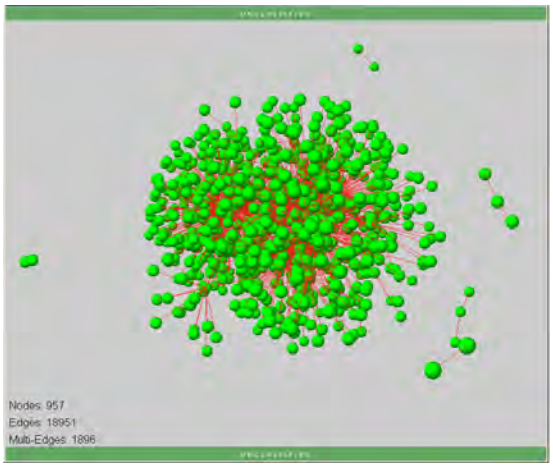
   - (U) **Basic Options**:

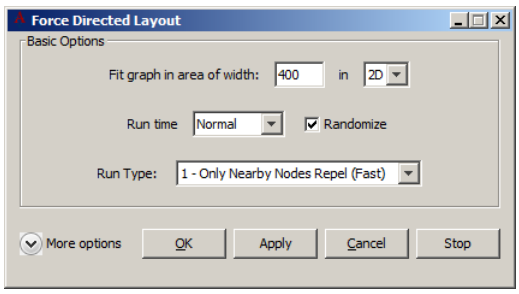
     - (U) **Width** – The **Width** parameter specifies the size of the area in which the final graph displays in the 3D Viewer window. The larger the width, the greater the spread of nodes will be. You can enter a number between 1 and 9999 (see Width examples in Figure 7-8).

Figure 7-8: (U) Width variations in a 3D layout (Enron.session)

400 width

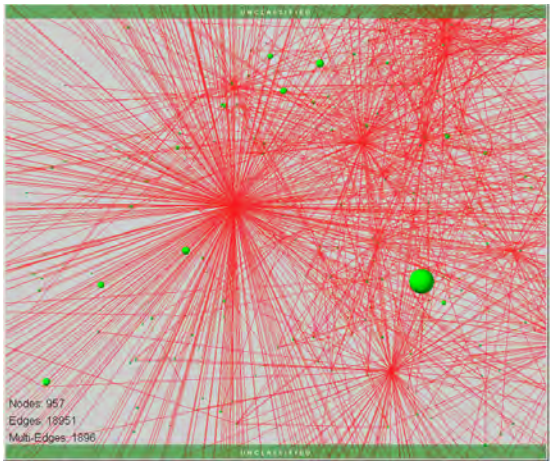


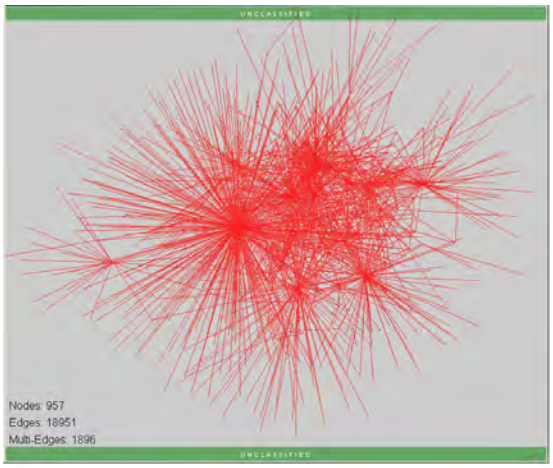


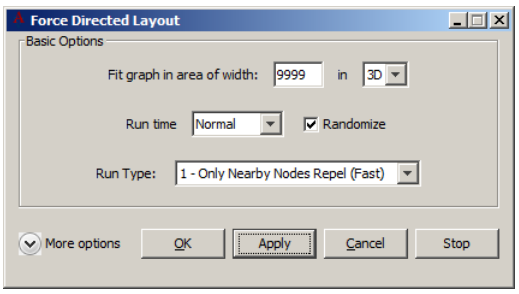


Fit graph in area of width: 400 in 3D

9999 width





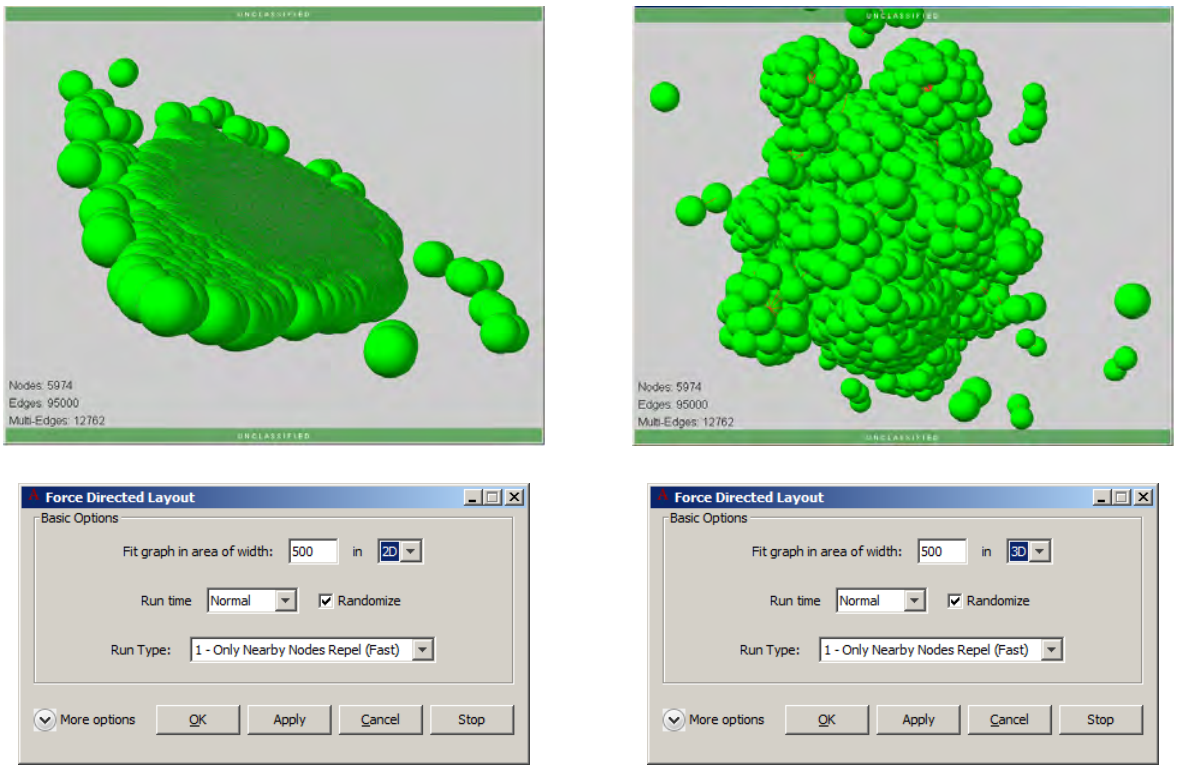


Fit graph in area of width: 9999 in 3D
Note: 9999 is the maximum width

- (U) **2D/3D** – The 2D/3D menu controls whether FANTOM draws the layout in two dimensions, producing a flat graph, or in a full three-dimensions. While both a 2D or a 3D graph can be rotated and examined from different perspectives in the 3D Viewer window, a 3D graph can sometimes make it easier to identify relationships.

(U) In using the 2D/3D control, you should be careful to note whether you are starting with an initial graph that differs from your setting of this parameter. A 2D starting graph will produce a 2D result, even if you choose the 3D option. Using the 2D option on a 3D starting graph may produce an oddly shaped result. In either of these cases you can select the **Randomize** check box to reformat the initial graph to be compatible with your chosen result before running the layout.

Figure 7-9: (U) 2D/3D layout examples



Fit graph in area of width: 500 in 2D

Fit graph in area of width: 500 in 3D

- (U) **Randomize** – The **Randomize** check box, selected by default, causes FANTOM to reformat the initial graph so it is compatible with your dimension choice (2D or 3D). FANTOM selects this check box for you automatically if you change your choice in the 2D/3D menu.

Note: (U) It is not always desirable to randomize your current layout before running a new one. For example, if you have already run the Force Directed Layout once, running it again with **Randomize** deselected usually causes FANTOM to improve upon the graph and produce an even better result.

- (U) **Run time** – Select one of the following Run time options: **Very Short**, **Short**, **Normal**, **Long**, or **Very Long**. This setting

controls how long the Force Directed Layout's "physics simulation" runs, and thus how accurately nearness reflects connectedness in the resulting graph. Longer run times make the resulting graph better reflect the connection strengths, but take longer to draw.

- (U) **Run Type** – **Run Type** lets you select options between high speed (Level 1) and high accuracy (Level 3). Level 1 (option **1 - Only Nearby Nodes Repel (Fast)**) runs a "grid variant" form of the Fruchterman-Reingold Force Directed algorithm, in which nodes do not repel if they are "far enough" away from each other in the layout. This can often provide a reasonably good approximation to the correct result in much shorter time. Level 2 (option **2 - All Nodes Repel, Approx. (Slower)**) provides a more rigorous approximation that takes longer to run. Level 3 (option **3 - All Nodes Repel, Exact (Slowest)**) calculates the exact result with no approximation at all, but may take up to several minutes to complete on an extremely large graph.

- (U) **Advanced Options** – Click **More options** / **Fewer Options** to toggle between showing and hiding the Advanced Options section of this dialog box.

  (U) While not needed by most people who use FANTOM, you can use these options to provide even greater control over the layout that FANTOM produces. The Advanced Options are:

  - (U) **Custom Runtime (max. iterations)** – The Force Directed Layout operates by running repeated "steps," or iterations, of its force-directed physics simulation. Selecting the **Custom Runtime** check box allows you to enter an exact number of iterations for the maximum run time of the Force Directed Layout.

Note: (U) The **Run Time** menu remains dimmed while the **Custom Runtime** check box is selected.

  - (U) **Animate** – You can select the **Animate** check box to watch changes in the 3D Viewer window while FANTOM performs iterations of this layout. Selecting **Animate** causes the graph to be redrawn at the end of each step of the Force Directed Layout. This lets you observe the movement of nodes while the layout is running.

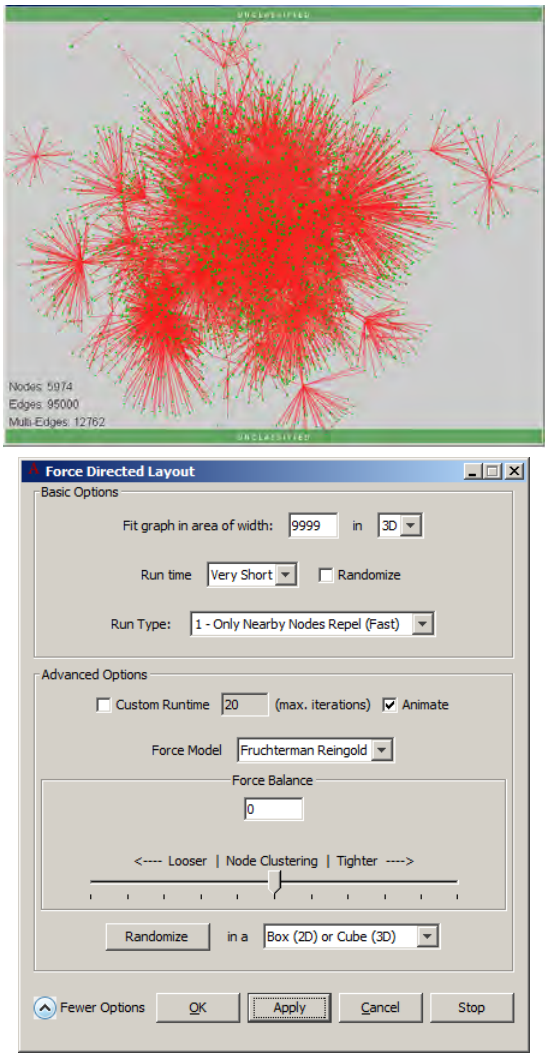
  - (U) **Force Model** – The Force Directed Layout allows for the development and selection of different Force Models that define the strength of the forces in the physics simulation, and how they change with the distance between nodes. The layout

currently lets you select the following force models. See Figure 7-10 for a comparison of the two models.

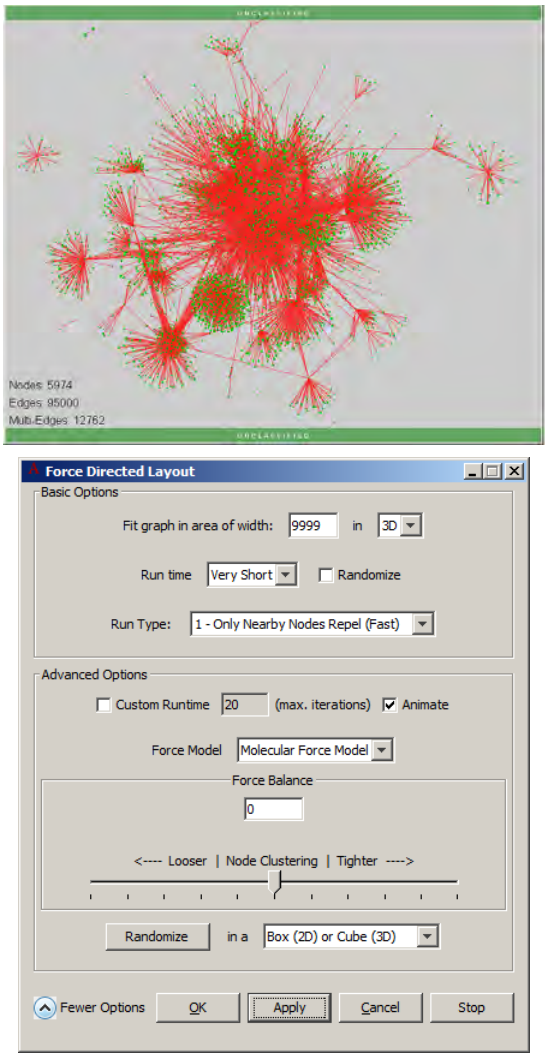
- (U) **Fruchterman-Reingold** (the default) uses a force model developed by the authors after which it is named. This model is well suited to finding a good layout where connected nodes tend to form into clusters, but are still separated enough to be easily distinguished.
- (U) The **Molecular Force** option uses a model based on the scale of forces that might be found in a molecular physics simulation. This model is often not suitable for an initial run, since it has difficulty forming the initial clusters that can more easily be found by using the Fruchterman-Reingold option. However, when used after an initial run of the Force Directed Layout, it tends to produce a graph with tighter and more isolated node groups.

Figure 7-10: (U) Force Model comparisons

Fruchterman Reingold



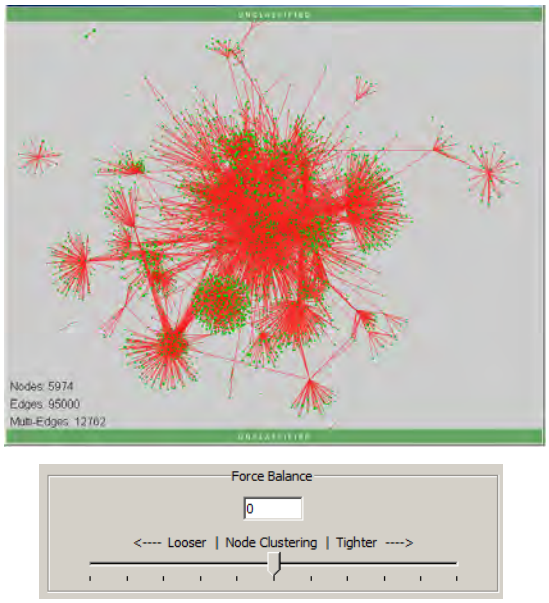
Molecular Force Model



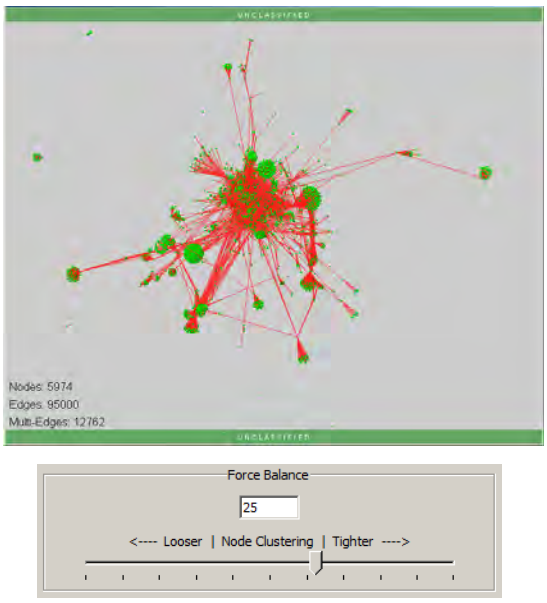
- (U) **Force Balance** – The Force Directed Layout works by finding a balance between attractive and repulsive forces in its "physics simulation." The Force Balance option allows you to shift the balance between those forces, favoring either *attractive forces* (which tends to produce tighter node clusters), or *repulsive forces* (which tends to produce looser ones). Zero (0) represents the default balance between the two. You can use the slider to adjust this balance, or enter a value between -100 and 100 in the **Force Balance** text box. See Figure 7-11 for a comparison of force balance settings.

Figure 7-11: (U) Node Clustering Force Balance comparisons

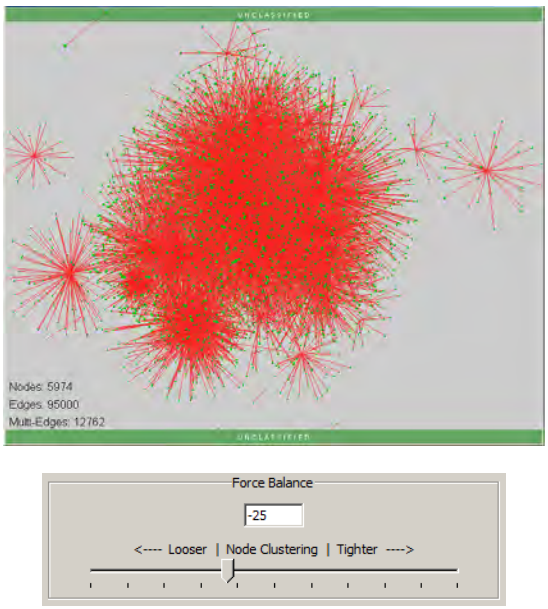
Force Balance: zero (0)



Force Balance: 25 tighter



Force Balance: -25 looser

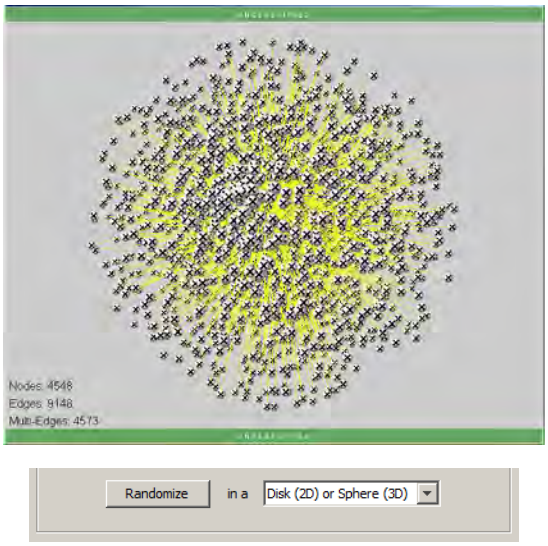


- (U) **Randomize** button – The **Randomize** button allows you to manually create a random distribution of the nodes in the 3D Viewer window without running the Force Directed Layout. It distributes them in a flat plane if the 2D option is selected, or in three dimensions if the 3D option is selected. You can also choose the shape in which the nodes will be distributed: a spherical shape, a square shape, or a cylindrical one.

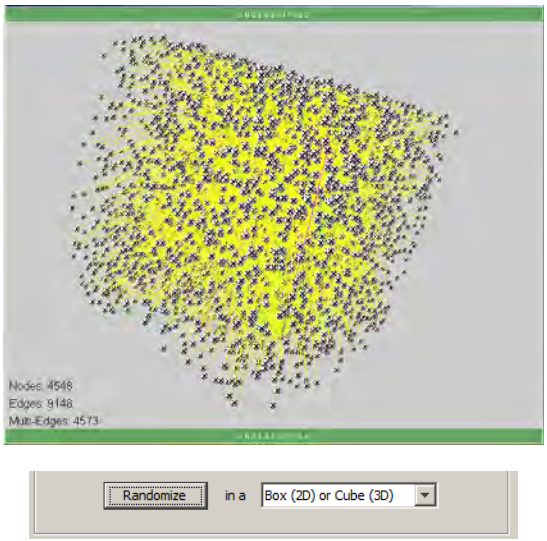
- (U) <***Shape***> **(2D) or** <***Shape***> **(3D)** menu – Choose the shape and number of dimensions FANTOM should use when Randomizing the layout results in the 3D Viewer window. The choices are: **Disk (2D) or Sphere (3D)**, **Box (2D) or Cube (3D)**, or **Disk (2D or Cylinder (3D)**.

Figure 7-12: (U) <Shape> (2D) or <Shape> (3D) comparisons

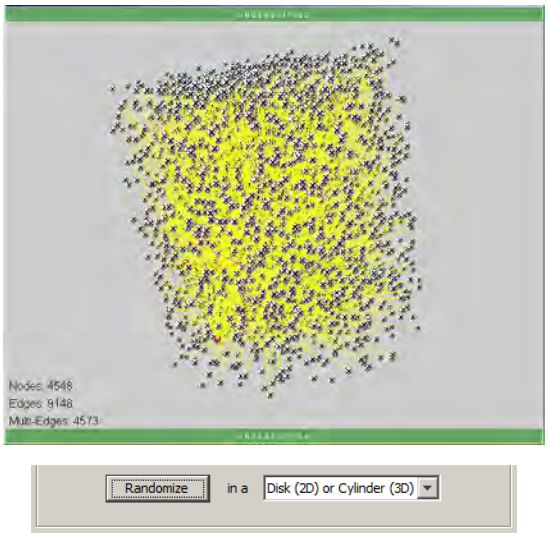
Disk (2D) or Sphere (3D)



Box (2D) or Cube (3D)



Disk (2D) or Cylinder (3D)



(U) **Usage Notes:** The quality of the graph produced by the Force Directed Layout often depends on the shape of the initial graph. This makes the Force Directed Layout well suited to the approach of doing successive runs that build on the results from previous ones. If a high quality result is sought, this can often be more efficiently arrived at by first doing a shorter or more approximate run to find a

good starting point, and then following it with a longer or more exact run (with the **Randomize** box deselected) to refine it into an even better one.

Link Cluster Layout

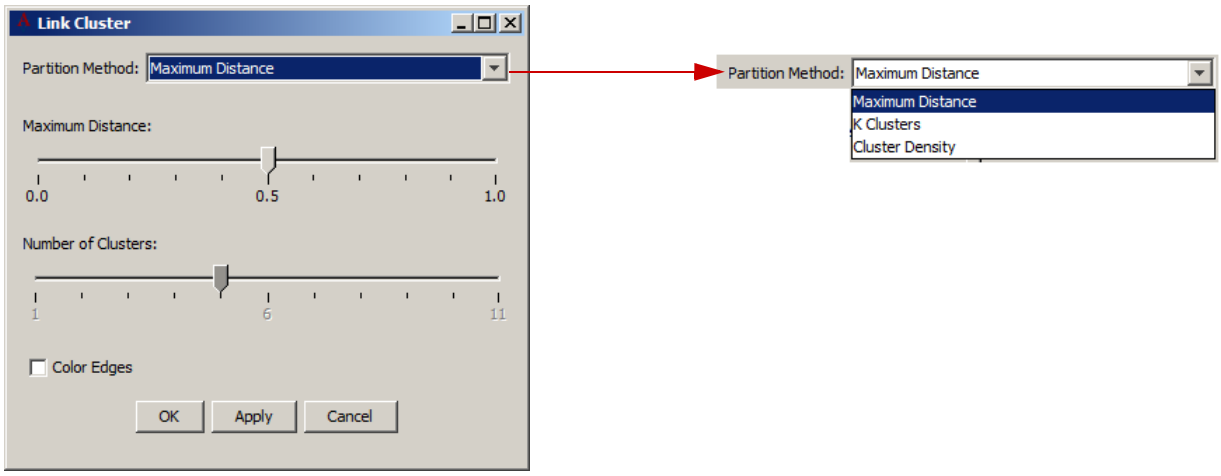
(U) The Link Cluster Layout lets you arrange nodes in the graph in clusters based on the connections.

To use the Link Cluster layout:

1. (U) Choose **Layouts** > **Link Cluster**.

   (U) The Link Cluster Layout dialog box displays.

Figure 7-13: (U) Link Cluster Layout dialog box

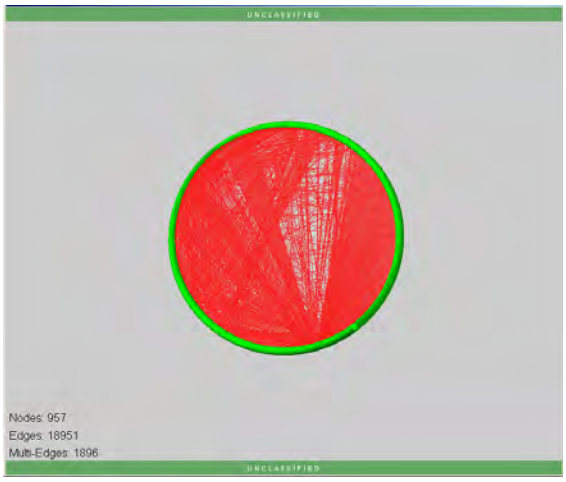


2. (U) Select the options you prefer:

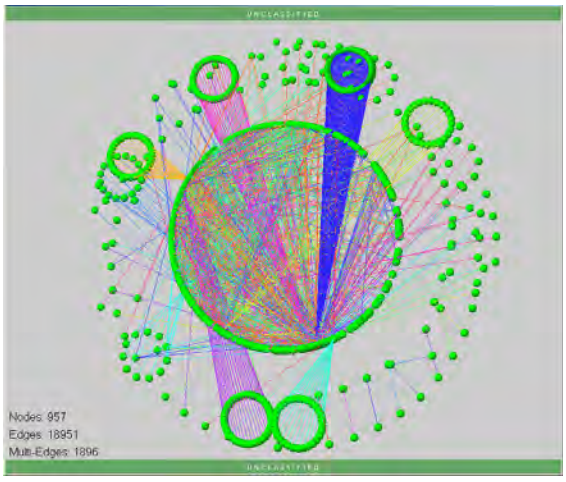
   - (U) **Partition Method** – You can select one of the following methods:

     - (U) **Maximum Distance** – While this method is selected, the **Maximum Distance** slider is active where you can set a distance between 0.0 and 1.0.

Figure 7-14: (U) Link Cluster layout – Maximum Distance example (Enron.session)



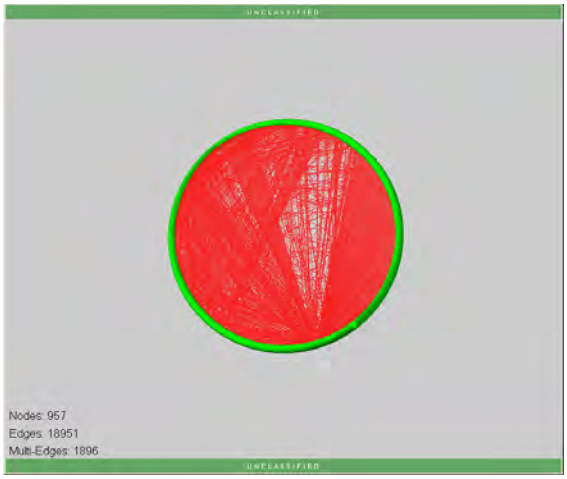
Starting graph in a circle layout



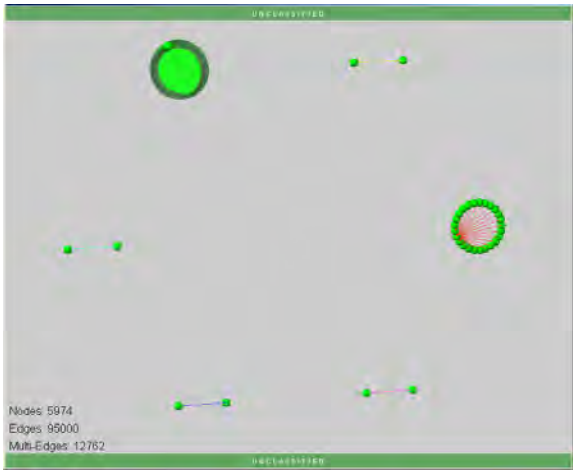
Maximum Distance at 0.7 with Color Edges

- (U) **K Clusters** – While this method is selected, the **Number of Clusters** slider is active where you can set the number of clusters to identify between 1 and 11.

Figure 7-15: (U) Link Cluster Layout - K Clusters example (Enron.session)



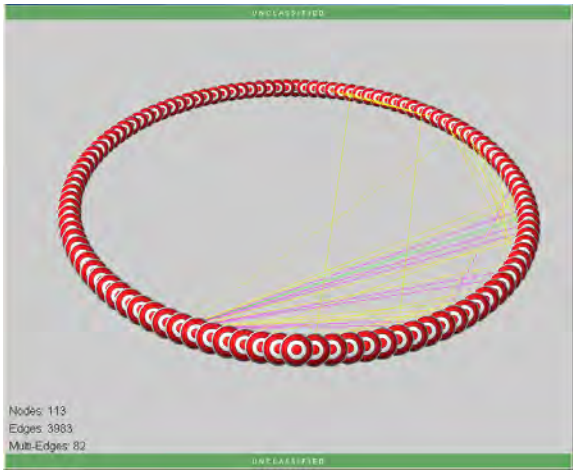
Starting graph in a circle layout



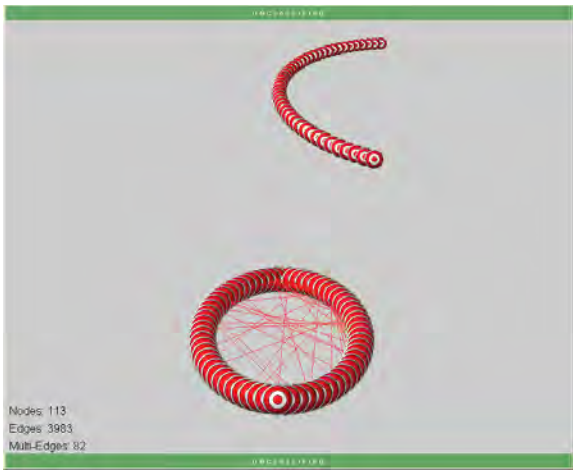
Number of Clusters at 6 with Color Edges

- (U) **Cluster Density** – While this method is selected, neither slider is active. You can select the **Color Edges** check box with this method. For an example of Cluster Density layout results, see Figure 7-16.

Figure 7-16: (U) Link Cluster Layout - Cluster Density example (airplane.graphml)



Starting graph in a circle layout



Number of Clusters at 6 with Color Edges

- (U) **Maximum Distance** slider – When the **Maximum Distance** partition method is selected, this slider is active.
- (U) **Number of Clusters** slider – When the **K Clusters** partition method is selected, this slider is active.
- (U) **Color Edges** – The **Color Edges** check box is available with any of the partition methods. When you select this option, FANTOM applies different colors to the edges of nodes in ranges of communities.

3. (U) Click **OK** or **Apply** and wait for the layout to finish.

Note: (U) You can double-click the progress bar at the bottom right corner of the FANTOM Controller window to open the Task Monitor. Here you can see the progress along with the elapsed time to better determine how long the layout processing may take.

(U) After the layout completes, FANTOM adds a Community ID column in the Node and Edge tables.

Tiered Layout

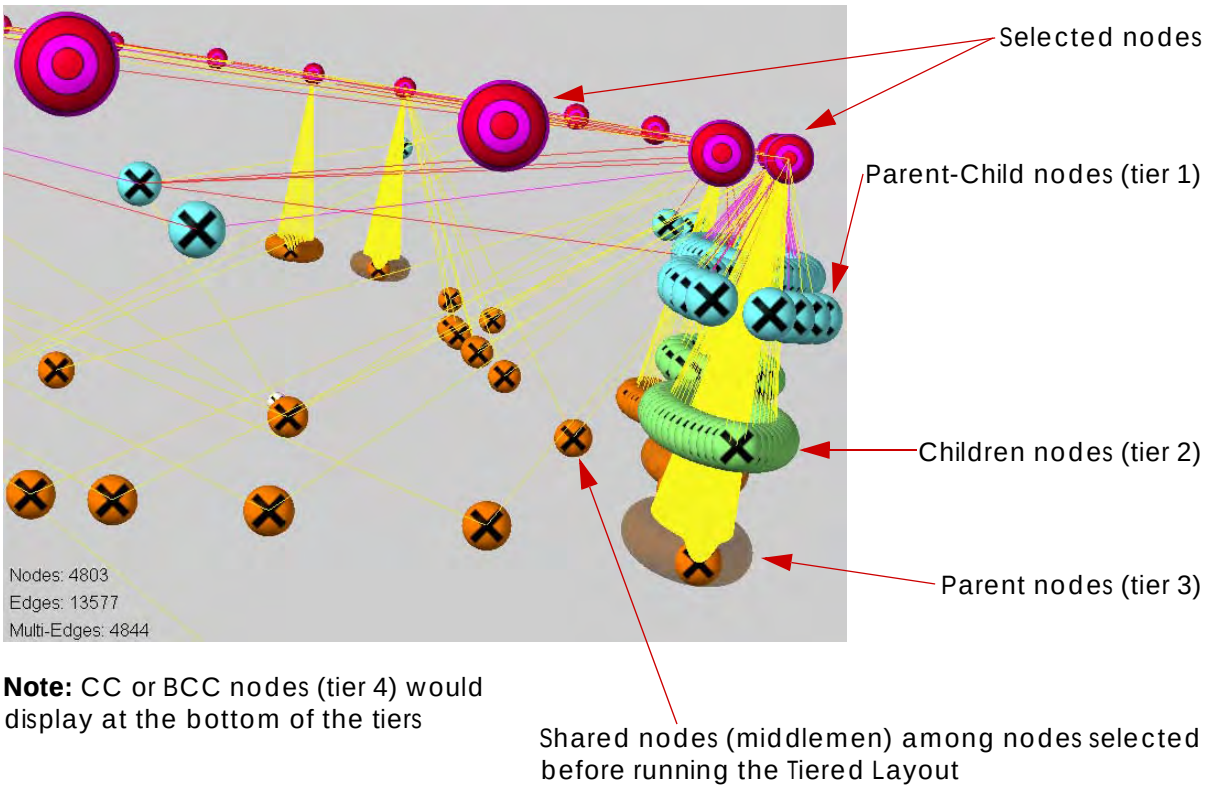
(U) The Tiered Layout was envisioned by an ECAU Intelligence Analyst. You can use the Tiered Layout with any relational data set that contains edges. Before you choose this layout command, you must select one or more nodes. These nodes will display at the top of the graph tiers showing you the relationship they have with other nodes.

(U) FANTOM arranges the graph in cone tiers starting at each node selected before running the layout and moving in cone rings in the following order:

- (U) **Parent-Child** – Inbound/outbound connections (tier 1)
- (U) **Children** – Outbound only connections (tier 2)
- (U) **Parent** – Inbound only connections (tier 3)
- (U) **CC or BCC with Target** – (tier 4)

(U) Nodes that float in the middle are *shared nodes*, with connections to multiple selected nodes. Shared nodes gravitate horizontally toward the nodes they connect with the most. They also are positioned vertically to indicate the tier level.

Figure 7-17: (U) How FANTOM visualizes edge relationships in the Tiered Layout (two-hops.session)



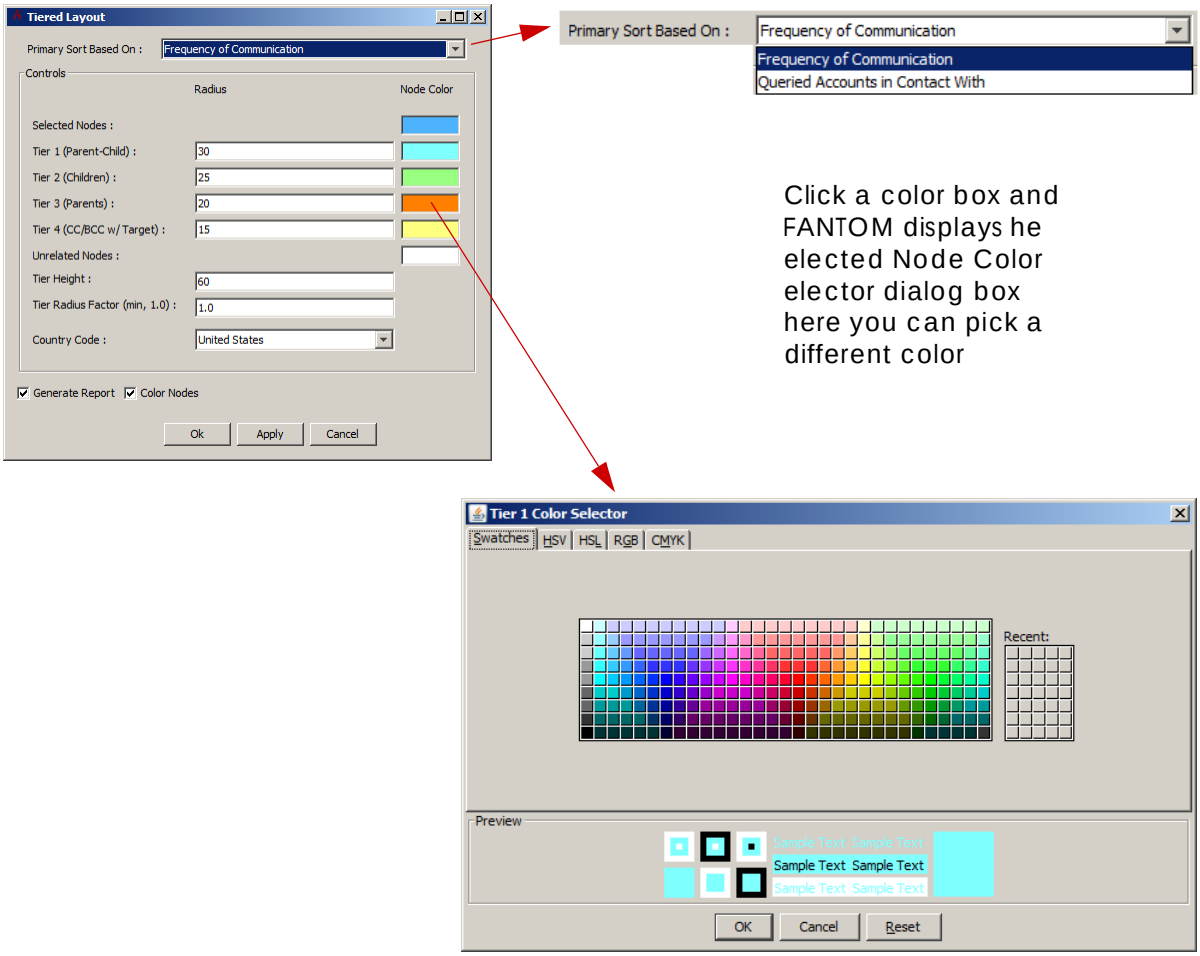
Note: CC or BCC nodes (tier 4) would display at the bottom of the tiers

(U) To use the Tiered Layout:

1. (U) Access data in one of the following ways:
   - (U) Open a session.
   - (U) Import data.
   - (U) Run a database query.
2. (U) Select one or more nodes of interest in the Controller window.
3. (U) Choose **Layouts** > **Tiered**.

(U) The Tiered Layout dialog box displays (Figure 7-18).

Figure 7-18: (U) Tiered Layout dialog box



4. (U) Select the options you prefer:

   - (U) **Primary Sort Based On** – Frequency of Communication or Queried Accounts in Contact With:
     - (U) **Frequency of Communication** – Sorts the report by the following columns:
       - (U) **Tier Level** – Tier Level is the Primary sort level
       - (U) **Rec. From Tgt** – Received from Target
       - (U) **Sent To Tgt** – Sent to Target
       - (U) **#T1 Edges** – Number of Tier 1 edges
       - (U) **#T2 Edges** – Number of Tier 2 edges
       - (U) **#T3 Edges** – Number of Tier 3 edges

- (U) **On Rec W/ Tgt** – On Received list with Target (CC or BCC)

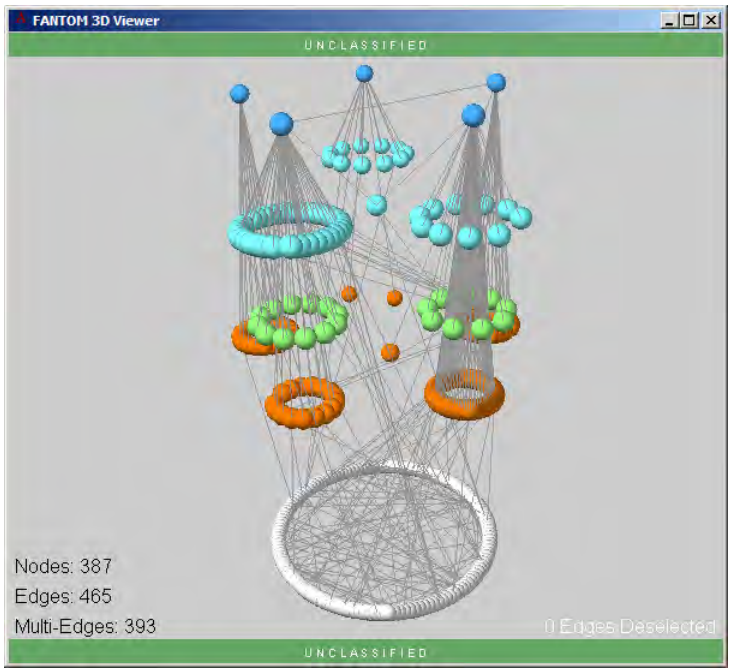
- (U) **Queried Accounts in Contact With** – Sorts the report by the following columns:
  - (U) **Tier Level** – Tier Level is the Primary sort level
  - (U) **#T1 Edges** – Number of Tier 1 edges
  - (U) **#T2 Edges** – Number of Tier 2 edges
  - (U) **#T3 Edges** – Number of Tier 3 edges
  - (U) **#T4 Edges** – Number of Tier 4 edges
  - (U) **Rec. From Tgt** – Received from Target
  - (U) **Sent To Tgt** – Sent to Target
  - (U) **On Rec W/ Tgt** – On Received list with Target (CC or BCC)

- (U) **Tier 1 Radius (Parent-Child's)** – Inbound/outbound connections
- (U) **Tier 2 Radius (Children)** – Outbound only connections
- (U) **Tier 3 Radius (Parents)** – Inbound only connections
- (U) **Tier 4 Radius (on CC or BCC with Target)** – CC or BCC on received list with target
- (U) **Tier Height** – Height of each tier in the 3D Viewer window
- (U) **Generate Report** – If you select this check box, you can also choose the sort order to be based on the Frequency of Communication or Queried Accounts in Contact With.

5. (U) Click **OK**.

   (U) FANTOM takes a few moments to change the layout (Figure 7-19) and create the report (Figure 7-20).

Figure 7-19: (U) Tiered Layout (animals.session)



Tiered Layout Report

(U) The Tiered Layout report is optional when you run the Tiered Layout for the currently selected nodes.

(U) **To create this report:**

1. (U) Select the **Generate Report** check box in the Tiered Layout dialog box (Figure 7-18).

2. (U) Select an option from the **Primary Sort Based On** menu.

   (U) When the Tiered Report is complete, FANTOM changes the graph appearance and displays the Tiered Layout Report Dialog box which contains several tabs of information as well as the capability to find, sort, and export information. The following sections explain the contents and capabilities of the Tiered Layout Report dialog box which has several tabs of information:

   - Tiered Layout Report Dialog Box – Overall Tab
   - Tiered Layout Report Dialog Box – Selected Nodes Tab
   - Tiered Layout Report Dialog Box – Shared Tab
   - Tiered Layout Report Dialog Box – <Target ID> Tab

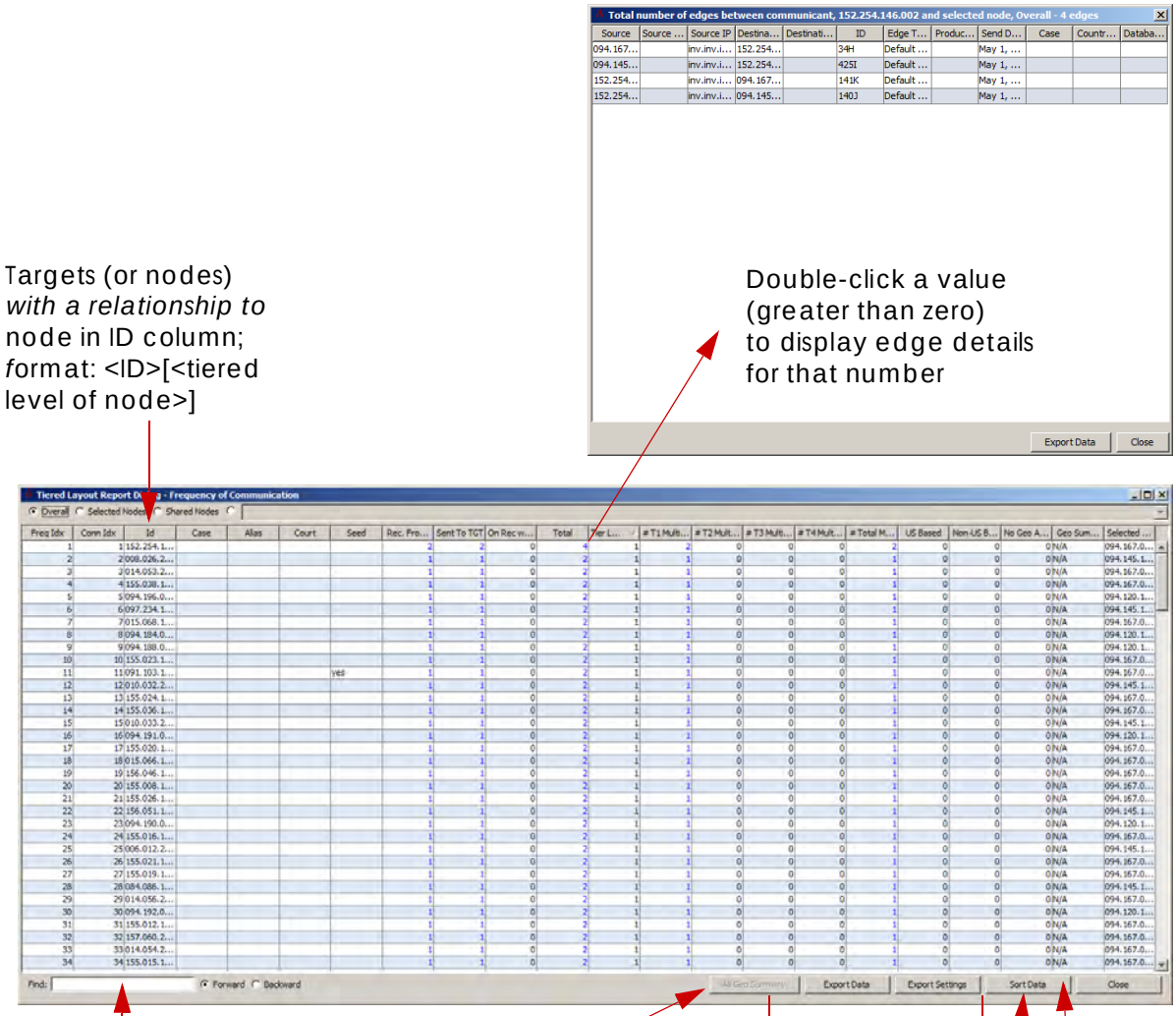
   (U) The Tiered Layout Report dialog box also provides capabilities to find, sort, and export information:

   - Finding Information in the Tiered Report Dialog Box

- Creating a Custom Sort of the Tiered Layout Report
- Specifying Tiered Layout Report Export Settings
- Exporting Tiered Layout Report Data

Tiered Layout Report Dialog Box – Overall Tab

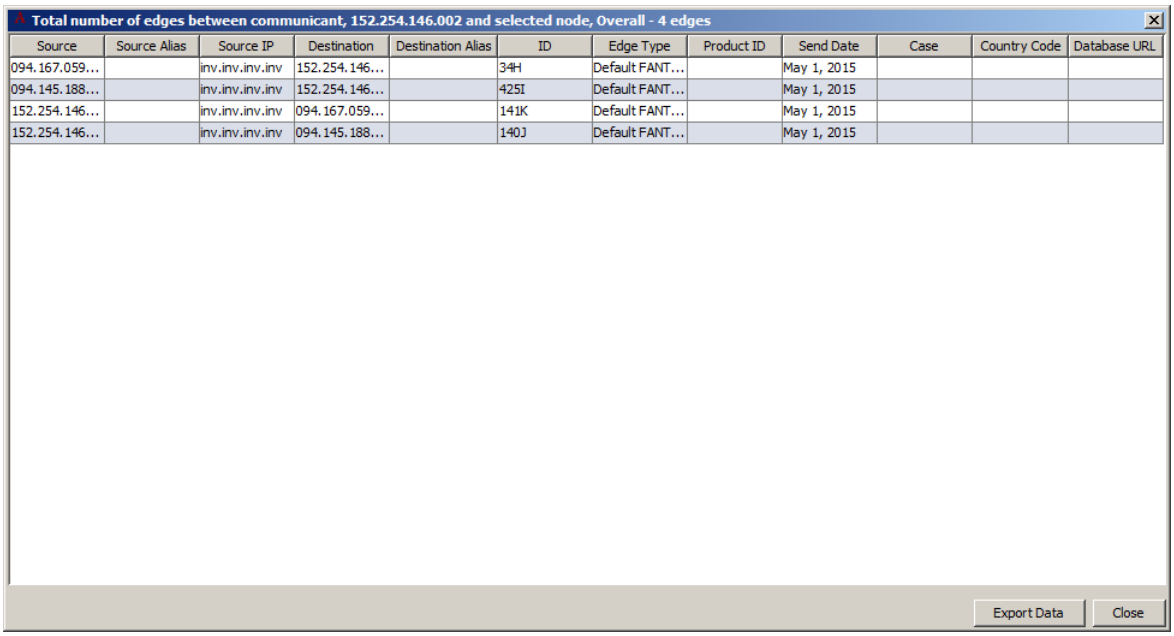
Figure 7-20: (U) Example of a Tiered Layout Report Dialog – Overall tab



(U) The Overall tab contains the following columns:

- (U) **FREQ IDX** – Frequency Index is the first Primary Sort option: Frequency of Communication
- (U) **CONN IDX** – Connection Index is the second Primary Sort option: Queried Accounts in Contact With
- (U) **ID** – Identifier for the communicant node with a relationship to nodes listed in the Targets column; the ID is a connection identifier, such as an IP or email address
- **Case** –
- **Alias** –
- (U) **Court** – Lists the collection authority for this record of data.
- (U) **SEED** – Nodes you selected before running Tiered Layout
- (U) **REC. FROM TGT** – Connections received from the target by communicant; double-click the number to view edge details

Figure 7-21: (U) Example of Edge Details



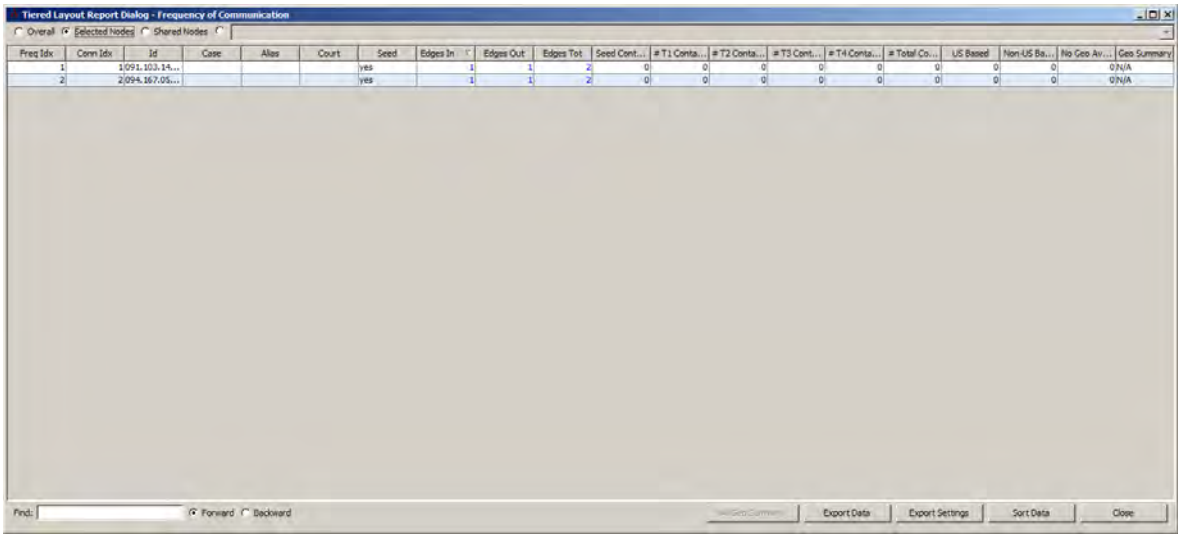
- (U) **SENT TO TGT** – Edges sent to target by communicant; double-click the number to view edge details
- (U) **ON REC W/ TGT** – CC or BCC on Recipient list with target
- (U) **TOTAL** – Total of edges received from and sent to target; double-click the number to view edge details
- (U) **TIER LEVEL** – FANTOM supports the following tier levels:

- (U) **Tier Level 1 – Parent-Child** – Inbound/outbound connections
- (U) **Tier Level 2 – Children** – Outbound only connections
- (U) **Tier Level 3** – Inbound only connections
- (U) **Tier Level 4 – CC or BCC with Target**

- (U) **#T1 Multiedges** – Number of tier one edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T2 Multiedges** – Number of tier two edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T3 Multiedges** – Number of tier three edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T4 Multiedges** – Number of tier four edges; double-click the number to view a list of target IDs and tier levels
- (U) **# Total Multiedges** – The sum of tier one through tier four edges; double-click the number to view a list of target IDs and tier levels
- (U) **US Based** – US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **Non-US Based** – Non-US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **No Geo Available** –
- (U) **Geo Summary** – Each button in the right column where GeoIP summary data is available is active; click it to display Geo Summary information; if a row has no GeoIP summary data, FANTOM changes the button to N/A (Not Available) and makes it inactive
- (U) **Selected Nodes** – Selected nodes shows the indicated tier level relationship to the communicant node listed in the corresponding row of the ID column; the target format is: <*node identifier*>[<*tier level of connection to communicant*>]

Tiered Layout Report Dialog Box – Selected Nodes Tab

Figure 7-22: (U) Example of a Tiered Layout Report Dialog – Selected Nodes tab



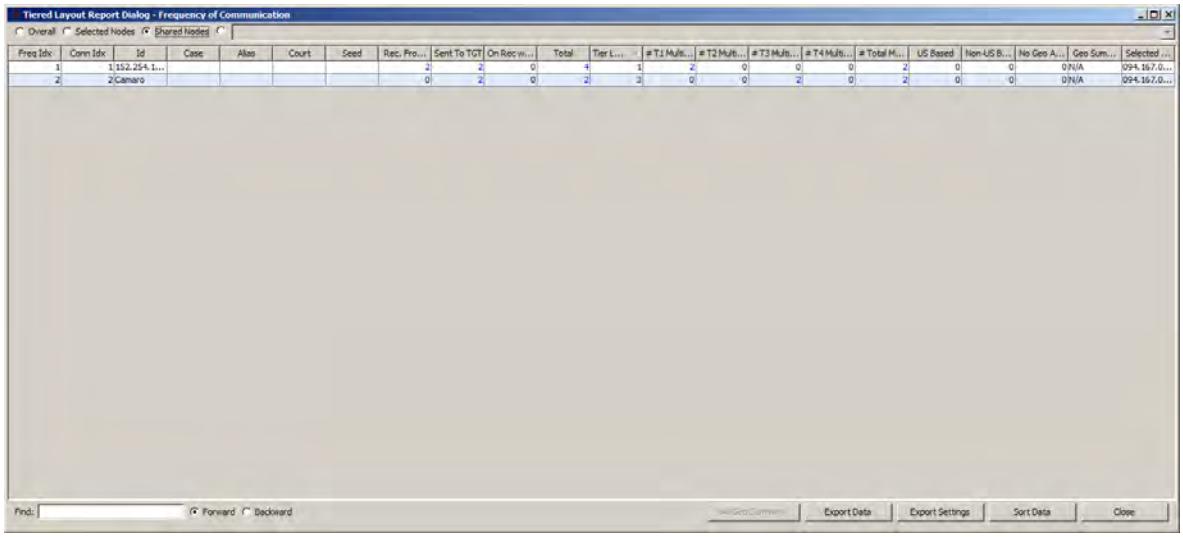
(U) The Selected Nodes tab contains the following columns:

- (U) **FREQ IDX** – Frequency Index is the first Primary Sort option: Frequency of Communication
- (U) **CONN IDX** – Connection Index is the second Primary Sort option: Queried Accounts in Contact With
- (U) **ID** – Identifier for the node you selected before running Tiered Layout
- (U) **Court** – Lists the collection authority for this record of data.
- (U) **SEED** – Nodes you selected before running Tiered Layout
- (U) **Edges In** – Number of edges to the target by communicants; double-click the number to view edge details
- (U) **Edges Out** – Number of edges from the target to communicants; double-click the number to view edge details
- (U) **Edges Total** – Total connections from and to the target; double-click the number to view edge details
- (U) **Seed Contacts** – The number of seed contacts.
- (U) **#T1 Contacts** – Total number of edges for the target node; double-click the number to view a list of IDs for all contacts
- (U) **#T2 Contacts** – Total number of edges for the target node; double-click the number to view a list of IDs for all contacts
- (U) **#T3 Contacts** – Total number of edges for the target node; double-click the number to view a list of IDs for all contacts

- (U) **#T4 Contacts** – Total number of edges for the target node; double-click the number to view a list of IDs for all contacts
- (U) **# Total Contacts** – Total number of edges for the target node; double-click the number to view a list of IDs for all contacts
- (U) **US Based** – US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **Non-US Based** – Non-US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **No Geo Available** –
- (U) **Geo Summary** – Each button in the right column where GeoIP summary data is available is active; click it to display Geo Summary information; if a row has no GeoIP summary data, FANTOM changes the button to N/A (Not Available) and makes it inactive

Tiered Layout Report Dialog Box – Shared Tab

Figure 7-23: (U) Example of a Tiered Layout Report Dialog – Shared tab



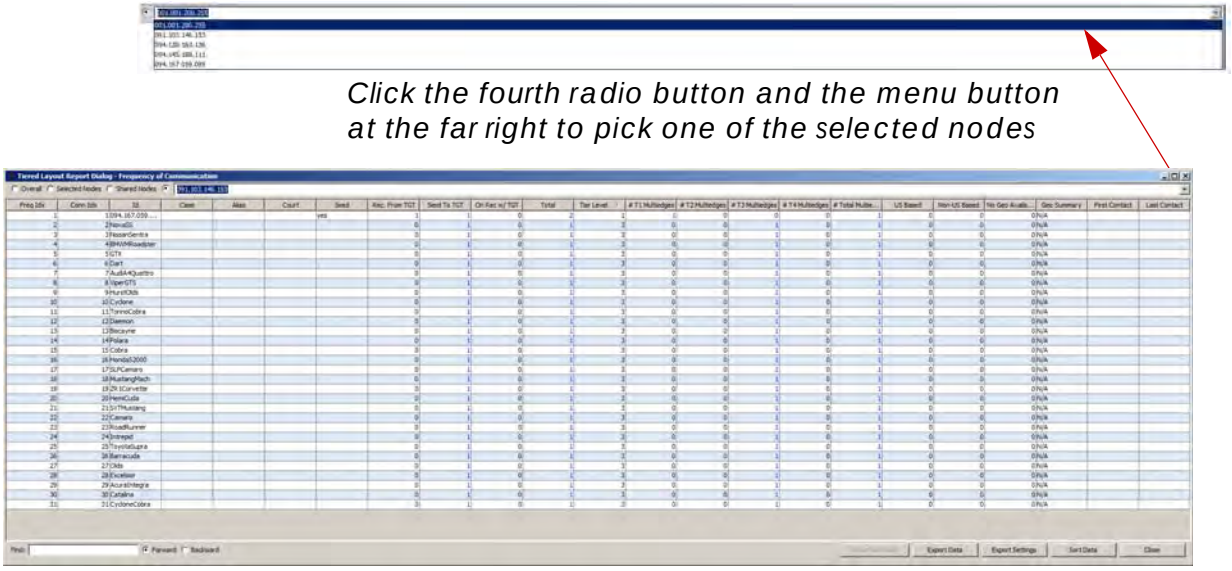
(U) The Shared tab contains the following columns:

- (U) **FREQ IDX** – Frequency Index is the first Primary Sort option: Frequency of Communication
- (U) **CONN IDX** – Connection Index is the second Primary Sort option: Queried Accounts in Contact With
- (U) **ID** – Identifier for the node you selected before running Tiered Layout
- (U) **Court** – Lists the collection authority for this record of data.
- (U) **SEED** – Nodes you selected before running Tiered Layout

- (U) **REC. FROM TGT** – Edges received from the target by communicant; double-click the number to view edge details
- (U) **SENT TO TGT** – Edges sent to target by communicant; double-click the number to view edge details
- (U) **ON REC W/ TGT** – CC or BCC on Recipient list with target
- (U) **TOTAL** – Total of edges received from and sent to target; double-click the number to view edge details
- (U) **TIER LEVEL** – FANTOM supports the following tier levels:
  - (U) **Tier Level 1 – Parent-Child** – Inbound/outbound connections
  - (U) **Tier Level 2 – Children** – Outbound only connections
  - (U) **Tier Level 3** – Inbound only connections
  - (U) **Tier Level 4 – CC or BCC with Target**
- (U) **#T1 Multiedges** – Number of tier one edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T2 Multiedges** – Number of tier two edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T3 Multiedges** – Number of tier three edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T4 Multiedges** – Number of tier four edges; double-click the number to view a list of target IDs and tier levels
- (U) **# Total Multiedges** – The sum of tier one through tier four edges; double-click the number to view a list of target IDs and tier levels
- (U) **US Based** – US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **Non-US Based** – Non-US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **No Geo Available** –
- (U) **Geo Summary** – Each button in the right column where GeoIP summary data is available is active; click it to display Geo Summary information; if a row has no GeoIP summary data, FANTOM changes the button to N/A (Not Available) and makes it inactive
- (U) **Selected Nodes** – Selected nodes showing the indicated tier level relationship to the communicant node listed in the corresponding row of the ID column; target format is: <*node identifier*>[<*tier level of connection to communicant*>]

Tiered Layout Report Dialog Box – <*Target ID*> Tab

Figure 7-24: (U) Example of a Tiered Layout Report Dialog – <Target ID>



(U) The <*Target ID*> table contain the following columns specific to the target identified in the tab title:

- (U) **FREQ IDX** – Frequency Index is the first Primary Sort option: Frequency of Communication
- (U) **CONN IDX** – Connection Index is the second Primary Sort option: Queried Accounts in Contact With
- (U) **ID** – Identifier for the communicant node with a relationship to this target; the ID is a connection identifier, such as an IP or email address
- (U) **Court** – Lists the collection authority for this record of data.
- (U) **SEED** – Nodes you selected before running Tiered Layout
- (U) **REC. FROM TGT** – Edges received from the target by communicant; double-click the number to view edge details
- (U) **SENT TO TGT** – Edges sent to target by communicant; double-click the number to view edge details
- (U) **ON REC W/ TGT** – CC or BCC on Recipient list with target
- (U) **TOTAL** – Total of edges received from and sent to target; double-click the number to view edge details
- (U) **TIER LEVEL** – FANTOM supports the following tier levels:
  - (U) **Tier Level 1** – **Parent-Child** – Inbound/outbound connections
  - (U) **Tier Level 2** – **Children** – Outbound only connections

- (U) **Tier Level 3** – Inbound only connections
- (U) **Tier Level 4 – CC or BCC with Target**

- (U) **#T1 Multiedges** – Number of tier one edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T2 Multiedges** – Number of tier two edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T3 Multiedges** – Number of tier three edges; double-click the number to view a list of target IDs and tier levels
- (U) **#T4 Multiedges** – Number of tier four edges; double-click the number to view a list of target IDs and tier levels
- (U) **# Total Multiedges** – The sum of tier one through tier four edges; double-click the number to view a list of target IDs and tier levels
- (U) **US Based** – US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **Non-US Based** – Non-US-based communications; double-click the number to view a list of target IDs and tier levels
- (U) **No Geo Available** –
- (U) **Geo Summary** – Each button where GeoIP summary data is available is active; click it to display Geo Summary information; if a row has no GeoIP summary data, FANTOM changes the button to N/A (Not Available) and makes it inactive

Finding Information in the Tiered Report Dialog Box

(U) To find information in the Tiered Report dialog box, type information to find, select the **Forward** or **Backward** button, and then press the ENTER key. FANTOM searches in the table you are currently viewing.

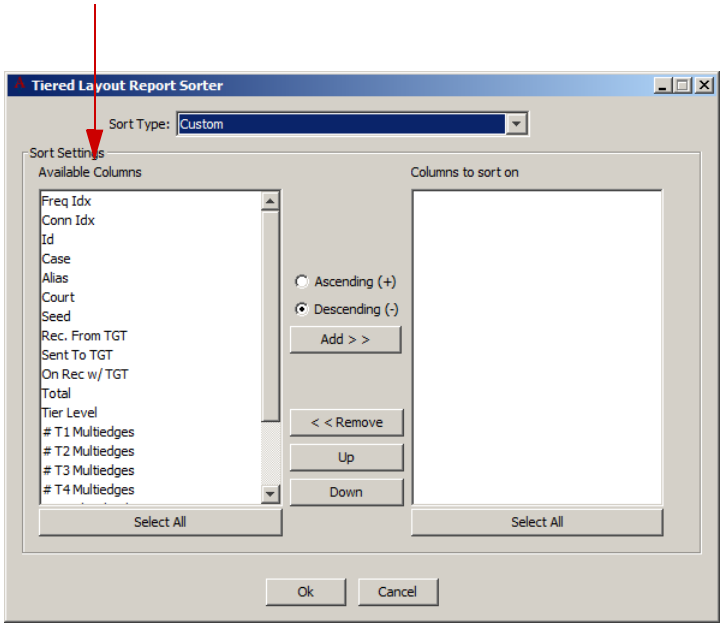
Creating a Custom Sort of the Tiered Layout Report

(U) You can specify a sort order for the Tiered Layout report by choosing **Frequency of Communication** or **Queried Accounts in Contact With** from the **Primary Sort Order Based On** menu on the Tiered Layout dialog box (Figure 7-18).

(U) FANTOM also lets you change the primary sort order after the report displays by clicking a column title. If you click the current Primary Sort column title that displays a small triangle, it toggles to reverse the order (from ascending to descending).

(U) FANTOM also lets you create a custom sort by clicking the **Sort Data** button and defining one or more sort levels in the Custom Sort dialog box.

Figure 7-25: (U) Custom Sort dialog box



(U) You can select whether each sort level should be ascending or descending by selecting a column title and then selecting the **Ascending** or **Descending** radio button.

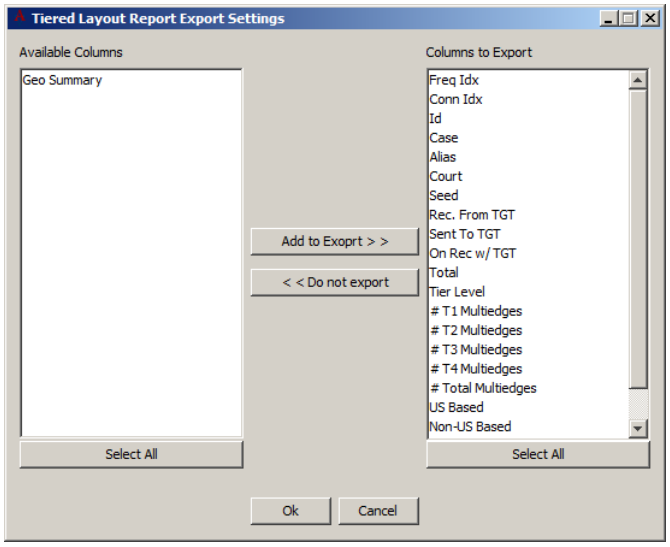
(U) FANTOM lets you arrange the sort order by selecting a column title in the Columns to sort on list and clicking the **Up** and **Down** buttons.

(U) To remove a column title from the sort list, select it and click **<< Remove**.

Specifying Tiered Layout Report Export Settings

(U) While viewing the Tiered Layout report, you can specify export settings by clicking the **Export Settings** button and selecting the columns to include in the export.

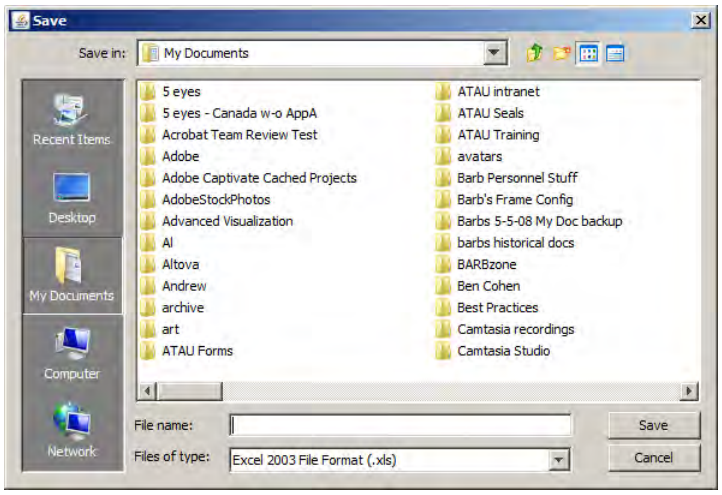
Figure 7-26: (U) Export Settings dialog box



Exporting Tiered Layout Report Data

(U) After specifying the Export Settings you prefer, click the **Export Data** button. A standard File Save dialog box displays so you can specify where the export file should be stored and what file type will be used.

Figure 7-27: (U) Export Data dialog box



Filtering Your Data

(U) One of the simplest ways to analyze your data is to use filters. *Filters* are a mechanism for temporarily reducing the information displayed to a subset of the full data set. When you add and enable a filter, FANTOM hides the information that matches the filter criteria. When you disable that filter, FANTOM shows the hidden information again. Filtered information is not deleted.

(U) Filtering lets you selectively hide information so you can focus more easily on relevant nodes and edges. Also, you might want to filter out irrelevant information before copying the table data and pasting it into another application's document, such as a Microsoft Word, Excel, or PowerPoint document if you are preparing a report.

(U) If an analytic or layout runs slowly, you might want to filter out some nodes, particularly disconnected ones, to speed up the process.

Tip: (U) After you import a data set, FANTOM creates a filter for it. This way if you are working with multiple data sets, you can easily show or hide the entire data set using the default filter.

Adding a Filter

(U) You can add filters on any of the Controller window tabs or on the 3D Viewer window.

Adding a Filter of Selected Nodes, Edges, or Multi-Edges

(U) If you want to filter information on the Nodes, Edges, or Multi-Edges tabs, you probably want to sort the information in the table first so it is easier to select a range of items based on a similar or easy to locate value in one of the columns.

(U) To filter information in the 3D Viewer:

1. (U) Select one or more nodes in the 3D Viewer window.
2. (U) Do one of the following:
   - (U) Right-click the mouse button and choose the **Filter** command to filter out the selected nodes.
   - (U) Right-click the mouse button and choose the **Filter Others** command to filter out all but the selected nodes.

(U) To add a filter of selected nodes, edges, or multi-edges:

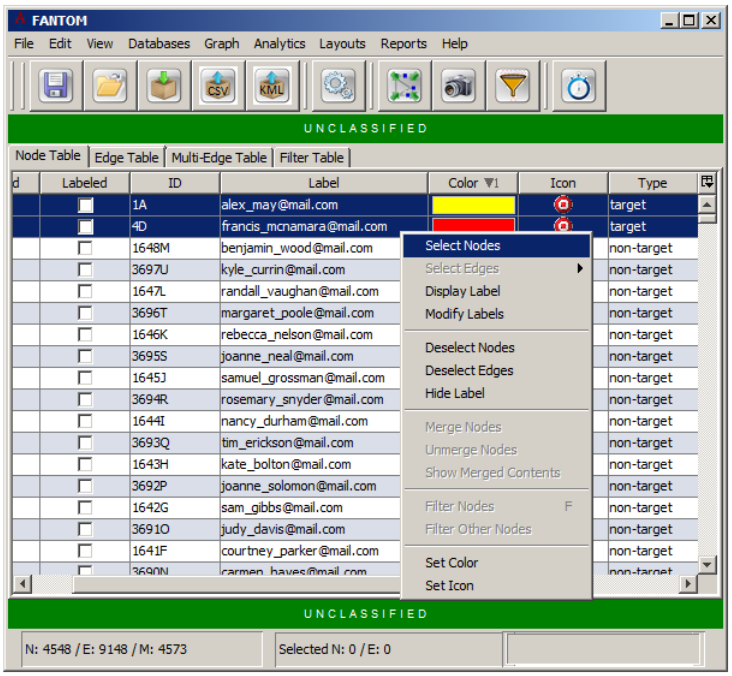
1. (U) Sort the Node Table, Edge Table, or Multi-Edge Table by clicking a table's column title (Figure 8-1).

Figure 8-1: (U) Example of sorting the Node Table by case

2. (U) Select one or more items in any of the following ways:

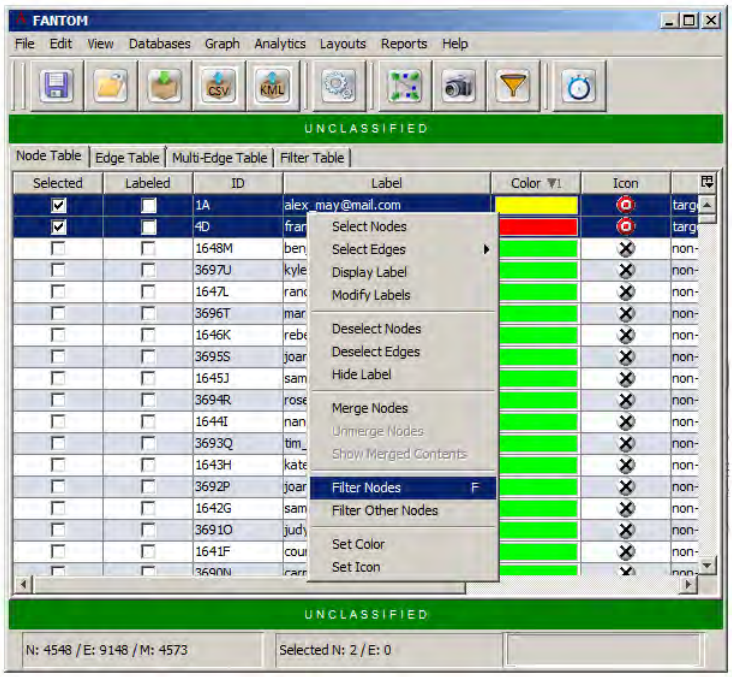
   - (U) Click one or more of the **Selected** check boxes.
   - (U) Highlight one or more rows in the Node Table (Figure 8-2), and then right-click and choose **Select Nodes**.

Figure 8-2: (U) Example of selecting a range of nodes



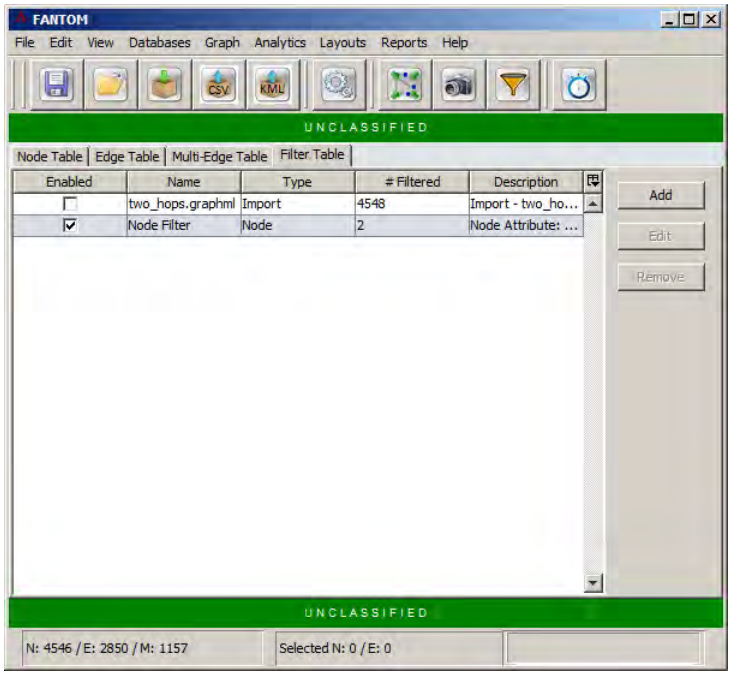
3. (U) Right-click the selection and choose the **Filter Nodes** command (or press the F key).

Figure 8-3: (U) Filter Nodes command



(U) The selected nodes disappear from the table and graph, and FANTOM adds a corresponding filter entry on the Filters tab. (Figure 8-4)

Figure 8-4: (U) Example of filter added from table



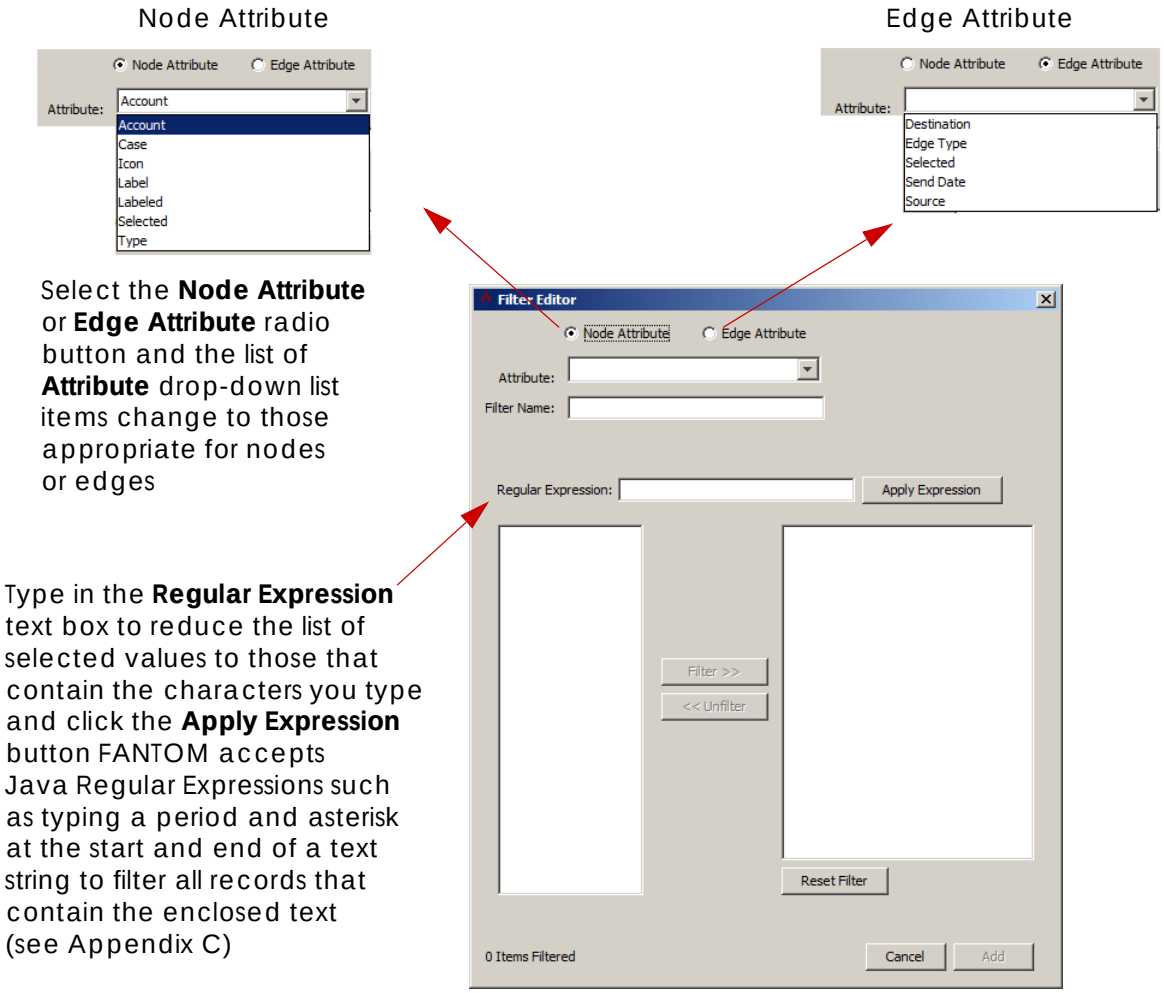
Adding a Filter by Attribute on the Filters Table Tab

(U) To add a filter by Attribute on the Filters Table tab:

1. (U) Access data and then perform a query.
2. (U) Click the **Filters Table** tab in the Controller window (Figure 8-4).
3. (U) Click the **Add** button.

   (U) The Filter Editor dialog box displays (Figure 8-5).

Figure 8-5: (U) Add Filter dialog box



4. (U) Select the **Node Attribute** or **Edge Attribute** radio button.
5. (U) Choose an **Attribute**.

   (U) When you choose an attribute, the text box at the bottom left becomes populated with a list of values in your data that occur in that attribute.

6. (U) Select one or more values to filter—that is, to exclude from the graph—and click the **Filter >>** button.

Note: (U) Based on the field you choose as the **Attribute**, you can use Java Regular Expressions to select records to highlight based on patterns in the field. For example, to find one word OR another, use the following format:

.* <*word*> | <*word*>.*

to find exact multiple words, use the following format:

.* <*word*> <*word*>.*

(U) For more information about Java Regular Expressions, see Appendix C "Java Regular Expressions."

(U) You can highlight multiple attribute values in one of these ways:

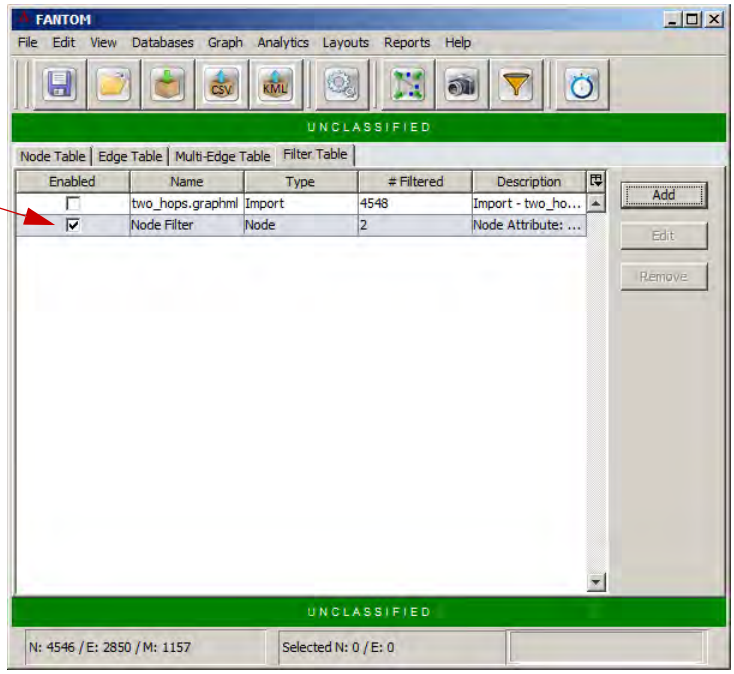
- (U) SHIFT+CLICK to select a contiguous range of items in the list.
- (U) Ctrl+click (Windows) or COMMAND+CLICK (Macintosh) to select a non-contiguous items in the list.

7. (U) Verify that you are satisfied with the selected Filter attributes that are excluded and included, and click the **Add** button.

(U) The Controller window becomes active again with the filter you just added listed in the Filters tab.

Figure 8-6: (U) Example of an added filter

After you add a filter, it displays in the Filters tab with its **Enabled** check box selected; you can add, remove, or edit a filter to show the nodes it is hiding based on the filter criteria you specified



(U) The graph in the Viewer window, and the tables in the Node Table, Edge Table, and Multi-Edge Table tabs show the reduced data set.

(U) While the filter is enabled, the layouts and analytics only apply to the filtered graph.

Disabling and Enabling a Filter

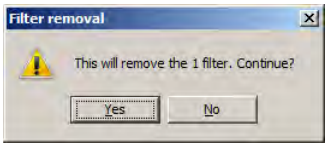
(U) **Disable a filter** – Go to the **Filters Table** tab and deselect the **Enabled** check box for the filter you want to disable.

(U) **Enable a filter** – Go to the **Filters** tab and deselect the **Enabled** check box for the filter you want to disable.

Removing a Filter

1. (U) Click the **Filters Table** tab in the Controller window.
2. (U) Select a filter to remove from the list.
3. (U) Click the **Remove** button.

   (U) FANTON displays a confirmation message asking if are sure you want to remove the filter.



4. (U) Click **Yes** to remove the filter or **No** to keep it.

Analyzing Your Data

(U) This chapter explains how to analyze your data in FANTOM using the following analytics:

- (U) Activity Date Range Analytic
- (U) Articulation Points Analytic
- (U) Attribute Colorizer
- (U) Case Count
- (U) Call Chaining Analytic
- (U) Centrality
  - (U) Betweenness Analytic
  - (U) Closeness Analytic
  - (U) Degree Analytic
  - (U) Eigenvector Analytic
- (U) Colorizer Analytic
- (U) Date Attribute Aggregation
- (U) DeDuplication Analytic
- (U) Financial Chaining Analytic
- (U) K-Core Analytic
- (U) Multi-Edge Date Range Analytic
- (U) Neighborhood Index Analytic
- (U) Non-Target Communication Analytic
- (U) Prestige Centrality Analytic

- (U) Reciprocated Links Analytic
- (U) Related Nodes Analytic
- (U) Social Network Analytic
- (U) Source to Destination Path Analytic
- (U) Using the Time Controller

(U) In general, all analytics commands operate on selected nodes or, if no nodes are selected, they operate on the entire graph.

Activity Date Range Analytic

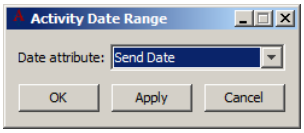
(U) The Activity Date Range analytic lets you add an Activity Start and Activity End column to the Controller window's Node Table which populates the rows based on source edge date values for the node in the **Date attribute** you select.

To specify an activity date range:

1. (U) Choose the **Analytics** > **Activity Date Range** command.

   (U) The Activity Date Range dialog box displays.

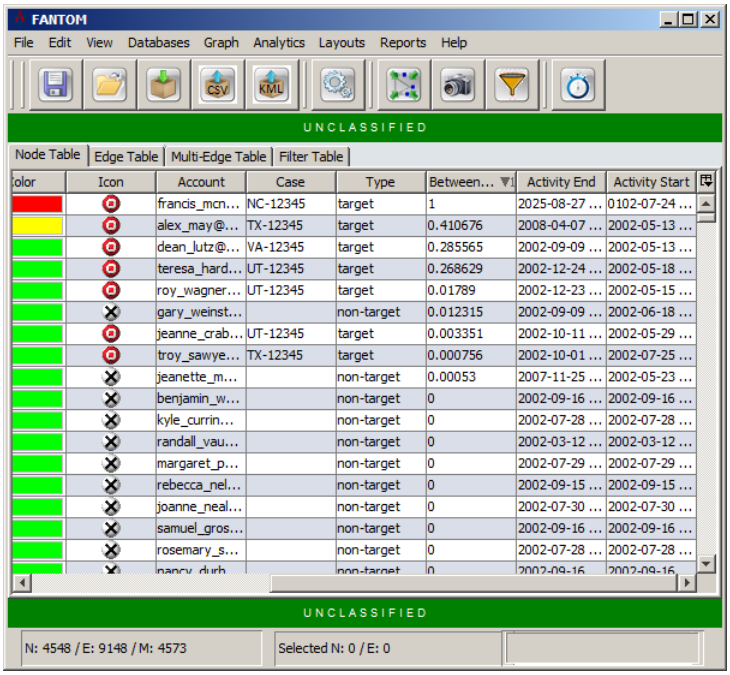
   Figure 9-1: (U) Activity Date Range dialog box

2. (U) Select a **Date attribute** and then click **OK**.

   (U) FANTOM adds an Activity Start and Activity End column to the Node Table. It determines the values by finding all the specified dates in the Edge table for the Source of each connection and then entering the first and last date in the corresponding column.

Figure 9-2: (U) Activity End and Activity Start date columns added to Node Table (two-hops.session)



Articulation Points Analytic

(U) The Articulation Points Analytic command identifies nodes in the graph that are like "bridges" between clusters of nodes. If you removed or filtered out these articulation point nodes from the Controller table, FANTOM would break the graph into multiple, independent clusters.

(U) The Articulation Points analytic is similar to the Betweenness Centrality analytic in that the goal of both is to help identify nodes that are important in some way. For Articulation, "important nodes" keep clusters in the graph connected globally. For Betweenness Centrality, "important nodes" are the busiest intersections.

(U) This analytic determines a true or false value of articulation for each node and adds it to an Articulation Point column in the Node Table.

Tip: (U) You can quickly see the nodes that are articulation points by clicking the **Articulation Points** column title until the **True** values are at the top. Or, if you kept the **Apply Colors** check box selected, you could sort the nodes by the **Color** column until the selected articulation point color is at the top.

Note: (U) To set your preferences for the Articulation Point analytic, see "Articulation Point Preferences" on page 11-7.

(U) To run the Articulation Point analytic:

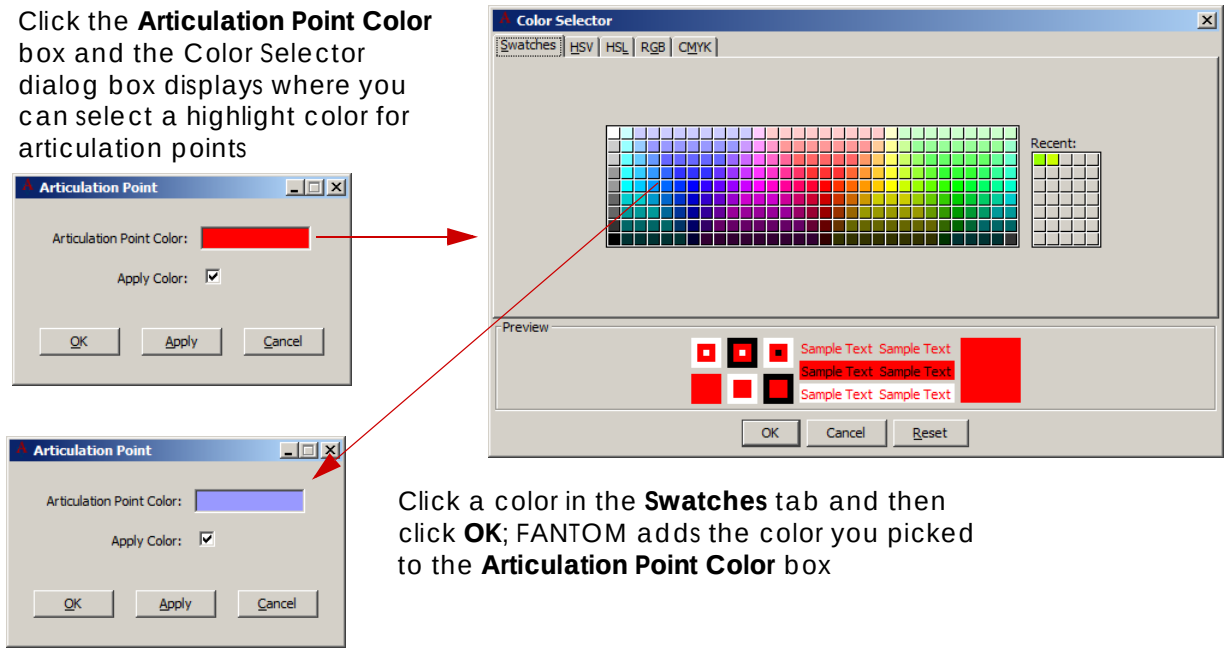
1. (U) Choose **Analytics** > **Articulation Points**.

   (U) The Articulation Point dialog box displays (Figure 9-3).

2. (U) Select options and then click **OK**:

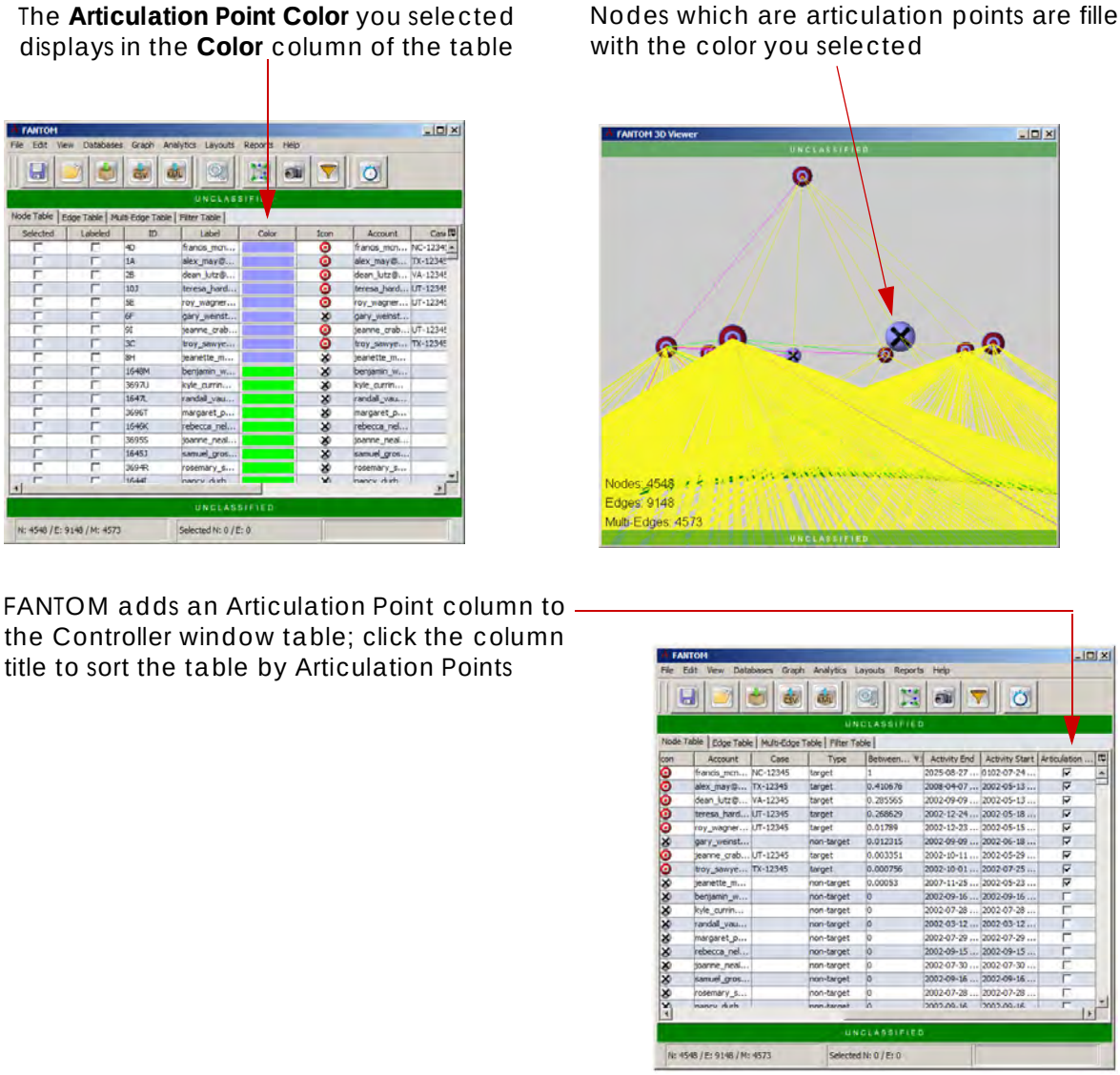
   - (U) Click the **Articulation Point Color** box to change the default green color in the Color Selector dialog box (Figure 9-3).

Figure 9-3: (U) Articulation Point dialog box (two-hops.session)



   - (U) Select the **Apply Color** check box (deselected by default) if you want articulation point nodes to be highlighted with the selected color in the Controller and FANTOM 3D Viewer windows.

Figure 9-4: (U) Articulation Point analytic results (two-hops.session)



Attribute Colorizer

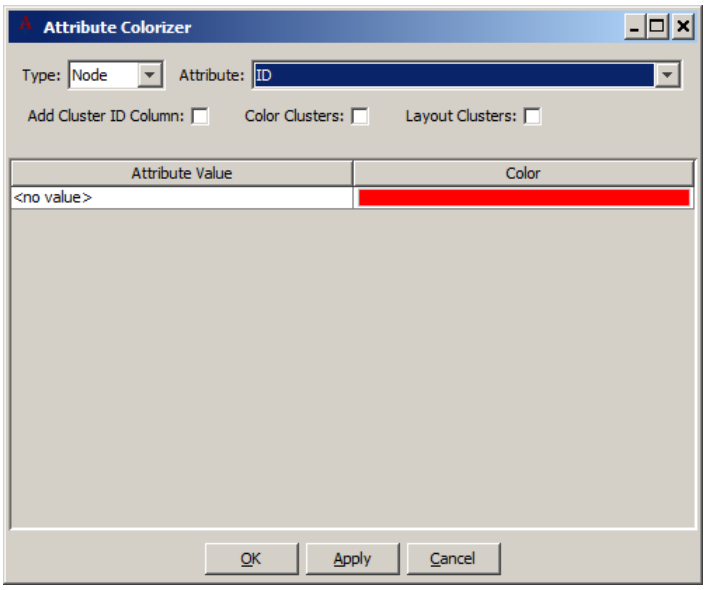
(U) FANTOM 3.1.3 and later combines the functionality of the Single Attribute Cluster Layout and Single Edge Attribute Cluster Analytic into the Attribute Colorizer analytic, and removed the former two.

(U) To run the Attribute Colorizer analytic:

1. Choose **Analytics** > **Attribute Colorizer**.

   The Attribute Colorizer dialog box displays (Figure 9-5).

Figure 9-5: Attribute Colorizer dialog box



2. (U) Select the **Type** of Node or Edge Table where the column values you want to color are located.

3. (U) Select the column to color as the **Attribute**.

4. (U) Select the other options (**Add Cluster ID Column**, **Color Clusters**, and **Layout Clusters**) if you like and then click **OK**.

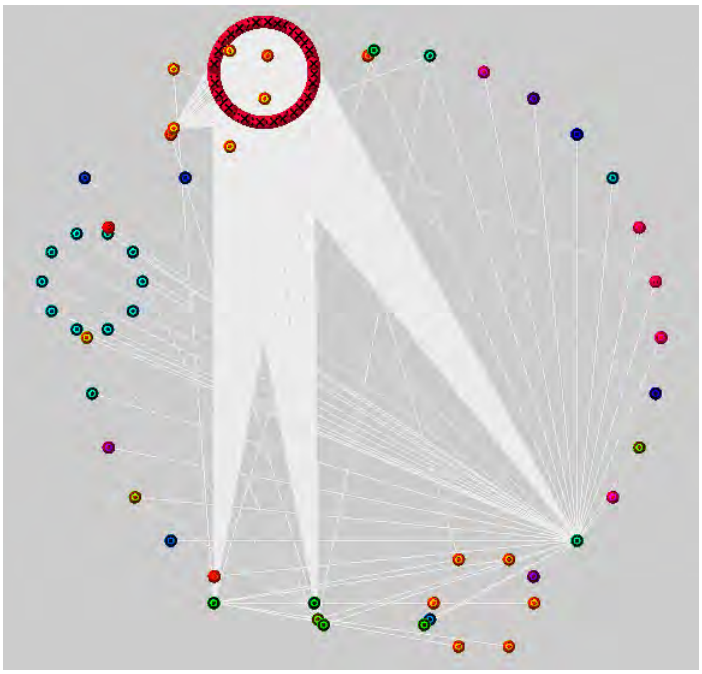
   (U) FANTOM rearranges the graph into clusters based on the attribute you selected.

   (U) If you selected **Add Cluster ID Column**, FANTOM adds a new Cluster ID column in the Node Table.

   (U) If you selected **Color Clusters**, FANTOM colors nodes in the Graph Viewer to identify the cluster each node is associated with.

   (U) If you selected **Layout Clusters**, FANTOM arranges the clusters in a circle with subgraph circles.

Figure 9-6: (U)Attribute Colorizer of a graph example



Case Count

(U) FANTOM can obtain a count of the following counts when columns are available in the Node Table that have the column title indicated below:

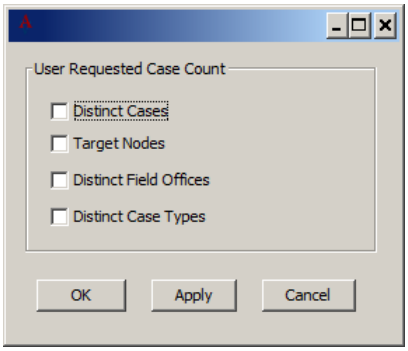
Get This Count	When Node Table Has This Column
Distinct Cases	Case
Target Nodes	Type (Values: target or non-target)
Distinct Field Offices	Case (Values: second part of case ID)
Distinct Case Types	Case (Values: first part of case ID)

(U) To run the Case Count:

1. (U) Choose **Analytics** > **Case Count**.

   (U) The Case Count dialog box displays (Figure 9-7).

Figure 9-7: (U) Case Count dialog box



2. (U) Select the check boxes for the counts you want to be calculated.
3. (U) Click **OK**.

   (U) FANTOM adds columns at the right side of the Node Table for each of the check boxes above that you selected.

Call Chaining Analytic

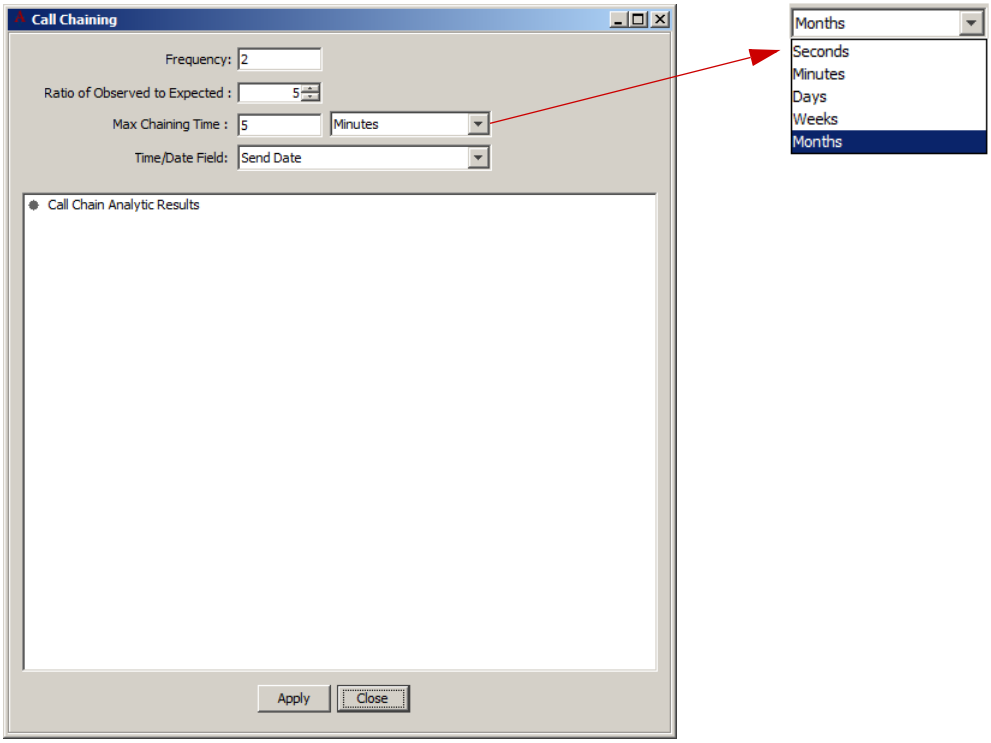
(U) The Call Chaining Analytic is intended to provide a search capability for communications-based data sets. Call chain analysis lets you analyze communications data for directly-linked graph events. In the case of call chain events, the domain is defined as linked communications (edges) occurring between entities (nodes) within a predetermined time frame. Call chaining can be used to find relevant sub-graphs within a specified domain, but can also provide statistical summaries of and predictive insight to communication pathways, gateways, and patterns. Call chains event sub-graphs will generally express small-world, scale-free network characteristics.

(U) To use the Call Chaining analytic:

1. (U) Choose **Analytics** > **Call Chaining**.

   (U) The Call Chaining Analytic dialog box displays (Figure 9-8).

Figure 9-8: (U) Call Chaining Analytic dialog box



2. (U) Set the **Max Chaining Time** units to **Months** unless the communications are primarily taking place more often.

3. (U) Click **Apply** and wait for the information to be calculated.

   (U) FANTOM changes the Call Chain Analytic Results icon from a document to a folder (Figure).

4. (U) Double-click the folder icon to expand the tree and examine the call chain details.

Centrality

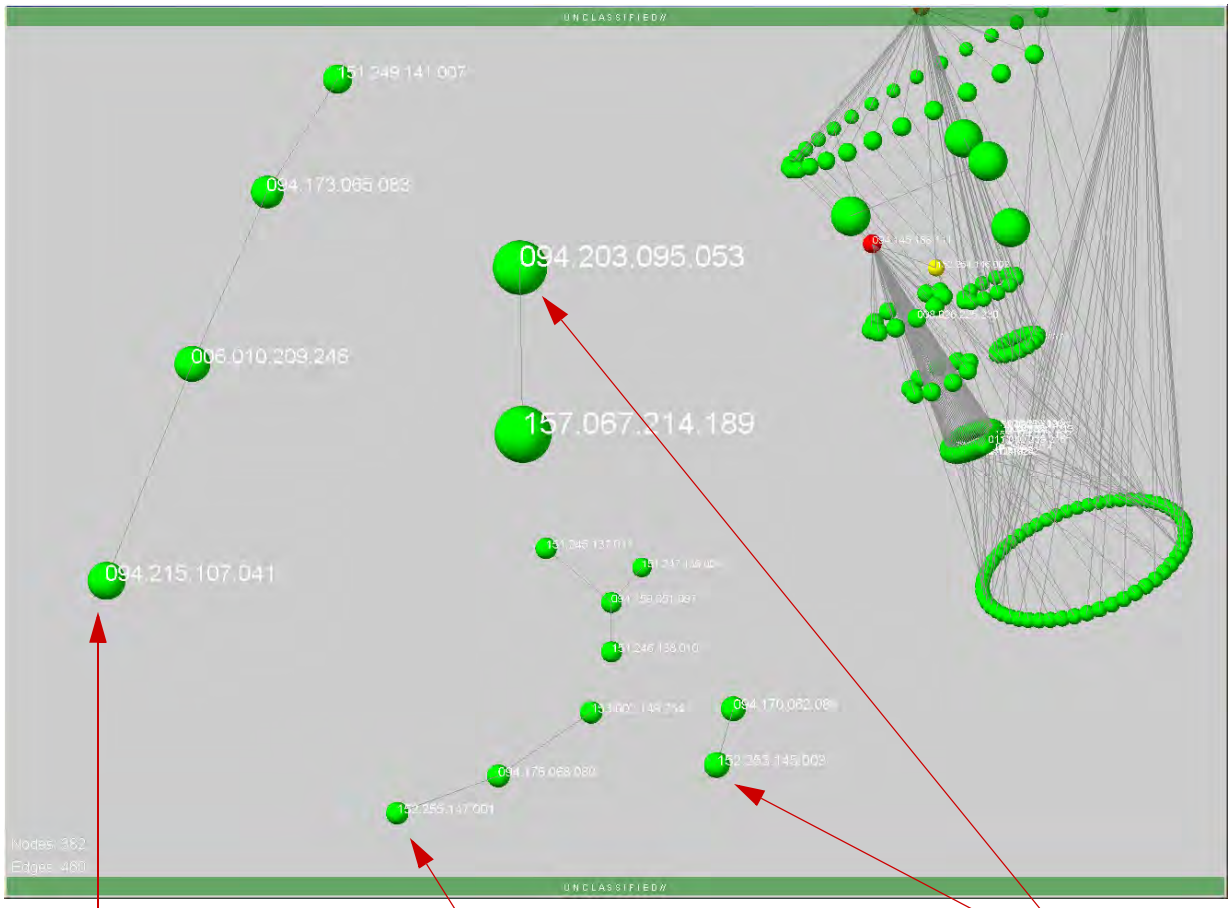
(U) The Centrality menu provides the following subcommands:

- Betweenness Analytic
- Closeness Analytic
- Degree Analytic
- Eigenvector Analytic

Betweenness Analytic

(U) Betweenness Centrality is a measure of the importance of a node in terms of how often it shows up as a critical part of a path between other nodes. One-hop, or direct, connections between two nodes are not included in Betweenness calculations, only two-hop, three-hop or longer paths connecting two nodes are considered.

Figure 9-9: (U) One-hop, two-hop, and three-hop examples



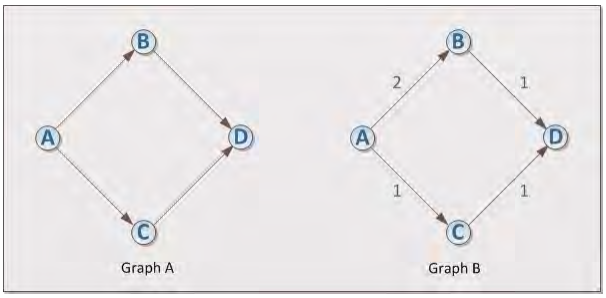
(U) The Betweenness Centrality analytic identifies nodes that are included in a large number of the shortest paths between two other nodes. In other words "all roads lead through" these highly central nodes. Nodes with the highest betweenness centrality (the red nodes) are the *busiest intersections*.

(U) This analytic calculates centrality based on the weighted likelihood—determined by edge counts of relevant paths— that a given node shows up in the shortest path between all other pairs of nodes. The higher the Betweenness value, the stronger the bond between a node and other connected nodes.

(U) If you *deselect* the **Use Edge Direction** check box, then paths are taken into account without regard to the edge direction where a node is a "go between".

(U) If you *select* **Use Edge Direction**, then these paths take into account the direction of edges when calculating shortest paths. If more than one edge exists between a pair of nodes (e.g. multi-edges) then the betweenness centrality score factors in this influence 'weight'. In this calculation we interpret more weight to mean more influence (e.g. more communications = more frequent contact => greater influence). Thus paths that contain edges with high weights are more likely to be taken and nodes along these paths are considered more influential, and therefore have a higher betweenness centrality. Consider the simple diagrams below.

Figure 9-10: (U) Using Edge Direction diagrams



(U) In Graph A and B the only non-trivial paths between a pair of nodes is between A and D (the other paths do not contain any intermediate nodes). The two paths of interest for Betweenness calculations are A -> B -> D and A -> C -> D. In Graph A nodes B and C have a betweeness score of 1 while nodes A and D have a betweeness of 0.

(U) Edge weights (often based on frequency of communications or edge count) as shown in Graph B change this calculation. Note that this applies only when there are multiple paths with the same number of hops. When **Use Edge Direction** is selected, path A->B->D has a weight of 2+1=3 and path A->C->D = 2. Thus node B gets a weights of 3 and node C gets a weight of 2. When normalized (see next paragraph) these are reduced to node B = 2/3 = 0.67 and node C = 1/3 = 0.33. Nodes A and D still get a score of 0.

(U) Betweenness centrality scores are normalized so that all values are between 0 (zero) and 1 for each node in the graph. This allows you to understand the relative, rather than absolute, importance of each node in the graph.

(U) Normalization is accomplished simply by dividing all raw scores by the maximum. Nodes are also placed into three colored categories: high (red), medium (yellow) and low (green), to make it easy to visually identify the most central nodes. If you keep the **Apply Colors** check box selected, the analytic changes the nodes' **Color** value to red, yellow, or green for the highest, medium, and lowest level of betweenness centrality scores, respectively.

Tip: (U) You can quickly see the nodes with the highest betweenness centrality by clicking the **Betweenness Centrality** column title until the biggest scores are at the top. Or, if you kept the **Apply Colors** check box selected, you could sort the nodes by the **Color** column until the red colors are at the top.

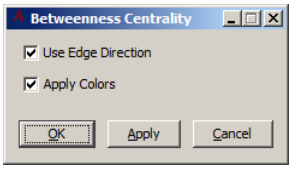
Note: (U) To set your preferences for the Betweenness analytic, see "Betweenness Preferences" on page 11-9.

To run the Betweenness analytic:

1. (U) Choose **Analytics** > **Betweenness**.

   (U) The Betweenness Centrality dialog box displays (Figure 9-11).

Figure 9-11: (U) Betweenness Centrality dialog box



2. (U) Select options and then click **Apply** or **OK**:

   - (U) **Use Edge Direction** – Select the **Use Edge Direction** check box and these paths take into account the direction of edges when calculating shortest paths.
   - (U) **Apply Colors** – Select or deselect this check box to apply or not apply colors to nodes as illustrated in Figure 9-12.

Figure 9-12: (U) Betweenness Centrality analytic results in Controller (two-hops.session)

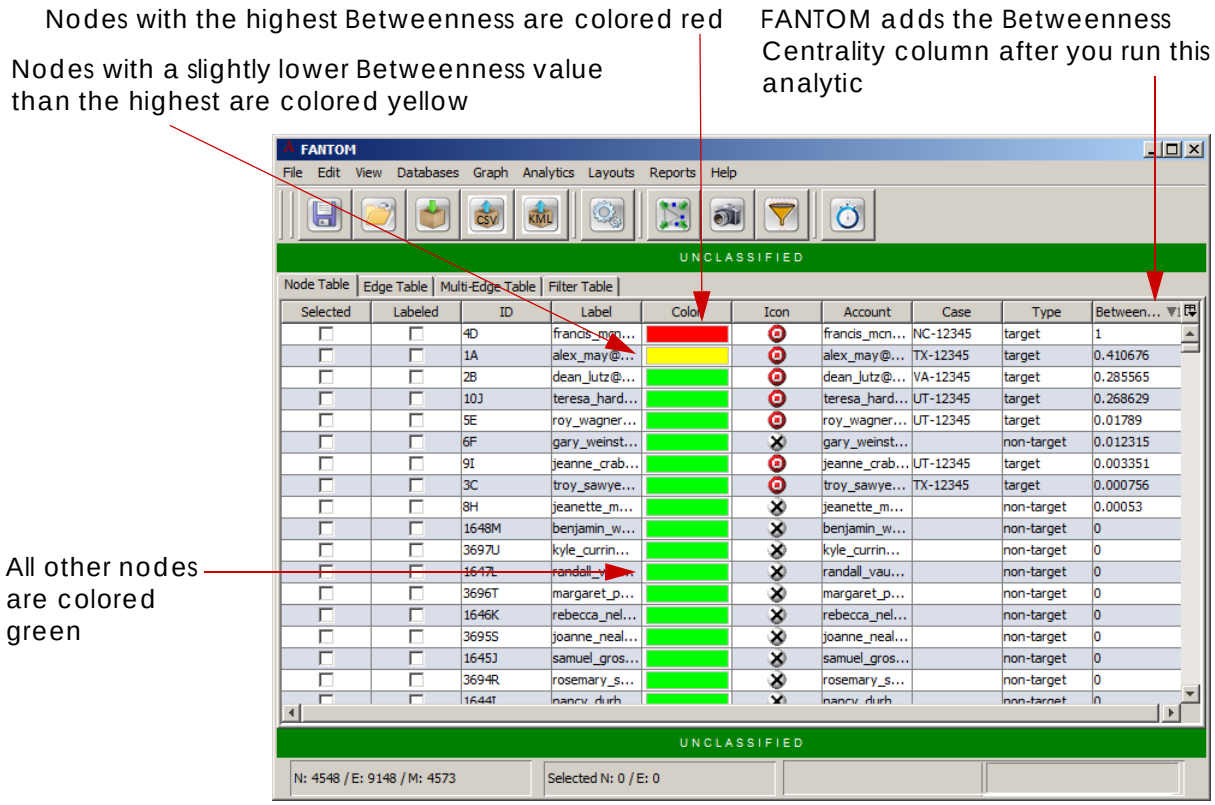
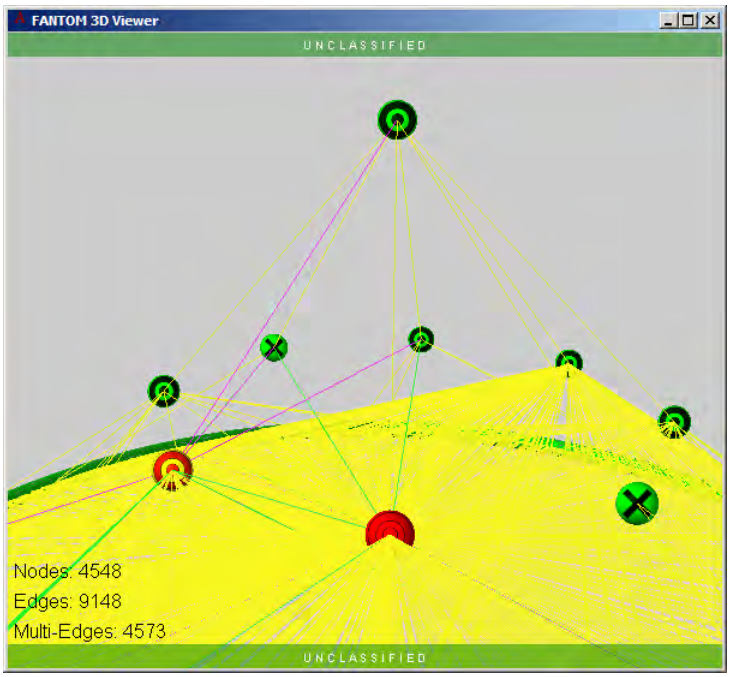


Figure 9-13: (U) Betweenness Centrality results in 3D Viewer (two-hops.session)



Closeness Analytic

Note: (U) The information in this topic enclosed in quotation marks is extracted from *Introduction to social network methods*, "Chapter 10. Centrality and power" an online text by Robert A. Hanneman (Department of Sociology, University of California, Riverside) and Mark Riddle (Department of Sociology, University of Northern Colorado). The full text is available on the Internet at:

http://faculty.ucr.edu/~hanneman/nettext/C10_Centrality.html

(U) "Closeness centrality approaches emphasize the distance of an actor to all others in the network by focusing on the distance from each actor to all others. Depending on how one wants to think of what it means to be "close" to others, a number of slightly different measures can be defined."

Path distances

(U) "Network>Centrality>Closeness provides a number of alternative ways of calculating the "far-ness" of each actor from all others. Far-ness is the sum of the distance (by various approaches) from each ego to all others in the network."

(U) ""Far-ness" is then transformed into "nearness" as the reciprocal of farness. That is, nearness = one divided by farness. "Nearness" can be further standardized by norming against the minimum possible nearness for a graph of the same size and connection."

(U) "Given a measure of nearness or farness for each actor, we can again calculate a measure of inequality in the distribution of distances across the actors, and express "graph centralization" relative to that of the idealized "star" network."

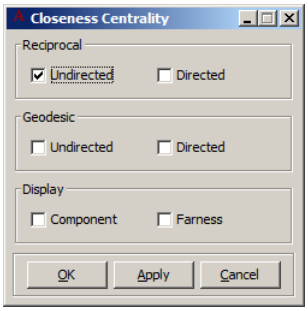
(U) These different measures of what it means to be "close" are defined where you make the related selections in the following procedure (step 2).

(U) To use the Closeness Centrality analytic:

1. (U) Choose **Analytics** > **Closeness Centrality**.

   (U) The Closeness Centrality dialog box displays (Figure 9-14).

Figure 9-14: (U) Closeness Centrality dialog box



2. (U) Select any combination of the following options:

   - (U) **Reciprocal** options: **Undirected** and/or **Directed**.
     - (U) Selecting the **Undirected** check box causes FANTOM to add the **Closeness Centrality (Both)** column.
     - (U) Selecting the **Directed** check box causes FANTOM to add the **Closeness Centrality (Output)** and **Closeness Centrality (Input)** columns at the right.

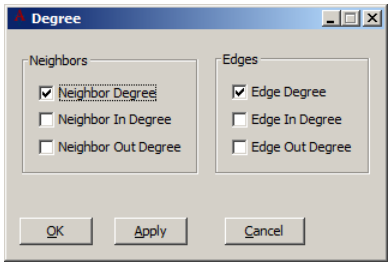
Note: (U) If you select one of these options, FANTOM makes the **Farness Display** option active.

   - (U) **Geodesic** options: **Undirected** and/or **Directed**.
     - (U) Selecting the **Undirected** check box causes FANTON to add the **Closeness Centrality (Geodesics Both)** column.
     - (U) Selecting the Directed check box causes FANTOM to add the **Closeness Centrality (Geodesics Output)** and **Closeness Centrality (Geodesics Input)** columns.
   - (U) **Display** options: **Component** and/or **Farness**.
     - (U) Selecting the **Component** check box causes FANTOM to add the **Groups (Components)** and **Size (Components)** columns.
     - (U) Selecting the **Farness** check box with the **Reciprocal Undirected** check box also selected causes FANTOM to add the **Farness (Both)** and **Closeness Centrality (Both)** columns.
     - (U) Selecting the **Farness** check box with the **Reciprocal Directed** check box also selected causes FANTOM to add the **Closeness Centrality (Output)**, **Farness (Input)**, **Farness (Output)**, and **Closeness Centrality (Input)** columns.

Degree Analytic

(U) The Degree analytic command can compute the number of connections between different nodes in a variety of ways.

Figure 9-15: (U) Degree Analytic dialog box



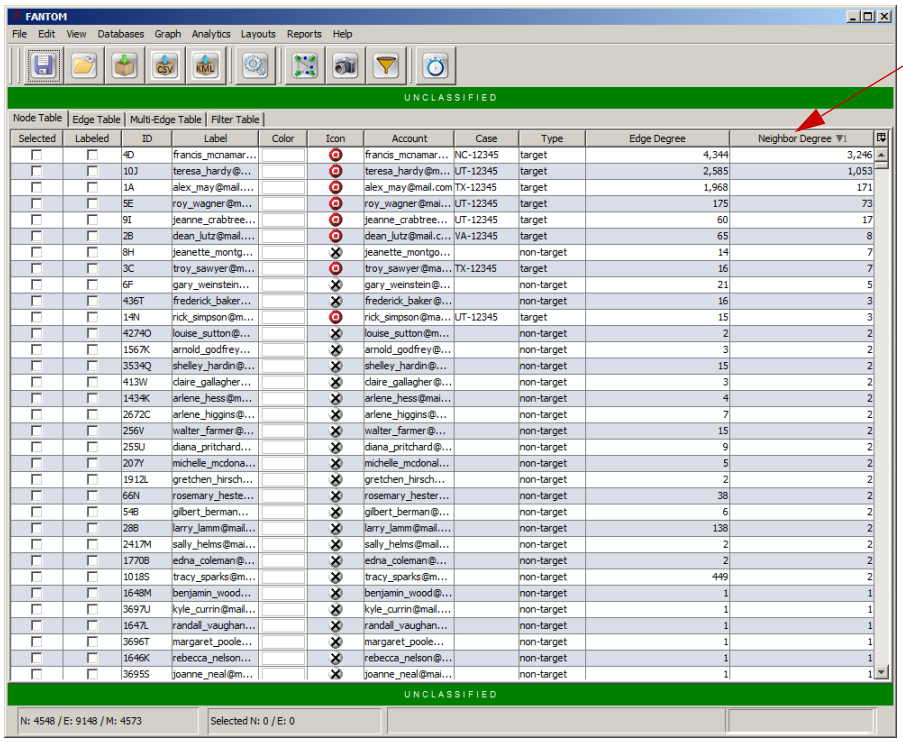
(U) There is an *multi-edge* between two nodes when there is at least one connection between them. There is a *edge* between two nodes for every connection between them. For example, there might be several calls between two phone numbers, making several edges but only one multi-edge. Therefore, the Degree analytic can count both edges and multi-edges, as desired. For many graphs the edge originates with one node (like a phone call) and terminates with another (called a *directed edge*). Therefore, the Degree analytic can count incoming, outgoing, and total for each node, depending on what you select.

(U) To run the Degree analytic:

1. (U) Choose **Analytics** > **Degree**.
2. (U) Select any combination of the following check boxes and then click **Apply** or **OK**:
   - (U) **Neighbor Degree** – The sum of the neighbors in and out degrees.
   - (U) **Parent Degree** – The number of communications entering a node.
   - (U) **Child Degree** – The number of communications originating from a specified node.
   - (U) **Edge Degree** – The sum of the edge in and out degrees.
   - (U) **Edge In Degree** – The number of connections that enter a specific node.
   - (U) **Edge Out Degree** – The number of connections that originate from a specific node.

   (U) The Degree analytic adds the selected options as columns in the Node Table tab in the Controller window.

Figure 9-16: (U) Degree results (two-hops.session)



Double-click a **Neighbor Degree Neighbors** cell and FANTOM displays a list of all the values in the cell

Eigenvector Analytic

(U) *Eigenvector Centrality* is the measure of the importance of a node.

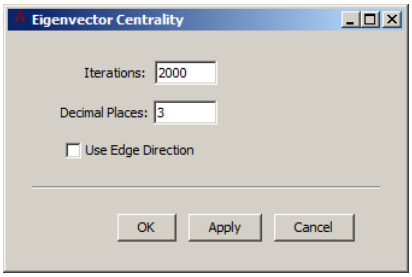
(U) The Eigenvector Centrality analytic adds an **Eigenvector Centrality** column to the Controller window's Node tab that populates each cell with a value between zero and one. The value is a percentage, with one being the item with the highest Eigenvector Centrality.

(U) Figure 9-18 shows an example of the results of running this analytic and performing the following actions:

1. (U) Choose **Analytics** > **Eigenvector Centrality**.

   (U) The Eigenvector Centrality dialog box displays (Figure 9-17).

Figure 9-17: (U) Eigenvector Centrality dialog box

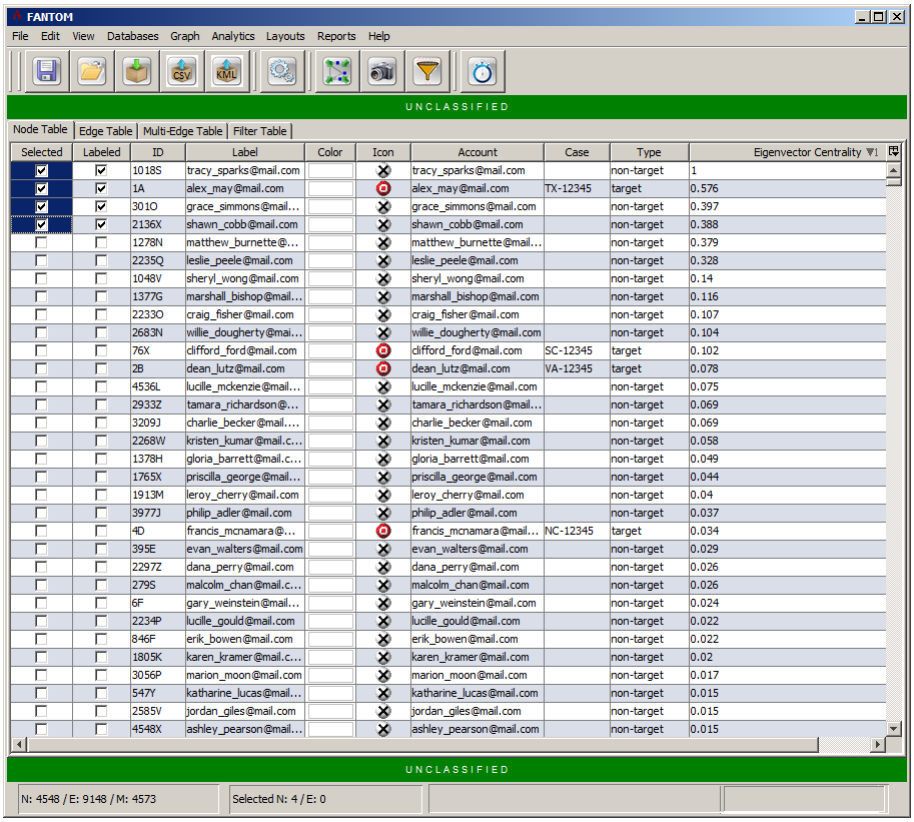


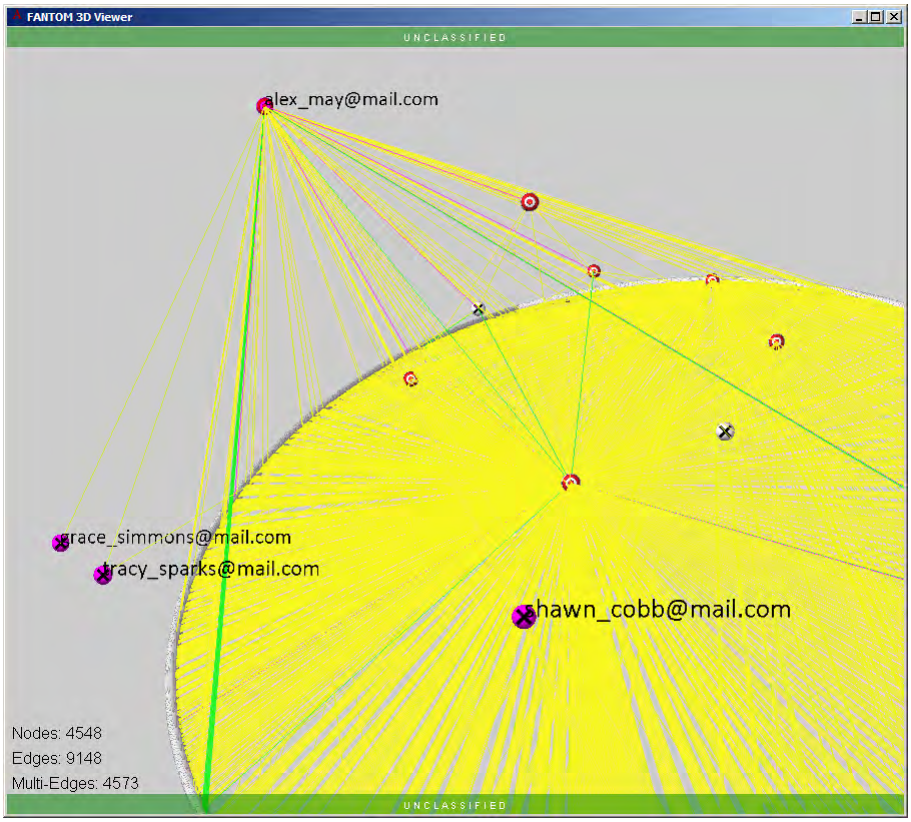
2. (U) Select options or accept the defaults and click **OK**.

(U) FANTOM adds an Eigenvector Centrality column in the Controller window's Node Table.

3. (U) Click the **Eigenvector Centrality** column title twice to sort with the highest value at the top.
4. (U) Drag to highlight the nodes with the highest numbers.
5. (U) Right-click and choose **Select Nodes**, and then right-click and choose **Set Color**.
6. (U) Select a color for these nodes and click **OK**.
7. (U) Hold down the ALT key while dragging away from the center of the graph so you can see the connections more clearly.

Figure 9-18: (U) Eigenvector Centrality analytic results with top four nodes selected





Colorizer Analytic

(U) The Colorizer Analytic lets you define rules that will color or select nodes or edges based on:

- (U) Attributes you specify and
- (U) Whether or not the nodes or edges are selected.

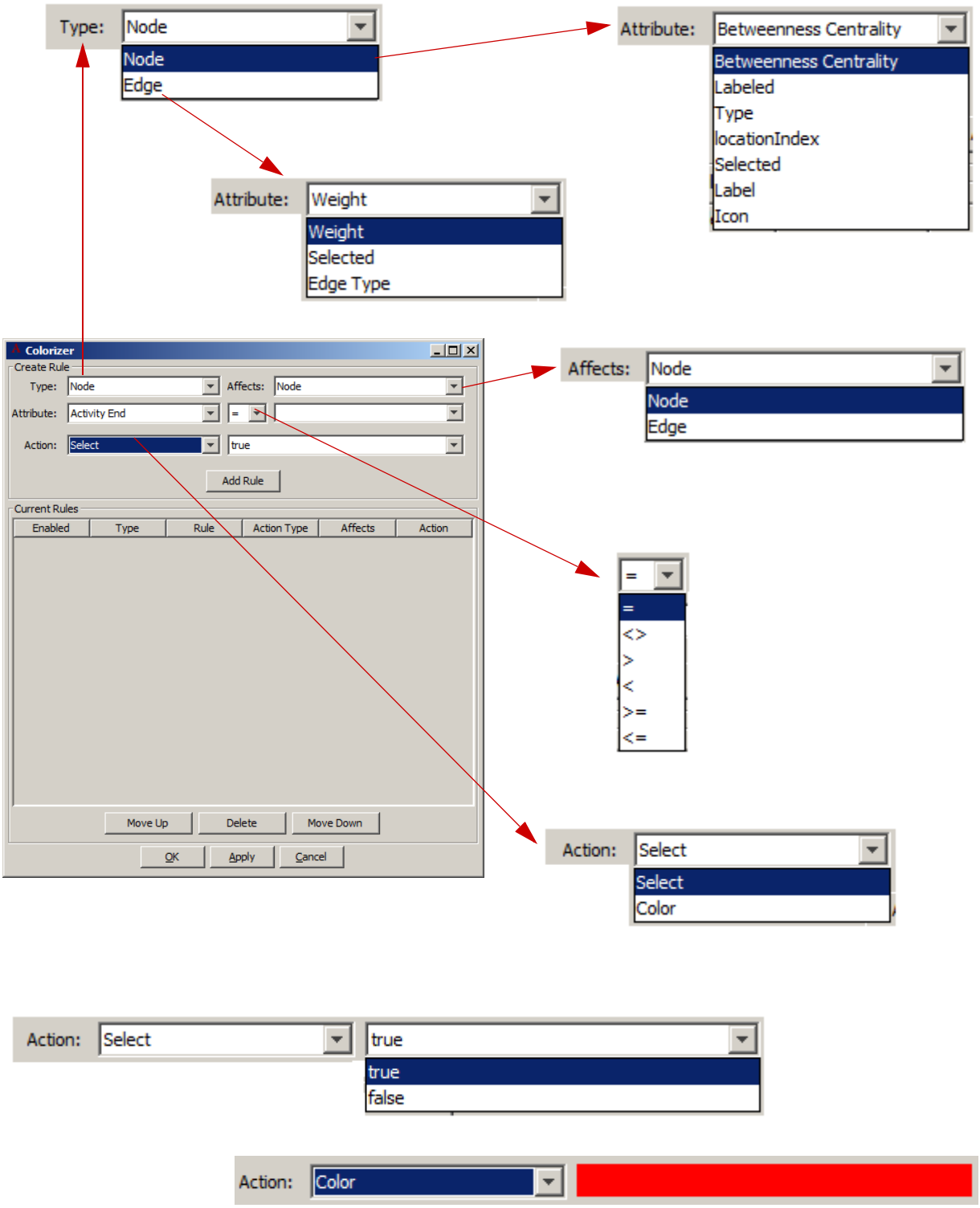
(U) When enabled and performed (by clicking **Apply** or **OK**), your rules will either select or color nodes or edges based on attributes that have interesting properties to you. After running a rule that either selects or colors nodes or edges, you can sort the **Color** or **Selected** column in the Controller window to make it locate the items of interest more quickly.

(U) **To run the Colorizer analytic:**

1. (U) Choose **Analytics** > **Colorizer**.

   (U) The Colorizer dialog box displays (Figure 9-19).

Figure 9-19: (U) Colorizer dialog box



2. (U) Select rule options, click the **Add Rule** button, and then click **Apply** or **OK**:

- (U) **Type** – Choose a type of **Node** or **Edge** that the rule criteria applies to.
- (U) **Affects** – Choose whether the rule should colorize nodes or edges. For example, you might add a rule that colorizes based on a column in the Node Table (the **Type** is set to Node) but set **Affects** to Edge so that FANTOM colors the edges based on the node value matching the rule.
- (U) **Attribute** / **Operator** / **Value** – The attributes available depend on whether you chose **Node** or **Edge**:
  - (U) **Node** – Available attributes are the Node Table column titles with the exception of **Color**.
  - (U) **Edge** – Available attributes are the Edge Table column titles with the exception of **Source**, **Destination**, and **Color**.

  (U) The Attribute you choose determines the available Operators and Value type
- (U) **Action** / **Value** – Choose an action of **Select** or **Color**. The available **Value** format depends on your **Action** choice.

Note: (U) Another way to color nodes based on an attribute is using the **Color Clusters** option in "Attribute Colorizer."

Date Attribute Aggregation

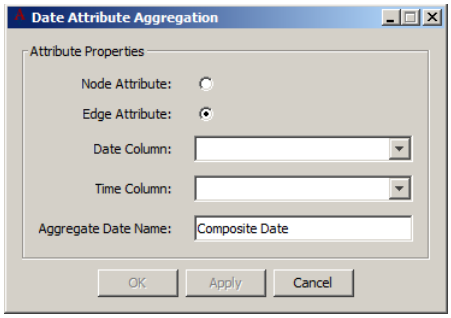
(U) The Date Attribute Aggregation analytic lets you merge separate Date and Time columns and create a third combined Date/Time column so that the data can be analyzed using the FANTOM Time Controller.

To run the Date Attribute Aggregation analytic:

1. (U) Import data or open a session that contains a separate Date and Time column.
2. (U) Choose **Analytics** > **Date Attribute Aggregation**.

   (U) FANTOM displays the Date Attribute Aggregation dialog box (Figure 9-20).

Figure 9-20: (U) Date Attribute Aggregation dialog box



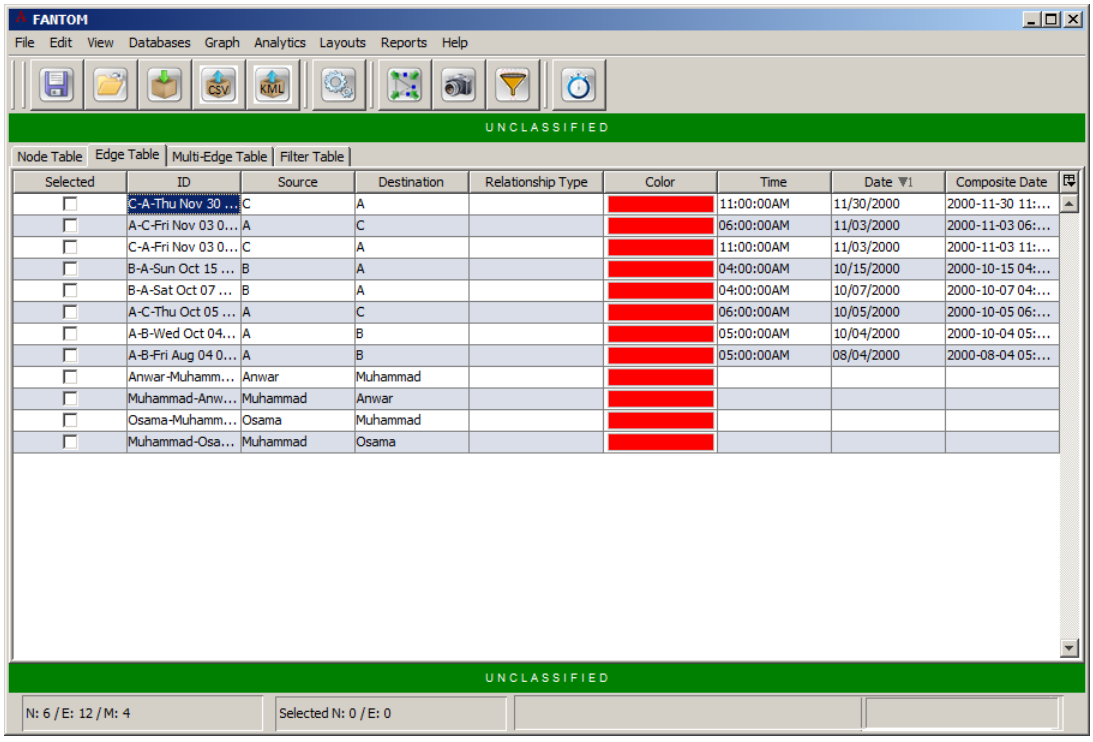
3. (U) Select the **Node Attribute** or **Edge Attribute** radio button to indicate the table where the Date and Time columns are located in the Controller window.

4. (U) Select a **Date Column** and a **Time Column**.

5. (U) Type a name for the combined column in the **Aggregate Date Name** text box and then click **OK**.

6. (U) FANTOM adds your new column to the Node or Edge table.

Figure 9-21: (U) Aggregate date column (Date_Time_after_Aggregation.session)



DeDuplication Analytic

(U) When you import data sets into FANTOM, it automatically eliminates exact duplicates where the values in all columns of a row are identical to the values in another row. However, in some data sets, such as financial data, multiple transactions may occur on the same date and for the same amount, but come from different sources and also be defined as "duplicates."

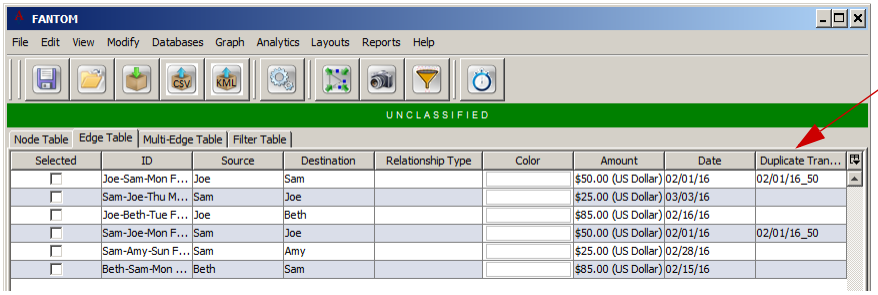
(U) The DeDuplication analytic identifies duplicate transactions and allow the user to review the potential duplicate transactions and provide the user the option to ignore them. It may be necessary for the user to identify a specific column as the source and create a new attribute type that can be used in this process.

To run the DeDuplication analytic:

1. (U) Import data or open a session that contains a column imported into FANTOM as a **Date** or **Date/Time** and one or two columns imported as a **Currency** amount.
2. (U) Choose **Analytics** > **DeDuplication**.

   (U) FANTOM examines the dates and currency amounts to identify potential duplicates.

Figure 9-22: (U) DeDuplication adds a Duplicate Transactions column (DeDuplication-simple-example.session)



FANTOM examines currency values in the specified sequential date range to find possible duplicates and adds a column to the Edge table with the results

Financial Chaining Analytic

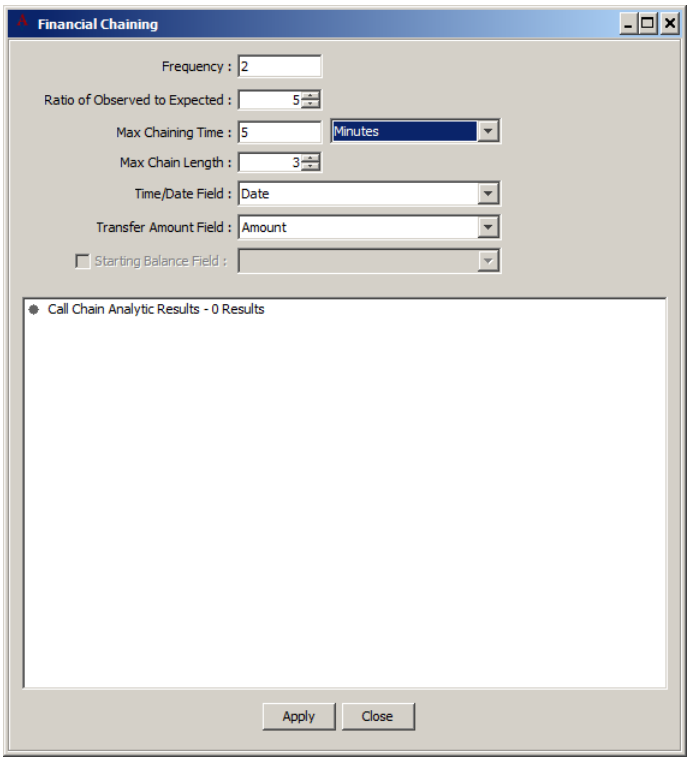
(U) The Financial Chaining analytic is based on the Call Chaining analytic and allows you to trace backwards to identify victims and where the money came from.

To run the Financial Chaining analytic:

1. (U) Choose **Analytics** > **Financial Chaining**.

   (U) The Financial Chaining dialog box displays (Figure 9-23).

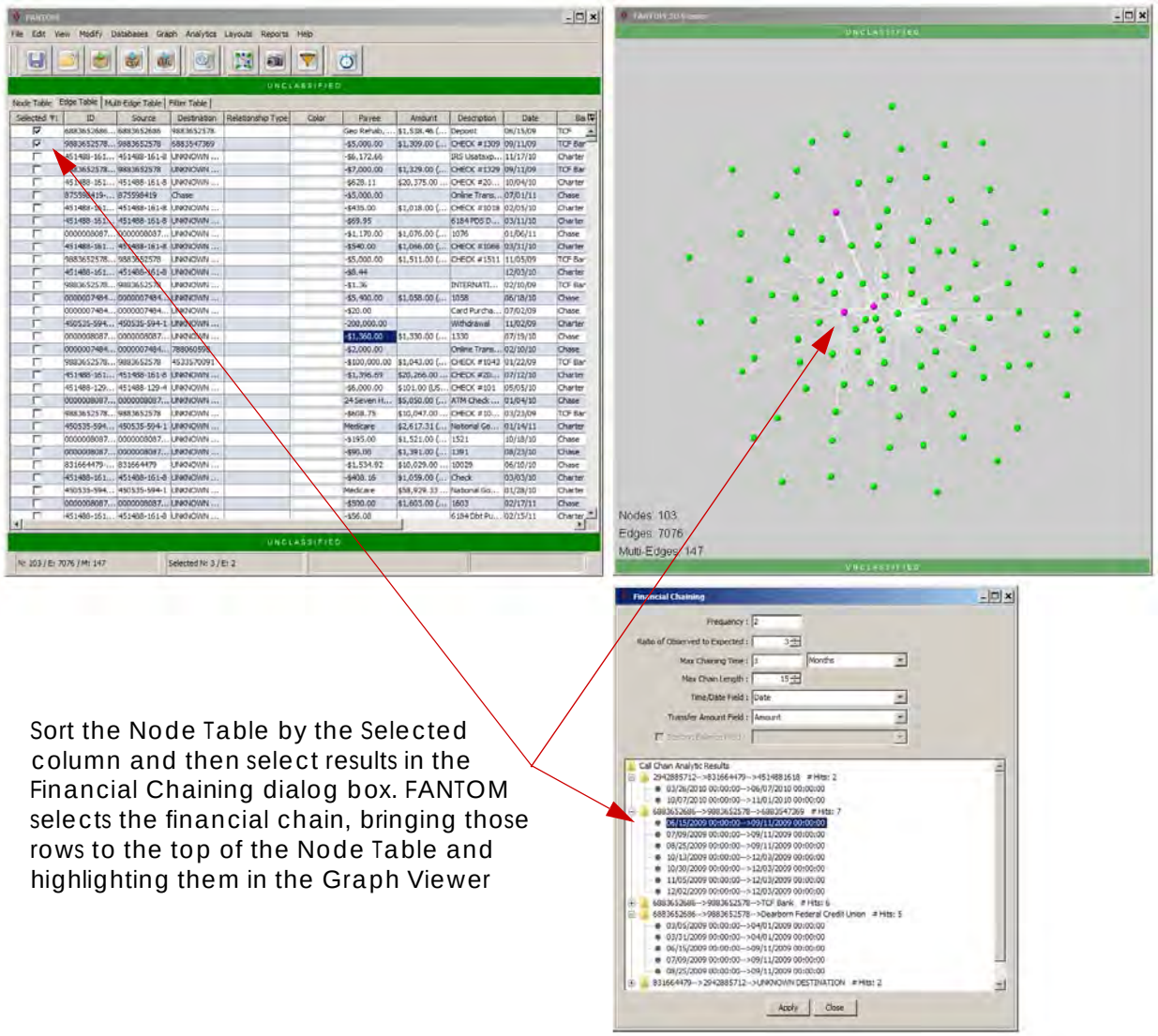
Figure 9-23: (U) Financial Chaining dialog box



2. (U) Select the following options and then click **Apply**:

   - (U) **Frequency** –
   - (U) **Ratio of Observed to Expected** –
   - (U) **Max Chaining Time** – Set the Max Chaining Time to Months initially and then reduce the time period if you want to reduce the results.
   - (U) **Max Chain Length** –
   - (U) **Time/Date Field** – Select the title of the Date/Time column for these transactions.
   - (U) **Transfer Amount Field** – Select the title of the currency column for these transactions.

Figure 9-24: (U) Financial Chaining results example



K-Core Analytic

(U) The K-Core analytic identifies a community where each node is a member of the community when it is connected to at least *K* other nodes in the subgroup.

Caution: (U) The K-Core analytic can take a long time depending on the number of nodes and edges. For example, one data set with 20,000 edges took 12 hours to complete. K-Core performs extensive processing to determine the connections between each node and all others in a data set. FANTOM team recommends that for large data sets, you may want to start running the analytic before leaving work for the day.

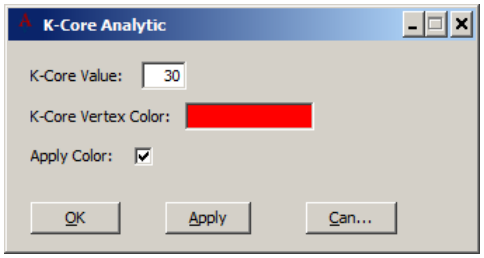
(U) To reduce the time needed to perform K-Core calculations, FANTOM uses the Half Intervals method.

To run the K-Core analytic:

1. (U) Choose **Analytics** > **KCore**.

   (U) The K-Core Analytic dialog box displays.

   Figure 9-25: K-Core Analytic dialog box

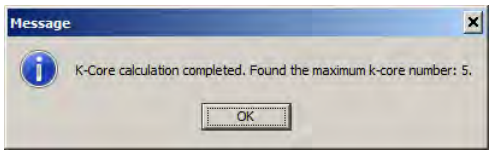


2. (U) Select the following options or accept the defaults and then click **OK**:

   - (U) **K-Core Value** – The default K-Core Value is set to 30. This is the number of connections that a node must have with one or more other nodes in the subgraph for it to be considered a member of the subgraph.
   - (U) **K-Core Vertex Color** – Select the color that you want FANTOM to apply to nodes in the identified subgroup.
   - (U) **Apply Color** – Keep the Apply Color check box selected if you want nodes in the identified subgroup to have the K-Core Vertex Color applied to them in the Node Table and Graph Viewer window.

   (U) If the maximum number of connections is less than the K-Core Value specifed, FANTOM displays a message to let you know the maximum number. It uses this number to complete the analysis.

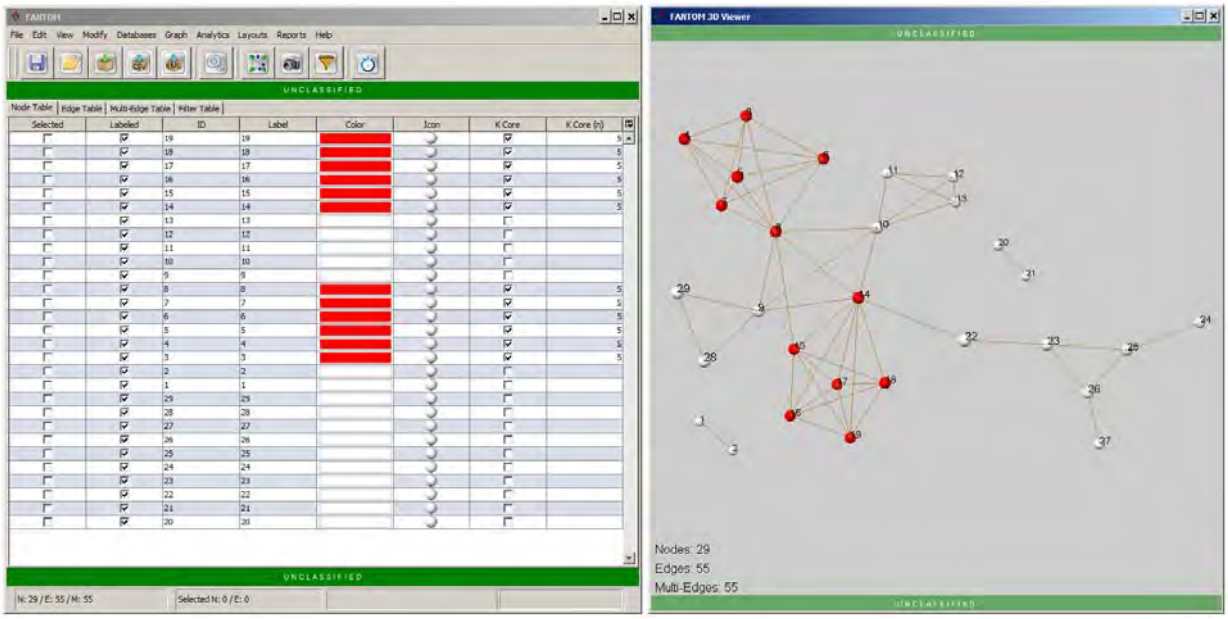
   Figure 9-26: (U) K-Core calculation message



3. (U) Click **OK**.

   (U) FANTOM identifies the subgraph and if you have the Apply Color check box selected, it highlights the nodes so you can see the community more easily in the Graph Viewer window (Figure 9-27).

Figure 9-27: (U) K-Core analysis results with nodes in the subgraph colored red (K-Core-Sample.session)



Multi-Edge Date Range Analytic

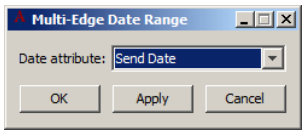
(U) The Multi-Edge Date Range analytic adds an Activity Start and Activity End column to the Multi-Edge table and provides the corresponding dates for each row.

(U) **To run the Multi-Edge Date Range:**

1. (U) Choose **Analytics** > **Multi-Edge Date Range**.

   (U) The Multi-Edge Date Range dialog box displays.

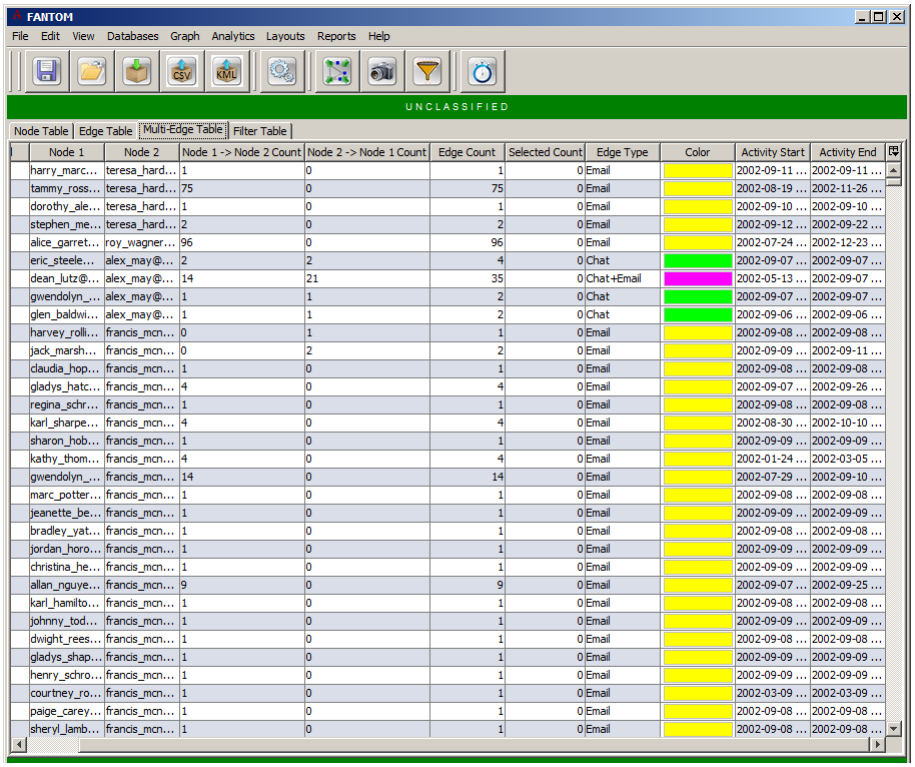
Figure 9-28: (U) Multi-Edge Date Range dialog box



2. (U) Choose a date column from the **Date attribute** menu.
3. (U) Click **OK**.

   (U) FANTOM adds an Activity Start and Activity End column to the Multi-Edge table, populating the cells with dates for each row of the table.

Figure 9-29: (U) Activity Start and Activity End columns on the Multi-Edge table



Node 1	Node 2	Node 1 -> Node 2 Count	Node 2 -> Node 1 Count	Edge Count	Selected Count	Edge Type	Color	Activity Start	Activity End
harry_marc...	teresa_hard...	1	0	1	0	Email		2002-09-11 ...	2002-09-11 ...
tammy_ross...	teresa_hard...	75	0	75	0	Email		2002-08-19 ...	2002-11-26 ...
dorothy_ale...	teresa_hard...	1	0	1	0	Email		2002-09-10 ...	2002-09-10 ...
stephen_me...	teresa_hard...	2	0	2	0	Email		2002-09-12 ...	2002-09-22 ...
alice_garret...	roy_wagner...	96	0	96	0	Email		2002-07-24 ...	2002-12-23 ...
eric_steele...	alex_may@...	2	2	4	0	Chat		2002-09-07 ...	2002-09-07 ...
dean_lutz@...	alex_may@...	14	21	35	0	Chat+Email		2002-05-13 ...	2002-09-07 ...
gwendolyn_...	alex_may@...	1	1	2	0	Chat		2002-09-07 ...	2002-09-07 ...
glen_baldwi...	alex_may@...	1	1	2	0	Chat		2002-09-06 ...	2002-09-06 ...
harvey_rolli...	francis_mcn...	0	1	1	0	Email		2002-09-08 ...	2002-09-08 ...
jack_marsh...	francis_mcn...	0	2	2	0	Email		2002-09-09 ...	2002-09-11 ...
claudia_hop...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
gladys_hatc...	francis_mcn...	4	0	4	0	Email		2002-09-07 ...	2002-09-26 ...
regina_schr...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
karl_sharpe...	francis_mcn...	4	0	4	0	Email		2002-08-30 ...	2002-10-10 ...
sharon_hob...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
kathy_thom...	francis_mcn...	4	0	4	0	Email		2002-01-24 ...	2002-03-05 ...
gwendolyn_...	francis_mcn...	14	0	14	0	Email		2002-07-29 ...	2002-09-10 ...
marc_potter...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
jeanette_be...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
bradley_yat...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
jordan_horo...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
christina_he...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
allan_nguye...	francis_mcn...	9	0	9	0	Email		2002-09-07 ...	2002-09-25 ...
karl_hamilto...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
johnny_tod...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
dwight_rees...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
gladys_shap...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
henry_schro...	francis_mcn...	1	0	1	0	Email		2002-09-09 ...	2002-09-09 ...
courtney_ro...	francis_mcn...	1	0	1	0	Email		2002-03-09 ...	2002-03-09 ...
paige_carey...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...
sheryl_lamb...	francis_mcn...	1	0	1	0	Email		2002-09-08 ...	2002-09-08 ...

Neighborhood Index Analytic

(U) The Neighborhood Index Analytic command compares the neighbors of all nodes with the selected nodes. This analytic has no options, so just choose the command to run it.

(U) This analytic returns, for each node, the number of selected nodes that are its neighbors. This analytic adds a column to the node table in the Controller window.

(U) Neighborhood Index is useful when trying to determine which nodes in a large graph are well connected to a set of "interesting nodes". These interesting nodes could be known targets or victims. With a score for every node, it is easy to sort on that column and identify potential new nodes of interest. That is, nodes with many connections to known important nodes might be important themselves.

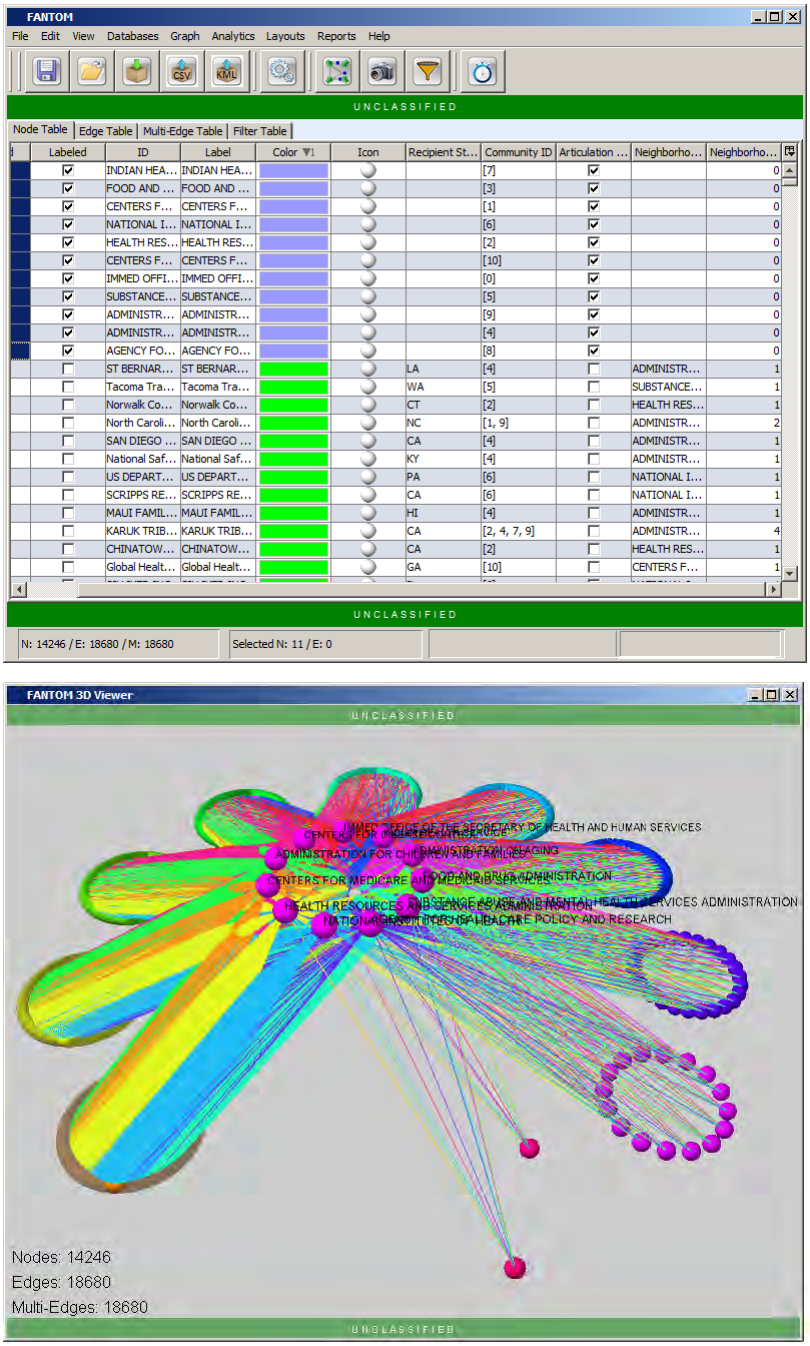
(U) To run the Neighborhood Index analytic:

1. (U) Select one or more nodes.
2. (U) Choose **Analytics** > **Neighborhood Index**.

   (U) FANTOM runs the analytic and adds the results in a **Neighborhood Index** column of the Node Table.

Tip: (U) You might want to follow this analytic by running the **Layouts** > **Single Attribute Cluster Layout** command, selecting **Neighborhood Index** as the **Cluster Attribute**, and selecting both check boxes to organize and color the clusters so they stand out more clearly.

Figure 9-30: (U) Neighborhood Index analytic results followed by Single Attribute Cluster Layout with Neighborhood Index selected as the cluster and Color Clusters option selected



Non-Target Communication Analytic

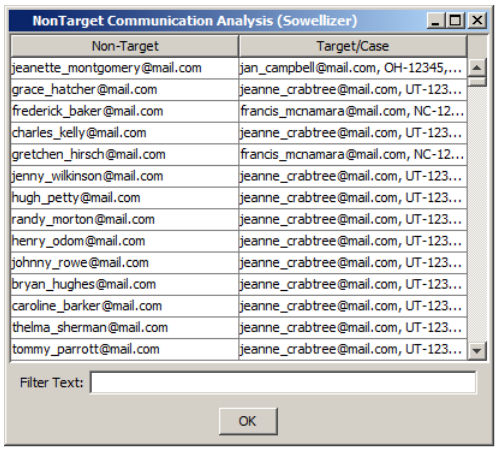
(U) This analytic produces a simple table containing non-targets who communicated to the target. The table displays the date range within which the communications took place.

To run the Non-Target Communication Analysis Analytic:

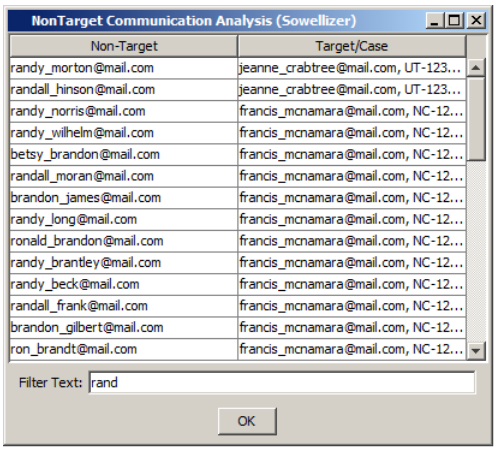
1. (U) Select one or more target **Type** nodes.
2. (U) Choose **Analytics** > **Non-Target Communication Analysis**.

   (U) FANTOM displays the Non-Target Communication Analysis (Sowellizer) dialog box.

Figure 9-31: (U) Non-Target Communication Analysis (Sowellizer)



Unfiltered list



Filtered list

3. (U) Type characters in the **Filter** text box.

   (U) FANTOM shows only Non-Target entries containing the combination of characters you've typed. These characters can be in any location.

Tip: (U) You can copy/paste selected list rows in this dialog box to another application, such as to Microsoft Word or Excel. To do this, drag up or down in the list. Press CTRL+C to place the selected text on the Clipboard, and then Paste the information elsewhere.

Prestige Centrality Analytic

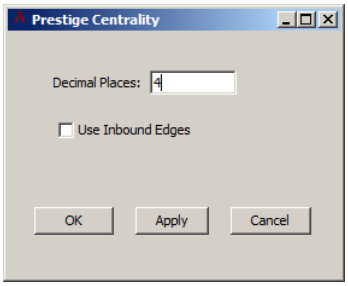
(U) The Prestige Centrality analytic adds a **Prestige Centrality** column to the Controller window's Node tab that populates each cell with a value between zero and one. The value is a percentage, with one being the node that has the highest Prestige Centrality. *Prestige* is an indication of power within a group. This can be indicated, for example, by a node who communicates only once before an event is triggered. It can also be indicated by a node who communicates the most.

(U) Figure 9-33 shows an example of the results of running this analytic and performing the following actions:

1. (U) Choose **Analytics** > **Prestige Centrality**.

   (U) The Prestige Centrality dialog box displays.

   Figure 9-32: (U) Prestige Centrality dialog box

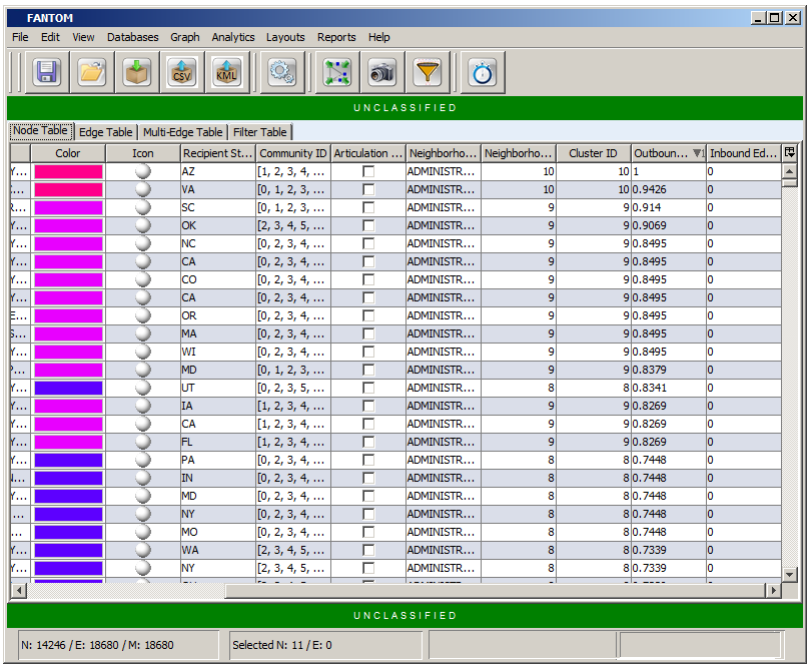
2. (U) Select the **Use Inbound Edges** check box or leave it deselected (which uses Outbound Edges) and click **OK**.

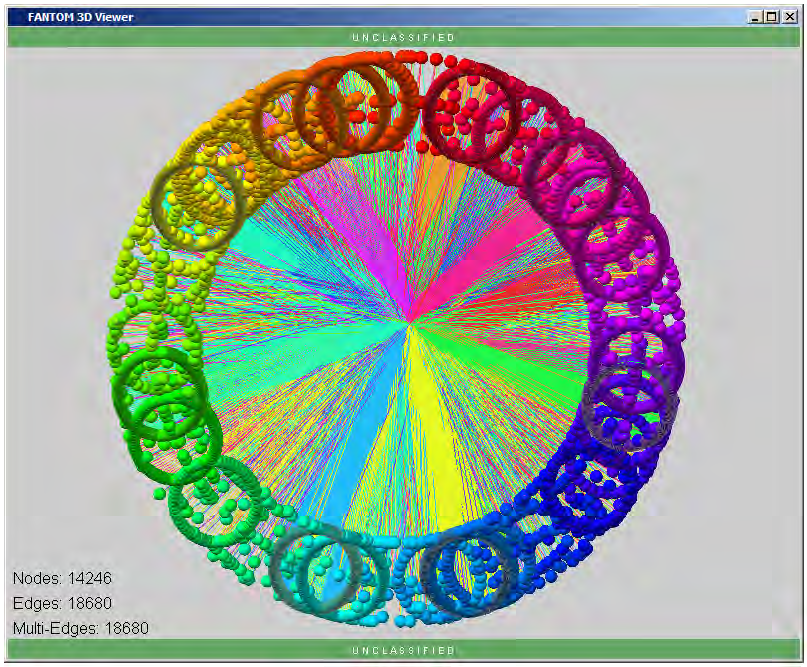
   (U) FANTOM adds a Prestige Centrality column in the Controller window's Node Table.

3. (U) Click the **Prestige Centrality** column title twice to sort with the highest value at the top.

   (U) You may want to run the Layouts > Single Attribute Cluster Layout command and select Prestige Centrality as the attribute to more easily see the results in the graph (Figure 9-33).

Figure 9-33: (U) Example of Prestige Centrality analytic with Single Attribute Cluster Layout run afterward using Outbound Edge Prestige Centrality as the attribute





Related Nodes Analytic

(U) The Related Nodes analytic lets you compare all nodes to the node chosen in the **Node** menu of the Related Nodes dialog box.

Note: (U) All values produced by the Related Nodes analytic–in the Neighborhood Similarity, Longest Common String, String Edit Distance, Alias Min, Alias Mean, and Allis Max columns of the Node Table–are "normalized." This means the results only range between 1 and zero (0).

(U) For example, if you select osama@yahoo.com, this analytic will find other occurrences of osama@yahoo.com (and return a value of 1.0 to indicate the two values are identical). In addition, it identifies similar values like osama@gmail.com or osama590@msn.com, and defines the similarity as a percentage using decimal numbers (1.0 is identical, 0.9 is 90 percent, 0.8 is 80 percent, and so on).

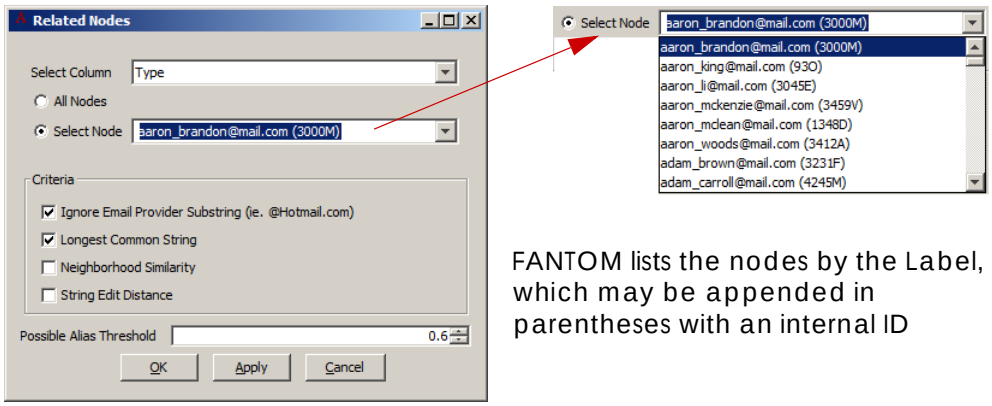
Note: (U) To set your preferences for the Related Nodes analytic, see "Related Nodes Preferences" on page 11-27.

(U) To run the Related Nodes analytic:

1. (U) Choose **Analytics** > **Related Nodes Analytic**.

   (U) The Related Nodes Analytic dialog box displays (Figure 9-34).

Figure 9-34: (U) Related Nodes Analytic dialog box



2. (U) Select the following options and then click **Apply** or **OK**:

   - (U) **Node** – Select a node to which you want to compare all other nodes in the data set.

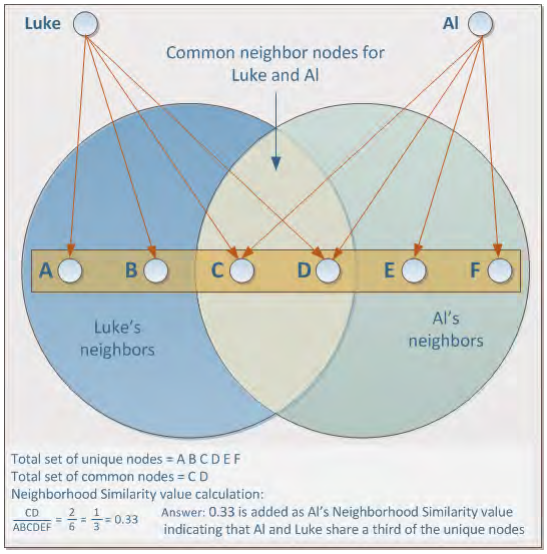
Note: (U) If you select a different node and rerun this analytic, FANTOM updates only the Related Nodes columns in the Node Table that you select each time. It retains the data in any of the **Criteria** or

Aggregation Method columns that haven't been selected in the latest run. Since the **Aggregation Method** columns are derived from the Criteria, you need to select each one and click the **Apply** button to update those columns of data after you analyze a different node. FANTOM lets you hide columns, but the data is retained throughout a session.

- (U) **Criteria** – Select any of the following check boxes; FANTOM performs the indicated calculations and adds a corresponding column in the Node Table to display the results:
  - (U) **Neighborhood Similarity** – This criteria discovers the set of neighbors for the chosen node and then compares it to the set of neighbors for each of the other nodes in the data set.

    (U) Given the node that is chosen in the **Node** menu, FANTOM discovers who the neighbors are for that node (the other nodes who have relationships with the selected node). Then it finds the node relationship for each of the other nodes which are then compared to the selected node.Figure 9-35

Figure 9-35: (U) How many friends do Al and Luke share? Related Nodes Neighborhood Similarity example

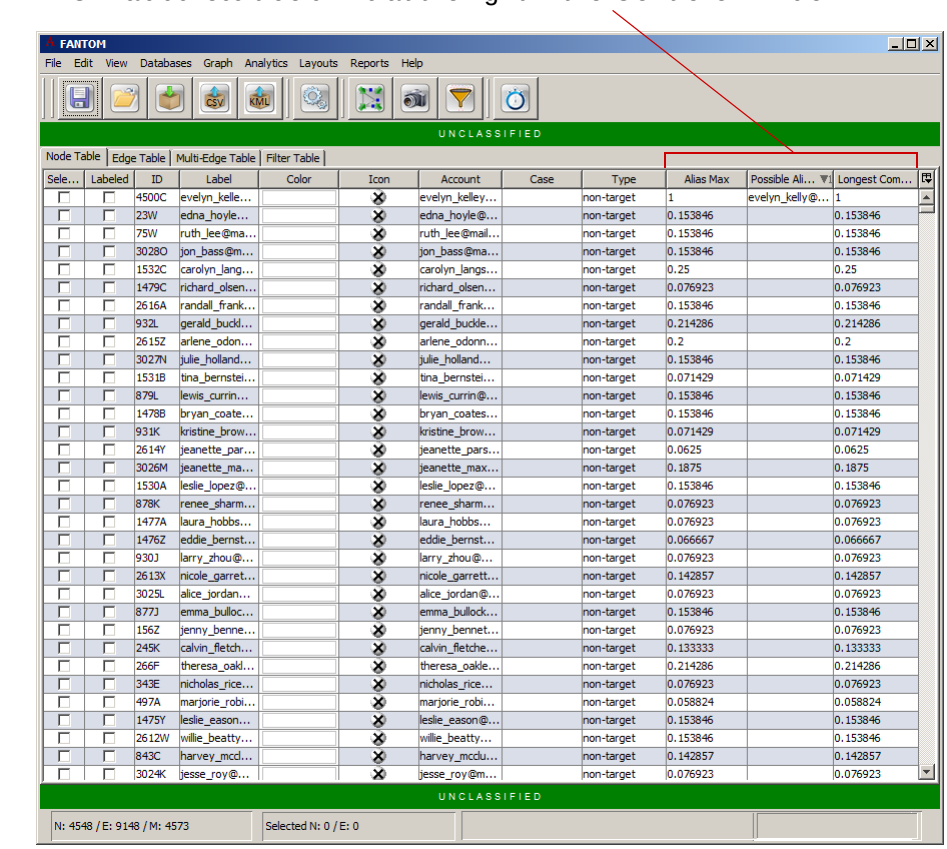


  - (U) **Longest Common String** criteria – This analytic determines the longest common string between the selected node and each of the other nodes in the data set. It indicates the longest common string as a percentage.
  - (U) **String Edit Distance** criteria – This criteria calculates how many keystrokes would be needed to change one value to the other between the selected item and other items in the table.

- (U) **Aggregation Method** – FANTOM offers three aggregation methods; each of which produces a separate column of results:
  - (U) **Minimum Aggregation** – Displays the smallest result for each node among the up to three criteria you selected: **Neighborhood Similarity**, **Longest Common String**, and **String Edit Distance**.
  - (U) **Mean Aggregation** – *Mean* is the average of a set of numbers. It is calculated by summing a set of numbers and then dividing by the count of numbers in that set. If you select this aggregation method, FANTOM adds an **Alias Mean** column in the Node Table after you run the Related Nodes analytic.
  - (U) **Maximum Aggregation** – Displays the largest result for each node among the up to three criteria you selected: **Neighborhood Similarity**, **Longest Common String**, and **String Edit Distance**.

(U) See the example results in Figure 9-36.

Figure 9-36: (U) Example of Related Nodes results



Report Service

(U) FANTOM version 3.1.0.x and later provide a separate Reports menu to make it easier to navigate to and use reports. See Chapter 10, "Using Reports"

Reciprocated Links Analytic

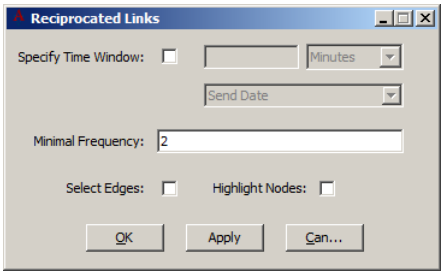
(U) The Reciprocated Links analytic finds strongly connected pairs of nodes with bidirectional links.

(U) To run the Reciprocated Links analytic:

1. (U) Choose **Analytics** > **Reciprocated Links**.

   (U) The Reciprocated Links dialog box displays (Figure 9-37).

   Figure 9-37: (U) Reciprocated Links *dialog box*



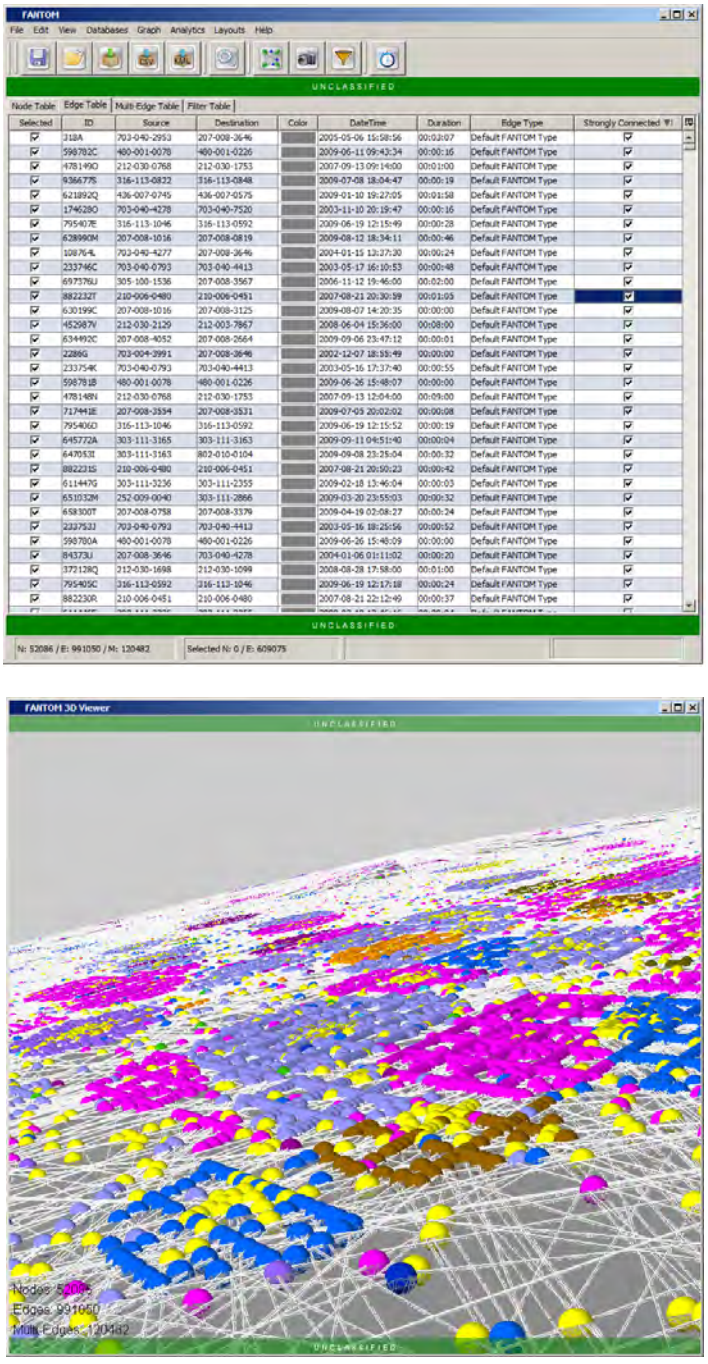
2. (U) Select the following options and then click **OK**:

   - (U) **Specify Time Window** – Select the Specify Time Window check box and then type the length of time and choose the time unit within which activity much occur to be counted for reciprocated. If you don't enter a value, time is not considered when determining reciprocation.
   - (U) **Minimum Frequency** – Type the minimum number of times A to B and B to A must occur within the time window for the nodes A and B to be selected. The default is 2.
   - (U) **Select Events** – If you select this check box, FANTOM selects the events in the events table that satisfy these user-given parameters.
   - (U) **Highlight nodes** – If you select this check box, FANTOM colors the nodes that participate in a reciprocated relationship with one (or more) other nodes.

   (U) FANTOM adds a **Strongly Connected** column in the Node Table listing any nodes that have a strong connection to each node. Multiple

strongly connected nodes are separated by commas. If you selected the **Highlight Nodes** check box, you can quickly see which nodes have reciprocated nodes.

Figure 9-38: (U) Reciprocated Links with edges selected (telephone.graphml sample data)



Social Network Analytic

(U//FOUO) FANTOM offers several presets: SNA: High Leader, SNA: Emerging Leader, SNA: Gatekeeper/Facilitator, and SNA: Boundary Spanner.

Figure 9-39: (U//FOUO) Social Network Analytic dialog box

Source to Destination Path Analytic

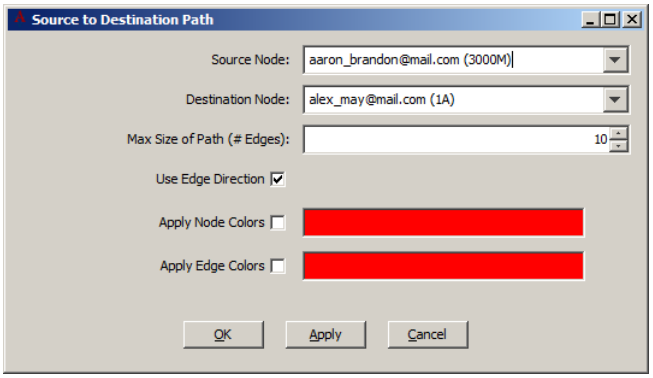
(U) Use the Source to Destination Path analytic to find the shortest path between a source and target node.

(U) To run the Source to Destination Path analytic:

1. (U) Choose **Analytics** > **Source to Destination Path**.

   (U) The Source to Destination Path dialog box displays (Figure 9-40).

Figure 9-40: (U) Source to Destination Path Analytic dialog box



2. (U) Choose a **Source Node** and a **Target Node** from the respective menus.

   (U) If you have one or more nodes selected before running this analytic, FANTOM displays only the selected nodes in these two menu. If no nodes are selected, the Label IDs of all nodes are accessible in these menu.

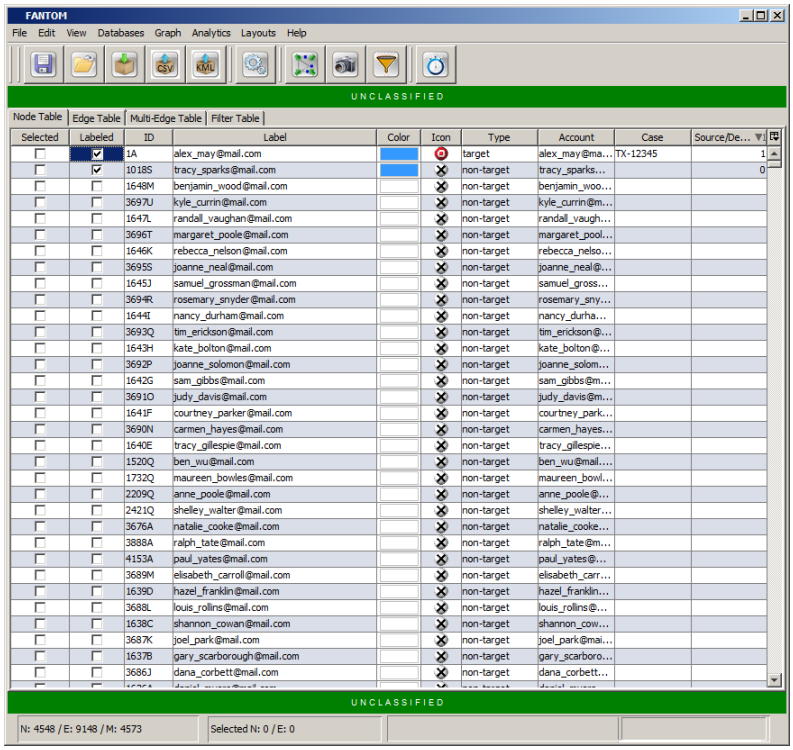
3. (U) Select other options and then click **OK** or **Apply** to run the analytic:

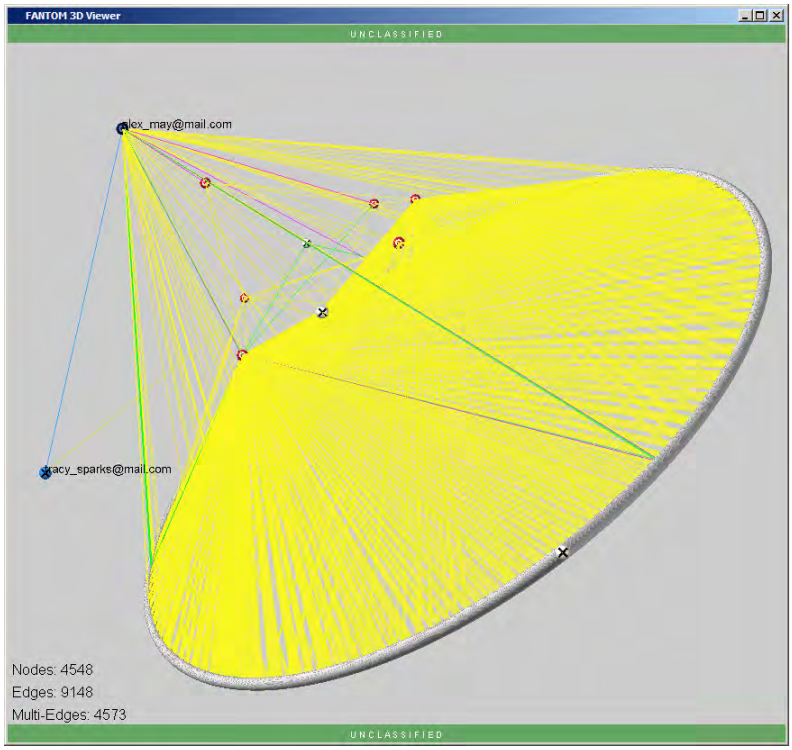
   - (U) **Max Size of Path (# Edges)** – Type or select the number of edges for the maximum size of the path that you want FANTOM to include in the results.
   - (U) **Use Edge Direction** – Select the **Use Edge Direction** check box if you want this analytic to take edge direction into consideration when determining the source to destination path.

- (U) **Apply Colors** – Select this check box to apply the color in the color swatch. To change the color swatch, click the color and then make a selection in the Color Selector dialog box.

(U) After you run this analytic, FANTOM adds a Shortest Path column in the Controller window (Figure 9-41). You can click the column title twice to bring the shortest paths to the top of the list.

Figure 9-41: (U) Example of Source To Destination Path analytic results

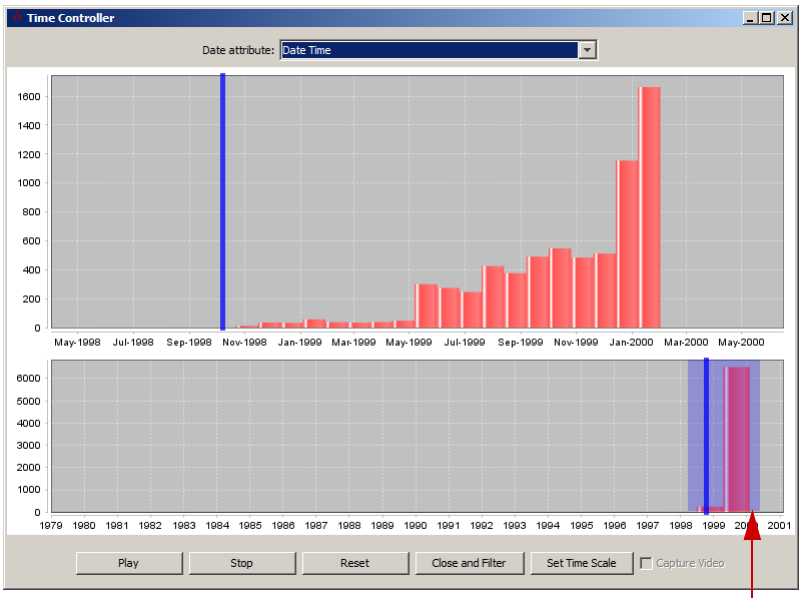




Using the Time Controller

(U) The Time Controller lets you examine the point-to-point connections in your data across time.

Figure 9-42: (U) Time Controller dialog box



The bottom Timeline graph lets you select a smaller time range by dragging the sides of the transparent selection rectangle left or right

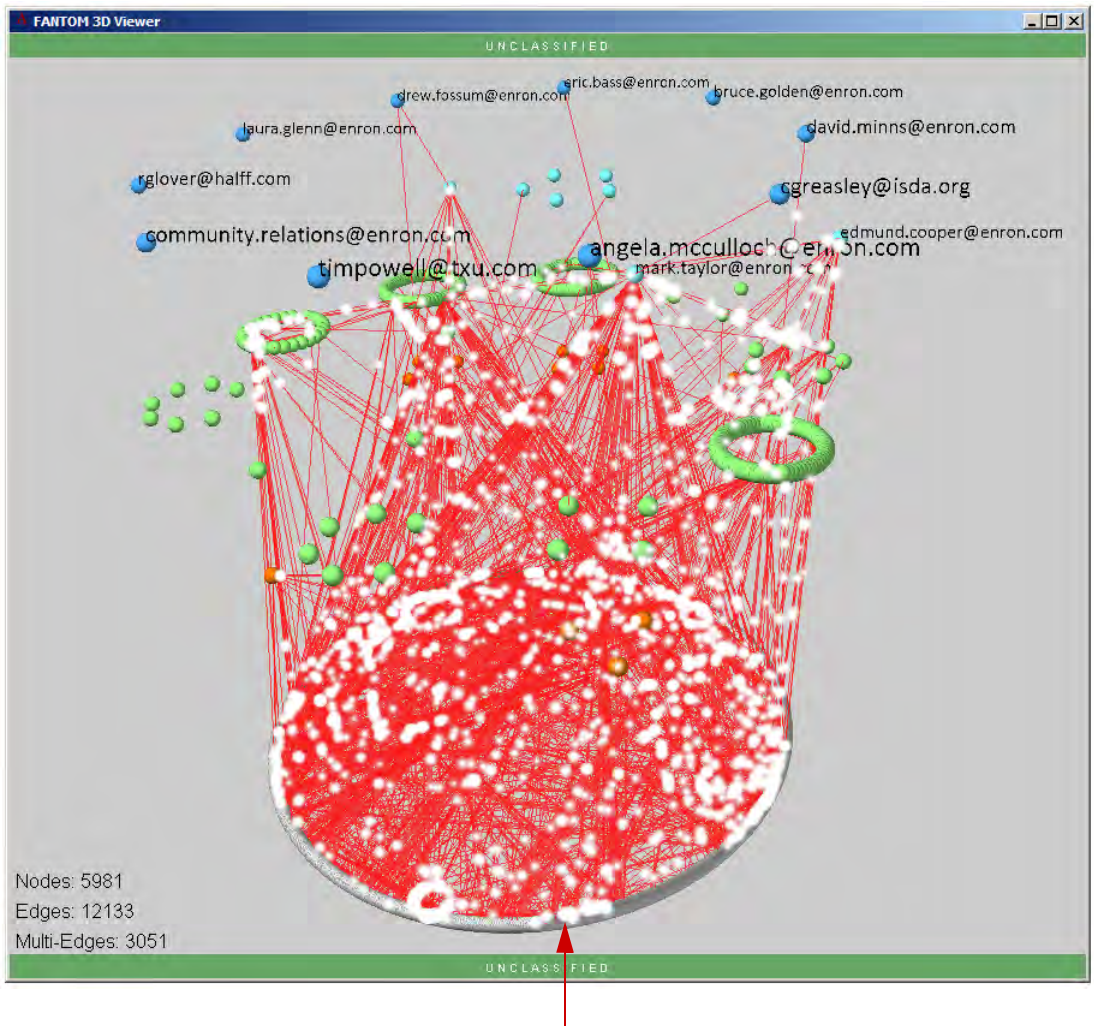
(U) The Time Controller displays connection events that take place after you click the **Play** button. When you click **Play**, the button dims and the **Pause** and **Stop** buttons become active.

(U) You can watch these connections display as "blips" moving from node to node in the 3D Viewer window.

(U) FANTOM lets you drag from left to right in the bottom bar chart to select a smaller time range. As you drag, a selection rectangle displays. It remains visible and you can drag it forward or backward across time to adjust the time range that will display in the top timeline chart.

(U) If your data set has multiple Date/Time columns in the Edge table, you can select the one of interest in the **Date attribute** menu (Figure 9-45).

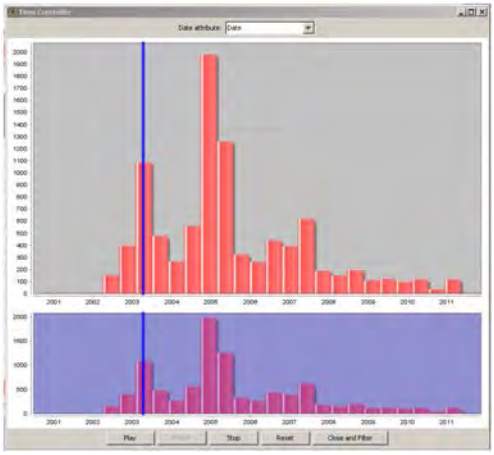
Figure 9-43: (U) Example of Timeline Controller showing communications

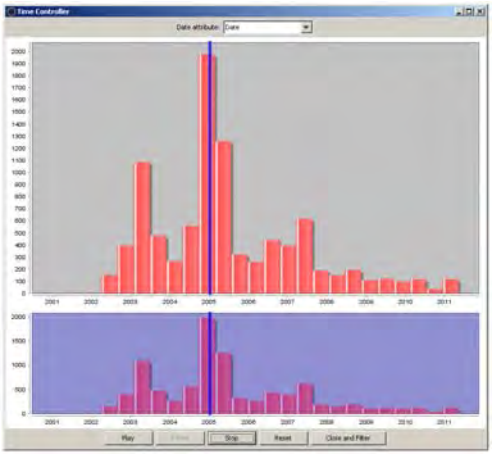


As the Timeline plays, the Current value changes and the Viewer window shows you the sequence and direction of communications with white circular "blips" moving along the edge lines from node to node

(U) You can drag the vertical blue slider in the Time Controller to observe relationships across time in the Graph Viewer window (Figure 9-44).

Figure 9-44: (U) Drag the vertical blue slider in the top chart and relationships change across time in the 3D Graph Viewer window





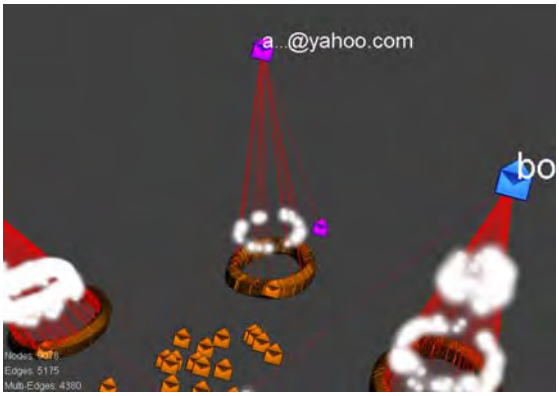
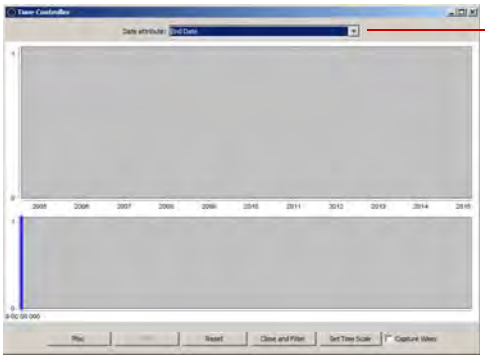


Figure 9-45: (U) Example of changing the selected Date Attribute in the Time Controller



The **Date attribute** menu includes all the Date/Time columns in the Edge table

If a selected **Date attribute** has no values in the corresponding column, the Time Controller has nothing to populate the two timeline charts and they display a gray background; select a different Date attribute to see the activity as vertical red bars

Using Reports

(U) The Advanced Visualization Team designed a collection of customizable and interactive reports in collaboration with FBI Case Agents and Intelligence Analysts. These reports emulate what Intelligence Analysts do in the field and let you share your results as exported Excel tables and saved chart bitmap images (.png), much more quickly.

(U) Most importantly, with FANTOM reports you can explore relationships in your data sets at the macro level. For instance, you can analyze selected entities across critical time ranges or surrounding an event, compare patterns of communication by selected entities across time to see if it is likely that one person is using multiple email addresses or user names, and so on.

Note: (U) FANTOM reports require data sets with a **Date** column defined as a Date during the import process. That is, it cannot be defined as a string.

(U) FANTOM 3.1 and later has moved its reports to a new Reports menu. Earlier FANTOM versions offered reports through Report Service command on the Analytics menu. These FANTOM reports include:

- (U) Around Event Report
- (U) Attribute Lookup Report
- (U) Attribute Tracker Report
- (U) Conversation Report
- (U) Histogram Report
- (U) Pattern of Life Report
- (U) Pie Report
- (U) Scatter Plot Report

- (U) Summation Report
- (U) Timeline Report

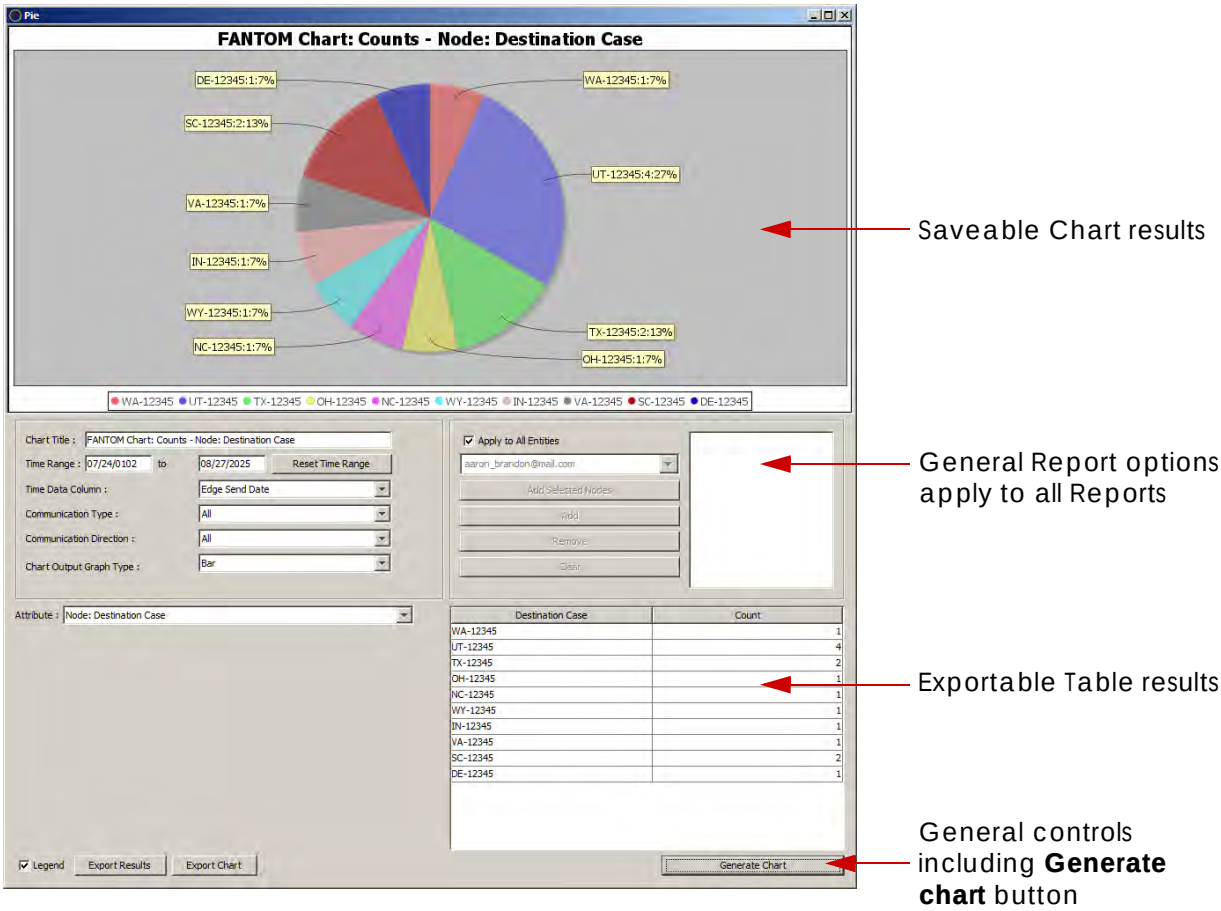
Note: (U) The Tiered Layout Report is discussed in Chapter 7, "Changing the Layout."

(U) If you need additional reporting capabilities after exploring the reports described in this chapter, contact the Advanced Visualization Team.

Standard Parts of Report Windows

(U) The Report windows contains several sections identified below.

Figure 10-1: (U) Report window parts



Saveable Chart results

General Report options apply to all Reports

Exportable Table results

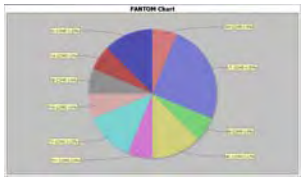
General controls including **Generate chart** button

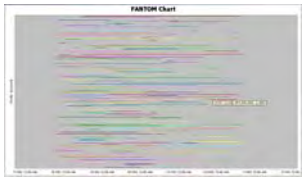
Report Charts

(U) The chart's contents are determined by your data set, the general report options selected, and the active Report tab and its settings.

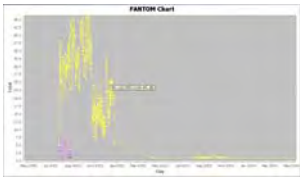
Figure 10-2: (U) Report Charts at a glance

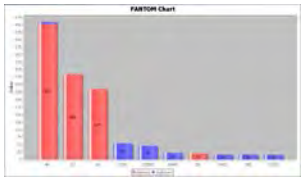

Histogram - Bars

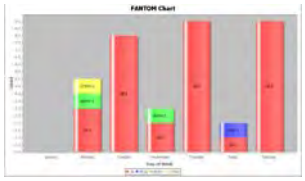

Pie - Pie


Attribute Tracker - Lines


Attribute Tracker - Dots

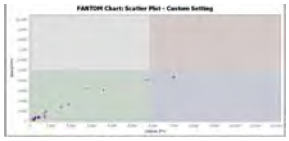

Timeline - Lines

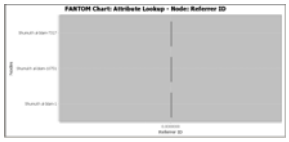

Around Event - Bars

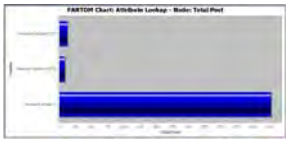

Pattern of Life - Bars


Pattern of Life - Lines


Conversation - Bars


Scatter Plot - Dots


Attribute Lookup - Dots


Attribute Lookup - Histogram

(U) **To create a FANTOM report:**

1. (U) Choose the report of interest from the Reports menu.
2. (U) Select general report options, especially a **Time Range** and the entities of interest: deselect the **Apply to All Entities** check box to activate options to make more focused entity selections.
3. (U) Specify unique options, and then click the **Generate Chart** button.

   (U) FANTOM processes the report and changes the Chart display. After you create a report, you can use the navigation tools to zoom in or out on the chart, resize the Report Service window, export the Excel-like table, save the chart as a .png, or edit general or specific options and click **Generate Chart** to update the chart and table results.

Navigating in a Report Window

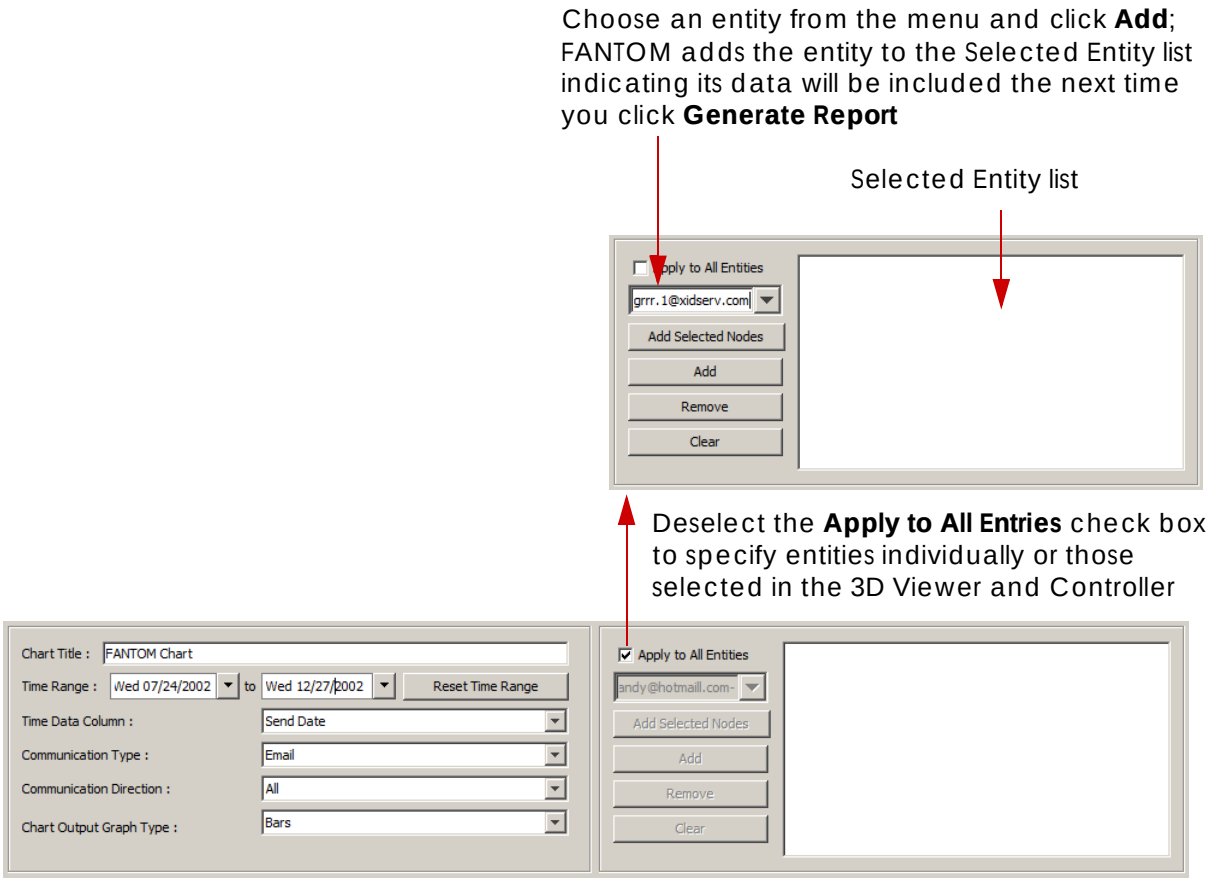
(U) Report windows offer some standard navigation functionality:

- (U) Drag right across the graph to zoom in on the FANTOM Chart
- (U) Drag left across the graph to zoom out on the FANTOM Chart
- (U) Drag the bottom right corner of the Report window to resize it
- (U) Hover the Arrow pointer above bars, slices, and nodes in the charts to view tool tips with more information about each object

General Report Options

(U) The Report windows provide several general options.

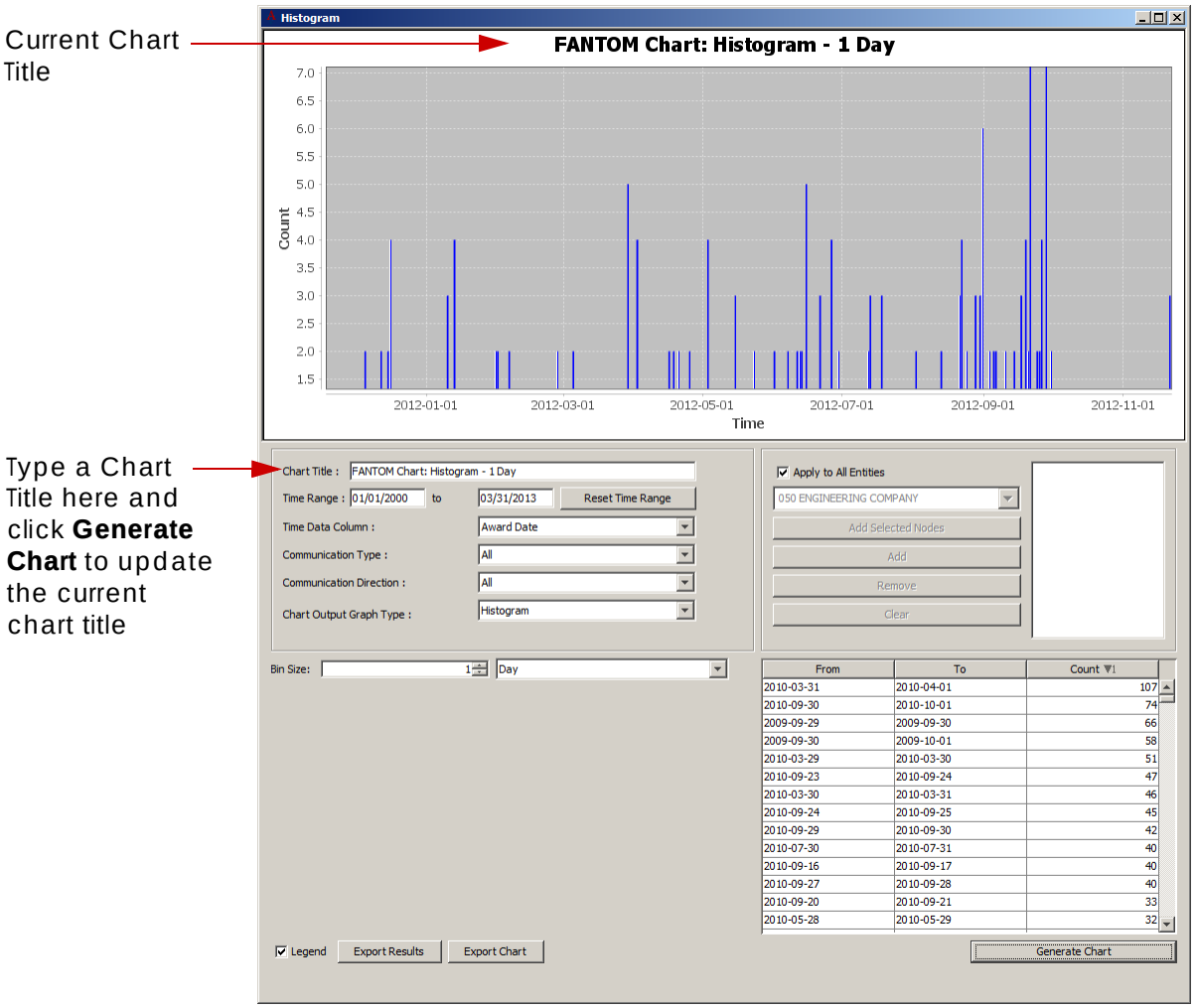
Figure 10-3: (U) *Report window – General Report options*



(U) The general Report options are:

- (U) **Chart Title** – The text you type in the **Chart Title** text box displays at the top of the Report window (Figure 10-4). When you copy or save the chart, the Chart Title is included in the .png image.

Figure 10-4: (U) Chart Title example (sample data: All_ContractsY12Q3+12Q4+13Q1.session)



- (U) **Time Range / to** – Initially, the time range is set to the earliest and latest date in your data set for the selected **Time Data Column**.

  (U) Type a new date in the from or **to** date text boxes in MM/DD/YYYY format, and then press TAB or ENTER to accept the change.

Tip: (U) To specify a 24-hour time range, specify one day as both the from and **to** dates.

Tip: (U) If Wed 12/31/1969 displays in the **Time Range** from text box, it indicates that the field for a row is either empty or invalid.

- (U) **Reset Time Range** – Click the **Reset Time Range** button to change the **Time Range** dates back to the earliest and latest date in the selected **Time Data Column**.
- (U) **Time Data Column** – All date columns available in your data set display in the **Time Data Column** menu so you can choose one of them.
- (U) **Communication Type** – This menu lets you choose Email, Chat, or All.
- (U) **Communication Direction** – The choices on the Communication Direction menu are: **All**, **Inbound**, and **Outbound.**
- (U) **Chart Output Graph Type** – The choices on the **Chart Output Graph Type** menu change to match the current Report:
  - (U) **Around Event** report – **Bar**
  - (U) **Attribute Lookup** report – **Dot** and **Histogram**
  - (U) **Attribute Tracker** report – **Line** and **Dot**
  - (U) **Conversation** report – **Bar**
  - (U) **Histogram** report – **Histogram**
  - (U) **Pattern of Life** report – **Bar** and **Line**
  - (U) **Pie** report – **Pie**
  - (U) **Scatter Plot** report – **Dot**
  - (U) **Timeline** report – **Line**
- (U) **Apply to All Entities** – When selected, FANTOM generates a report based on all records in the data set; when deselected, the following options become available:
  - (U) **Entities** – Choose an entity from the menu and click **Add**.
  - (U) **Add Selected Nodes** – Click the **Add Selected Nodes** button to add all nodes currently selected in the FANTOM Controller/3D Viewer windows.
  - (U) **Add** – Choose an entity from the Entities menu and click **Add**. This adds the entity currently chosen in the Entities menu to the Entities list at the right. The next time you click **Generate Chart** button, the entity will be included in the report.
  - (U) **Remove** – Select an entity in the Entities list at the right and click the **Remove** button to remove it. The next time you click **Generate Chart**, the entity will no longer be included in the report.

- (U) **Clear** – Click the **Clear** button to remove all entities from the Entities list.

Around Event Report

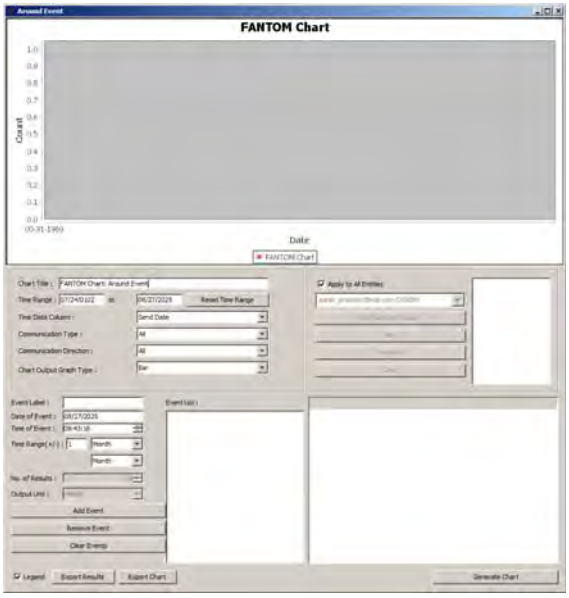
(U) The Around Event report in FANTOM lets you create a report around an event in time. The Date of an event, time of an event and number of results gives you the number most active. The purpose of this report is to help you find who is the most interesting.

To create an Around Event report:

1. (U) Choose **Reports** > **Around Event**.

   (U) The Around Event window displays.

   Figure 10-5: (U) Around Event window



2. (U) Specify the options you prefer:

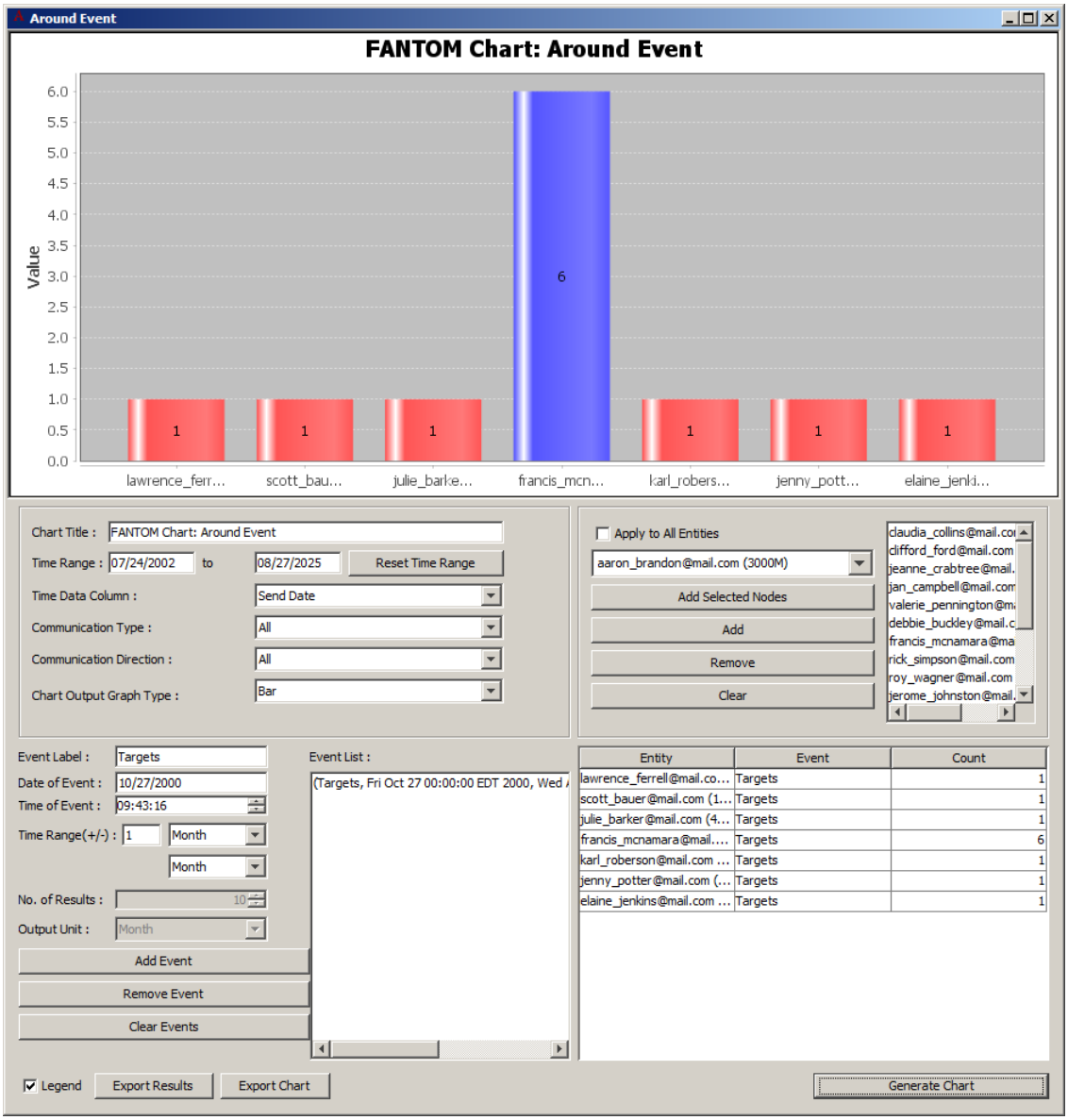
   - (U) **Date of Event** – Click the Arrow button ( ) beside the **Date of Event** text box to display the selection Calendar, or type a date in MM/DD/YYYY format, and then press ENTER to accept the entry.
   - (U) **Time of Event** – Click the hour, minutes, or seconds to highlight it and either type a new value or use the Up or Down Arrow buttons ( ) to scroll through the numbers.
   - (U) **Time Range** – Type a number, if needed, and select **Second**, **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

- (U) **Number of Results** – Type a new number of results or use the Up or Down Arrow buttons ( ) to scroll through the numbers.
- (U) **Output Unit** – Select **Second**, **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year** for the time unit displayed in the chart's horizontal axis.

3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your selections (Figure 10-6).

Figure 10-6: (U) Example of Around Event report for email of selected entities across a one month time period surrounding the day of 10/27/2000 (sample data: two-hops.session)



Attribute Lookup Report

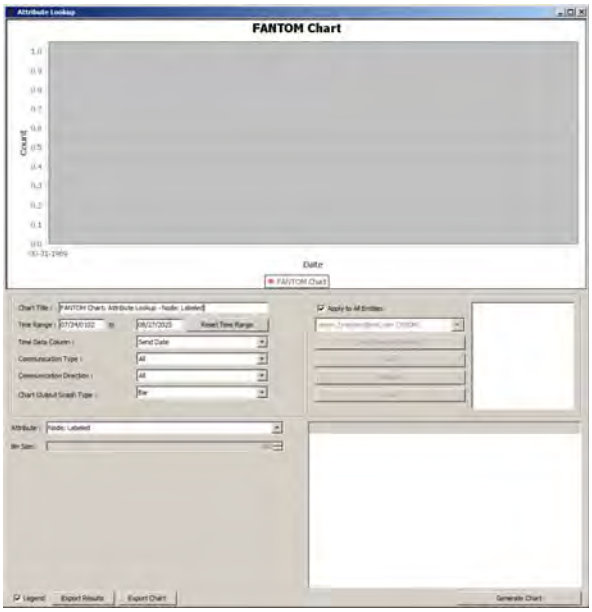
(U) The Attribute Lookup report looks up attribute values and then plots them into a chart. It only works with number values and dates and plots them into a visual chart.

(U) To create an Attribute Lookup report:

1. (U) Choose **Reports** > **Attribute Lookup**.

   (U) The Attribute Lookup report window displays.

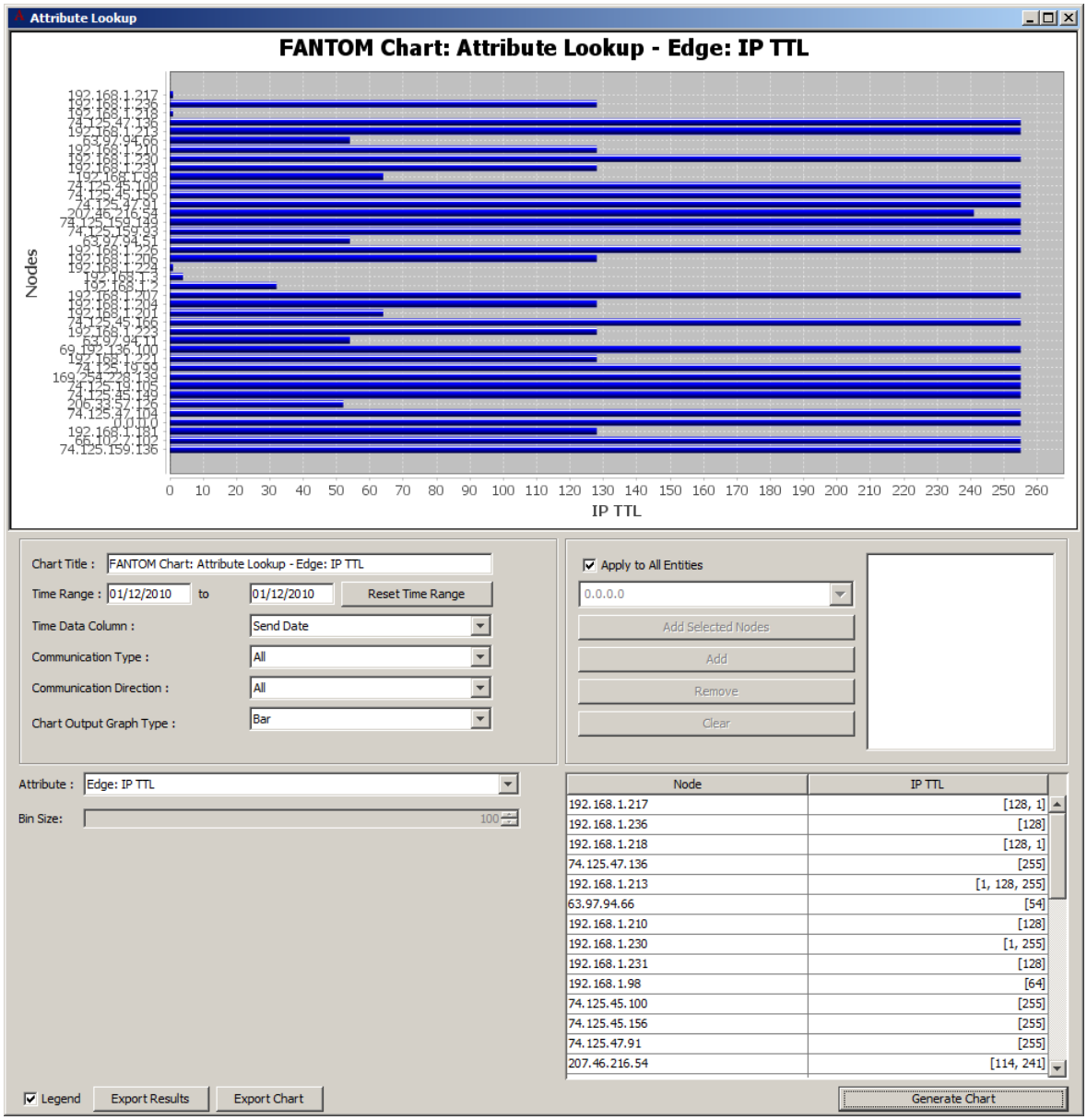
Figure 10-7: (U) Attribute Lookup report window



2. (U) Select an **Attribute** and a **Bin Size**.
3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your general selections (Figure 10-12). The color bars identify recipients.

Figure 10-8: (U) Example of Attribute Lookup report (sample data: http-snifer-test.session)



Attribute Tracker Report

(U) The Attribute Tracker report lets you look deeper into node relationships. In the Attribute Tracker report, you select options that display in the graph as follows:

- (U) **Horizontal X-axis** – Displays the node or edge attribute you select in the Attribute Tracker tab. Email addresses, IP addresses, locations like City or Country, and Targets are examples of good attribute choices for this report. Edge attributes work better than node attributes.
- (U) **Vertical Y-axis** – Displays the number of entities you select: one, multiple, or all Entities (the Node ID) across the specified Time Range. Selecting fewer entities to examine will make it easier to gain insight. If you discover email addresses with identical geo-locations and send dates, you may want to merge those nodes.

Tip: (U) When choosing a **Chart Output Graph Type**, use **Lines** for physical locations and **Dots** for everything else.

(U) **To create an Attribute Tracker report:**

1. (U) Choose **Reports** > **Attribute Tracker**.

   (U) The Attribute Tracker report window displays.

Figure 10-9: (U) Attribute Tracker report window

2. (U) Select a Node or Edge attribute from the **Attribute** menu.

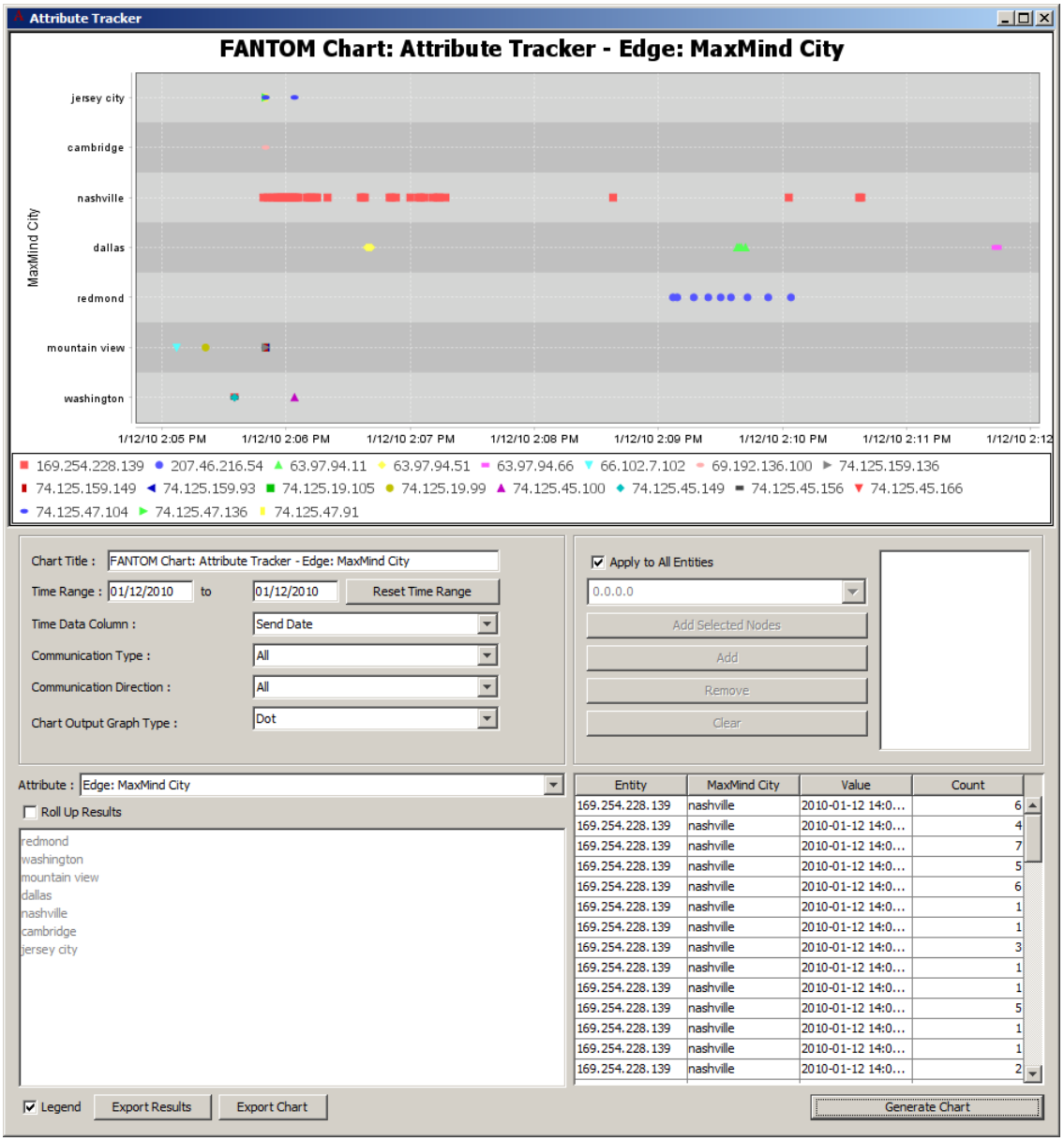
   (U) Node and Edge Table column titles are the available attributes.

3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your selections (Figure 10-10). In the following figure, you can determine the likelihood of the same person using an email address located in Buffalo NY within hours of someone using it in Dubai or Riyadh. You might use these small facts to help you decide whether multiple people are sharing one email address or if one person is using several email addresses.

Note: (U) The **Databases** > **GeoIP Server** or **GeoIP Local** commands let you identify locations like City and Country based on IP addresses. You can recognize columns generated by this analytic because they start with "LMM-" as is used in the following example.

Figure 10-10: (U) Example of Attribute Tracker Report (Edge: MaxMind City) (sample data: http-snifer-pcap-lat-long-geoip-server.session)



Conversation Report

(U) The Conversation report lets you track a subset of a clique or group. You can zoom in to see the count for each entity in the bars. This report may help you narrow your search down or find someone you didn't know about before.

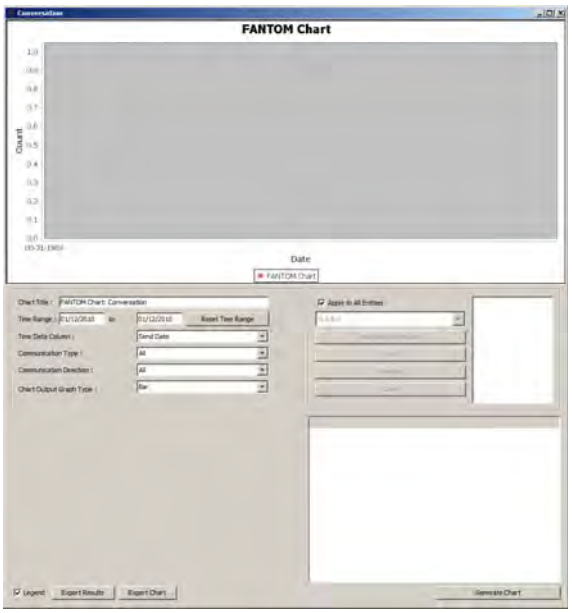
Note: (U) You can get the same benefits using Filters in FANTOM; however, the Conversation report is easier to use than the Edge table.

(U) To create a Conversation report:

1. (U) Choose **Reports** > **Conversation**.

   (U) The Report Service dialog box displays.

   Figure 10-11: (U) Conversation report window

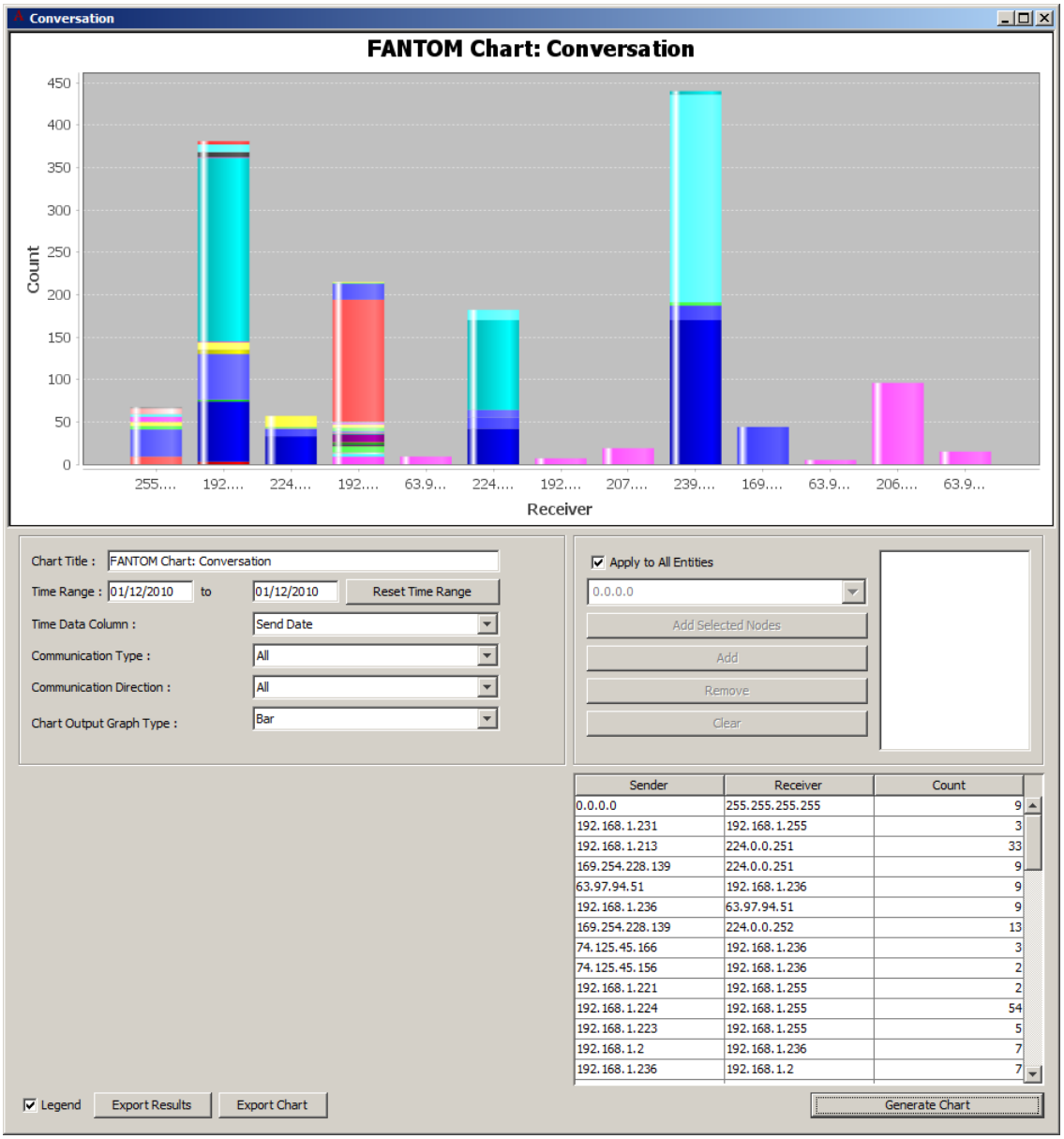


   (U) The Conversation report relies entirely on general options and has no specific ones at this time.

2. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your general selections (Figure 10-12). The color bars identify recipients.

Figure 10-12: (U) Example of Conversation report for All Entities using Bar graph type (sample data: http-snifer-pcap-lat-long-geoip-server.session)



Histogram Report

(U) In FANTOM, the Histogram report produces a bar graph where the bar widths are proportional to the duration of date data in the selected date range.

(U) To create a Histogram report:

1. (U) Choose **Reports** > **Histogram**.

   (U) The Histogram report window displays.

Figure 10-13: (UHistogram report window

2. (U) Specify the options you prefer:

   - (U) **Bin Size** – Type a number of bins (or classes) to divide the selected unit of time into. For example, the Bin and unit of time values could specify time periods like 2 weeks, 3 days, 8 hours, and so on. The Bin Size determines the width of bars in the histogram. The bar height indicates the total number of edges inside one bin in the histogram.

   - (U) **Unit of Time** – Select from the following options: **Second**, **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

3. (U) Click the **Generate Chart** button.

Note: (U) FANTOM only displays column titles for dates in the **Time Data Column** menu.

(U) FANTOM calculates and displays the Histogram report based on your selections (Figure 10-14).

Figure 10-14: (U) Example of Histogram report (sample data: two-hops.session)

Count is the number of edges; the bar height indicates the total number of edges inside one bin

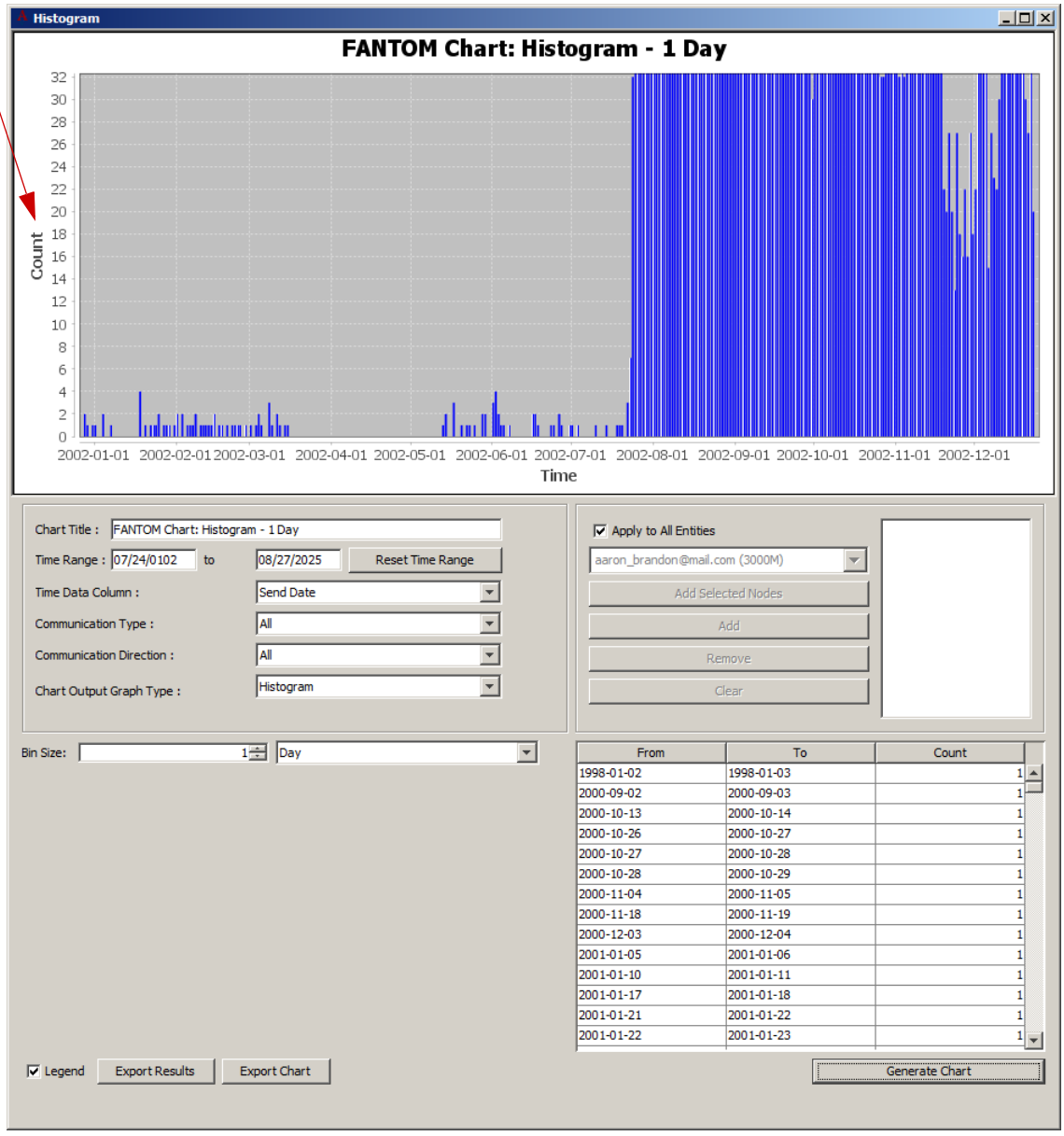
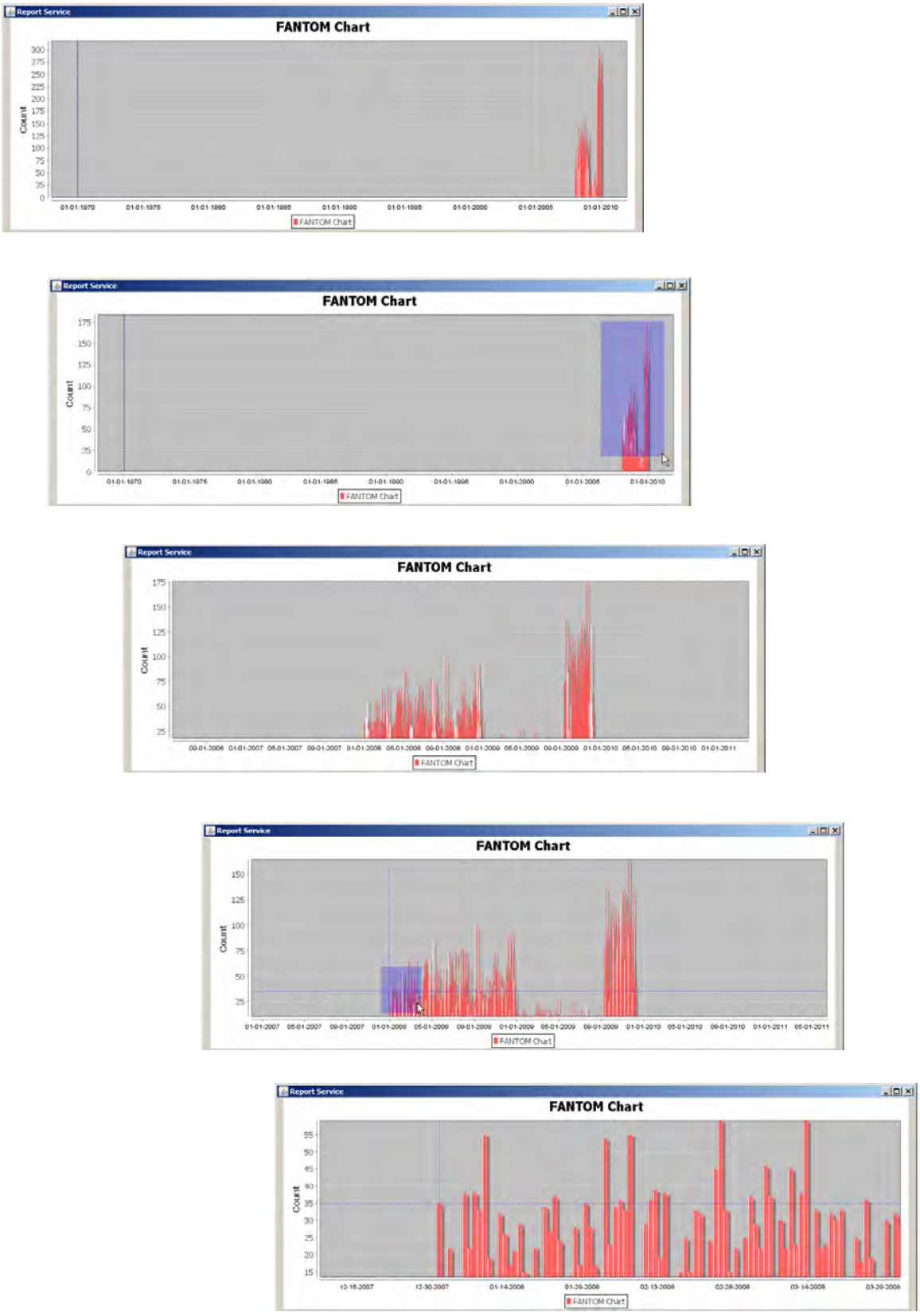


Figure 10-15: (U) Zoom in by dragging left to right to surround a smaller area



Pattern of Life Report

(U) The Pattern of Life report lets you examine weekly patterns of communication behavior for the selected *entity* (or ID column of the Node Table). A good way to use this report is with data sets that have email addresses as node IDs.

(U) Select three or four email addresses and if the resulting generated report shows the same pattern for multiple email addresses, then it may suggest that the same person is using all these email addresses.

(U) To create a Pattern of Life report:

1. (U) Choose **Reports** > **Pattern of Life**.

   (U) The Pattern of Life report window displays.

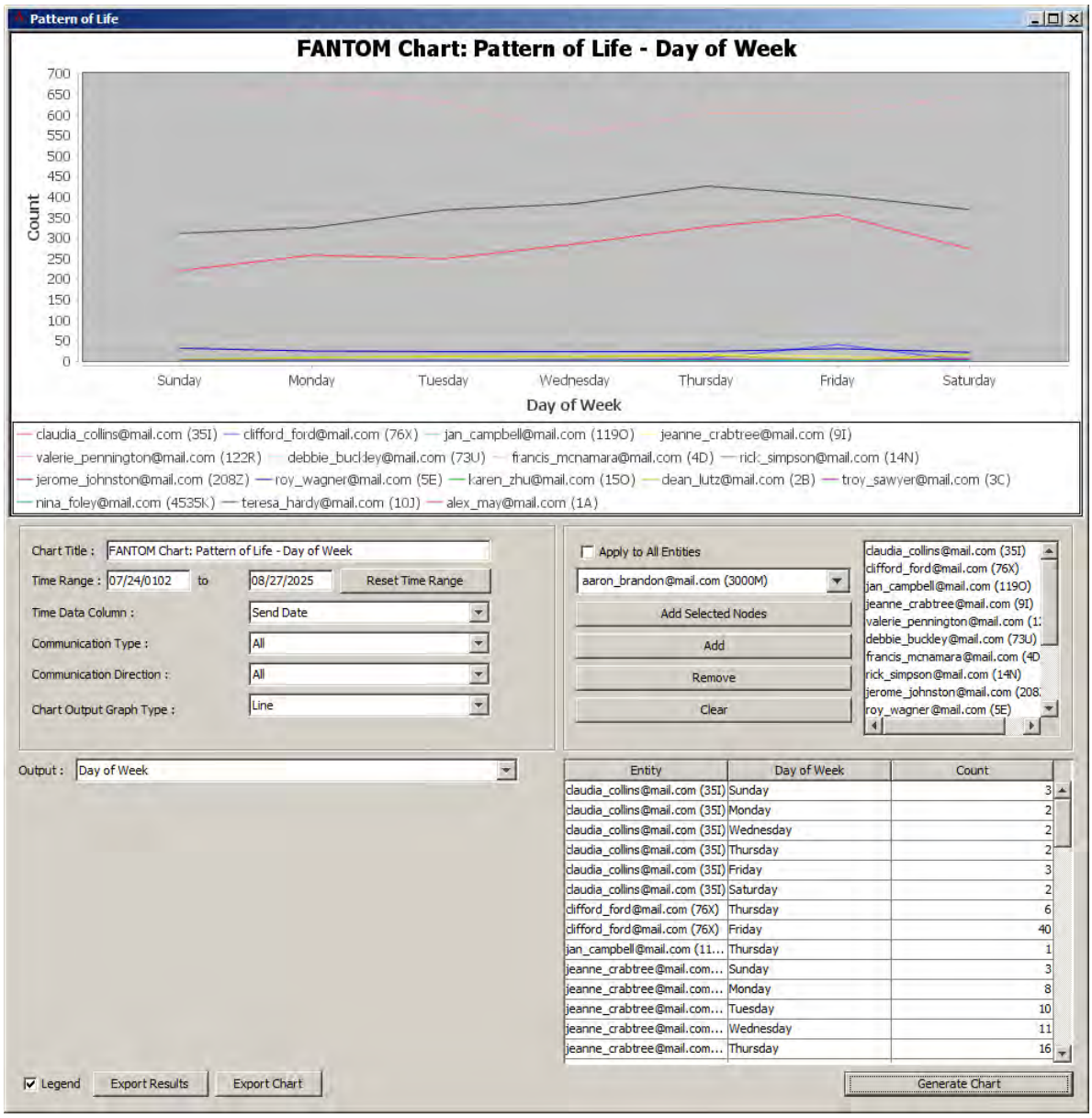
   Figure 10-16: (U) Pattern of Life report window

2. (U) Select the **Output**: **Hour of Day**, **Day of Week**, **Day of Month**. or **Month of Year**.

3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the Pattern of Life report based on your selections (Figure 10-17).

Figure 10-17: (U) Pattern of Life report for selected nodes by Day of Week using the Line graph type (sample data: two-hops.session)



Pie Report

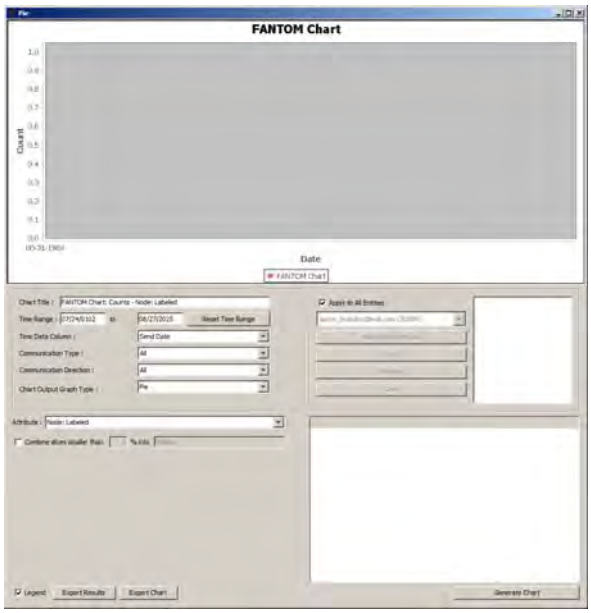
(U) The Pie report in FANTOM is a basic proportional chart that shows the relative sizes of values in the selected attribute of the data set in comparison to one another and to the whole set.

(U) To create a Pie report:

1. (U) Choose **Reports** > **Pie**.

   (U) The Pie report window displays.

   Figure 10-18: (U) Pie Report window



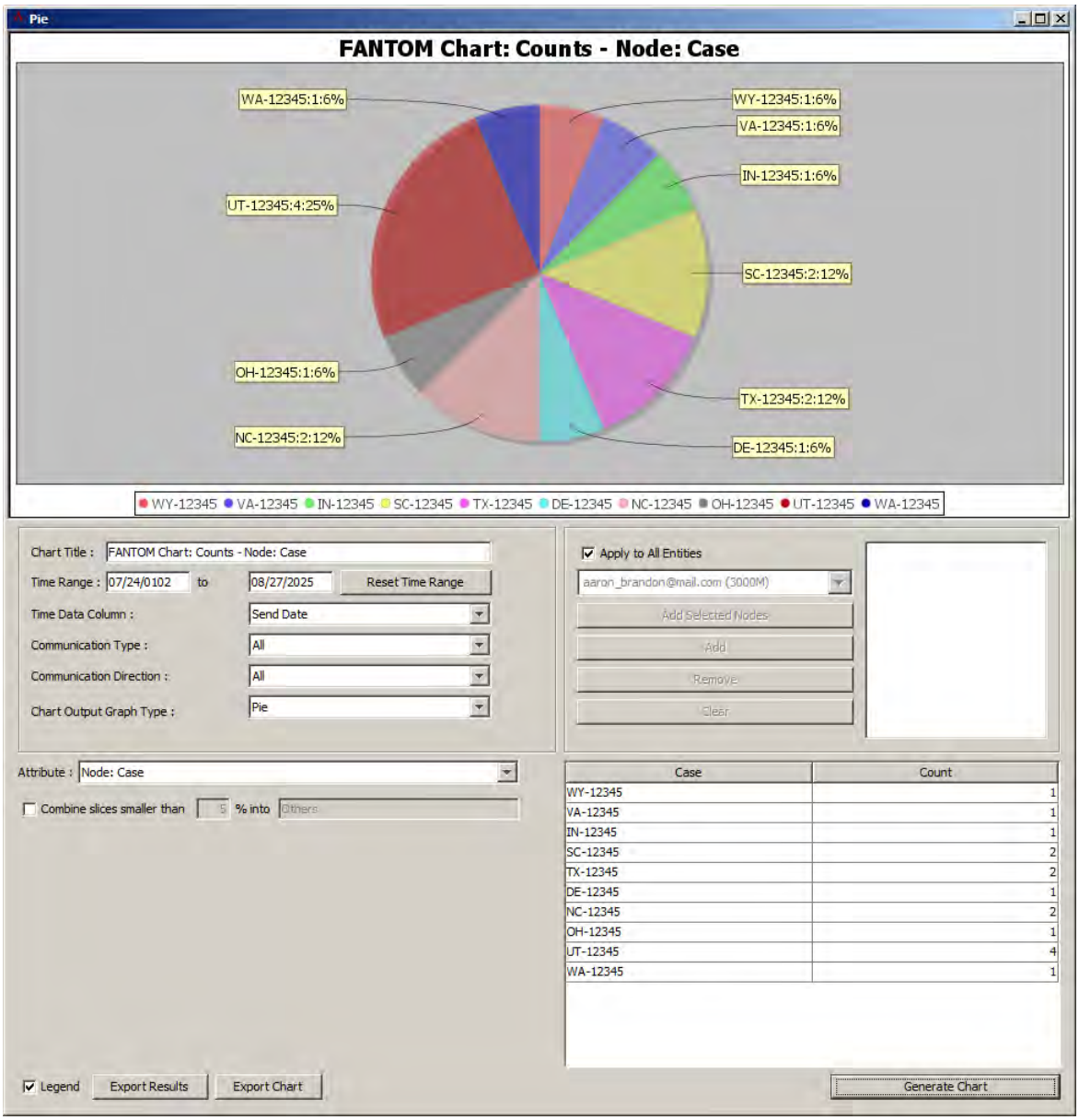
2. (U) Select a Node or Edge attribute from the **Attribute** menu.

   (U) Node Table and Edge Table column titles are the available attributes.

3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your selections (Figure 10-19).

Figure 10-19: (U) Pie report for the Node: Case attribute (sample data: two-hops.session)



Scatter Plot Report

(U) The Scatter Plot report is a graph that plots two along two axes to show the relationship between the two. Scatter plots are useful for illustrating a trend.

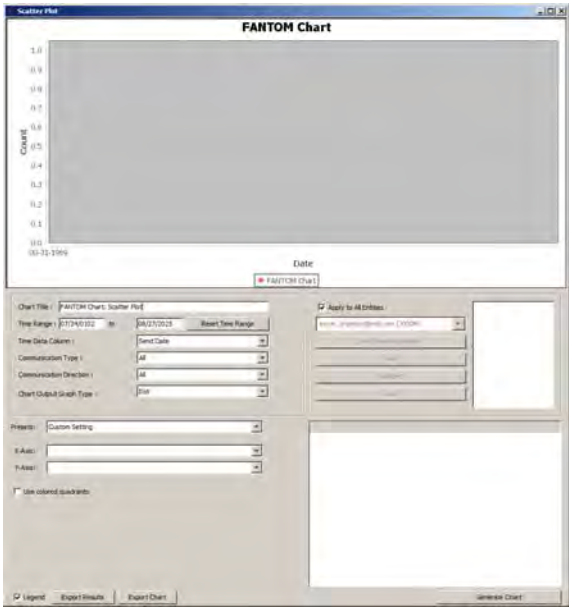
(U) To create a Scatter Plot report:

1. (U) Run any combination of analytics that add numeric columns, such as Betweenness, Degree, Eigenvector Centrality, Neighborhood Index, and so on.

2. (U) Choose **Reports** > **Scatter Plot**.

   (U) The Scatter Plots report window displays.

   Figure 10-20: (U) Scatter Plot report window

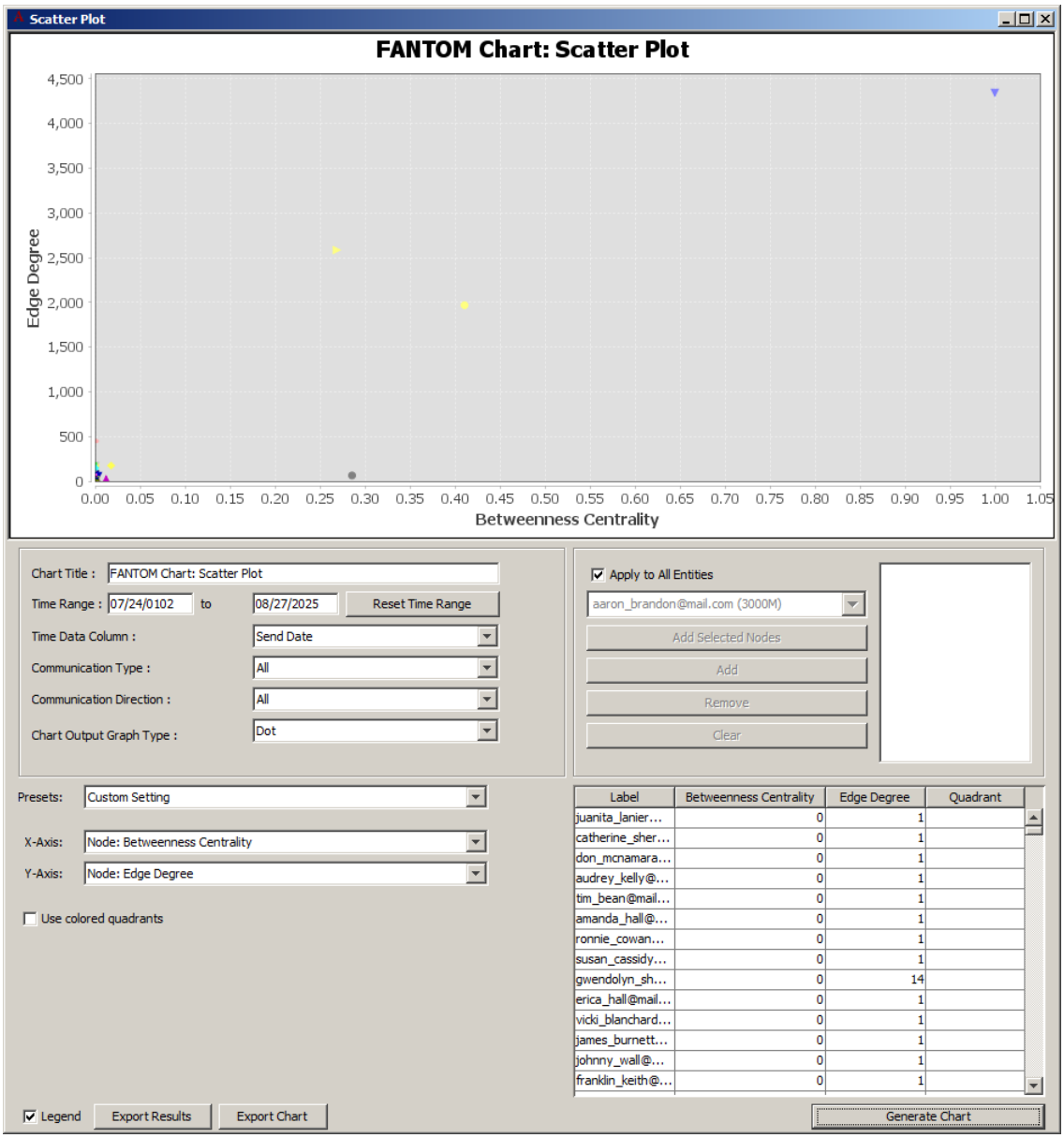


   (U) The report allows you to select the numeric values for the X-Axis and Y-Axis.

3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your general selections (Figure 10-21). The color dots identify recipients.

Figure 10-21: (U) Scatter Plot report run after running the Betweenness Centrality and Degree analytics (sample data: two-hops.session)



Summation Report

(U) The Summation report sums the total currency amounts in a data set that move from source to destination and from destination to source. It then subtracts one total from the other to determine a positive or negative currency amount.

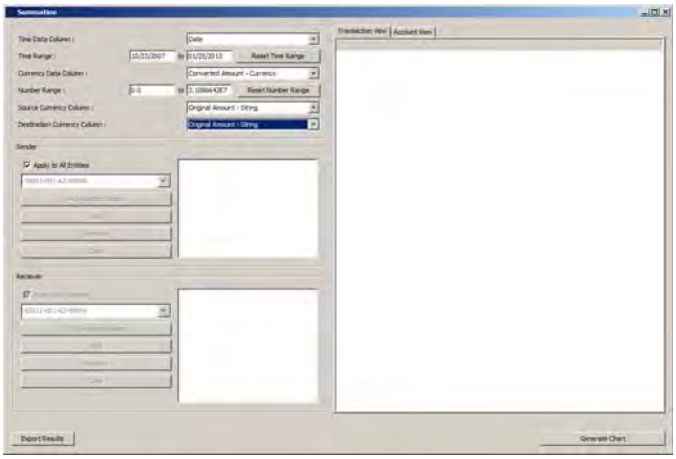
Note: (U) If you import a data set with currency columns, be sure to add the columns by clicking the **Add** button and selecting the **Currency** data type. Click the **$** button to define the currency country either manually or by selecting a column. You may need to use the **Manual** option.

To create a Summation report:

1. (U) Choose **Reports** > **Summation**.

   (U) The Summation report window displays.

   Figure 10-22: (U) Summation report window



2. (U) Select a column name for at least the **Currency Data Column**, the **Source Currency Column**, and the **Destination Currency Column**.

3. (U) Click the **Generate Chart** button.

   (U) FANTOM displays the Summation report in the Transaction View and Account View tabs at the right (Figure 10-23 and Figure 10-24).

   (U) You can click the **Export Results** button to save the Summation report as an Excel file (.xlsx or .xls) or delimited file (.csv or .txt).

Figure 10-23: (U) Example Summation report - Transaction View (bank-example.session)

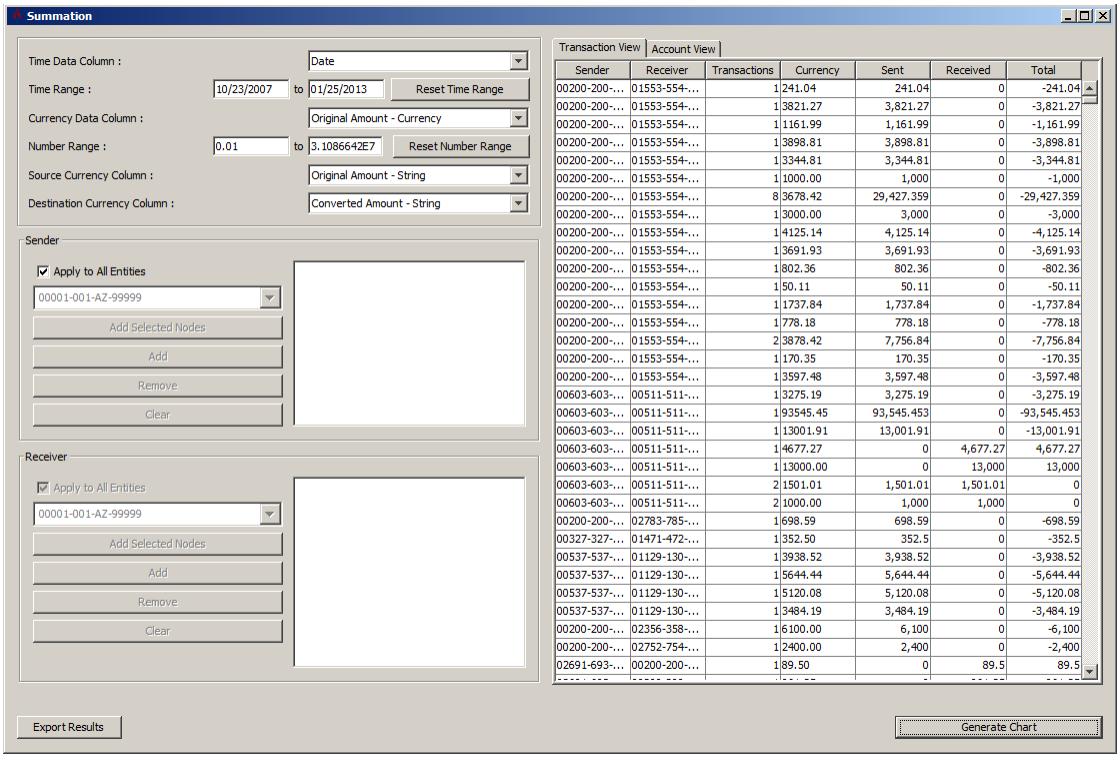
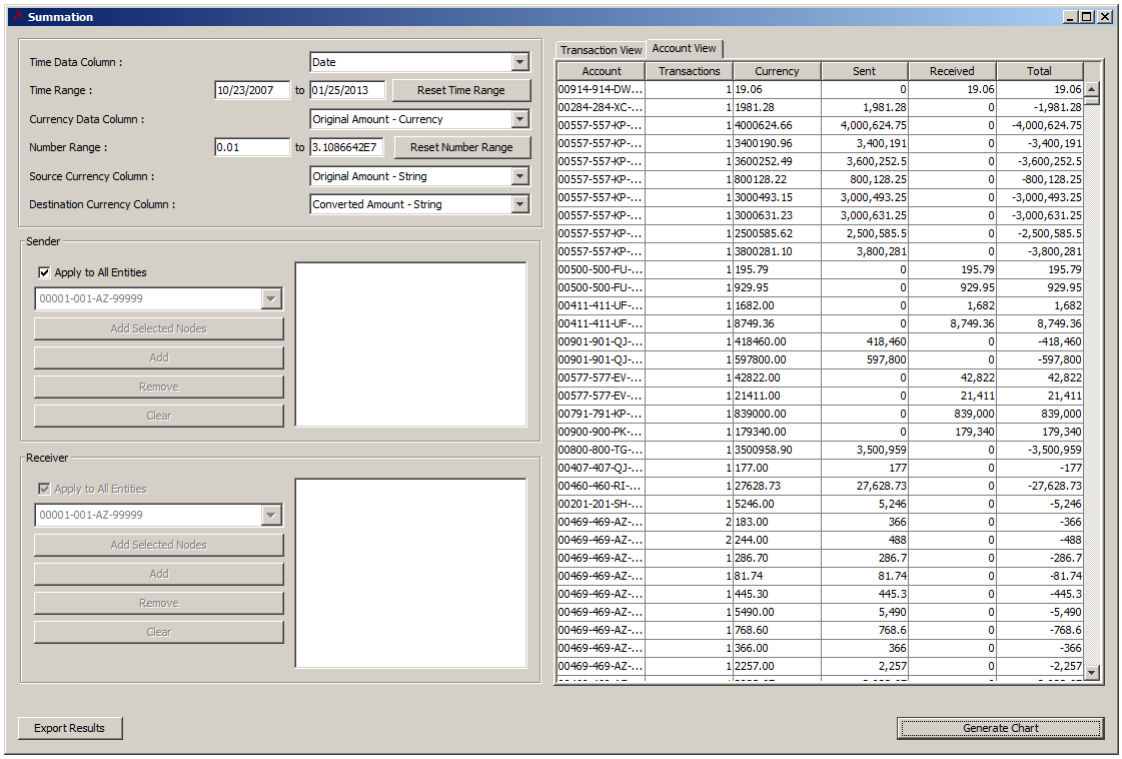


Figure 10-24: (U) Example Summation report - Account View (bank-example.session)



Timeline Report

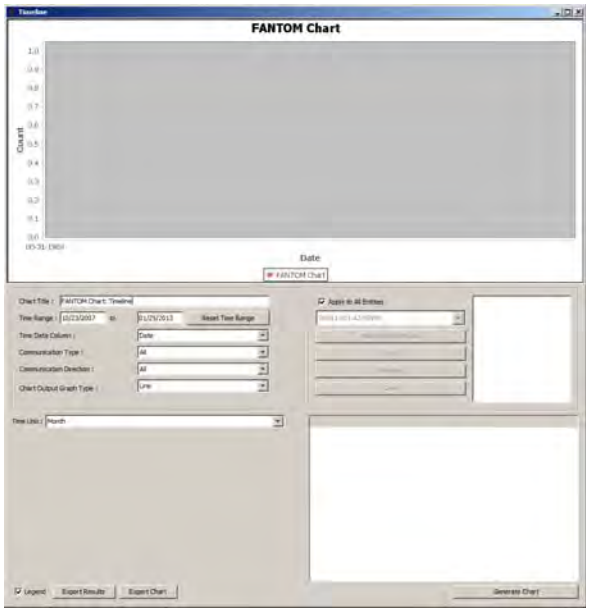
(U) You can customize the Timeline report by adding one or more sets of node criteria to show along the timeline. You can also remove individual sets of node criteria.

To create a Timeline report:

1. (U) Choose **Reports** > **Timeline**.

   (U) The Timeline window displays.

   Figure 10-25: (U) Timeline window



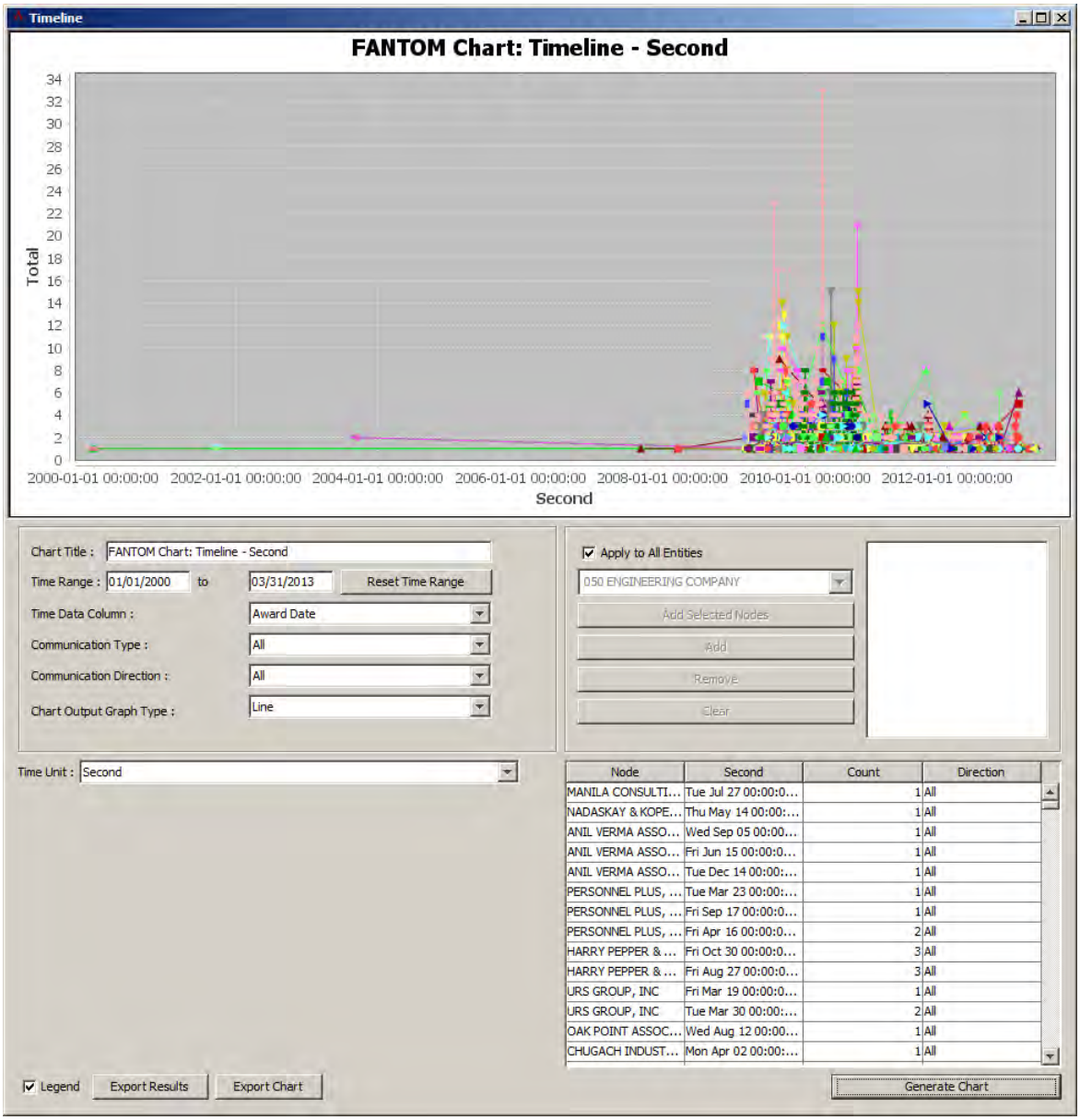
2. (U) **Time Unit** – Select **Second**, **Minute**, **Hour**, **Day**, **Month**, or **Year**.
3. (U) Click the **Generate Chart** button.

   (U) FANTOM calculates the report based on your selections (Figure 10-26).

Tip: (U) Hover the mouse pointer above the lines to see more information about activity across time.

Note: (U) Zero values don't get recorded.

Figure 10-26: (U) Timeline report for all entities with Dot graph type and Second time unit (sample data: All_ContractsY12Q3+12Q4+13Q1.session from Recovery.gov)



Setting Your Preferences

(U) FANTOM lets you set the following preferences:

- (U) 3D Viewer Preferences
- (U) Articulation Point Preferences
- (U) BIDMAS Importer Preferences
- (U) Betweenness Preferences
- (U) CSV Exporter
- (U) Call Chaining Preferences
- (U) Circle Layout Preferences
- (U) Closeness Centrality Preferences
- (U) Degree Analytic Preferences
- (U) Disperser Layout Preferences
- (U) Edge Display Preferences
- (U) Eigenvector Centrality Preferences
- (U) Force Directed Preferences
- (U) General Preferences
- (U) General Importer Preferences
- (U) GeoIP Local Preferences
- (U) Icon Palettes Preferences
- (U) Link Cluster Layout Preferences
- (U) PCAP Importer Preferences

- (U) Prestige Centrality Preferences
- (U) Random Layout Preferences
- (U) Reciprocated Analytic Preferences
- (U) Related Nodes Preferences
- (U) Research Conduit Preferences
- (U) Research Importer Preferences
- (U) Source to Destination Path Preferences
- (U) Tiered Layout Preferences
- (U) Time Controller Preferences

3D Viewer Preferences

(U) The 3D Viewer Preference Manager let you select values determining appearance of objects in the 3D Viewer window.

(U) To set 3D Viewer preferences:

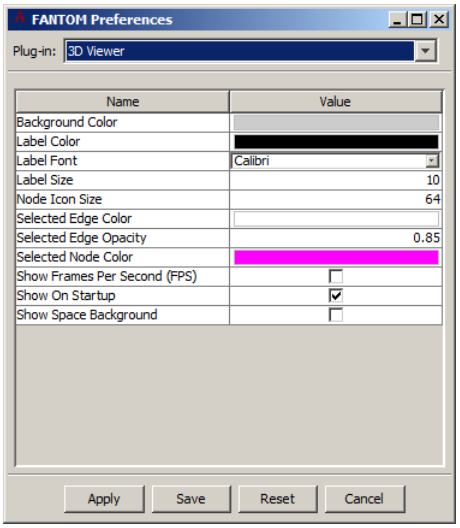
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **3D Viewer** from the **Plug-in** menu.

   (U) The 3D Viewer preferences display (Figure 11-1).

Figure 11-1: (U) 3D Viewer preferences

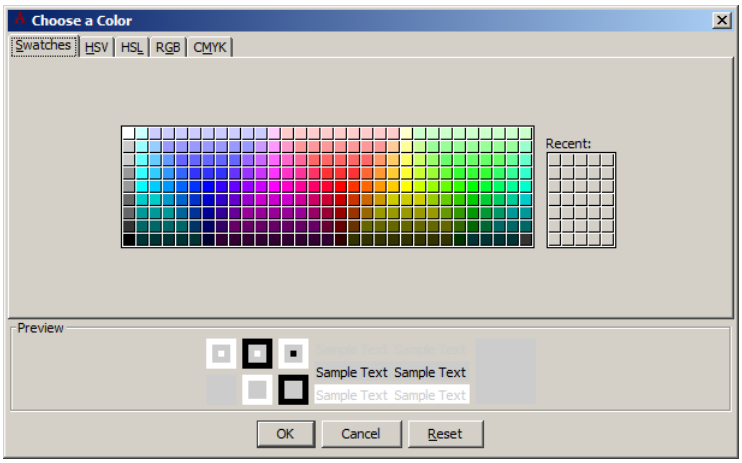


3. (U) Select the options you prefer and then click **Save**:

   - (U) **Background Color** – Double-click the color swatch.

(U) The Choose a Color dialog box displays (Figure 11-2).

Figure 11-2: (U) Choose a Color dialog box

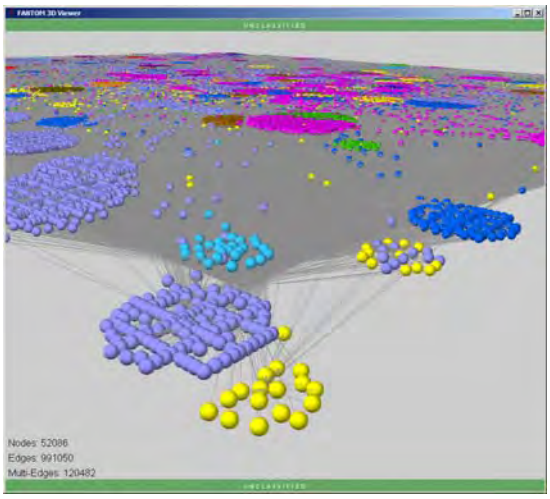


(U) Select a color and click **OK**.

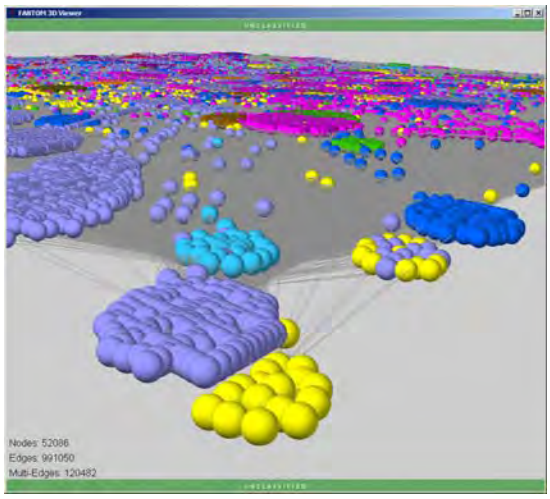
- (U) **Label Color** – Double-click the color swatch, select a color that you can see on the currently selected background color, and then click OK.
- (U) **Label Font** – Select a font to use for labels in the 3D Graph Viewer window.
- (U) **Label Size** – Type a font size (in points) for the labels. If the label size does not look like you expect, choose the **Graph** > **Reset Graph View** command in the Controller window to move the graph to the origin in 3D space.
- (U) **Node Icon Size** – Specify a node icon size. The default is 64, so to double the icon size, increase the value to `128` or to reduce the node icon size by half, enter `32`.

  (U) The size of node icons is relative to the distance away from you in 3D space, which is easy to observe by holding down the scroll wheel while dragging the mouse in different directions to rotate a graph. As nodes move farther away, they get smaller just like objects do in the physical world.

Figure 11-3: (U) Node size examples



Default Node Size of 64

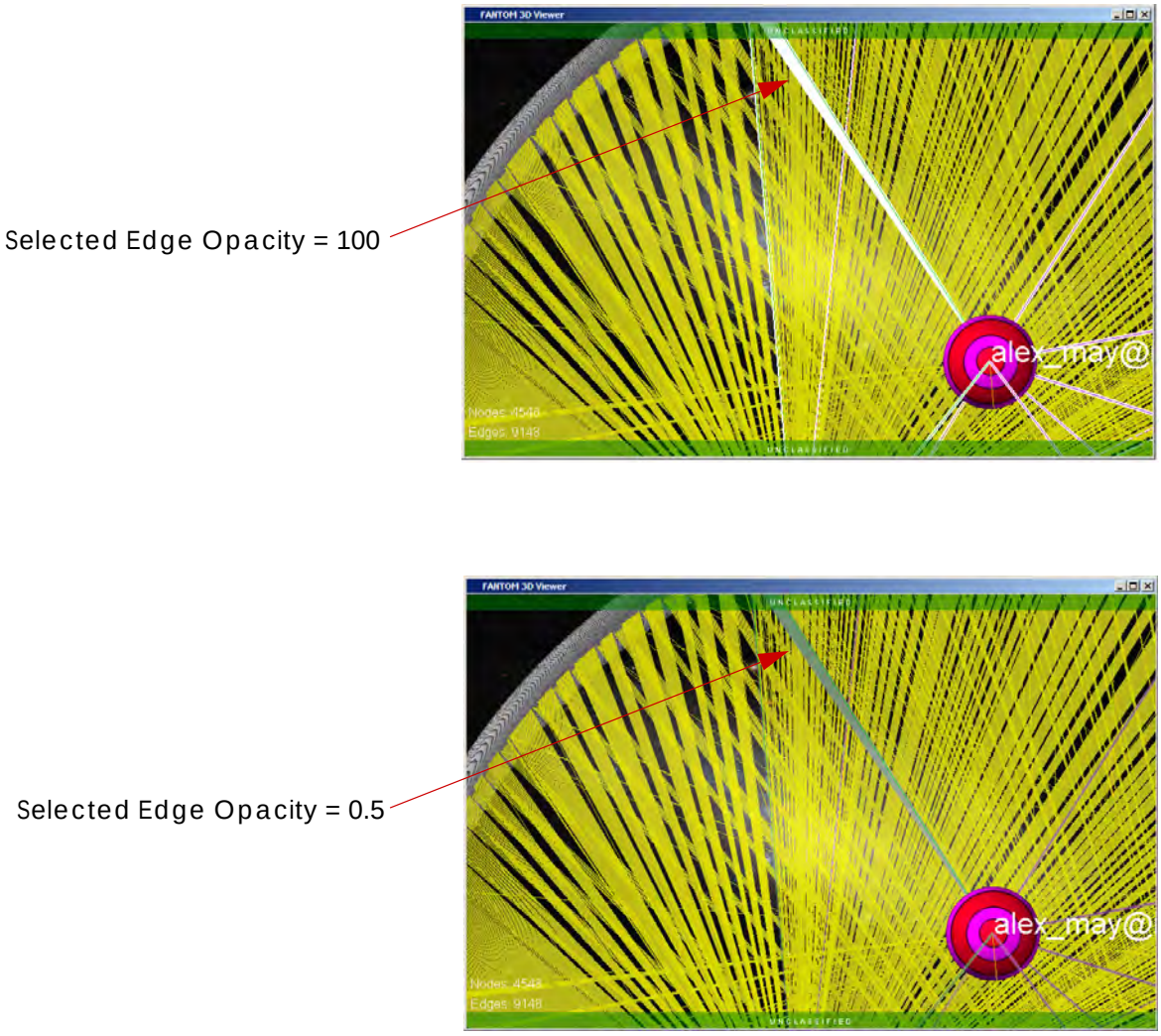


Node Size of 128

- (U) **Selected Edge Color** – Double-click the color swatch, select a new color, and click **OK**.
- (U) **Selected Edge Opacity** – Enter a smaller number to reduce the opacity of selected edges making them more transparent; enter a larger number to increase the opacity of these edges making them less transparent.

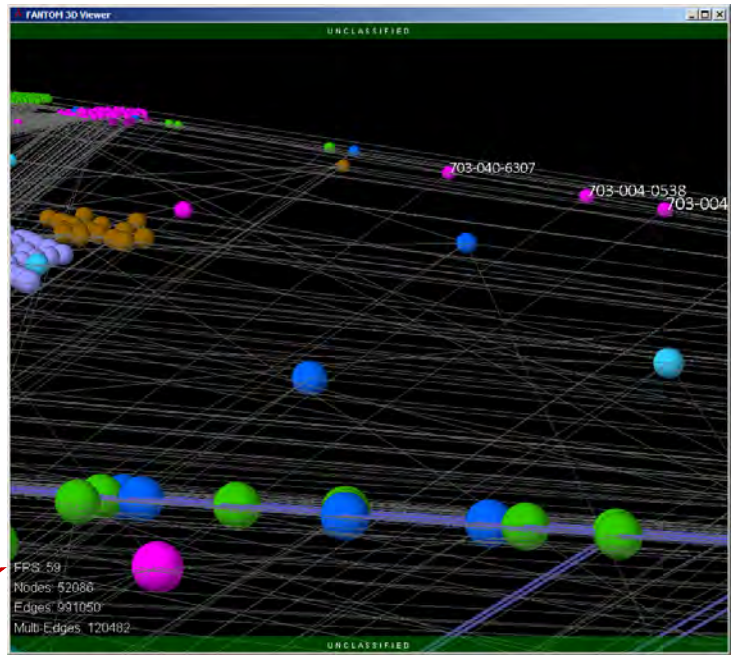
Tip: (U) It is easiest to observe the current level of opacity in the 3D Viewer by rotating the graph so that selected edges overlap unselected edges.

Figure 11-4: (U) Selected Edge Opacity example



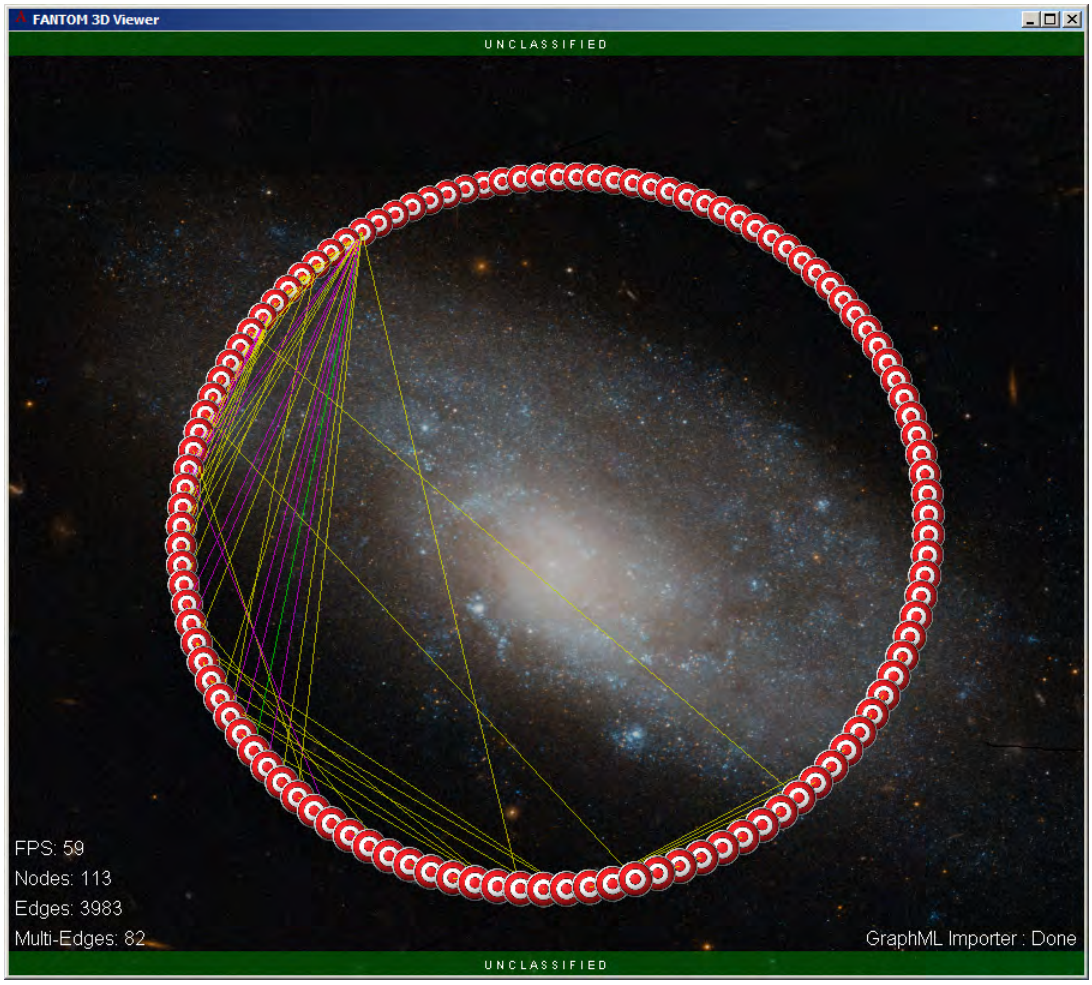
- (U) **Selected Node Color** – Double-click the color swatch, select a new color, and click **OK**.
- (U) **Show Frames Per Second (FPS)** – Select this check box if you want to see the current FPS above the Nodes and Edges values at the bottom left of the 3D Viewer window.

Figure 11-5: (U) FPS display in 3D Viewer window



- (U) **Show on Startup** – Select this check box if you want FANTOM to automatically display the Graph Viewer window when you start the application.
- (U) **Show Space Background** – Select this check box if you want to display a NASA/ESA Hubble Space Telescope photograph of the NGC 5253 blue compact dwarf galaxy as a background image behind your graph.

Figure 11-6: (U) NASA/ESA Hubble NGC 5253 Space Background (airplane.graphml)



Articulation Point Preferences

(U) The Articulation Point preferences let you select default options for the Articulation Point analytic (see "Articulation Points Analytic" on page 9-3).

(U) To set Articulation Point Analytic preferences:

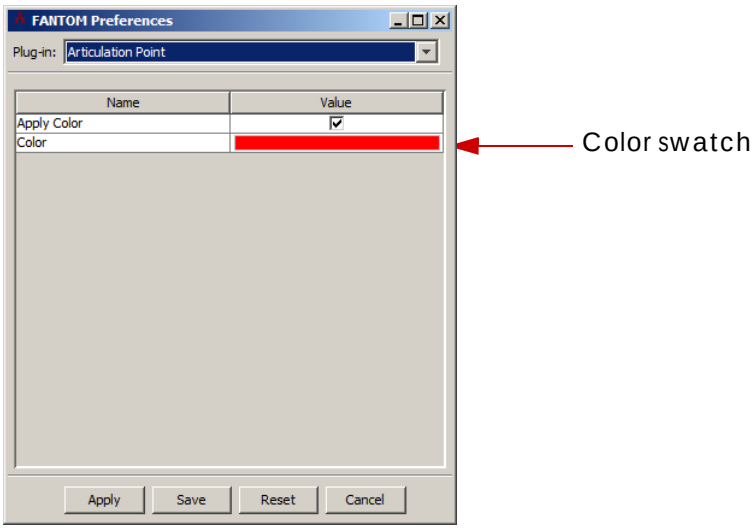
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Articulation Point** from the **Plug-in** menu.

   (U) This plug-in's options display.

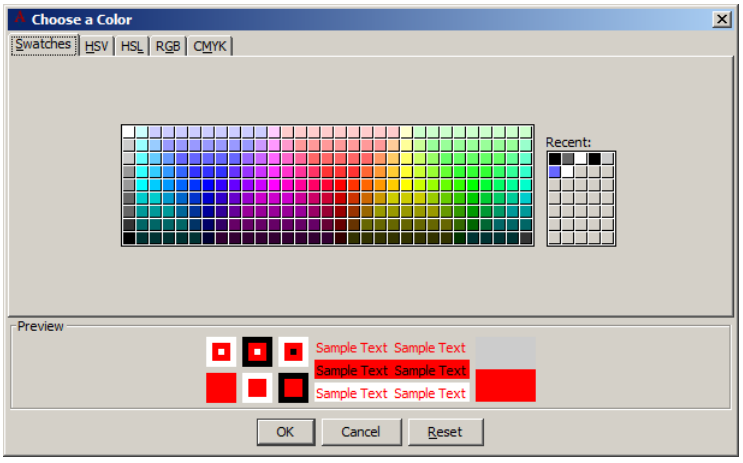
Figure 11-7: (U) Articulation Point Preferences



3. (U) Select the options you prefer and then click **Save**:

   - (U) **Apply Color** – If you select the **Apply Colors** check box, FANTOM colors the articulation nodes using the currently selected ap-color.
   - (U) **Color** – The Articulation Point Color option lets you select the default color to use for articulation point nodes. To select a new color, double-click the **Color** swatch and the Choose a Color dialog box displays (Figure 11-8).

Figure 11-8: (U) Choose a Color dialog box



4. (U) Select a color and then click **OK**.

BIDMAS Importer Preferences

(U) The BIDMAS Importer Preference includes an option for **Debug Dat File Hex**. The option is for internal use so you can keep it deselected.

Betweenness Preferences

(U) These preferences set the default settings for the Betweenness Centrality Analytic (see "Betweenness Analytic" on page 9-10).

(U) To set Betweenness preferences:

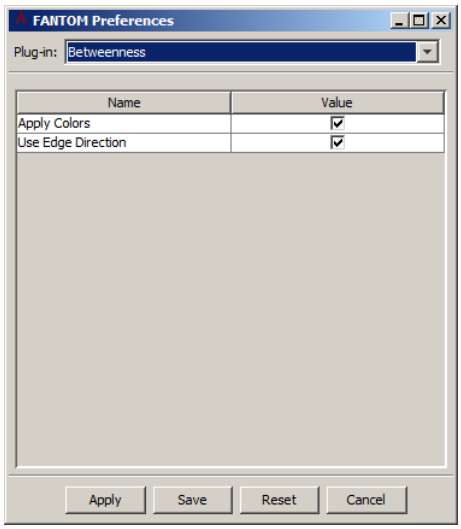
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Betweenness** from the **Plug-in** menu.

   (U) The options for this plug-in display (Figure 11-9).

Figure 11-9: (U) Betweenness preferences



3. (U) Select the options you prefer and then click **Save**:

   - (U) **Apply Colors** – When this check box is selected, FANTOM color codes the nodes with high Betweenness red, those with slightly lower Betweenness yellow, and the rest green.
   - (U) **Use Edge Direction** – If this check box is selected, FANTOM takes the edge direction into consideration when computing the Betweenness values.

CSV Exporter

(U) CSV Exporter preferences let you specify the maximum number of rows per sheet for data sets exported from FANTOM to a .csv file (see "Exporting FANTOM Data to a Delimited File" on page 2-23). The default value is 500,000.

(U) **To set CSV Exporter preferences:**

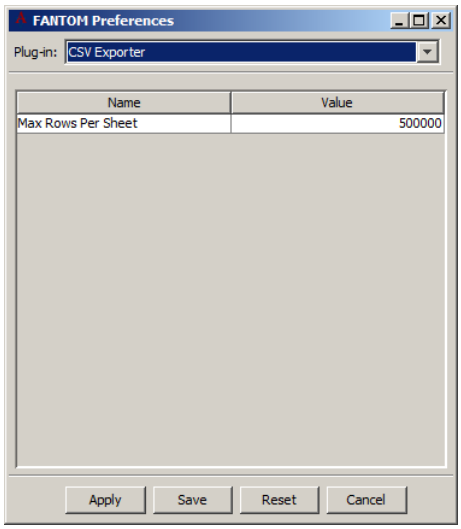
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **CSV Exporter** from the **Plug-in** menu.

   (U) The CSV Exporter preferences display (Figure 11-10).

   Figure 11-10: (U) CSV Exporter preferences



3. (U) Type a new maximum number of rows per sheet value and click **Apply** or **Save**.

Call Chaining Preferences

(U) These preferences set the default settings for the Call Chaining Analytic (see "Call Chaining Analytic" on page 9-8).

(U) To set Call Chaining preferences:

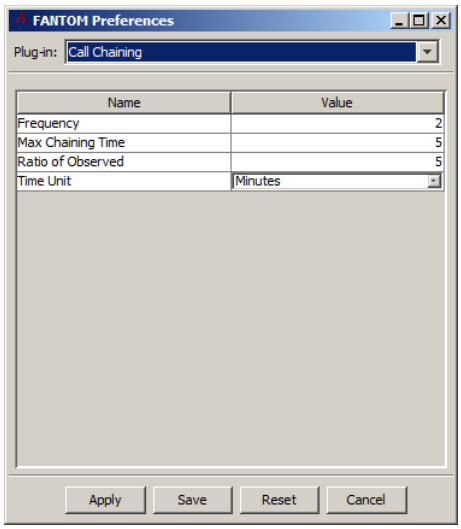
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Call Chaining** from the **Plug-in** menu.

   (U) The options for this plug-in display (Figure 11-9).

   Figure 11-11: (U) Call Chaining preferences



3. (U) Select the options you prefer and then click **Save**.

Circle Layout Preferences

(U) The Circle Layout preferences let you select the default **Radius** for the Circle Layout (see "Circle Layout" on page 7-2).

(U) To set Circle Layout preferences:

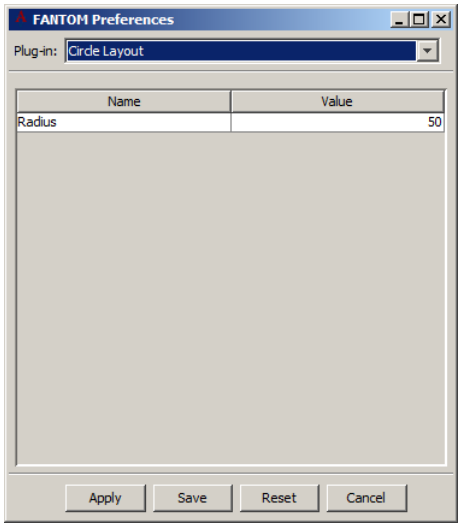
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Circle Layout** from the **Plug-in** menu.

   (U) The options for this plug-in display (Figure 11-12).

Figure 11-12: (U) Circle Layout preferences



3. (U) Click the `50` **Radius** value to make it editable, and then type the factor value you want to use as the default in the **Value** text box.

4. (U) Click **Save**.

Closeness Centrality Preferences

(U) The Closeness Centrality preferences let you select options about how this analytic will behave and which columns it produces (see "Closeness Analytic" on page 9-14).

(U) To set Closeness Centrality preferences:

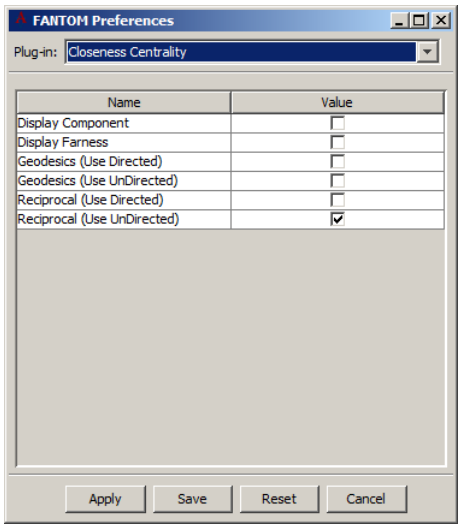
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Closeness Centrality** from the **Plug-in** menu.

3. (U) The options for this plug-in displays.

Figure 11-13: (U) Closeness Centrality preferences



4. Select the options you prefer and click **Apply** or **Save**.

DeDuplication Analytic Preferences

(U) The DeDuplication Analytic preferences lets you specify the default options for the number of days in the Date or Date/Time column sequence to compare for potential duplicates.

(U) To set DeDuplication Analytic preferences:

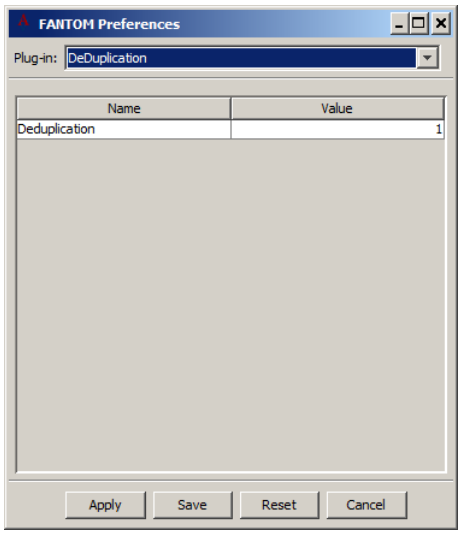
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **DeDuplication** from the **Plug-in** menu.

   (U) The options for this plug-in display (Figure 11-14).

Figure 11-14: DeDuplication preferences



3. Enter the number of days in the sequence of dates in the Date or Date/Time column that you want FANTOM to compare for potential duplicate transactions. The default number is one (1).

4. Click **Apply** or **Save**.

Degree Analytic Preferences

(U) The Degree Analytic preferences lets you specify the default options for the **Degree Analytic** (see "Degree Analytic" on page 9-15).

(U) To set Degree Analytic preferences:

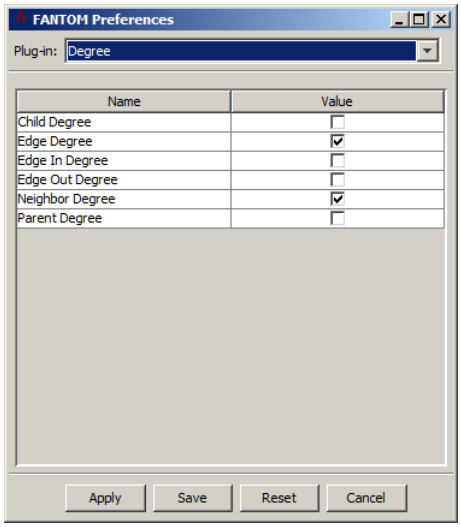
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Degree Analytic** from the **Plug-in** menu.

   (U) The options for this plug-in display (Figure 11-15).

Figure 11-15: (U) Degree Analytic preferences



3. (U) Select any combination of the options.

   (U) There is an *edge* between two nodes when there is at least one connection between them. There is a *multi-edge* between two nodes for every connection between them. For example, there might be several calls between two phone numbers, making several edges but only one multi-edge. Therefore, the Degree Analytic can count both edges and multi-edges, as desired. For many graphs the edge originates with one node (like a phone call) and terminates with another (called a *directed edge*). Therefore, the Degree Analytic can count incoming, outgoing, and total for each node, depending on what you select:

   - (U) **Neighbor Degree**– The sum of the neighbors (inbound and outbound connections).
   - (U) **Parent Degree**– The sum of the parents (inbound connections).
   - (U) **Child Degree**– The sum of the children (outbound connections).
   - (U) **Edge Degree** – The sum of the edges in and out degrees.
   - (U) **Edge In Degree** – The number of communications inbound to a selected node.
   - (U) **Edge Out Degree** – The number of connections outbound from a selected node.

4. (U) Click **Save**.

Disperser Layout Preferences

(U) The Disperser Layout preference let you select default options for the Disperser Layout command (see "Disperser Layout" on page 7-3). The Disperser Layout lets you spread out clusters in the graph. It is useful in order to fully "pull apart" the graph into its separate clusters, if any exist. *Clusters* in a graph are separate groups of connected nodes.

(U) To set Disperser Layout preferences:

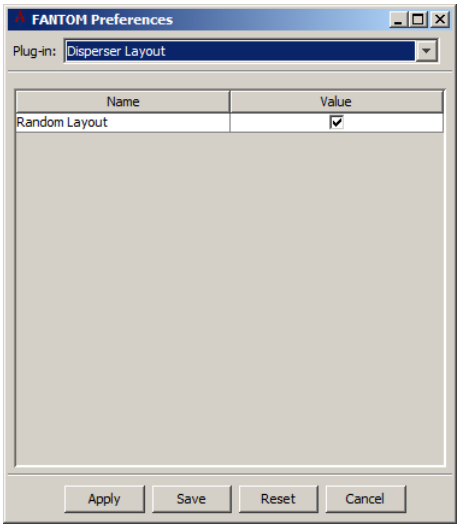
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Disperser Layout** from the **Plug-in** menu.

   (U) The preferences display (Figure 11-16).

Figure 11-16: (U) Disperser Layout preferences



3. (U) Select or deselect **Sort Layout**.

   (U) The Disperser Layout's Sort Layout option spreads out the connected clusters of the graph, sorting them left to right from largest to smallest. If you deselect this check box, the Disperser Layout uses a Random layout by default. The Sort layout is usually faster than a Random layout, but a Random layout takes up less space in the 3D Viewer window.

4. (U) Click **Save**.

Edge Display Preferences

(U) The Edge Display preferences lets you specify colors for default and mixed edges.

(U) To set Edge Display preferences:

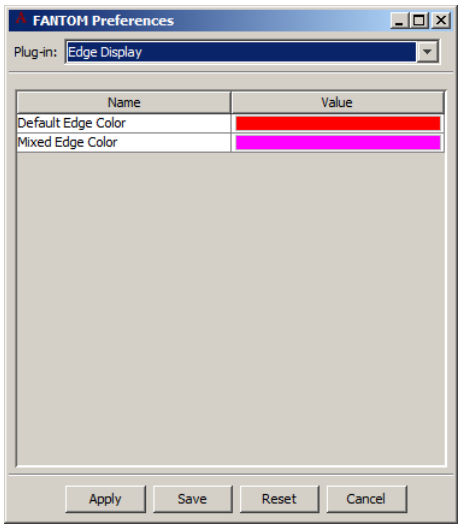
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Edge Display** from the **Plug-in** menu.

   (U) The options display (Figure 11-17).

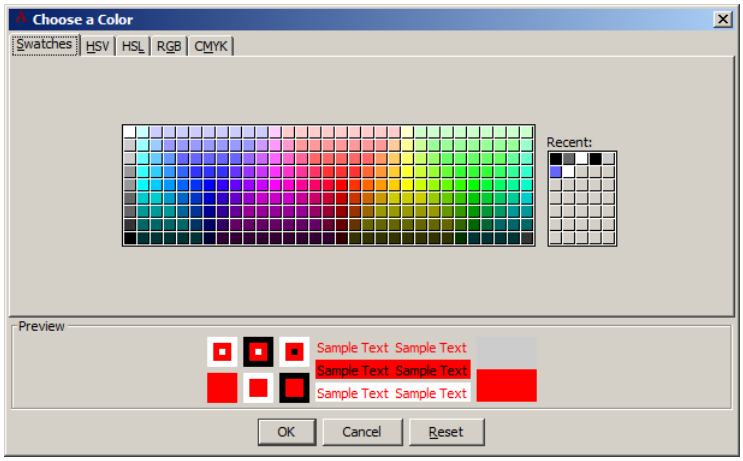
Figure 11-17: (U) Edge Display preferences



3. (U) Double-click a color that you want to change.

   (U) The Choose a Color dialog box displays (Figure 11-18).

Figure 11-18: (U) Choose a Color dialog box



4. (U) Select a new color and click **OK**.
5. (U) Click **Save**.

Eigenvector Centrality Preferences

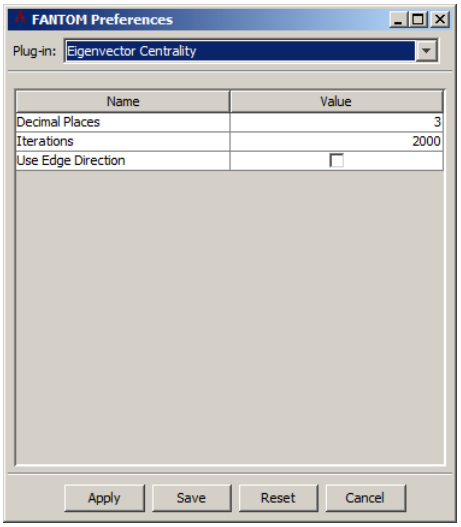
(U) These preferences let you select the default decimal places, iterations, and whether or not to use edge direction.

(U) To set Eigenvector Centrality preferences:

1. (U) Choose **Edit** > **Preferences Manager** in the Controller window.

   (U) The Preferences dialog box displays.
2. (U) Choose **Eigenvector Centrality** from the **Plug-in** menu.
3. (U) The options for this plug-in display (Figure 11-19).

Figure 11-19: Eigenvector Centrality preferences



4. (U) Select the default options you prefer and click **Save**.

Force Directed Preferences

(U) The Force Directed preferences let you select default options for the Force Directed layout command (see "Force Directed Layout" on page 7-7).

(U) To set Force Directed preferences:

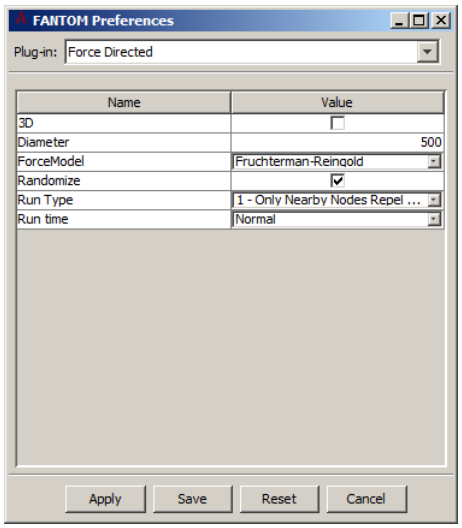
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Force Directed** from the **Plug-in** menu.

   (U) The options display (Figure 11-20).

Figure 11-20: (U) Force Directed Preferences tab



3. (U) Specify any of the options you prefer and then click **Save**.

   - (U) **3D** – Select this check box if you want the Force Directed layout to produce 3D layouts by default.
   - (U) **Diameter** – The Diameter default scale is 250; increase the number to increase the diameter or reduce it to reduce the diameter of the graph.
   - (U) **Force Model** – Select the force model you want to use by default: **Fruchterman-Reingold** or **Molecular Force Model**. For more information about these models, see "Force Directed Layout" on page 7-7.
   - (U) **Randomize** – If you want to use this layout repeatedly to increase the separation between clusters in the graph, you may want to deselect this check box to change the default setting.
   - (U) **Run Type** – Select the default Run Type you prefer:
     - **1 - Only Nearby Nodes Repel (Fast)**
     - **2 - All Nodes Repel, Approx. (Slower)**
     - **3 - All Nodes Repel, Exact (Slowest)**
   - (U) **Run Time** – Select your preference for Run Time: **Very Short**, **Short**, **Normal**, **Long**, or **Very Long**.

General Preferences

(U) The General preferences let you select general default options for FANTOM.

(U) To set General preferences:

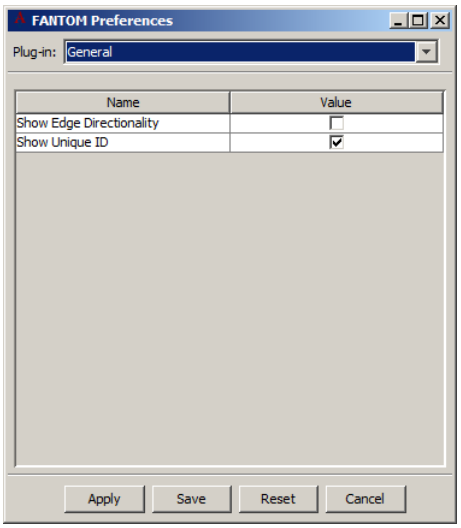
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **General Preferences** from the **Plug-in** menu.

   (U) The General preferences display.

Figure 11-21: (U) General Preferences



3. (U) Specify any of the options and then click **Save**.

   - (U) **Show Unique ID** – If you select this check box, FANTOM displays the node and edge **ID** column in the controller tables.

General Importer Preferences

(U) The General Importer preferences let you indicate whether to display the Show Merge dialog box at the end of the import process.

(U) T**o set General Importer preferences:**

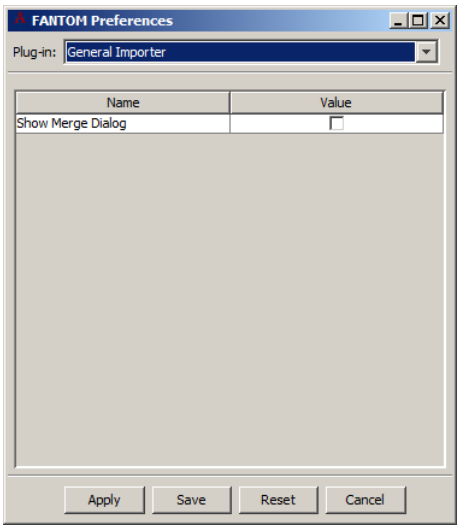
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **General Importer** from the **Plug-in** menu.

(U) The General Importer preferences displays.

Figure 11-22: (U) General Importer preferences



3. (U) Deselect the **Value** check box to hide the Merge Nodes dialog box at the end of the importer process or keep the check box selected to show it.

GeoIP Local Preferences

(U) The GeoIP Local Analytic preferences specify settings for using the Max Mind GeoIP data set. Max Mind GeoIP lets you determine the geographical location of IP addresses in the data sets you are analyzing with FANTOM.

(U) To view or change your GeoIP Local Analytic preferences:

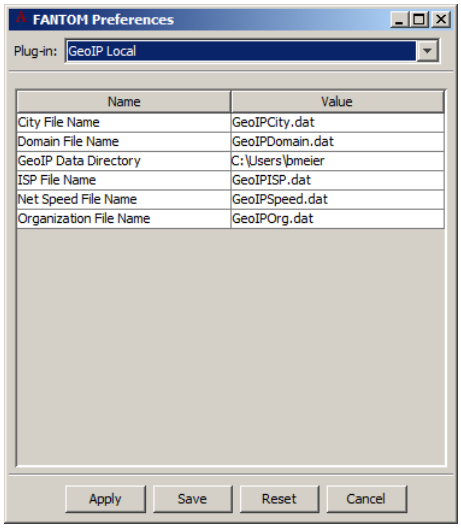
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **GeoIP Local** from the **Plug-in** menu.

3. (U) This plug-in's options display (Figure 11-31).

Figure 11-23: (U) GeoIP Local Analytic preferences dialog box



4. (U) View or specify options as needed and click **OK** or **Apply**.

Icon Palettes Preferences

(U) Keep the Icon Palettes preferences unchanged unless instructed by FANTOM support engineers to change the value.

Link Cluster Layout Preferences

(U) These preferences let you specify the default values for the Link Cluster Layout command (see "Link Cluster Layout" on page 7-17). This includes whether or not to color edges, the maximum distance, the number of clusters, and the partition method.

(U) **To view or change your Link Cluster Layout preferences:**

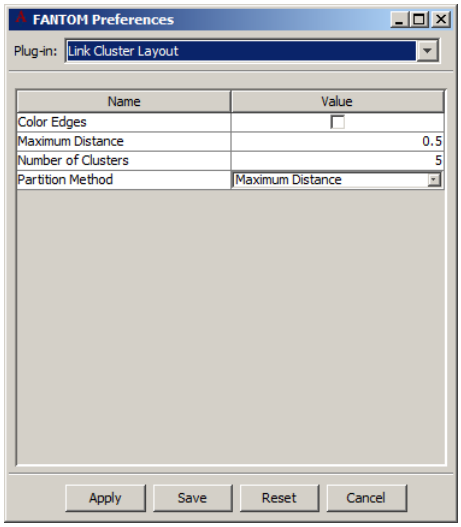
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Link Cluster Layout** from the **Plug-in** menu.

3. (U) This plug-in's options display (Figure 11-24).

Figure 11-24: (U) Link Cluster Layout preferences



4. (U) Select the default options you prefer and click **Save**.

PCAP Importer Preferences

(U) The PCAP Importer preferences let you specify preferences to use during a PCAP import (see "Importing PCAP Data" on page 2-19).

(U) **To set PCAP Importer preferences:**

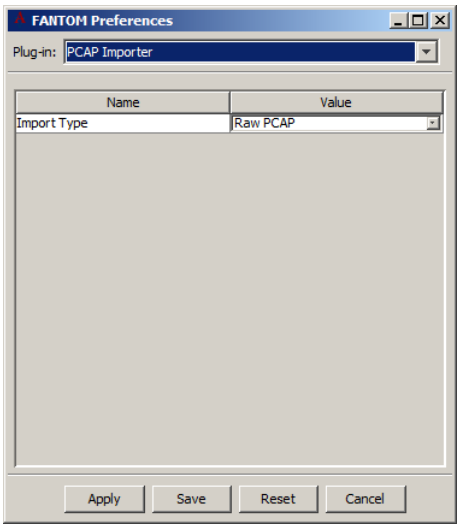
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **PCAP Importer** from the **Plug-in** menu.

   (U) The PCAP Importer preferences display (Figure 11-25).

Figure 11-25: (U) PCAP Preferences dialog box



3. (U) Select the **Import Type** to use as a default (**Raw PCAP** or **Aggregate TCP PCAP**), and then click **Save**.

Prestige Centrality Preferences

(U) The Prestige Centrality preferences let you select the default number of decimal places and whether or not to use the reverse measure (see "Prestige Centrality Preferences" on page 11-25).

(U) To set Prestige Centrality preferences:

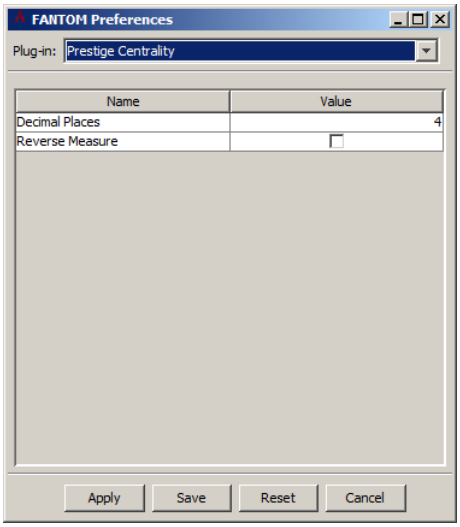
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Prestige Centrality** from the **Plug-in** menu.

   (U) The Prestige Centrality preferences display (Figure 11-26).

Figure 11-26: (U) Prestige Centrality preferences

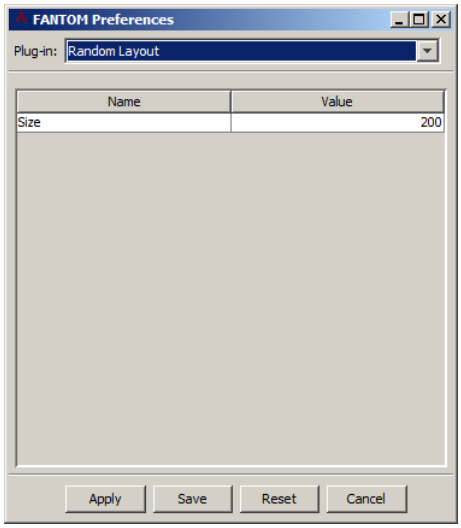


3. (U) Choose the default preferences you prefer and click **Save**.

Random Layout Preferences

(U) The Random Layout preferences let you specify the default size for the Random Layout.

Figure 11-27: (U) Random Layout preferences



Reciprocated Analytic Preferences

(U) These preferences let you specify the default values for the Reciprocated analytic (see "Reciprocated Links Analytic" on page 9-37).

(U) **To set Reciprocated Analytic preferences:**

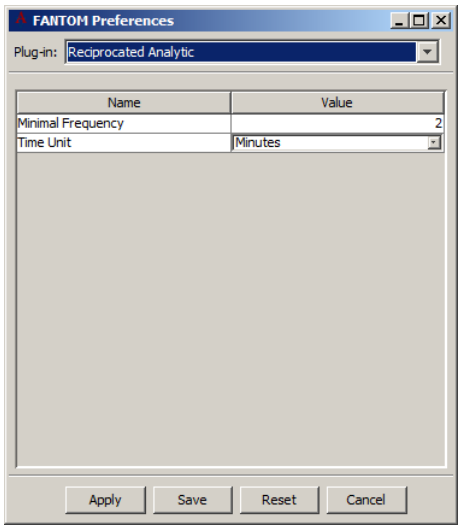
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Reciprocated Analytic** from the **Plug-in** menu.

3. (U) The Reciprocated Analytic preferences display (Figure 11-28).

Figure 11-28: (U) Reciprocated Analytic preferences



4. (U) Select the options you prefer and click **Save**.

Related Nodes Preferences

(U) The Related Nodes preferences allow you to select default values for the Related Nodes analytic (see "Related Nodes Analytic" on page 9-34).

(U) To set Related Nodes preferences:

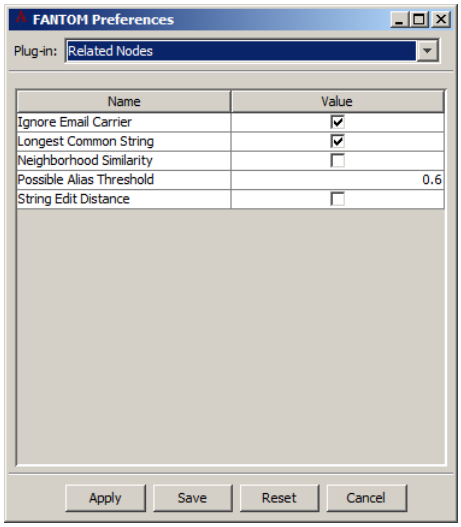
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Related Nodes** from the **Plug-in** menu.

   (U) The Related Nodes preferences display (Figure 11-29).

Figure 11-29: (U) Related Nodes Analytic preferences



3. (U) Select an **Aggregation Method** (**Minimum Aggregation**, **Mean Aggregation**, or **Maximum Aggregation**) or the check boxes beside any of the other options for this analytic.

   (U) For more information about how FANTOM handles Aggregation Method in the Related Nodes analytic, see "Related Nodes Analytic" on page 9-34.

4. (U) Click **Save**.

Research Conduit Preferences

(U) The Research Conduit preference lets you choose the Open Research SQL database to query.

(U) **To set Research Conduit preferences:**

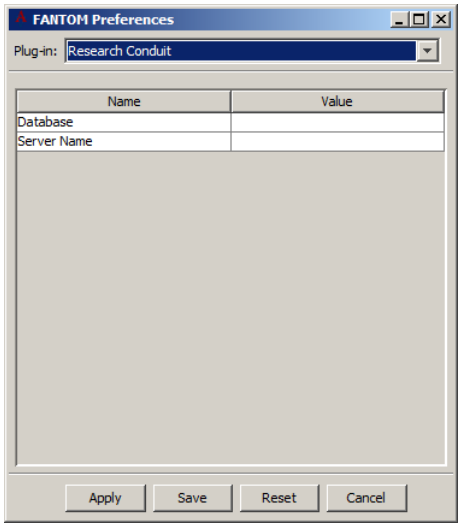
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Reference Conduit** from the **Plug-in** menu.

   (U) The Reference preferences display (Figure 11-25).

Figure 11-30: (U//FOUO) Reference Conduit preferences



3. (U//FOUO) Specify the **Database** and **Server Name** for the Open Research conduit to query.

Research Importer Preferences

(U//FOUO) The Research Importer preferences lets you specify options for Open Research file imports.

(U) To set Research Importer preferences:

1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Research Importer** from the **Plug-in** menu.

3. (U) This plug-in's options display.

4. (U) Select the options you prefer and click **Save**.

Source to Destination Path Preferences

(U) The Source to Destination Path preferences let you select the default options for the Source to Destination Path analytic (see "Source to Destination Path Analytic" on page 9-39).

(U) To set Source to Destination Path preferences:

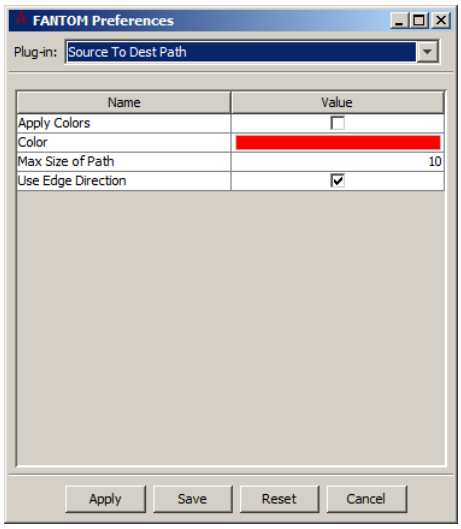
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Source to Dest Path** from the **Plug-in** menu.

3. (U) This plug-in's options display (Figure 11-31).

Figure 11-31: (U) Source to Destination Path Analytic preferences



4. (U) Select the options you prefer and then click **Save**:

   - (U) **Apply Colors** – Select this check box if you want the Source to Destination Path analytic to apply the selected color to the Source and Target nodes you've selected when running the analytic.
   - (U) **Color** – Double-click the Color swatch and select a default color for this analytic.
   - (U) **Max Size of Path** – Specify the default maximum size of the paths to include when running this analytic.
   - (U) **Use Edge Direction** – Select this check box to select it by default in the Source to Destination Path analytic dialog box.

Tiered Layout Preferences

(U) To set Tiered Layout preferences:

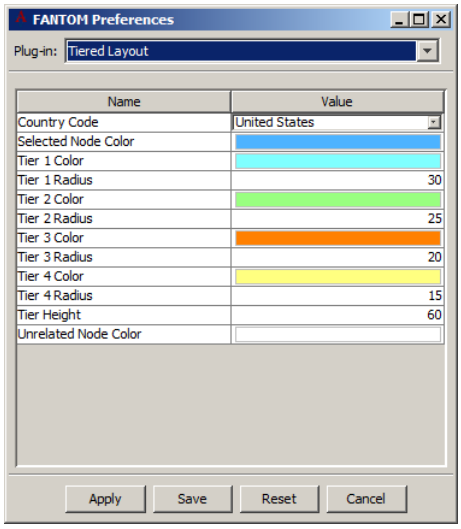
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Tiered Layout** from the **Plug-in** menu.

   (U) This plug-in's options display (Figure 11-32).

Figure 11-32: (U) Tiered Layout Preferences



3. (U) Select the options you prefer and then click **Save**:
   - (U) **Selected Node Color**
   - (U) **Tier 1 Color**
   - (U) **Tier 1 Radius**
   - (U) **Tier 2 Color**
   - (U) **Tier 2 Radius**
   - (U) **Tier 3 Color**
   - (U) **Tier 3 Radius**
   - (U) **Tier 4 Color**
   - (U) **Tier 4 Radius**
   - (U) **Tier Height**
   - (U) **Unrelated Node Color**

Time Controller Preferences

(U) To set Time Controller preferences:

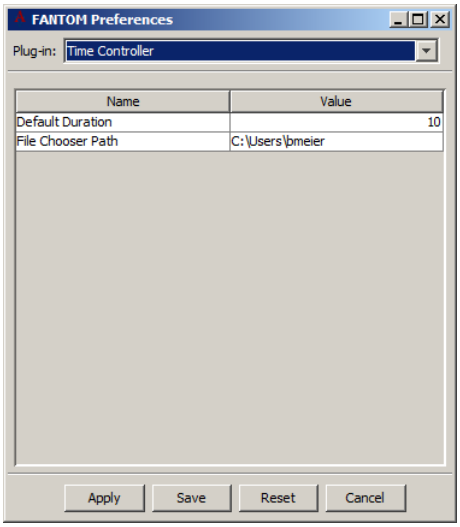
1. (U) Choose **Edit** > **Preference Manager** in the Controller window.

   (U) The Preferences dialog box displays.

2. (U) Choose **Time Controller** from the **Plug-in** menu.

(U) The Time Controller preferences display (Figure 11-33).

Figure 11-33: (U) Time Controller preferences



3. (U) Type a new duration value and click **Apply** or **Save**.

Creating Import Templates

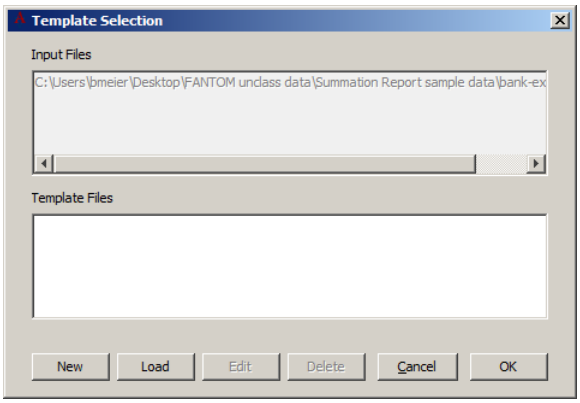
(U) Before importing a file or after connecting to an Oracle, MySQL, or PostgreSQL database using the **Databases** > **Database Importer** command, you may still need to create a template that defines what information FANTOM should copy from the file or database and display in the FANTOM Controller window table.

(U) To access the Template Editor dialog box:

1. (U) Perform the first three (3) steps in "Importing Delimited Data" on page 2-9.

   (U) The Template Selection dialog box displays.

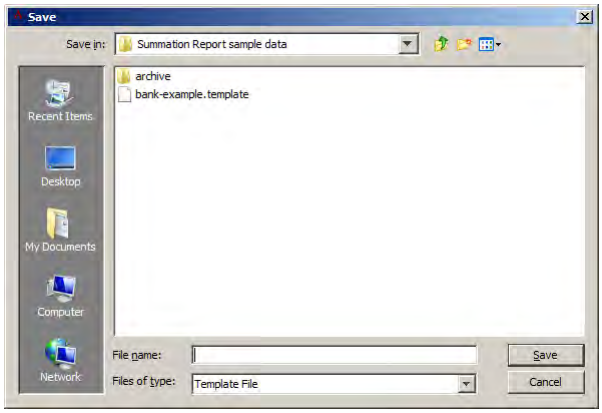
Figure 12-1: (U) Template Selection dialog box



2. (U) Click the **New** button to create a new template for this data set.

   (U) FANTOM displays a Save dialog box where you can provide a filename for the new template and then define template settings (Figure 12-2).

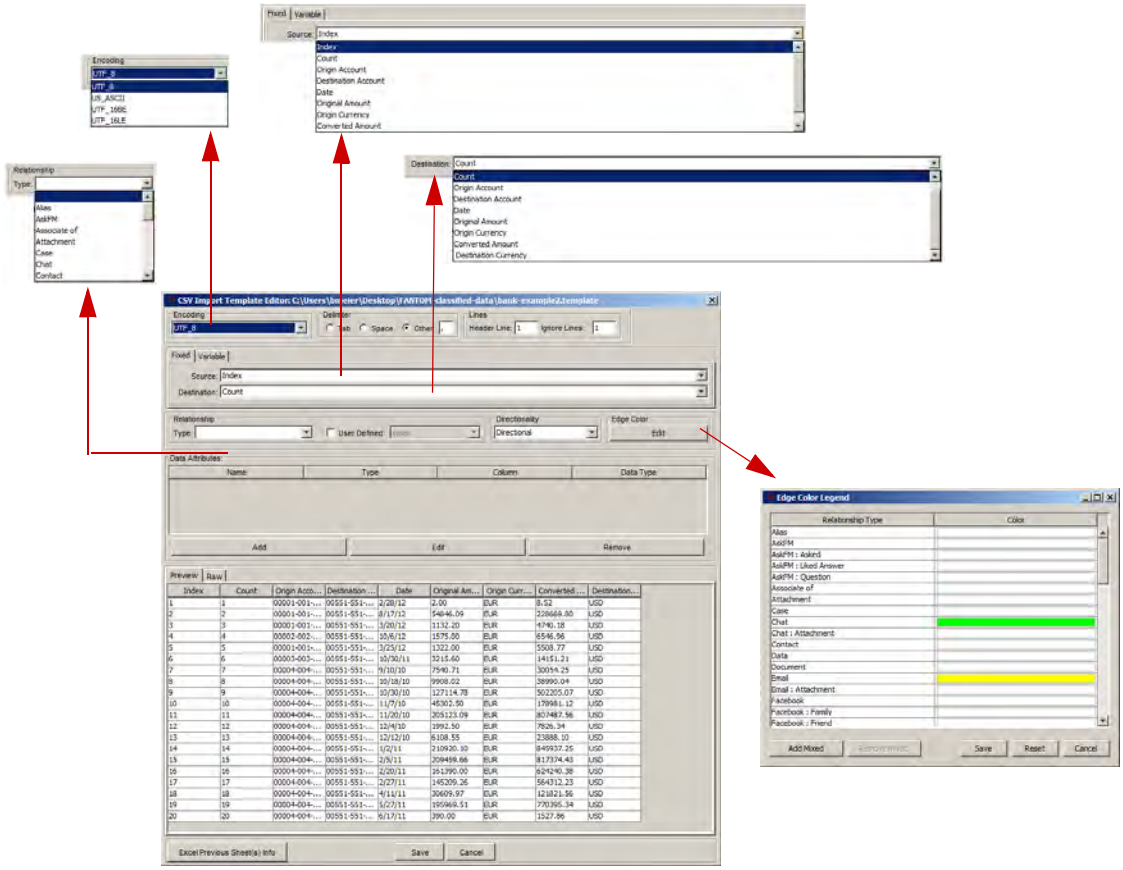
Figure 12-2: (U) Save dialog box for new template



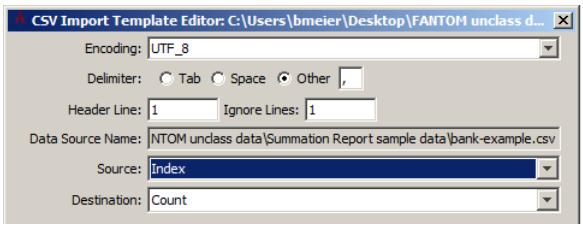
3. (U) Type a template filename in the **File name** text box and click **Save**.

   (U) The Template Editor dialog box displays.

Figure 12-3: (U) Template Editor dialog box

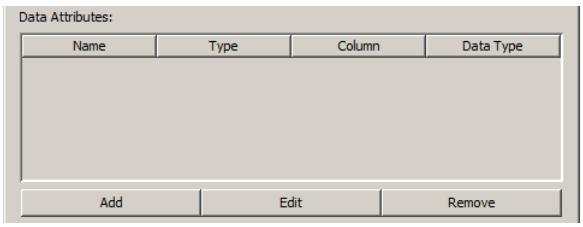


4. (U) Specify template settings to use for this imported data:



- (U) **Encoding** – FANTOM examines the database table and automatically selects one of the available character encoding types: US-ASCII, UTF-8, UTF-16BE (big endian), or UTF-16LE (little endian). You should not need to change this selection.
- (U) **Delimiter** – Specify the character that separates individual fields in the table (**Tab**, **Space**, or the character you type in the **Other** text box).
- (U) **Header Line** – Type the number of rows used for table column headings.
- (U) **Ignore Lines** – Type the number of rows at the top of the table that FANTOM should ignore. This is typically the number of Header lines in the file.
- (U) **Source** – Select the table column (in the format <*column number*>-<*column title*>) that lists the initiator of the point-to-point communication. For example, the sender email address or caller phone number.
- (U) **Destination** – Select the table column (in the format <*column number*>-<*column title*>) that lists the recipient of the point-to-point communication.
- (U) **Relationship** section provides settings that will be used in future versions of FANTOM.

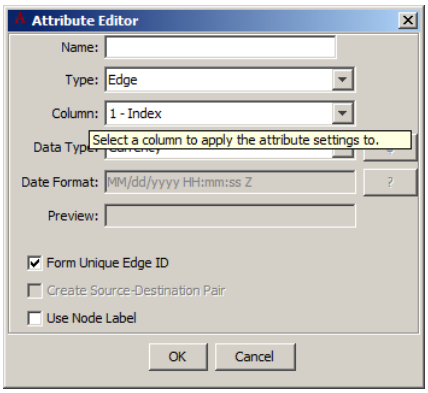
- (U) **Data Attributes** section



- (U) Click the **Add** button to include columns in addition to the **Source** and **Destination** in the Controller table. You can have more than one attribute defined for a column. For example, you might want to define an attribute for a Date or Time column.

(U) The Attribute Editor dialog box displays (Figure 12-4).

Figure 12-4: (U) Attribute Editor dialog box



(U) Specify the following Attribute options, and then click the **OK** button:

- (U) **Name** – Type the attribute name to use to describe this column of information. If you type a name that exactly matches one of the column titles in the database, FANTOM applies the attribute settings to determine how that column of information is treated. If you type a different name than the column you select, FANTOM creates a new column at the right in the Controller window which applies the attributes you specify using the **Attribute Name** as the Column title.
- (U) **Type** – Select whether this column is a **Source Node**, **Destination Node**, or **Edge** (an *edge* is one or more relationships, or connections, between nodes).
- (U) **Column** – Select a column to apply the attribute settings to.
- (U) **Data Type** – Select the type of data the column contains: **String** (alphanumeric text), **Number**, **Date and Time**, **Date**, **Time**, **Boolean**, **Epoch Time**, **Phone Number**, **IP Address**, **IP Address IPv6**, **URL**, or **Currency**.
- (U) **Date Format** – Edit the characters that define the format of the selected column that contains date information. Click the **?** button to display a Help window defining the options.

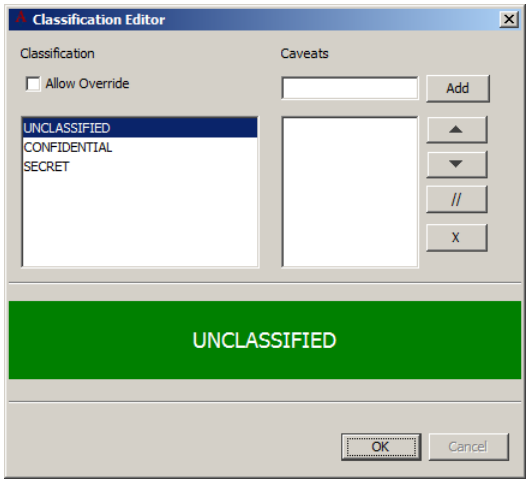
- (U) **Form Unique Edge ID** – If your database does not contain a column defining a unique edge ID, you can add an attribute that is used to create a unique ID by selecting this check box.
- (U) **Create Source-Destination Pair** – Select this check box and FANTOM creates a source and a destination Attribute row for this attribute.
- (U) **Use Node Label** – Select the Use Node Label check box

- (U) **Preview** and **Raw** – Select the type of sample information you want to see. **Preview** displays the information in a simple table format. **Raw** displays values separated with the delimiter character used in the file to separate individual pieces of information (*fields*).

5. (U) Click the **Save** button to save these settings in case you need to retrieve the information again later, or retrieve updated information later.
6. (U) Click the **OK** button in the Template Selection dialog box.
7. (U) Click the **Process CSV Import** button to retrieve the data specified and display it in FANTOM so you can begin analysis.

   (U) The Classification Editor dialog box displays.

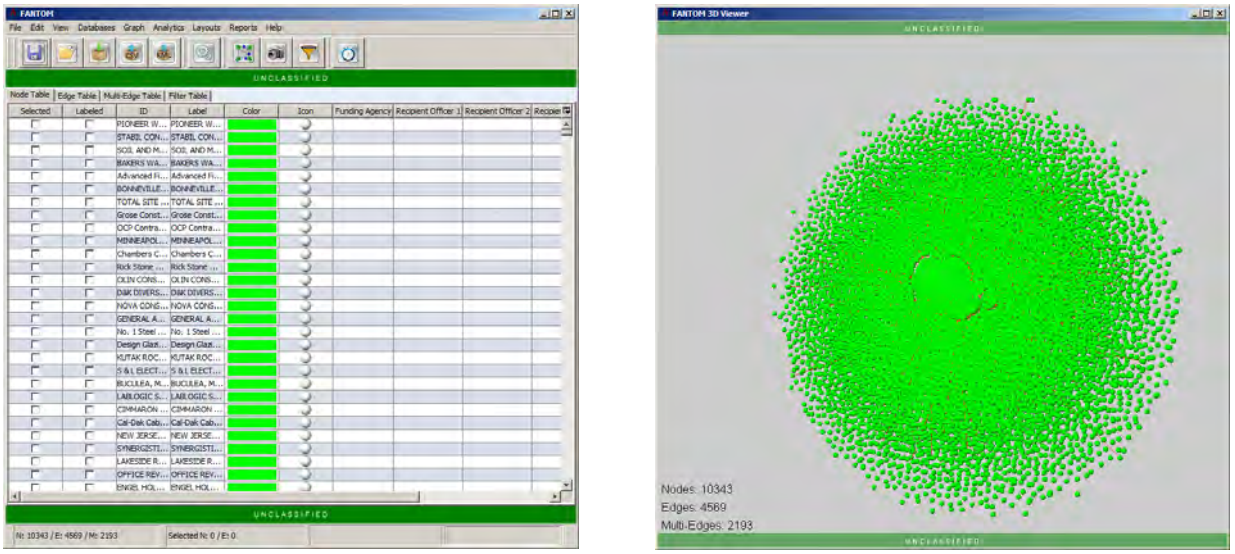
Figure 12-5: (U) Classification Editor dialog box



8. (U) Select the classification settings for this data set and click **OK**.

   (U) FANTOM imports the data set using the settings you specified and displays the information in table form in the Controller window and as a graph in the 3D Graph Viewer window.

Figure 12-6: (U) FANTOM Controller and 3D Graph Viewer windows (sample data: All_ContractsY12Q3+12Q4+13Q1.session)



Troubleshooting

(U) This appendix provides answers to common questions and identifies where you can obtain FANTOM log information.

Questions and Answers

I was zooming in the 3D Viewer and the graph disappeared. What happened?

(U) If you zoom in and everything changes to the background color, you have "gone past" the nodes and edges. Zoom out until you start seeing the graph again.

FANTOM starts, but the 3D Viewer window does not display. How can I fix the problem?

(U) Choose **View** > **3D Viewer** in the FANTOM Controller window.

(U) Until the next software update, FANTOM will remember your choice and open the 3D Viewer window when it opens the Controller window.

The FANTOM 3D Viewer window displays, but I cannot see any nodes or edges. What do I do next?

(U) Contact your administrator and request the latest version of the NVIDIA video card driver be installed on your workstation.

(U) You can verify the current version by choosing **Start** > **Settings** > **Control Panel** and double-clicking the **NVIDIA Control Panel**. Next, click the **System Information** link at the bottom left of the control panel window. The System Information dialog box displays your workstation's current video card hardware component and the installed **Driver version**.

Viewing Task Details

(U) In FANTOM, *tasks* are the commands you choose that cause the application to perform actions, such as querying a database, running an analytic, rearranging the graph with a layout, or producing a report.

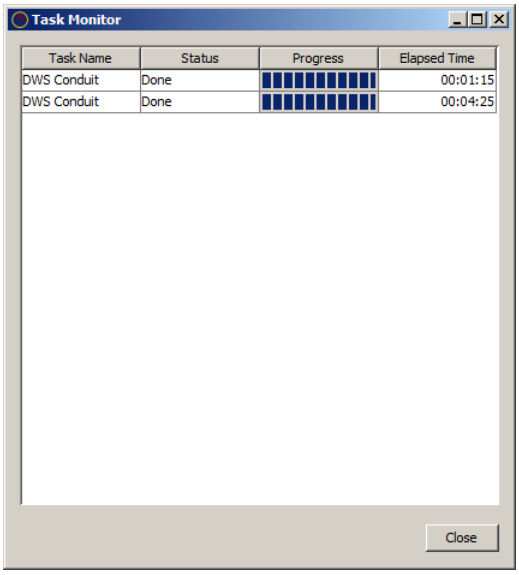
(U) You can watch the progress of these tasks by opening the Task Monitor.

(U) To view task details:

(U) Choose **View** > **Task Monitor**.

(U) FANTOM displays the Tasks dialog box (Figure A-1) with one or more **Task Names** along with the **Status** and **Elapsed Time**.

Figure A-1: (U) Task Details



Viewing the History Log

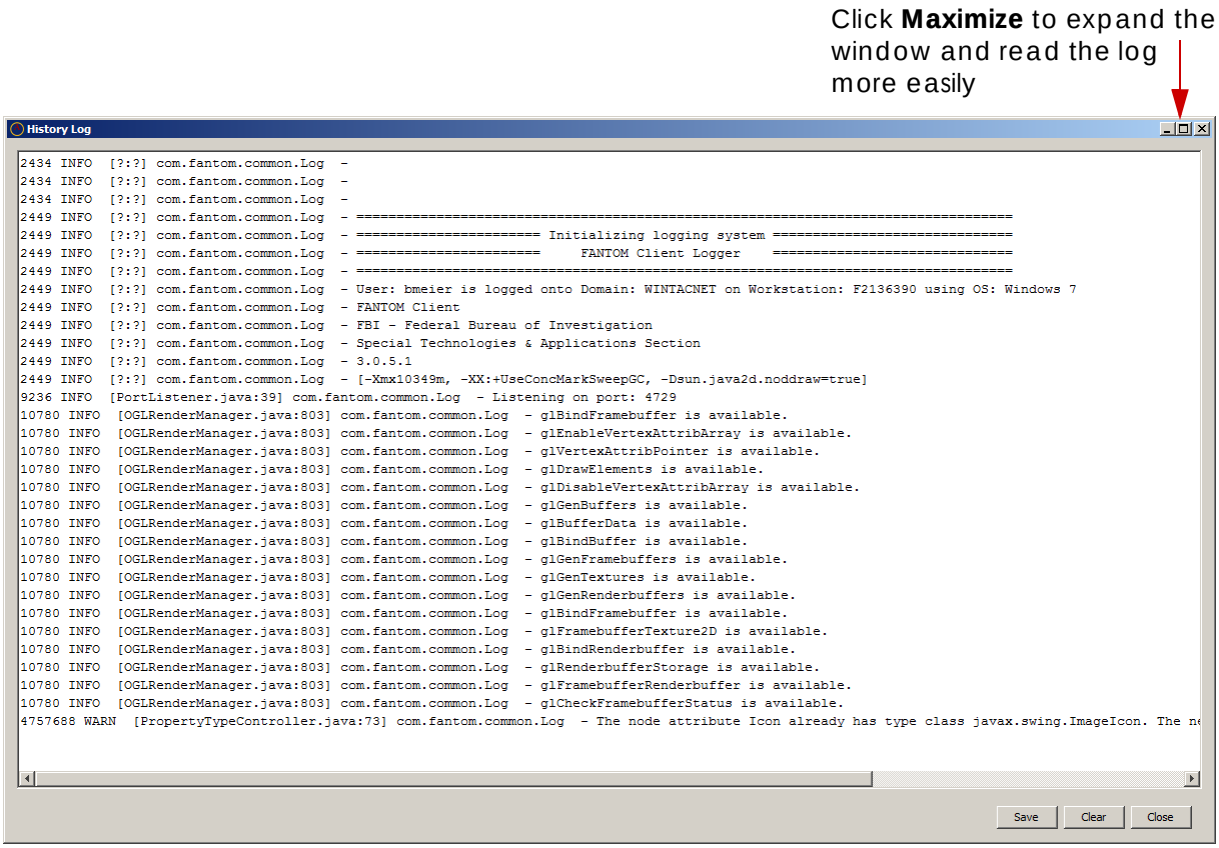
(U) The FANTOM History Log shows application messages, such as start-up information, warnings, and errors. If you have any problems with FANTOM but the application does not crash, you could open this window and either Copy/Paste the text or Save it. Then send the information to the Advanced Visualization Team. This information can help them to discover and correct issues you might encounter.

(U) **To view the History Log:**

(U) Choose **View** > **History Log**.

(U) FANTOM displays the History Log window (Figure A-2).

Figure A-2: (U) History Log



(U) You can drag the bottom right corner to resize the window or click the **Maximize** button at the top right to read the information more easily.

Tip: (U) You can copy the contents of the History Log to your Clipboard by clicking or dragging inside the window, pressing CTRL+A and then pressing CTRL+C.

Opening the Comprehensive FANTOM.Log File

(U) The comprehensive FANTOM.log file is the first place you should look if you encounter a problem. This information can also help the FANTOM Team to identify an issue or bug.

(U) **To open the comprehensive FANTOM log:**

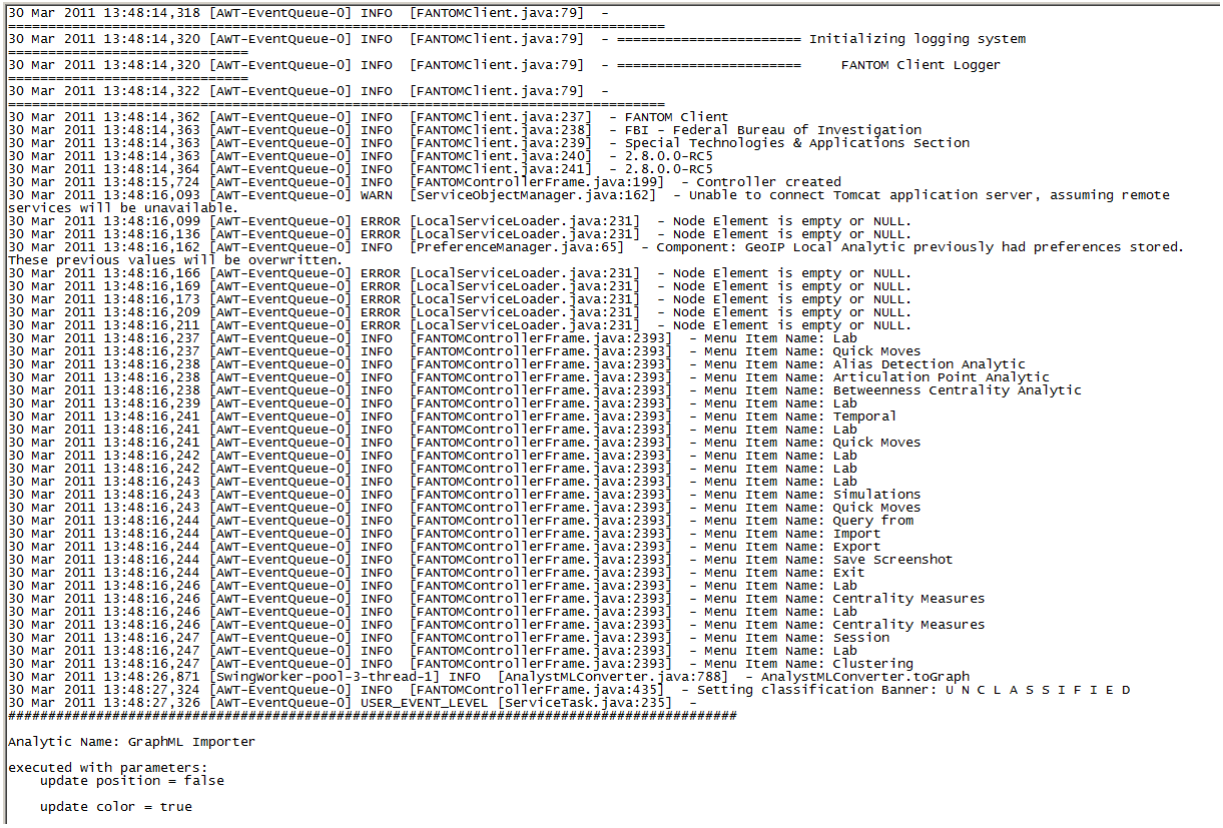
1. (U) Go to the desktop and locate the file at:

`<user_home_directory>\FANTOM\log\FANTOM.log<date-time><incremented number>.`

2. (U) Double-click the file to open it in Notepad.

   (U) Notepad displays the contents of your comprehensive log (see Figure A-3).

Figure A-3: (U) Example of comprehensive FANTOM Log data



```
30 Mar 2011 13:48:14,318 [AWT-EventQueue-0] INFO  [FANTOMClient.java:79]  -
================================================================================
30 Mar 2011 13:48:14,320 [AWT-EventQueue-0] INFO  [FANTOMClient.java:79]  - ======================== Initializing logging system
==============================
30 Mar 2011 13:48:14,320 [AWT-EventQueue-0] INFO  [FANTOMClient.java:79]  - ========================     FANTOM Client Logger
==============================
30 Mar 2011 13:48:14,322 [AWT-EventQueue-0] INFO  [FANTOMClient.java:79]  -
================================================================================
30 Mar 2011 13:48:14,362 [AWT-EventQueue-0] INFO  [FANTOMClient.java:237]  - FANTOM Client
30 Mar 2011 13:48:14,363 [AWT-EventQueue-0] INFO  [FANTOMClient.java:238]  - FBI - Federal Bureau of Investigation
30 Mar 2011 13:48:14,363 [AWT-EventQueue-0] INFO  [FANTOMClient.java:239]  - Special Technologies & Applications Section
30 Mar 2011 13:48:14,363 [AWT-EventQueue-0] INFO  [FANTOMClient.java:240]  - 2.8.0.0-RC5
30 Mar 2011 13:48:14,364 [AWT-EventQueue-0] INFO  [FANTOMClient.java:241]  - 2.8.0.0-RC5
30 Mar 2011 13:48:15,724 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:199]  - Controller created
30 Mar 2011 13:48:16,093 [AWT-EventQueue-0] WARN  [ServiceObjectManager.java:162]  - Unable to connect Tomcat application server, assuming remote
services will be unavailable.
30 Mar 2011 13:48:16,099 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,136 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,162 [AWT-EventQueue-0] INFO  [PreferenceManager.java:65]  - Component: GeoIP Local Analytic previously had preferences stored.
These previous values will be overwritten.
30 Mar 2011 13:48:16,166 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,169 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,173 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,209 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,211 [AWT-EventQueue-0] ERROR [LocalServiceLoader.java:231]  - Node Element is empty or NULL.
30 Mar 2011 13:48:16,237 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,237 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Quick Moves
30 Mar 2011 13:48:16,238 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Alias Detection Analytic
30 Mar 2011 13:48:16,238 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Articulation Point Analytic
30 Mar 2011 13:48:16,238 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Betweenness Centrality Analytic
30 Mar 2011 13:48:16,239 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,241 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Temporal
30 Mar 2011 13:48:16,241 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,241 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Quick Moves
30 Mar 2011 13:48:16,242 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,242 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,243 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,243 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Simulations
30 Mar 2011 13:48:16,243 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Quick Moves
30 Mar 2011 13:48:16,244 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Query from
30 Mar 2011 13:48:16,244 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Import
30 Mar 2011 13:48:16,244 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Export
30 Mar 2011 13:48:16,244 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Save Screenshot
30 Mar 2011 13:48:16,244 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Exit
30 Mar 2011 13:48:16,246 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,246 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Centrality Measures
30 Mar 2011 13:48:16,246 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,246 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Centrality Measures
30 Mar 2011 13:48:16,247 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Session
30 Mar 2011 13:48:16,247 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Lab
30 Mar 2011 13:48:16,247 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:2393]  - Menu Item Name: Clustering
30 Mar 2011 13:48:26,871 [SwingWorker-pool-3-thread-1] INFO  [AnalystMLConverter.java:788]  - AnalystMLConverter.toGraph
30 Mar 2011 13:48:27,324 [AWT-EventQueue-0] INFO  [FANTOMControllerFrame.java:435]  - Setting classification Banner: U N C L A S S I F I E D
30 Mar 2011 13:48:27,326 [AWT-EventQueue-0] USER_EVENT_LEVEL [ServiceTask.java:235]  -
################################################################################

Analytic Name: GraphML Importer

executed with parameters:
    update position = false

    update color = true
```

Viewing Retraceable Steps

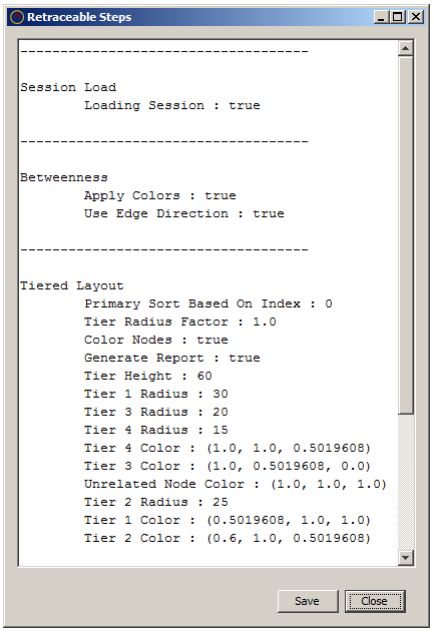
(U) FANTOM now records the steps you take with a data set. This includes the commands you choose along with the settings. When you save a session file, this information is included. If you open the session file and perform more steps, that information is appended to the Retraceable Steps.

(U) To view retraceable steps:

1. (U) Choose **View** > **Retraceable Steps**.

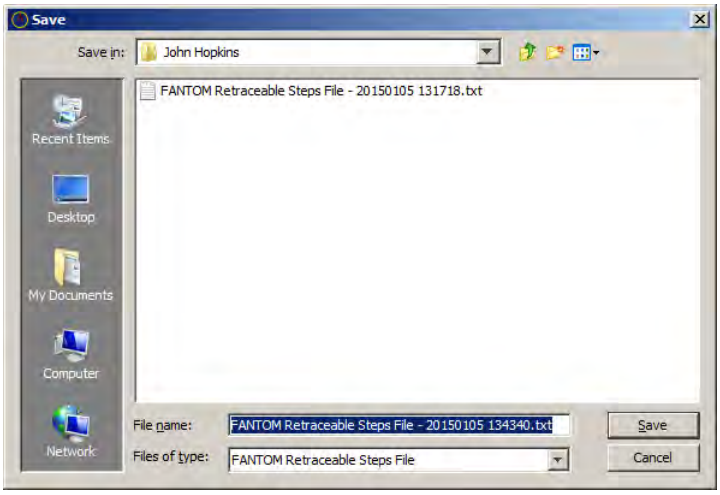
   (U) FANTOM displays the Retraceable Steps window (Figure A-4).

Figure A-4: (U) Retraceable Steps window



2. (U) Click the **Save** button if you want to save a copy of the current Retraceable Steps list.

   (U) FANTOM displays a standard Save dialog box.



3. (U) Select a location, specify a filename and click **Save**.

   (U) FANTOM saves the text file to the location you selected.

Duplicates Error Message

(U) If a data set you import contains duplicate records, FANTOM displays a message to let you know. It only displays identical records one time in the Controller and 3D Viewer windows.

Glossary

(U) This appendix provides a list of visualization and technology terms.

Alias Detection Analytic

(U) In FANTOM version 3.0.8, the Alias Detection analytic has been renamed to the Related Nodes analytic. See Chapter 9, "Related Nodes Analytic".

Analytic

(U) An analytic command performs a computation upon records in a set of data and adds the results in one or more columns in the Controller table. Analytics point out meaningful patterns in data, such as Articulation Points (or "bridges"), Betweenness Centrality ("busiest intersections"), and so on. Analytics may color nodes to highlight those with the highest levels of results. Analytics do not rearrange nodes in the 3D Viewer like the Layout commands do (see Layout).

BMP file

(U) BMP is the standard bitmap image file format used with Microsoft Windows-based computers. You can open a BMP file using Microsoft Paint or many other graphics applications.

Children

(U) A *child* is a node at the remote end of an out-directed edge from a given node. For example, if the graph represents communications, then a child node of node A, is one that receives a communication from node A.

Compressed file

(U) A *compressed* file uses mathematical algorithms and other strategies to reduce the size of a file.

Delimited file

(U) A *delimited file* is a plain text file—comma separated value (.csv), delimiter separated value (.dsv), Microsoft Excel (.xls), or text (.txt).

Domain Axis

(U) The horizontal axis in the Report Services chart.

Edge

(U) Prior to FANTOM 3.0, an *edge* was called a *link* and defined as a line that represented one or more relationships between two nodes. In FANTOM 3.0, an edge has been redefined to indicate one relationship between two nodes. Multiple relationships between two nodes is now called a *Multi-Edge*.

FANTOM Deployment Kit (FDK)

(U) A high-end standalone computer to run the FANTOM software for intensive analysis work.

Filters

(U) *Filters* are a way to selectively hide information displayed. When you add and enable a filter, FANTOM hides the information that matches the filter criteria. When you disable that filter, FANTOM shows the hidden information again. Filtered information is not deleted.

GraphML file

(U) GraphML (Graph Markup Language) files are XML-based files used to define the contents and characteristics of a graph. FANTOM imports GraphML files, but no longer exports them.

GUI

(U) A Graphic User Interface (GUI) is the objects you see, and can interact with, on the computer display. Objects include windows, dialog boxes, messages, text boxes, check boxes, radio buttons, and buttons.

IVML

(U) Information Visualization Markup Language

KML

(U) Keyhole Markup Language stores geographic modeling information in XML format including placemarks, text descriptions, and so on. KML files are used in Google Earth and other geospatial software applications.

Layout

(U) Layout commands arrange nodes in the 3D Viewer window in meaningful ways. For example, the Force Directed Layout moves nodes

based on magnetic attraction, repulsion, so that connected nodes attract and are closer while unconnected nodes repel and are pushed away.

Link

(U) In FANTOM versions prior to 3.0, a *link* was a single connection or relationship between two nodes. This term has been replaced in FANTOM 3.0 with the term *Edge*.

LMM

(U) Local MaxMind

MIME

(U) Multipurpose Internet Mail Extensions (MIME) data is a protocol developed and adopted by the Internet Engineering Task Force (IETF) that permits the transmission of mixed media messages on the Internet. The MIME standard defines how transmitted email messages can contain images, file attachments, headers identifying message routing and other information, and foreign language text.

Modes

(U) Before FANTOM 3.0, the application was *modal*, requiring you to click a button to indicate the kind of action you wanted to perform in the 3D Viewer window. In FANTOM 3.0, modes have been replaced with accelerator keys as shown in the following table.

Table B-1: 3D Viewer window modes replaced by accelerator keys

FANTOM 2.8.x Modes	FANTOM 3.0 Accelerator Keys
Node Select	Press SHIFT and drag to select nodes
Node Movement	Press ALT and drag to move selected nodes
View Movement	Hold down the middle scroll wheel on the mouse while dragging to move the view
Edge Select	Unused; no longer available
Zoom	Roll the middle scroll wheel on the mouse up to zoom in and down to zoom out

Multi-Edge

(U) In FANTOM 3.0, the term *multi-edge* has been introduced to define more than one connection or relationship between two nodes. Multi-edges are shown in the 3D Viewer window as a single line. The term multi-edge replaces the term *Edge* which now indicates a single connection.

Neighbors

(U) A neighbor is any connecting node, including parents and children.

Node

(U) A node is an object or entity, such as a financial transaction, IP address or email account.

One Hop

(U) One hop is a common term for a direct connection (A sends a message to B, D, and C). See Two Hops.

Parents

(U) A parent is a node at the remote end of an in-directed edge from a given node. For example, if the graph represents communications, then a parent node of node A is one that sends a communication to node A.

PCAP file

(U) PCAP (Packet Capture Data) files are created by network analyzer software, such as Wireshark

PNG file

(U) PNG (Portable Network Graphics) is a compressed bitmap image file format widely used on the Internet and intranets.

Range Axis

(U) The vertical axis in the Report Service chart.

Relational database

(U) A relational database in which all data are represented in tabular form. The description of a particular entity is provided by the set of its attribute values, stored as one row or record in a table. The relational approach supports queries that involve several tables by providing automatic edges across tables. Complete information can be obtained by joining the tables. Definition from: *Encyclopedia Britannica*. In FANTOM, the Controller window provides the Node Table, Edge Table, Multi-Edge Table and Filters Table, while the 3D Viewer window "joins" all this information in graphical form.

Seed

(U) A value, such as an account or facility, that you search for in a database. A node you select before running an analytic, layout, or report.

SMS

(U) Short Message Service. Short messages transmitted to and from mobile telephones.

Task

(U) In FANTOM, a task is a command you choose such as importing data or running an analytic, layout, or report. FANTOM lets you watch the progress of tasks by viewing the Task Monitor.

Template

(U) In FANTOM, templates you create "map" columns of data from the source file to the Controller window table. These templates also let you specify other presentational information, such as the classification of the data set, how many rows are used for the table headings and how many should be ignored, what character is used in the source file as a separator character (often a comma), and so on.

Two Hops

(U) Two hops is a common term for an indirect connection (A sends a message to B who in turn sends a message to C and D; A is two hops from C and D). See One Hop.

Visual analysis

(U) The science of analytical reasoning facilitated by interactive visual interfaces. It is a unique blend of human computer interaction, analytical reasoning, cognitive science, high-performance computing, and computer graphics. It lets you expose meaningful patterns and identify hidden relationships in any structured data set. Revealing these relationships helps you find answers to questions about your case data.

Java Regular Expressions

(U) This appendix provides details about Java Regular Expressions, which you can enter to select records based on patterns in the Filter dialog box.

Java Regular Expression Patterns

(U) A regular expression is notation for specifying a set of strings, e.g., the set of all valid email addresses or the set of all binary strings with an even number of 1s. Since the set might contain infinitely many members, we can't simply enumerate them. There are five basic operations for creating regular expressions, and the table below illustrates them by example.

Table 1: (U) Five Basic Operations for Creating Regular Expressions

Operation	Regular Expression	Yes	No
Concatenation	aabaab	aabaab	every other string
Logical OR (Alternation)	aa | baab	aa baab	every other string
Replication (Kleene closure)	ab*a	aa aba abba	e ab ababa
Grouping	a(a|b)aab	aaaab abaab	every other string
Wildcard	a..a	abba abaa	aa aaaaa

- (U) **Concatenation** – the simplest type of regular expression is formed by concatenating a bunch of symbols together, one after the other, like aabaab. This regular expression matches only the single string aabaab.

- (U) **Logical OR** – the logical OR operator enables us to choose from one of several possibilities. For example, the regular expression aa | baab matches exactly two strings aa and baab.
- (U) **Replication** – the replication operator enables us to specify infinitely many possibilities. For example, the regular expression ab*a matches aa, aba, abba, abbba, an so forth. Note that 0 replications of b are permitted.
- (U) **Grouping** – the grouping operator enables us to specify precedence to the various operators. The replication operator has the highest precedence, then concatenation, then logical OR. If we want to specify the set of strings a, aba, ababa, abababa, and so forth, we must write (ab)*a to indicate that the ab pattern must be replicated together.
- (U) **Wildcard** – the wildcard symbol matches exactly one occurrence of any single character.

Note: (U) You must use quotation marks to delimit the pattern, since otherwise the operating system would interpret the | and * symbols before passing along the string.

Table 2: (U) *Additional Operations for Creating Regular Expressions*

Operation	Java Regular Expression	Yes	No
One or more	a(bc)+de	abcde abcbcde	ade abc
Once or not at all	a(bc)?de	ade abcde	abc abcbcde
Character classes	[a-m]*	blackmail imbecile	above below
Negation of character classes	[^aeiou]	b c	a e
Exactly N times	[^aeiou]{6}	rhythm syzygy	rhythms allowed
Between M and N times	[a-z]{4,6}	spider tiger	jellyfish cow
Whitespace characters	[a-z\s]*hello	hello say hello	Othello 2hello

(U) This topic is extracted from Section 7.2, "Regular Expressions" in *Introduction to Programming in Java* (http://introcs.cs/princeton.edu/java/70theory) Copyright © 2002–2012 Robert Sedgewick and Kevin Wayne. All rights reserved.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

FANTOM Hot Keys Quick Reference Card

C	Select children of selected nodes
D	Deselect all nodes and edges
F	Filter selected nodes
L	Toggle labels on/off for selected nodes
N	Select neighbors of selected nodes
P	Select parents of selected nodes
R	Reset graph orientation to Home view
T	Re-center on graph
SHIFT	Node Select
CTRL	Selected Node Movement
ESCAPE	Deselect All
CTRL+F	Find text in Controller window
Ctrl+Z	Undo last action

Display Shortcut menu

View Movement

Pan graph to move it along 2D XY plane.

CTRL+ALT and drag on touchpad or with left Mouse button to rotate graph.

Drag while middle scroll wheel is held down to rotate graph

Scroll up and down to zoom in and out on graph

Node Select

SHIFT+click to select a node you are pointing at

SHIFT+drag to select nodes inside a bounding box

Alt+click to deselect selected node you point at

Node Movement

Drag with middle scroll wheel is held down to rotate selected nodes

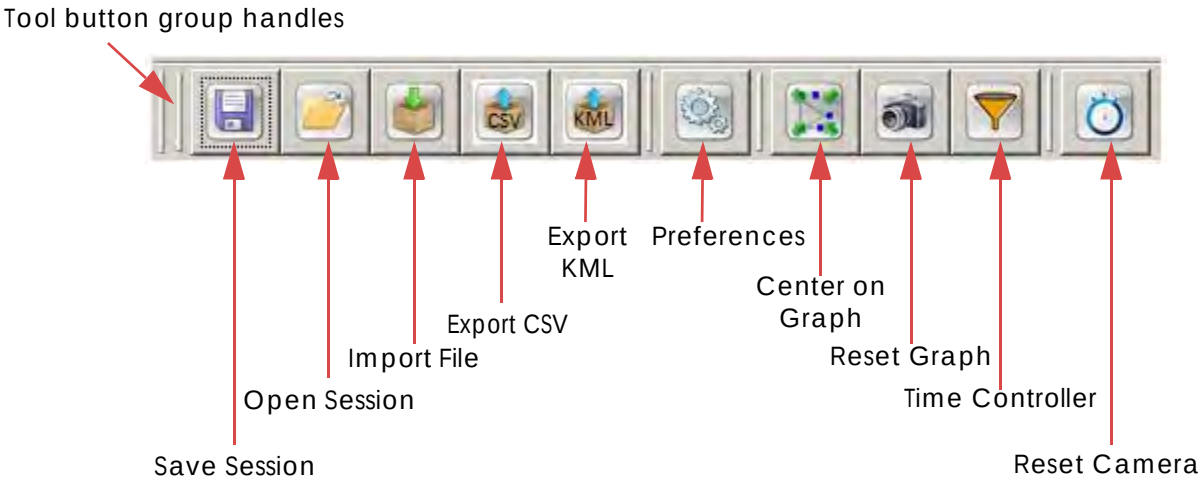
CTRL+drag to move selected nodes

Zoom

Scroll in to zoom in

ALT+scroll to zoom selected nodes in and out

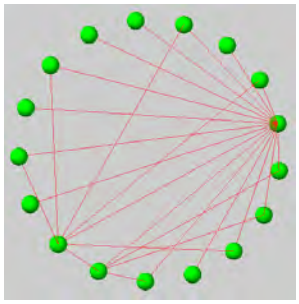
Scroll out to zoom out


Tool button group handles
CSV
KML
Export KML
Preferences
Center on Graph
Export CSV
Import File
Reset Graph
Time Controller
Open Session
Save Session
Reset Camera

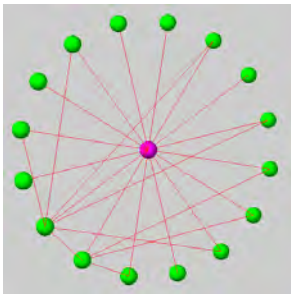
FANTOM Layouts Quick Reference Card

Circle Layout

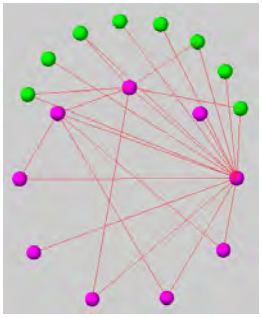
Displays nodes in a circle. Sometimes with a large graph, nodes may overlap or stack. What you select before running this layout affects results.



No nodes selected



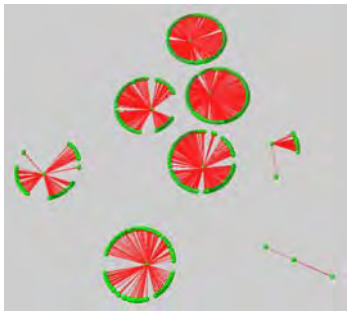
One node selected



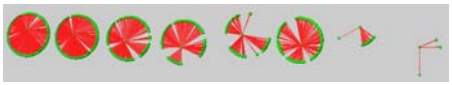
Multiple nodes selected

Disperser Layouts (Random and Sort)

Pushes disconnected nodes outward in a single layer. Nodes remaining in the center have the most connections. *Sort Disperser* spreads disconnected nodes sorting them left to right from largest to smallest. Random Disperser is faster, but uses more space.



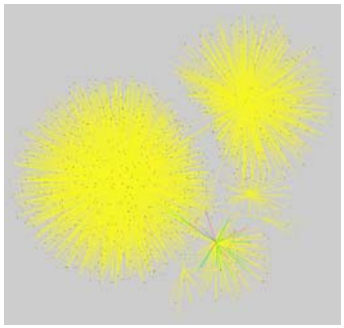
Random Disperser



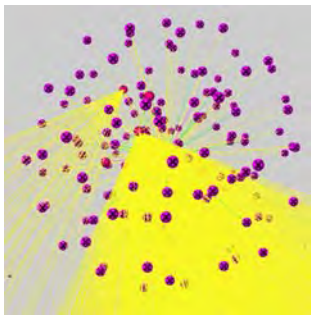
Sort Disperser

Magnetic Attraction, Repulsion: Force Directed Layout

Connected nodes *attract*, or *pull*, toward each other. Unconnected nodes *repel*, or push away from each other. Strongly connected nodes are closest, weakly connected nodes are less close, and unconnected nodes are farthest apart. Selected nodes affect results:



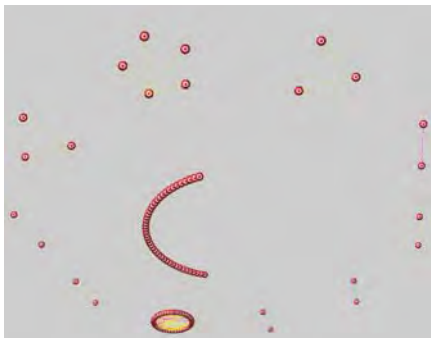
No nodes



Multiple nodes (Fruchterman Reingold force model)

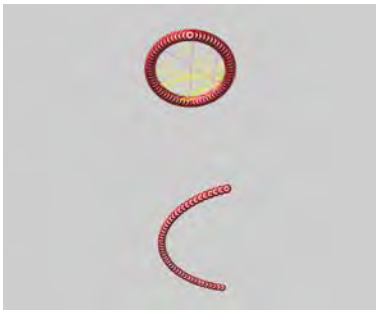
Link Cluster Layout

Link Cluster layout identifies communities by grouping nodes with shared edges.



Maximum Distance

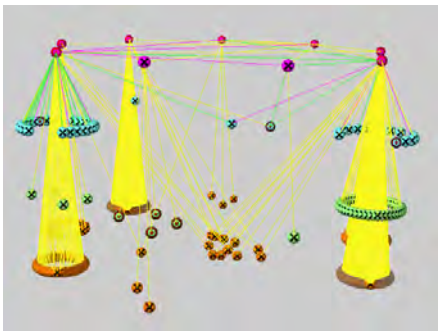
K Clusters

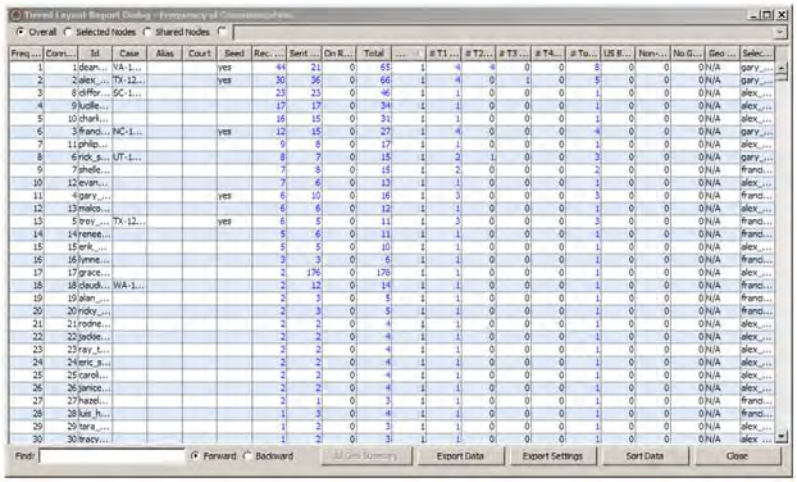


Cluster Density

Tiered Layout

Tiered Layout identifies To, From, and To/From communications for selected nodes and displays results in a chart and table.



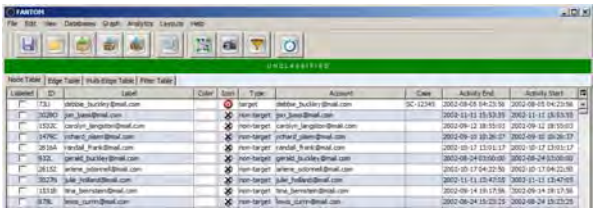


*Tiered Layout with default settings accepted including **Generate Report** and **Color Nodes** selected*

FANTOM Analytics Quick Reference Card

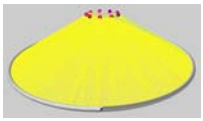
Activity Date Range Analytic

FANTOM adds an Activity Start and Activity End column to the Node Table. It determines the values by finding all the specified dates in the Edge table for the Source of each connection and then entering the first and last date in the corresponding column.



Bridges: Articulation Points Analytic

Articulation points are nodes that are like *bridges* between clusters of nodes. If you filter out these nodes, FANTOM would break the graph into multiple, independent clusters.



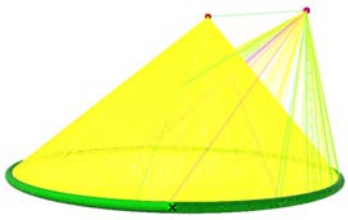
Articulation points at top

Filter articulation points

Edge Table is empty and Random Disperser shows no edges; all connections go through these articulation points

Busiest Intersections: Betweenness Analytic

Nodes with the highest betweenness centrality (the red nodes) and next highest betweenness (the yellow nodes) are the *busiest intersections*. That is, "all paths lead through" the nodes with the highest Betweenness scores.



Find Email Flows: Call Chaining Analytic

Analyzes communications data for directly-linked graph events. In the case of call chain events, the domain is defined as linked communications (edges) occurring between entities (nodes) within a predetermined time frame.

Click the Plus/Minus toggle buttons top open/close folders

Highlight Interesting Properties: Colorizer Analytic

The Colorizer Analytic lets you color, select, or deselect nodes or edges based on their attributes. Its value is in highlighting nodes or edges that have interesting properties.

Add Rules defining colors or selections by attribute for nodes or edges

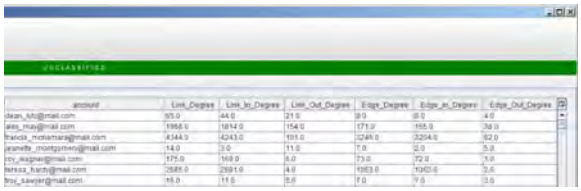
Nodes in this phone data set are colored by Case ID

Date Attribute Aggregation

Creates a Date/Time column from separate Date and Time columns.

Count Inbound, Outbound: Degree Analytic

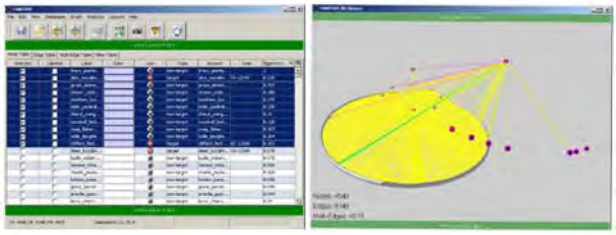
Computes the number of connections between nodes in a variety of ways. Can count both multi-edges and edges, and can count incoming, outgoing, and total edges and multi-edges for each node.



Select the edges and multi-edges to count, FANTOM adds a column for each one

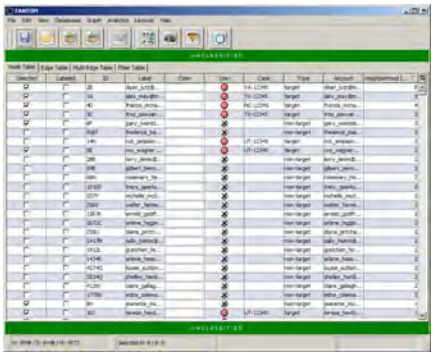
Eigenvector Centrality Analytic

Identifies nodes that are close to everyone else in graph. Eigenvector Centrality is the measure of the importance of a node. It adds a column to the Node Table that populates each cell with a value between zero and one (a percentage, with one being the highest).



Birds of a Feather: Neighborhood Index Analytic

Useful when trying to determine which nodes are strongly connected to the selected nodes (often the target set). It does this by counting (for every node) how many of the target set are directly connected.



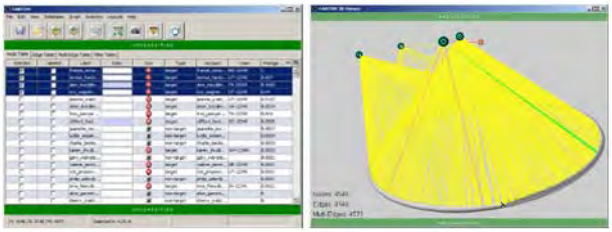
Select at least one node, FANTOM calculates the Neighborhood Index value for nodes

Non-Target Communication Analysis Analytic

Explains why non-targets are in the graph. It produces a simple table containing non-targets who communicated with the target. The table displays the date range within which communications took place.

Prestige Centrality

Identifies popular nodes based on relationship directions. It adds a column to the Node Table, populating each cell with a percentage between zero and one (the highest Prestige). Prestige indicates power within a group; for example, by a node who communicates only once before an event is triggered or by a node who communicates the most.



Reciprocated Links Analytic

Finds strong, two-way links.

Similarities & Differences: Related Nodes Analytic

Formerly called Alias Detection. Compares all nodes to a selected set of nodes. Determines similarity based on comparison of node properties: 1) the number of shared neighbors and 2) similarity of name/label. Shared neighbors is calculated by counting the number of nodes directly connecting a given node to the selected set (shared friends). Name similarity is calculated by longest common substring (how many characters in the two names match in a row), and edit distance (the number of keystrokes needed to change one name into another).

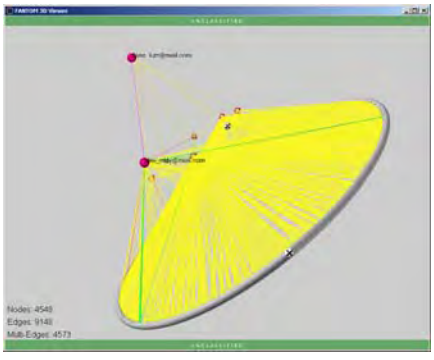
Case	Type	Account	Articulation Point	Neighborhood Similarity	Longest Common String	String Edit Distance	Alias Mean
	non-target	aaron_brandon@mail.com		1	1	1	1
	non-target	greg_brandon@mail.com		1	0.772727	0.818182	0.863636
	non-target	betsy_brandon@mail.com		1	0.772727	0.772727	0.848485
	non-target	albert_brandon@mail.com		1	0.73913	0.782609	0.84058
	non-target	ronald_brandon@mail.com		1	0.73913	0.782609	0.84058
	non-target	dorothy_brandon@mail.com		1	0.708333	0.791667	0.833333
	non-target	thomas_brandon@mail.com		1	0.73913	0.73913	0.826087
	non-target	shannon_herndon@mail.com		1	0.541667	0.708333	0.75
	non-target	ron_brandt@mail.com		1	0.409091	0.818182	0.742424
	non-target	carol_burton@mail.com		1	0.5	0.727273	0.742424
	non-target	terry_blanton@mail.com		1	0.5	0.727273	0.742424

Social Network Analytic

The Social Network analytic is the study of graphs of people.

Who's in the Middle?: Source to Destination Path Analytic

Finds the shortest path between a source and destination node. You can type the first characters of the source and target node labels and FANTOM will display an auto-complete menu showing the closest match to your entry.



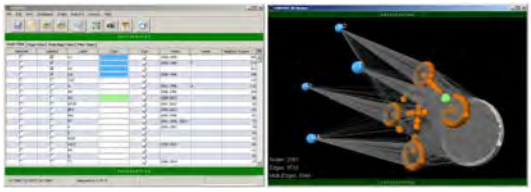
Specify source and destination node IDs, FANTOM adds a Shortest Path column with nodes numbered sequentially

FANTOM Reports Quick Reference Card

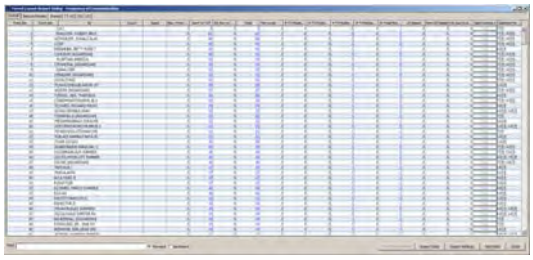
Tiered Layout Reports

Select "seed" nodes to be the starting point for the Tiered Layout. You might select a few nodes with the highest Neighbor Degree.

1. Choose **Analytics** > **Degree**, select **Neighbor Degree,** click **OK**.
2. Click the **Neighbor Degree** column title twice to sort highest to lowest, and then select a few rows with the highest degree values.
3. Run Tiered Layout with **Generate Report** selected.



Controller window 3D Graph Viewer window



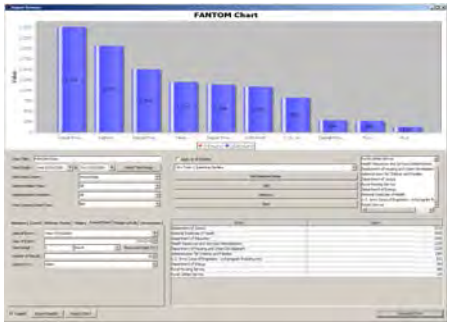
Tiered Report window: Find, Sort, or Export data for Overall, Selected Nodes, Shared, or Seed Node Tables

Report Service Overview

All Report Services results can be exported. Standard options include defining the Chart Title, Time Range, Column to use for Time, Communication Type and Direction (Inbound/Outbound), and Graph Types. Produce reports for all or selected entities.

Around Event

The Date of an event, time of an event, and number of results helps you find who is the most active and interesting.



Attribute Lookup

The Attribute Lookup report looks up attribute values and then plots them into a chart. It only works with number values and dates and plots them into a visual chart.

Attribute Tracker

Horizontal X-axis – Displays selected node or edge attribute. Email addresses, IP addresses, locations like City or Country, and Targets are good attribute choices. Edge attributes work best.

Vertical Y-axis – Displays selected number of entities: one, multiple, or all *entities* (Node ID) across specified Time Range. Selecting fewer entities makes it easier to gain insight. If you discover email addresses with identical geo-locations and send dates, try merging those nodes.

Conversation

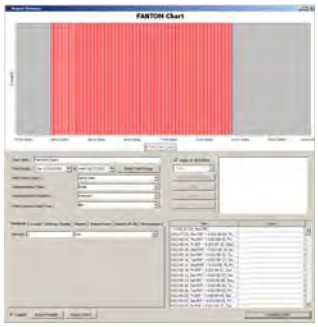
Tracks a subset of a clique or group. Zoom in to see the count for each entity in the bars. Helps you narrow a search or find someone you didn't know about before. You can get the same benefits using Filters; however, the this report is easier to use than the Edge table.

Counts

Proportional chart shows relative sizes of values in the selected attribute in comparison to one another and to the whole data set.

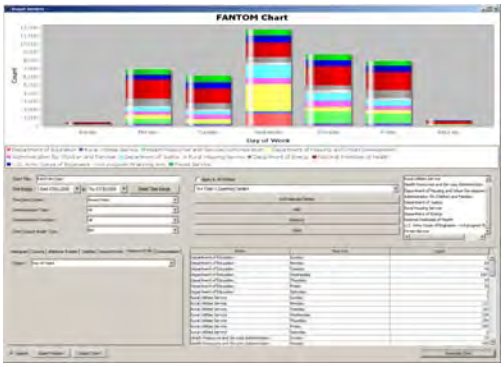
Histogram

Bar widths are proportional to duration of date data in selected date range. Select Bin Size from a number of Seconds to Years.



Pattern of Life

Examine patterns of communication behavior for selected entities across specified time period. A good way to use this report is with data sets that have email addresses as node IDs. If multiple addresses have the same pattern, it may suggest the same person is using all of these addresses.



Scatter Plot

The Scatter Plot report is a graph that plots two along two axes to show the relationship between the two. Scatter plots are useful for illustrating a trend.

Timeline

Customize this report by adding or removing one or more sets of node criteria to show along the timeline. In addition to standard options, select a Time Unit (Seconds to Years).

FANTOM Hot Keys Quick Reference Card

C	Select children of selected nodes
D	Deselect all nodes and edges
F	Filter selected nodes
L	Toggle labels on/off for selected nodes
N	Select neighbors of selected nodes
P	Select parents of selected nodes
R	Reset graph orientation to Home view
T	Re-center on graph
SHIFT	Node Select
CTRL	Selected Node Movement
ESCAPE	Deselect All
CTRL+F	Find text in Controller window
Ctrl+Z	Undo last action

Display Shortcut menu

View Movement

Pan graph to move it along 2D XY plane.

CTRL+ALT and drag on touchpad or with left Mouse button to rotate graph.

Drag while middle scroll wheel is held down to rotate graph

Scroll up and down to zoom in and out on graph

Node Select

SHIFT+click to select a node you are pointing at

SHIFT+drag to select nodes inside a bounding box

Alt+click to deselect selected node you point at

Node Movement

Drag with middle scroll wheel is held down to rotate selected nodes

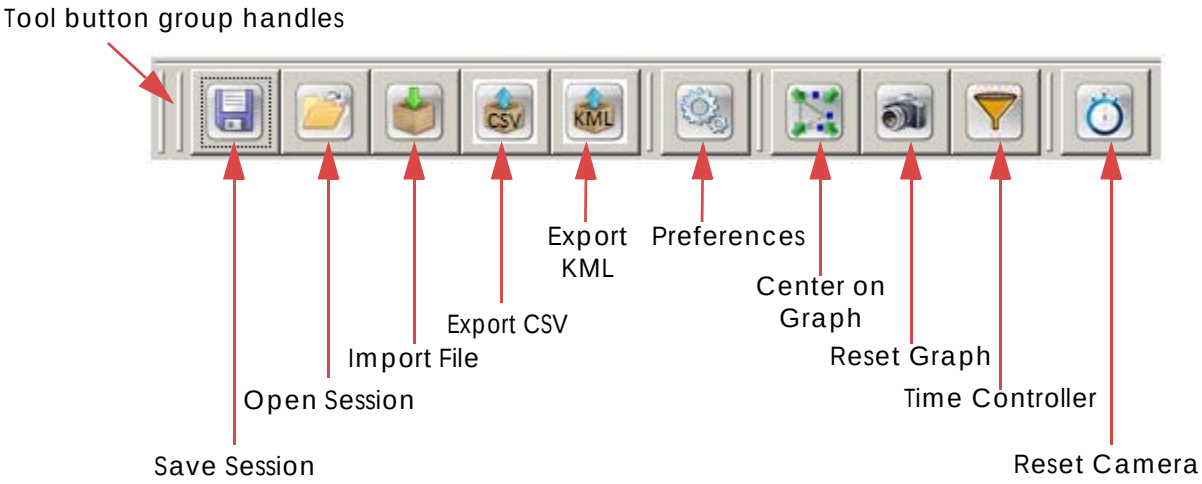
CTRL+drag to move selected nodes

Zoom

Scroll in to zoom in

ALT+scroll to zoom selected nodes in and out

Scroll out to zoom out


Tool button group handles
CSV
KML
Export KML
Preferences
Center on Graph
Reset Graph
Time Controller
Export CSV
Import File
Open Session
Save Session
Reset Camera