



NetWitness Investigator User Guide

for RSA NetWitness® Platform 11.4



Copyright © 1994-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

February 2020

Contents

| | |
|---|-----------|
| Introduction | 6 |
| Related Documentation | 6 |
| Contacting RSA Customer Support | 6 |
| Preparing to Contact RSA Customer Support | 6 |
| Overview | 7 |
| System Requirements | 7 |
| Install NetWitness Investigator | 7 |
| Uninstall Investigator | 10 |
| Activate Investigator | 10 |
| Activate NetWitness Investigator for Enterprise Use | 11 |
| Activate NetWitness Investigator for Freeware Use | 12 |
| Enable Windows 10 and High DPI Displays | 15 |
| Investigator Basics | 16 |
| About Parsers | 17 |
| Lua Parsers | 17 |
| Investigator Concepts | 17 |
| About the Investigator Menus | 18 |
| Collection Menu | 19 |
| Edit Menu | 20 |
| View Menu | 21 |
| Bookmarks Menu | 22 |
| History Menu | 22 |
| Help Menu | 22 |
| Collection Navigation | 22 |
| Navigation View | 23 |
| Navigation Toolbar | 23 |
| Navigate Multiple Views | 24 |
| Content Pane Display Options | 25 |
| Session List View | 26 |
| Session List Toolbar | 26 |
| Content View | 27 |
| Content Toolbar | 27 |
| Getting Started | 28 |
| Configure Investigator | 29 |
| General | 30 |

| | |
|--------------------------------------|-----------|
| Display | 31 |
| Theme | 31 |
| Session View Options | 32 |
| Content View Options | 32 |
| Reports | 33 |
| Capture | 34 |
| Process | 34 |
| Audio Codecs | 35 |
| Advanced | 36 |
| Collection Management | 38 |
| Accessing Data | 38 |
| Collection Configuration | 38 |
| Collection Level | 38 |
| Investigator Toolbar | 39 |
| Create a New Collection | 40 |
| Configure the New Collection | 40 |
| Import a Data File | 41 |
| Reprocess a Collection | 41 |
| Data Capture | 45 |
| Custom and Specialized Parsers | 45 |
| Configure Parsers | 46 |
| NetWitness Live | 47 |
| Preview Content | 49 |
| Rules Overview | 50 |
| Network Layer Rules | 51 |
| Capture Configuration | 58 |
| Capture Configuration Settings | 59 |
| Network Adapter | 59 |
| Advanced Capture Settings | 59 |
| Evidence Handling | 59 |
| Real-Time Network Capture | 60 |
| Start/Stop the Live Capture | 60 |
| Data Analysis | 62 |
| Views | 62 |
| Summary View | 62 |
| Navigation View | 63 |
| Navigation Toolbar | 65 |
| View Logs | 71 |
| Context Menus | 73 |
| Navigation Context Menu | 74 |

| | |
|--|-----------|
| Drills and Filters | 75 |
| Create a New Tab | 75 |
| View Sessions | 76 |
| Session View | 77 |
| Session List Toolbar | 78 |
| More Context Menus | 79 |
| Display Sessions on Google Earth | 80 |
| Content View | 81 |
| Content Toolbar | 81 |
| Search View | 82 |
| Quick Search | 82 |
| Simple Search | 83 |
| Search Preferences | 84 |
| Advanced Search | 84 |
| Search Results | 86 |
| Session List View | 86 |
| Content View | 87 |
| NetWitness Search Tips | 88 |
| Rules | 89 |
| Packet Data Options | 89 |
| Session Options | 89 |
| Rule Order | 90 |
| Rule Sets and Expressions | 90 |
| Rule Syntax | 90 |
| Supported Fields | 91 |
| Reference Documents | 92 |
| About Lua Parsers | 93 |
| SDK Data Types | 94 |
| Supported Fields | 94 |

Introduction

The *NetWitness Investigator User Guide* provides information about performing the analysis of the data captured from your network or from other collection sources using the Investigator application. To use this dynamic tool effectively, basic strategies are presented to illustrate the possible approaches. There are no absolutes. The user must become familiar with the capabilities of the application in order to effectively evaluate potential threats to your network.

This guide applies to releases beginning with the version 9.0 series. There will be periodic updates made to the content.

Anyone using this guide should possess experience as a network engineer, equivalent to at least that of a journeyman, and also have a strong understanding of network concepts and TCP/IP communications.

Related Documentation

The following document is also available:

NetWitness Platform Online Documentation: The documents on this site provide information about the setup, configuration and management of RSA NetWitness Platform. They are available at <https://community.rsa.com/community/products/netwitness/documentation/overview>.

Contacting RSA Customer Support

If you have questions or any issues with this product, contact Customer Support for assistance at <https://community.rsa.com/docs/DOC-1294>.

Preparing to Contact RSA Customer Support

When you contact RSA Customer Support, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness or Security Analytics product or application you are using.
- The type of hardware you are using.

Overview

RSA NetWitness Platform provides a group of products to capture all network traffic and use the same data to solve a broad range of business and security problems.

- **Decoder**—an appliance-based network capture device that fully reassembles and normalizes traffic at every layer for full session analysis. This enables users to collect, filter, and analyze full network traffic by multiple dimensions.
- **Concentrator**—a network appliance that consolidates multiple Decoders to create single logical views for analysis. This enables users to instantly analyze network and application layer detail across multiple capture locations, including full content.
- **Broker** —a NetWitness Platform application that brokers and distributes queries across multiple Concentrators (concentration points) to provide a single view across an entire network
- **Investigator** —a NetWitness Platform client application that provides the capability to process pre-existing data or to capture live data from a network interface and perform analysis on data collected by either of the two capture methods. The Enterprise version can connect to any NetWitness NextGen service and perform investigations.
- **NwConsole**—a command-line interface (CLI) program accessed through the Windows Command Shell or the Secure Socket Shell (SSH). This tool can perform many tasks related to NextGen services, including connecting to them remotely and performing Administrative tasks. Since it is a CLI, you can also use it for scripting tasks.

System Requirements

Investigator requires a minimum of Windows 7 x64. 32 bit operating systems are not supported.

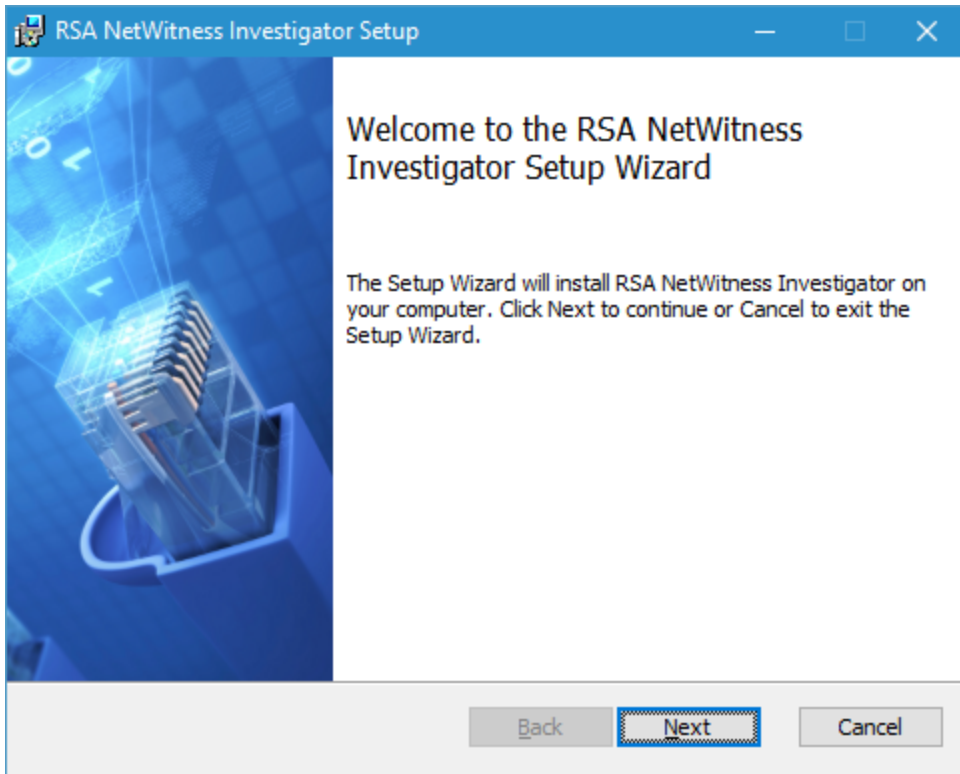
Install NetWitness Investigator

Note: Current users must close any open version of Investigator before proceeding with the installation of a newer version or updating an existing one.

The installation of NetWitness Investigator must be performed on the Windows 64-bit platform. The necessary files are included in the installer package, which is available from <https://community.rsa.com/community/products/netwitness/investigator>.

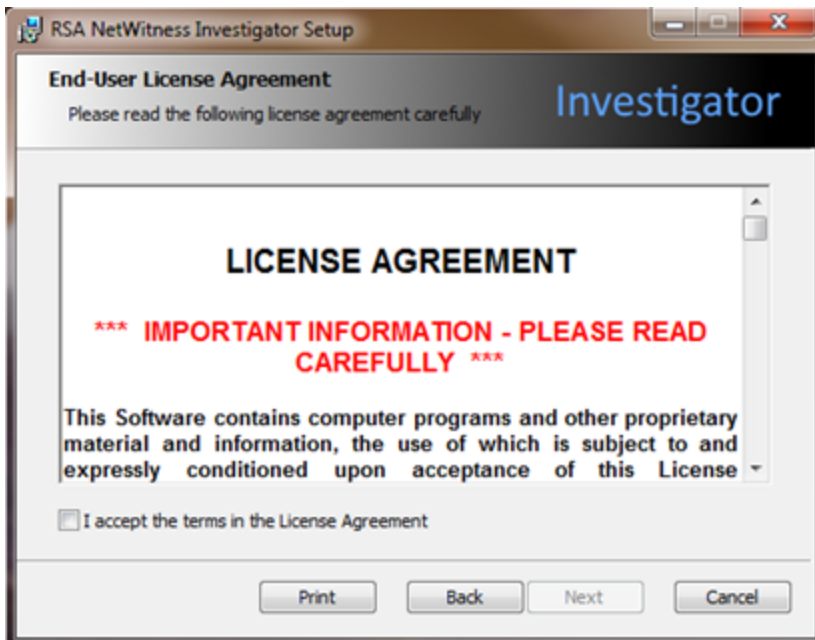
Note: You must have an Internet connection to install and activate the Freeware version of NetWitness Investigator. For the Enterprise version, you do not need an Internet connection for installation and activation. You can download the client, install the product and then connect to an existing internal network.

1. Double-click on the installation file (**.msi**).
The RSA Investigator Setup Wizard opens.



2. Click Next.

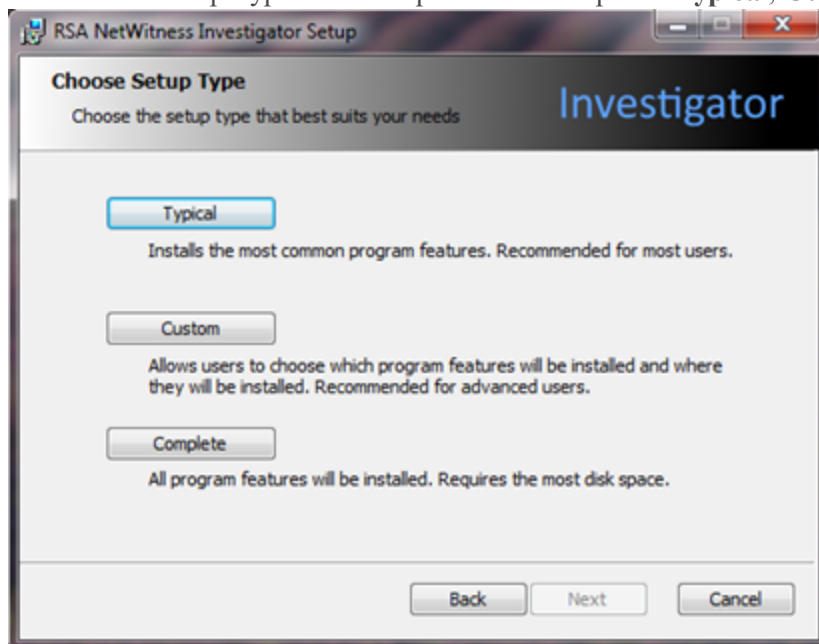
The License Agreement window opens.



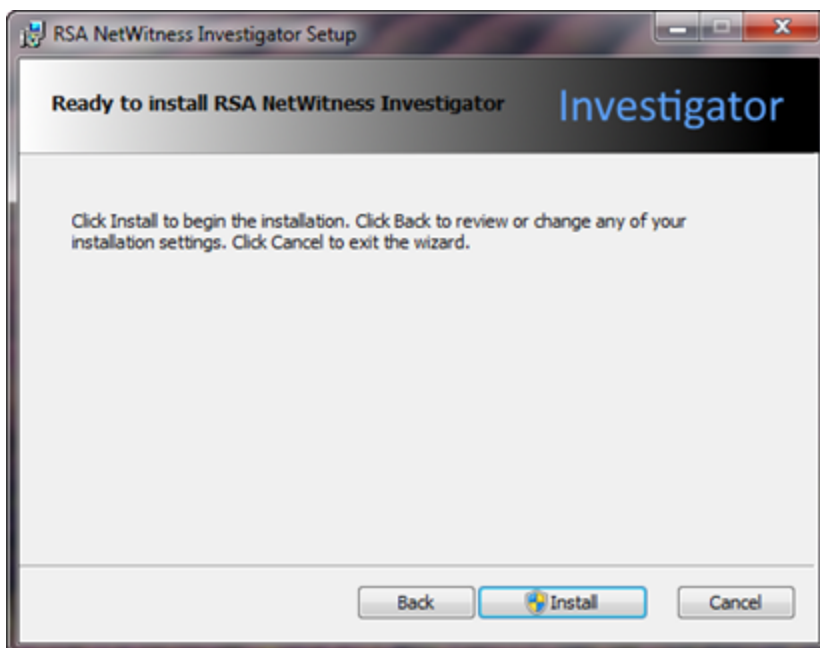
3. Select the I accept the terms in the License Agreement check box, and then click Next.

Note: Clicking I accept the terms in the License Agreement is a required step.

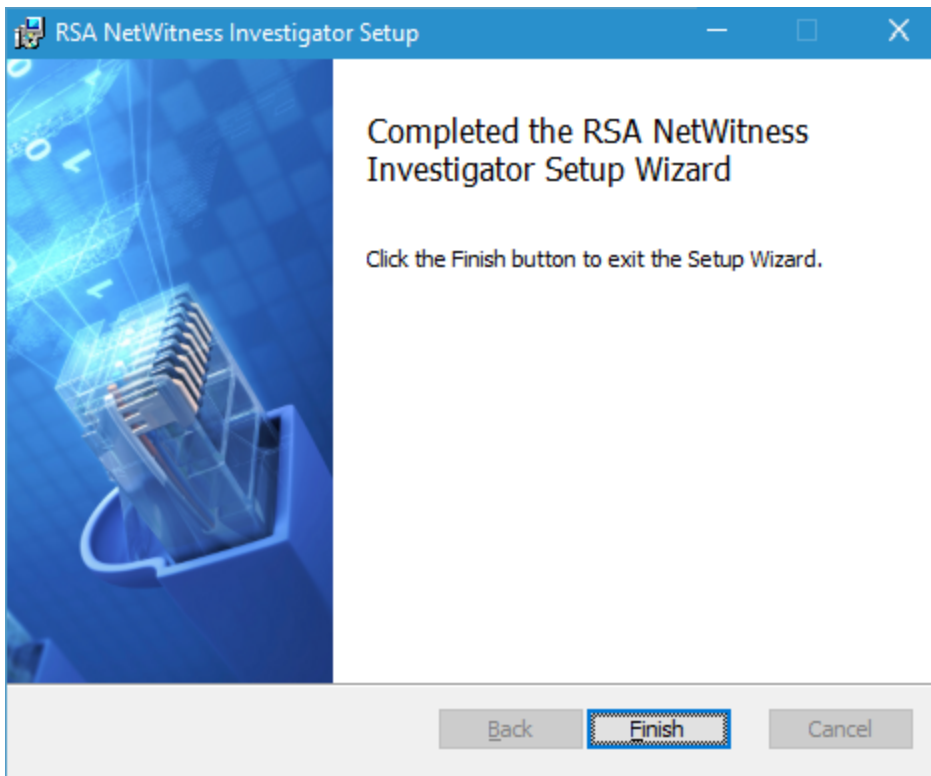
The Choose Setup Type window opens with the options **Typical**, **Custom**, and **Complete**



4. Click the option that is most appropriate (in this document, **Typical** is used), and then click **Next**. The Ready to install RSA NetWitness Investigator window opens.



5. Click **Install**.
A window opens that shows the progress of the installation.
6. When the installation process completes, the Completed the RSA NetWitness Investigator Setup Wizard window opens.



7. Click **Finish** to complete the installation.

Uninstall Investigator

1. Close all programs.
2. From the **Start** menu, click **Control Panel**.
3. Double-click the **Programs and Features** icon.
4. Highlight **NetWitness Investigator 10.6** from the list of installed applications, and then click **Remove**.
5. Follow the instructions.

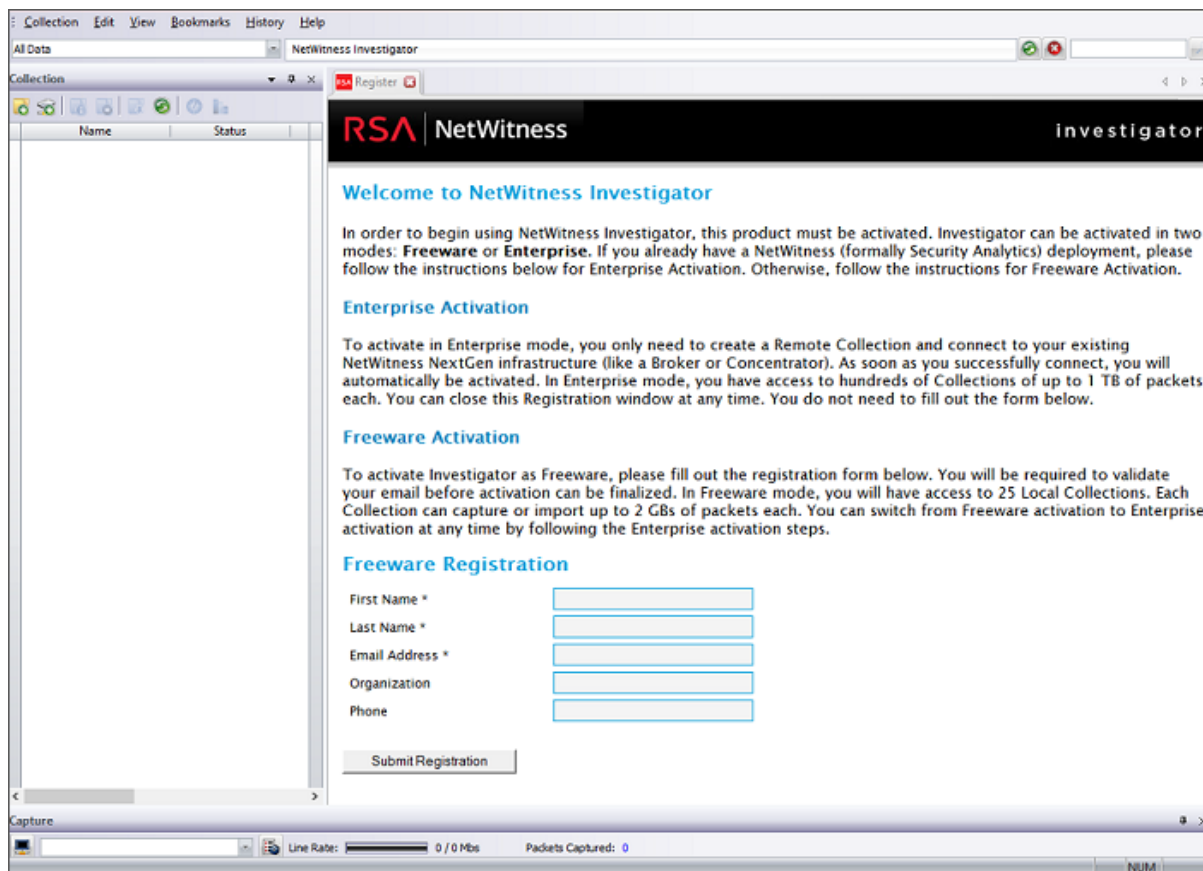
Activate Investigator

Note: If you want to capture packets to and from your local desktop, you must download and install the WinPcap library. A link to this download page is provided on the Welcome page after you activate NetWitness Investigator.

Activate NetWitness Investigator for Enterprise Use

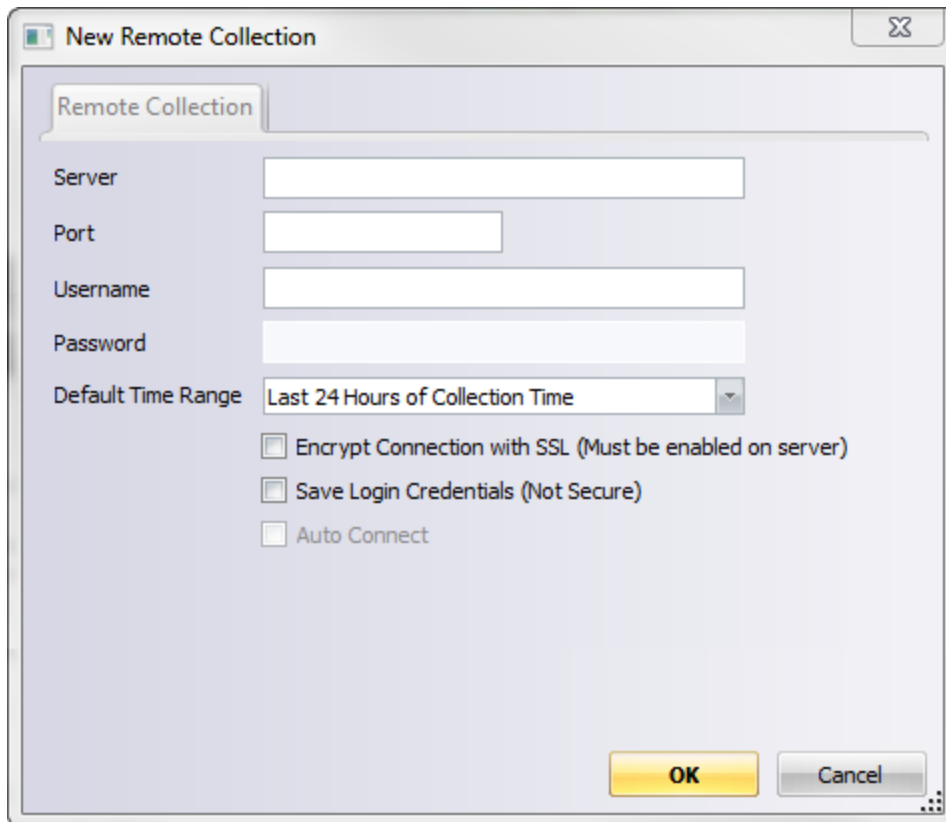
1. From the Start menu, open NetWitness Investigator.

The Welcome to NetWitness Investigator registration page is displayed.



2. In the menu bar, click **Connection > New Remote Collection**.

The New Remote Collection dialog is displayed.



3. Enter the server information for the Remote Collector system and click **OK**. The following message is displayed:

Congratulations, you have successfully activated the product for Enterprise use. You have a full license for all local and remote collections.

4. Click **OK**.

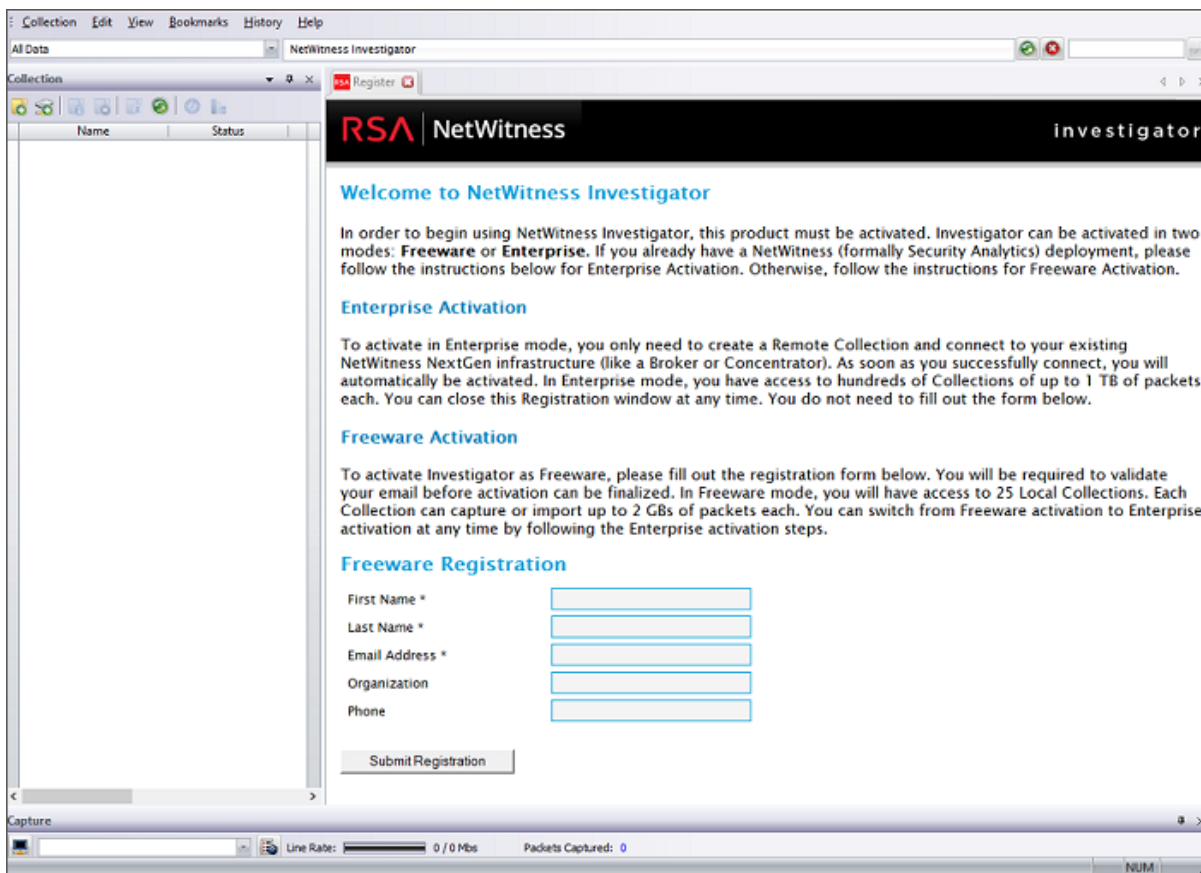
A message is displayed that asks if you would like to install a Demo Collection, which contains sample data that you can use to explore the features of Investigator.

5. To install the Demo Collection, click **Yes**.

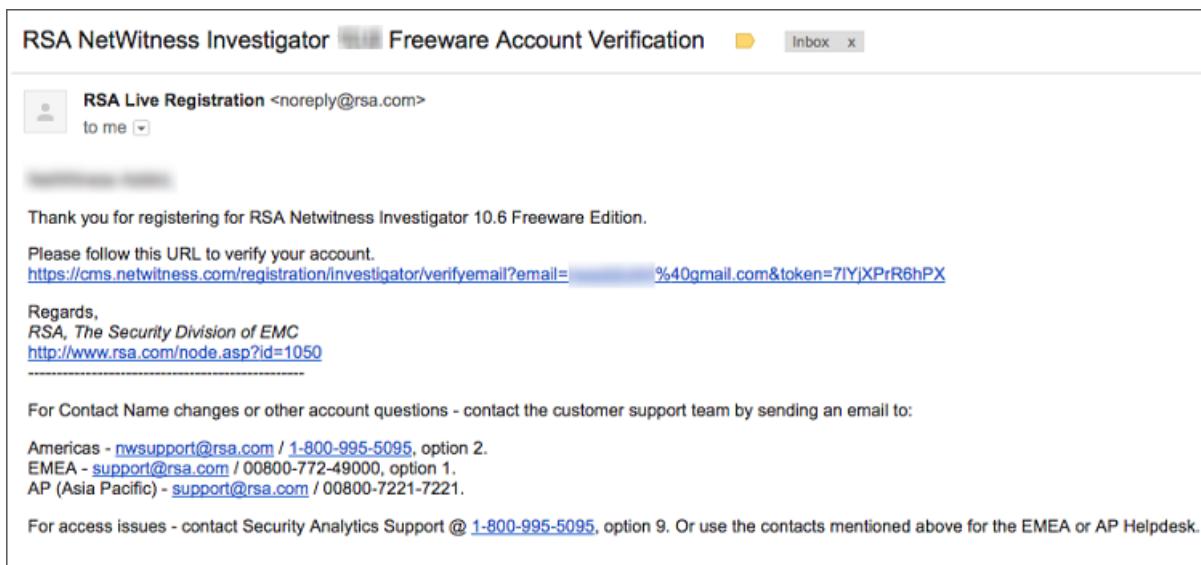
The NetWitness Investigator user interface is now activated and ready for use. You can use the sample data in the Demo Collection to learn more about NetWitness Investigator.

Activate NetWitness Investigator for Freeware Use

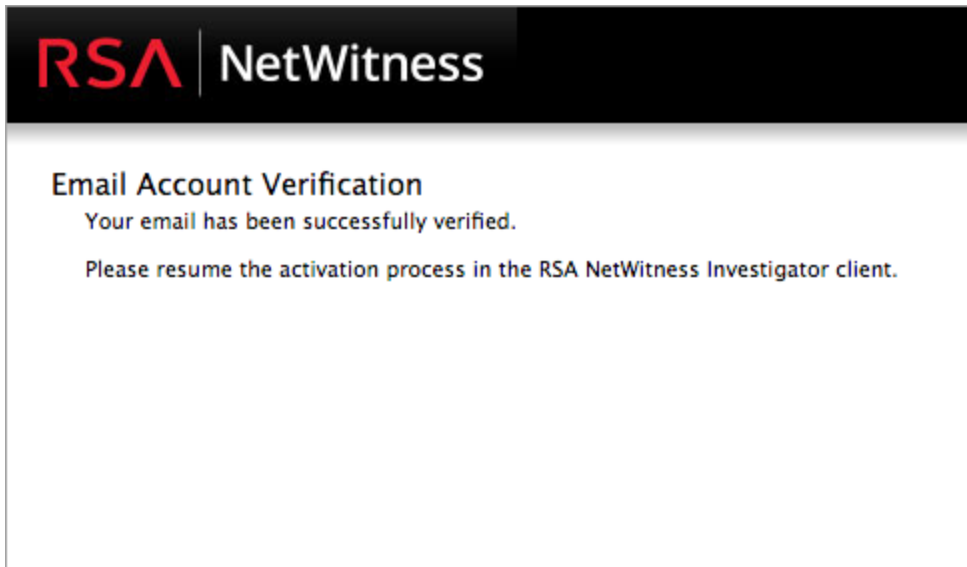
1. From the **Start** menu, open NetWitness Investigator. The Welcome to NetWitness Investigator registration page is displayed.



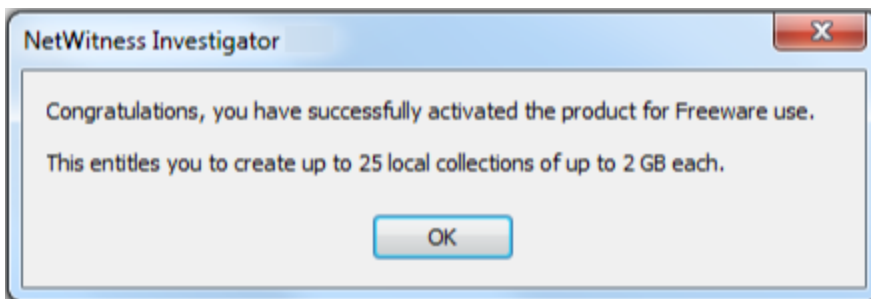
2. In the **Freeware Registration** section, complete the information. The fields with the stars (*) are required. Click **Submit Registration**.
3. You receive an email from RSA Live Registration asking you to click on a URL to verify your account. Click on the URL.



4. After your email address is validated, you receive confirmation similar to the following:

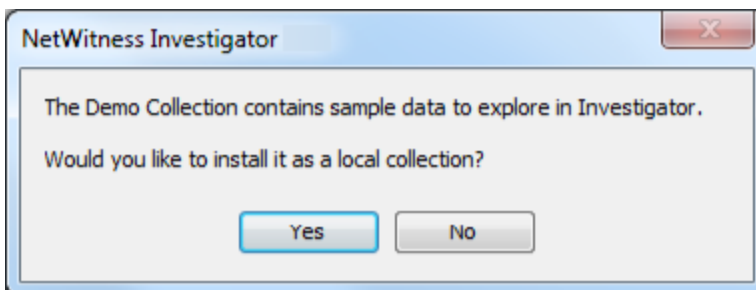


5. In NetWitness Investigator, the Email Validation Required dialog is displayed. Click **Activate Freeware**. The following message is displayed:



6. Click **OK**.

A message is displayed that asks if you would like to install a Demo Collection, which contains sample data that you can use to explore the features of Investigator.



7. To install the Demo Collection, click **Yes**.

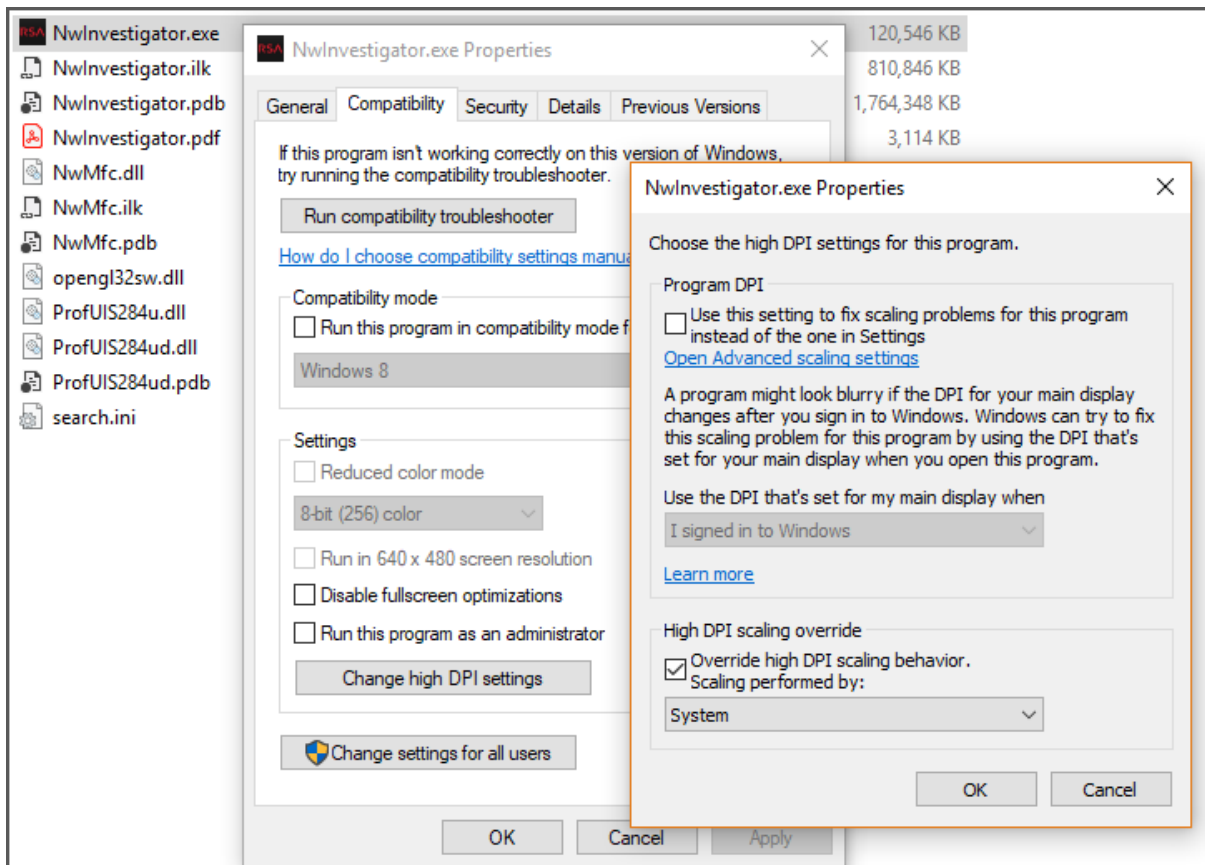
The NetWitness Investigator user interface is now activated and ready for use. You can use the sample data in the Demo Collection to learn more about NetWitness Investigator. For information that describes the user interface, see "Chapter 2: Investigator Basics" in the *Investigator User Guide*.

Enable Windows 10 and High DPI Displays

If you are using high-DPI displays, the newer versions of Windows 10 add support for DPI scaling of programs that use older graphics libraries. You can turn on this feature for Investigator so it looks and works correctly using a high DPI display.

To enable this feature:

1. Navigate to the install directory of Investigator (for example, C:\Program Files\RSA\NetWitness Investigator), right click on the Investigator.exe program file, and then click **Properties**.
2. Click on the **Compatibility** tab and click **Change high DPI settings**.
3. In the next dialog, under **High DPI scaling override**, select the **Override high DPI scaling behavior** check box, and then select **System** from the dropdown menu.
The following image shows these options:



4. Click **OK**.
Graphics performance may slow down slightly, but the application should look and behave normally now.

Investigator Basics

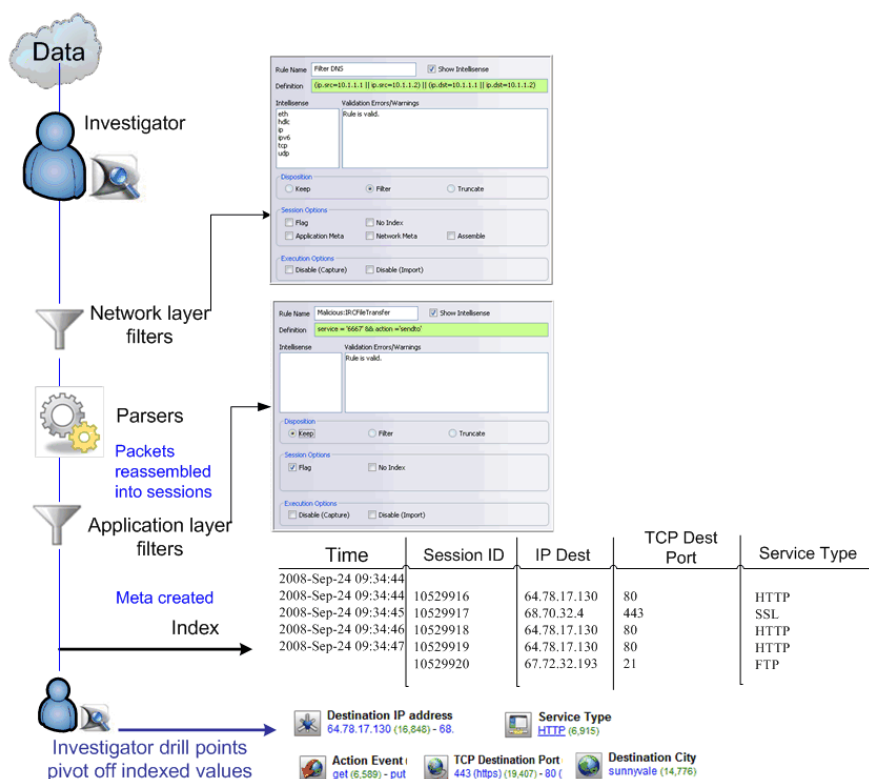
NetWitness is a security intelligence product that audits and monitors all traffic on a network. It creates a comprehensive log of all network activities and interprets the activities into a format that network engineers and non-engineers alike can quickly understand.

NetWitness INVESTIGATOR is the application you use to analyze the data captured from your network in order to identify possible internal or external threats to your security and IP infrastructure. You can import data from other collection sources or, if you have the Field Edition, perform live data capture.

You can capture directly from a local network interface or download a collection from a localhost or a remote service (such as a DECODER or CONCENTRATOR). Username/password are required to authenticate to the NetWitness Framework. You can encrypt the connection with SSL.

Application and Network rules are created for live capture collections as well as for imported collections. Users can customize these rules or disable them as needed (see *Rules Overview* in [Data Capture](#)).

NetWitness converts each protocol into a common language, so knowledge of protocols is no longer necessary. Performing analysis using INVESTIGATOR can be as simple as looking for user names, e-mails, applications, resources, actions, or computer names.



The user can keep several windows open, arrange them on the screen to facilitate comparison, or create tabs to view the content as the analysis progresses.

- [Investigator Concepts](#)
- [About the Investigator Menus](#)

- [Collection Navigation](#)
- [Navigate Multiple Views](#)

About Parsers

A parser is a set of instructions written to decode protocols. Currently, all new parsers are written in a language called Lua. The older XML Flex parsers are deprecated but still supported. However, Lua is more powerful and efficient.

Parsers are written to create meta values from decoded protocols so that the interesting parts of the protocol are easy to view and search on. For example, many parsers search for entities like hostnames, usernames, passwords, and IP addresses, and create meta keys for those values. This makes it easy to find all the sessions with the same values or to correlate them to other sessions via their meta values.

The metadata contains important information such as network and application events. All enabled parsers examine sessions and produce metadata. For example, in an FTP session, the FTP parser will produce metadata such as **login name**, **password**, and file operations including **get**, **put**, or **delete**.

Lua Parsers

There are a number of Lua parsers that are available from NetWitness Live. For information about Live, see the **Live Services Guide** in the RSA NetWitness Platform online Help on RSA Link (<https://community.rsa.com/>). For detailed information about how to work with Lua parsers, see the **Parsers Book** on RSA Link (<https://community.rsa.com/docs/DOC-41370>).

Investigator Concepts

Some of the concepts that pertain to using Investigator are briefly described in the following table.

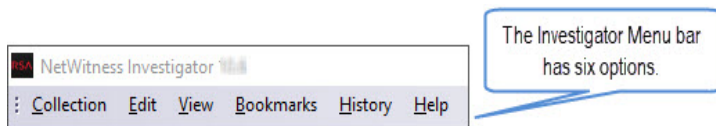
| Concept | Description |
|------------|---|
| Parser | A set of instructions written to decode protocols. Parsers are written to create meta values from decoded protocols so that the key parts of the protocol are easy to view and to search on. All enabled parsers examine sessions and produce metadata. The metadata contains important information such as network and application events. |
| Drill | <p>The action of clicking on a link to the next level of detail. A drill point refers to focusing the analytic view on a specific subset of a collection defined by a particular metadata element.</p> <p>For example, to focus analysis on sessions related to a specific IP address, the user can drill into that IP address to refocus the analytic view to only those sessions related to the selected IP address. Drilling will create a <i>breadcrumb</i> trail in the Navigation view that shows the user the path traversed to the current drill point.</p> |
| Collection | A collection is a logically related group of packets. It consists of one or more capture or remote device files. A collection can be created either by the live capture capability within NetWitness Investigator, by importing existing pcap files, or by connecting to another NetWitness appliance. |

| Concept | Description |
|--------------------|--|
| Collection Summary | A scalable high-level view of the characteristics (session count, session size, packet count) of a selected collection for a specific timeline. |
| Navigation View | The central mechanism for drilling into the extracted metadata. |
| Search View | The mechanism for locating individual sessions with specified string values or regular expressions. |
| Bookmark | Analogous to a web browser bookmark, NetWitness Investigator bookmarks let the user create a reference to a single session or a group of sessions. A single-click mechanism returns the user to the selected session(s). |
| Breadcrumb | Breadcrumbs are a way to maintain a path from the root of the collection to the current drill point. The user can click on any element within the breadcrumb to jump back to that point in the drill path. For example, if the user has drilled into service HTTP:size medium:protocol TCP:time 11 AM, clicking on size medium will jump the navigation window back to that drill point. |
| View | The relative position you are using to look at the captured data, in descending order: <ul style="list-style-type: none"> • Summary • Collection • Report • Session • Search • Content |
| Sessions | A group of related data packets. These packets are grouped into sessions based on the transactional nature of the communication, as in the client/service request and response. |
| Content | The actual information or object represented in the data capture. The content of a session consists of every packet captured for that session. Session content can be viewed by its content type (web, e-mail, IM, text, etc.). |
| Metadata | Specific data types (Service Type, Action Event, Source IP Address, etc.) used by the parsers to count and itemize in the captured data. A detailed list of metadata for each parser may be found in the NetWitness System Administrator Guide. |
| Index | Indexes are internal NetWitness data structures that organize the metadata elements of sessions and are generated during data processing for a collection. The content of the index, and consequently the metadata elements that are displayed in the Navigation view, are controlled by settings in effect during collection processing. Rebuilding a collection will regenerate the index. |

About the Investigator Menus

The menus for Investigator are:

- [Collection Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Bookmarks Menu](#)
- [History Menu](#)
- [Help Menu](#)



Each menu contains commands that perform specific functions inherent in Investigator procedures. While the menus are available on all screens in Investigator, some of the menu options are dependent upon the level where you are working. An option must appear highlighted for it to be available. If it is gray or dimmed, the option is not available.

Note: You should also be aware of the **right-click option** menus. There may be options available that are not represented by an icon on the toolbar for a particular view. For more information, see [Data Analysis](#).

Each menu lists commands that can be executed by clicking on the command or by using a shortcut key. An underlined character in a command, when pressed simultaneously with the CTRL key, serves as a shortcut key for that command. Some commands have an additional shortcut key or keystroke combination that is listed alongside the command. Some commands carry out an action immediately while others open a dialog box allowing you to select options. A description of each menu and its options follows.

Collection Menu

| Collection Menu Option | Keyboard Shortcut | Description |
|------------------------|-------------------|---|
| Connect | Ctrl + T | Initiate a connection with the database. |
| Disconnect | Ctrl + D | Terminate the connection with the database. |
| New Local Collection | Ctrl + L | Create a new local collection. |
| New Remote Collection | Ctrl + R | Create a new remote collection. |
| Edit Collection | Ctrl + E | Edit the selected collection's properties. |
| Import Packets | Ctrl + I | Import packet files into the selected collection. |

| Collection Menu Option | Keyboard Shortcut | Description |
|------------------------|-------------------|--|
| Export Collection | [none] | Export packet files to a saved format (.pcap, .payload, .xml, .csv, .txt). |
| Reprocess Collection | [none] | Allows the user to export the selected collection to a new collection, thereby reprocessing into a new collection and applying the active rules. |
| Delete Collection | [none] | Delete the selected collection. |
| Navigate Collection | Ctrl + N | Navigate to the selected collection. |
| Summarize Collection | Ctrl + S | Creates a high-level snapshot of the selected collection |
| Delete Content Cache | Ctrl + Del | Clears the content cache for the selected collection. |
| Exit | [none] | Close the application. |

Edit Menu

| Edit Menu Option | Keyboard Shortcut | Description |
|------------------|-------------------|--|
| Undo | Ctrl + Z | Resets the field last entered to its previous value. |
| Cut | Ctrl + X | Removes the value from the field (or highlighted text) and places it on the Windows Clipboard. |
| Copy | Ctrl + C | Copies the value from the field (or highlighted text) and places it in the Windows Clipboard. |
| Paste | Ctrl + V | Places the contents of the Windows Clipboard in the active field. |
| Select All | Ctrl + A | Selects all the values or items based on where the cursor is placed. |
| Find | Ctrl + F | Creates a search for a user-defined term. |
| Rules | Ctrl + U | Opens the Rules Configuration dialog box: Net Rules App Rules |
| Custom Actions | Ctrl + M | Enables the user to execute external operations on selected metadata in the Navigation View |

| Edit Menu Option | Keyboard Shortcut | Description |
|------------------|-------------------|--|
| Options | Ctrl + O | Opens the Options dialog box: General Display Reports Capture Process Audio Codecs Advanced |

View Menu

| View Menu Option | Keyboard Shortcut | Description |
|------------------|-------------------|---|
| Refresh | F5 | Refresh the collection list with the latest information. |
| Session | [none] | Allows the user to view a specific session in the active collection by entering the session ID. |
| Google Earth | [none] | Allows the user to represent the active data within the Google Earth desktop client. The GeoIP2 parser must be active when the data is processed. |
| Live Content | | If checked, allows the user to access the Live Content to manage live feeds |
| Collections | | If checked, the Collection page displays the collections by name, status, and size. |
| URL Bar | | If checked, the time range, collection view, and search fields are displayed. |
| Capture Bar | | If checked, the Capture Bar is displayed. |
| IM Window | | If checked, an Instant Message pane is displayed below the Collection pane. |
| Welcome Page | | The Welcome Page contains Frequently Asked Questions about Investigator and Recent NetWitness News. |
| Status Bar | | System status messages and warnings appear on the Status Bar. |

Bookmarks Menu

| Bookmark Menu Option | Keyboard Shortcut | Description |
|----------------------|-------------------|---|
| Add Bookmark | [none] | Adds the current drill path or session listing as a bookmark. This option is only available while navigating within a collection. |
| Organize Bookmarks | [none] | Allows the user to arrange existing bookmarks or remove them. This list is user-specific. |

History Menu

The **History Menu** displays and allows an immediate jump to any of the last 10 drill points created by the user.

Help Menu

| Help Option | Description |
|--------------------|---|
| Help Documentation | Opens the following URL in your default browser: https://community.rsa.com/community/products/netwitness/investigator , which contains links to Investigator documentation and the product download files. |
| Registration Page | Displays your Registration ID for Investigator. |
| Show Log | This text file is analogous to the log files created by the Decoder and Concentrator. It provides a record of all Investigator actions and also records system warnings and failures. |
| About Investigator | Displays the version of the Investigator software installed on your system |

Collection Navigation

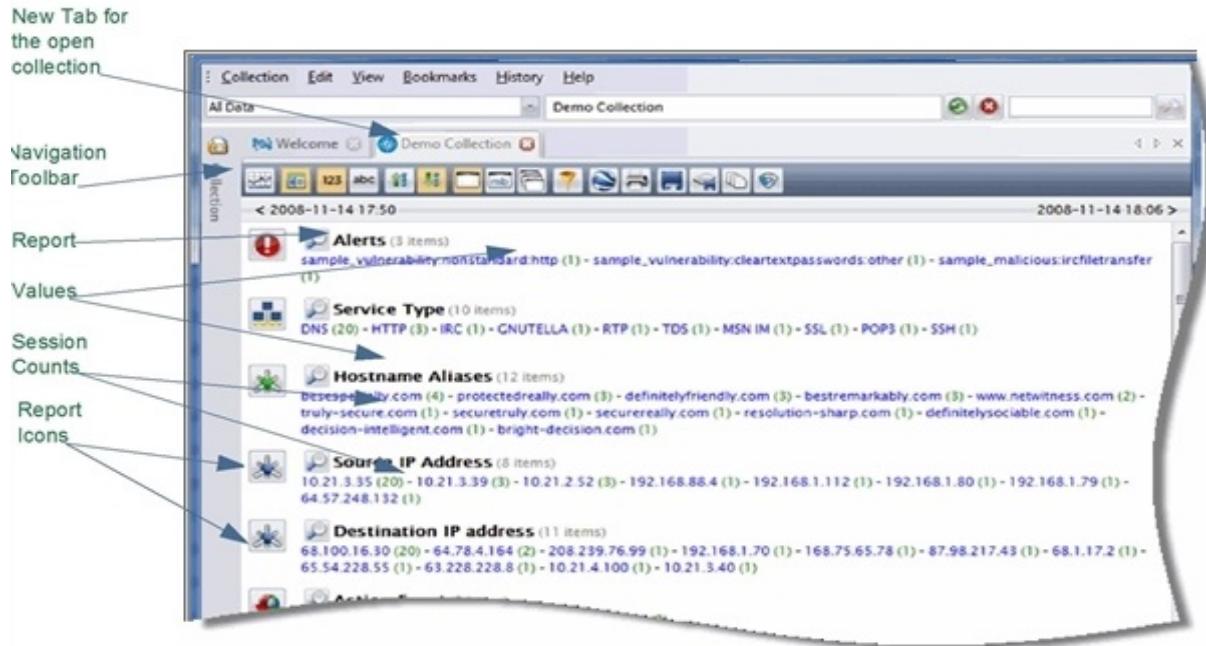
As you explore the data in a collection, it is important that you understand the features in Investigator so that you know where you are in the collection. Because there are multiple data items that you can drill into at any point along the way, it would be easy to direct yourself away from an item of interest and proceed down a less productive path.

- [Navigation View](#)
- [Navigate Multiple Views](#)
- [Session List View](#)

- [Content View](#)


Navigation View

On the main **Collection** screen, double-click the desired collection (**Sample Data**) to open a new tab for the **Navigation** process.



The tab for the selected collection shows a listing of the processed reports (e.g. **IP Protocol**, **Service Type**, **Action Event**, etc.). Each of the report types lists report values and their associated session counts.

Navigation Toolbar

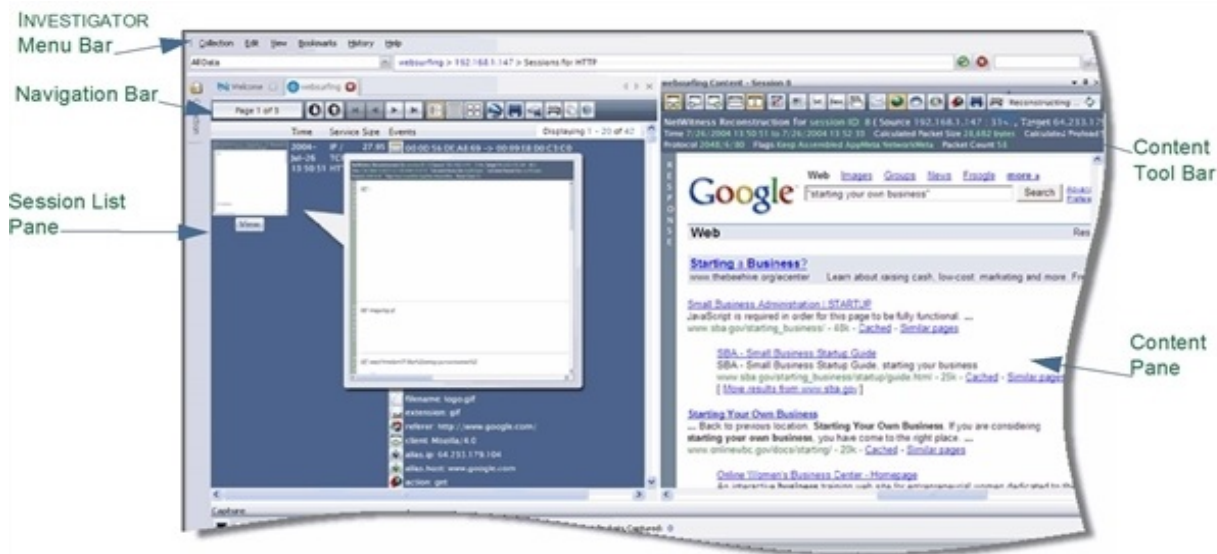
The appearance of the collection reports and the data contained are determined by the combination of selections you make on the Navigation toolbar. For example, the **Time Graph**  allows you to expand a section of time for closer examination. For a detailed explanation, see Navigation Toolbar.

The user can now perform either of the following two functions:

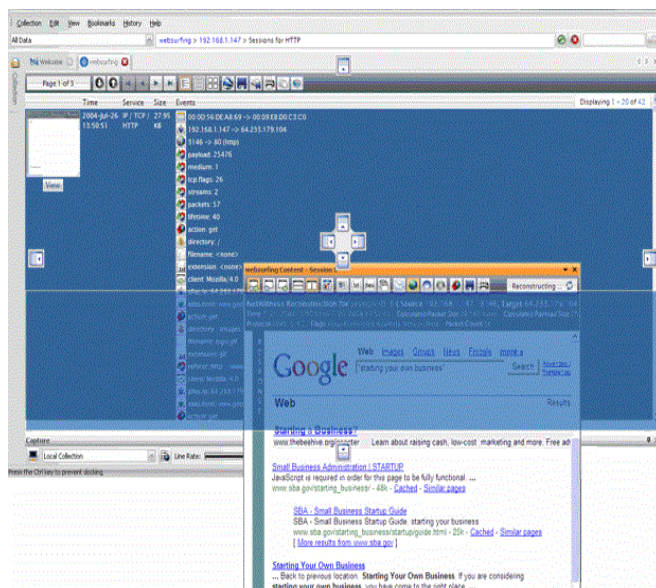
| Function | Description |
|---------------------------|---|
| Drill into a Report Value | This will refocus the current view into a Navigation View with that particular report value as a filter. |
| Drill into a Session List | This will display a list of all the sessions for a specified drill point and their associated metadata. Session content may be viewed from this list. |

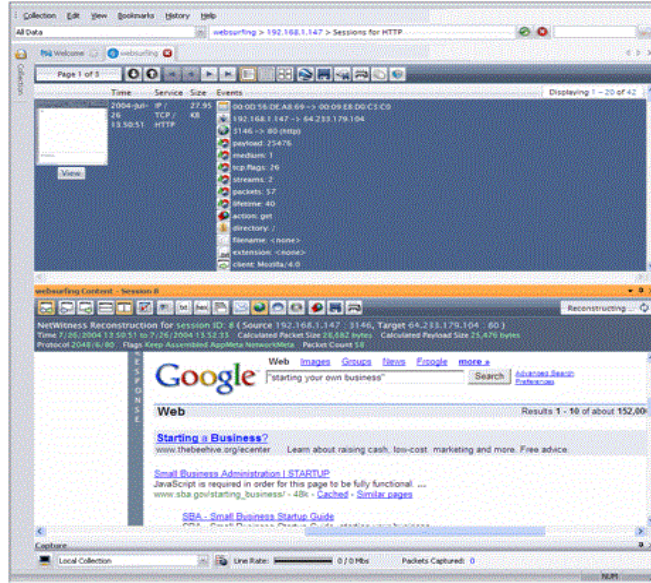
Navigate Multiple Views

As you begin to drill into sessions and values, it is usually helpful to arrange the session and content panes so that you can easily compare data. Each of the labeled elements can be undocked and moved, or hidden. The displayed arrangement is the default when Investigator is installed.



If you want change the position or orientation of the **Session List** pane or the **Content** pane, grab the edge of the pane and drag it out of position. Docking guides show possible positioning for the pane. The transparent blue area indicates the new position for the content. Releasing the cursor docks the Content pane in the new position.








The Docking Guides are only available if you are using one of the 2007 themes (EditOptions). One possible re-arrangement of the panes is shown here. You can determine which arrangement works best for yourself.

Content Pane Display Options

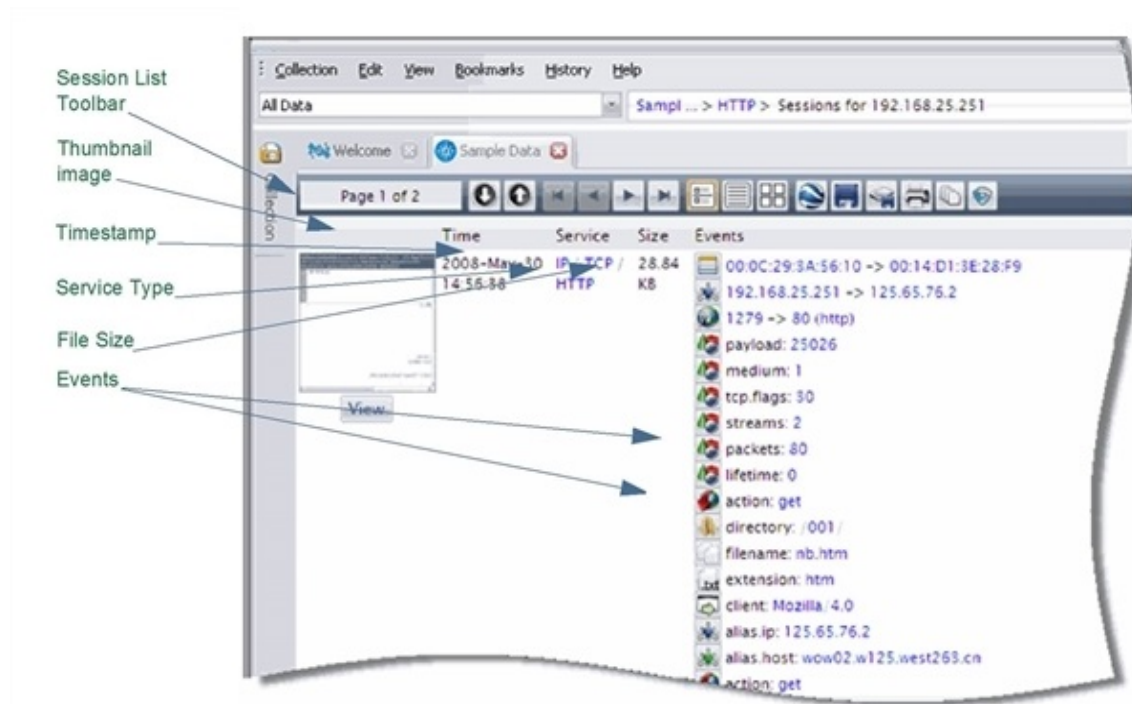
You can also use the display buttons in the upper right-hand corner of the **Content** pane.

| Click this... | To do this... |
|---|--|
|  | <p>View the Options menu to change the location of the Content pane.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <ul style="list-style-type: none"> Floating <input checked="" type="checkbox"/> Dockable Tabbed Document Auto Hide Hide </div> <p>The Floating option is useful if you are using dual monitors.</p> |
|  | <p>AutoHide hides the current Content pane and creates a tab to restore the content view.</p> |
|  | <p>The Hide button closes the Content pane.</p> |

Click on the **Options** icon to change the properties of the pane.

Session List View

The **Session List** view will display a representation of all the sessions that correspond to the drill from the **Navigation** view:




- **Thumbnail image** – A small image of the content for that session. If you click on the image, the Content pane opens.
- **Time** – The date and time of the data capture.
- **Service** – The protocol(s) used by the network.
- **Size** – The session size.
- **Events** – List of metadata items found in the session.

For example, if a user has clicked on a session count of 212 to the right of a particular **Address** report value from the **Navigation** view, the resulting 212 sessions will be listed on the **Session List** view.

Session List Toolbar

This toolbar facilitates moving among the individual sessions for the chosen **Report** and **Value**. The appearance of the collection reports and the data contained are determined by the combination of selections you make on the **Navigation** toolbar.

Content View

To view the content in a particular session, you click on the Thumbnail image. A separate pane displays the content detail for that session. You can select any one of the following formats, such as **View Web** , from the **Content Toolbar**.



You can continue to explore the data through drilling into specific items, search the session for a particular term, string, or other values.

Content Toolbar

When you view content, Investigator selects the probable best format, based on the collection's type of service. Once you open the **Content** view, you are able to change from the default **Auto** to any of the other options.

Getting Started

This User Guide illustrates the capabilities of Investigator, although your effectiveness depends upon the types of threats your organization is experiencing. Generally, there are two main categories that concern an organization:

- Malicious user activity—The introduction of malware that is destructive to your network, such as virus or other intrusive programming.
- Anomalous activity—This can be anything from downloads from your network during off-peak hours to excessive activity with a suspicious source or content.

Investigator, through the NetWitness Data Model, enables you to see the content through filters that you customize to fit your specific objective(s). How you do this necessarily depends on your understanding of the characteristics of your network. It is beyond the scope of this document to attempt to illustrate an extensive number of scenarios describing how Investigator should be utilized on any specific network.

Investigator can enable a historical investigation into events leading up to a network alarm or incident.

If you know that a certain type of activity is taking place on your network, you can select only the reports of interest to examine the content of data collections.

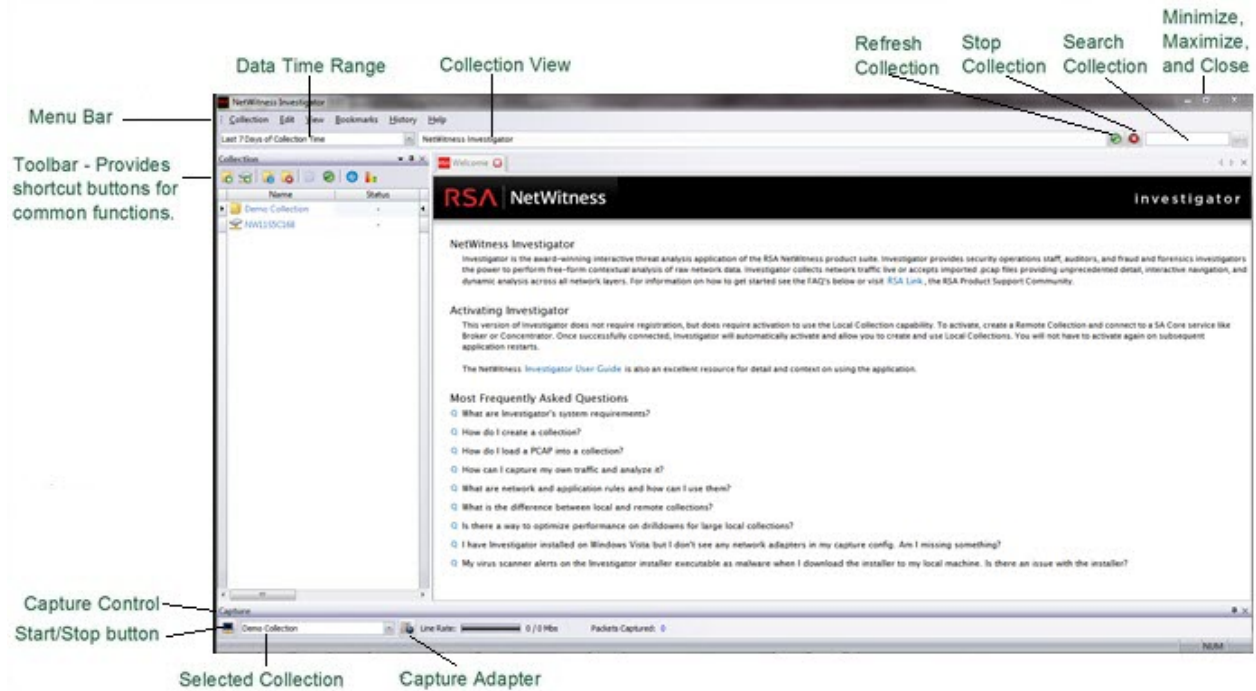
Once you become familiar with data navigation methods, you can explore the data more completely through:

- Drilling into reports and report values
- Searching for specific types of information
- Reviewing specific sessions and session content in detail.

The initial task of configuring Investigator is described in the remainder of this chapter. As you work with the application, you may decide to change certain settings to optimize performance.

About the Investigator Main Window

When you first open Investigator, the **Collections** screen and the **Welcome Page** display. This window enables you to create new collections and manage the existing saved collections.



A Collection may display any of the following in the **Status** column:

- **Not Connected**
- **Connecting**
- **Unable to Connect**
- **Ready**
- **Processing**
- **Exporting**
- **Importing**
- **Error**

Configure Investigator

You access the configuration options from the **Edit** menu on the Investigator main window. Settings that are not listed in these options may be viewed or changed in the Application Data File



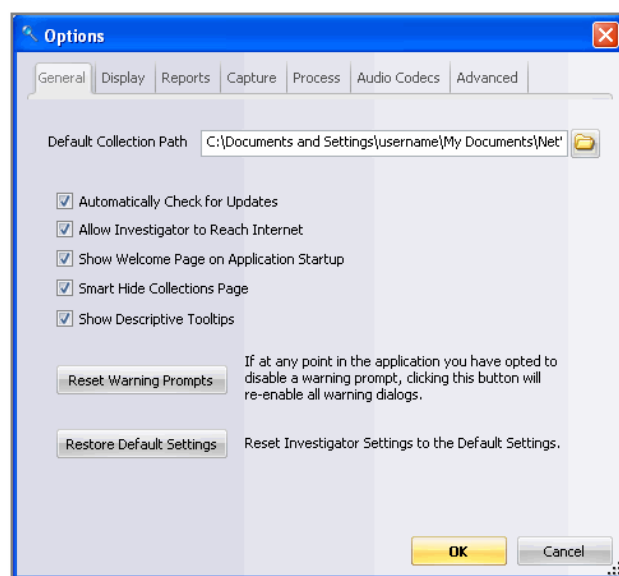
The **Options** dialog box has seven categories:

- [General](#)
- [Display](#)
- [Reports](#)
- [Capture](#)
- [Process](#)
- [Audio Codecs](#)
- [Advanced](#)

Note: The complete configuration settings for Investigator are available in the **Application Data File** on your system after installation.

General

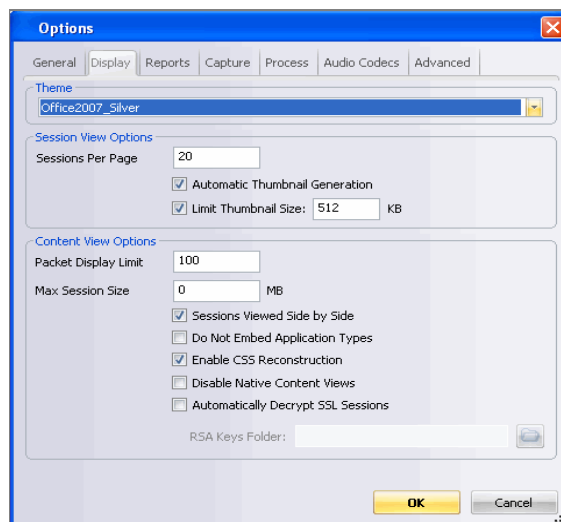
This section allows you to determine where all collections are stored, thumbnail size, and warning prompt settings.



- **Default Collection Path**—This is the default directory path where all collections are stored on the system. The default path is My Documents\NetWitness\Collections.
- **Automatically Check for Updates**—When checked, Investigator automatically checks for new updates and prompts the service to download them.
- **Allow Investigator to reach Internet**—When checked, Investigator reaches out to the NetWitness web service to load the most recent FAQs, News and Community posts in the Welcome page.
- **Show Welcome Page on Application Startup**—When checked, the Welcome page is automatically displayed when Investigator opens.
- **Smart Hide Collections Page**—When checked, the Collection bar collapses when a collection is navigated.
- **Show Descriptive Tooltips**—When checked, tooltip descriptions display as you roll over icons or regions of the Investigator pane(s).
- **Reset Warning Prompts**—This button re-enables all warning dialogs.
- **Restore Default Settings**—This button restores all settings to their default values.

Display

This section allows you to specify the way Investigator appears and options for Session and Content View.



Theme

A theme is a set of elements, such as color scheme, that allows the user to personalize the appearance of Investigator.

Choosing any of the 2007 themes allows the use of docking guides, as described in [Navigate Multiple Viewson page 1](#).

Session View Options

- **Sessions per Page**—The number of sessions shown in **Session List** view.
 - **Automatic Thumbnail Generation**—If checked, thumbnails will automatically be generated when viewing a session list.
 - **Limit Thumbnail Size**—When **Automatic Thumbnail Generation** is checked, the user can specify a size limit for thumbnail generation for any session content above the limit.

Content View Options

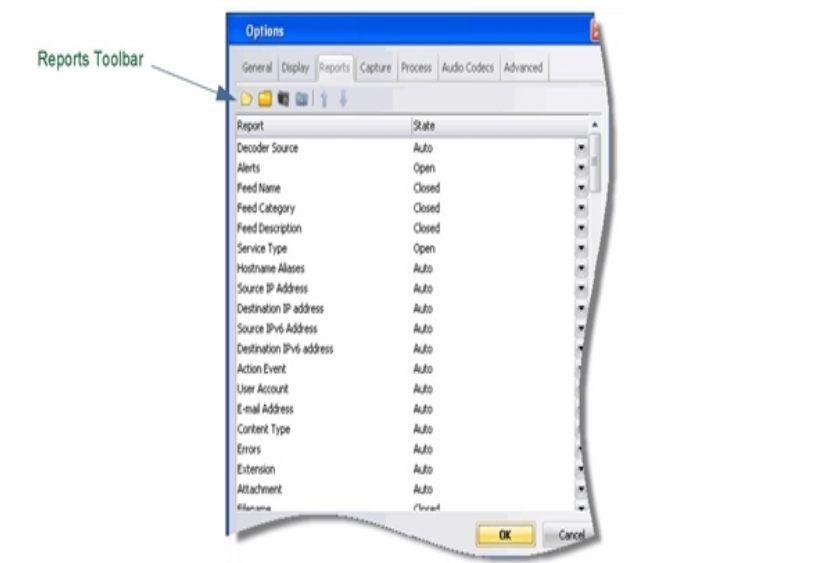
- **Packet Display Limit**—The number of content packets to display. Default is 100.
- **Max Session Size**—The maximum session size in MB. Default is unlimited (0).
- **Sessions Viewed Side by Side**—When checked, **Content View** shows **side1/side 2** side by side, as opposed to top down. You must clear the content cache for each collection for this option to take effect.
- **Do Not Embed Application Types**—When checked, **application**, **audio**, and **video** content types are not embedded into the NetWitness content display page.
- **Enable CSS Reconstruction**—When checked, the application attempts to find and load the website's CSS files from other sessions. If you are having problems viewing specific websites, try checking this option.
- **Disable Native Content Views**—When checked, the user is prevented from viewing content in Web, MAIL, IM, and VOIP formats. This option is not normally used.
- **Automatically Decrypt SSL Sessions**—When checked, the content display page decrypts SSL sessions that were encrypted with any of the provided RSA keys.
 - **RSA Keys Folder**—When the Decrypt SSL Sessions is checked, the user can specify the location to specify RSA keys.
 - **TLS Certificate Hashing** - You can view hashes of certificates that are seen in the packet stream. These hashes are the SHA-1 value of any DER- encoded certificate encountered during a TLS handshake. The hashes produced can be used to compare network traffic with hashes from public SSL blacklists, such as the one from sslbl.abuse.ch. The SHA-1 is stored as a text value in the meta key cert.checksum. Investigator can decrypt up to TLS version 1.2.
 - **JA3 and JA3S TLS fingerprints** - You can view the JA3 value of TLS clients and the JA3S value of TLS servers that are observed in a network session. The values that are produced conform to the values generated by the open source JA3 tools (<https://github.com/salesforce/ja3>). JA3 is stored as a text value in the meta key ja3. JA3S is stored as a text value in the meta key ja3s.
 - **Community ID** - Investigator generates Community ID flow hash values that are compatible with the Community ID specification defined by <https://github.com/corelight/community-id-spec>. The Community ID is written to a text-formatted meta key named `community`. The Community ID is generated on sessions containing TCP over IPv4, TCP over IPv6, UDP over IPv4, and UDP over IPv6.

Reports

The user specifies the reports that are compiled when data is processed. The available settings for reports are:


- Auto - This selection allows the application to determine whether the report is opened. If there are less than 10,000 sessions, it is opened.
- Open - This selection opens the report regardless of the number of sessions.
- Closed - This selection does not display the query results for the report
- Hidden - This selection does not display the report.

For example, if the user only sets the Service, Time, and Address reports as Open and sets the rest of the reports as Hidden, any Collection processed with those settings, only those three reports are listed in the view. If you change the report settings, you must refresh the collection to reflect those changes. The Reports Toolbar allows the user to group or re-arrange reports for ease of use.



Reports Toolbar

| Click this... | To do this... |
|---------------|---|
| | Set all reports in the list to Open |
| | Set all reports in the list to Closed |
| | Set all reports in the list to Auto |
| | Set all reports in the list to Hidden |
| | Move the selected report up in the list |

| Click this... | To do this... |
|---|---|
|  | Move the selected report down in the list |

Capture

In this section, you specify the capture configuration options for Investigator.

Network Adapter

Select the appropriate adapter for your network. If you are using a wireless capture device, see [Wireless Packet Capture](#) on page 1.

The default network adapters available are set at installation. Consult your System Administrator for more information.

Advanced Capture Settings

- **Max Disk Usage**—The percentage of drive space allowed to be used by the system.
If this value is 100, the drive is allowed to fill up completely
- **Buffer Size(MB)**—Specify the size in MB that is used to cache packets on the network

Evidence Handling

If enabled, Hash files are saved in the specified location. By default, Hash Capture is disabled.

- **Hash Captures**—External files that can be used to validate that the original capture files are intact.
- **Hash Directory**—Specifies the file location.

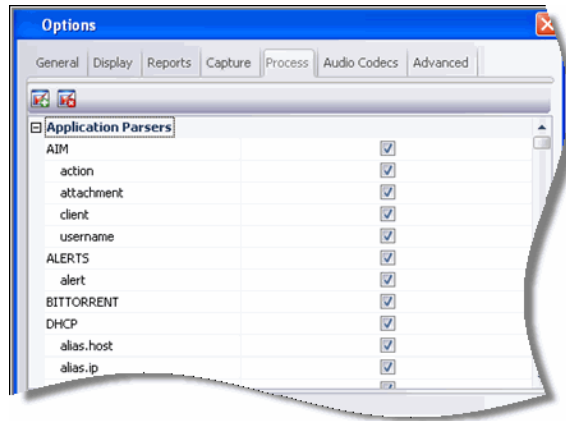
Process

There are three processes configured on this tab. Use the scroll bar to move through the dialog box.

- Application Parsers
- Assembler Properties
- Memory

Application Parsers

Use the Select All  icon or the Clear All  icon to make your selections.



Assembler Properties

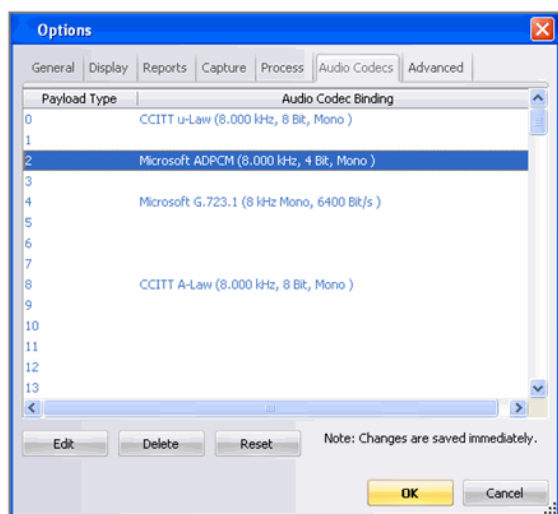
| Setting | Descriptions |
|----------------------|---|
| Maximum Session Size | <p>Assembler maximum session size in bytes. This is the maximum amount of data a single session can retain. If the size exceeds this value, the data is truncated to the maximum size.</p> <p>Reducing the amount of memory can improve performance; however, sessions above this byte limit will be truncated.</p> |
| Minimum Parser Bytes | Specifies the minimum number of bytes to parse |
| Maximum Parser Bytes | Specifies the maximum number of bytes to parse |
| Packet Partial | Allows for truncated packets and ignores checksum. Enabling partial packets will allow assembly of truncated packets and also not perform a checksum for ip and tcp packets. |

Memory

| Setting | Description |
|---------------|---|
| Session Pool | Total number of sessions to keep in the preallocation pool. This is a performance setting which allocates the number of sessions at NetWitness startup. |
| Session Pages | Total number of session pages to keep in the preallocation pool. This is a performance setting which allocates the number of session pages at NetWitness startup. |
| Packet Pages | Total packets pages to keep in the preallocation pool. This is a performance setting which allocates the number of packet pages at NetWitness startup. |

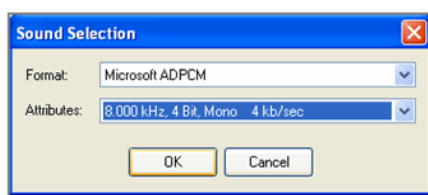
Audio Codecs

NetWitness loads the standard Microsoft Operating System codecs; however, the user can modify existing codecs. Codecs can be bound to the channels for replay; however, the required codecs must be installed locally to be available for channel assignment.



When you highlight a row, there are three actions available:

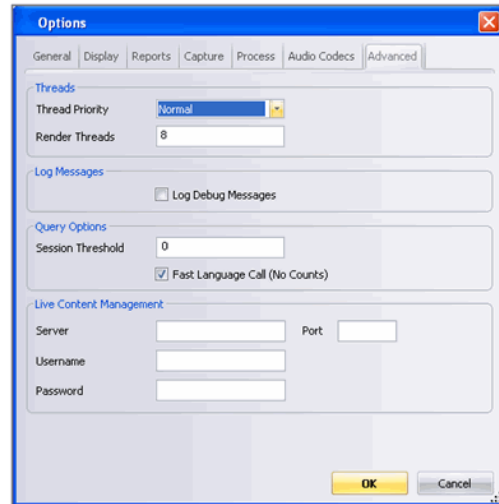
- **Edit**—When you click the Edit button, a dialog box opens that allows you to select:
 - **Format**—Select the format you want associated with the codes from the dropdown list.
 - **Attributes**—Select the attributes you want associated with the codes from the dropdown list.



- **Delete**—When you click the Delete button, the actual audio codec is not deleted. Its content is merely cleared.
- **Reset**—When you click the Reset button and click Yes to confirm, all the standard Microsoft Operating System codecs are reinstated.

Advanced

This section allows you to set options for Threads, Log Messages, Queries, and Live Content Management.



Threads

- **Thread Priority**—The user can control the thread priority of the overall user interface.
 - Normal—This setting gives priority to the data capture thread during a sustained capture.
 - Below Normal—This setting gives no priority to the data capture thread.
- **Render Threads**—The maximum number of CPU threads allocated for rendering data, as users perform other analysis operations simultaneously.

Log Messages

- **Log Debug Messages**—Select this option to troubleshoot Investigator. When selected, all debug messages are written to the log file.

Query Options

- **Session Threshold**—The maximum number of sessions that are accurately displayed in the Navigation window. Set to zero for unlimited accuracy, but slightly slower queries.
- **Fast Language Call**—Select this option for maximum performance. If you deselect it, this can greatly slow down opening reports, but provides more accurate information (in some cases) on the full number of items next to the report name.

Live Content Management

- Login information to the CMS system for downloading content, for example, rules, parsers and feeds.

Collection Management

Collections are logically-related sets of packet data. This packet data is processed by NetWitness® Investigator into the NetWitness Data Model. Once processed it is available for analysis.

Investigator has very flexible configuration options to reduce the amount of time required to process the data analysis. This chapter describes how to configure your data collection to find a specific kind of activity.

Collections are created and populated with data through import from another source or live network capture before analysis with Investigator may occur.

Accessing Data

Investigator enables you to analyze data from two sources:

- A remote device, such as a Broker, Concentrator, or Decoder
- A **Local** collection, either a live capture or packet imports

Collection Configuration

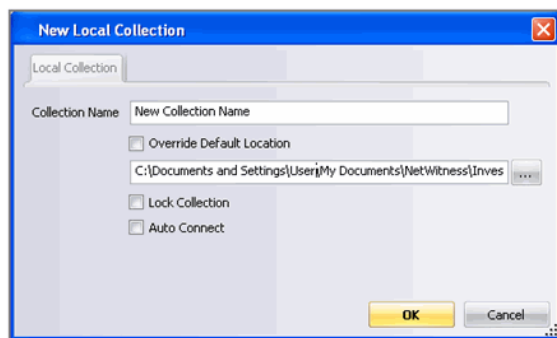
Before actually capturing data for analysis, you must set the options for the collection that govern the behavior of data processing and the user interface.

There are two levels of configuration that are required with Investigator.

- **Application Level** - Settings for new collections, such as where collections are stored, thumbnail size, index settings and content view, and warning prompt settings. Changes at this level do not affect existing saved collections.
- **Collection Level** - Settings for file location, locking a collection, or making a collection the default collection.

Collection Level

When you create a new collection, the configuration dialog box displays.



- Enter a unique name for the new collection in the **New Local Collection** dialog box.









Note: Collection names may not contain the following characters: / \ * ? : " < > |

- Specify a location for the new collection if you want it saved other than the displayed folder by checking the **Override Default Location** checkbox.
- Check the **Lock Collection** checkbox if you want to prevent the collection from being deleted or used for future capture/import.
- Check the **Auto Connect** checkbox if you want the collection to open each time you open Investigator.

Note: The settings for a collection can be changed at any time.

Investigator Toolbar


The Investigator toolbar contains shortcut buttons that are used frequently to work with collections. Some of these operations can be accessed with keyboard shortcuts. There are other actions available from the Collection menu.

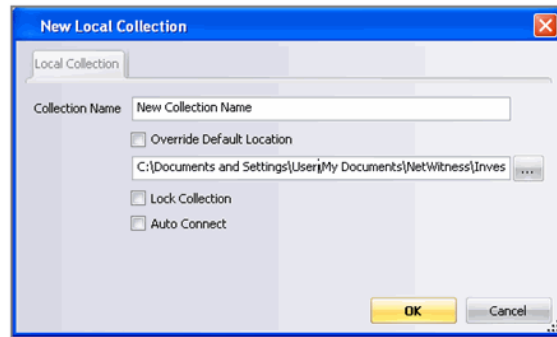
| Click this... | or press this... | To do this... |
|---|------------------|--|
|  | Ctrl + L | Create a new local collection. |
|  | Ctrl + R | Create a new remote collection. |
|  | Ctrl + E | Edit the selected collection's properties. |
|  | [none] | Delete the selected collection. |
|  | Ctrl + I | Import packet files into the selected collection. |
|  | F5 | Refresh the collection list with the latest information. |
|  | Ctrl + N | Navigate to the selected collection. |
|  | Ctrl + S | Creates the sample Data Summary for the selected collection. |

How To...

- [Create a New Collection](#)
- [Configure the New Collection](#)
- [Import a Data File](#)
- [Reprocess a Collection](#)

Create a New Collection

1. On the Investigator Toolbar, click the **New Local Collection**  icon.
The settings for a collection can be changed at any time.



- a. Enter a unique name for the new collection in the **New Local Collection** dialog box. Collection names may not contain the following characters: / \ = * ? : " < > |
- b. Specify a location for the new collection if you want it saved other than the displayed folder by checking the **Override Default Location** checkbox.
- c. Check the **Lock Collection** checkbox if you want to prevent the collection from being deleted or used for future capture and import.
- d. Check the **Auto Connect** checkbox if you want the collection to open each time you open Investigator.

Note: The settings for a collection can be changed at any time.

2. Click **OK**. The named collection is added to the list on the **Collections** tab. Double-click the collection to connect to the database. When the **Status** shows **Ready**, continue to the **Capture Control** box.
3. Select the target collection from the drop-down menu. Proceed to configure the collection.

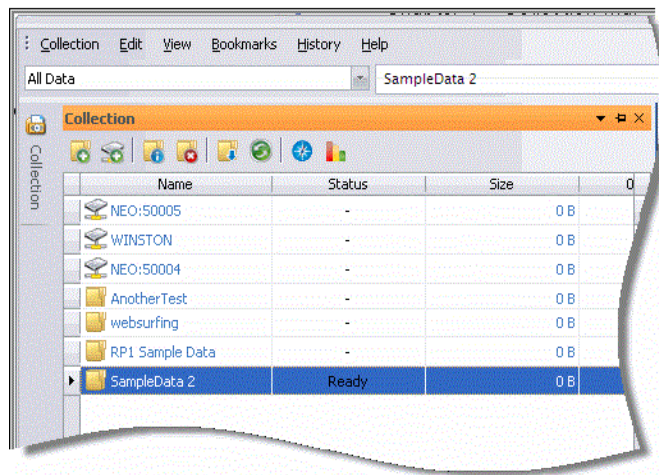
Configure the New Collection


You can create a new collection in one of two ways:

- Importing an existing data file:
The file is processed based on the current Investigator configuration settings
- Configure live data from the network:
You set the **Adapter** and **Rules** before you begin the capture process .

Import a Data File

1. Double-click the **New Collection Name** to connect to the database. The **Status** changes to **Ready**.



2. On the Capture Toolbar, click the **Import**  icon.
3. Navigate to the folder where the capture files are saved. Select the file to import and click **OK**.

Note: If you are importing multiple files, you can select the check box to enable you to track the file names. If you import a collection under a different name, you can apply a different set of Network and Application layer rules to obtain a different view of the same data.

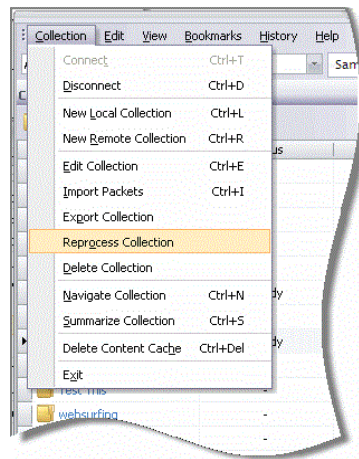
Reprocess a Collection

When you capture data with Investigator, the Network layer and Application layer rules that you define are applied to the data. You might decide that it would be beneficial to use a different set of rules. The rules on Investigator apply to all collections. In order to reprocess an existing collection, you must delete the existing rules and replace them with the new set of rules.

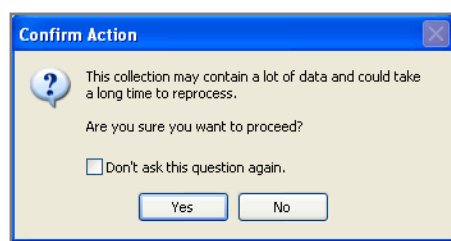
1. Export your rules to a file (.nwr) and then delete the existing files for the Network layer and Application layer rules.

Any rules you do not delete will be applied with the new rules to the collection when it is reprocessed.

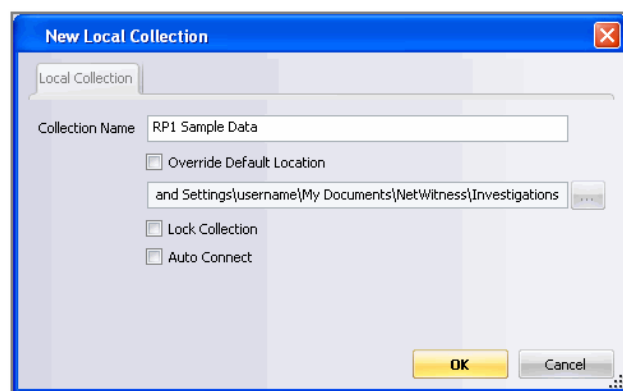
2. On the **Collections Pane**, highlight the collection that you want to reprocess.
3. From the **Collections** menu, select **Reprocess**.



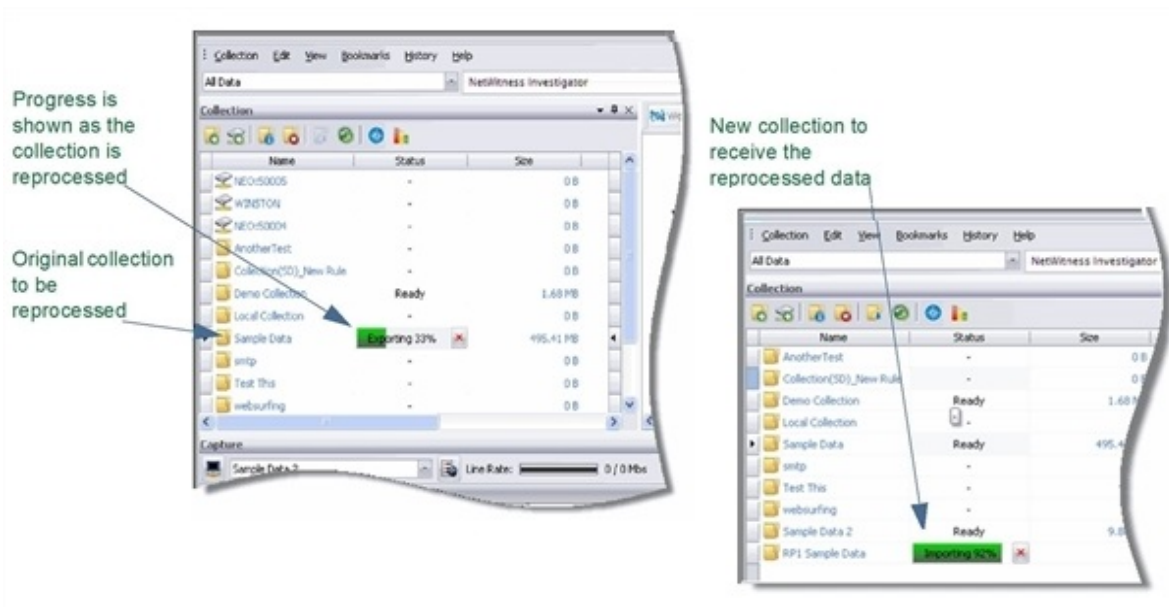
4. Click **Yes** to confirm that you want to proceed with reprocessing the selected collection. If you click **No**, the procedure terminates.



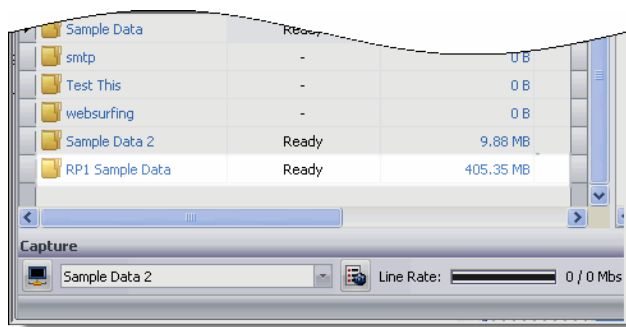
5. Enter a unique name for the reprocessed collection and click **OK**.



6. As the data is exported from the original collection and imported into the new collection, the progress is shown in the **Collection Pane**.



7. When reprocessing is complete, the new collection displays a **Ready** status.



Input File Types List

NetWitness Investigator can read as file-based input any of the file types listed in the table below. Packets provided in **TCPDump** format are preferred since this is the industry standard for packet data.

| Type of File | |
|------------------------------|---------------|
| TCPDump | |
| NetMon | .cap, .cap.gz |
| EtherPeek | .pkt, .pkt.gz |
| IPTrace | .ipt, .ipt.gz |
| NAIDOS | .enc, .enc.gz |
| RAW | .raw, .raw.gz |
| NetWitness Data | .nwd |
| Network Instruments Observer | .bfr |

NetWitness Data files (.nwd) are a proprietary file type that can be created when exporting data from one NetWitness Collection to another.

Data Capture

This chapter explains the steps necessary to prepare Investigator for live data capture, as well as the way captured data is processed. The two areas that affect how the data will be processed are:

- **Custom and Specialized Parsers**—This introduces specialized and user-defined parsers.
- **NetWitness Live**—NetWitness Live provides immediate access to multiple sources of threat intelligence and reputational content.
- **Rules**—There are two categories of rules that affect data capture, **Network Layer** and **Application Layer** rules.

Use this list to prepare to capture live data with Investigator.

Steps to complete before beginning a capture:

1. Select the parsers to use for the capture
 - Define any custom parsers for use
2. Define the Rules to be applied to the captured data
 - Network Layer
 - Application Layer
3. Verify the Capture Configuration settings
 - Network Adapter
 - Advanced Capture Settings
 - Evidence Handling
4. Start the capture

Custom and Specialized Parsers

NetWitness Investigator users can create custom parsers to unique specifications using any one of several special parsers.

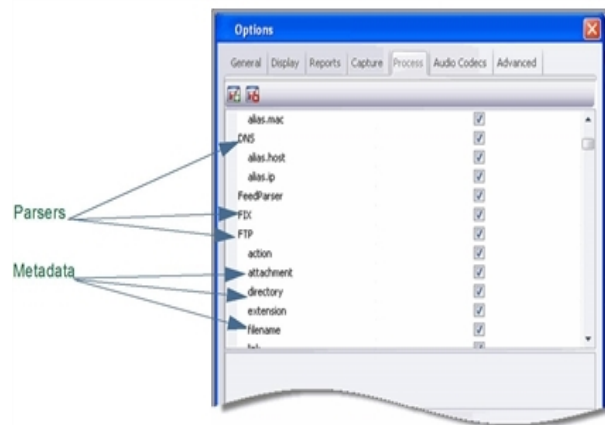
- **GeoIP2**—This parser associates the IP addresses with actual geographical locations.
- **Search**—This parser is user-configured to generate metadata by scanning for pre-defined keywords and regular expressions.
- **Entropy**—This parser is a NetWitness native parser. When the Entropy parser is enabled, analysts have visibility into channels that are trying to blend in with other traffic, but do not follow normal protocol behavior. This helps to identify channels that do not conform to the normal environment traffic baseline, and may be worthy of investigation.
- **Lua**—A parser created in the Lua language that has nearly as much capability as those parsers compiled directly into the product.

For more information about these parsers, see the *Decoder Configuration Guide* on RSA Link. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents. To configure these parsers in NetWitness Investigator, see [Configure Parsers](#).


Configure Parsers

In Investigator, to configure the parsers:


PATH: **Edit > Options > Process**



To customize the parsers for use in a particular collection, you can begin with all parsers selected or clear the entire list of parsers and manually enable the parser(s) and which associated metadata you wish to use. For the first method:

1. Click on the **Select All Parsers**  icon to select all parsers and associated metadata enabled.
2. Scroll through the list to disable any of the parsers or the associated metadata in the list. Click **OK**.

For the second method:

1. Click on the **Clear All Parsers**  icon to disable all the parsers and associated metadata.
2. Scroll through the list to select the parsers and the associated metadata to enable.
Click **OK**.

Note: When you define a new parser, it does not appear in this list of parsers until the next time you open Investigator.

NetWitness Live

NetWitness Live is a content management system that enables users to subscribe to similar rules, protocols, flex parsers, and feeds that have been validated and made available by NetWitness. When your subscription to the NetWitness Live services is activated, you are given the credentials to access the NetWitness Live service. You are then able to select from the available content to download to Investigator. For information about the NetWitness Live service, see the **Live Services Management Guide** on RSA Link at <https://community.rsa.com/>.

There are more than 200 alerts that can be imported into Investigator and applied during live capture or **.pcap** import. These are excellent examples of how to author your own rules for Investigator.

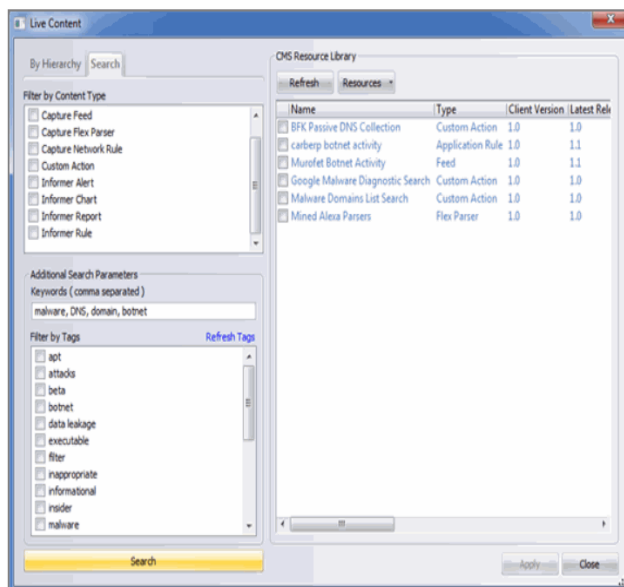
Some of the data types that the baseline rules provided will help identify are:

| | | | | |
|----------------------|---------------------|------------------|---------------------|--------------------------|
| Beaconing | Watchlists | Tunneling | BOTs | Password Vulnerabilities |
| Exploit Kits | Attack Profiles | Insider Activity | Remote Shell | |
| Malware Applications | Malicious Downloads | Torrents | Malicious Redirects | Non-standard Traffic |

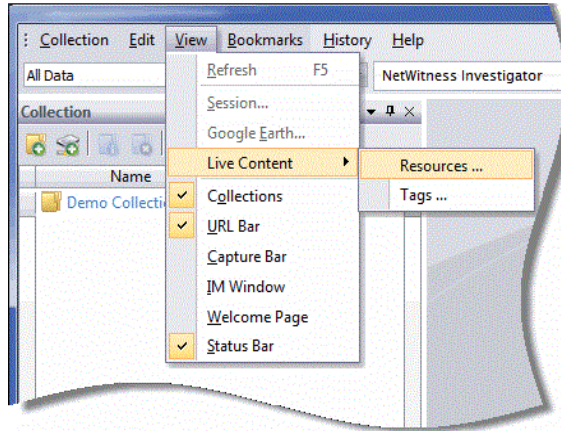
The SANS Internet Storm Center, contains the top 10,000 source IPs, associated with malicious activity and tracked by SANs and its contributors. As a NetWitness Feed, sessions containing these IP addresses are flagged as new meta data for analysis. For more information on the SANs Top Source list, visit <http://isc.sans.org>.

To get started, follow these steps:

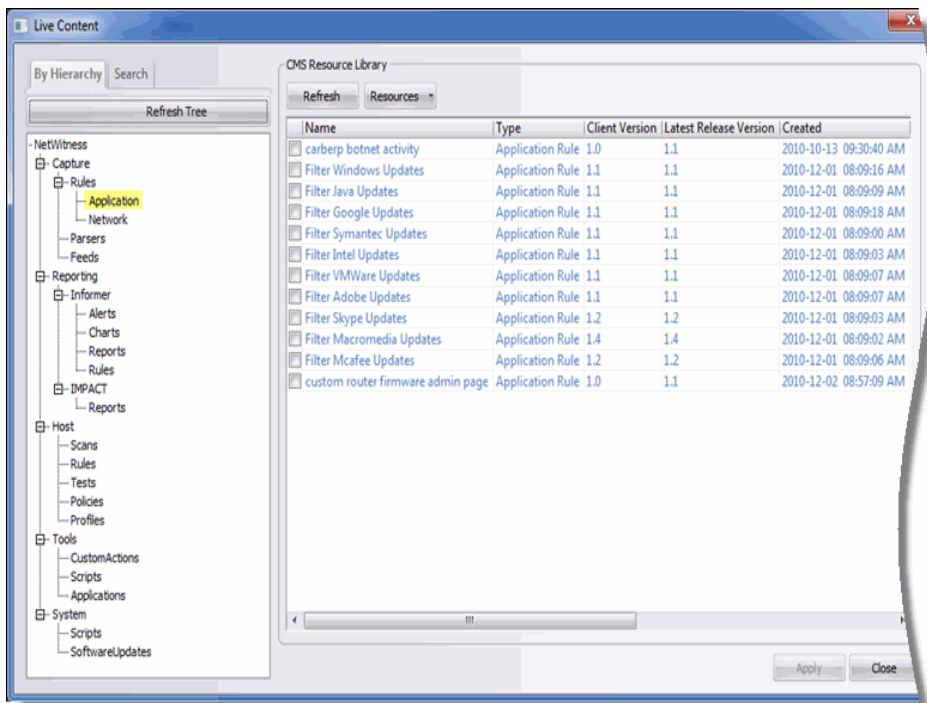
1. Navigate to the **Edit > Options** menu and click on the **Advanced** tab. Complete the **Live Content Management** credentials for your subscription. Click **OK**.



2. On the **View** menu, select **Live Content** and the **Resources** option.



The **Live Content** dialog is displayed. When you select a topic in the **Refresh Tree Hierarchy**, the results are displayed in the **CMS Resource Library** pane to the right.

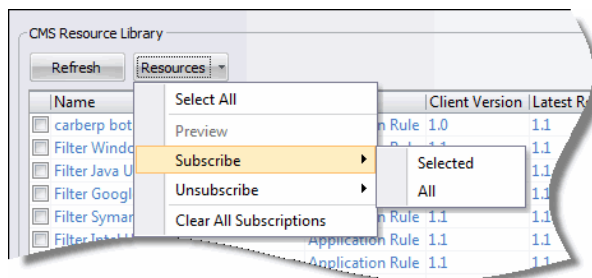


- The **Hierarchy** view allows the user to browse all of the content in the system to which he has access, arranged by content type.

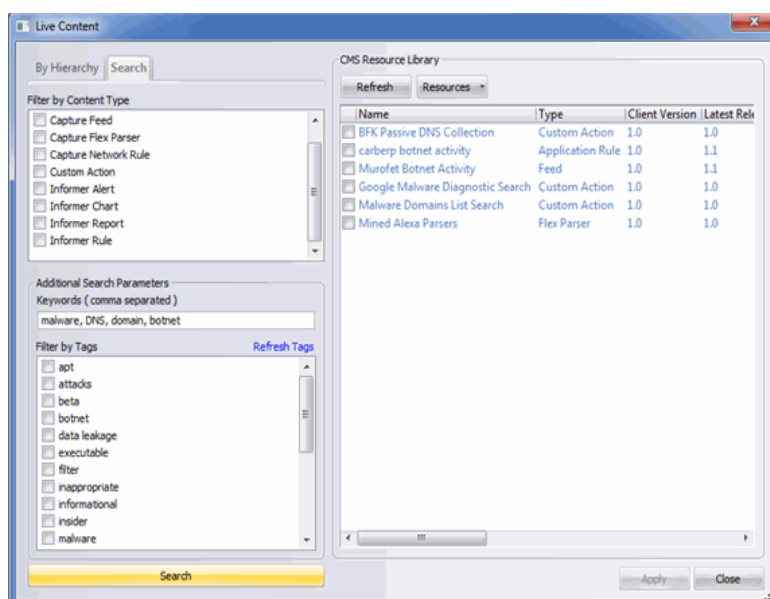
Additional information about the displayed results are shown as you scroll to the right:

| Name | Client Version | Created | Downloaded On | Size |
|------|------------------------|------------|---------------|------|
| Type | Latest Release Version | Updated On | URL | |

- When you click on the **Resources** in the **CMS Resource Library**, an option menu displays that allows the user to control the subscriptions.

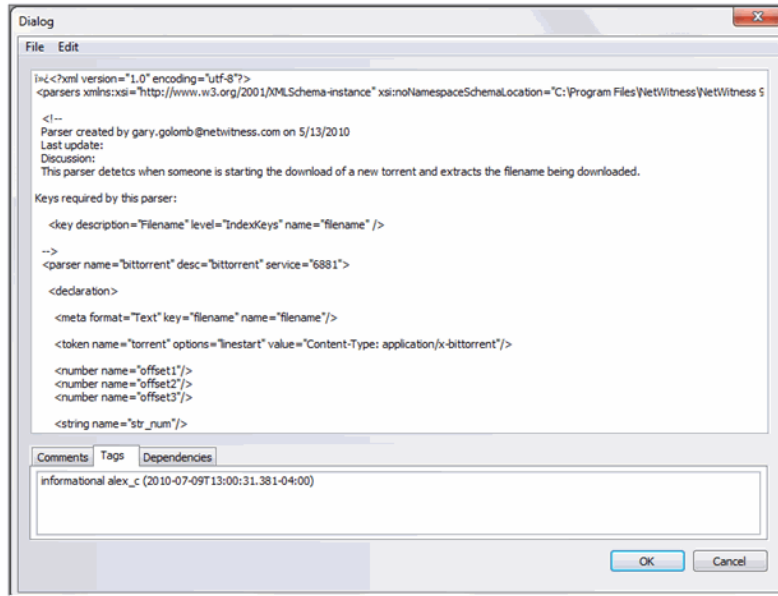


- The **Search** tab allows you to search your subscribed content on the system. You can narrow your search by content type, tag, and keyword.



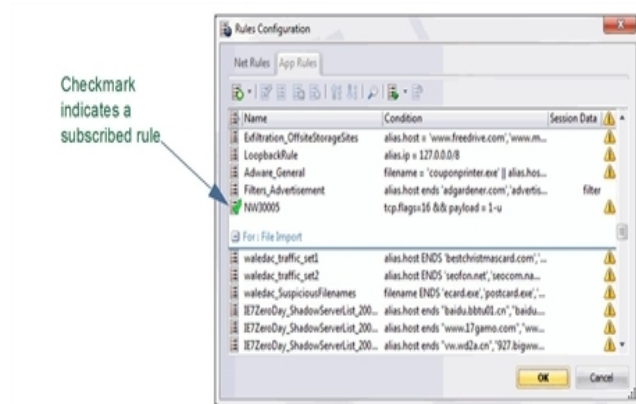
Preview Content

When browsing the content, you can click the **Preview**  icon for any selected item. This opens a dialog window that allows you to view text-based content. You will not be able to preview binary content, such as a binary feed file. The preview dialog also allows you to view a resource’s comments, tags, and any dependencies.



Update Content

When you click the subscribed check box in the content list the system downloads the content from the server and checks that content against the server each time the application is started. This happens without user intervention and is currently not configurable. An installed resource is displayed with a check on its icon in the **Rules Configuration dialog**.



Rules Overview

Rules can be defined as filters created for specific metadata, that when matches are found, can result in predefined behavior(s), known as actions. For example, if the user wanted to keep all traffic that fit certain criteria, but filter all others, they might create a rule with the necessary actions in order to fulfill this requirement. When applied, rules will affect both packet capture file importing, as well as live network capture.

The two most common uses of rules within Investigator are:

- To filter out certain types of traffic that does not add value to the analysis of the data.
- To alert, and thereby create a custom alert meta value, when certain conditions are found while Investigator is processing and reconstructing packets into sessions.

By default, there are no rules defined when you first install Investigator. Unless there are rules specified, the packet(s) will not be filtered.

To configure the **Network Layer** and **Application Layer** rules, from the Investigator menu bar:

PATH: **Edit > Rules**

You configure the software rules for live network capture, as well as processing packet data previously collected. There is a tab for each type of rules:

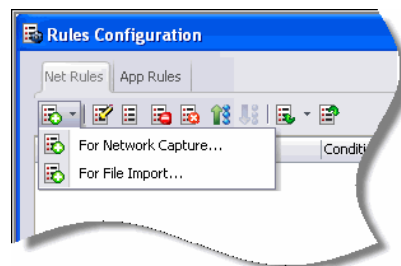
- Network Layer Rules
- Application Layer Rules


Note: Network Rules are applied prior to session reconstruction and Application Rules are applied after session reconstruction.

Network Layer Rules

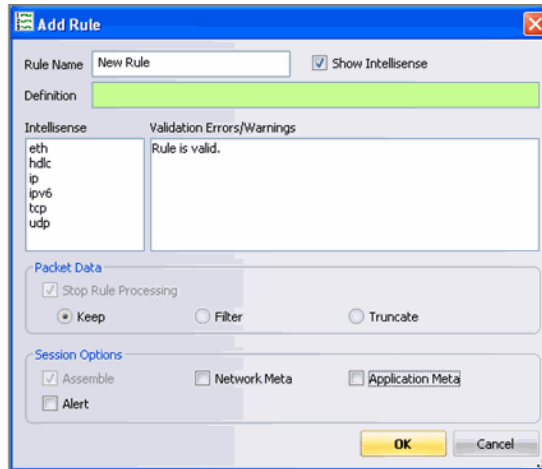
Network layer rules are applied at the packet level and are made up of rule sets from Layer 2 - Layer 4. Multiple rules may be applied to the Investigator. Rules may apply to multiple layers (for example, when a network rule filters out specific ports for a specific IP address).

1. From the Investigator **Edit** menu, select the **Rules** option. The Rules Configuration dialog displays.
2. The **Net Rules** tab is selected by default.



3. Click the **New Rule** Type  icon to specify whether the rule applies to:
Network Capture
or
File Import
The same rules can be applied for both live **Network Capture** or **File Import**.

- In the **Add Rule** dialog, enter a descriptive name in the **Rule Name** field.



- Complete the **Definition** field by entering directly in the field or by double clicking a meta from the Intellisense window. As you build your rule definition, Intellisense displays syntax errors and warnings.
If the **Stop Rule Processing** option is checked, network rule evaluation ends if the rule is matched.
- Click **OK** to submit the rule.

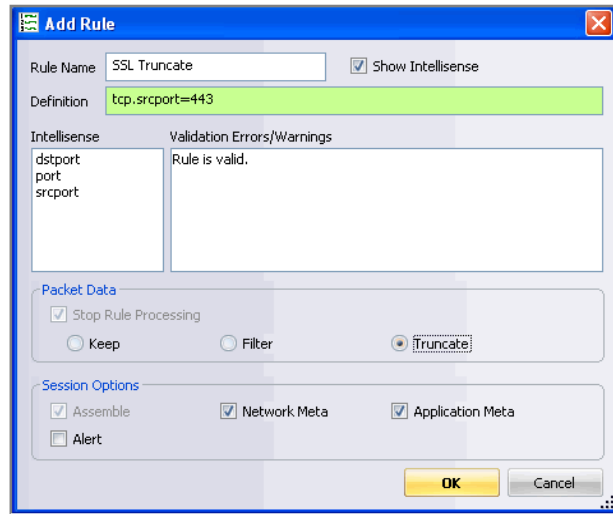
Intellisense lets you know that the rule you created is valid.

| Rule Action | Description |
|------------------|--|
| Packet Data | |
| Keep | The packet is saved when it matches the rule. |
| Filter | The packet is not saved when it matches the rule. |
| Truncate | The packet payload is not saved when it matches the rule. |
| Session Options | |
| Assemble | The assembler assembles the packet chain when it matches the rule. |
| Network Meta | The packet generates network metadata when it matches the rule. |
| Application Meta | The packet generates application metadata when it matches the rule. |
| Alert | The packet generates a custom metadata when metadata matches the rule. |

Sample Network Layer Rules

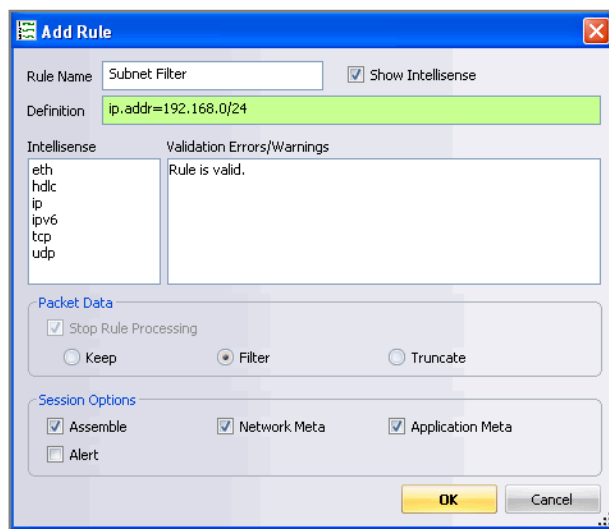
- Truncate all SSL from the source port – **tcp.srcport=443**

Rule Action – Truncate



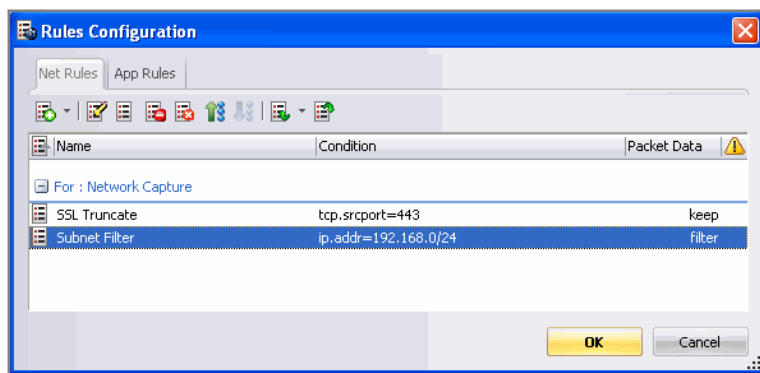
2. Create a subnet filter – ip.addr=192.168.2.0/24

Rule Action – Filter












Working with Network Layer Rules

When several Network layer rules exist, you can edit or delete rules or change the rule priority.



When you select a rule, the following options are available:

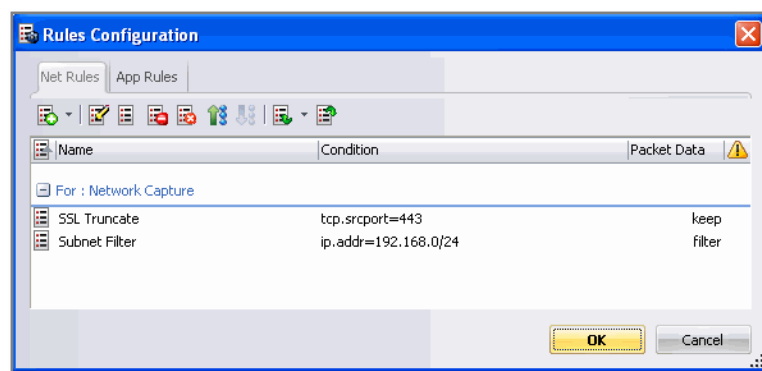
- **Add** – Click the  icon to continue adding new rules.
- **Edit** – Click the  icon to change the parameters of the existing rule.
- **Enable** – Click the  icon to make the selected rule active.
- **Disable** – Click the  icon to make the selected rule inactive.
- **Delete** – Click the  icon to remove the selected rule.
- **Promote** – Click the  icon to move the selected rule up in execution priority.
- **Demote** – Click the  icon to move the selected rule down in execution priority.
- **Import** – Click the  icon to load rules from a file and append to the rules list.
- **Export** – Click the  icon to save all rules to a file.

Caution: When you attempt to import a group of rules, Investigator checks the type of rules imported. If you are successful, a message displays the number of rules imported. If the rule type differs from the active tab type, you must re-import the group under the correct tab or select another file to import.

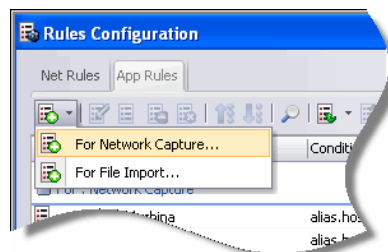
Application Layer Rules

Application layer rules are applied at the session level. Once the first application layer rule is hit, rule evaluation stops. If the first rule listed is not a match, Investigator then attempts to match the next rule listed, until a match is found.










1. From the Investigator **Edit** menu, select the **Rules** option. The **Rules Configuration** dialog displays.
2. The **Net Rules** tab is selected by default. Select the **App Rules** tab.



3. Click the **Add a New Rule**  icon. You must designate the rule type.

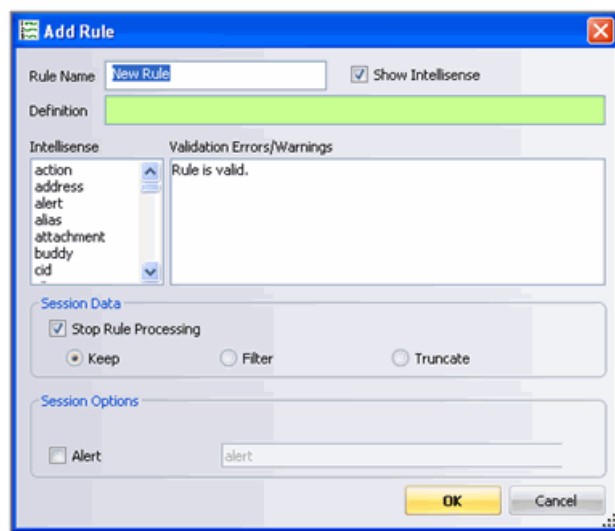


When you add a rule, the following options are available:

- **Add** – Click the  icon to continue adding new rules.
- **Edit** – Click the  icon to change the parameters of the existing rule
- **Enable** – Click the  icon to make the selected rule active.
- **Disable** – Click the  icon to make the selected rule inactive.
- **Delete** – Click the  icon to remove the selected rule.
- **Promote** – Click the  icon to move the selected rule up in execution priority.
- **Demote** – Click the  icon to move the selected rule down in execution priority.
- **Import** – Click the  icon to load rules from a file and append to the rules list.
- **Export** – Click the  icon to save all rules to a file.

When you attempt to import a group of rules, Investigator checks the type of rules imported. If you are successful, a message displays the number of rules imported. If the rule type differs from the active tab type, you must re-import the group under the correct tab or select another file to import.

4. In the **Add Rule** window, enter a descriptive name in the **Rule Name** field.

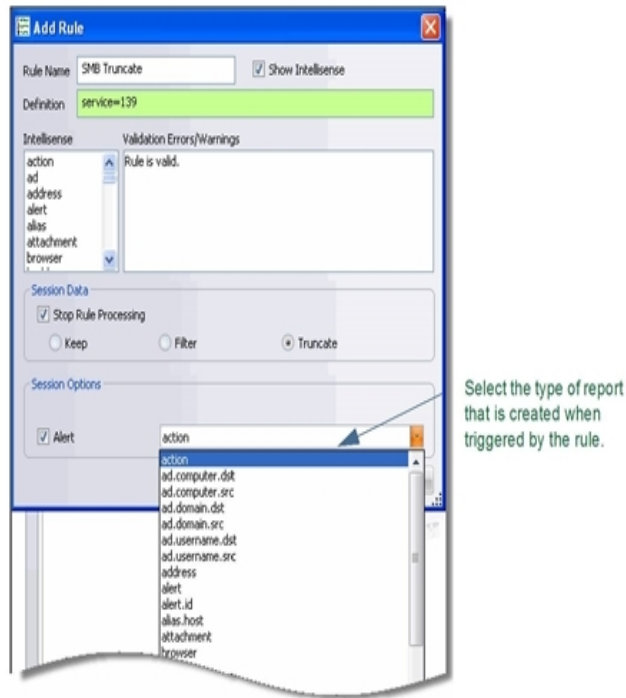


5. Complete the **Definition** field by entering directly in the field or by double clicking a meta from the Intellisense window. As you build your rule definition, Intellisense displays syntax errors and warnings.
Intellisense lets you know that the rule you created is valid.
6. In the **Session Data** area, specify the action for the new rule.
7. In the **Session Data** area, indicate whether you want an Alert to be created and verify that the new rule is valid.
8. Click **OK** to submit the rule.

| Rule Action | Description |
|----------------------|---|
| Session Data | |
| Keep | The packet is saved when it matches the rule. |
| Filter | The packet is not saved when it matches the rule. |
| Truncate | The packet payload is not saved when it matches the rule. |
| Stop Rule Processing | If checked, further rule evaluation ends if the rule is matched. The session is saved as indicated. |
| Session Options | |
| Alert | The packet generates a custom metadata when metadata matches the rule. |

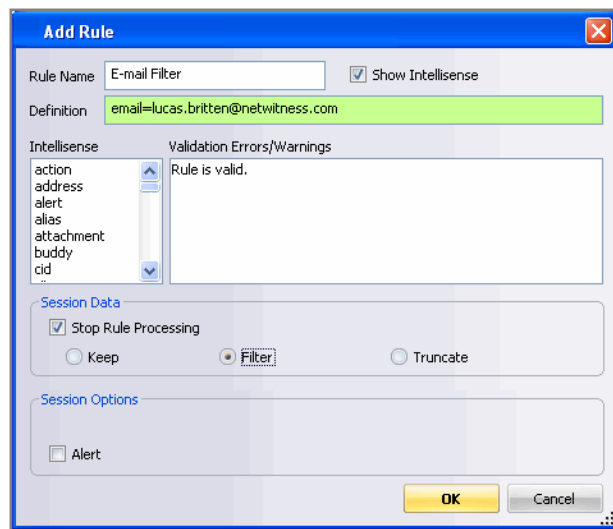
Sample Application Layer Rules

1. Truncate SMB – **service=139**
Rule Action – Truncate



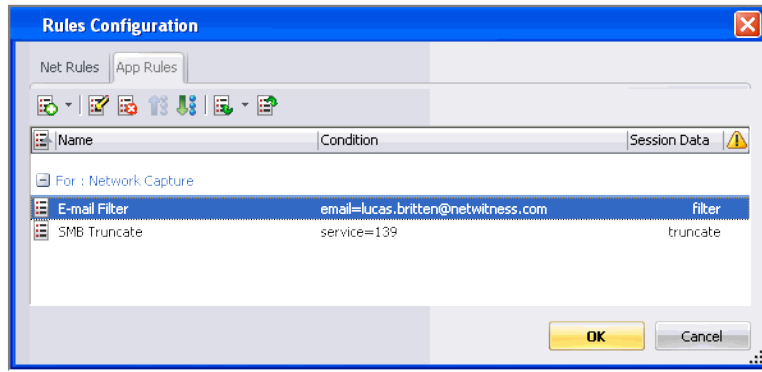
2. E-mail Filter to retain a specific e-mail address– **email= name@company.com**

Rule Action – Filter










Working with Application Layer Rules

When several Application Layer Rules exist, you can edit or delete rules or change the priority of the rules.



When you select a rule, the following options are available:

- **Add** – Click the  icon to continue adding new rules.
- **Edit** – Click the  icon to change the parameters of the existing rule.
- **Delete** – Click the  icon to remove the selected rule.
- **Demote** – Click the  icon to move the selected rule down in execution priority.
- **Promote** – Click the  icon to move the selected rule up in execution priority.
- **Import** – Click the  icon to load rules from a file and append to the rules list.
- **Export** – Click the  icon to save all rules to a file.

Note: When you attempt to import a group of rules, Investigator checks the type of rules imported. If you are successful, a message displays the number of rules imported. If the rule type differs from the active tab type, you must re-import the group under the correct tab or select another file to import.

Capture Configuration

1. From the Investigator **Edit** menu, select **Options**. The **Options** dialog displays. The default focus is on the **General** tab.
2. Click on the **Capture** tab.

The three areas to configure are:

- **Network Adapter**– Select the appropriate adapter for your network.
The default network adapters available are set at installation. Consult your System Administrator for more information
- **Advanced Capture Settings**
 - **Max Disk Usage**–The percentage of drive space allowed to be used by the system.
If this value is 100, the drive is allowed to fill up completely.

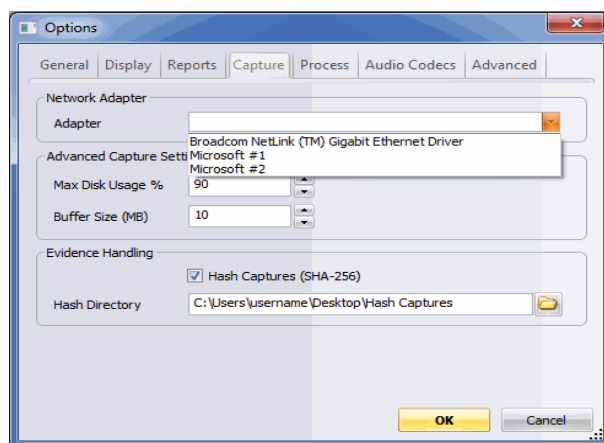
- **Buffer Size(MB)**–Specify the size in MB that is used to cache packets on the network card.
- **Evidence Handling**– Specify whether **Hash Captures** are to be saved and their file location.

Capture Configuration Settings

The **Capture** tab controls the **Network Adapter**, **Advanced Capture Settings**, and **Evidence Handling**. This is where you set the parameters for disk usage and hash files.

Network Adapter

Verify that the appropriate setting is being used.



There are three wireless capture devices available:

- **packet_netmon_** (Microsoft Netmon)
- **packet_mac80211_** (Linux mac80211)
- **packet_airport_** (Mac OS X AirPort)

Advanced Capture Settings

- **Max Disk Usage**–This setting allows the user to designate a percentage of total disk space (5% - 100%) that will be used to store collected data. For example, if this is set to 95%, then live network capture will only use 95% of the target drive for the storage.
- **Buffer**–The user designates the percentage (1% - 100%) of the drive that is reserved as a temporary storage area.

Evidence Handling

This setting allows the user to designate whether the system hashes the output **.pcap** files as they are written to the hard drive. The user can also designate where the hash value file will be written. There will be a hash file written for every **.pcap** file written.

Note: To protect the integrity of the hash values written during live capture, the user should consider designating an external drive for the hash value files.



Real-Time Network Capture

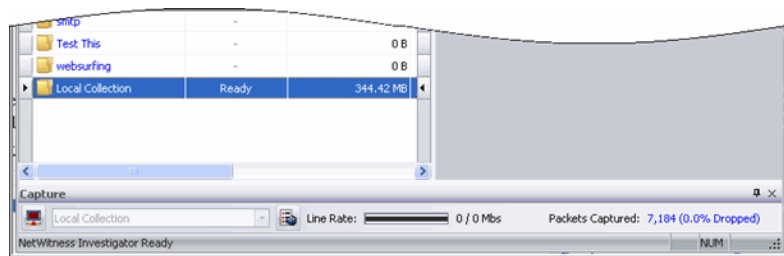
Real-time network capture allows the collection of traffic from the network using the WinPCap capture driver. NetWitness monitors on a hub, a port-spanned switch, or a passive network tap. Inserting NetWitness between your corporate firewall and the corporate intranet allows monitoring of outbound and inbound Internet traffic. NetWitness does support wireless data capture.

Note: This feature may or may not be supported under your organization's license agreement with NetWitness. Please contact your account manager for more information.

When NetWitness Investigator Collection window opens, the live traffic capture configuration options and controls are located on the Capture Toolbar in the lower panel.

Start/Stop the Live Capture

1. Verify that Parsers are correctly configured.
2. Verify that the Network Layer and Application Layer Rules are correctly defined.
3. On the Capture toolbar, click the Start  button. The Line Rate counter and the Packets Captured counter begin increasing as the device actively captures traffic. In addition, the Start  button will blink red to indicate that live capture is in process.



4. To stop the live capture, click the **Start/Stop** button again and it will stop blinking red when the capture process terminates.

StealthMode is a configuration that keeps the point of collection logically invisible to hackers or other targets. NetWitness Investigator can collect data in stealth mode on Windows XP and Windows 2003. Stealth mode is only applicable to Ethernet networks; it is not applicable to Token Ring or FDDI networks.

1. From the Start menu, select **Control Panel**.
2. Open **Network Connections**.
3. Position the cursor over a network connection and then right-click the mouse button. In the **Options** menu, select the **Properties** option.

4. In the **This connection uses the following items** panel, clear all check boxes. Click **OK**.
5. in NetWitness Investigator, select the network adapter that you want use to collect data on the Capture Configuration dialog.

Data Analysis

Data analysis is the process of looking systematically into processed network data for specific patterns of activity or content that may indicate a threat to the network or to highlight network sessions of interest.

This chapter describes the two primary methods for analyzing network data processed by NetWitness. You must become familiar with both methods so that you develop the critical ability to choose the most effective way to look at the data from your network. Every situation is somewhat unique in terms of the types of information you are attempting to find. The two methods to examine the data in a collection are:

- **Navigation** – the central mechanism for drilling into the extracted metadata
- **Search** – the mechanism to locate sessions with specified string values or regular expressions

Investigator presents the content of the captured packet as a **Collection**. The defined target metadata are shown as **Reports** and the number of **Sessions** is represented as a numerical value. When you click on one of these values at any given level, you are presented with a view of the results on the next level.

Views


You can move between the views of data in Investigator. They are presented in the order of specificity. Your familiarity and use of **Bookmarks** and **History** as well as the **Drill Path** makes navigation among the levels easier. The available views are:



- **Summary**
- **Navigation**
- **Session**
- **Content**

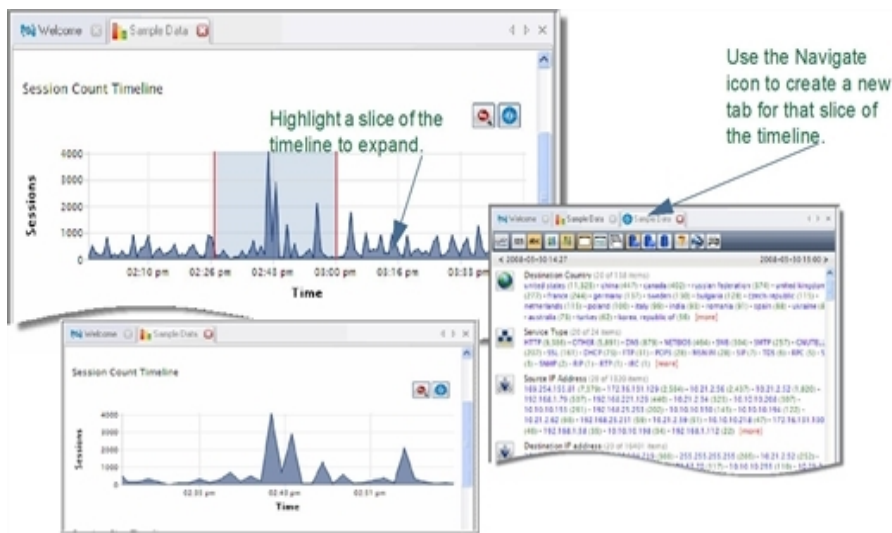
Summary View

This is the highest level that you can look at the characteristics of a selected collection. There are three snapshots displayed over the timeline.

- Session Count
- Session Size
- Packet Count


1. Highlight a **Collection** in the Investigator Collection Pane.
2. Double-click the collection to connect to the database.
3. When the **Status** displays **Ready**, click on the **Collection Summary**  icon.

In each of the snapshot views, you can zoom into a selected portion of the timeline. You can use the **Navigate**  icon to open a new tab to navigate to a selected slice of the timeline. You can return to the previously selected time range by using the **Zoom Out**  icon.



Navigation View

To begin data analysis, highlight the desired **Collection** in the Investigator Main window. The steps you utilize are simply moving from the general to the specific by selecting a more specific value to add to the drill path. There are many variations in the way you display the data. The basic pattern is the following:

1. Select a **Collection**. Click on the **Navigation**  icon to view the collection.
2. Select a **Report**.
3. Select a group of **Sessions**.
4. View the **Content** in the selected **Sessions**.
5. **Search** for specific content to determine whether it meets your threat criteria.
6. Repeat the process for the next potential threat type in your network.

Note: There may be circumstances that cause you to alter the order or deviate from this

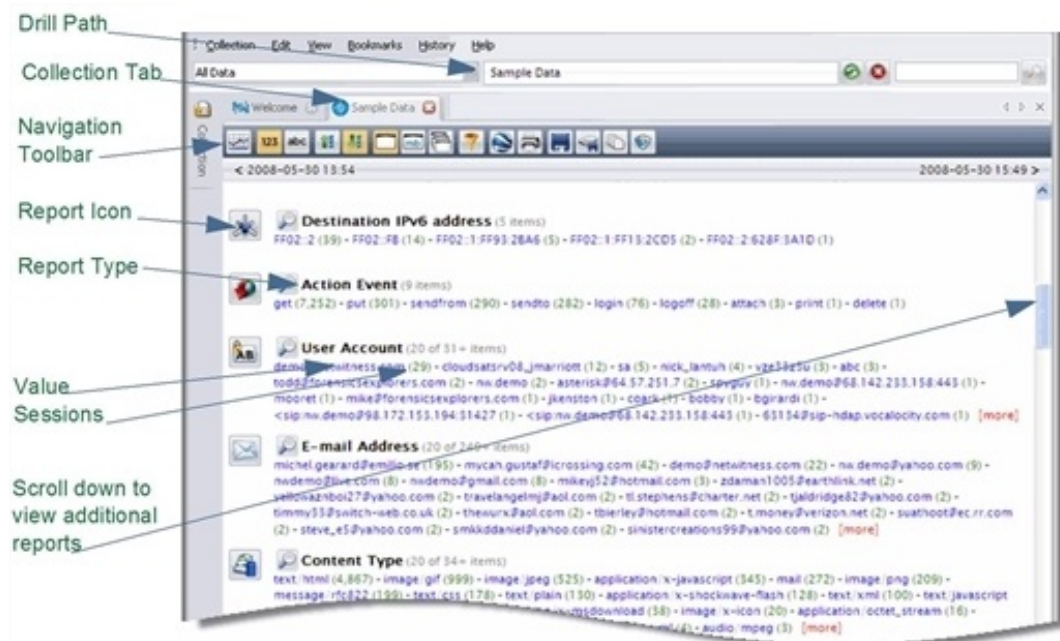
basic pattern. Your general knowledge about network traffic and that of your organization determines the perception of anomalous activity and how you use Investigator to look more closely.

7. Select a **Collection** and double-click the name to connect to the database.

8. When the **Status** field shows **Ready**, click on the **Navigation**  icon on the toolbar.

The listing displays the processed reports (e.g. **Address**, **E-mail Address**, **File**, etc.). Each of the report types lists the report values and the associated session counts. Generally, it is useful to narrow the scope of your drill in order to reveal the amount and type of activity you are searching.

In this illustration, the reports are ordered to display **Destination Country** first, so a concern is evident for suspicious traffic with foreign countries.

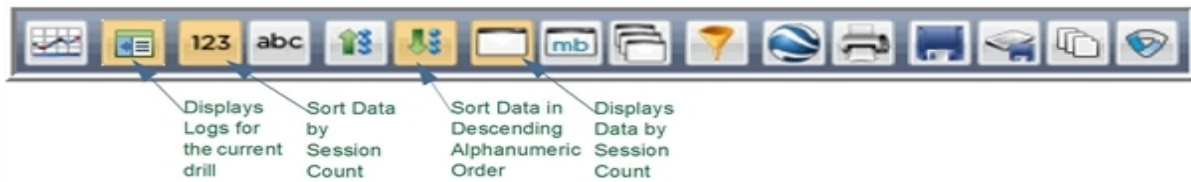


- **Drill Path**—Shows the items you have selected as part of your analysis (This allows a quick method for stepping back to an earlier view of the data.)
- **Collection Tab**—Shows the active collection in this view
- **Navigation Toolbar**—Controls the appearance of the reports and the data
- **Report Icon**—Symbol for the report with a context menu for results display
- **Report Type**—The items selected in the **Collection** configuration (metadata fields)
- **Value**—The instances in the collection that match the **Report Type** (20 are displayed by default)
- **Sessions**—The number of instances identified in the network data containing the specific metadata


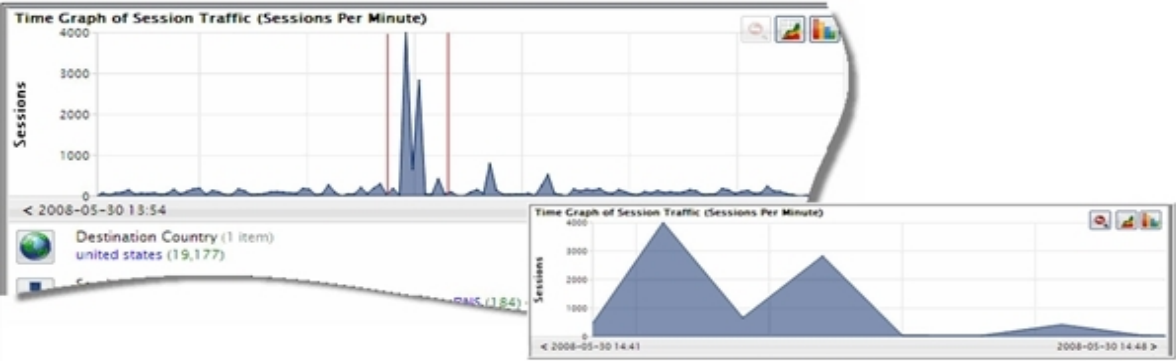

Navigation Toolbar

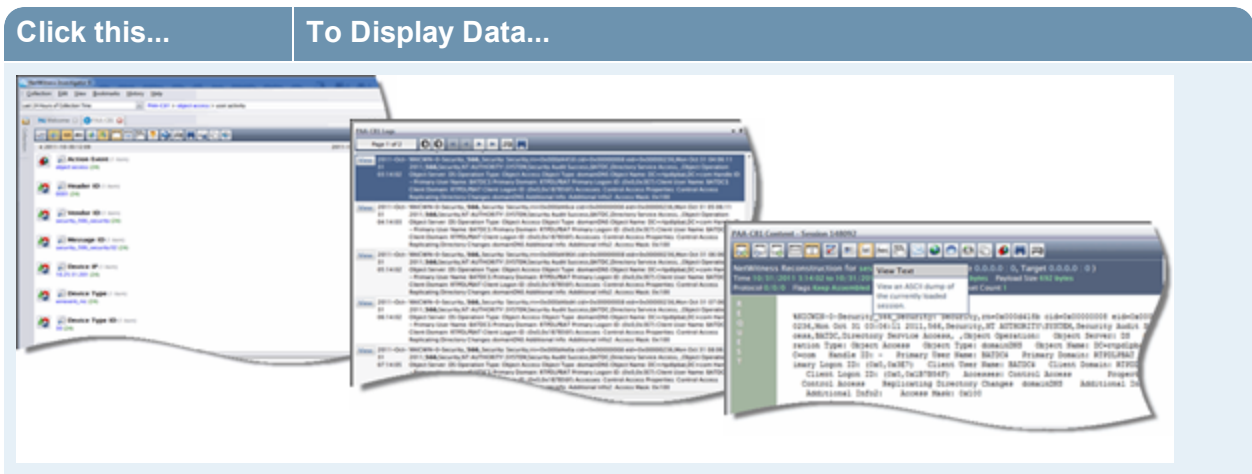
The appearance of the collection reports and the data contained are determined by the combination of selections you make on the **Navigation** toolbar.

When you first install Investigator, the default settings are highlighted:



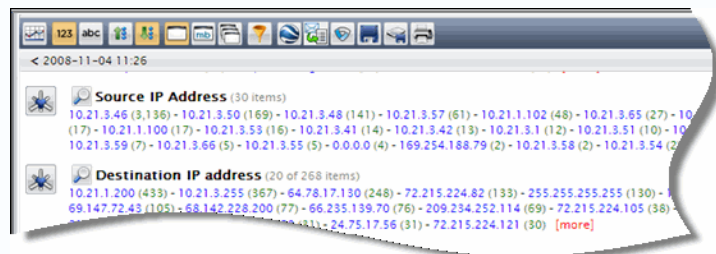
As each icon is selected, the resulting view is displayed in the following table:

| Click this... | To Display Data... |
|--|---|
| <p>Time Graph</p>  | <p>Time Graph—Shows session traffic (sessions per minute) in your current drill. You can select a part of the graph to expand the view.</p>  |
| <p>View Log Data</p>  | <p>Log Data—Shows the log packets created by the Series 4 Log Decoder for the current session. You can select a particular log event to view as a text file for more information.</p> |



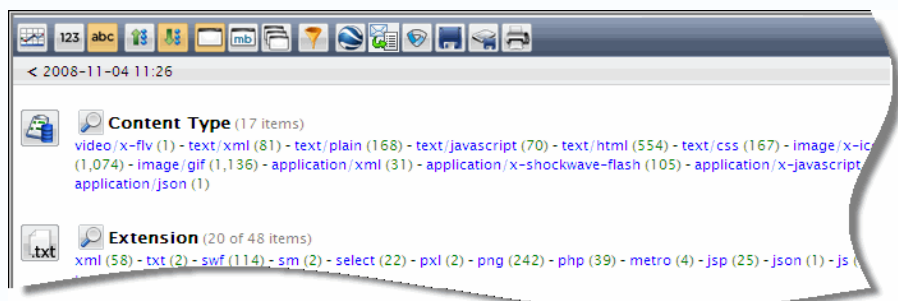
Sort Data

123 Order by Total—Arranges the data by number of sessions.




When you sort the values by the number of session counts, the default descending setting is still operant.

abc Sort Alphanumeric—Arranges the data by alphabetic order. If there are numbers as part of the value or alias, they will precede the first alphabetic value.

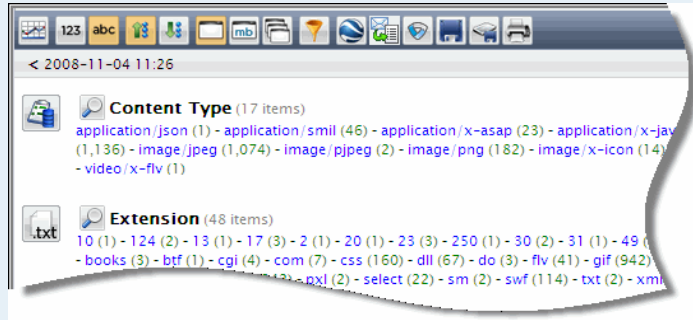


When you sort the data by alphanumeric order, the default descending setting is still operant.

Arrange Data

 Ascending Sort:
 Numeric—Arranges the data from least to greatest.
 Alphabetic—Arranges the data in a-z order.

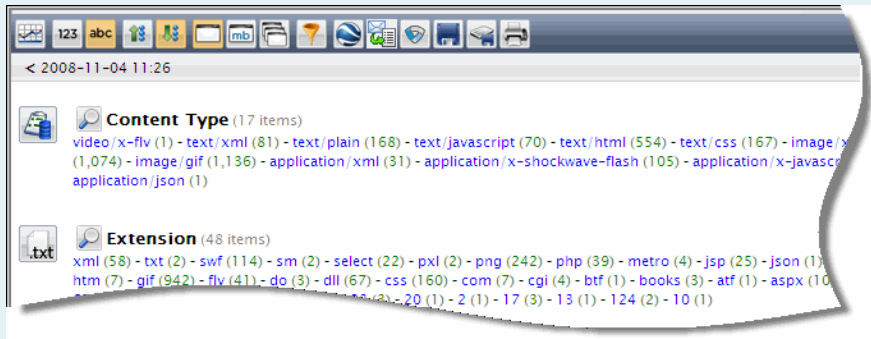
Click this... To Display Data...



When you sort the data in ascending order, the alphabetic order setting is still operant.



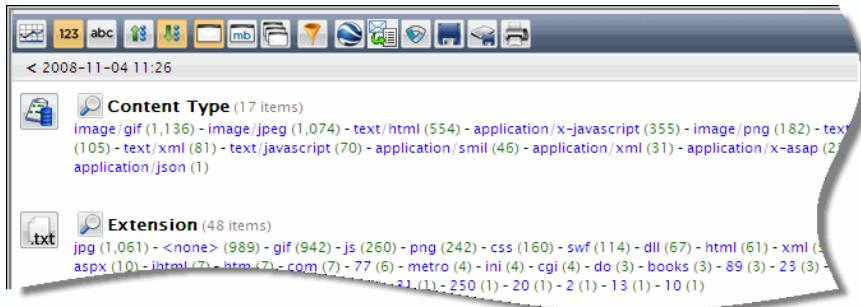
Descending Sort:
 Numeric—Arranges the data from greatest to least.
 Alphabetic—Arranges the data in z-a order.



Session Quantifier

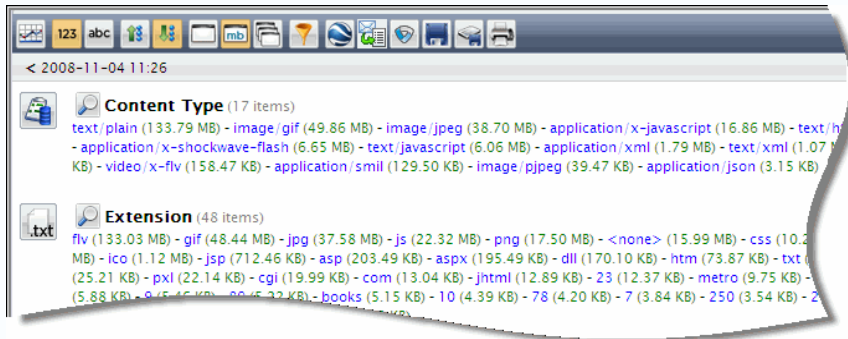



Session Count—Displays the metadata by session count.
 The values are displayed according to the greatest number of sessions for each value in descending order.

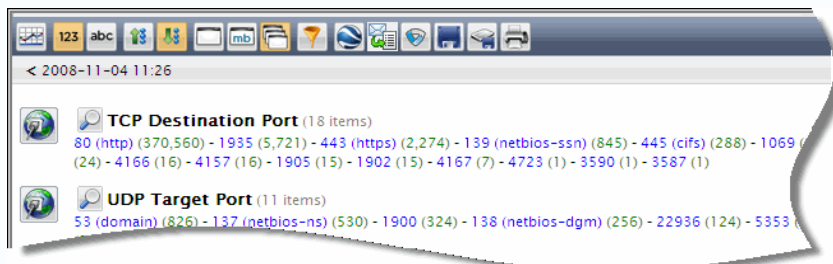


Session Size—Displays the metadata by session size total.
 The values are displayed according to the session size for each value in descending order.

Click this... To Display Data...



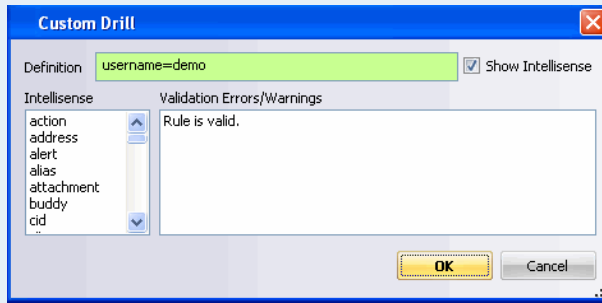
 Packet Count—Displays the metadata by packet count
The values are displayed according to the number of packets for each value in descending order.



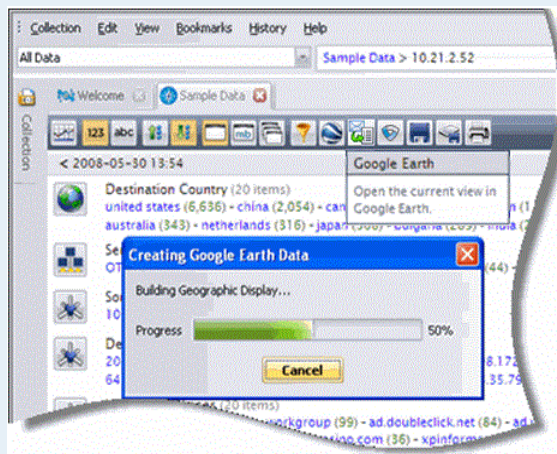
Actions

 Custom Drill—The user defines the drill criteria.

Click this... To Display Data...



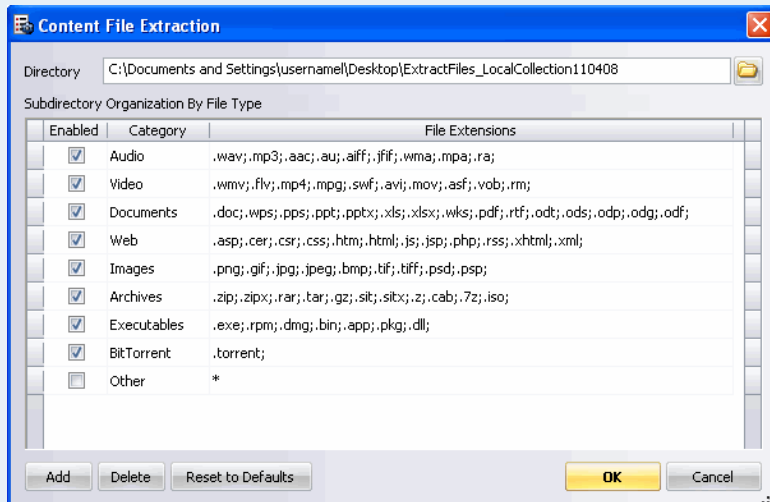
View the Session in Google Earth—Using Shift +  icon bypasses the dialog box and displays the last session viewed.



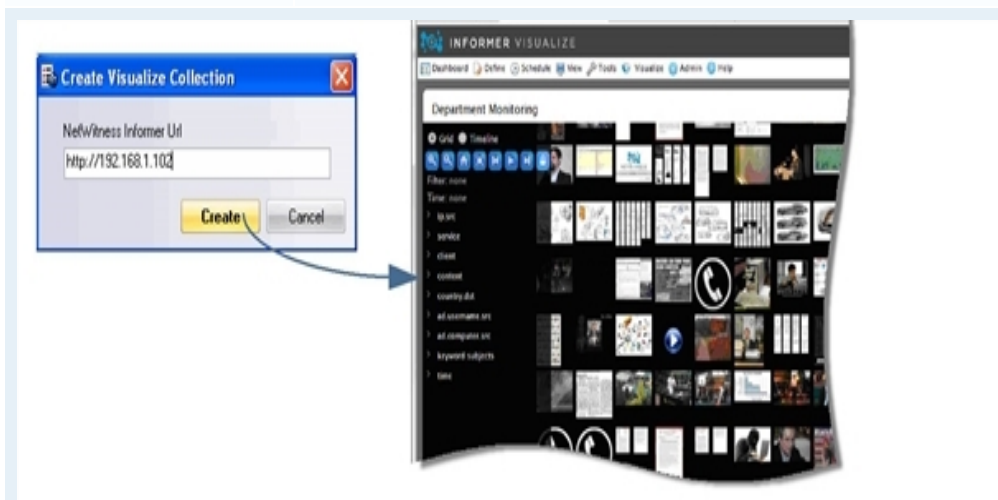
File Extract—Extract files from common protocols into a local directory.

Click this...

To Display Data...

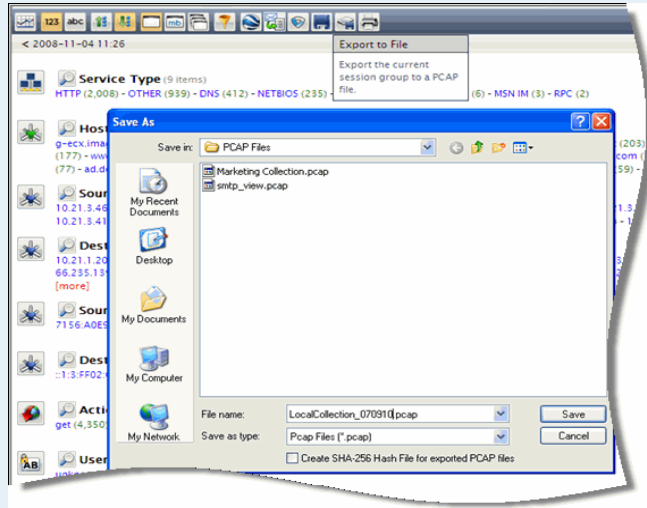


Visualize Collection—Create a visual collection using NetWitness Informer from the current drill.

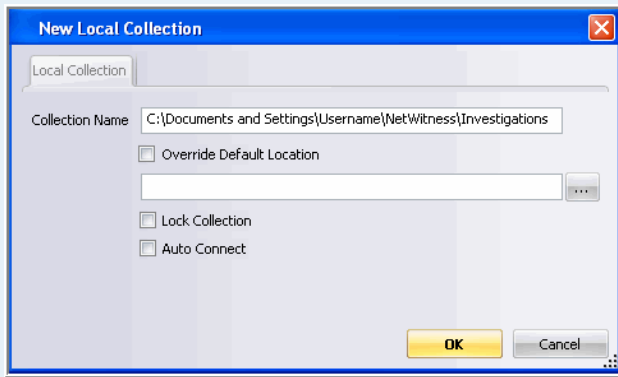


File Export—Export the current session group to a pcap file in a local directory.

Click this... To Display Data...



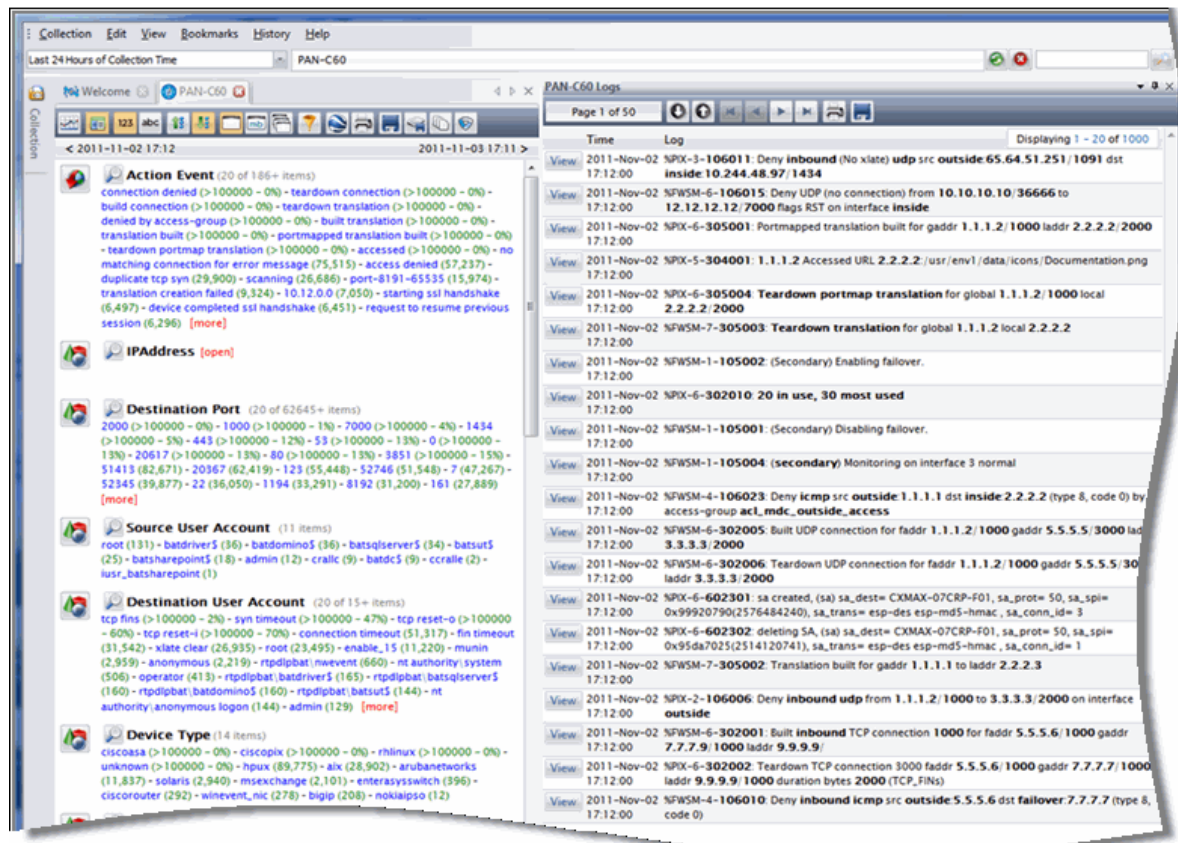
Session Group Export—Export the current session group to a new collection.



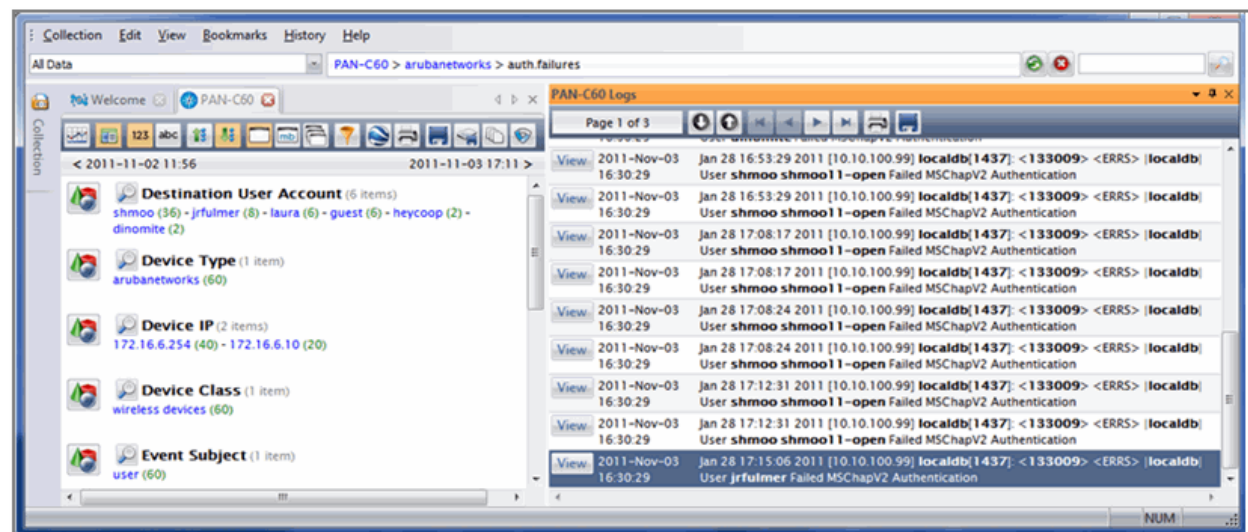
Print—The displayed content is printed.

View Logs

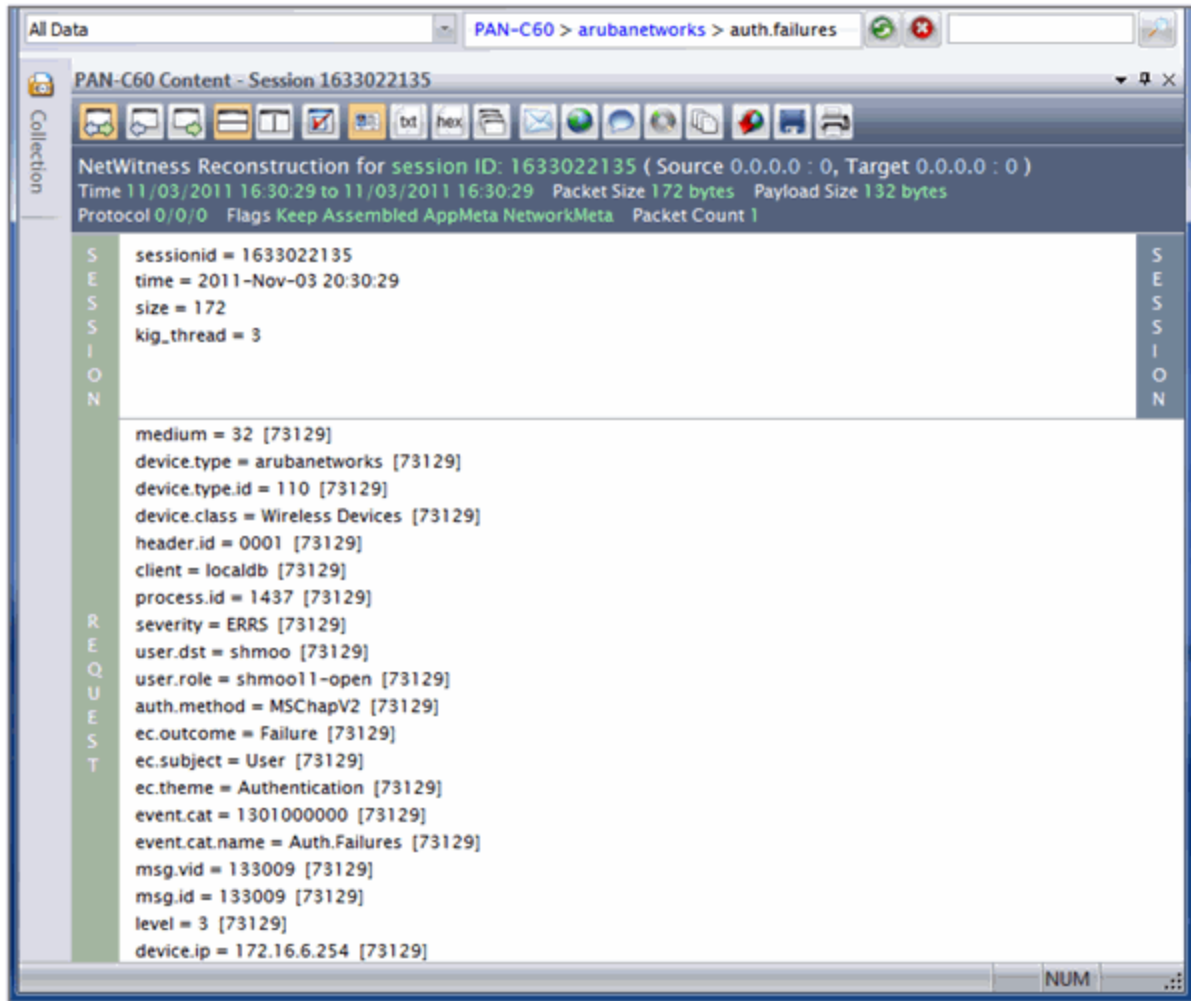
When LogDecoder is part of your organization's architecture, the Log Data icon  displays the raw log in time order.



When you drill into the meta, the Logs View pane updates to reflect that content.



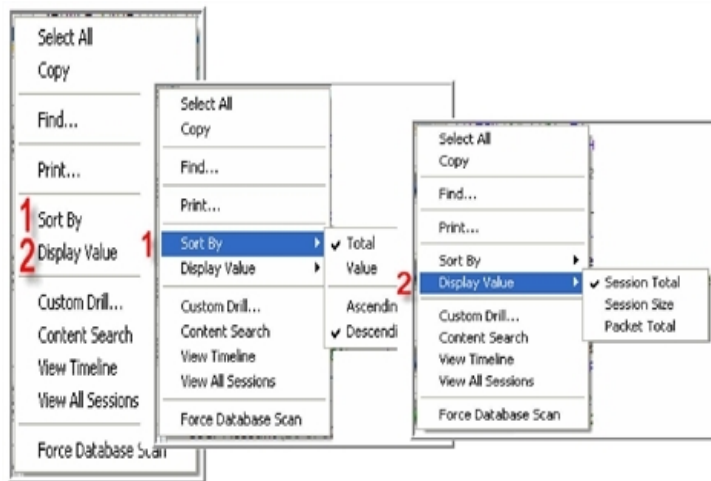
If you click on the View button for a specific log event, you can view the details for the currently loaded session.



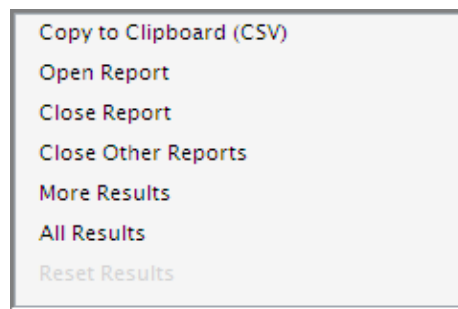
Context Menus

When you right-click in a pane (**Collection** or **Navigation**) on the Investigator screen, a **Context** menu opens. The functions on the toolbar, such as **Print** and **Custom Drill**, are accessible, as well as current settings.

Navigation Context Menu



The reports display the first 20 results by default. If [open] or [more] is displayed at the end of the list of value, that means that there are more results that you can view. When you click on a **Report** icon, the following options are available:



If the options are greyed out, they are not available from the current view.

| Option | Description |
|-------------------|--|
| Copy to Clipboard | Copies comma separated values (CSV) |
| Open Report | To open the report, the user must confirm that the process may be time consuming the <div data-bbox="649 1465 1071 1696" data-label="Image"> <p>The image shows a 'Confirm Open' dialog box with a question mark icon. The text inside reads: 'This report may contain a lot of data and could take a long time to retrieve. Are you sure you want to proceed?' Below this is a checkbox labeled 'Don't ask this question again.' and two buttons labeled 'Yes' and 'No'.</p> </div> Confirm Open dialog: |
| Close Report | Returns the display to hidden |

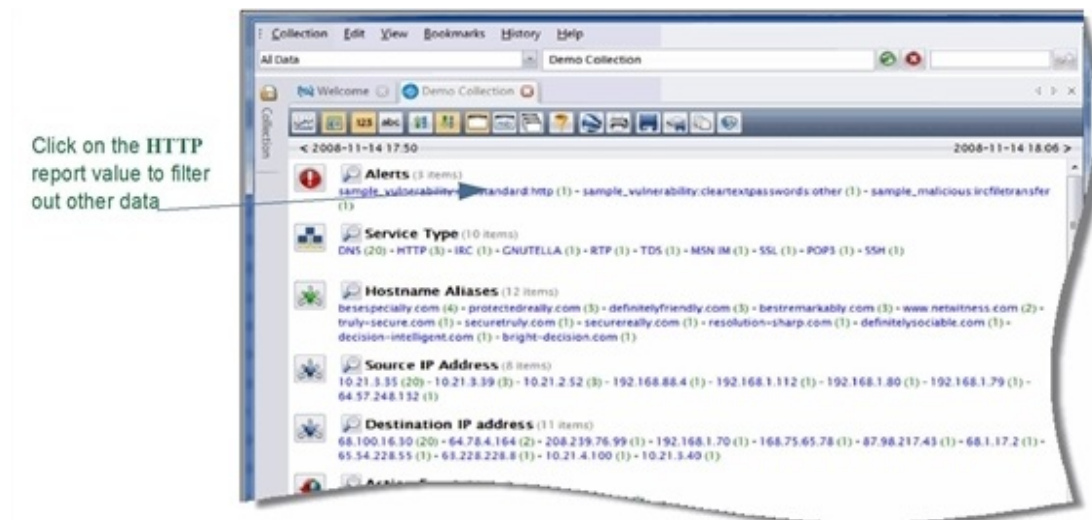
| Option | Description |
|---------------------|---|
| Close Other Reports | Closes all the reports |
| More Results | Displays an additional 20 values |
| All Results | When there are large numbers of results, the user must specify a maximum number (1000, 2500, etc. to 50,000) to display |
| Reset Results | Returns the display to the original default 20 values |

Drills and Filters

There are many possible approaches for analyzing the data with Investigator. The primary purpose of this chapter is to show how you can use the Investigator features. As you become more familiar with the application, your preferred approach may vary from what is presented in this guide.

Clicking on a **Report Value** in the collection removes all items not associated with the chosen value. This is useful because you are able to see patterns in events more easily. You can also create a separate tab when you drill into a value or session group. The decision whether to continue to extend the drill path in one tab, to create a separate tab for a secondary drill, or to create a new tab with the last level as the root for the drill path depends upon your experience and personal preference.

If a user were interested in HTTP activity with foreign countries, especially activity that contained javascript files, a preliminary method for analysis of their network data is provided in this chapter.



In order to keep the drill path clear, a new tab is needed for this drill.

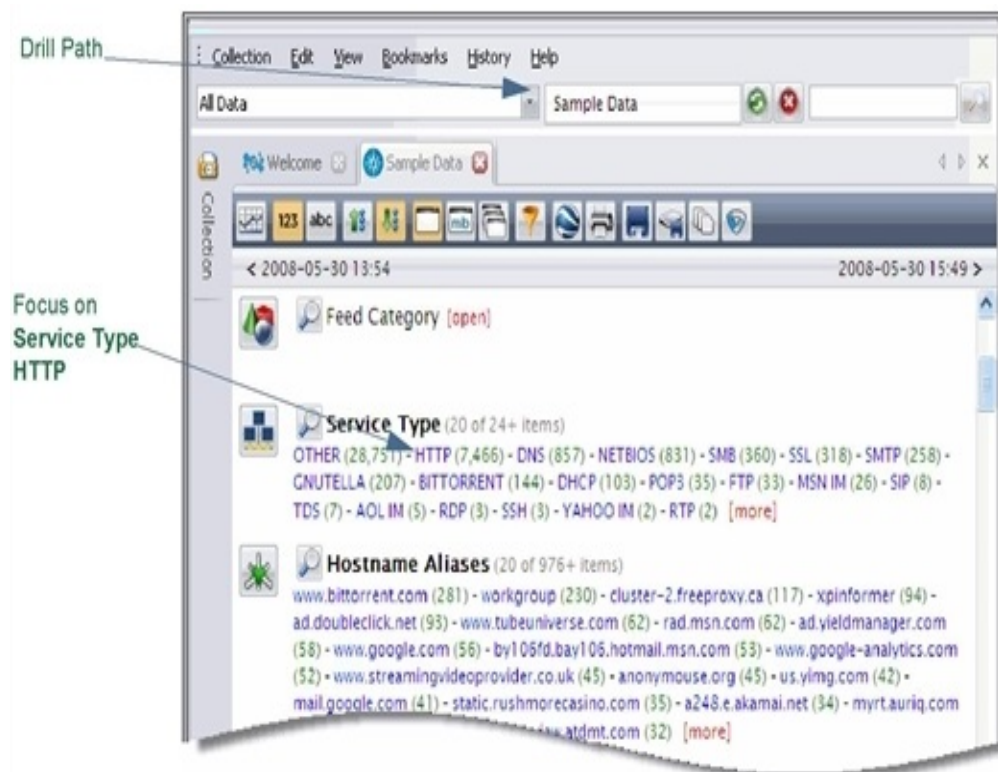
Create a New Tab

This can be done on the report value level or on a specific value

- **Ctrl +Click** on the report to open a separate tab.
- **Alt +Click** to make the report value the root of the **Drill Path** in a separate tab.

As you drill further into the collection, having these separate tabs improves your ability to go back and refine the drill and look more closely at items of interest.

The new view of the data has filtered out the other **Service Types**.

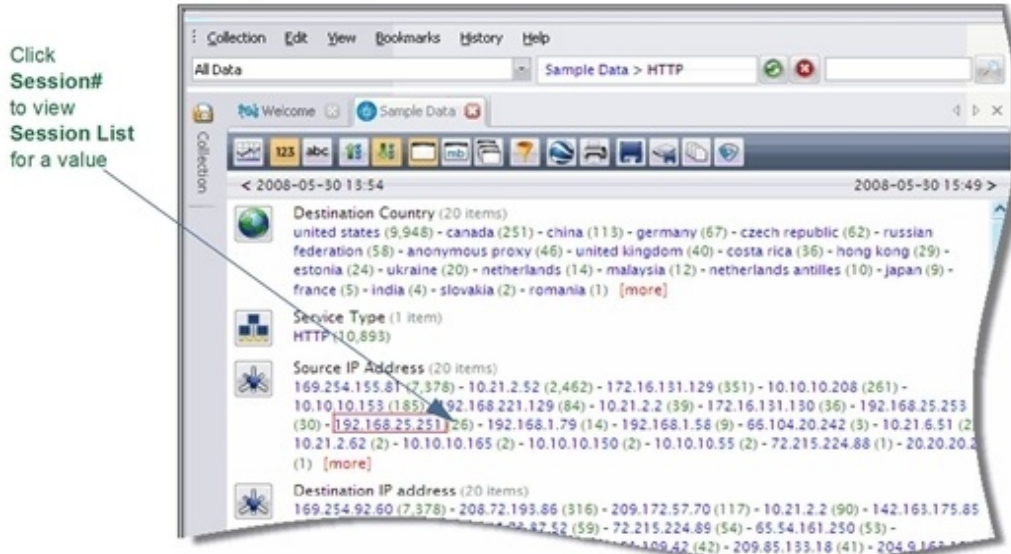


At this point, you must evaluate the **Report Values** and **Session** counts to determine the next item of interest. Possible drills of interest might include an additional filter for:

- A **Destination Country (China)**
- A specific **Source IP Address**
- A **Destination IP Address**
- An **Action Event** with an unusual number of sessions (**get**)

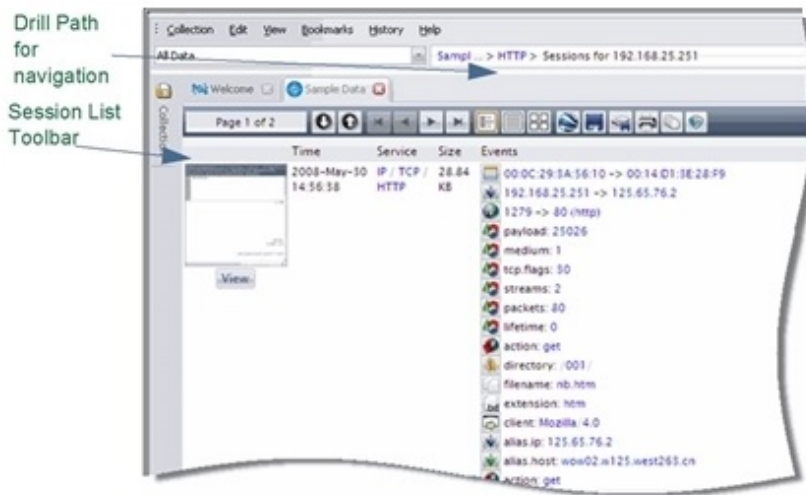
View Sessions

Once the focus of the analysis has been narrowed to a particular type of event, clicking on the number opens the drill to the **Session** level.



Session View

The **Session** view displays a representation of all the sessions that correspond to the drill from the **Navigation** view. For example, if a user clicks on a session count of 26 to the right of a particular **IP Address** in the **Navigation** view, the resulting 26 sessions will be listed on the **Session List** view.













You can use the **Session List** toolbar to:

- Move through the pages of sessions.
- Change the way you view the sessions.
- View the sessions with Google Earth.
- Export or print the session information.


Session List Toolbar

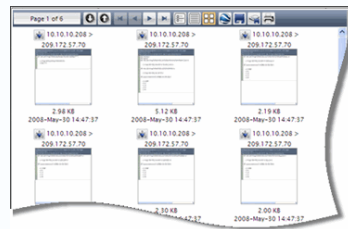
This toolbar facilitates moving among the individual sessions for the chosen **Report** and **Value**. The appearance of the collection reports and the data contained are determined by the combination of selections you make on the **Navigation** toolbar.

| Function | Description |
|---|---|
| Paging Control | |
|  | Click directly on the Page Display to open the Go To Page dialog box. This lets you move to a specific page of sessions without paging through each group of sessions. This session group contained only 26 sessions, but often values are considerably larger. Other ways to find a specific session are using Bookmarks and History.> |
|  | Next Session– Moves the view to the next session |
|  | Previous Session– Moves the view to the previous session |
|  | First Page– Moves the view to the first page |
|  | Previous Page– Moves the view to the previous page |
|  | Next Page– Moves the view to the next page |
|  | Last Page– Moves the view to the last page |
| Display Control | |
|  | Hybrid View– Displays the session details and thumbnails. |
|  | |
|  | Event View– Displays each session on the page in one line (Time, Service, Size, Events) with hyperlinks to create a new drill. |





| Function | Description |
|----------|-------------|
|----------|-------------|



| | |
|---|--|
|  | <p>Thumbnail View– The sessions appear as thumbnail images. This serves as a preview for session content. Click on the image to view the content for that session.</p> |
|---|--|



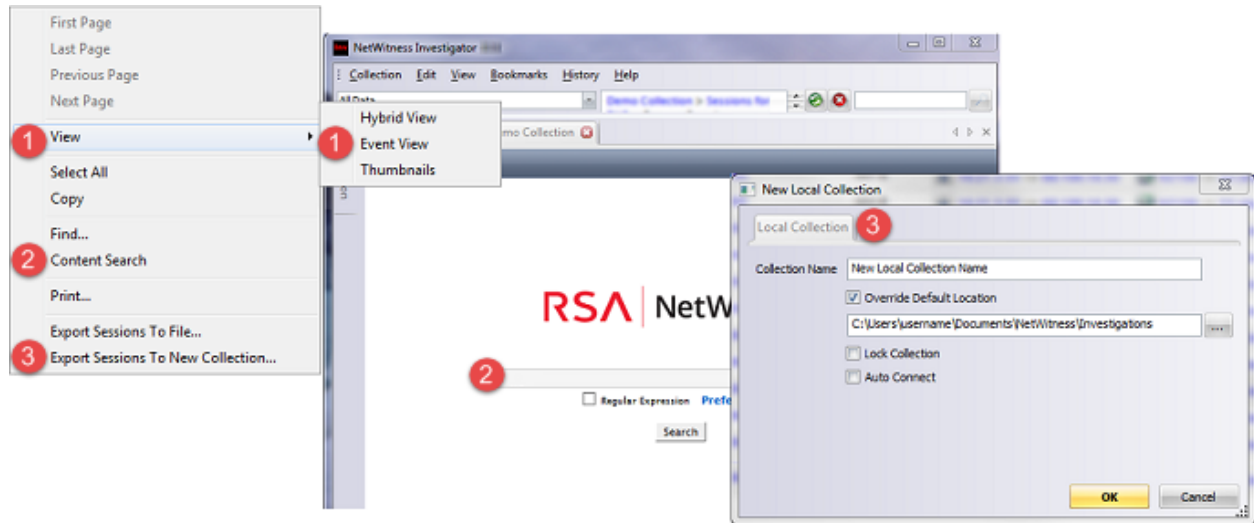
Actions

- | | |
|---|---|
|  | <p>Google Earth Session View– Displays the session on Google Earth</p> |
|  | <p>Export to File– Export the sessions in the current Session View list to a.pcap file.</p> |
|  | <p>Export to Collection– Export the current session group to a new Collection.</p> |
|  | <p>Print– Print the session information in the current view.</p> |

More Context Menus

Several of the functions on the toolbar (**Paging, View, Print,**and **Export to File**) are also available by right-clicking any place on the Investigator **Session View** screen. The **Context** menu opens.

This Context menu allows you to create a new collection without leaving the current view.




Display Sessions on Google Earth

This feature uses Google Earth to map session activity from source and destination IP addresses, using the **GeoIP2** database.

Note: You must enable the **GeoIP2** parser to see this functionality.



Content View

To view the content in a particular session, you click on the Thumbnail View  icon. A separate pane displays the content detail for that session. You can select any one of the following formats on the **Content Toolbar**.



Content Toolbar

When you view content, Investigator selects the probable best format, based on the collection's type of service. Once you open the **Content** view, you are able to change from the default **Auto** to any of the other options.

Click this... To view this...



View Both Sides

Show both the request and response for the currently loaded session.



View Request

Show only the request for the currently loaded session.



View Response

Show only the response for the currently loaded session.



Top to Bottom

Alternate request and response packets from top to bottom.



Side to Side

Alternate request and response packets from left to right.



Best Reconstruction

View data in Auto format, which allows Investigator to select the format.



View Details

View meta information for each side of session (IP address, port, number of packets, bytes for

Click this... To view this...

 Data and Payload, and Flags, if applicable).

 View Text

View data in text format.

 View Hex

View data in Hex format.

 View Packets

View data in packet format.

 View Mail

View data in Mail format.

 View Web

View data in Web format.

 View IM

View data in IM format.

 Play Audio

Access data in audio (VoIP) format.

 Files

Extracts all files found in the session.

 Open PCAP

Open the currently loaded session as a PCAP.

 Export Session

Export the currently loaded session.

You can continue to explore the data through drilling into specific items, search the session for a particular term, string, or other values

Search View

NetWitness Search allows users to search collections for keywords and regular expressions (pattern matches). You have the option to create a new search or use any combination of various common search criteria (e.g. social security numbers, credit card numbers, EIN tax numbers) found in a compiled library.

The following describes the capabilities of the NetWitness Search engine and explains the various options that users have when searching through their NetWitness data.

Quick Search

To perform a simple search on a report using operators:

1. Open and navigate to a collection from the list of NetWitness Collections. Click the **Quick Search**

 icon found next to the name of a report.

A dropdown menu with operators displays.



2. Click Drill to perform a search using the new criteria.

Simple Search

To search a collection:

1. Open and navigate to a collection from the list of NetWitness Collections. In the Content pane, right-click in an empty place and select **Content Search** from the context menu.
2. The **Search Dialog** displays, which allows users to create and run ad hoc searches on either a keyword or a regular expression.



You could expand the search to include metadata by changing the settings in **Preferences**. You could also specify that your search criteria are to be **Case Insensitive**, if necessary.

3. The user has the option to designate whether or not the search is in the form of a regular expression by making the appropriate check in the Regular Expression checkbox. If **Regular Expression** is enabled, but the search string entered by the user is not a valid regular expression, NetWitness

notifies the user of an invalid query. If **Regular Expression** is not enabled, the search engine treats the search string as a keyword.

NetWitness uses the Boost Perl regular expression engine. All regular expressions must be formatted in the appropriate syntax. More information about the Boost Perl regular expression library and syntax can be found at the Boost Homepage

4. Click on the Advanced  icon in the upper-left corner of the **Search** screen to go to **Advanced Search**.

Search Preferences

Before initiating either a **Simple** or **Advanced Search**, You can set or change your search preference options by clicking on the **Preferences** text beneath the search box.

- **Search Content:** This is the default setting.
- **Search Metadata:** If this option is enabled, NetWitness will search the metadata for each session as well as the content. By default, NetWitness Search only searches through the content of a session.
- **Decode Sessions:** Often, the payload of a session will be compressed, usually in a gzip format, to reduce the amount of information sent over the network. If this option is enabled, NetWitness attempts to decompress the content of every session it searches to find a match for the search. Many web pages are gzipped on the web service and unzipped by the web browser. NetWitness also unzips the content so that the search engine can search through the original plain text.

Note: This option does not mean that NetWitness decrypts the content of a session and extract matches from encrypted traffic.

- **Case Insensitive:** This option designates whether the search should be case-sensitive.

Advanced Search

Advanced Search allows users to create a more advanced search and save that search to a search library for future use or use one of the many pre-packaged searches that are standard with NetWitness Investigator.

In the **Advanced Search** dialog, users can select from saved searches by clicking on the drop down menu, located to the right of **Search Name**. This list includes all default searches along with any other advanced searches created and saved by the user.

RSA | NetWitness

Search Name:

New Search Delete Search

Search Description:

Search For:

Regular Expression [Preferences >](#)

[Reload Default Search Criteria](#)

Convert ASCII:

To Unicode:

The **Search Description** box is used to describe each saved search.

RSA | NetWitness

Search Name:

New Search Delete Search

Search Description:

Search For:

Regular Expression [Preferences >](#)

[Reload Default Search Criteria](#)

Convert ASCII:

To Unicode:

If you are creating a custom regular expression, it is often useful to include which strings will match the saved regular expression and which will not. See the description of Social Security Numbers as an example of how to best save the description of a new regular expression.

The actual search pattern (or text) is specified in the text box next to **Search For**.

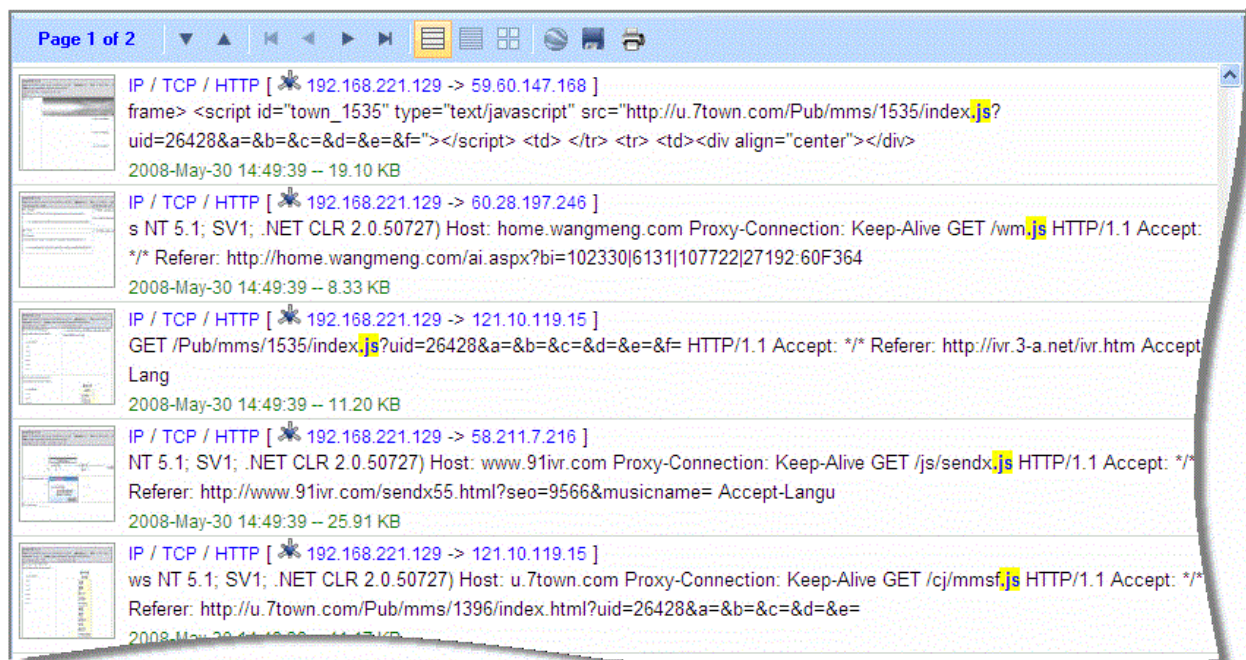
Advanced Searches created by a user must be given a name, description, and search string before they can be saved. These saved searches continue to exist until they are deleted by selecting the search to be deleted and clicking the **Delete Search** text.

If one of the original **Advanced Searches** is changed, the user can revert to the default criteria by clicking **Reload Default Search Criteria**.

Search Results

The search for .js files in the 84 sessions from IP Address 192.168.221.129 produced two pages of results.

The original search results show all .js files in bold. When you enter .js in the search field a second time, each instance in the results is highlighted.





Session List View

Regardless of the type of search, the engine returns all instances of the search criteria in the following form:

- A thumbnail of the matching session
- The service type of the matching session (e.g. HTTP, FTP, MSN IM, etc.)
- The source and destination IP addresses and ports

- The chunk of text in which the search term was found
- The time stamp of the beginning of the matching session
- The size of the matching session

Once any results are displayed, the user can use the NetWitness **Search** toolbar to execute any of the following actions:

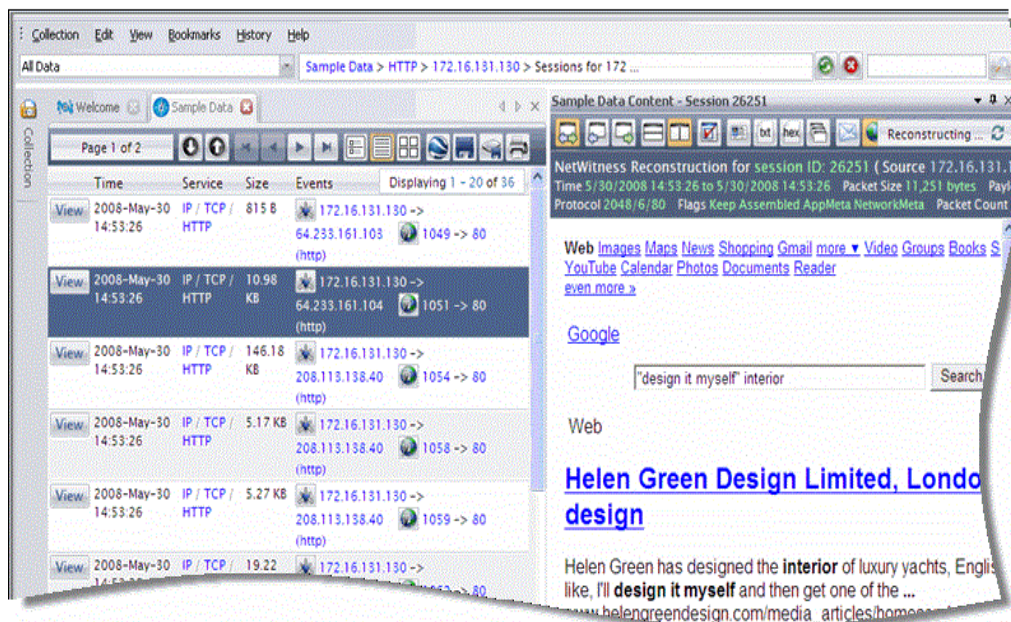
- Export the results to another collection for further searching and navigating (Click the Export  icon on the toolbar)
- Export the results to a **.pcap** file (Click the Export  icon on the toolbar)
- Page through the results using the paging controls on the top toolbar
- Change the number of results displayed per page.
- Jump to a specific page of the result set
- Initiate another **Simple Search**

The top bar will also give feedback as to the number of sessions that contained a match. Another way to export the results of a NetWitness Search is to right click the body of the results page and select Export Sessions.


Content View

To open and view the content of a search result, either click on the pre-generated thumbnail or the search term in the content snippet.

Note: The matching search text will be in bold text to make the match stand out from the other text.



NetWitness Search Tips

- A NetWitness **Search** can be stopped at any point by clicking on the **Stop**  icon while the search is in progress. Stopping the search leaves any of the already displayed results on the page.
- An **Advanced Search** can be initiated from the results page by clicking on the **Advanced Search** text underneath the input box.
- NetWitness **Search** maintains a record of the last 10 searches. This list drops down automatically when the user begins a search in the text box.
- NetWitness **Search** caches the results of each search so that the search can be repeated very quickly.
- Multiple search windows can be open and running at the same time. The user is advised that the number of simultaneous searches may affect the overall performance of NetWitness Investigator, especially when NetWitness is collecting in a sustained mode with heavy traffic volumes.

Rules

Network layer rules are applied at the packet level and are made up of rule sets from Layer 2 – Layer 4. Multiple rules may be applied to multiple layers (for example, when a network rule filters out specific ports for a specific IP address.)

Application rules are used to define the data collected by the NetWitness system at the session level. A rule can be used to either include or exclude all traffic not otherwise selected. NetWitness processes rules in the order they are listed in the **Rules Configuration** dialog. A default rule, if used, must always be placed at the bottom of the rule list. Otherwise, rule processing stops as soon as the default rule is evaluated since, by definition, all traffic is selected by the default rule.

A general rule of thumb for order of rules is to have **filter** and **truncation** rules set as the first rules to be tested. Then any **alert** rules follow. Finally, any additional **keep** or **filter** rules would be placed at the very bottom of the list.

Packet Data Options

When creating or working with both network and application rules, one of three actions can be performed, based on a rule match:

- **Keep** – Keeps or retains the data based on a match.
- **Filter** – Filters the data based on a match.
- **Truncate** – The payload information is not saved, but the metadata elements are retained.

Note: If the criteria match, no subsequent rules will be evaluated, if the Stop Rule Processing checkbox is checked.

Session Options

For **Network Rules**, when choosing to **Keep** or **Truncate** a rule, the following options are available:

- **Network Meta**–When selected, the capture system directs those packets to the component that will extract network meta elements (i.e. MAC Address, IP address, tcp/udp port information, etc.).
- **Application Meta**–When selected, the capture system directs those packets to the component that will extract application meta elements (i.e. hostnames, filenames, e-mails accounts, passwords, etc.).
- **Alert**–Creates a new meta element when the rule criteria matches. The new meta element is listed under the Alert field and the value of the meta element will be the name of the rule.

For **Application Rules**, when choosing to **Keep** or **Truncate** a rule, the following option is available:



- **Alert**– Creates a new meta element when the rule criteria matches. The new meta element will be under the alert field and the value of the meta element will be the name of the rule.

Rule Order

Both network and application rules are applied in a top-down order. When a specific rule is matched, the operation and options are acted upon. At that point, if the **Stop Processing** flag is checked, then no further rules will be applied for that session. Rule evaluation will continue if **Stop Processing** checkbox is unchecked.

For example, if there are three network rules and three application rules defined and network rule #2 has the **Stop Processing** option checked. If network rule number 2 is matched for a session which designates a **Keep**, then network rule number three will not be applied. The application rules will then be measured against that specific session.

Rule Sets and Expressions

Groups of capture rules form rule sets. These rule sets can be imported and exported from the system using the  **Load Rules** (import) or the  **Save Rules** (export) icons on the **Rules Configuration** dialog. This feature enables multiple rule sets to be maintained for various scenarios. The exported rule set, in the form of an **.nwr** file, can be copied to other NetWitness devices, simplifying the deployment and configuration of multiple devices.

Capture rules consist of three logical parts, called an expression. The simplest form of a expression would contain these elements:

Example: [**<Field>** + **<Operator>** + **<Value>**] + **Action**

Expressions may be grouped and logically combined with other expressions using Boolean **Operator(s)**. A **Value** can be a single value or a range of values.

Actions are assigned to a rule to tell the NetWitness system how to deal with packets that match the rule. The following table lists the possible actions for a rule.

| Action | Description |
|----------|---|
| Keep | Instructs NetWitness to keep the packet and write it to disk. |
| Filter | Instructs NetWitness to discard the packet. It is not written to disk. |
| Truncate | The payload information is not saved, but the metadata elements are retained. |

Rule Syntax

The syntax for writing capture rules consists of comparing a field to a value using a comparison operator. The supported comparison operators are equals (=) and not equals (!).

Values can be expressed as discrete values, a range of values, an upper or lower bound or a combination of these three. Greater than (>) and less than (<) comparisons are accomplished through the use of ranges. You can create a greater than or less than comparison, test equality or inequality against a range of values or an upper or lower bound.

The following table summarizes the supported comparison operators and the syntax for expressing values.

| Syntax | Description |
|--------------|--|
| * | Default rule. By using an asterisk (*) as the sole character in a rule, that rule will select all traffic. |
| = | Equality operator |
| != | Inequality operator |
| < | Less than operator |
| > | Greater than operator |
| <= | Less than or equal to operator |
| >= | Greater than or equal to operator |
| && | Logical AND operator |
| | Logical OR operator |
| -u | Upper bound. For example, to select all TCP ports above 40000 the syntax would be: tcp.port = 40000-u |
| l - | Lower bound. For example, to select all TCP ports below 40000 the syntax would be: tcp.port = l-40000 |
| - (dash) | Denotes a range. This is only applicable to numeric values. Separate the lower and upper bounds of the range with a dash (-) character. For example, to select TCP ports between 25 and 443 the syntax would be: tcp.port = 25-443 |
| , (comma) | Denotes a list of values. Single values may be used as well as any combination of ranges and upper or lower bounds. For example, the following is valid syntax: tcp.port = l-10,25,110,143-255,40000-u |
| () | Grouping Operator. An expression can be enclosed in parentheses to create a new logical expression. For example, (ip.addr=192.168.1.1 && tcp.port=80) (ip.addr=10.10.10.1 && tcp.port=443) would select traffic on port 80 to/from 192.168.1.1 OR traffic on port 443 to/from 10.10.10.1 |

Supported Fields

Supported metadata fields for creating capture rules are different for Network or Application Layer Rules. The following metadata fields are supported for use in Network Layer Rules:

| Metadata | Description |
|----------|--|
| eth.addr | Ethernet source or destination address. Commonly known as the MAC address. |
| eth.dst | Destination Ethernet address. This is the same as the Ethernet address field except it selects only packets where the destination address matches the selected value(s). |
| eth.src | Same as Ethernet destination except focuses on the source address. |
| eth.type | Ethernet frame type. |

| Metadata | Description |
|-------------|---|
| hdlc.type | Frame type of the HDLC frame. |
| ip.addr | IPv4 source or destination address in standard form. IP addresses can be entered in CIDR notation for subnets. |
| ip.dst | Destination IPv4 address in standard form. IP addresses can be entered in CIDR notation for subnets. |
| ip.proto | IPv4 protocol field. Internet Protocol Reference List on page 1 for a list of possible values and descriptions. |
| ip.src | Source IPv4 address in standard form. IP addresses can be entered in CIDR notation for subnets. |
| ipv6.addr | IPv6 source or destination address in hex format. Generally IPv6 addresses are written as eight groups of four hex digits, thus expressing the entire 128 bit address length. Supports notation to represent multiple blocks of 0000 in an address. Does not support CIDR notation. |
| ipv6.dst | Destination IPv6 address in hex format. |
| ipv6.proto | IPv6 protocol field. This maps to the Next Header field in the IPv6 header and uses the same values as the IPv4 protocol field. See Internet Protocol Reference List on page 1 for a list of possible values and descriptions. |
| ipv6.src | Source IPv6 address in hex format. |
| tcp.dstport | Destination TCP port. See TCP Protocol |
| tcp.port | TCP source or destination port. |
| tcp.srcport | Source TCP port. |
| udp.dstport | Destination UDP port. See UDP Protocol |
| udp.port | UDP source or destination port. |
| udp.srcport | Source UDP port. |

Reference Documents

For more information about how to define the appropriate rules for NetWitness capture configuration, see the following documents on RSA Link. Go to the [Master Table of Contents](#) to find all RSA NetWitness Platform 11.x documents.

- *Decoder Configuration Guide for RSA NetWitness Platform*
- *Core Database Tuning Guide for RSA NetWitness Platform*
- *Deployment Guide for RSA NetWitness Platform*

About Lua Parsers

You can use Lua to write and to customize parsers. For detailed information about how to work with Lua parsers, see the **Parsers Book** on RSA Link (<https://community.rsa.com/docs/DOC-41370>).

If you develop and install your own Lua parsers, you must place them in the `C:\ProgramData\NetWitness\ng\parsers` directory. Some sample parsers are included with the installer and should be installed in that location by default.

You must restart Investigator to see new parsers. If you update an existing parser, it will be picked up when **capture** or **import** starts.

SDK Data Types

Supported Fields

For information about currently supported fields, refer to <https://community.rsa.com/community/products/netwitness/rsa-content/udm>.