Investigator User Guide

Version 9.8

August 2012

NetWitness® Corporation
10700 Parkridge Boulevard
6th Floor
Reston, VA 20191
www.netwitness.com

NetWitness®NextGen Investigator User Guide

Table of Contents

Version 9.8
November 2012

Chapter 3

Getting Started

Chapter 4

Collection Management

Chapter 5

Data Capture

Chapter 6

Data Analysis

Appendix A

Rules

Appendix B

Custom Parsers

Appendix C

Reference List Documents

Appendix D

SDK Data Types

Appendix E

Wireless Packet Capture

About This Guide

This *NetWitness*® Investigator User Guide provides information about performing the analysis of the data captured from your network or from other collection sources using INVESTIGATOR. 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 8.6 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® System Administrator Guide* – This document provides information about the setup, configuration and management of the NetWitness appliances (DECODER and CONCENTRATOR).

Conventions

Fonts and Typefaces

This Guide uses fonts and typefaces to connect what you read in this book to what you see on the screen or what you need to type when using the system. Of particular importance are the following:

bold sans serif	For text that appears in windows or dialog boxes (e.g., the **Close** and **OK** buttons, the **File** menu) and for file names (e.g., **c:\control.ini**, **/etc/hosts**) that appear within the text of paragraphs.
SMALL CAPITALS	For keyboard key names, such as ENTER or TAB.

`monospaced font`	Used for listing the contents of files and code samples.
`bold monospaced font`	Identifies actual characters you should type. For example: … type **`exit`** at the prompt … means you should type the characters **`e`**, **`x`**, **`i`**, and **`t`**
Bold-italic	Indicates that you should replace the text with the actual value appropriate for your system. For example: … locate the file ***d:\directory*control.ini** … means you should replace ***d:*** and ***directory*** with the actual drive and path of the file in question, when performing the task; for example, **c:\windows\control.ini**

Special Symbols

→ This arrow is used to show a series of selections (menu options, tabs, links, etc.). For example:

… select **File** → **New** → **Folder** …

means you should pull down the **File** menu and select **New** and then **Folder**.

The book symbol identifies a cross-reference to related information.

The caution symbol indicates that you should carefully read and follow any directions associated with it to prevent serious errors or data loss.

The note symbol identifies a helpful tip or technique, or additional information about the current topic.

Contact Customer Care

If you have any questions about your NETWITNESS® software, refer to the particular software's user guide or online help. If you cannot find the answer, contact one of our representatives. Customer Care is available Monday through Friday, 8:00 AM–8:00 PM Eastern Time, except holidays:

Phone: 866.601.2602

Fax: 703.651.3126

Contact: http://community.netwitness.com

Preparing to Call

When you contact Customer Care, you should be at your computer and have the appropriate product documentation at hand. Be prepared to give the following information:

- The version number of NETWITNESS® product or application you are using.
- The type of hardware you are using.
- The exact wording of any messages that appear on your screen.
- A description of what happened and what you were doing when the problem occurred.
- A description of how you tried to solve the problem.
- If possible, a screen print demonstrating where the problem or issue occurs. This helps the Customer Care Engineer with the resolution process.

Trademarks and Copyrights

Chapter 1

Overview

NetWitness Products

NETWITNESS 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.

- **Administrator**—a Graphical User Interface (GUI) that allows you to manage a NetWitness Service product. Management capabilities include:
  - Configuration
  - Stopping and starting services
  - Monitoring service health and performance
  - Monitoring application performance
  - Viewing service logs
- **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 an infinite number of 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.

> Both DECODER and CONCENTRATOR are compatible with the free NetWitnessAPI/SDK applications.
> For more information about these applications, contact *support@netwitness.com*.

- **Broker**—a NetWitness application that brokers and distributes queries across multiple CONCENTRATORS (concentration points) to provide a single view across an entire network
- **Investigator**—a NetWitness application that provides the capability to process pre-existing data or capture live data from a network interface and perform analysis on data collected by either of the two capture methods. INVESTIGATOR can connect live into DECODER or CONCENTRATOR for interactive browsing and searching.

- **Informer**—a NetWitness application that enables users to create customized reports on real-time incidents, threats, anomalies, misconfigurations, compliance violations, and other malicious or benign activities on the network. Report results can be verified by using links to NetWitness INVESTIGATOR.
- **NwConsole**—a command interface accessed through the Windows Command Shell or the Secure Socket Shell (SSH). In addition to the management capabilities outlined in Administrator, you can run scripts from the NwConsole.

System Requirements

Hardware

Hardware requirements vary greatly based on the volume and nature of the network being monitored. The following are the core hardware specifications and configuration for NetWitness DECODER and CONCENTRATOR products:

- Intel Xeon (or AMD equivalent) x86-64 dual-core processor – 2 GHz or higher
- 16GB RAM
- High speed, high capacity RAID storage system with 4 separate physical and logical volumes, with ample storage for collected data(>4TB)
- Optional high-speed capture interface card (DECODER)

If you need assistance, see *Contact Customer Care* on page viii.

Software

NetWitness products are offered as software for certain environments. The following are the core operating system requirements:

- Servers
  - Linux Fedore Core 8, x86-64 (highly recommended)
    Kernel Version 2.6.23.9-85fc8
  - Windows 2003 Server RC2 with proper capture drivers
- Client Applications—Windows® XP, 2003 Server, or Vista with Internet Explorer v7+

NetWitness recommends that client applications should be IE v7+.

Install NetWitness Investigator

Current users must close any current version of INVESTIGATOR before proceeding with the installation of a newer version or update installation.

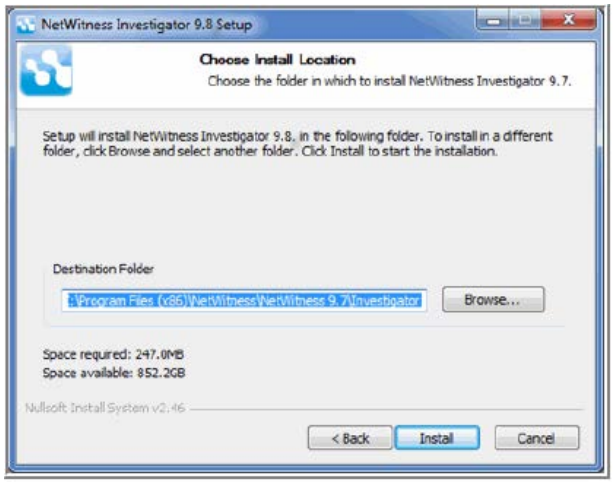
The installation of ADMINISTRATOR must be performed on the Windows platform. The necessary files are included in the installer package, available from netwitness.com/downloads.

1. Double-click on the installer file (**.exe**).
2. The SETUP WIZARD opens the **License Agreement** window automatically.

   In the **License Agreement** window, click **I Agree** to continue.

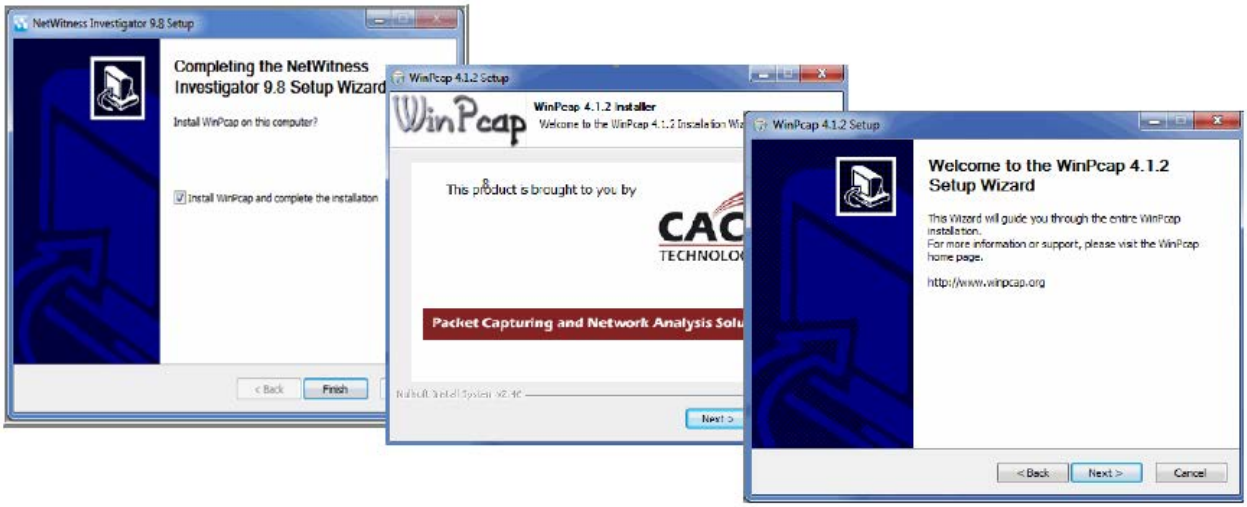
NOTE: Clicking **I Agree** is required by the SETUP WIZARD.

3. The **Choose Install Location** window opens. Click **Install** to accept the default Destination Folder displayed or click **Browse** to select another folder.



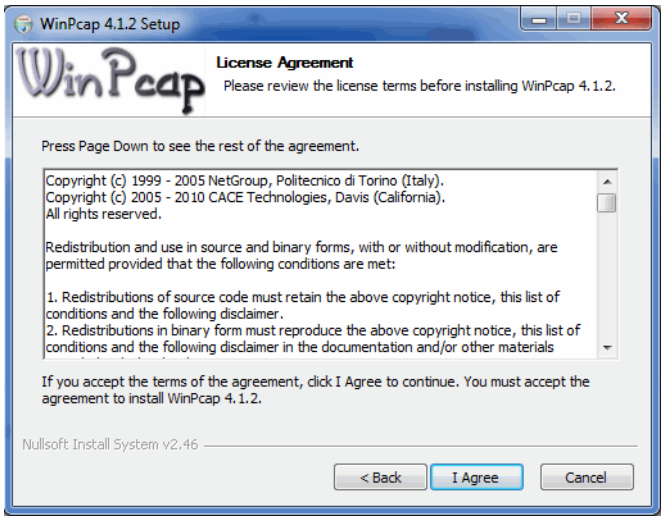
4. You have the option to install WINPCAP on your computer. It is only necessary if you will be capturing packets directly while using NETWITNESS INVESTIGATOR, rather than importing **pcap** files. To complete the **Setup Wizard**, check the option to install **WinPcap** and click FINISH.

   If not, click FINISH to complete the NETWITNESS INVESTIGATOR installation. When the installation is complete, click **Close** to close the SETUP WIZARD.

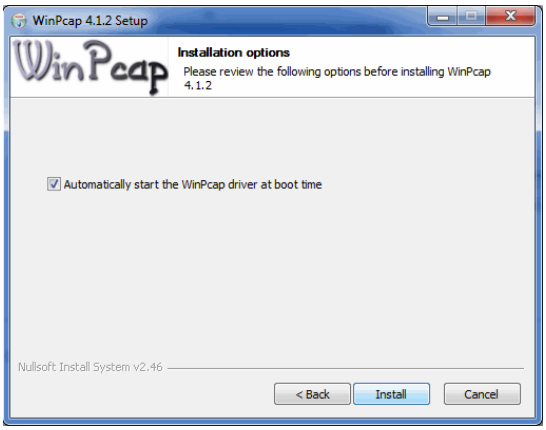


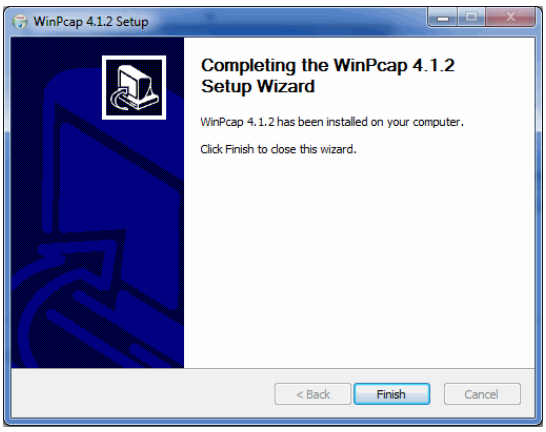
   The **License Agreement** dialog is displayed.

5. You must accept the license agreement. Click on **I Agree** to continue.



6. By default, WINPCAP installs to start when you open NETWITNESS INVESTIGATOR. Click **Install**.





7. When the installation is complete, click **Close** to close the SETUP WIZARD.

Uninstall Investigator

1. Close all programs.
2. From the **Start** menu, click **Control Panel**.
3. Double-click the **Add/Remove Programs** icon.
4. Highlight **NetWitness Investigator 8.6** from the list of installed applications, and then click **Remove**.
5. Follow the instructions.

License Key Management

NetWitness requires a valid license key. License keys can be set to expire. Every computer will have a unique Computer ID, which is associated with a specific license key.

1. Request a license key for NetWitness:

   PATH: `Start → Programs → NetWitness → NetWitness 8.6 → Investigator → License Manager`

   The **NetWitness License Key Manager** window appears.

2. In the **Computer ID** field, copy the computer ID and send it to *support@NetWitness.com*.

   NetWitness will respond with an e-mail containing a key file (.nwk) attachment.

3. Re-open the **License Key Manager** window and click the **IMPORT KEYS** button. The **Open** window appears.

4. Select the .nwk file and then click the **OPEN** button.
5. Click **OK**. The valid keys display on the **NetWitness License Key Manager** window.
   a. To view the **Product**, **Status**, **Generated** and **Expires** for the license key, click the **KEY DETAILS** button.
   b. To delete a key, select the key that you want to delete and then click the **DELETE KEYS** button.
6. Click the **EXIT** button.
7. Incorrect license key entry is a common source of NetWitness operation errors. Therefore, please verify your key options including **product**, **number of sources**, and **expiration date**. If you are still having problems, please contact NetWitness Support at *support@NetWitness.com*, preferably with a screenshot of the **KEY DETAILS** dialog.

Chapter 2

Investigator Basics

Overview

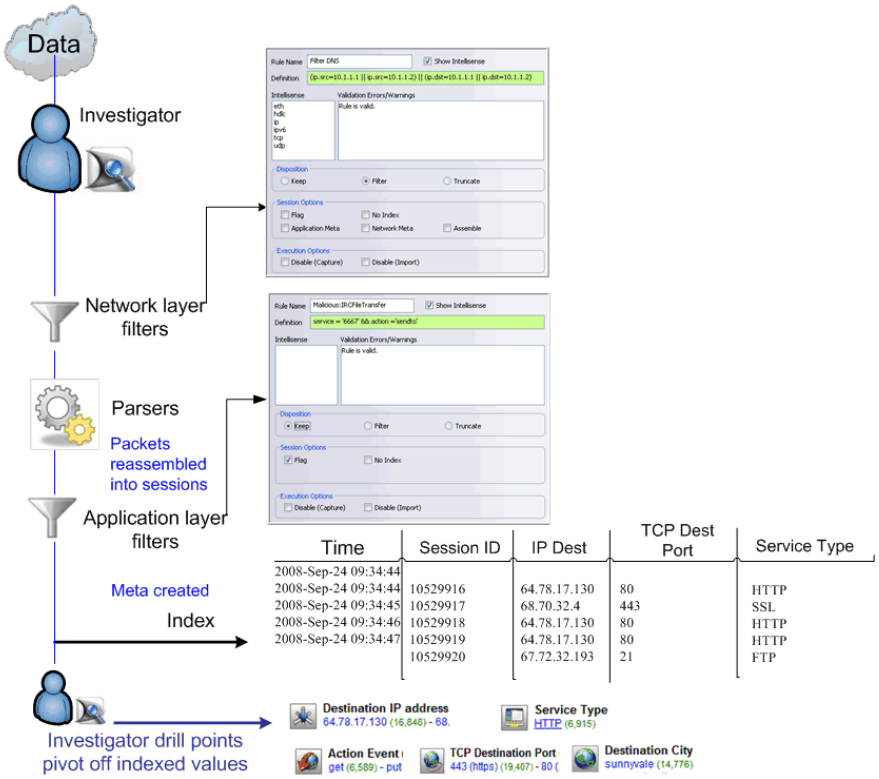
NetWitness is a security intelligence product that audits and monitors all traffic on a network. It creates a comprehensive log of all network activities and interprets the activities into a format that network engineers and non-engineers alike can quickly understand.

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 (see *License Options* on page 8).

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. Connection can be encrypted 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* on page 49).

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

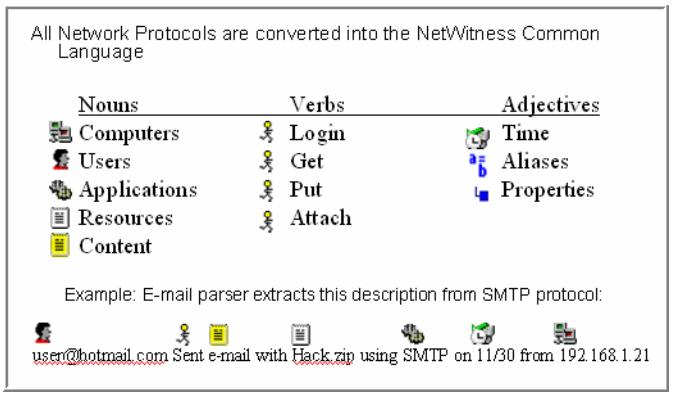
- **Investigator Concepts** (see page 10)
- **Menus**(see page 11)
- **Navigation** (see page 15)
- **Navigate Multiple Views** (see page 17)

License Options

NetWitness INVESTIGATOR has extensive licensing options. Some features in this User Guide may not be available to you. Please contact your account manager for more details.

About Parsers

A parser is a program, usually part of a compiler, that receives input in the form of sequential source program instructions, interactive online commands, markup tags, or some other defined interface and breaks them up into parts (for example, the nouns (objects), verbs (methods), and their attributes or options) that can then be managed by other programming (for example, other components in a compiler). A parser may also check to see that all input has been provided that is necessary.



The metadata contains important information such as network and application events. All enabled parser plugins 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**. For a detailed list of the 45 parsers used by NetWitness, see *Parsers and Associated Metadata* on page 110.

The custom-defined **Search** parser and the **FLEXPARSE™** tool can be configured by the user, extending your analysis capabilities considerably (see page 57).

Investigator Concepts

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

CONCEPT	DESCRIPTION
Parser	A program, usually part of a compiler, that receives input in the form of sequential source program instructions, interactive online commands, markup tags, or some other defined interface and breaks them up into parts (for example, the nouns (objects), verbs (methods), and their attributes or options) that can then be managed by other programming
Drill	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 (See *About Parsers* on page 9). 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 *breadcrumb* trail in the **Navigation** view that shows the user the path traversed to the current drill point.
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.
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: ◆ Summary ◆ Collection ◆ Report ◆ Session ◆ Search ◆ Content

CONCEPT	DESCRIPTION
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** (see page 12)
- **Edit** (see page 13)
- **View** (see page 13)
- **Bookmarks** (see page 14)
- **History** (see page 14)
- **Help** (see page 14)

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.

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. These are explained in the chapter on *Data Analysis* on page 63.

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	[NONE]	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.
Export Collection	[NONE]	Export packet files to a saved format (.pcap, .raw, .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	[NONE]	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.
Options	CTRL + O	Opens the **Collection Configuration** (see page 33) dialog box: ◆ General ◆ Display ◆ Reports ◆ Capture ◆ Process ◆ Audio Codecs ◆ Advanced
Rules	CTRL + U	Opens the **Rules Configuration** (see page 33) dialog box: ◆ Net Rules ◆ App Rules

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 Google Earth. The GeoIP parser must be active when the data is processed.

View Menu Option	Keyboard Shortcut	Description
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.
Welcome Page	✓	The Welcome Page contains Frequently Asked Questions about Investigator and Recent News from NetWitness.
Status Bar	✓	System status messages and warnings appear on the Status Bar.

Bookmarks Menu

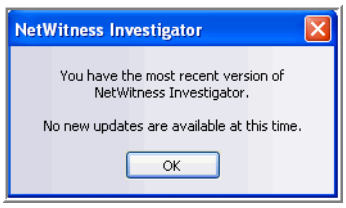
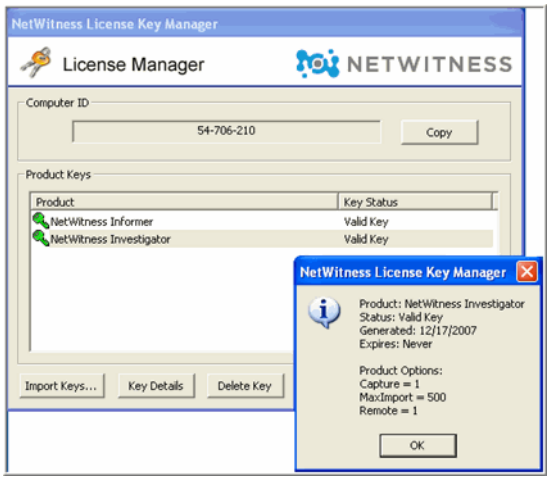
Bookmark Menu Option	Keyboard Shortcut	Description
Add Bookmark	[NONE]	Adds the current drill path or session listing as a bookmark. This option is only available while navigating within a collection.
Organize Bookmarks	[NONE]	Allows the user to arrange existing bookmarks or remove them. This list is 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	A fully searchable PDF of the NetWitness Investigator User Guide. To be able to view PDF files, you must have the latest version of Adobe Acrobat® Reader installed. You can download this free application from www.adobe.com.
Registration ID	Displays your Registration ID for Investigator.

HELP OPTION	DESCRIPTION
Check for Update	Advises if there is a more current Version of INVESTIGATOR available. 
License Manager	Displays your computer ID and the Product Keys for each NetWitness application. The status of the Product Keys and the date generated is provided, as well as any applicable expiration date. 
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

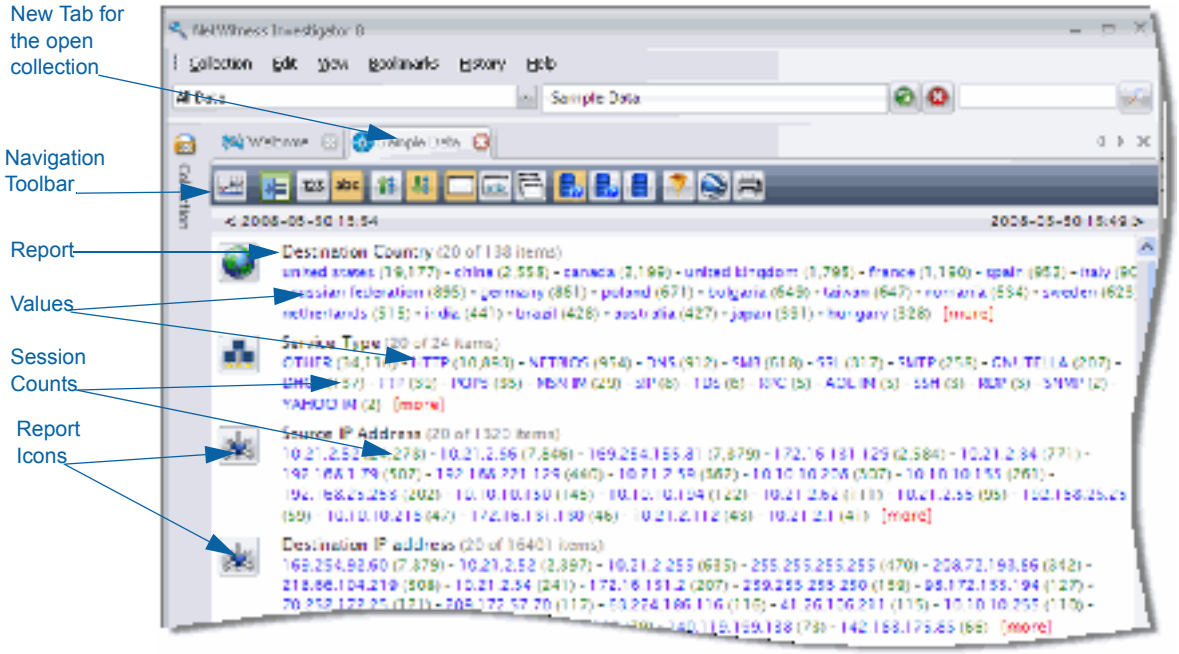
Collection Navigation

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** (see page 16)
- **Navigate Multiple Views** (see page 17)
- **Session List View** (see page 19)
- **Content View** (see page 20)

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 (see page 110) lists report values and their associated session counts.

Navigation Toolbar

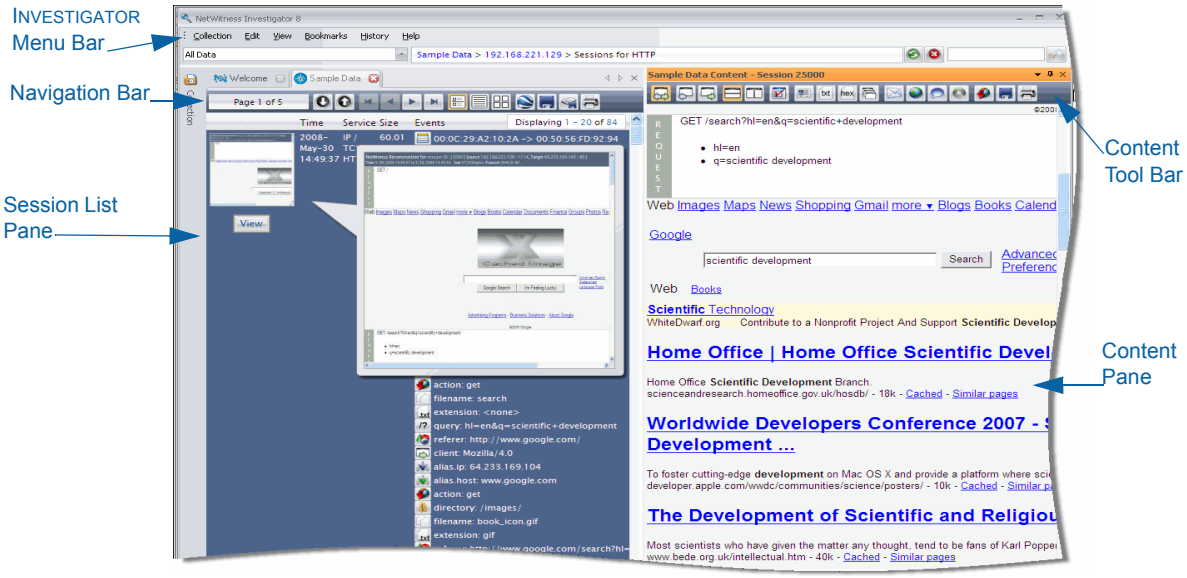
The appearance of the collection reports and the data contained are determined by the combination of selections you make on the **Navigation** toolbar. For example, the **Time Graph** allows you to expand a section of time for closer examination. For a detailed explanation, see *Navigation Toolbar* on page 67.

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

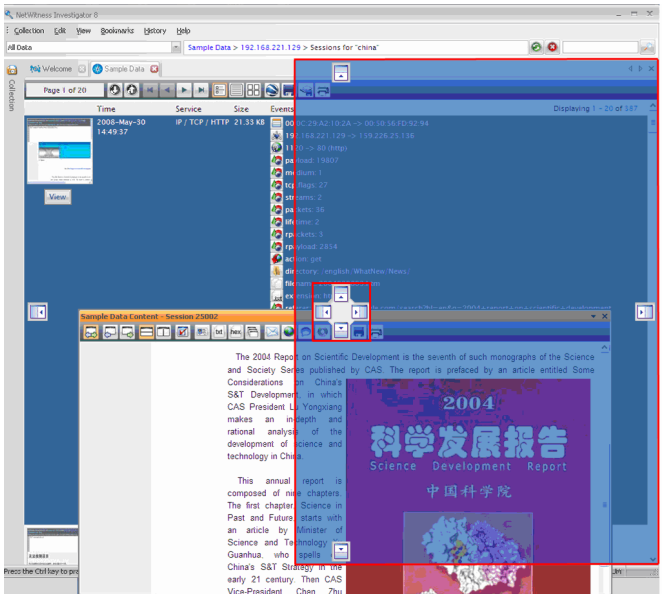
FUNCTION	DESCRIPTION
Drill into a Report Value	This will refocus the current view into a Navigation view with that particular report value as a filter.
Drill into a Session List	This will display a list of all the sessions for a specified drill point and their associated metadata. Session content may 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 original position of the pane.

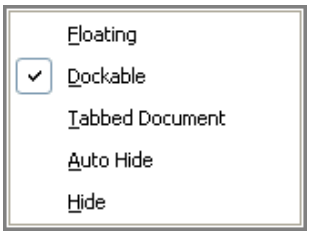


One possible re-arrangement of the panes is shown below. You can determine which arrangement works best for yourself.

The Docking Guides are only available if you are using one of the 2007 themes (Edit → Options).

Content Pane Display Options

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

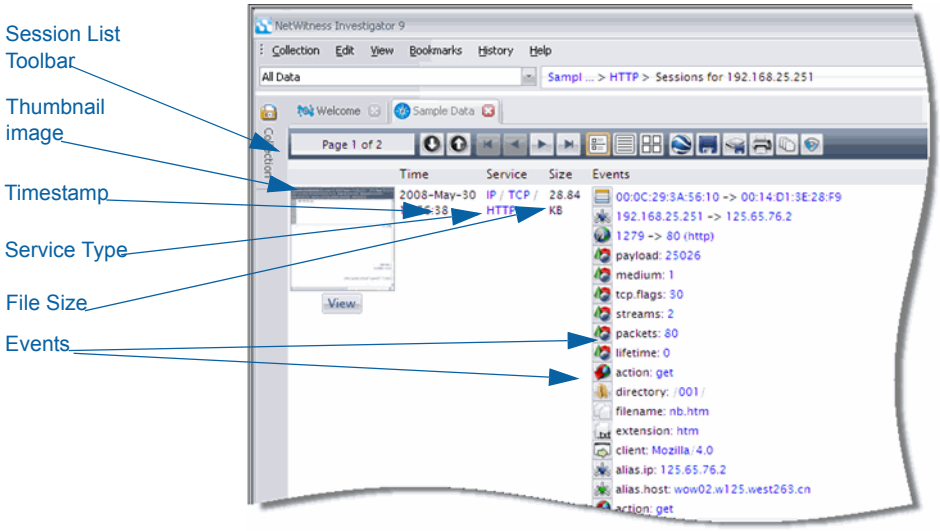
CLICK THIS...	TO DO THIS...
	View the **Options** menu to change the location of the **Content** pane.  **NOTE:** The **Floating** option is useful if you are using dual monitors.

CLICK THIS...	TO DO THIS...
	AutoHide hides the current **Content** pane and creates a tab to restore the content view.
	The **Hide** button closes the **Content** pane.

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.

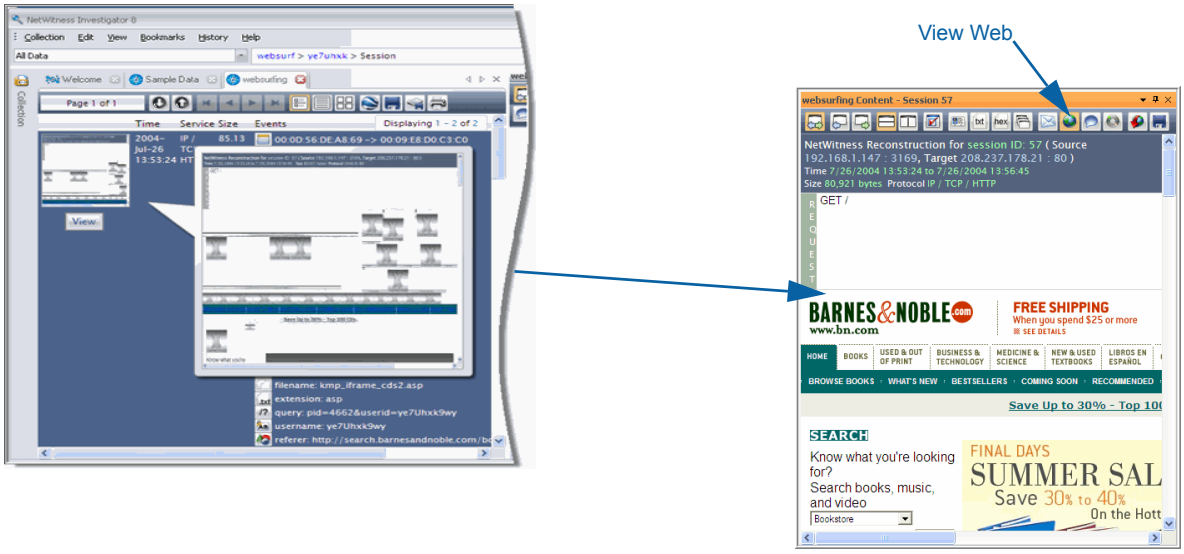
For example, if a user has clicked on a session count of 212 to the right of a particular **Address** report value from the **Navigation** view, the resulting 212 sessions will be listed on the **Session List** view.

Session List Toolbar

This toolbar facilitates moving among the individual sessions for the chosen **Report** and **Value**. appearance of the collection reports and the data contained are determined by the combination of selections you make on the **Navigation** toolbar. For a detailed explanation, see *Session List Toolbar* on page 79.

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.

For more details about viewing content through INVESTIGATOR, see *Content View* on page 82.

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. For more information, see *Content Toolbar* on page 83

Chapter 3

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 an 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.

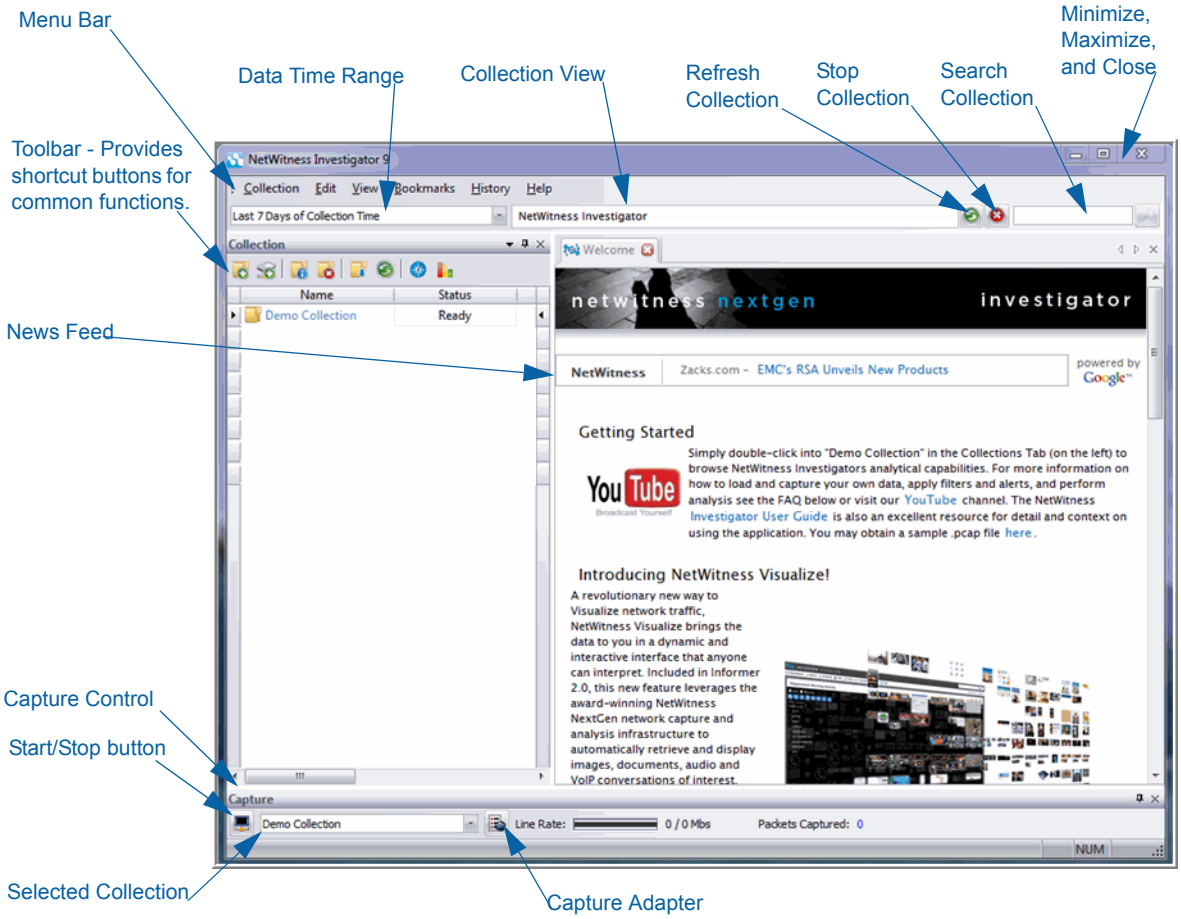
Once you become familiar with data navigation methods, you can explore the data more completely through:

- 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.

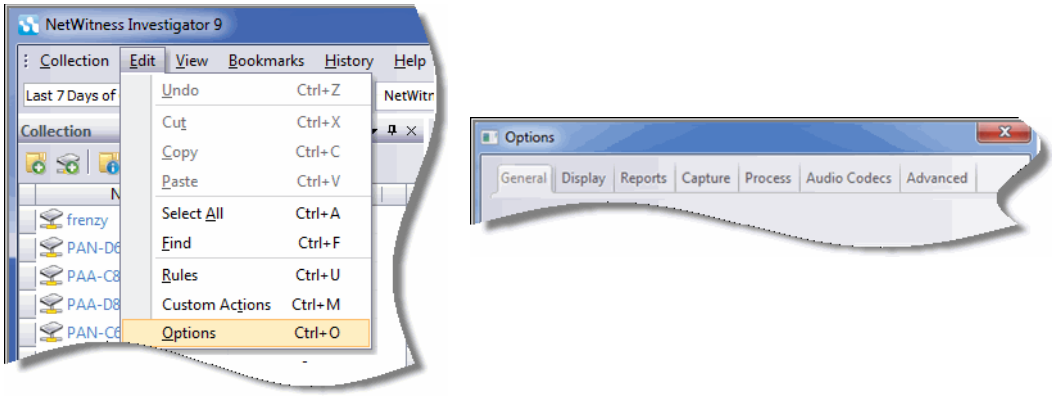


A **Collection** may display any of the following in the **Status** column:

- **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



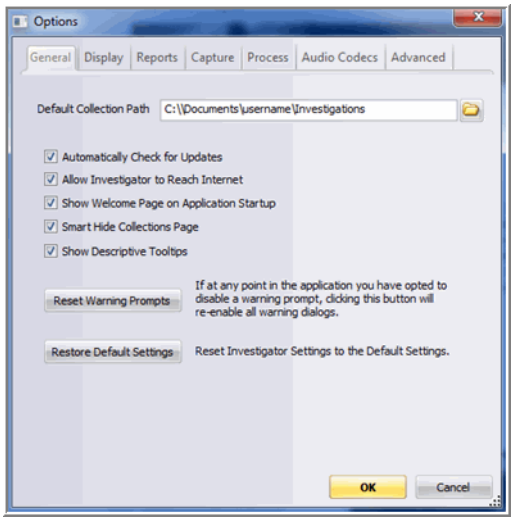
The **Options** dialog box has seven categories:

- **General** (see page 24)
- **Display** (see page 25)
- **Reports** (see page 26)
- **Capture** (see page 27)
- **Process** (see page 28)
- **Audio Codecs** (see page 30)
- **Advanced** (see page 31)

The complete configuration settings for INVESTIGATOR are available in the **Application Data File** on your system after installation. For a detailed description of these settings, see *Investigator Configuration Settings* on page 131.

General

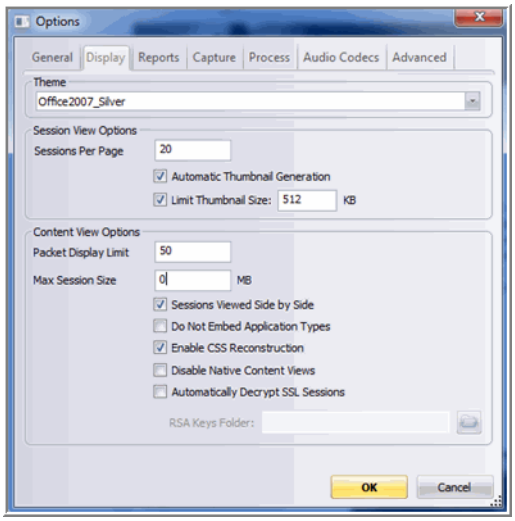
This section allows you to determine where all collections are stored, thumbnail size, and warning prompt settings.



- **Default Collection Path**–This is the default directory path where all collections are stored on the system. The default path is `My Documents\NetwWitness\Collections`.
- **Automatically Check for Updates**–When checked, INVESTIGATOR automatically checks for new updates and prompts the ser 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 Views* on page 17.

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

- **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.

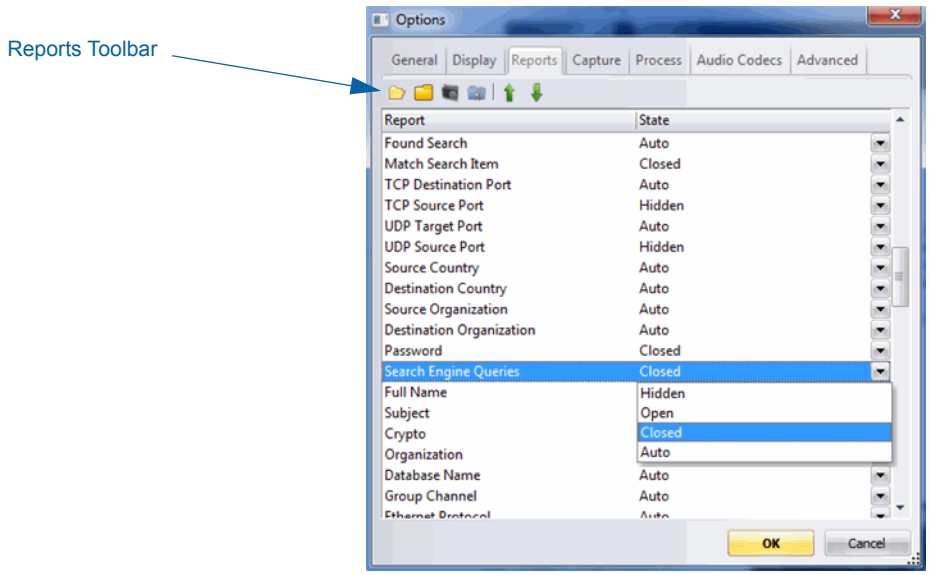
- **Enable CSS Reconstruction**–When checked, the application attempts to find and load the website's CSS files from other sessions. If you are having problems viewing specific websites, try checking this option.
- **Disable Native Content Views**–When checked, the user is prevented from viewing content 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 save RSA keys.

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 to Open
	Set all reports to Closed
	Set all reports to Auto
	Set all reports to Hidden
	Move the selected rule up in the list
	Move the selected rule 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.

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

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

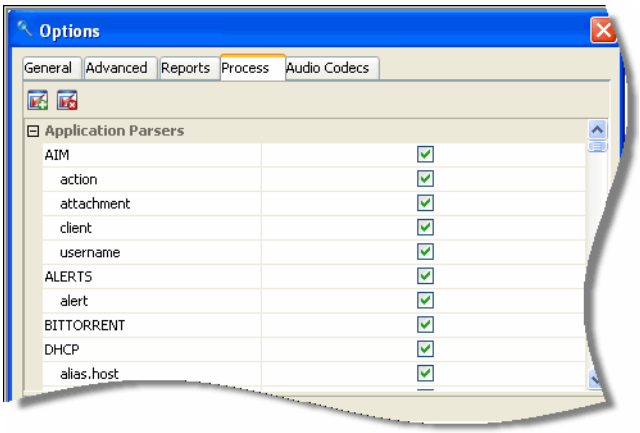
Process

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

- Application Parsers (see page 28)
- Assembler Properties (see page 29)
- Memory (see page 29)

Application Parsers

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



Assembler Properties

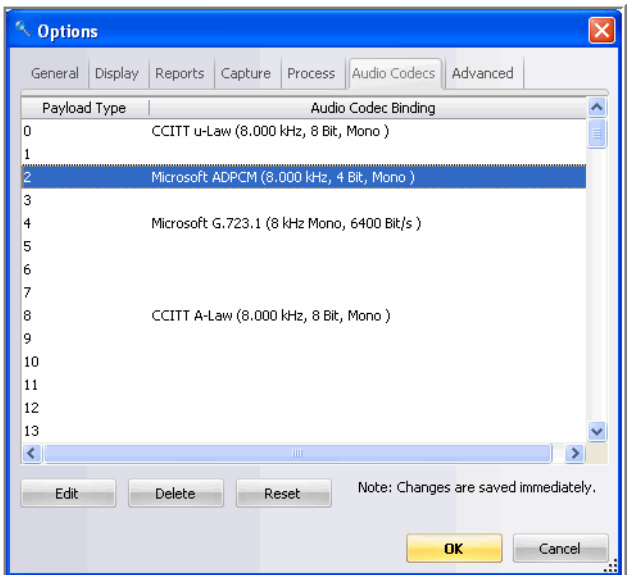
SETTING	DESCRIPTIONS
Session Timeout	Assembler active session timeout in seconds. This is how long a session can be idle inside the assembler's cache. The assembler timeout value specifies the time the assembler waits for a session to complete prior to timing it out. Too many sessions waiting to be timed out can occupy large amounts of memory (large timeout value); however, too many sessions timing out at once can cause system-degraded write performance (small timeout value). **NOTE:** Timeout values less than 15 seconds or greater than 180 seconds are not recommended.
Chain Timeout	Assembler active chain timeout in seconds
Maximum Session Size	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. **NOTE:** Reducing the amount of memory can improve performance; however, sessions above this byte limit will be truncated.
Maximum Index Size	Specifies the maximum index size
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 ip and tcp cheksumming.

Memory

SETTING	DESCRIPTION
Session Pool	Total sessions to keep in preallocation pool. This is a performance setting which allocates the number of sessions on NetWitness start.
Packet Pool	Total packets to keep in preallocation pool. This is a performance setting which allocates the number of packets on NetWitness start. Using a larger packet pool can increase performance.
Chain Pool	Total number of chain entries in the preallocation pool.

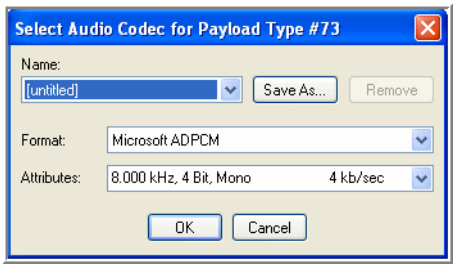
Audio Codecs

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:

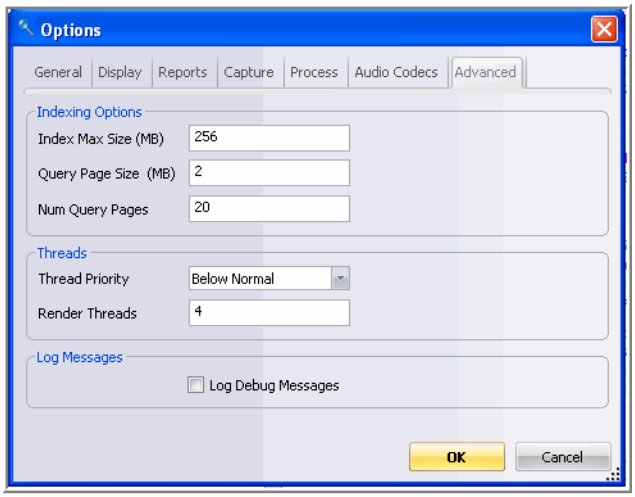
- **Edit**–When you click the **Edit** button, a dialog box opens that allows you to select:
  - **Name** (sound quality)–The choices are CD, radio, or telephone.
    Click **Save As...** to give the new codec a Name.
    Click **Remove** to remove the value from the dropdown list.
  - **Format**–Select 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 Indexing, Threads, and Log Messages.



Indexing Options

- **Index Max Size**–The maximum size in MB that the local index can attain.
- **Query Page Size**–The query page size in KB. For large queries, an increased size can produce more accurate results.
- **Num Query Pages**–The number of memory query pages to be cached for reuse.

Changing either of the query page settings requires a service restart.

Threads

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

Log Messages

- When checked, all debug messages are written to the log.

Configuration Settings File

The configuration settings for INVESTIGATOR in the **Edit → Options** menu described in this chapter are not the complete settings available. The complete list of settings is found in the **NwInvestigator8.settings** file created on your system at installation (see *Investigator Configuration Settings* on page 131).

PATH: `C:\Documents and Settings\user\Application Data\NetWitness\`

Chapter 4

Collection Management

Overview

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 DECODER or CONCENTRATOR
- A **Local** collection, either a live capture or packet imports (size is defined by NetWitness License Agreement (see *License Options* on page 8)

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.

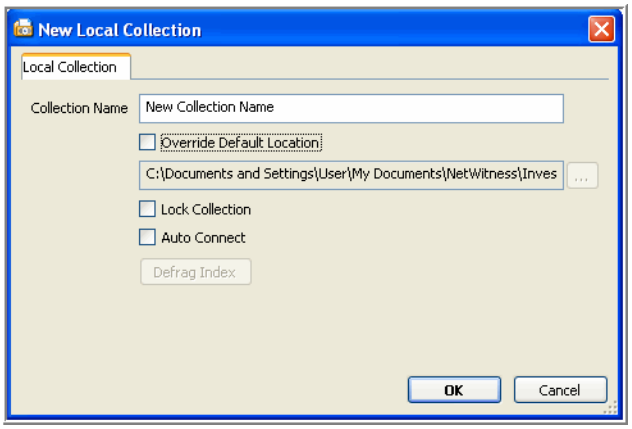
There are two levels of configuration that are required with INVESTIGATOR.

- **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. (see page 23)

- **Collection Level** - Settings for file location, locking a collection, or making a collection the default collection. (see page 34)

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.

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 (see *Collection Menu* on page 12).

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.

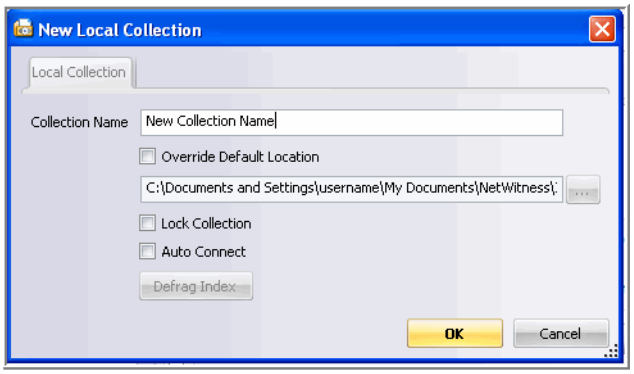
How To...

- Create a new collection in INVESTIGATOR (see page 36)
- Configure the new collection (see page 37)
- Import a data file (see page 38)
- Reprocess a collection (see page 38)

Create a New Collection

1. On the INVESTIGATOR Toolbar, click the **New Local Collection** icon.

These steps are included as part of the **Welcome Page** under **Frequently Asked Questions**.



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

NOTE: 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.

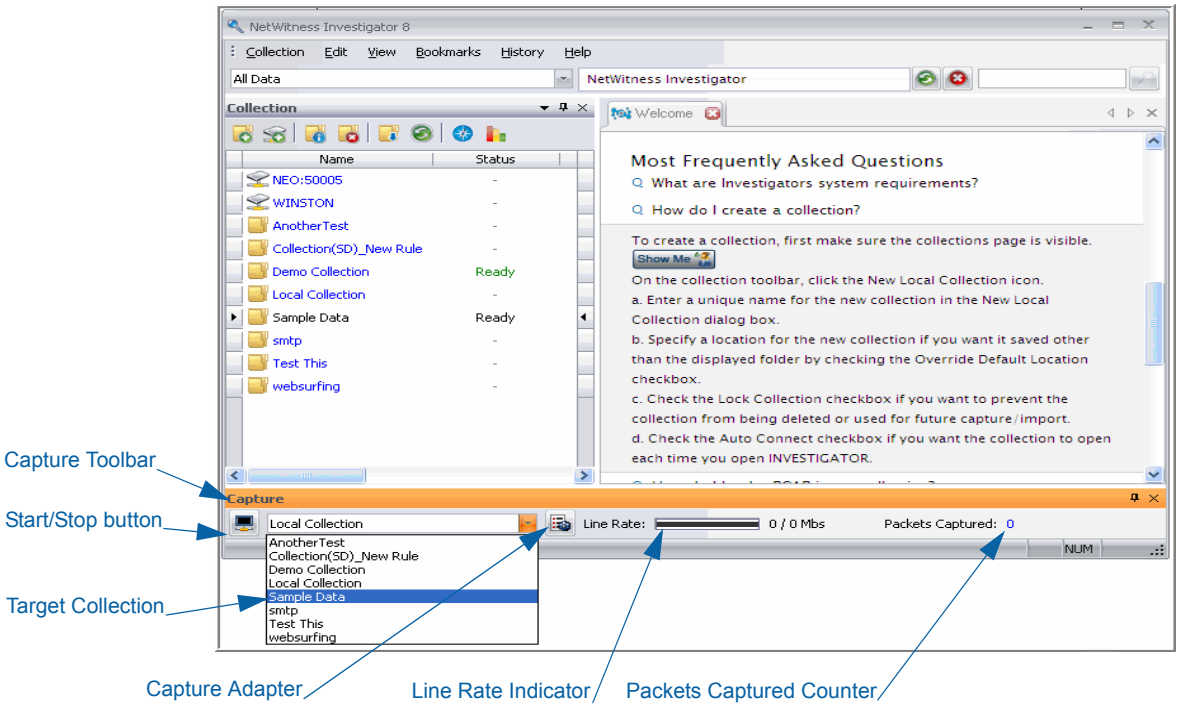
c. Check the **Lock Collection** checkbox if you want to prevent the collection from being deleted or used for future capture/import.

d. Check the **Auto Connect** checkbox if you want the collection to open each time you open INVESTIGATOR.

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.

The INVESTIGATOR Welcome Page provides a group of **Frequently Asked Questions** (FAQs).



3. Select the target collection from the dropdown box. 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 (see *Input File Types List* on page 41)

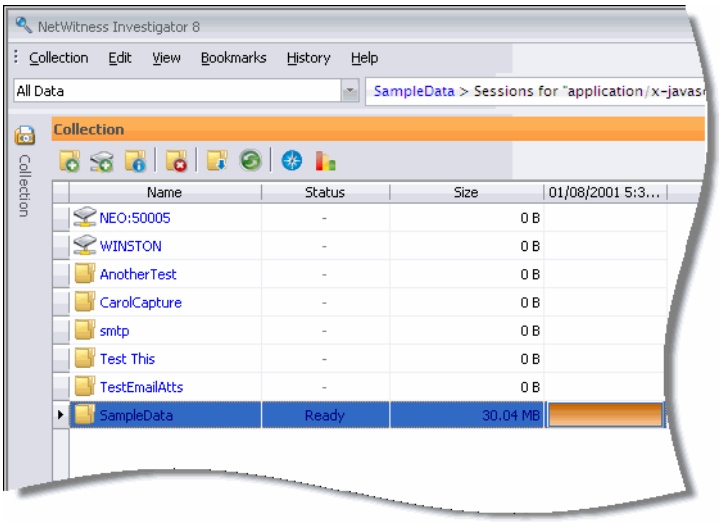
  The file is processed based on the current INVESTIGATOR configuration settings (see *Configure Investigator* on page 23).

- Configure live data from the network.

  You set the **Adapter** and **Rules** before you begin the capture process (see *Data Capture* on page 43).

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**.

If you import a collection under a different name, you can apply a different set of Network and Application layer rules (see *Rules Overview* on page 49) to obtain a different view of the same data.

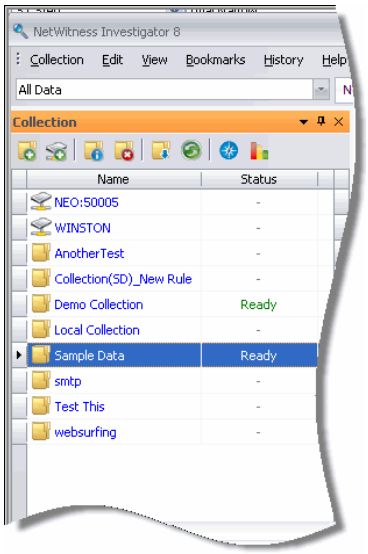
Reprocess a Collection

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.

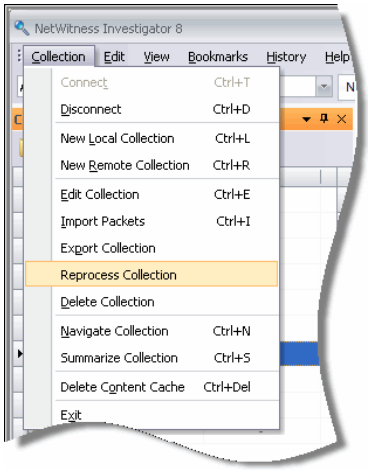
1. Export your rules to a file (.nwr) and then delete the existing files for the Network layer and Application layer rules.

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

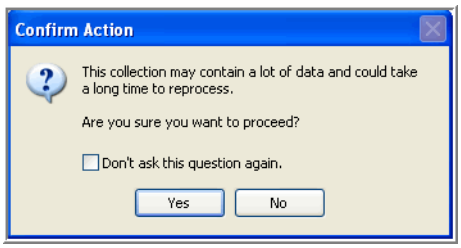
2. On the **Collections Page**, highlight the collection that you want to reprocess.



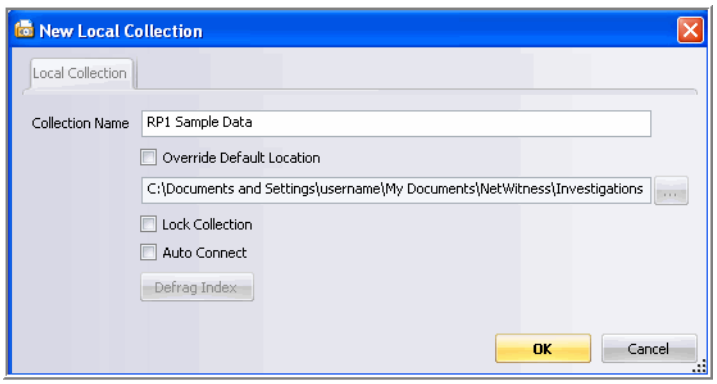
3. From the **Collections** menu, select **Reprocess**.



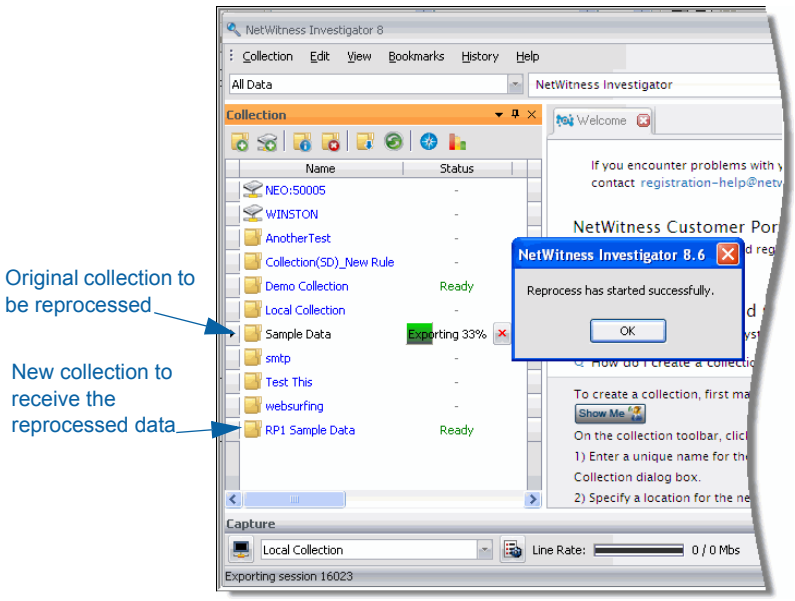
4. Click YES to confirm that you want to proceed with reprocessing the selected collection. If you click NO, the procedure terminates.



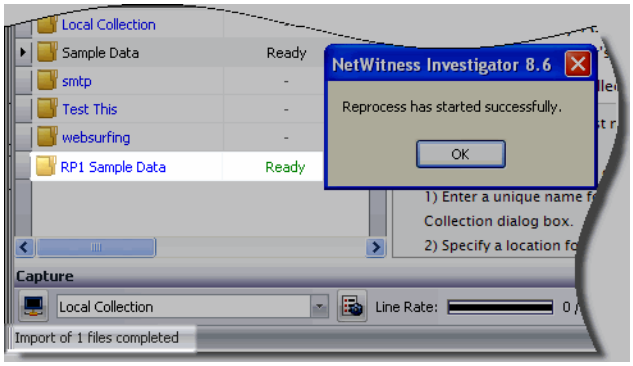
5. Enter a unique name for the reprocessed collection and click OK.



6.



7. When reprocessing is complete, click OK.



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. If data is in a format not listed here, a conversion utility, **editcap**, can perform format conversions either the open-source **Ethereal** or **Wireshark**.

TYPE OF FILE	COMMON FILE EXTENSION
TCPDump	.tcp, .tcp.gz, .pcap, .pcap.gz
NetMon	.cap, .cap.gz
EtherPeek	.pkt, .pkt.gz
IPTrace	.ipt, .ipt.gz
NAIDOS	.enc, .enc.gz
RAW	.raw, .raw.gz
CAYMAN	.ppp
Network Instruments Observer	.bfr

Chapter 5

Data Capture

Overview

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 Parsers**–This introduces specialized or user-defined parsers. For a general discussion of parsers and what they do, see *About Parsers* on page 9.
- **NetWitness Live**–NETWITNESS LIVE provides immediate access to multiple sources of threat intelligence and reputational content. For a discussion of the process, see *NetWitness Live* on page 45.
- **Rules**–There are two categories of rules that affect data capture, **Network Layer** and **Application Layer** rules.For a discussion of the process, see *Rules Overview* on page 49.

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

✓	STEPS TO COMPLETE BEFORE BEGINNING A CAPTURE	
❒	Select the parsers to use for the capture.	
	◆ Define any custom parsers for use.	(see page 44)
❒	Define the Rules to be applied to the captured data.	
	◆ Network Layer	(see page 50)
	◆ Application Layer	(see page 53)
❒	Verify the Capture Configuration settings.	
	◆ Network Adapter	(see page 58)
	◆ Advanced Capture Settings	(see page 59)
	◆ Evidence Handling	(see page 59)

✓ **STEPS TO COMPLETE BEFORE BEGINNING A CAPTURE**

❒ Start the capture. (see page 60)

Custom Parsers

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

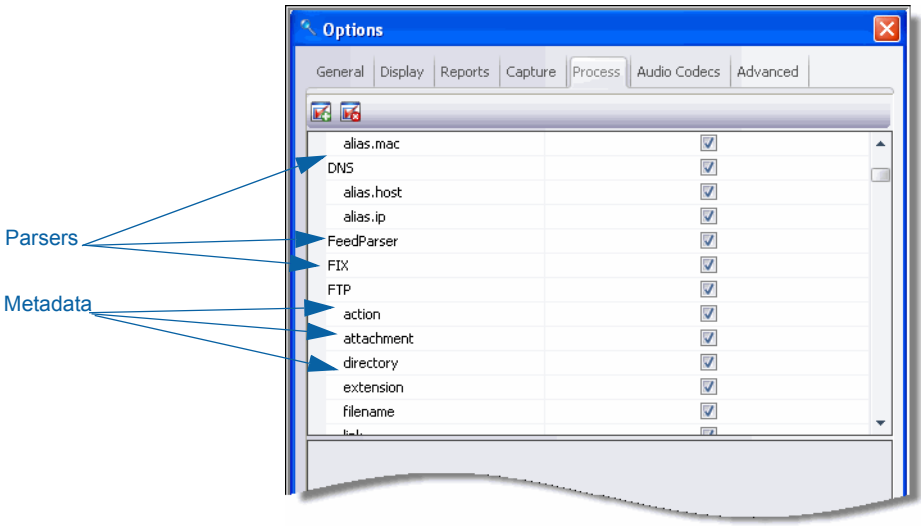
- GeoIP–This parser associates the IP addresses with actual geographical locations.
- Search–This parser is user-configured to generate metadata by scanning for pre-defined keywords and regular expressions.
- FLEXPARSE™–This parser format that allows the user to define a parser for a new application protocol.

For more information about these parsers, see *Custom Parsers* on page 97.

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**.

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 2.0 Service**. You are then able to select from the available content to download to INVESTIGATOR.

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.

For more detailed information, see the *NetWitness LiveManager User Guide*.

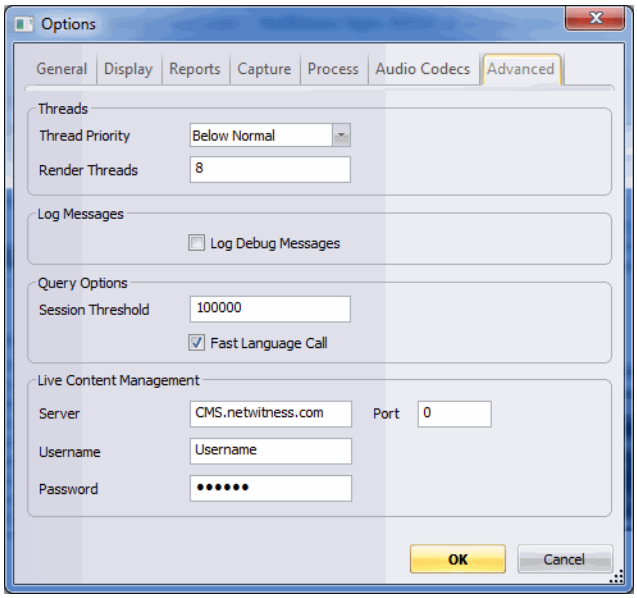
Some of the data types that the baseline rules provided will help identify are:

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

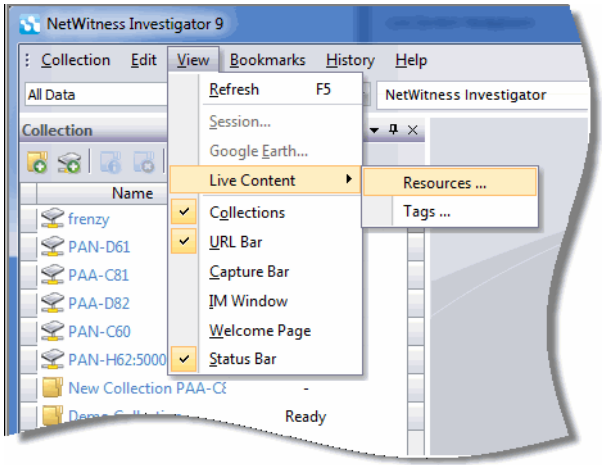
The *SANS Internet Storm Center*, contains the top 10,000 source IPs, associated with malicious activity and tracked by *SANs* and its contributors. As a NETWITNESS Feed, sessions containing these IP addresses are flagged as new meta data for analysis. For more information on the SANs Top Source list,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

To get started, follow these steps:

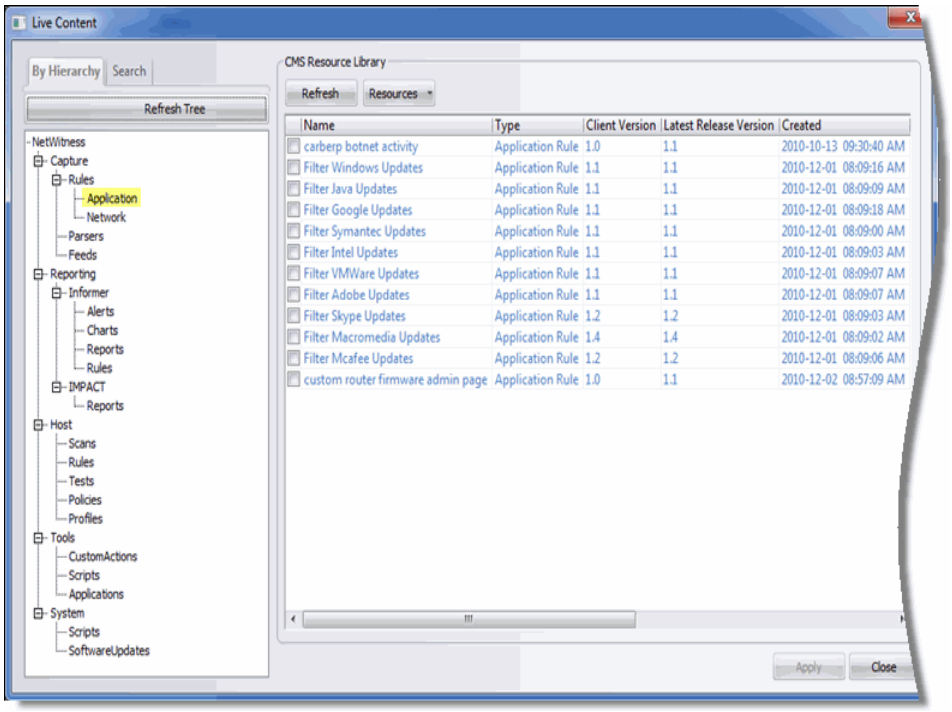
1. Navigate to the **Edit** → **Options** menu and click on the **Advanced** tab. Complete the **Live Content Management** credentials for your subscription. Click **OK**.



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.

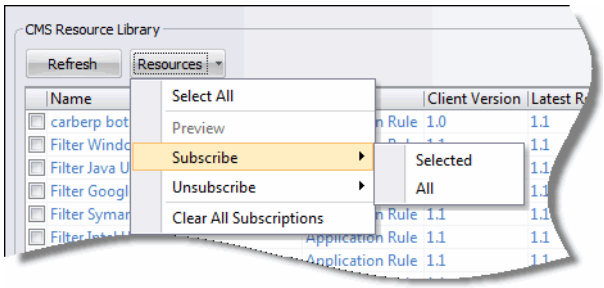


- The **Hierarchy** view allows the user to browse all of the content in the system to which he has access, arranged by content type.

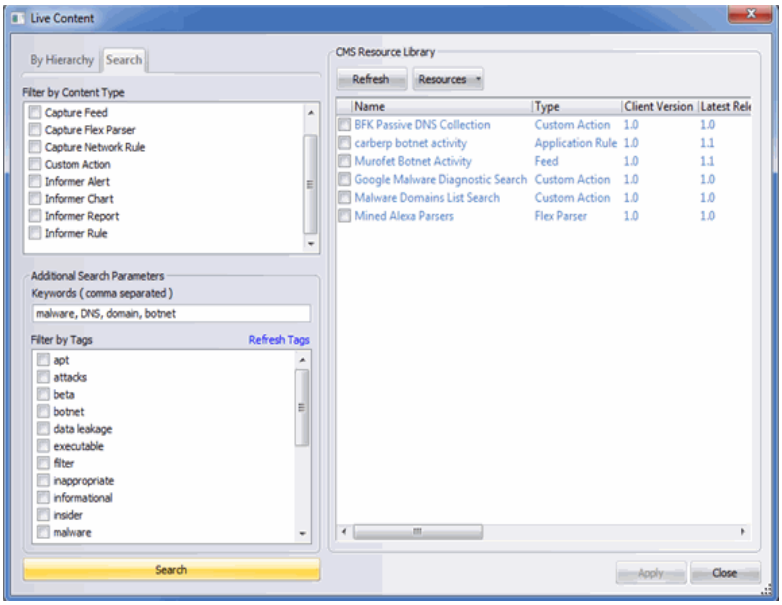
  Additional information about the displayed results are shown as you scroll to the right:

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.

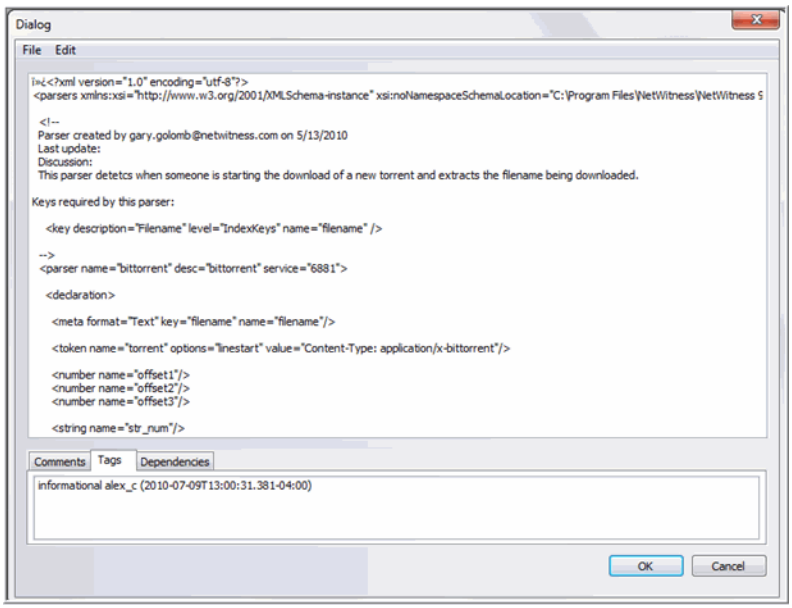


- The **Search** tab allows you to search your subscribed content on the system. You can narrow your search by content type, tag, and keyword.



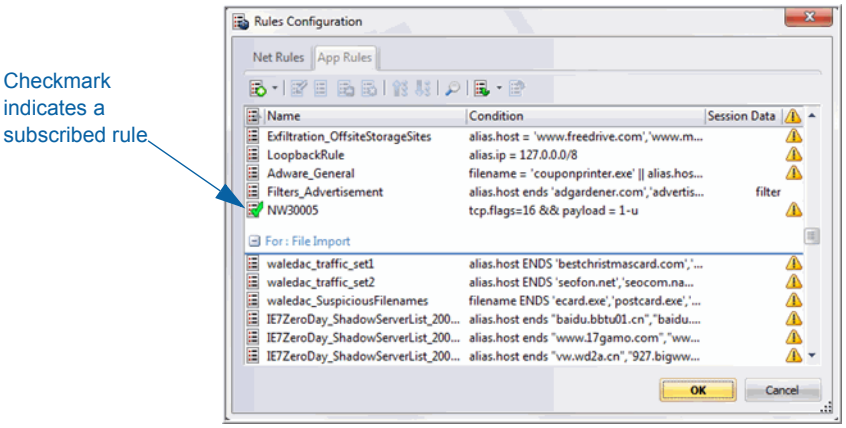
Preview Content

When browsing the content, you can click the **Preview** 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 (see page 50)

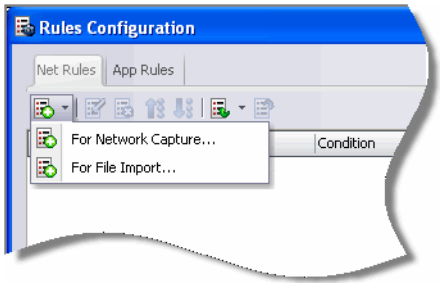
- Application Layer Rules (see page 53)

Network Rules are applied prior to session reconstruction and Application Rules are applied after session reconstruction. For additional information about creating rules, see *Rules* on page 91.

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.



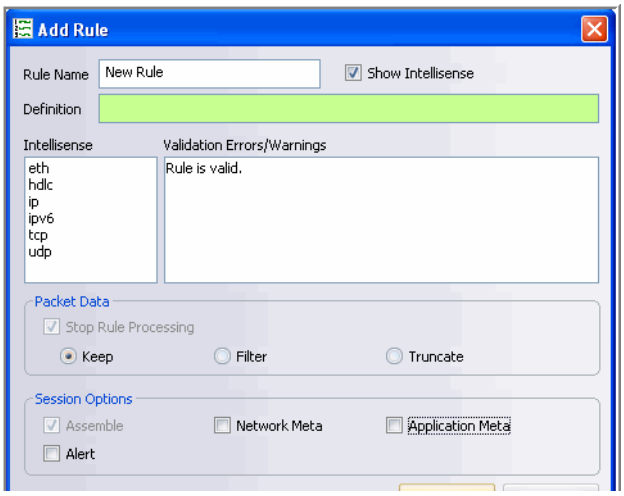
3. Click the **New Rule Type**  icon to specify whether the rule applies to:
   a. **Network Capture**

      or

   b. **File Import**

The same rules can be applied for both live **Network Capture** or **File Import**.

4. In the **Add Rule** dialog, 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.

If the **Stop Rule Processing** option is checked, network rule evaluation ends if the rule is matched.

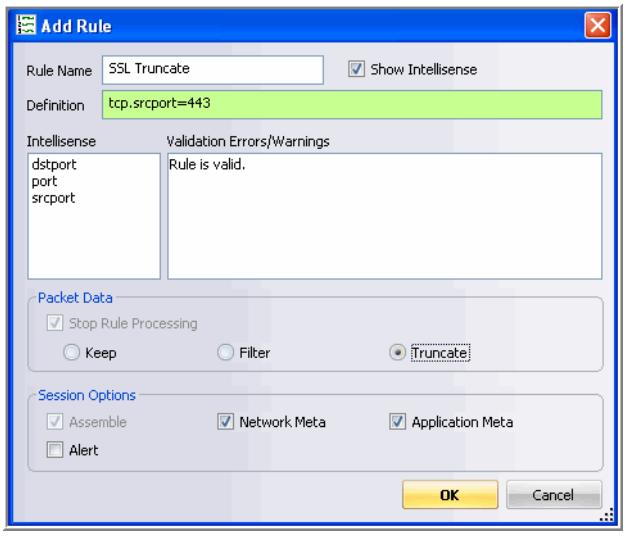
6. Click **OK** to submit the rule.

Intellisense lets you know that the rule you created is valid. For more information about capture rules, refer to *Rules* on page 91.

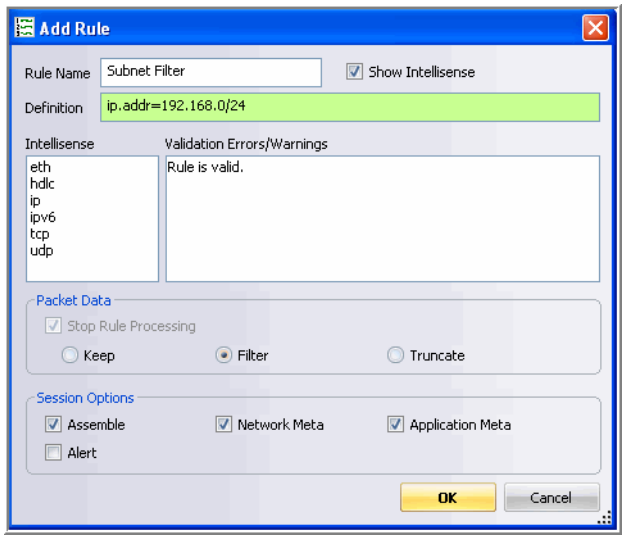
Rule Action	Description
Packet Data	
Keep	The packet is saved when it matches the rule.
Filter	The packet is not saved when it matches the rule.
Truncate	The packet payload is not saved when it matches the rule.
Session Options	
Assemble	The assembler assembles the packet chain when it matches the rule.
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

a. Truncate all SSL from the source port – **`tcp.srcport=443`**
Rule Action – Truncate

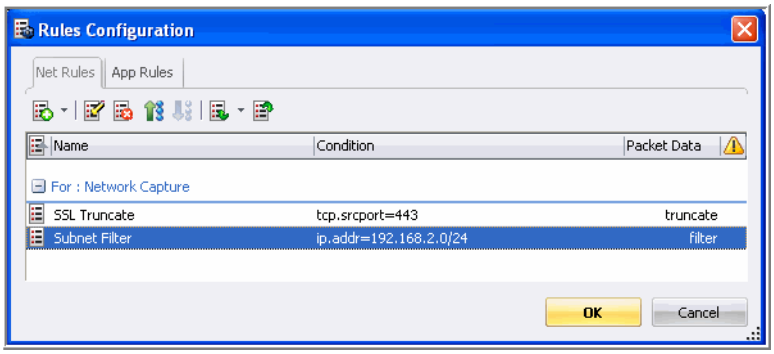


b. Create a subnet filter – **`ip.addr=192.168.2.0/24`**
Rule Action – Filter



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:

a. **Add** – Click the icon to continue adding new rules.

b. **Edit** – Click the icon to change the parameters of the existing rule.

c. **Enable**– Click the icon to make the selected rule active.

d. **Disable**– Click the icon to make the selected rule inactive.

e. **Delete** – Click the icon to remove the selected rule.

f. **Promote** – Click the icon to move the selected rule up in execution priority.

g. **Demote** – Click the icon to move the selected rule down in execution priority.

h. **Import** – Click the icon to load rules from a file and append to the rules list.

i. **Export** – Click the icon to save all rules to a file.

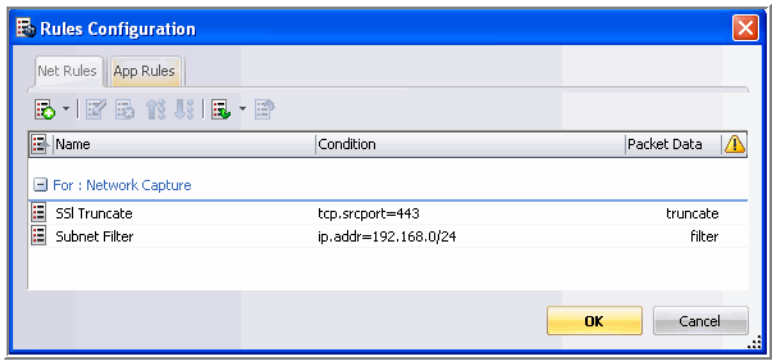
When you attempt to import a group of rules, INVESTIGATOR checks the type of rules imported. If you are successful, a message displays the number of rules imported. If the rule type differs from the active tab type, you must re-import the group under the correct tab or select another file to import.

Application Layer Rules

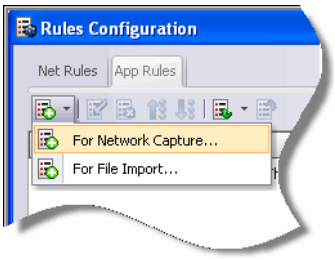
Application layer rules are applied at the session level. Once the first application layer rule is hit, rule evaluation stops. If the first rule listed is not a match, INVESTIGATOR then attempts to match the next rule listed, until a match is found.

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:

a. **Add** – Click the icon to continue adding new rules.

b. **Edit** – Click the icon to change the parameters of the existing rule.

c. **Enable**– Click the icon to make the selected rule active.

d. **Disable**– Click the icon to make the selected rule inactive.

e. **Delete** – Click the icon to remove the selected rule.

f. **Promote** – Click the icon to move the selected rule up in execution priority.

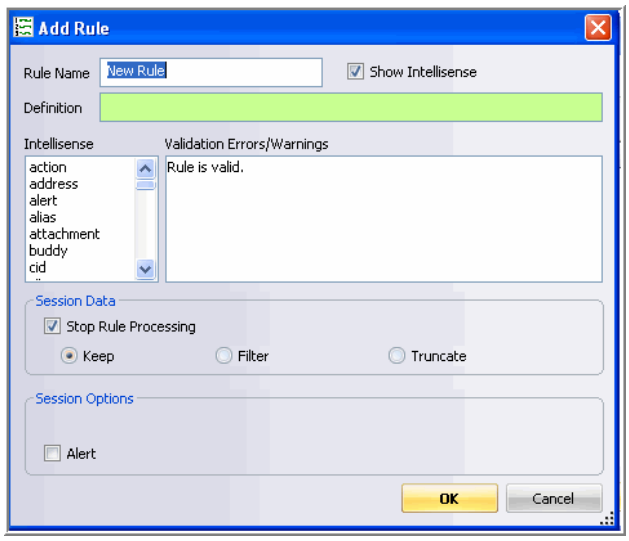
g. **Demote** – Click the icon to move the selected rule down in execution priority.

h. **Import** – Click the icon to load rules from a file and append to the rules list.

i. **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. For more information about capture rules, refer to *Rules* on page 91.

6. In the **Session Data** area, specify the action for the new rule.

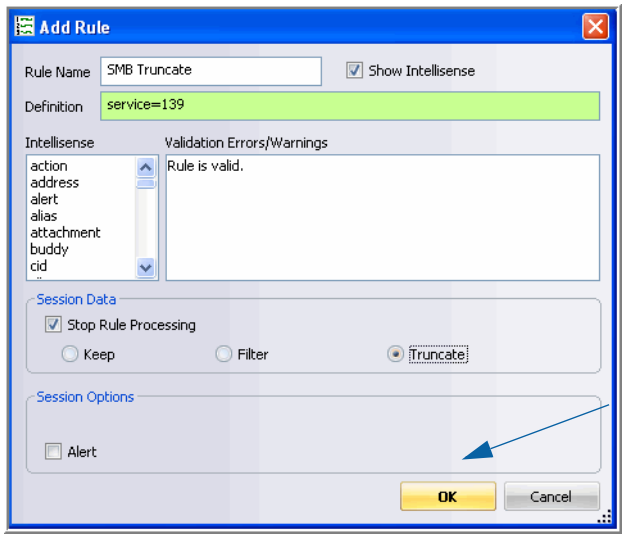
7. In the **Session Data** area, indicate whether you want an **Alert** to be created and verify that the new rule is valid.

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.

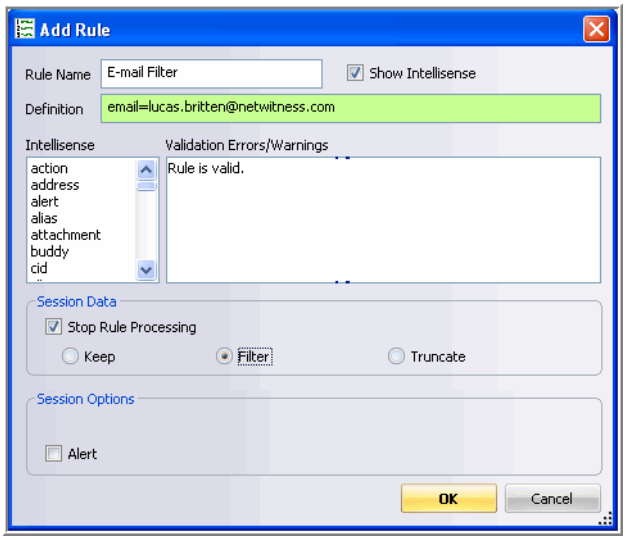
Sample Application Layer Rules

a. Truncate SMB – **`service=139`**
Rule Action – Truncate



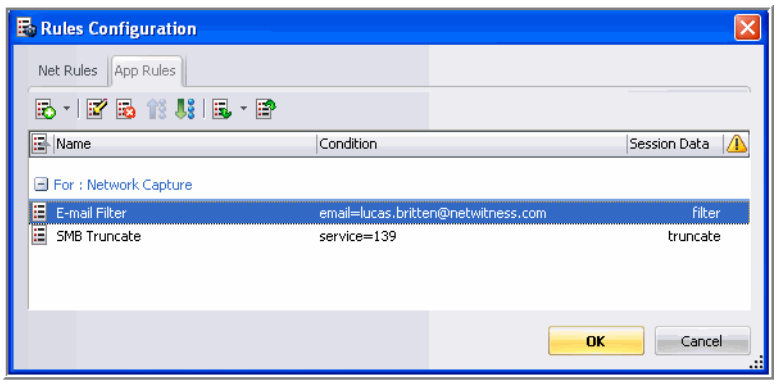
Select the type of report that is created when triggered by the rule.

b. 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:

a. **Add** – Click the icon to continue adding new rules.

b. **Edit** – Click the icon to change the parameters of the existing rule.

c. **Delete** – Click the icon to remove the selected rule.

d. **Demote** – Click the icon to move the selected rule down in execution priority.

e. **Promote** – Click the icon to move the selected rule up in execution priority.

f. **Import** – Click the icon to load rules from a file and append to the rules list.

g. **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.

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

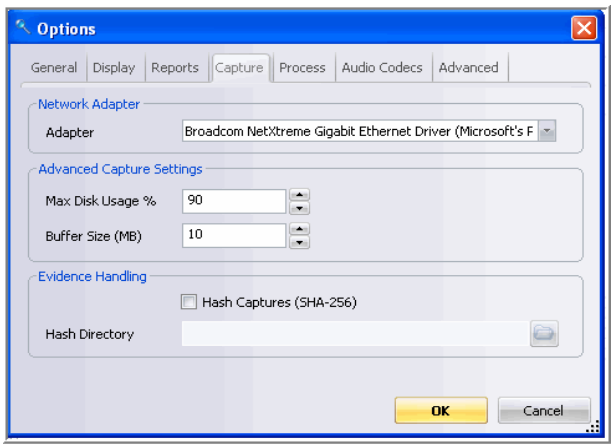
- **Advanced Capture Settings**
  - **Max Disk Usage–**The percentage of drive space allowed to be used by the system. If this value is 100, the drive is allowed to fill up completely.
  - **Buffer Size**(MB)**–**Specify the size in MB that is used to cache packets on the network card.
- **Evidence Handling–**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

For more information about wireless LAN capture, see *Capture Devices* on page 143.

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.

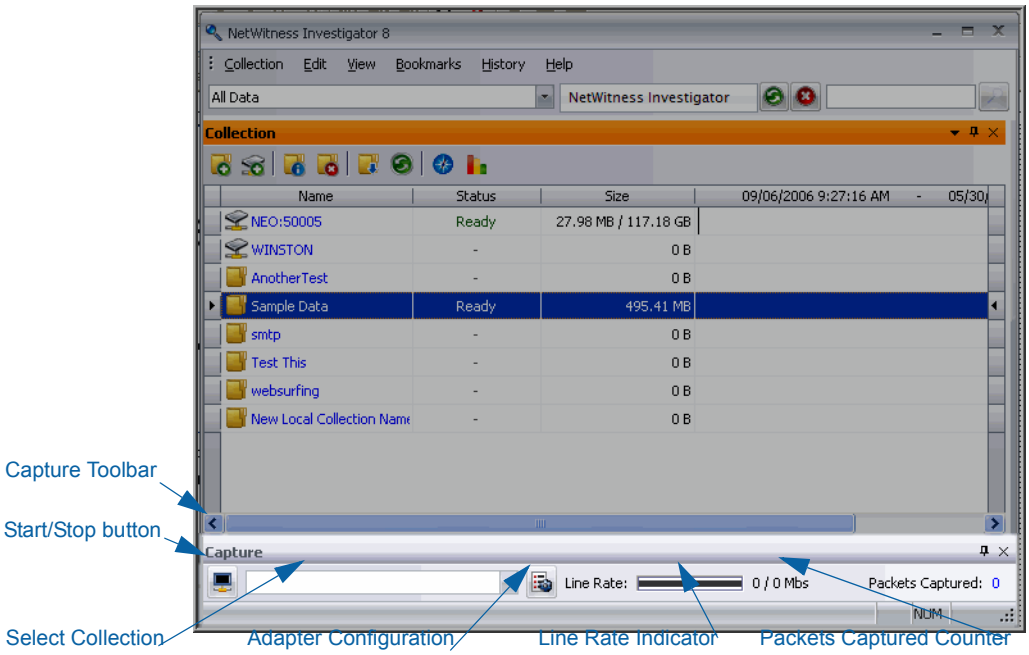
To protect the integrity of the hash values written during live capture, the user should consider designating an external drive for the hash value files.

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. For a more detailed description of its requirements, see *Wireless Packet Capture* on page 143.

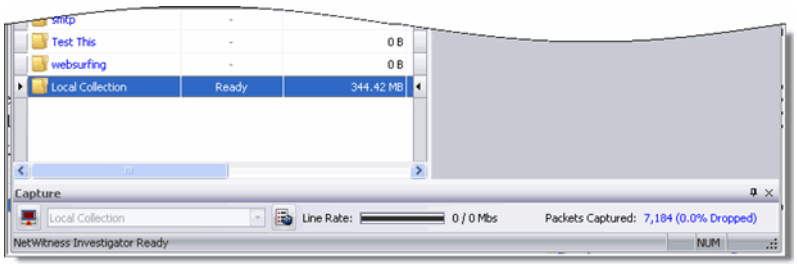
This feature may or may not be supported under your organization's license agreement with NetWitness. Please contact your account manager for more information.

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. (*Configure Parsers* on page 44)
2. Verify that the **Network Layer** and **Application Layer Rules** are correctly defined. (*Rules Overview* on page 49)
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.

- From the **Start** menu, select **Control Panel**.
- Open **Network Connections**.
- Position the cursor over a network connection and then right-click the mouse button. In the Options menu, select the **Properties** option.
- In the *This connection uses the following items* panel, clear all check boxes. Click **OK**.
- in NetWitness INVESTIGATOR, select the network adapter that you want use to collect data on the **Capture Configuration** dialog.

Chapter 6

Data Analysis

Introduction

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 (see page 65)
- **Search** – the mechanism to locate sessions with specified string values or regular expressions (see page 82)

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**(see page 64)
- **Navigation** (see page 65)
- **Session** (see page 78)
- **Content** (see page 82)

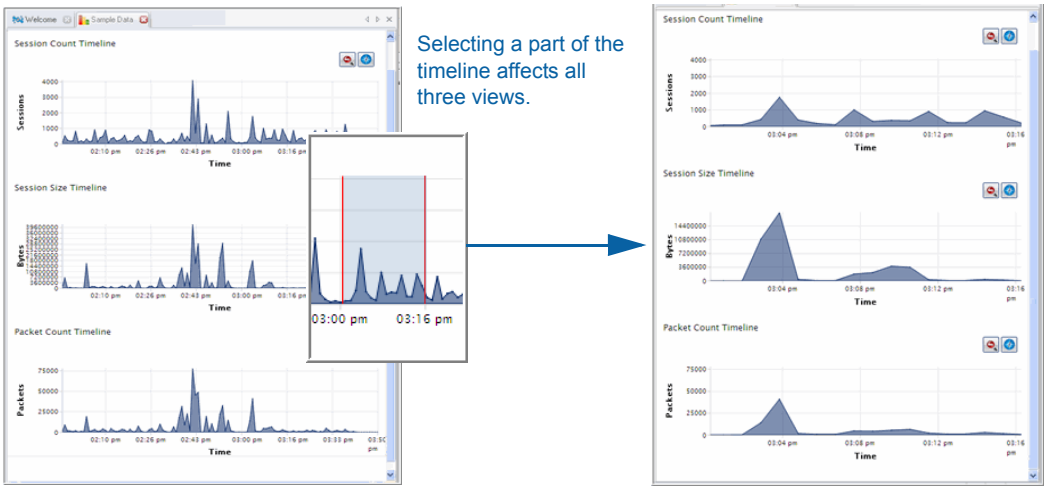
Summary View

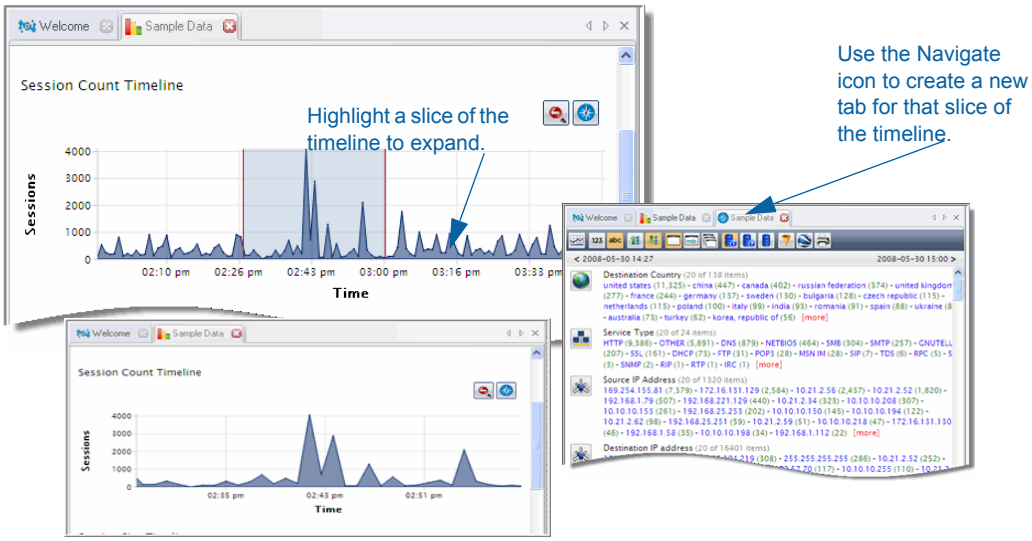
This is the highest level that you can look at the characteristics of a selected collection. There are three snapshots displayed over the timeline.

- 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.





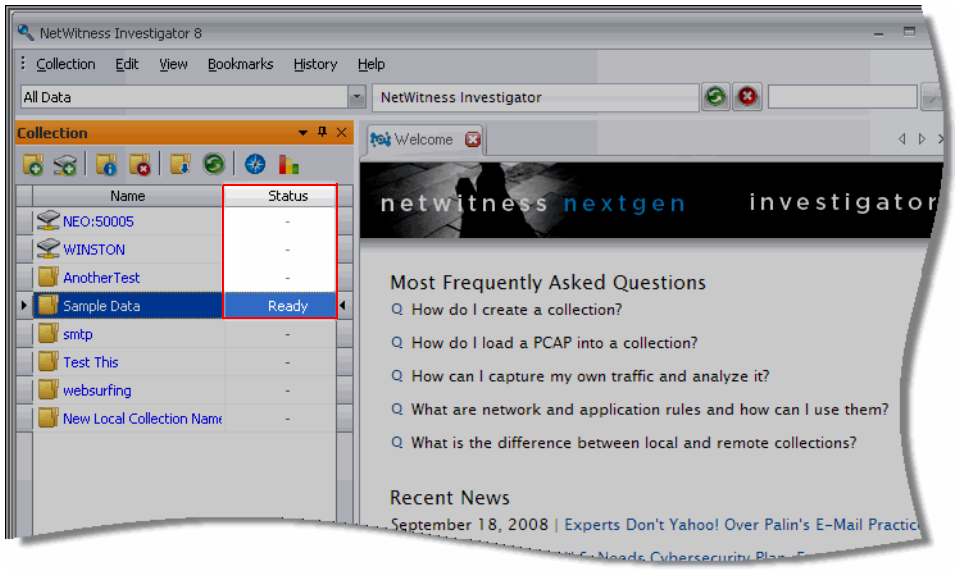
Navigation View

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.

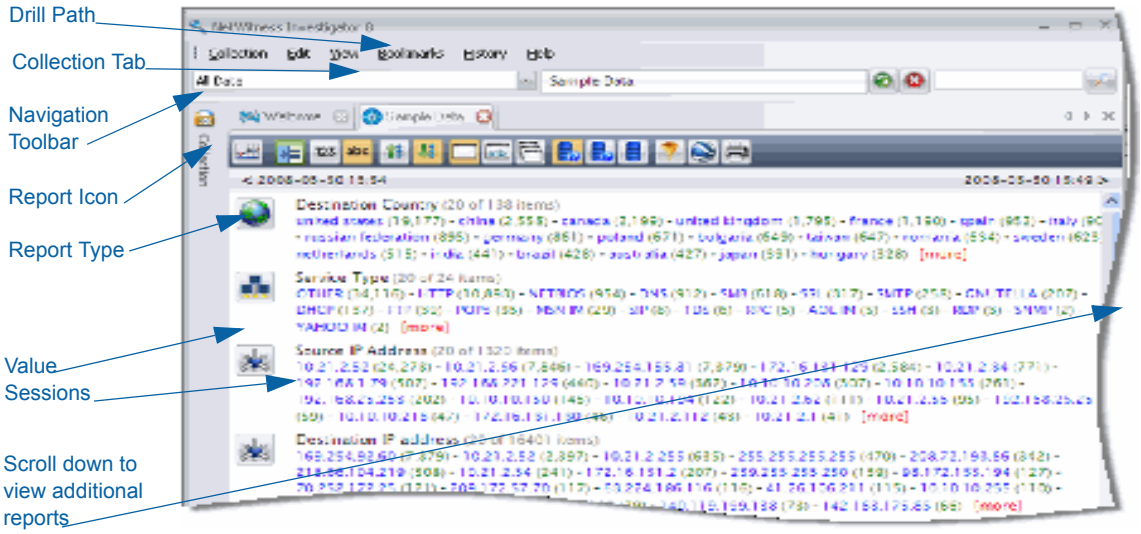
There may be circumstances that cause you to alter the order or deviate from this basic pattern. Your general knowledge about network traffic and that of your organization determines the perception of anomalous activity and how you use INVESTIGATOR to look more closely.

Select a **Collection** and double-click the name to connect to the database.
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. For more information on configuring the report display in collections, see *Reports* on page 26.



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 (see page 67)

Report Icon–Symbol for the report with a context menu for results display (see page 73)

Report Type–The items selected in the **Collection** configuration (metadata fields)

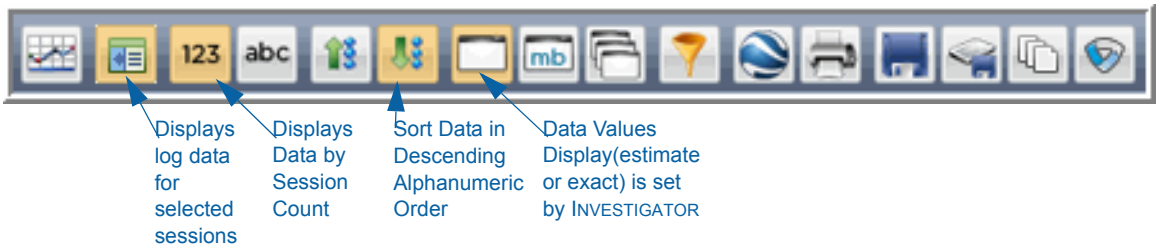
Value–The instances in the collection that match the **Report Type** (20 are displayed by default)

Sessions–The number of instances identified in the network data containing the specific metadata

Navigation Toolbar

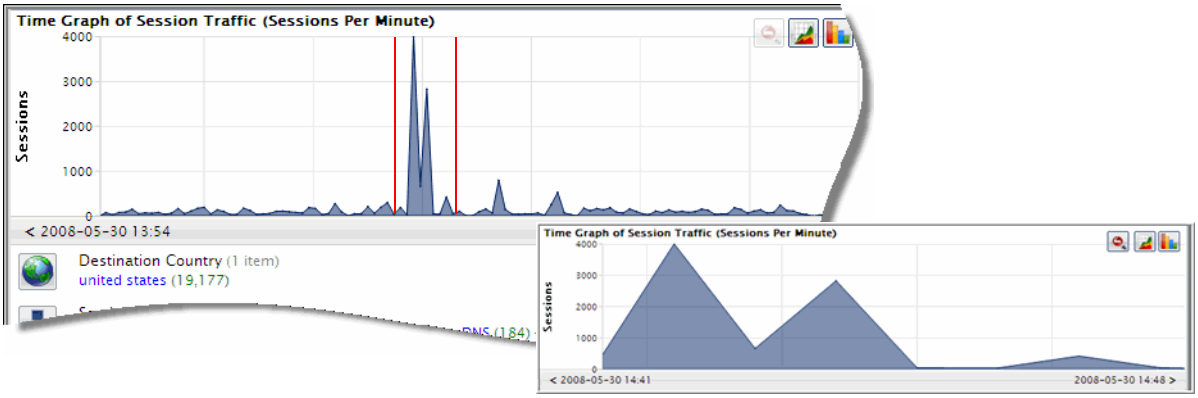
The appearance of the collection reports and the data contained are determined by the combination of selections you make on the **Navigation** toolbar.

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

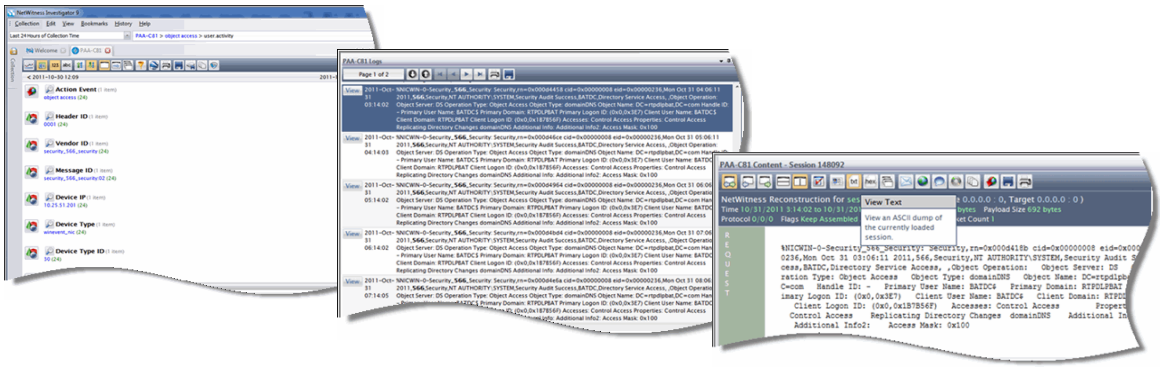


As each icon is selected, the resulting view is displayed in the following table:

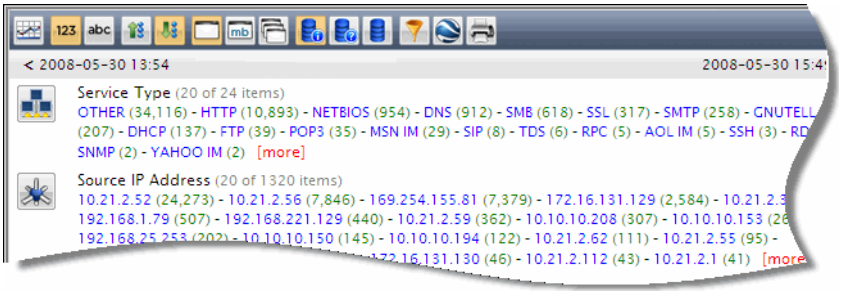
CLICK THIS...	TO DISPLAY DATA...
Time Graph	
	Time Graph–Shows session traffic (sessions per minute) in your current drill. You can select a part of the graph to expand the view.



CLICK THIS...	TO DISPLAY DATA...
View Log Data	
	Log Data–Shows the log packets created by the Series 4 LOGDECODER for the current session. You can select a particular log event to view as a text file for more information.



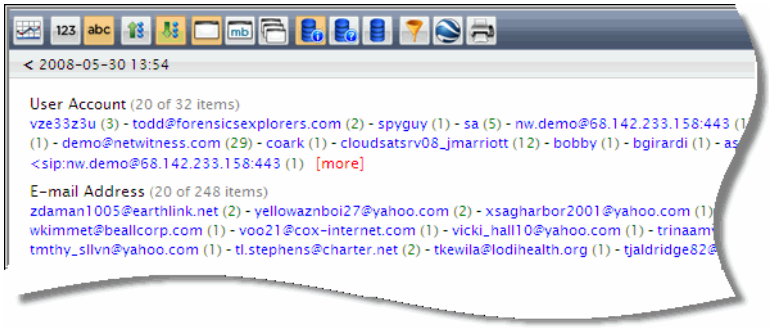
Sort Data	
	Sort by Count–Arranges the data by number of sessions.



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

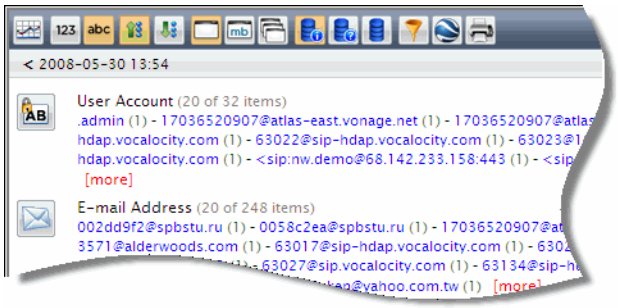
	Sort Alphanumeric–Arranges the data by alphabetic order. If there are numbers as part of the value or alias, they will precede the first alphabetic value.

CLICK THIS...	TO DISPLAY DATA...



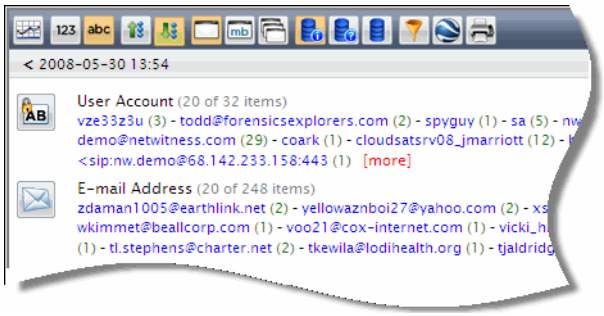
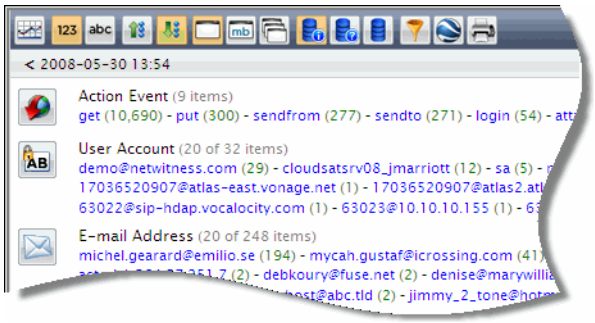
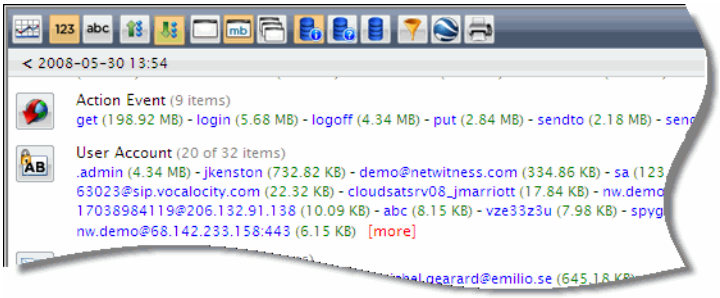
NOTE: When you sort the data by alphanumeric order, the default descending setting is still operant.

Arrange Data	
	Ascending Order: ◆ Numeric–Arranges the data from least to greatest. ◆ Alphabetic–Arranges the data in a-z order.

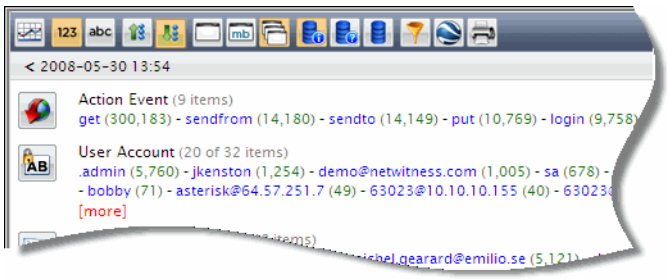


NOTE: When you sort the data in ascending order, the alphabetic order setting is still operant. The leading **.** character (**.admin**) is listed before the first numeric character.

	Descending Order: ◆ Numeric–Arranges the data from greatest to least. ◆ Alphabetic–Arranges the data in z-a order.

CLICK THIS...	TO DISPLAY DATA...
	
Session Quantifier	
	Session Count–Displays the metadata by session count. **NOTE:** 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 **NOTE:** 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 **NOTE:** The values are displayed according to the number of packets for each value in descending order.



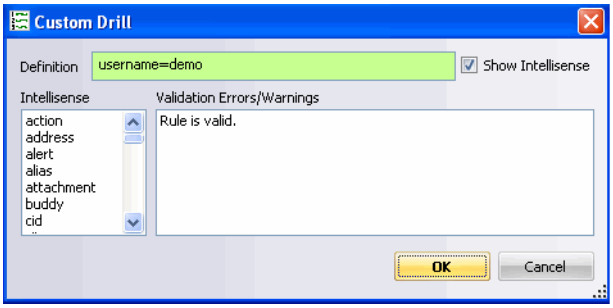
Index Calculation

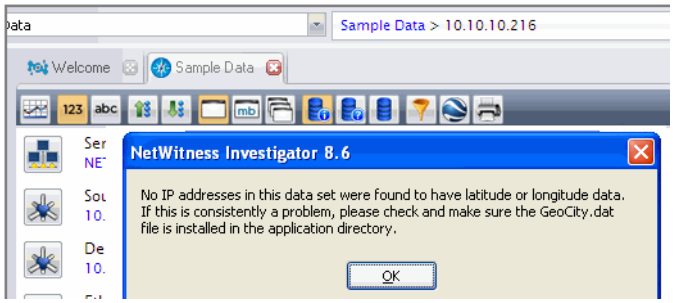
These options determine how INVESTIGATOR displays values totals.

	Hybrid (Normal)–INVESTIGATOR decides when to display exact or estimated values.
	Estimates (Fast)–This is the fastest way to obtain results, but is the least accurate.
	Exact (Slow)–Depending on the amount of data being indexed, this can slow operations considerably. If Navigation is taking too long to load, switch to Estimates.

Actions

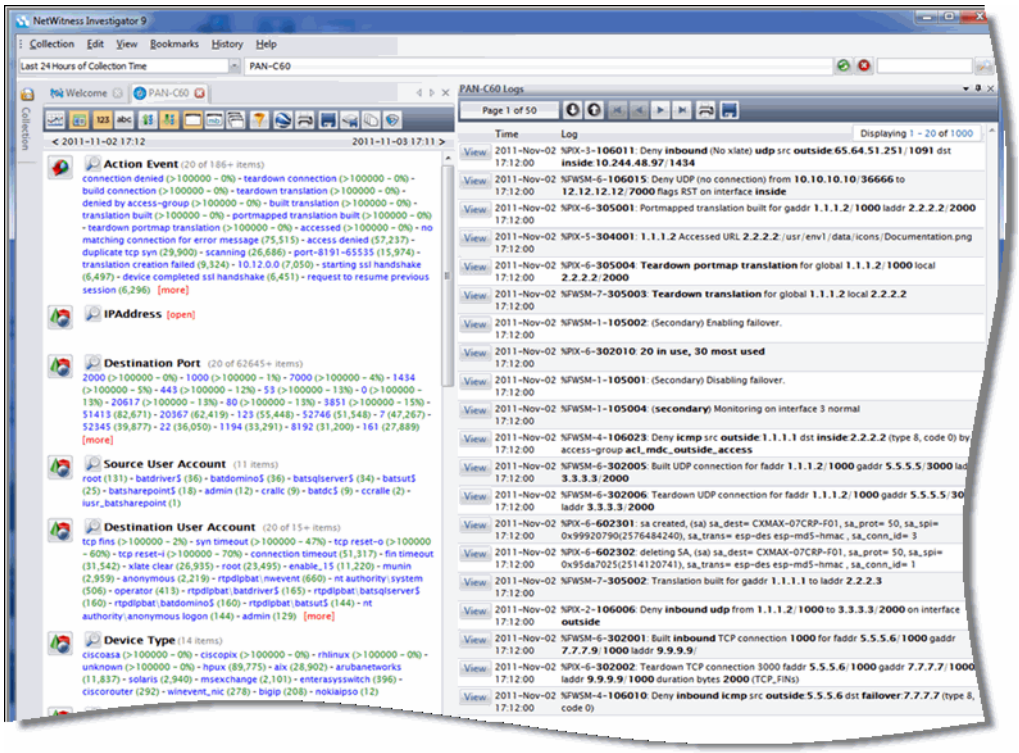
	Custom Drill–The user defines the drill criteria.



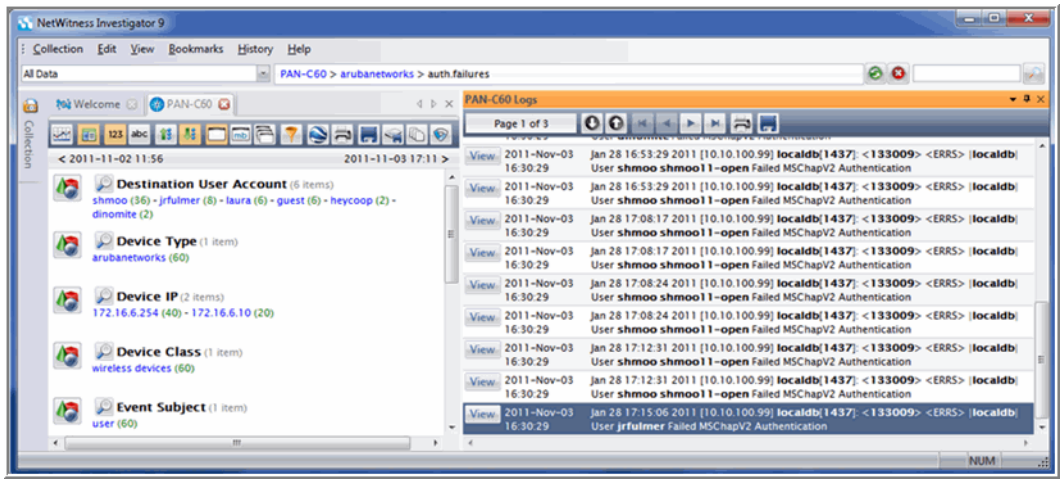
CLICK THIS...	TO DISPLAY DATA...
	View the Session in Google Earth– Using SHIFT+ icon bypasses the dialog box and displays the last session viewed.
	
	Print–The displayed content is printed.

View Logs

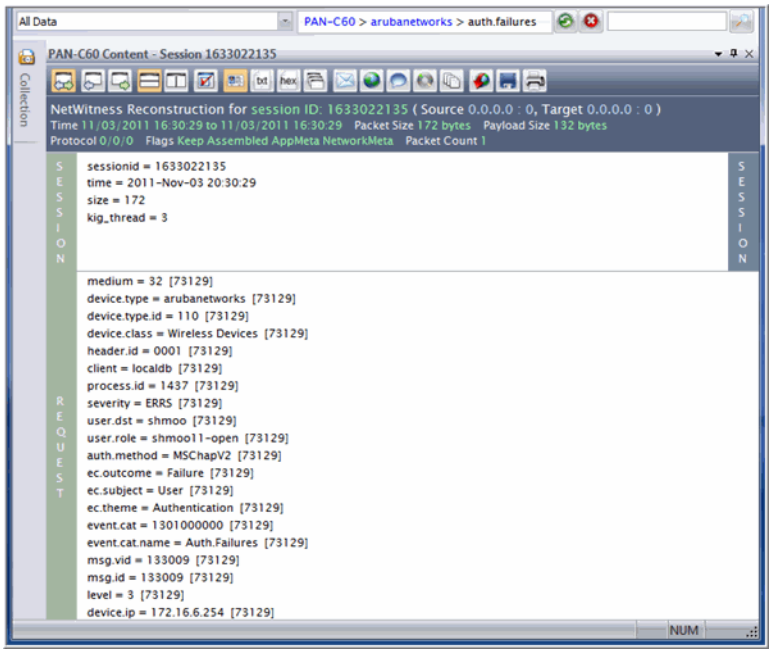
When the LOGDECODER is part of your organization's architecture, the **Log Data** icon displays the raw logs in time order.



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



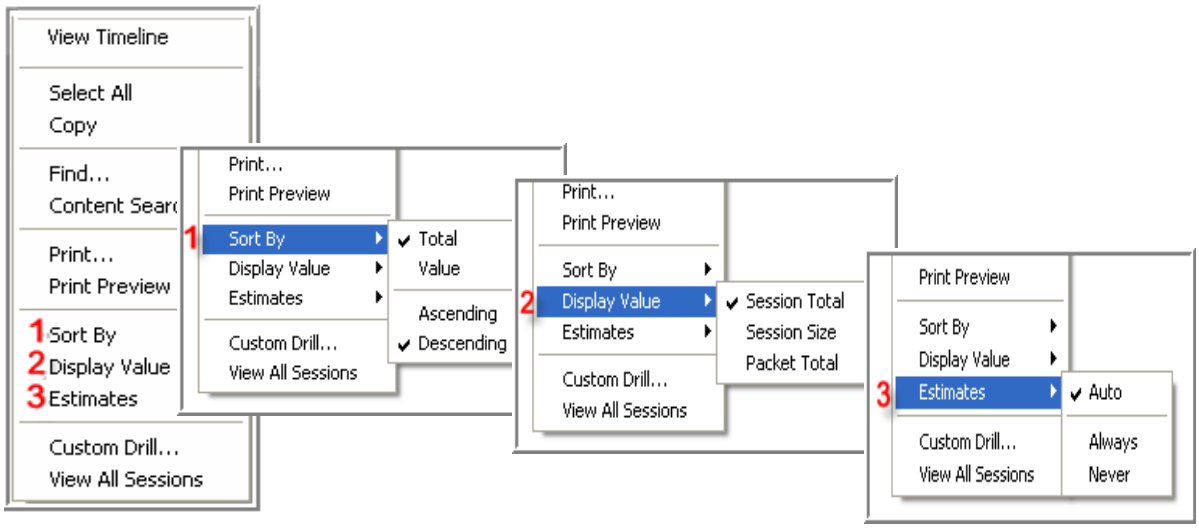
If you click on the VIEW button for a specific log event, you can view the details for the currently loaded session.



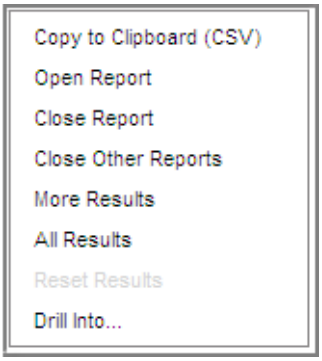
Context Menus

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.

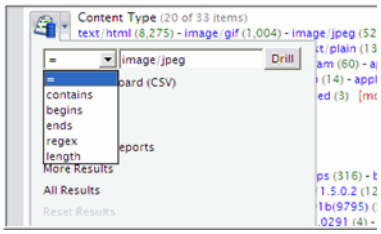
Navigation Context Menu

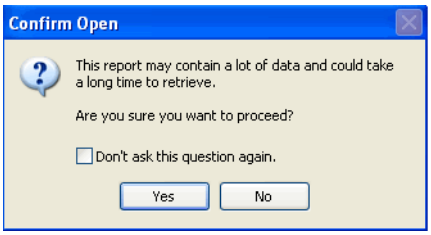


The reports display the first 20 results by default. If **[open]** or **[more]** is displayed at the end of the list of value, that means that there are more results that you can view. When you click on a **Report** icon, the following options are available:



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

OPTION	DESCRIPTION
Drill 	Allows the user to define a **custom query?**. The resulting Navigation view allows for all report operations, including drilling and the viewing of session listings.
Copy to clipboard	Copies comma separated values (CSV)

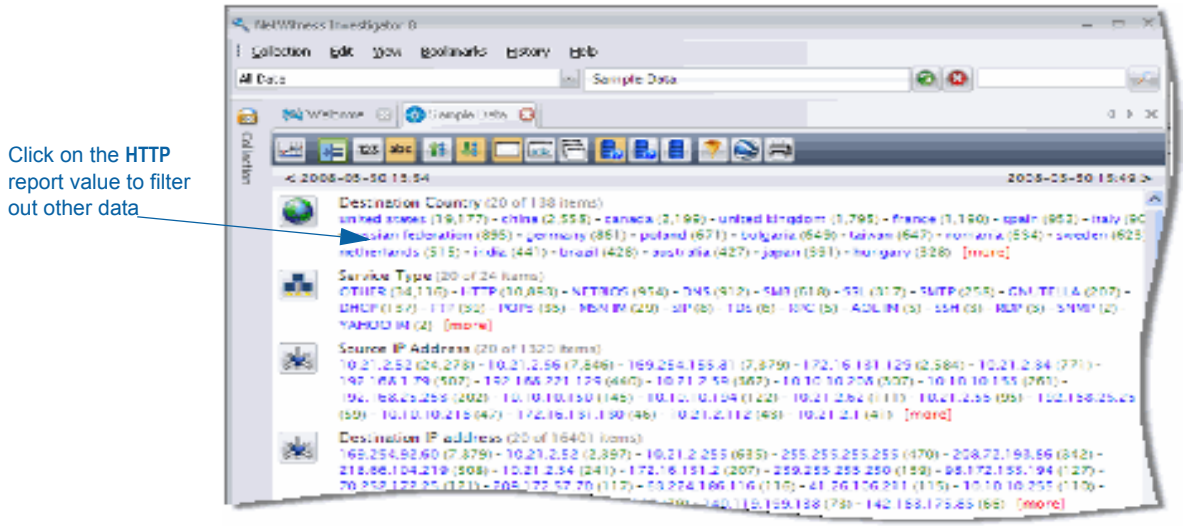
OPTION	DESCRIPTION
Open Report	To open the report, the user must confirm that the process may be time-consuming in **Confirm Open** dialog: 
Close Report	Returns the display to hidden
Close Other Reports	Closes all the reports
More Results	Displays an additional 20 values
All Results	When there are large numbers of results, the user must specify a maximum number (1000, 2500, 5000, etc. to 50000) to display
Reset Results	Returns the display to the original default 20 values
Drill into...	Allows the user to input specific values for a **custom query?**. The result set is a Navigation view, which will allow for all report operations, including drilling and the viewing of session listings.

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.

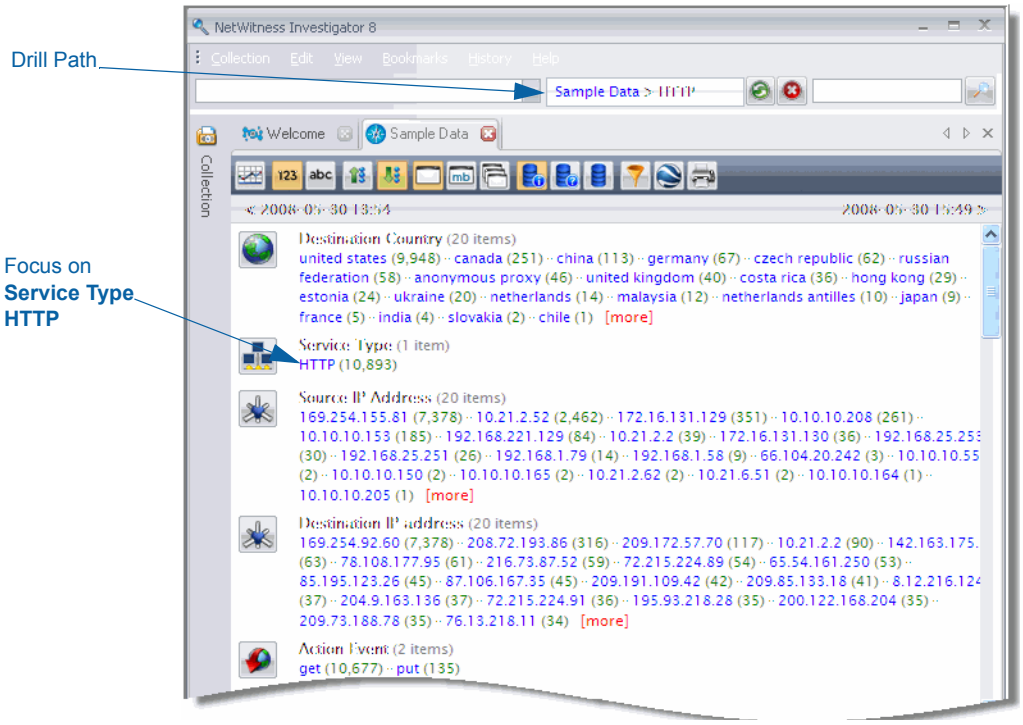
Create a New Tab

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**.

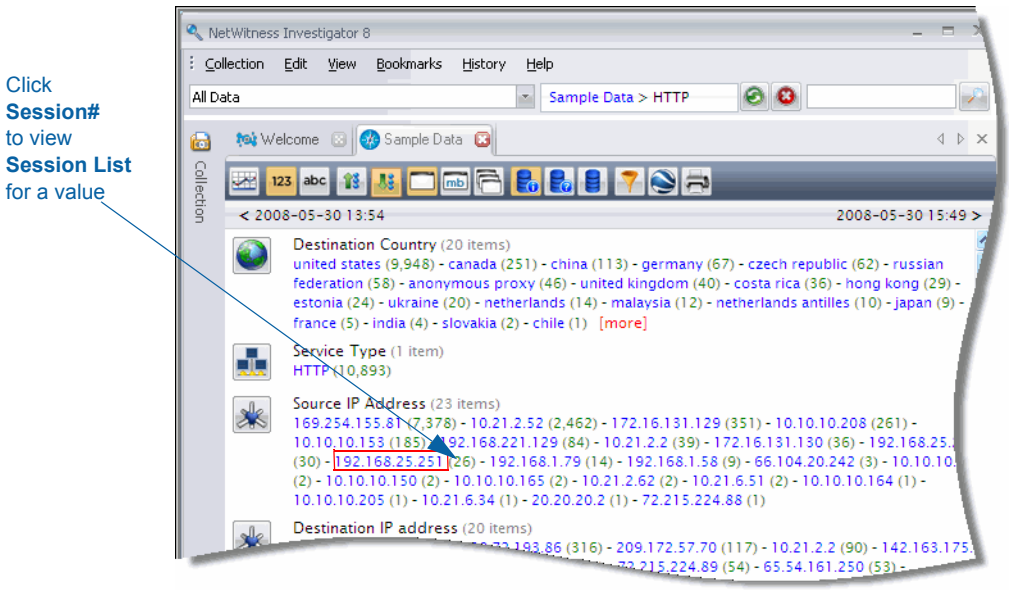


At this point, you must evaluate the **Report Values** and **Session** counts to determine the next item of interest. Possible drills of interest might include an additional filter for:

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

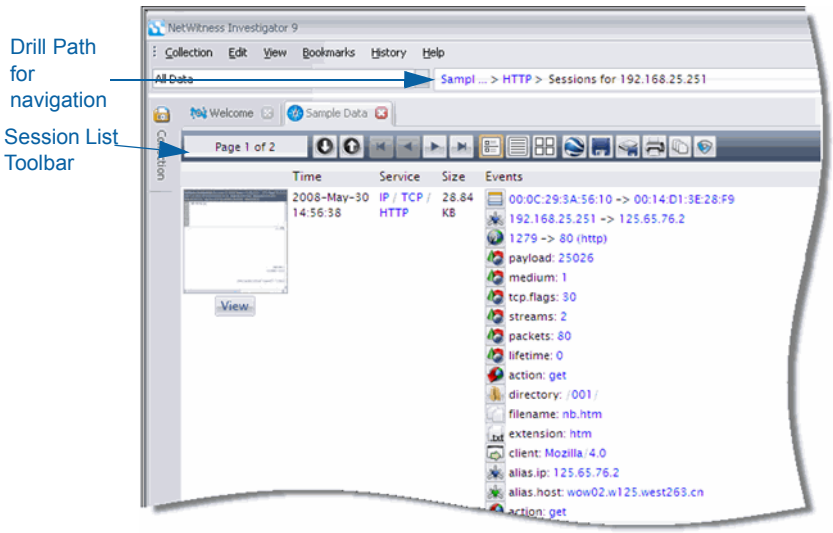
View Sessions

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.

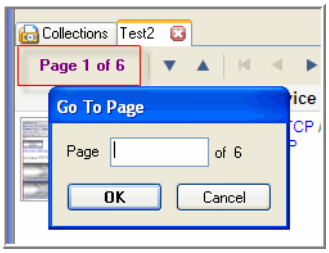


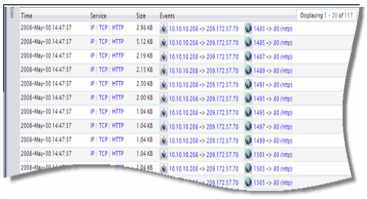
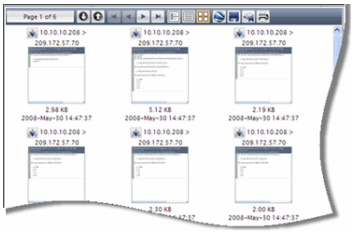
You can use the **Session List** toolbar to:

- 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 (see page 67).

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** **(see page 14)****.**
	**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

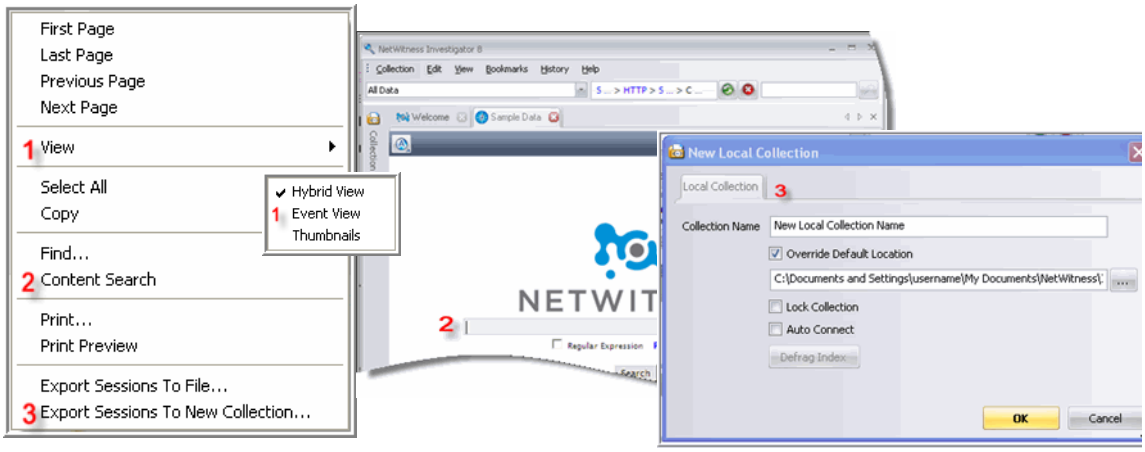
FUNCTION	DESCRIPTION
	Last Page– Moves the view to the last page
Display Control	
	Hybrid View– Displays the session details and thumbnails.
	
	Event View– Displays each session on the page in one line (Time, Service, Size, Events) with hyperlinks to create a new drill.
	
	Thumbnail View– The sessions appear as thumbnail images. This serves as a preview for session content. Click on the image to view the content for that session.
	
Actions	
	Google Earth Session View– Displays the session on Google Earth (see page 81).

FUNCTION	DESCRIPTION
	Export– Export the sessions in the current Session View list to either an external .pcap file or to a new Collection.
	Print– Print the session information in the current view.

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.

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

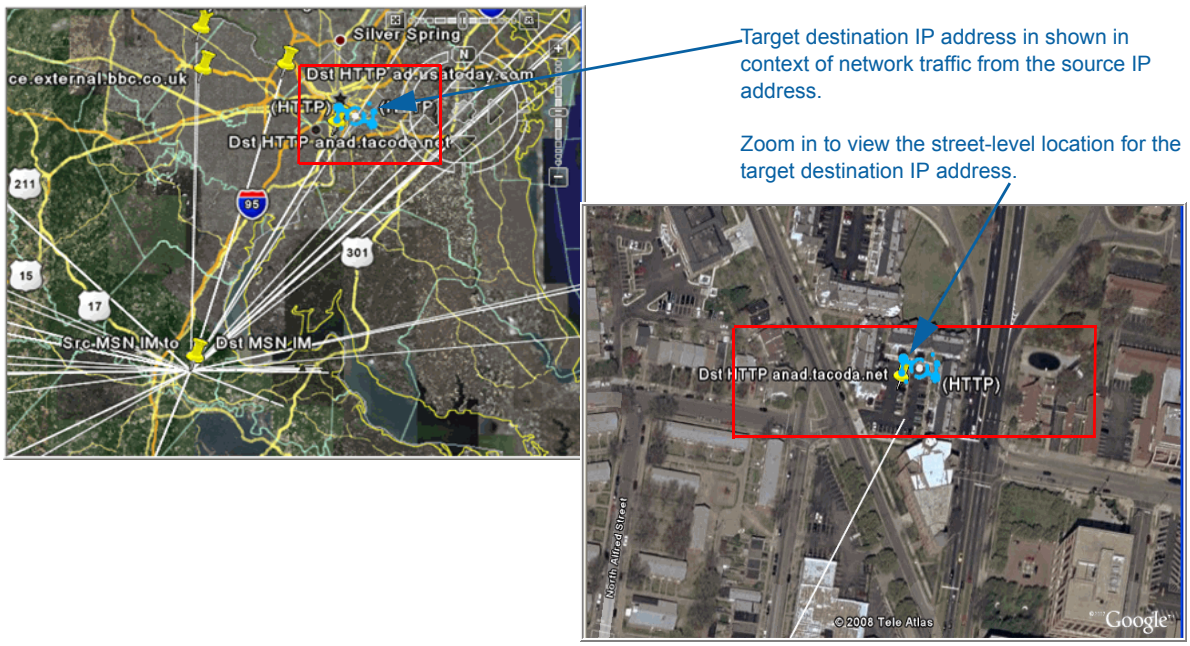


Display Sessions on Google Earth

This feature uses Google Earth to map session activity from source and destination IP addresses, using the **GeoIP** database. By default, NetWitness installs the GeoIP Lite version of the database.

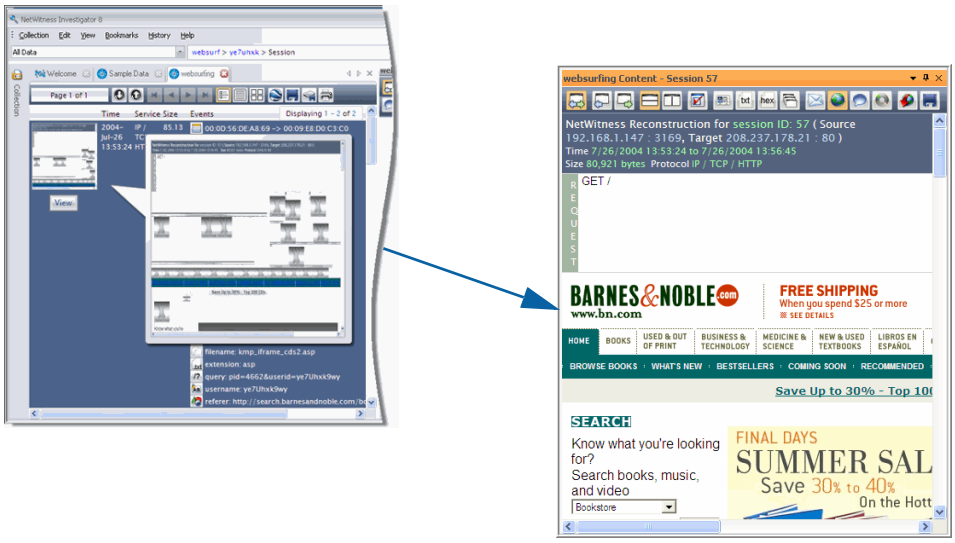
You must enable the **GeoIP** parser to see this functionality.

PATH: `Edit` → `Options` → `Process`



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 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 **Details** summary for each side of session (IP address, port, number of packets, bytes for Data and Payload, and Flags, if applicable).
	VIEW TEXT View data in text format.
	VIEW HEX View data is **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.

CLICK THIS...	TO VIEW THIS...
	PLAY AUDIO Access data in audio (**VoIP**) format.
	OPEN PCAP Open the currently loaded session as a PCAP.
	EXPORT SESSION Export the currently loaded session.
	PRINT SESSION Prints 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

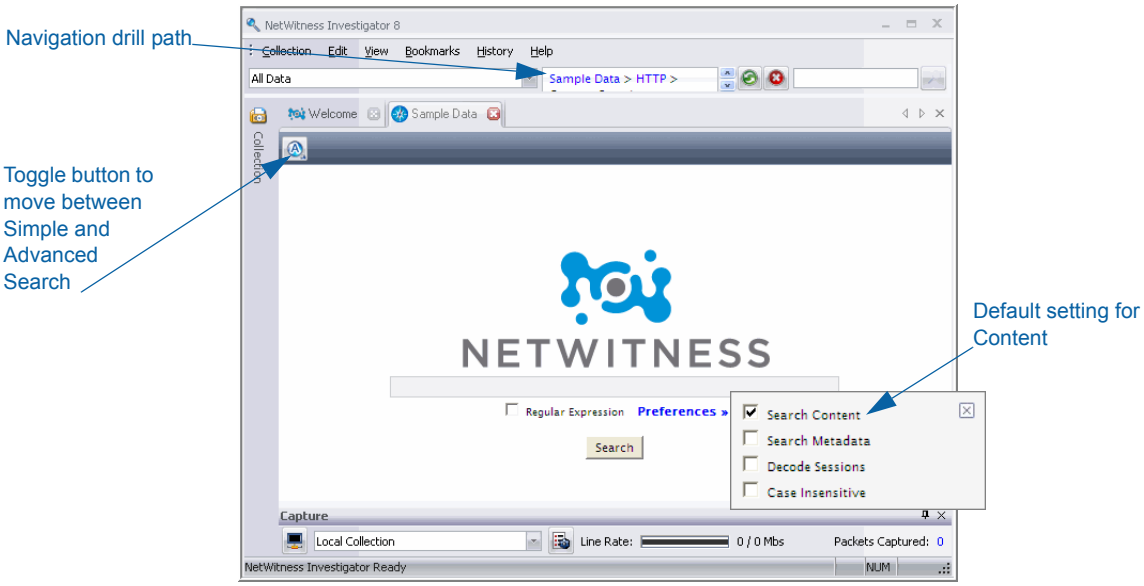
NetWitness Search allows users to search collections for keywords and regular expressions (pattern matches). You have the option to create a new search or use any combination of various common search criteria (e.g. social security numbers, credit card numbers, EIN tax numbers) found in a compiled library.

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

Simple Search

To search a collection:

1. Open and navigate to a collection from the list of NetWitness Collections. Click the **Content Search** icon found on the **Collection Toolbar**. 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. For more details about preference options, see *Search Preferences* on page 85.

2. 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 will notify the user of an invalid query. If **Regular Expression** is not enabled, the search engine will treat 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

3. Click on the 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** will only search 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.

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.

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

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**.

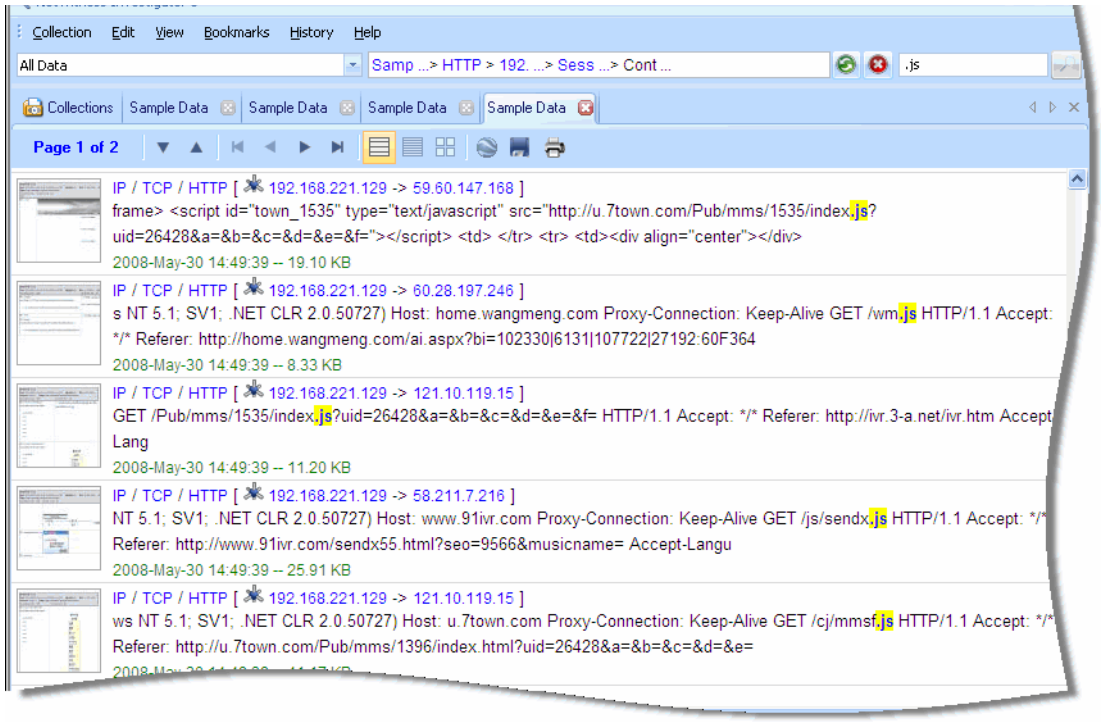
Advanced Searches created by a user must be given a name, description, and search string before they can be saved. These saved searches continue to exist until they are deleted by selecting the search to be deleted and clicking the **Delete Search** text.

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:

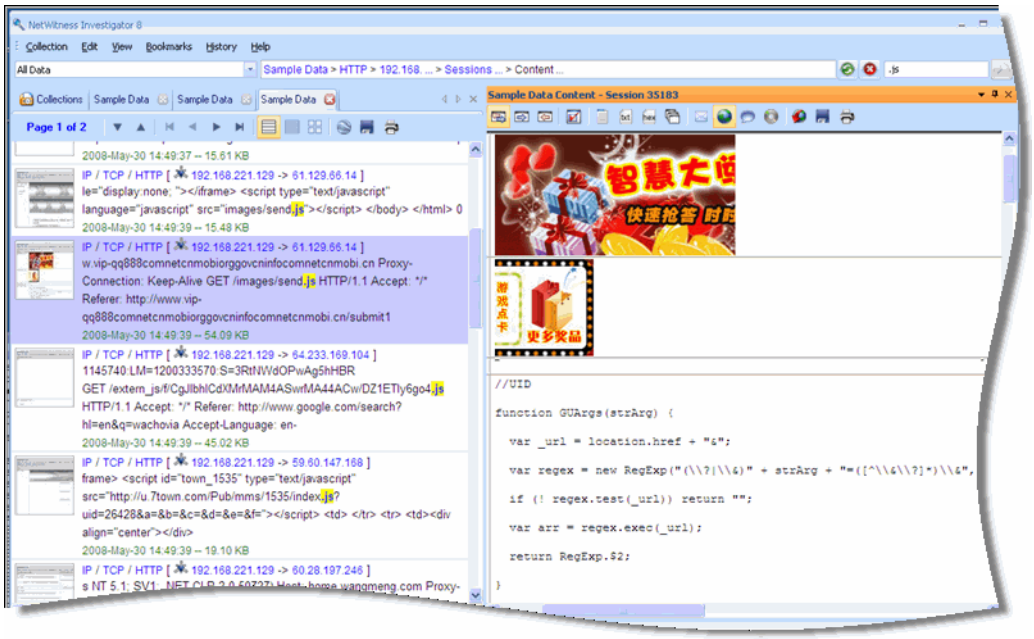
- Export the results to another collection for further searching and navigating (Click the **Export** icon on the toolbar)
- Export the results to a **.pcap** file (Click the **Export** icon on the toolbar)
- Page through the results using the paging controls on the top toolbar
- Change the number of 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.

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.

Appendix A

Rules

Introduction

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.

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.

Session Options

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/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
&&	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`

SYNTAX	DESCRIPTION
()	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. Refer to *Parsers and Associated Metadata* on page 110 for the metadata fields supported for use in 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. See *Ethernet Protocol Reference List on page 121* for a list of possible values and descriptions.
fddi.addr	Fiber Distributed Data Interface (FDDI) physical source or destination address. Same concept as the Ethernet address. FDDI is an older Layer 2 protocol that has largely been replaced with Ethernet. However, it may still be found in some older networks.
fddi.dst	Same as the Ethernet destination except uses the FDDI address.
fddi.src	Same as the Ethernet source except uses the FDDI address.
fddi.type	Frame type of the FDDI frame.
hdlc.addr	High-level Data Link Control physical source or destination address. Same concept as the Ethernet address.
hdlc.dst	Same as the Ethernet destination except uses the HDLC address.
hdlc.src	Same as the Ethernet source except uses the HDLC address.
hdlc.addr	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.

METADATA	DESCRIPTION
ip.proto	IPv4 protocol field. *Internet Protocol Reference List* on page 128 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 128 for a list of possible values and descriptions.
ipv6.src	Source IPv6 address in hex format.
tcp.dstport	Destination TCP port. See *TCP Protocol Reference List* on page 133 for a list of common TCP port assignments.
tcp.port	TCP source or destination port.
tcp.srcport	Source TCP port.
tr.addr	Token Ring source or destination address.
tr.dst	Destination Token Ring address.
tr.src	Source Token Ring address.
tr.type	Token Ring frame type.
udp.dstport	Destination UDP port. See *UDP Protocol Reference List* on page 136 for a list of common UDP port assignments.
udp.port	UDP source or destination port.
udp.srcport	Source UDP port.
eth.addr	Ethernet source or destination address. Commonly known as the MAC address.

Appendix B

Custom Parsers

Introduction

The NetWitness parsing engine allows the user to customize definitions of the core parsers for parsing network data. These parsers, known as the FLEXPARSE™ tool, are loaded and compiled when either processing capture files in INVESTIGATOR or capturing data with DECODER. Most commonly, they are used for static meta extraction and service identification. This flexible definition allows users to easily extend the core NetWitness-defined services to provide extra service type identification and metadata extraction. This is important in today's world due to the volume of custom applications that are used on networks around the world.

Each custom parser is defined as an XML-formatted **.parser** file. Each definition file must contain at least one parser definition but may contain more. When the definition is created in a text editor that understands the XML format, it is possible to provide full syntax validation as well as *Intellisense* support for the designer.

Types of Custom Parsers

There are two types of custom parsers:

- **Service identification based solely on port.** These are parsers that just use the source and/or destination ports to identify the session application type (service). These are the most basic, easiest to define.
- **Service identification based on a found token(s).** These parsers use tokens to identify the service type. This is also an easy way to expand which service types are identified. These are important when identifying non-internet standard applications. These parsers require that the protocol has a definable token that can uniquely identify the service type.

Language Definition

The following table describes the XML schema used to define a parser using the FLEXPARSE™ tool. The XML node, attribute, and values referenced in descriptive text are **bold**. The root node of every file must be the **parsers** node. Under that node there can be any number of **parser** nodes. Each **parser** node defines a single parser. A **parser** node can have an optional **declaration** node and any number of **match** nodes.

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
parsers	The root node in each definition file.	
	xmlns:xsi	Defines the namespace to use for the schema inclusion. This attribute is not required; however, language definition is not possible without it. This node must have the following value: **http://www.w3.org/2001/XMLSchema-instance**
	xsi:noNamespaceSchemaLocation	Defines the XSD schema validation file used to validate the language definition. This attribute is not required; however, language definition is not possible without it. This node must have the following value: **parsers.xsd**
parser	The node that defines a single parser definition. This node must be directly under the **parsers** node. There can be more than one per file.	
	name	The name that uniquely identifies the parser. This name should be short and succinct. This is used by the system to allow enabling and disabling. It should contain only the letters [a-z] and [A-Z].
	desc	This node provides a friendly description of what the parser does.
	service	This is the unique number assigned to the session when identified.
declaration	The node that delineates the definition. Each of these definitions can have an associated **match** entry.	
token	Specifies a definition for identifying a token somewhere in the session protocol. This defines a **match** callback when the specified tokes in encountered in a session payload. The **read** position is set to the byte immediately following the matched token.	
	name	This is a unique identifier for the declaration.
	value	This is the exact token value to be identified.
	options	Options specify that the token should start on a new line or at end of a line (**linestart** or **linestop**).
number	Defines a numeric variable that can be referenced elsewhere within the parser definition. All numeric values are 64-bit unsigned values.	

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can either be for each side of a two-sided session or only after a new session is detected. The possible values are **global**, **constant**, **stream**, and **session** (default).
string	Defines a numeric variable that can be referenced elsewhere within the parser definition.	
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can either be for each side of a two-sided session or only after a new session is detected. The possible values are **global**, **constant**, **stream**, and **session** (default).
port	Defines a **match** callback when a session is encountered using the specified port. The **read** position is set to the first byte of the first stream (client) in the session.	
	name	This is a unique identifier for the declaration.
	value	This is the port number to identify.
session	Defines a **match** callback for session begin/end events. These events only occur if a token for the parser is encountered in the session.	
	name	This is a unique identifier for the declaration.
	value	Specifies that processing takes place at the beginning of a new session or at the end of a session (**begin** or **end**).
stream	Defines a **match** callback for stream begin/end events. These events only occur if a token for the parser is encountered in the stream.	
	name	This is a unique identifier for the declaration.
	value	Specifies that processing takes place at the beginning or at the end of a stream (**begin** or **end**).
meta		
	key	Specifies the key name. The key needs to be 1-16 bytes in size.
	format	Specifies the variant type (e.g. **Text**, **IPv4**, **UInt32**). Refer to the SDK documentation for a full list.
pattern	Defines a regular expression variable for use by the **regex** function.	
	name	This is a unique identifier for the declaration.
	scope (optional)	Specifies when to reset the variable. This can be for each side of a two-sided session or only after a new session is detected. Possible values are **global**, **constant**, **stream**, and **session** (default).

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
	value (optional)	Specifies a regular expression to assign to the pattern variable. This attribute is only valid when the **scope attribute** is set to **constant**.
match	The possible entries for taking an action once a match criterion has been found for a declaration. These nodes can be nested to provide deeper logic. There are several categories of execution elements (functions) that can appear as children of a match element: ◆ General ◆ Arithmetic ◆ String ◆ Payload	
General Functions		
identify	Marks the session with the parser's service type if the service type has not already been identified.	
assign	Assigns a value to a variable.	
	name	The unique identifier assigned to the item in the declaration section.
	value	Optional. If specified, the action defined in the match is only applied when the declaration matches the given value.
end	This terminates the execution of the current **match** section.	
if	Compares two values. If the comparison is true, executes any sub-actions. Comparisons can be **number** or **string** types, as long as both values are the same type.	
	name	The unique variable identifier assigned to the item in the **Declaration** section.
	equal notequal less lessequal greater, greaterequal and or	The operation value to compare. If true, any sub-actions are executed.
register	Adds metadata to the session.	
	name	The unique identifier of a meta variable to be created, as defined in the **declaration** section.
	value	The value of the metadata to be created.
while	Compares two values and executes any sub-actions if the comparison is true. Comparisons can be **number** or **string** types, as long as both values are the same type.	
	name	The unique variable identifier assigned to the item in the declaration section.

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
	equal notequal less lessequal greater, greaterequal and or	Specifies the operation value to compare. If true, any sub-action is executed. The **and** and **or** attributes signify bitwise operations and can only be applied to **number** variables.

Arithmetic Functions

NOTE: All numbers are 64-bit unsigned values and subject to both underflow and overflow, depending on the operation.

and	Performs bitwise AND between two numbers.	
	name	Variable to AND result into
	value	Number to AND into result
or	Performs bitwise OR between two numbers.	
	name	Variable to OR result into
	value	Number to OR into result
increment	Performs ADDITION of two numbers.	
	name	Variable containing the initial value AND to receive ADDITION results
	value	Number to ADD to initial value
decrement	Performs SUBTRACTION of two numbers.	
	name	Variable containing initial value AND to receive SUBTRACTION results
	value	Number to SUBTRACT from initial value
divide	Performs DIVISION of two numbers.	
	name	Variable containing the initial value AND to receive DIVISION results
	value	Number by which to divide the initial value. **NOTE:** Division by zero generates an error and stops any further processing of the current session by this parser.
modulo	Performs MODULO of two numbers.	
	name	Variable containing the initial value AND to receive MODULO results
	value	Number by which to divide initial value. **NOTE:** Division by zero generates an error and stops any further processing of the current session by this parser.

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
multiply	Performs MULTIPLICATION of two numbers.	
	name	Variable containing the initial value AND to receive MULTIPLICATION results
	value	Number by which to MULTIPLY the initial value.
shiftleft	Performs a binary shift left.	
	name	Variable containing the initial value AND to receive shift results
	value	Number of bits to shift by
shiftright	Performs a binary shift right.	
	name	Variable containing the initial value AND to receive shift results
	value	Number of bits to shift by
String Functions		
append	Attaches a number or string to the end of a **string** variable.	
	name	The unique identifier of a string variable to which the specified value is to be attached
	value	A number or string to attach
find	Searches a string for a provided string value. If it is found, the position is returned and any child elements will execute. Otherwise, child elements will not execute.	
	name	A **number** variable to receive the zero-based position, where the provided value string was found in the **in** string.
	value	A string to find
	in	A string to search
	length (optional)	A limit to the length of the **in** string to be searched. If a limit is not provided, all of **in** will be searched.
length	Assigns the length of a string to a **number** variable.	
	name	A **number** variable to receive the length of the specified string.
	value	A string value whose length is to be determined.
regex	Searches a string for matches to the provided regular expression. If a match is found, the position and, optionally, the matching string is returned. Any child elements will then execute. If not found, any child elements will not execute. **NOTE:** Regular expression operations can adversely affect system performance.	

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
	name	A number variable to receive the zero-based position, where the provided regular expression matched in the **in** string.
	value	A regular expression to be searched for.
	in	A string to search.
	length (optional)	A limit to the length of the **in** string to be searched. If a limit is not provided, all of **in** will be searched.
	found (optional)	The name of a string variable to receive the matched string.
substring	At least one of the optional attributes **from** and **length** must be specified.	
	name	The unique identifier of a string variable to receive the extracted value.
	value	A string value from which to extract a substring.
	from (optional)	The zero-based position from which to begin the substring. If not specified, it defaults to zero.
	length (optional)	The number of characters to extract. If not specified, it defaults to the remaining length of the string.
tolower	Converts a string to all lowercase letters.	
	name	The name of a **string** variable to process.
toupper	Converts a string to all uppercase letters.	
	name	The name of a **string** variable to process.
Payload Functions	These functions operate on a **read** position, set at the beginning of a **match** element, as described in the **declaration** section above.	
find	Searches the stream payload starting at the read position for a provided string value. If the value is found, the offset from the read position is returned. Any child elements will then execute. If not found, any child elements will not execute.	
	name	A **number** variable to receive the offset from the **read** position where the match begins.
	value	A string to find
	length (optional)	A limit to the length of the payload to be searched. If a limit is not provided, the remainder of the payload is searched. **NOTE:** It is recommended to always use the smallest value possible here in order to reduce the effect on performance.

NODE NAME	ATTRIBUTE NAME	DESCRIPTION
move	Moves the **read** position forward in the current stream by a specified number of bytes. If there is sufficient data in the stream, the **read** position is updated and any child elements will then execute. If not found, the **read** position remains unchanged and any child elements will not execute.	
	value	The number of bytes to move the **read** position.
read	Reads a specified number of bytes starting at the **read** position into a variable. If there is sufficient data in the stream, the **read** position is updated, the data read assigned, and any child elements will then execute. If not found, the **read** position remains unchanged and any child elements will not execute.	
	name	The name of a **string** or **number** variable to receive stream data. If a **number** variable is provided, the bytes read are interpreted as a single unsigned numeric value.
	length	The number of bytes to read from a stream.
	endianess (optional)	The byte ordering to use when reading into a number variable. Can be **big** (default) or **little**. **NOTE:** The attribute is invalid when reading into a **string** variable.
Regex–Searches the stream payload starting at the **read** position for matches to a provided regular expression. If found, the offset from the **read** position and, optionally the matched string, is returned. Any child elements execute. Otherwise, child elements do not execute. **NOTE:** Regular expression operations can adversely affect system performance.		
	name	A **number** variable to receive the offset from the **read** position where the match begins.
	value	A regular expression to find.
	length (optional)	A limit to the length of the payload to be searched. If a limit is not provided, the remainder of the payload is searched. **NOTE:** It is recommended to always use the smallest value possible here in order to reduce the effect on performance.
	found (optional)	The name of a **string** variable to receive a matched string.

Common Parser Operations

Examples of defining six common parser operations are included.

- Match Port and Identify Immediately (see page 105)
- Match Port and Delay Identification (see page 105)
- Match Token and Identify Immediately (see page 106)
- Match Multiple Tokens (see page 106)
- Match Token and Create Metadata (see page 107)

Match Port and Identify Immediately

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="parsers.xsd">

      <parser name="CustApp" desc="Acme Custom App" service="45324">

            <declaration>
                  <port name="port" value="45324" />
            </declaration>

            <match name="port">
                  <identify />
            </match>
      </parser>
</parsers>
```

Match Port and Delay Identification

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
    xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
    xsi:noNamespaceSchemaLocation="parsers.xsd">

      <parser name="MSRPC" desc="Microsoft RPC protocol" service="135">

            <declaration>
                  <port name="port" value="135" />
                  <number name="state" scope="session" />
                  <session name="end" value="end" />
            </declaration>

            <match name="port">
                  <assign name="state" value="1" />
            </match>

            <match name="end">
                  <if name="state" equal="1">
                        <identify />
                  </if>
            </match>

      </parser>
</parsers>
```

Match Token and Identify Immediately

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="parsers.xsd">

      <parser name="RDP" desc="Remote Desktop Protocol" service="3389">

            <declaration>
                  <token name="signature" value="Cookie: mstshash=" />
            </declaration>

            <match name="signature">
                  <identify />
            </match>
      </parser>
</parsers>
```

Match Multiple Tokens

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="parsers.xsd">

      <parser name="MyServiceMultiToken" desc="Multiple Tokens"
service="333">
            <declaration>
                  <number name="state" scope="stream" />
                  <token name="user" value="USER " />
                  <token name="pass" value="PASS " />
                  <session name="session" value="end" />
            </declaration>
            <match name="user">
                  <or name="state" value="1" />
            </match>
            <match name="pass">
                  <or name="state" value="2" />
            </match>

            <match name="session">
                  <if name="state" equal="3">
                      <identify />
                  </if>
            </match>

      </parser>
```

Match Token and Create Metadata

```
<?xml version="1.0" encoding="utf-8"?>
<parsers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="parsers.xsd">
      <parser name="SHELL" desc="Command Shell Identification">

            <declaration>
                  <token name="cmd.exe" value="(C) Copyright 1985-2001
Microsoft Corp" options="linestart" />
                  <meta name="client" key="client" format="Text" />
            </declaration>

            <match name="cmd.exe">
                  <register name="client" value="MS Command Shell" />
            </match>

      </parser>
</parsers>
```

Appendix C

Reference List Documents

This section contains several reference lists that you use to help define the appropriate rules for the NetWitness capture configuration:

- **Parsers and Associated Metadata** (see page 110)
- **Ethernet Protocol Reference List** (see page 121)

  These protocols are valid for Ethernet, Token Ring, and FDDI.
- **Internet Protocol Reference List** (see page 128)
- **TCP Port Reference List** (see page 133)
- **UDP Port Reference List** (see page 136)

Parsers and Associated Metadata

The following table presents a complete list of parsers and their associated metadata. You can indicate, for DECODER or INVESTIGATOR, which parsers to enable and specify the meta for the parsers to use.

PARSER	METADATA	DESCRIPTION
AIM AOL Instant Messenger	action attachment client username	Action Event Attachment Client Application User Account
ALERTS	alert	Alerts
BITTORRENT BitTorrent File Sharing Protocol	None	
DHCP Dynamic Host Configuration Protocol	alias.host alias.ip	Hostname Alias Record IP Address Alias Record
DNS Domain Name Service	alias.host alias.ip	Hostname Alias Record IP Address Alias Record
enVision LogDecoder Service	See separate table on on page 115.	
FIX Financial Information eXchange Protocol	None	
FTP File Transfer Protocol	action attachment data_chan directory extension filename password username	Action Event Attachment Data Channel Directory Extension Filename Password User Account
GeoIP Geographic data based on ip.src	city.dst city.src country.dst country.src latdec.dst latdec.src longdec.dst longdec.src	Destination City Source City Destination Country Source Country Destination Decimal Latitude Source Decimal Latitude Destination Decimal Longitude Source Decimal Longitude
GNUTELLA File Sharing Protocol	None	
GTalk Google Talk	action username	Action Event User Account
H323 H.323 Teleconferencing Protocol	action username	Action Event User Account

Parser	Metadata	Description
HTTP Hyper Text Transport Protocol	action alias.host alias.ip alias.ipv6 attachment content directory extension filename password query referer username	Action Event Hostname Alias Record IP Address Alias Record IPv6 Address Alias Record Attachment Content Type Directory Extension Filename Password Query Referer User Account
HTTPS Secure Socket Layer Protocol	client crypto	Client Application Crypto Key
IMAP Internet Message Access Protocol	None	
IRC Internet Relay Chat Protocol	action directory extension filename fullname group password username	Action Event Directory Extension Filename Full Name Group Channel Password User Account
LotusNotes Lotus Notes Mail Protocol	action alias.host alias.ip alias.ipv6 database username	Action Event Hostname Alias Record IP Address Alias Record IPv6 Address Alias Record Database Name User Account
MAIL Standard E-Mail Format (RFC822)	action attachment content email group orig_ip subject	Action Event Attachment Content Type E-mail Address Group Channel Originating IP Address Subject
MSN Mircosoft Instant Messenger	action attachment email	Action Event Attachment E-mail Address
MSRPC Microsoft Remote Procedure Call Protocol	None	
Net2Phone Net2Phone Protocol	action phone username	Action Event Phone Number User Account

PARSER	METADATA	DESCRIPTION
NETBIOS NETBIOS computer name and parser	alias.host alias.ip alias.ipv6	Hostname Alias Record IP Address Alias Record IPv6 Address Alias Record
NETWORK Network Layer parser	eth.dst eth.src eth.type ip.dst ip.proto ip.src ipv6.dst ipv6.proto ipv6.src service tcp.dstport tcp.srcport udp.dstport udp.srcport	Ethernet Destination Address Ethernet Source Address Ethernet Protocol Destination IP Address IP Protocol Source IP Address Destination IPv6 Address IPv6 Protocol Source IPv6 Address Service Type TCP Destination Port TCP Source Port UDP Target Port UDP Source Port
NFS Network File System	None	
NNTP Network News Transport Portocol	action group username	Action Event Group Channel User Account
PGP PGP blocks within network traffic parser	crypto	Crypto Key
POP3 Post Office Protocol	action password username	Action Event Password User Account
RDP Remote Desktop Protocol	action username	Action Event User Account
RIP Routing Information Protocol	None	
RTP Real Time Protocol for audio/video	None	
SAMETIME Lotus Notes Sametime Instant Messenger Protocol	action buddy username	Action Event Buddy Name User Account
SCCP Cisco Skinny Client Control Protocol	fullname phone	Full Name Phone Number
SEARCH Searches content for keywords and/or regular expressions	found match	Found Search Match Search
SHELL Command Shell Identification	client	Client Application

Parser	Metadata	Description
SIP Session Initiation Protocol	action content email fullname username	Action Event Content Type E-mail Address Full Name User Account
SMB Server Message Block	action alias.host alias.ip alias.ipv6 directory error extension filename username	Action Event Hostname Alias Record IP Address Alias Record IPv6 Address Alias Record Directory Error Extension Filename User Account
SMIME SMIME blocks within network traffic	crypto	Crypto Key
SMTP Simple Mail Transport Protocol	action email	Action Event E-mail Address
SNMP Simple Network Management Protocol	None	
SSH Secure Shell	crypto	Crypto Key
TDS MSSQL and Sybase Database Protocol	action database sql username	Action Event Database Name Sql Query User Account
TELNET TELNET Protocol	action username	Action Event User Account
TFTP Trivial File Transfer Protocol	action directory extension filename	Action Event Directory Extension Filename
TNS Oracle Database Protocol	action alias.host alias.ip alias.ipv6 sql username	Action Event Hostname Alias Record IP Address Alias Record IPv6 Address Alias Record Sql Query User Account
VCARD Extracts Full Name and E-mail information	fullname	Full Name
WEBMAIL Webmail via HTTP	action attachment email subject	Action Event Attachment E-mail Address Subject

PARSER	METADATA	DESCRIPTION
YCHAT Yahoo! Web Chat Protocol	action group username	Action Event Group Channel User Account
YMSG Yahoo Messenger	action attachment username	Action Event Attachment User Account

enVision Parser

PARSER	META DATA	DESCRIPTION
enVision LOGDECODER Service	OS access.point accesses action alias.host audit.class auth.method binary bytes bytes.src category cert.error cert.host.cat cert.host.name cert.status cert.subject change.attrib change.new change.old checksum child.pid cipher.dst cipher.size.dst cipher.size.src cipher.src client comments comp.version connection.id content.type content.version context context.subject context.target cpu crypto cve data database db.pid dclass.c1 dclass.c1.str dclass.c2 dclass.c2.str dclass.c3 dclass.c3.str ddomain dead device.class device.ip device.ipv6 dinterface	Operating System Access Point Accesses Action Event Hostname Aliases Audit Class Authentication Method Binary Data Bytes Sent Bytes Category Certificate Error Certificate Hostname Category Certificate Host Name Certificate Status Certificate Subject Change Attribute Change New Value Change Old Value Checksum Child Process ID Destination Cipher Destination Cipher Size Source Cipher Size Source Cipher Client Application Comments Component Version Connection ID Content Content Version Context Subject Context Target Context CPU Crypto CVE Reference Data Database Name Database Process ID Counter1 Counter1 String Counter2 Counter2 String Counter3 Counter3 String Destination Domain Dead Device Class Device IP Device IPv6 Destination Interface

PARSER	META DATA	DESCRIPTION
enVision LOGDECODER Service	direction	Direction
	directory	Directory
	disk.volume	Disk Volume
	disposition	Disposition
	dmask	Destination Mask
	dn	No Index
	dn.dst	Destination Distinguished Name
	dn.src	Source Distinguished Name
	doc.number	Document Number
	domain	Domain Name
	domain.id	Domain ID
	dtransaddr	Translated Destination Address
	dtransport	Translated Destination Port
	duration.str	Duration String
	duration.time	Duration
	ec.activity	Event Activity
	ec.outcome	Event Outcome
	ec.subject	Event Subject
	ec.theme	Event Theme
	effective.time	Effective Time
	email	E-mail Address
	endtime	End Time
	entry	Entry
	eth.dst	Ethernet Destination
	eth.host	Device Mac Address
	eth.src	Ethernet Source
	event.cat	Event Category
	event.cat.name	Event Category Name
	event.counter	Event Counter
	event.desc	Event Description
	event.log	Event Log
	event.queue.time	Event Queue Time
	event.source	Event Source
	event.state	Event State
	event.time.str	Event Time String
	event.type	Event Type
	event.vcat	Vendor Event Category
	expected.val	Expected Value
	expire.time	Expiration Time
	extension	Extension
	fcatnum	Filter Category Number
	federated.idp	Federated Identity Provider
	federated.sp	Federated Service Provider
	filename	Filename
	filename.size	Filename Size
	filter	Filter
	firstname	User First Name
	forward.ip	Forwarder IP
	forward.ipv6	Forwarder IPv6
	fqdn	FQDN
	fresult	Filter Result
	fullname	Full Name
	gateway	Gateway

Parser	Meta Data	Description
enVision LogDecoder Service	group	Group
	group.id	Group ID
	group.object	Group Object
	hardware.id	Hardware ID
	hcode	Hierarchy
	header.id	Header ID
	icmp.code	ICMP Code
	icmp.type	ICMP Type
	ike	IKE
	ike.cookie1	IKE Cookie P1
	ike.cookie2	IKE Cookie P2
	index	Index ID
	inode	Inode
	instance	Instance Name
	interface	Interface
	ip.addr	IP Address
	ip.dst	Destination IP address
	ip.dstport	Destination Port
	ip.host	IP Host
	ip.host.dst	IP Host Destination
	ip.host.src	IP Host Source
	ip.src	Source IP Address
	ip.srcport	Source Port
	ipv6.addr	IP Address v6
	ipv6.dst	Destination IPv6 address
	ipv6.src	Source IPv6 Address
	job.num	Job Number
	lastname	User Last Name
	level	Message Level
	library	Library
	listnum	Access List No
	loc.city	City
	loc.country	Country
	loc.desc	Location Description
	loc.state	State/Province
	log.session.id	Session
	log.session.id1	Linked Session ID
	logon.type	Logon Type
	lread	LRead
	lun	LUN
	lwrite	LWrite
	mail.id	MailBox
	mask	IP Mask
	medium	Medium
	message.body	Message Body
	middlename	User Middle Name
	msg	Message
	msg.id	Message ID
	msg.table	Message Table
	msg.vid	Vendor ID
	network.port	Network Port
	network.service	Network Service Name
	node	Node Name
	obj.name	Object Name
	obj.server	Object Server

PARSER	META DATA	DESCRIPTION
enVision LOGDECODER Service	obj.type	Object Type
	obj.val	Object Value
	observed.val	Observed Value
	operation.id	Operation ID
	org	Organization
	packets	Packets
	paddr	Device Address
	paddr.host	Device Host
	param	Parameters
	parent.node	Parent Node Name
	parent.pid	Parent Process ID
	parse.error	Parse Error
	patient.fname	Patient First Name
	patient.id	Patient ID
	patient.lname	Patient Last Name
	patient.mname	Patient Middle Name
	payload.dst	Destination Payload
	payload.src	Source Payload
	peer	Peer Gateway
	peer.id	Peer Identity
	permissions	Permissions
	phone	Phone Number
	policy.id	Policy ID
	policy.name	Policy Name
	policy.value	Policy Value
	pool.id	Pool ID
	pool.name	Pool Name
	port.name	Port Name
	pread	PRead
	privilege	Privilege
	process	Process
	process.id	Process ID
	process.id.val	Process ID Value
	process.time	Processing Time
	product	Product
	profile	User Profile
	protocol	Protocol
	protocol.detail	Protocol Detail
	pwwn	Port World Wide Name
	query	Querystring
	rbytes	Received Bytes
	realm	Realm
	recorded.time	Recorded Time
	reference.id	Reference ID
	reference.id1	Linked Reference ID
	reference.id2	Linked Reference ID2
	referer	Referer
	reputation.num	Reputation Number
	resource	Resource
	resource.class	Resource Class
	result	Result
	result.code	Result Code
	risk	Risk
	risk.num	Risk Number
	rule	Rule

Parser	Meta Data	Description
enVision LogDecoder Service	rule.group	Rule Group
	rule.name	Rule Name
	rule.template	Rule Template
	rule.uid	Rule UID
	scheme	Scheme
	sensor	Sensor
	serial.number	Serial Number
	server	Server Application
	service.name	Service
	severity	Severity
	sig.id	Signature ID
	sig.id.str	Signature ID String
	sig.id1	Signature ID1
	sig.name	Signature Name
	sig.type	Signature Type
	sinterface	Source Interface
	site	Site
	smask	Source Mask
	spi.dst	Destination SPI
	spi.src	Source SPI
	ssl.ver.dst	Destination SSLVersion
	ssl.ver.src	Source SSL Version
	starttime	Start Time
	statement	Statement
	stransaddr	Translated Source Address
	stransport	Translated Source Port
	subject	Subject
	table.name	Table Name
	terminal	Terminal
	threat.category	Threat Category
	threat.desc	Threat Description
	time	Time
	timezone	Time Zone
	tos	Type Of Service
	trans.from	Translated Sender Address
	trans.to	Translated Recipient Address
	transact.id	Transaction ID
	trigger.desc	Trigger Desc
	trigger.val	Trigger Value
	url	URL
	user.agent	User Agent
	user.dept	User Department
	user.dst	Destination User Account
	user.role	User Role
	user.src	Source User Account
	username	User Account
	version	Versions
	virusname	VirusName
	vlan.name	VLAN
	vm.target	VM Target
	vsys	Virtual Name
	vuln.ref	Vulnerability References
	web.cookie	Web Cookie
	web.domain	Web Domain
	web.page	Web Page
	web.ref.domain	Web Referer Domain

PARSER	META DATA	DESCRIPTION
enVision LOGDECODER Service	web.ref.page web.ref.query web.ref.root web.root wlan.channel wlan.name wlan.ssid workspace zone zone.dst zone.src	Web Referer Page Web Referer Query Web Referer Root Web Root WLAN frequency channel WLAN WLAN service set identifier Workspace Zone Destination Zone Source Zone

Ethernet Protocol Reference List

Use this network protocol reference list to help define the appropriate network rules for capture configuration. These protocols will be valid for Ethernet, Token Ring, and FDDI.

In typical operational scenarios, all ports are processed; however, performance can be enhanced by filtering specific protocols and turning content retention off.

To access **Capture Rules** in NetWitness INVESTIGATOR, click **Edit** → **Rules**. The **Rules Configuration** dialog displays. Click the tab for **Net Rules**.

NUMBER	NAME	DESCRIPTION
0x0000	802.3	IEEE 802.3 Length Field (0.:1500.)
0x0101		Experimental
0x0200	Xerox PUP	Xerox PUP (conflicts with 802.3 Length Field range)
0x0201	Xerox PUP	Xerox PUP Address Translation (conflicts with 802.3 Length Field range)
0x0400	Nixdorf	Nixdorf (conflicts with 802.3 Length Field range)
0x0600	Xerox NS IDP	
0x0601	XNS Address Translation	(3MB only)
0x0800	IP	Internet Protocol v4
0x0801	X.75 Internet	
0x0802	NBS Internet	
0x0803	ECMA Internet	
0x0804	CHAOSnet	
0x0805	X.25 Level 3	
0x0806	ARP	Address Resolution Protocol (for IP and for CHAOS)
0x0807	XNS Compatibility	
0x081C	Symbolics Private	
0x0888	Xyplex	
0x0900	Ungermann-Bass Network Debugger	
0x0A00	Xerox IEEE802.3 PUP	
0x0A01	Xerox IEEE802.3 PUP Address Translation	

NUMBER	NAME	DESCRIPTION
0x0BAD	Banyan Systems	
0x0BAF	Banyan VINES Echo	
0x1000	Berkeley Trailer Negotiation	
0x1001	Berkeley Trailer Encapsulation for IP	
0x1234	DCA – Multicast	
0x1600	VALID System Protocol	
0x1989	Artificial Horizons	Aviator dogfight simulator on Sun
0x1995	Datapoint Corporation	RCL LAN Protocol
0x3C00	3Com NBP virtual circuit datagram (like XNS SPP) not registered	
0x3C01	3Com NBP System Control Datagram not registered	
0x3C02	3Com NBP Connect Request (virtual cct) not registered	
0x3C03	3Com NBP Connect Response not registered	
0x3C04	3Com NBP Connect Complete not registered	
0x3C05	3Com NBP Close Request (virtual cct) not registered	
0x3C06	3Com NBP Close Response not registered	
0x3C07	3Com NBP Datagram (like XNS IDP) not registered	
0x3C08	3Com NBP Datagram Broadcast not registered	
0x3C09	3Com NBP Claim NETBIOS Name not registered	
0x3C0A	3Com NBP Delete NETBIOS Name not registered	
0x3C0B	3Com NBP Remote Adaptor Status Request not registered	
0x3C0C	3Com NBP Remote Adaptor Response not registered	
0x3C0D	3Com NBP Reset not registered	
0x4242	PCS Basic Block Protocol	
0x424C	Information Modes Little Big LAN Diagnostic	
0x4321	THD - Diddle	

NUMBER	NAME	DESCRIPTION
0x4C42	Information Modes Little Big LAN	
0x5208	BBN Simnet Private	
0x6000	DEC unassigned	experimental
0x6001	DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance	
0x6002	DEC Maintenance Operation Protocol (MOP) Remote Console	
0x6003	DECNET Phase IV	DNA routing
0x6004	DEC Local Area Transport (LAT)	
0x6005	DEC Diagnostic Protocol (at interface initialization?)	
0x6006	DEC Customer Protocol	
0x6007	DEC Local Area VAX Cluster (LAVC)	System Communication Architecture (SCA)
0x6008	DEC AMBER	
0x6009	DEC MUMPS	
0x6010	3Com Corporation	
0x7000	Ungermann-Bass Download	
0x7001	Ungermann-Bass NIUs	
0x7002	Ungermann-Bass Diagnostic/loopback	
0x7003	Ungermann-Bass (NMC to/from UB Bridge)	
0x7005	Ungermann-Bass Bridge Spanning Tree	
0x7007	OS/9 Microware	
0x7009	OS/9 Net	
0x7020	LRT (England) (now Sintrom)	
0x7030	Racal-Interlan	
0x7031	Prime NTS (Network Terminal Service)	
0x7034	Cabletron	
0x8003	Cronus VLN	
0x8004	Cronus Direct	
0x8005	HP Probe Protocol	
0x8006	Nestar	

NUMBER	NAME	DESCRIPTION
0x8008	AT&T/Stanford University	
0x8010	Excelan	
0x8013	Silicon Graphics Diagnostic	
0x8014	Silicon Graphics Network Games	
0x8015	Silicon Graphics reserved	
0x8016	Silicon Graphics XNS NameServer	Bounce server
0x8019	Apollo DOMAIN	
0x802E	Tymshare	
0x802F	Tigan, Inc.	
0x8035	Reverse Address Resolution Protocol (RARP)	
0x8036	Aeonic Systems	
0x8037	IPX (Novell Netware)	
0x8038	DEC LanBridge Management	
0x8039	DEC DSM/DDP	
0x803A	DEC Argonaut Console	
0x803B	DEC VAXELN	
0x803C	DEC DNS Naming Service	
0x803D	DEC Ethernet CSMA/CD Encryption Protocol	
0x803E	DEC Distributed Time Service	
0x803F	DEC LAN Traffic Monitor Protocol	
0x8040	DEC PATHWORKS DECnet NETBIOS Emulation	
0x8041	DEC Local Area System Transport	
0x8042	DEC unassigned	
0x8044	Planning Research Corporation	
0x8046	AT&T	
0x8047	AT&T	
0x8048	DEC Availability Manager for Distributed Systems DECamds	
0x8049	ExperData	

NUMBER	NAME	DESCRIPTION
0x805B	VMTP	VMTP (Versatile Message Transaction Protocol)
0x805C	Stanford V Kernel, version 6.0	
0x805D	Evans & Sutherland	
0x8060	Little Machines	
0x8062	Counterpoint Computers	
0x8065	University of Massachusetts at Amherst	
0x8066	University of Massachusetts at Amherst	
0x8067	Veeco Integrated Automation	
0x8068	General Dynamics	
0x8069	AT&T	
0x806A	Autophon	
0x806C	ComDesign	
0x806D	Compugraphic Corporation	
0x806E	Landmark Graphics Corporation	
0x807A	Matra	
0x807B	Dansk Data Elektronik	
0x807C	Merit Internodal	
0x807D	Vitalink Communications	
0x8080	Vitalink TransLAN III Management	
0x8081	Counterpoint Computers	
0x8088	Xyplex	
0x809B	EtherTalk - AppleTalk over Ethernet	
0x809C	Datability	
0x809F	Spider Systems Ltd.	
0x80A3	Nixdorf Computers	
0x80A4	Siemens Gammasonics Inc.	
0x80C0	DCA Data Exchange Cluster	
0x80C6	Pacer Software	
0x80C7	Applitek Corporation	

NUMBER	NAME	DESCRIPTION
0x80C8	Intergraph Corporation	
0x80CD	Harris Corporation	
0x80CF	Taylor Instrument	
0x80D3	Rosemount Corporation	
0x80D5	IBM SNA Services over Ethernet	
0x80DD	Varian Associates	
0x80DE	TRFS (Integrated Solutions Transparent Remote File System)	
0x80E0	Allen-Bradley	
0x80E4	Datability	
0x80F2	Retix	
0x80F3	AppleTalk Address Resolution Protocol (AARP)	
0x80F4	Kinetics	
0x80F7	Apollo Computer	
0x80FF	Wellfleet Communications	
0x8102	Wellfleet BOFL	WellFleet BOFL (Breath OF Life) pkts (every 5-10 secs.)
0x8103	Wellfleet Communications	
0x8107	Symbolics Private	
0x812B	Talaris	
0x8130	Waterloo Microsystems Inc.	
0x8131	VG Laboratory Systems	
0x8137	IPX	Novell NetWare IPX (ECONFIG E option)
0x8138	Novell Inc.	
0x8139	KTI	
0x813F	M/MUMPS Data Sharing	
0x8145	Vrije Universiteit (NL)	
0x8146	Vrije Universiteit (NL)	
0x8147	Vrije Universiteit (NL)	
0x814C	SNMP	SNMP over Ethernet

NUMBER	NAME	DESCRIPTION
0x814F	Technically Elite Concepts	
0x817D	XTP	
0x8191	PowerLAN	
0x81D6	Artisoft Lantastic	
0x81D7	Artisoft Lantastic	
0x8203	QNX Software Systems Ltd.	
0x8390	Accton Technologies (unregistered)	
0x852B	Talaris multicast	
0x8582	Kalpana	
0x86DD	IP version 6	
0x8739	Control Technology Inc.	
0x873A	Control Technology Inc.	
0x873B	Control Technology Inc.	
0x873C	Control Technology Inc.	
0x8820	Hitachi Cable (Optoelectronic Systems Laboratory)	
0x8856	Axis Communications AB	
0x8888	HP LanProbe test	
0x9000	Loopback (Configuration Test Protocol)	
0x9001	3Com XNS Systems Management	
0x9002	3Com TCP/IP Systems Management	
0x9003	3Com Loopback Detection	
0xAAAA	DECNET	
0xFAF5	Sonix Arpeggio	
0xFF00	BBN VITAL-LanBridge Cache Wakeups	
0x8863	PPPoe	PPPoe - PPP Discovery Over Ethernet
0x8864	PPPoe	PPPoe - PPP Session Over Ethernet

Internet Protocol Reference List

In typical operational scenarios, all ports are processed; however, performance can be enhanced by filtering specific protocols and turning content retention off.

To access **Capture Rules** in NetWitness INVESTIGATOR, click **Edit** → **Rules**. The **Rules Configuration** dialog displays. Click the tab for **Net Rules**.

NUMBER	NAME	DESCRIPTION
0	HOPOPT	IPv6 Hop-by-Hop Option [RFC1883]
1	ICMP	Internet Control Message [RFC792]
2	IGMP	Internet Group Management [RFC1112]
3	GGP	Gateway-to-Gateway [RFC823]
4	IP	IP in IP (encapsulation) [RFC2003]
5	ST	Stream [RFC1190,RFC1819]
6	TCP	Transmission Control Protocol [RFC793]
7	CBT	CBT [Ballardie]
8	EGP	Exterior Gateway Protocol [RFC888,DLM1]
9	IGP	Any private interior gateway [IANA] (used by Cisco for their IGRP)
10	BBN-RCC-M	BBN RCC Monitoring [SGC]
11	NVP-II	Network Voice Protocol [RFC741,SC3]
12	PUP	PUP [PUP,XEROX]
13	ARGUS	ARGUS [RWS4]
14	EMCON	EMCON [BN7]
15	XNET	Cross Net Debugger [IEN158,JFH2]
16	CHAOS	Chaos[NC3]
17	UDP	User Datagram [RFC768,JBP]
18	MUX	Multiplexing [IEN90,JBP]
19	DCN-MEAS	DCN Measurement Subsystems [DLM1]
20	HMP	Host Monitoring [RFC869,RH6]
21	PRM	Packet Radio Measurement [ZSU]
22	XNS-IDP	XEROX NS IDP [ETHERNET,XEROX]

NUMBER	NAME	DESCRIPTION
23	TRUNK-1	Trunk-1 [BWB6]
24	TRUNK-2	Trunk-2 [BWB6]
25	LEAF-1	Leaf-1 [BWB6]
26	LEAF-2	Leaf-2 [BWB6]
27	RDP	Reliable Data Protocol [RFC908,RH6]
28	IRTP	Internet Reliable Transaction [RFC938,TXM]
29	ISO-TP4	ISO Transport Protocol Class 4 [RFC905,RC77]
30	NETBLT	Bulk Data Transfer Protocol [RFC969,DDC1]
31	MFE-NSP	MFE Network Services Protocol [MFENET,BCH2]
32	MERIT-INP	MERIT Internodal Protocol [HWB]
33	SEP	Sequential Exchange Protocol [JC120]
34	3PC	Third Party Connect Protocol [SAF3]
35	IDPR	Inter-Domain Policy Routing Protocol [MXS1]
36	XTP	XTP [GXC]
37	DDP	Datagram Delivery Protocol [WXC]
38	IDPR-CMTP	IDPR Control Message Transport Proto [MXS1]
39	TP++	TP++ Transport Protocol [DXF]
40	IL	IL Transport Protocol [Presotto]
41	IPv6	Ipv6 [Deering]
42	SDRP	Source Demand Routing Protocol [DXE1]
43	IPv6-Rout	Routing Header for IPv6 [Deering]
44	IPv6-Frag	Fragment Header for IPv6 [Deering]
45	IDRP	Inter-Domain Routing Protocol [Sue Hares]
46	RSVP	Reservation Protocol [Bob Braden]
47	GRE	General Routing Encapsulation [Tony Li]
48	MHRP	Mobile Host Routing Protocol[David Johnson]
49	BNA	BNA [Gary Salamon]
50	ESP	Encap Security Payload for IPv6 [RFC1827]
51	AH	Authentication Header for IPv6 [RFC1826]

NUMBER	NAME	DESCRIPTION
52	I-NLSP	Integrated Net Layer Security TUBA [GLENN]
53	SWIPE	IP with Encryption [JI6]
54	NARP	NBMA Address Resolution Protocol [RFC1735]
55	MOBILE	IP Mobility [Perkins]
56	TLSP	Transport Layer Security Protocol [Oberg] using Kryptonet key management]
57	SKIP	SKIP [Markson]
58	IPv6-ICMP	ICMP for IPv6 [RFC1883]
59	IPv6-NoNx	No Next Header for IPv6 [RFC1883]
60	IPv6-Opts	Destination Options for IPv6 [RFC1883]
61	AnyHost	Any host internal protocol [IANA]
62	CFTP	CFTP [CFTP,HCF2]
63	AnyNetwork	Any local network [IANA]
64	SAT-EXPAK	SATNET and Backroom EXPAK [SHB]
65	KRYPTOLAN	Kryptolan [PXL1]
66	RVD	MIT Remote Virtual Disk Protocol [MBG]
67	IPPC	Internet Pluribus Packet Core [SHB]
68	AnyFile	Any distributed file system [IANA]
69	SAT-MON	SATNET Monitoring [SHB]
70	VISA	VISA Protocol [GXT1]
71	IPCV	Internet Packet Core Utility [SHB]
72	CPNX	Computer Protocol Network Executive [DXM2]
73	CPHB	Computer Protocol Heart Beat [DXM2]
74	WSN	Wang Span Network [VXD]
75	PVP	Packet Video Protocol [SC3]
76	BR-SAT-MO	Backroom SATNET Monitoring [SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary [WM3]
78	WB-MON	WIDEBAND Monitoring [SHB]
79	WB-EXPAK	WIDEBAND EXPAK [SHB]
80	ISO-IP	ISO Internet Protocol [MTR]

NUMBER	NAME	DESCRIPTION
81	VMTP	VMTP [DRC3]
82	SECURE-VM	SECURE-VMTP [DRC3]
83	VINES	VINES [BXH]
84	TTP	TTP [JXS]
85	NSFNET-IG	NSFNET-IGP [HWB]
86	DGP	Dissimilar Gateway Protocol [DGP,ML109]
87	TCF	TCF [GAL5]
88	EIGRP	EIGRP [CISCO,GXS]
89	OSPFIGP	OSPFIGP [RFC1583,JTM4]
90	Sprite-RP	Sprite RPC Protocol [SPRITE,BXW]
91	LARP	Locus Address Resolution Protocol [BXH]
92	MTP	Multicast Transport Protocol [SXA]
93	AX.25	AX.25 Frames [BK29]
94	IPIP	IP-within-IP Encapsulation Protocol [JI6]
95	MICP	Mobile Internetworking Control Protocol [JI6]
96	SCC-SP	Semaphore Communications Security Protocol [HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation [RDH1]
98	ENCAP	Encapsulation Header [RFC1241,RXB3]
99	AnyPrivate	Any private encryption scheme [IANA]
100	GMTP	GMTP [RXB5]
101	IFMP	Ipsilon Flow Management Protocol [Hinden]
102	PNNI	PNNI over IP [Callon]
103	PIM	Protocol Independent Multicast [Farinacci]
104	ARIS	ARIS [Feldman]
105	SCPS	SCPS [Durst]
106	QNX	QNX [Hunter]
107	A/N	Active Networks [Braden]
108	IPComp	IP Payload Compression Protocol [RFC2393]
109	SNP	Sitara Networks Protocol [Sridhar]

NUMBER	NAME	DESCRIPTION
110	Compaq-Pe	Compaq Peer Protocol [Volpe]
111	IPX-in-IP	IPX in IP [Lee]
112	VRRP	Virtual Router Redundancy Protocol [Hinden]
113	PGM	PGM Reliable Transport Protocol [Speakman]
114	AnyHop	Any 0-hop protocol [IANA]
115	L2TP	Layer Two Tunneling Protocol [Aboba]
116	DDX	D-II Data Exchange (DDX) [Worley]
117	IATP	Interactive Agent Transfer Protocol [Murphy]
118	STP	Schedule Transfer Protocol [JMP]
119	SRP	SpectraLink Radio Protocol [Hamilton]
120	UTI	UTI [Lothberg]
121	SMP	Simple Message Protocol [Ekblad]
122	SM	SM [Crowcroft]
123	PTP	Performance Transparency Protocol [Welzl]
124	ISIS	ISI over v4 [Przygienda]
125	FIRE	[Partridge]
126	CRTP	Combat Radio Transport Protocol [Sautter]
127	CRUDP	Combat Radio User Datagram [Sautter]
128	SSCOPMCE	[Waber]
129	IPLT	[Hollbach]
130	SPS	Secure Packet Shield [McIntosh]
131	PIPE	Prte IP Encapsulation within IP [Petri]
132	SCTP	Stream Control Transmission Protocol [Stewart]
133	FC	Fi Channel [Rajagopal]
134	RSVP-E2E-ORE	[RFC3175]
255	Reserved	[IANA]

TCP Protocol Reference List

Use this Transmission Control Protocol (TCP) port reference list to help define the appropriate network rules for capture configuration.

In typical operational scenarios, all ports are processed; however, performance can be enhanced by filtering specific protocols and turning content retention off.

To access **Capture Rules** in NetWitness INVESTIGATOR, click **Edit** → **Rules**. The **Rules Configuration** dialog displays. Click the tab for **Net Rules**.

TCP PORT	NAME	DESCRIPTION
7	echo	Echo
9	discard	Discard
13	daytime	Daytime
17	qotd	Quote of the day
19	chargen	Character generator
20	ftp-data	File Transfer
21	ftp	FTP Control
23	telnet	Telnet
25	smtp	Simple Mail Transfer
37	time	Time
42	nameserver	Host Name Server
43	nicname	Who Is
53	domain	Domain Name Server
70	gopher	Gopher
79	finger	Finger
80	http	World Wide Web
88	kerberos	Kerberos
101	hostname	NIC Host Name Server
102	iso-tsap	ISO-TSAP Class 0
107	rtelnet	Remote Telnet Service
109	pop2	Post Office Protocol – Version 2
110	pop3	Post Office Protocol – Version 3

TCP PORT	NAME	DESCRIPTION
111	sunrpc	SUN Remote Procedure Call
113	auth	Authentication Service
117	uucp-path	UUCP Path Service
119	nntp	Network News Transfer Protocol
135	epmap	DCE endpoint resolution
137	netbios-ns	NETBIOS Name Service
139	netbios-ssn	NETBIOS Session Service
143	imap	Internet Message Access Protocol
158	pcmail-srv	PC Mail Server
170	print-srv	Network PostScript
179	bgp	Border Gateway Protocol
194	irc	Internet Relay Chat Protocol
389	ldap	Lightweight Directory Access Protocol
443	https	Secure HTTP
445	cifs	Microsoft CIFS
464	kpasswd	Kerberos (v5)
512	exec	Remote Process Execution
513	login	Remote Login
514	cmd	Automatic Authentication
515	printer	Listens for incoming connections
520	efs	Extended File Name Server
526	tempo	Newdate
530	courier	RPC
531	conference	IRC Chat
532	netnews	Readnews
540	uucp	Uucpd
543	klogin	Kerberos login
544	kshell	Kerberos remote shell
556	remotefs	Rfs Server

TCP PORT	NAME	DESCRIPTION
636	ldaps	LDAP over TLS/SSL
749	Kerberos-adm	Kerberos administration
1109	kpop	Kerberos POP
1433	ms-sql-s	Microsoft-SQL-Server
1434	ms-sql-m	Microsoft-SQL-Monitor
1512	wins	Microsoft Windows Internet Name Service
1524	ingreslock	Ingres
1723	pptp	Point-to-point tunneling protocol
2053	knetd	Kerberos de-multiplexer
9535	man	Remote Man Server

UDP Protocol Reference List

Use this User Datagram Protocol (UDP) port reference list to help define the appropriate network rules for capture configuration.

In typical operational scenarios, all ports are processed; however, performance can be enhanced by filtering specific protocols and turning content retention off.

To access **Capture Rules** in NetWitness INVESTIGATOR, click **Edit** → **Rules**. The **Rules Configuration** dialog displays. Click the tab for **Net Rules**.

UDP PORT	NAME	DESCRIPTION
7	echo	Echo
9	discard	Discard
13	daytime	Daytime
17	qotd	Quote of the day
19	chargen	Character generator
37	time	Time
39	rlp	Resource Location Protocol
42	nameserver	Host Name Server
53	domain	Domain Name Server
67	bootps	Bootstrap Protocol Server
68	bootpc	Bootstrap Protocol Client
69	tftp	Trivial File Transfer
88	kerberos	Kerberos
111	sunrpc	SUN Remote Procedure Call
123	ntp	Network Time Protocol
135	epmap	DCE endpoint resolution
137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS Datagram Service
161	snmp	SNMP
162	snmptrap	SNMP TRAP
213	ipx	IPX over IP
443	https	Secure HTTP

UDP Port	Name	Description
445	cifs	Microsoft CIFS
464	kpasswd	Kerberos (v5)
500	isakmp	Internet Key Exchange (IPSec)
512	biff	Notifies users of new mail
513	who	Database of who is logged on (average load)
514	syslog	0
517	talk	Establishes TCP connection
518	ntalk	0
520	router	RIPv.1, RIPv.2
525	timed	Timeserver
530	courier	RPC
533	netwall	For emergency broadcasts
550	new-rwho	New-who
560	rmonitor	Rmonitor
561	monitor	0
749	kerberos-adm	Kerberos administration
1167	phone	Conference-calling
1433	ms-sql-s	Microsoft-SQL-Server
1434	ms-sql-m	Microsoft-SQL-Monitor
1512	wins	Microsoft Windows Internet Name Service
1701	l2tp	Layer Two Tunneling Protocol
1812	radiusauth	RRAS (RADIUS Authentication Protocol)
1813	radacct	RRAS (RADIUS Accounting Protocol)
2049	nfsd	Sun NFS Server
2504	nlbs	Network Load Balancing

Appendix D

SDK Data Types

Supported Fields

The following is a list of currently supported field names.

CATEGORY	ELEMENT NAME	DATA TYPE	DESCRIPTION
Network			
	session ID	UInt64	Session ID
	time	TimeT	Start Time
	size	UInt32	Size
	eth.src	MAC	Ethernet Source Address
	eth.dst	MAC	Ethernet Target Address
	eth.type	UInt16	Ethernet Protocol
	ip.proto	UInt8	IP Protocol
	ip.src	IPv4	Source IP Address
	ip.dst	IPv4	Destination IP Address
	ipv6.src	IPv6	Source IPv6 Address
	ipv6.dst	IPv6	Target IPv6 Address
	ipv6.proto	IPv6	IPv6 Protocol
	tcp.srcport	UInt16	TCP Source Port
	tcp.dstport	UInt16	TCP Destination Port
	udp.srcport	UInt16	UDP Source Port
	udp.dstport	UInt16	UDP Target Port

CATEGORY	ELEMENT NAME	DATA TYPE	DESCRIPTION
Application			
	service	UInt16	Service Type
	action	Text	Action Event (login, logoff, sendfrom, sendto, get, put, delete, attach, print)
Entities			
	username	Text	User Account
	email	Text	E-mail Address
	filename	Text	Filename resource
	handle	Text	Resource Handle
	database	Text	Database name
	group	Text	Group Channel
Alias Records			
	alias.ip	IPv4	IP Address Alias Record
	alias.host	Text	Hostname Record
Properties			
	content	Text	Content Type
	fullname	Text	Fullname
	nickname	Text	Nickname
	buddy	Text	Buddy Name
	client	Text	Client Application
	server	Text	Server Application
	password	Text	Password
	cookie	Text	Cookie
	response	Text	Response
	referer	Text	Referer
	created	Text	Created
	modified	Text	Modified
	generator	Text	Generated
	message	Text	Message
	subject	Text	Subject

CATEGORY	ELEMENT NAME	DATA TYPE	DESCRIPTION
Properties (continued)			
	attachment	Text	Subject
	crypto	Text	Crypto Key
	org	Text	Organization
	orig_ip	Text	Originating IP Address
	link	Text	Link
	renewal	Text	Renewal
	dns	Text	Dns
	address	Text	Address
	subnet	Text	Subnet
	sql	Text	Sql Query
	sqlresponse	Text	Sql Response
	create	Text	Create
	invite	Text	Invite
	crc	Text	32bit CRC Hash
	md5	Text	MD5 Hash
	phone	Text	Phone Number
	device	Text	Device Name
	signature	Text	Signature
	alertid	Text	Alert ID
	sourcefile	Text	Source File
	found	Text	Found
	match	Text	Match
	encapsulated	Text	Encapsulated
	data_chan	Text	Data Channel
	proxy	Text	Proxy Name

Appendix E

Wireless Packet Capture

Introduction

In version 9.0, support for 802.11 wireless LAN (WLAN) capture and parsing has been introduced. In addition, support for Wired Equivalent Privacy (WEP) decryption is available.

This section provides details about these components and how they relate to wireless packet capture.

Capture Devices

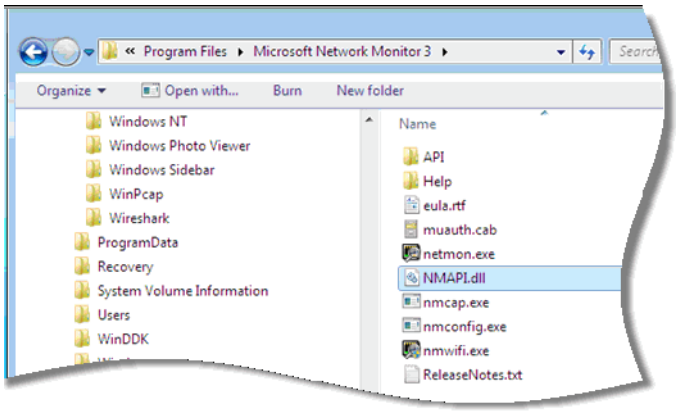
There are three radio capture devices in 9.0. These capture devices are designed to provide a source of captured packets for their respective operating system and hardware.

- Microsoft Netmon capture device ("packet_netmon_") (see page 143)
- Linux mac80211 capture device ("packet_mac80211_") (see page 145)

Netmon Capture Device

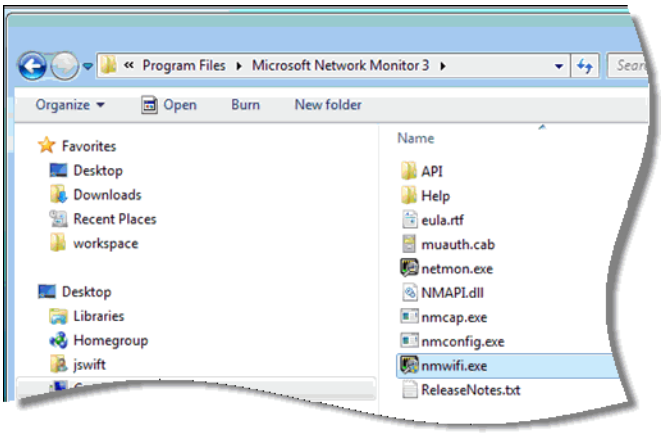
The Microsoft Network Monitor (Netmon) is a network analysis tool quite similar to Wireshark. Netmon can be downloaded directly from Microsoft's web site as a standalone application. Microsoft has published the underlying packet capture API that the Netmon application is based on. This means users are free to write their own custom network analysis tools in either C++ or .NET and link against the Netmon library. It is this library, namely NMAPI.dll, that the Netwitness Netmon capture device uses.

Since Microsoft does not yet permit redistribution of the Netmon DLL, users are required to download the Netmon application directly from Microsoft, install it, then copy the NMAPI.dll from the install directory into the directory where the Netwitness with INVESTIGATOR executable resides. This is all that is required to use the Netmon capture device.



1. Copy the NMAPI.dll to the 9.0 Install directory, specifically co-located with the application executable.

2. Use the **nmwifi.exe** application that comes with the Microsoft Network Monitor to place the USB wireless device into monitor mode as well as set the desired frequency channel.

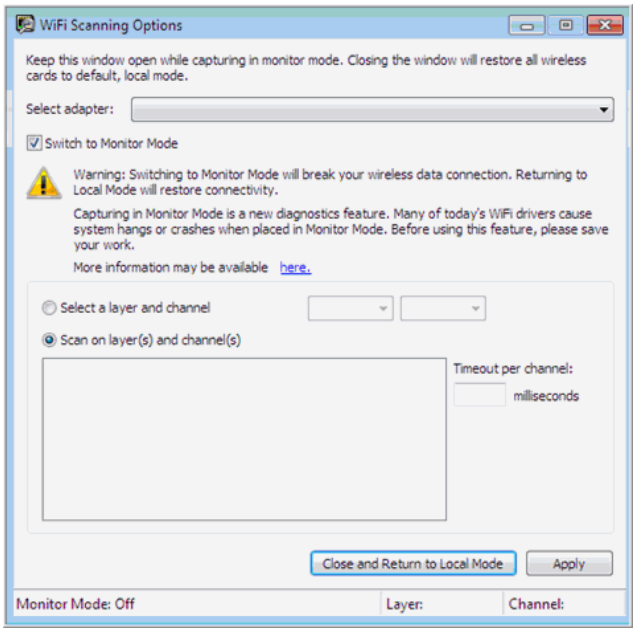


Windows versions prior to Vista are limited to NDIS 5, which does not support monitor (RFMON) mode. Therefore, the Netmon capture device does not support these operating systems for the purposes of wireless capture in monitor mode. However, the Netmon Capture Device does support **wired capture** in the same manneras WinPcap. This means that one can use the Netmon Capture device to capture wired traffic in lieu of installing WinPcap.

3. Start the **nmwifi.exe** application and select the wireless USB device from the dropdown list.

If your PC does not have a wireless USB device, the dropdown list will be empty.

4. Select the desired channel and check the box labeled **Switch to Monitor Mode** to enable RFMON on the wireless device.



5. Click the **Apply** button.
   You're ready to start capturing with the 9.0 Netmon capture device.

Linux Capture Device

The radio capture device for Linux requires the **mac80211** wireless stack that is the latest Linux kernels. This capture device offers the most control and capability over all other platforms.

> ⚠ Not all Linux wireless drivers support monitor mode. In addition, the firmware for the wireless chipsets found on the USB and PCI wireless adapters do not all support monitor mode. Therefore, one must take great care in selecting a device to use for wireless packet capture.

The target device for Linux is the USB form factor exclusively. Technically, any wireless USB device with a Ralink RT73 or RT2574 chipset are ideal. Like the current mmap(2) capture device, the Linux radio capture device provides a logical interface to capture wireless traffic across all installed wireless USB NICs simultaneously. This is useful for users who are using multiple wireless channels (e.g. 1, 6, 11).

802.11 Parsers

There are five link level parsers related to wireless LAN packet capture:

- IEEE 802.11 parser (data frames and beacons only)
- Radiotap w/ 802.11 header

- Absolute Value Systems (AVS) w/ 802.11 header
- Prism II w/ 802.11 header
- CACE's "Per Packet Information" (PPI) w/ 802.11 header

The IEEE 802.11 parser handles standard wireless frames. The other four parsers handle the link level encapsulation headers that are typically added by wireless drivers to the 802.11 frames captured by the wireless NIC. There is no standard format for these capture headers and they vary greatly according to the specific driver and operating system combination being used. We have attempted to provide parsers for the most prevalent formats available today.

The new 802.11 wireless parsers introduced in 9.0 all share a single configuration file. This configuration file is used to define any wireless access points the user may have in their network. The name of this file is wlan-config.xml and its primary purpose is to control decryption. The BSSID of the access point and the SSID that it's authoritative for is added to this file as well as all of the active default keys used by the access point. This file is technically optional. If decryption of 802.11 traffic is not desired, users are not required to create one at all.

Example **wlan-config.xml** configuration:

```
<wlan>
  <accesspoint bssid="00:1f:90:ea:6d:85" ssid="NwGuest"
channel="11">
    <wep>
      <key value="666f726765"/>
    </wep>
  </accesspoint>
</wlan>
```

This example includes every possible option currently supported. The only required attribute for the **<accesspoint/>** element is the **bssid**. The **ssid** and the channel are optional and are determined by the wireless parsers automatically by parsing 802.11 Management frames. If the wireless access point is configured to use 40/64 bit or 104/128 bit WEP, it should have a child element **<wep/>** defined that contains all of the default keys (the standard allows a maximum of 4). The **<key/>** element is used for this purpose and it has a single mandatory value attribute where a hexadecimal key is provided.

Only a string of hexadecimal values can be given for the **<key/>** element since there is no consistent method to turn a passphrase into a hex key for WEP for different vendors.

Supported Platforms

The supported platforms for wireless capture are:

- Windows 2000, XP (NDIS 5) (see page 146)
- Windows Vista, Windows 2003, Windows 2008, Windows 7 (NDIS 6) (see page 147)

- Linux (2.6.27+) (see page 148)

The most important goal for the radio capture devices is the ability to place the wireless network interface card (NIC) into what is known as monitor mode, also known as RFMON mode, which is one of six modes defined by IEEE 802.11. This mode, in particular, allows applications to monitor all traffic received from the wireless network, essentially grabbing raw 802.11 packets right out of the air. Unlike promiscuous mode, which is also used for packet sniffing, monitor mode allows packets to be captured without having to associate with an access point or ad-hoc network. The monitor mode is exclusive to wireless networks, while promiscuous mode can be used on both wired and wireless networks.

Windows 2000, XP

The versions of the Windows operating system are based on the Microsoft NDIS 5 standard, an API for network interface cards (NICs). Unfortunately, NDIS 5 does not support any extensions for monitor mode. Therefore, there is no radio capture device in the product that can directly capture 802.11 frames for those versions of Windows.

However, the existing WinPcap capture device in 9.0 has been updated to support the commercially available AirPcap wireless product from CACE Technologies. For users who have an AirPcap device, it is possible to use 9.0 to capture 802.11 traffic using one of two different link level frame capture formats, namely Radiotap or PPI.

In spite of the shortcomings of NDIS 5, older Windows users may still capture 802.11 packets, provided they have the AirPcap product. This is possible because the AirPcap product includes a branded wireless USB adapter and a proprietary device driver that can be used by the WinPcap library. This is the library that underpins popular network analysis applications such as Wireshark and WinDump as well as NetWitness. The latest version of AirPcap requires the WinPcap 4.1-beta library to work properly. This is included in the NetWitness product installation.

Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008

Starting with Vista, Windows operating systems began supporting NDIS 6, which allows for enabling monitor mode on the wireless NIC. As a result, we are able to utilize monitor mode for wireless packet capture with these platforms. The obvious limitation is that the new Netmon capture (see below) can only be used on platforms that support NDIS 6 *and* have wireless NICs that have NDIS 6 drivers that also support monitor mode.

In other words, using an wireless PCMCIA or USB adapter on Windows Vista that comes with a NDIS 5 or earlier driver will not support monitor mode. In those cases, the user's only options are to purchase and use the AirPcap product or obtain a NIC and driver from a vendor that supports NDIS 6.

Linux

Linux is the most powerful and enabling platform for wireless packet capture. The current wireless stack used by Linux 2.6 is called **mac80211** and is the API used by the Linux radio capture device. Despite the availability of a superior wireless API for controlling wireless devices, not all devices, specifically their internal chipset, nor all wireless Linux device drivers, support monitor mode. Fortunately, a great many do and have become popular choices for wireless Linux network analysis applications. NetWitness has chosen to develop and test against one of the most popular chipsets that offer monitor mode in the USB form factor, those produced by the Ralink Technology Corp. Ralink has been a exemplary supporter of the Linux driver community. Not surprisingly, their most popular chipsets--the RT73 and RT2500 series--are arguably the most fully supported of their class on Linux. Due to their cooperation with the Linux community, the rt73 and rt2500 Linux device drivers, and their respective firmware files, have been included in the mainline Linux kernel so there should be no need to download, compile, and install drivers for USB adapters with these Ralink chipsets. We chose to support the RT73 chipset specifically and all development and testing with that chipset has been exclusively on Fedora and Ubuntu. Ostensibly, any wireless USB adapter on the market that has the RT73 chipset could potentially be used by our Linux radio capture device. To date, the capture device on Linux 2.6.27 has been successfully tested against the following commercially available RT73 devices:

- ASUS WL-167G USB 2.0 WLAN Adapter
- Hawking HWUG1 Wireless G USB 2.0 Adapter w/ External SMA

Wired Equivalent Privacy

The Wired Equivalent Privacy (WEP) support allows for decryption of protected wireless frames captured from WLAN networks that operate in infrastructure mode which is typical of most 802.11 deployments today.

Support for 802.11i, which includes Wi-Fi Protected Access (WPA) is planned for a future release. It is likely that support for WPA2 will be added at the same time.

Index

E

H

I

L

M

N