RSA NETWITNESS® PLATFORM

NetWitness Investigate User Guide

for RSA NetWitness® Platform 11.3

Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

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

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

April 2019

Contents

How NetWitness Investigate Works **10**

Metadata, Meta Keys, Meta Values, and Meta Entities 10

Triggers for an Investigation 11

Workflow of an Investigation 11

Focus on Metadata, Query, and Time 13

Focus on NetWitness Respond Incidents and Alerts 15

NetWitness Investigate Views 15

Navigate View 15

Events View 16

Event Analysis View 17

Contextual Information for an Event 18

Event Reconstruction 20

Configuring NetWitness Investigate Views and Preferences **22**

Configure the Navigate View and Events View 23

Access the Navigate View and Events View Settings 23

Calibrate Navigate View Value Loading Parameters 25

Configure Navigate View and Events View Parameters 25

Configure the Default Log Export Format 26

Configure the Default Meta Export Format 27

Calibrate Events View Retrieval and Default Reconstruction 27

Enable or Disable Cascading Style Sheet Rendering in Web Content Reconstructions 27

Configure Search Options 28

Configure the Event Analysis View 29

Set the Default Investigate View 29

Set User Preferences for the Event Analysis View 30

Beginning an Investigation **32**

Focus on Metadata, Raw Events, and Event Analysis 32

Focus on Hosts and Files 32

Focus on Risky User and Entity Behavior 32

Focus on Scanning Files for Malware 33

Begin an Investigation in the Navigate or Events View 34

Begin an Investigation (No Default Service) 35

Set or Clear the Default Service 36

Begin an Investigation (Default Service Specified) 37

Change the Service or Collection to Investigate 38

Investigate Workbench Restoration Collections 39
Begin an Investigation in the Event Analysis View 41
Access the Event Analysis View (Version 11.1 and Later) 41
Access the Event Analysis View (Version 11.0) 44
Investigating Metadata in the Navigate View 45
Filter Results in the Navigate View 46
Set the Time Range 46
Set the Quantification Method and Sort Sequence of Meta Key Results 48
Manage and Apply Default Meta Keys in an Investigation 49
Drill into Data in the Navigate View Time Chart 52
Drill into Data in the Values Panel 53
Manage Meta Groups 61
Out-of-the-Box Meta Groups 61
Create a Meta Group and Add Meta Keys 62
Duplicate and Edit an Out-of-the-Box Meta Group 65
Edit a Meta Group 65
Delete a Meta Group 66
Export a Meta Group 67
Import a Meta Group 67
Visualize Metadata as Parallel Coordinates 68
Best Practices for Effective Parallel Coordinates Charts 68
RSA Meta Groups for Parallel Coordinates Use Cases 69
View a Parallel Coordinates Visualization 69
Select Meta Keys for a Parallel Coordinates Visualization 72
Optimize a Parallel Coordinates Visualization 74
Sample Use Case 76
Sample Visualization of a Large Data Set 77
Open an Event in the Events List 78
Export or Print a Drill Point 80
Launch a Malware Analysis Scan from the Navigate View 82
Visualize the Current Drill Point in Informer 84
Examining Raw Events in the Events View 85
Filter and Search Results in the Events View 86
Filter Events Displayed in the Events View 86
Search for Events in the Events View 88
Page Through Events in the Events View 89
Manage Column Groups in the Events View 90
Create Custom Column Group 90
Select a Column Group 92
Export Events in the Events View 94

Add Events to an Incident for Response 95
Combine Events from Split Sessions 97
Contextual Fragment Parsing 97
Session Fragments Highlighting 97
Find and Combine Fragments 99
Querying and Acting on Data in the Navigate and Events Views 101
Use Profiles to Encapsulate Common Areas for Investigation 102
Navigate to the Manage Profiles Dialog 102
Create, Edit, or Delete a Profile Group (Version 11.2 and Later) 103
Create and Edit Profiles 105
Delete a Profile 106
Change the Active Profile 106
Import Profiles 107
Download Profiles 107
Create a Custom Query 108
Create a Query Using the Basic Method 108
Create a Query Using the Advanced Method 110
Apply a Recent Query 111
Search for Text Patterns 113
Keyword Text Search 113
Search Examples 116
View and Modify Queries Using URL Integration 117
Service Id Known 117
Host and Port Known 117
Examples 118
Additional Notes 118
Launch an External Lookup of a Meta Key 119
Launch an Endpoint Thick Client Lookup 119
Launch Other External Lookups 121
Look Up Additional Context for a Data Point 122
Manage Context Hub Lists and List Values in the Navigate and Events Views 124
Add Meta Values to an Existing List 124
Remove a Meta Value from a Context Hub List 125
Create a New List 125
Reconstruct an Event 127
Reconstruct an Event from the Navigate View 127
Reconstruct an Event 128
View Side by Side or Top to Bottom 130
Select Event Information to View 130
Select Event Reconstruction Type 130

Open or Download an Email Attachment 131
Export an Event as a PCAP File 131
Extract Files from a Reconstructed Event 131
Analyzing Raw Events and Metadata in the Event Analysis View 132
Reconstruction Types in the Event Analysis View 133
The Text Analysis Panel 134
The Packet Analysis Panel 137
The File Analysis Panel 139
Analytical Tools for Each Type of Event Analysis 140
Filter Results in the Event Analysis View 142
Initial View 142
Select a Time Range 143
Create Filters in the Query Bar 144
Switch Between Guided Mode and Free-Form Mode 146
Work with Multiple Filters 146
Cancel Execution of a Query 148
View Status of a Query 148
Build a Query in Guided Mode 150
Create a Query in the Free-Form Mode 157
Examine Events in the Event Analysis View 159
Open, Close, and Adjust the Size of the Panels in the Event Analysis View 160
Select a Column Group and Columns in Event Analysis 162
Select the Event Analysis Type 164
Adjust the Display of Requests and Responses 164
View Event Metadata for an Event 165
Show or Hide the Event Header 167
Page Through Events in the Packet and Text Analysis Panels 167
Expand Truncated Text Entries in the Text Analysis Panel 168
Perform URL and Base64 Encoding and Decoding in the Text Analysis Panel 170
View Decompressed Text in an HTTP Network Session in the Text Analysis Panel 173
Use the Payload Only Option in the Packet Analysis Panel of a Network Session 175
View Highlighted Bytes in the Packet Analysis Panel 177
Highlight Common File Types in the Packet Analysis Panel 178
Look Up Additional Context in the Event Analysis View 180
Add an Entity to a Whitelist 183
Create a List 183
Pivot to Investigate > Navigate 184
Pivot to Archer 184
Pivot to NetWitness Endpoint Thick Client 185
Download Data in the Event Analysis View 186

Download a Log in the Text Analysis Panel 186
Download Network Event Data in the Text Analysis Panel or the Packet Analysis Panel 187
Download Files from a Network Event in the File Analysis Panel 188
Act on Data in the Event Analysis View 191
Open an Endpoint Event in the NetWitness Endpoint Thick Client 191
Perform Lookups of Meta Values in Event Analysis 192
Troubleshooting NetWitness Investigate 194
Navigate View and Events View Issues 194
Event Analysis View Issues 194
Investigate Reference Materials 198
Add Events to an Incident Dialog 199
Workflow 199
What do you want to do? 199
Related Topics 200
Quick Look 201
Add/Remove from List Dialog 202
Workflow 202
What do you want to do? 203
Related Topics 204
Quick Look in the Navigate and Events Views 204
Quick Look in the Event Analysis View (Version 11.2 and Later) 205
Context Lookup Panel 208
Workflow 208
What do you want to do? 208
Related Topics 209
Quick Look (in the Navigate and Events Views) 210
Quick Look in the Event Analysis View (Version 11.2 and Later) 212
Create an Incident Dialog 230
Workflow 230
What do you want to do? 230
Related Topics 231
Quick Look 231
Event Analysis View 233
Workflow 233
What do you want to do? 233
Related Topics 234
Quick Look 235
Query Console 237
Quick Look for Version 11.0.0.x (End-Of-Life) 238
Event Analysis View - File Analysis Panel 240

Workflow 240
What do you want to do? 240
Related Topics 241
Quick Look 241
Event Analysis View - Packet Analysis Panel 243
Workflow 243
What do you want to do? 243
Related Topics 244
Quick Look 244
Event Analysis View - Text Analysis Panel 246
Workflow 246
What do you want to do? 246
Related Topics 247
Quick Look 247
Event Reconstruction View 249
Workflow 249
What do you want to do? 249
Related Topics 250
Quick Look 250
Events View 253
Workflow 253
What do you want to do? 253
Related Topics 254
Quick Look 255
Detailed Description 257
Investigate Dialog 260
Workflow 260
What do you want to do? 260
Related Topics 261
Quick Look 262
Investigation Tab - User Preferences Panel 264
Related Topics 264
Quick Look 264
Investigate View 268
Workflow 268
What do you want to do? 269
Related Topics 269
Quick Look 270
Manage Column Groups Dialog 271
Related Topics 272

Quick Look 273
Manage Default Meta Keys Dialog 275
Related Topics 275
Quick Look 275
Manage Meta Groups Dialog 277
Related Topics 277
Quick Look 277
Manage Profiles Dialog 280
Related Topics 280
Quick Look 280
Navigate View 283
Workflow 283
What do you want to do? 283
Related Topics 284
Quick Look 285
Toolbar 286
Pause/Reload Button and Breadcrumb 289
(Optional) Debug Information 289
Time Banner 290
Visualizations 290
Values Panel 293
Query Dialog 297
Workflow 297
What do you want to do? 297
Related Topics 298
Quick Look 298
Settings Dialogs for Investigate Views 302
Related Topics 302
Quick Look 302

How NetWitness Investigate Works

NetWitness Investigate provides the data analysis capabilities in RSA NetWitness® Platform, so that analysts can analyze packet, log, and endpoint data, and identify possible internal or external threats to security and the IP infrastructure.

Note: In Version 11.1 and later, the Hosts and Files views provide a view into endpoint data. Earlier versions offer access to endpoint data using a standalone NetWitness Endpoint server.

Metadata, Meta Keys, Meta Values, and Meta Entities

RSA NetWitness Platform audits and monitors all traffic on a network. One type of service--a Decoder--ingests, parses, and stores the packets, logs, and endpoint data traversing the network.

The configured parsers and feeds on the Decoder create *metadata* that analysts can use to investigate the ingested logs and packets. Another type of service, called a Concentrator, indexes and stores the metadata.

The metadata is in the form of a *meta key* and *meta values* for the key. For example, `ip.src` is a meta key, and an IP address that is the source of the traffic is tagged as `ip.src`. When you view data in Investigate, you see the meta key `ip.src` and all of the IP addresses (values) that are tagged with that key. Some meta keys are built-in and others may be custom keys defined by the administrator.

Meta entities are available in Version 11.1 and later. A *meta entity* is an alias that groups together the results from other meta keys. Meta entities organize similar meta keys into a single, easier to use, meta type. Some meta entities are already included by default, and the administrator can create custom meta entities. Analysts can use a meta entity in a query, a meta group, a column group, and a profile. Parallel coordinates visualizations do not support meta entities. Administrators can use meta entities to define a query prefix to apply to a user role and a user. The *Decoder Configuration Guide* provides additional information about creating meta entities and how they can be used in rules.

Note: Meta entities need to be configured on all upstream Concentrators. If any Concentrator does not have a meta entity configured, that meta entity will be empty when you query the Broker.

For example, the default Core database language includes distinct meta keys for IP source and IP destination. One of the built-in meta entities named `ip.all` represents the combined set of all IP sources and destinations.

Analysts usually query the Concentrator to discover threats. The Concentrator handles queries, only going to the Decoder when a full reconstruction of sessions or raw logs is required. ESA, Malware Analysis, and Reporting Engine also query the Concentrator, where they can quickly get all the pertinent metadata associated with an event and generate information on the event without having to go to each Decoder. In some special cases, analysts may query a Decoder.

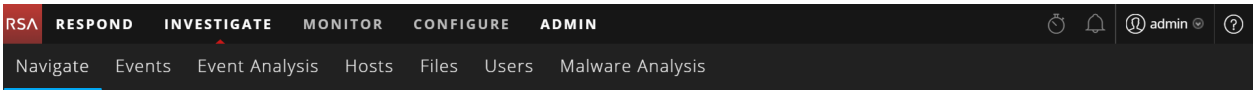
Triggers for an Investigation

These are a few examples of triggers for an investigation:

- You receive intelligence about a new active directory hack. Starting in the Events view, you use that intelligence to run a search across all of your raw Active Directory log data for the last 24 hours.
- You are asked by the SOC manager to find any Pokemon Go malware due to its popularity. Starting in the Navigate view, you craft a query to look for an HTTP session using a specific user agent related to the malware he found on a security blog.
- An incident responder escalates a ticket that shows some odd indicators related to a host. Starting in the Hosts view, you examine that host to find specific details.
- You are looking for the next zero day attack and start pivoting through network metadata in the Navigate view to find any abnormal automated sessions leaving the enterprise.
- You are asked by your SOC manager to find any information related to user `jarvis`, an employee who was just let go. Starting in the Hosts view, you query against the past week for that username.

Workflow of an Investigation

Analysts can investigate data captured by NetWitness Platform, and deep dive from information on a NetWitness Platform dashboard, a NetWitness Respond incident or alert, a report created by the NetWitness Platform Reporting Engine, or a third-party application. During the course of an investigation, analysts can move seamlessly between the views in Investigate: the Navigate view, the Events view, the Event Analysis view, the Hosts view, the Files view, the Users view, and the Malware Analysis view. This figure illustrates the NetWitness Investigate submenus.



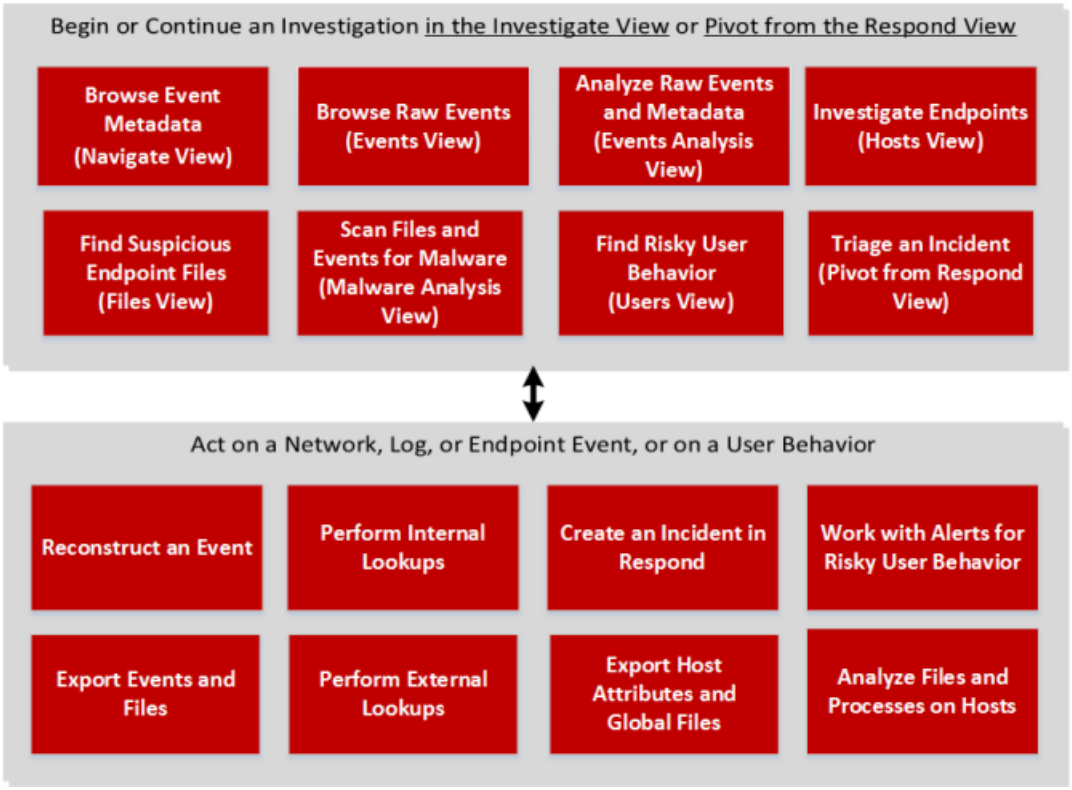
Note: The Files and Hosts views are available in Version 11.1 and later. The Users view is available in Version 11.2 and later. Specific user roles and permissions are required for a user to conduct investigations and malware analysis in NetWitness Platform. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you.

You can access each view from the Investigate submenu and from other Investigate views. You can also go directly into an Investigate view from NetWitness Respond, and go directly from NetWitness Investigate to NetWitness Respond and standalone NetWitness Endpoint. Your use case determines the starting point for your investigation. This table provides general guidance on the starting view for different use cases.

Go to...	Focus
Navigate view	All meta keys and meta values for logs, endpoints, and packets are grouped by meta key. You can pivot through the data to refine results, then go to the Events view or Event Analysis view, or look up in Malware Analysis or Live. This is the default NetWitness Investigate view. (See Investigating Metadata in the Navigate View.)

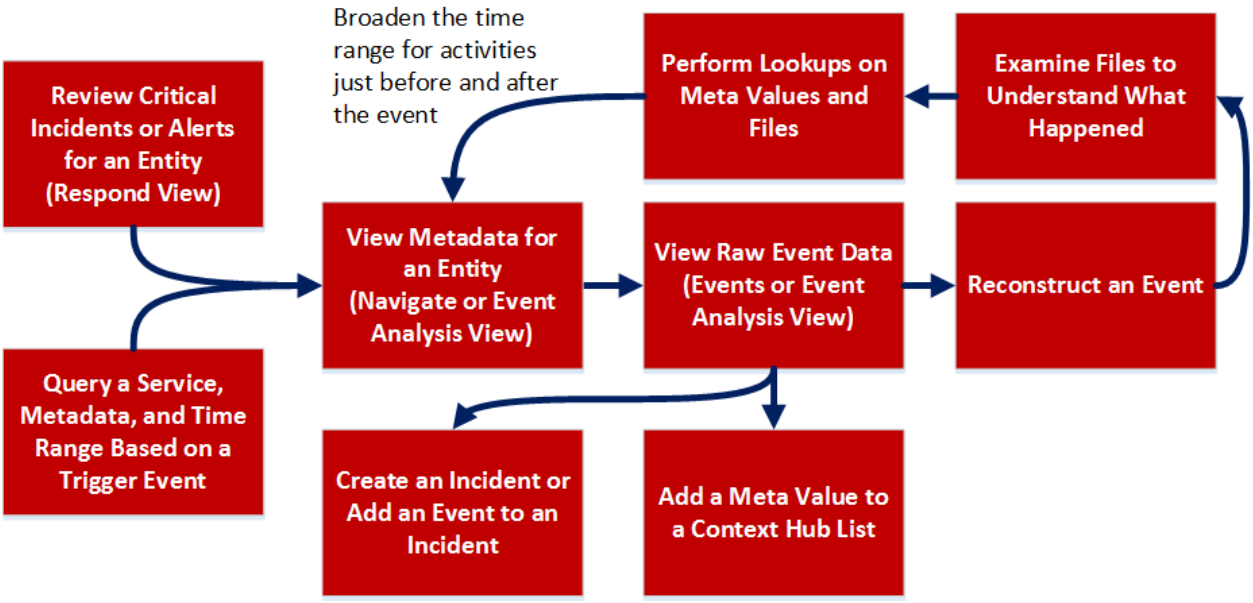
Go to...	Focus
Events view	Events are listed in order by time. You can view the raw event and related metadata, view a reconstruction, and download events and files. You can go to the Event Analysis view. (See Examining Raw Events in the Events View.)
Event Analysis view	Events are listed in order by time. You can view the raw event and related metadata, view a reconstruction that offers helpful cues to identify points of interest in a reconstruction, such as interesting bytes, file types, and encoded data. You can pivot to standalone Endpoint, look up in Live, and do external lookups. External lookups allow you to search the internet for meta values with which you interacted, determine passive DNS information related to an IP address, ascertain if a URL is blacklisted, and other third-party context integrations. (See Analyzing Raw Events and Metadata in the Event Analysis View)
(Version 11.1 and later) Hosts view	Hosts on which the NetWitness Endpoint Insights Agents are running are listed. For every host, you can view processes, drivers, DLLs, files (executables), services, anomalies, and autoruns that are running, and information related to logged-in users. From the Hosts view, you can go to the Navigate, Event Analysis, and Users views. (See the *NetWitness Endpoint User Guide*.)
(Version 11.1 and later) Files view	Unique files such as PE, Macho, and ELF in your deployment are listed. For each file, you can view details such as file name, reputation status, file status, risk score, signature, checksum, and others. From the **Files** view, you can go to the Navigate and Event Analysis views. (See the *NetWitness Endpoint User Guide*.)
Malware Analysis view	If you are running a Malware Analysis appliance, you can scan files and see results of four types of analysis: network, static, community, and sandbox. If a file is malware, you can go to the Hosts view to see which hosts downloaded the file. (See the *Malware Analysis User Guide*.)
(Version 11.2 and later) Users view	Provides visibility into risky user behaviors across your enterprise using NetWitness UEBA. You can view a list of high-risk users and a summary of the top alerts for risky behavior for your environment, and then select a user or an alert and view details about the risky behavior, and a timeline during which the behaviors occurred. NetWitness Platform users assigned the Administrators or UEBA Analysts role have access to this view. (See the *NetWitness UEBA User Guide*..

Every situation is unique in terms of the types of information the analyst is attempting to find. Many investigations start in one view, and end in a different view as the analyst learns something and then needs to follow that result to a different line of questioning. This figure shows the high-level capabilities of NetWitness Investigate. In the top box are all the possible starting points, and the lower box shows the tasks that you can accomplish from different starting points.



Focus on Metadata, Query, and Time

The following figure depicts the workflow for an investigation with focus on metadata, a query, and time range.



Analysts use NetWitness Investigate to hunt for events that drive the incident response workflow and to do strategic analysis after another tool has generated an event. Beginning in the Navigate view, Events view, or Event Analysis view:

- You start by executing a query on a service for a specific time range, then filter results to get a subset of events, reconstruct or analyze an event, and repeat the process to reconstruct or analyze another event. Built in profiles, meta groups, and column groups provide a good starting point. For example, you can choose the RSA Email Analysis profile to see only metadata that is useful when investigating email risks.
- When you encounter an event that bears a closer look, you view the context around the event, and decide whether to create an incident or add the event to an incident. If you decide not to add the event to an incident, you run another query to gain further insight, which starts again at the beginning of the workflow.
- If you notice suspicious activity or files on a specific host in the network, you can gather additional information about the host and files found on the host in the Hosts and Files view, or in a standalone NetWitness Endpoint server.
- If you find a file or event that potentially contains malware, you can do a Malware Analysis scan of the file or you can open Malware Analysis and start a scan of the service on which the event was seen.

Here is one simple use case: If there is a concern regarding suspicious traffic with foreign countries, the Destination Country meta key reveals all destinations and the frequency of the contact. Drilling into those values yields the specifics of the traffic, such as the IP address of the originator and the recipient. Checking other metadata can expose the nature of attachments exchanged between the two IP addresses. When suspect IP addresses are identified, looking at the addresses in the Navigate view or Event Analysis view with a broader time range can provide clues about what happened before and after the event being investigated.

Another use case is to investigate an alert to discover a malicious insider in the network who is exfiltrating intellectual property or other sensitive data from a specific IP address. The investigation begins with an **Upload without change request followed by download alert**. Start in the Navigate view by filtering the values to the IP address during the time range in which the alert was generated. Alerts metadata in the Navigate view show risk indicators as meta values and you can click on different meta values to reconstruct the event. Next extract files and examine the files to understand what happened. With this information, you can filter on the same IP address and broaden the time range to see activities before and after the event.

Focus on NetWitness Respond Incidents and Alerts

An analyst who is working on an incident or an alert in NetWitness Respond can open the incident in NetWitness Investigate (Navigate view) to do a deeper analysis of the event or alert.

- The workflow to respond to an incident typically begins in the Respond view, where the analyst who is investigating an incident needs to gather intelligence about the incident in NetWitness Investigate. You can hover over an underlined entity in an incident or alert, such as an IP address, and then select the action Pivot to Investigate > Navigate. The Navigate view opens and is filtered for the selected entity. After you launch an investigation from NetWitness Respond, defined meta keys are queried and the content of captured packets, logs, and endpoint events is displayed in the Navigate view.
- If you find events that are relevant to the incident, you can add the events to the incident in Respond. You can also create a new incident in Respond based on one or more events found in Investigate.
- (Version 11.2 and later) From the Incident Details view Indicators panel in Respond, you can open the Event Analysis view to get a better understanding of an indicator event.

NetWitness Investigate Views

This section provides a brief description and example of the Navigate view, Events view, and Event Analysis view, and views that provide additional context for data found--the Context Lookup panel and the Event Reconstruction view.

Refer to these guides for information about other Investigate views:

- The *NetWitness Endpoint User Guide* covers features and functions of the Hosts view and Files view.
- The *NetWitness UEBA User Guide* covers features and functions of the Users view.
- The *Malware Analysis User Guide* covers features and functions of the Malware Analysis view.

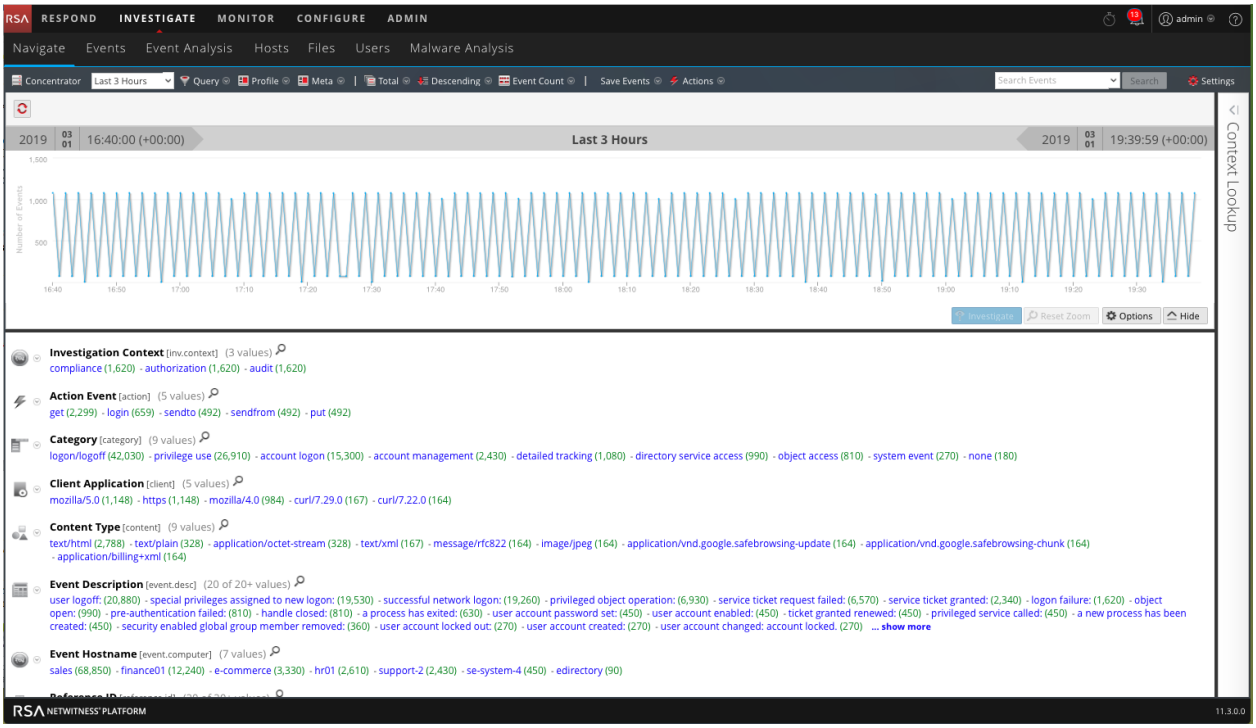
Navigate View

The Navigate view provides the capability to drill into and query contents of captured packets, logs, and endpoint events on a Broker, Concentrator, or Decoder (though investigating a Decoder is not typical).

- When you select a service, the defined meta keys for that service are queried, and values are returned along with the number of events. Clicking a value filters out the other value,s providing a view into a more focused set of data. This is called drilling into the data.

- For certain configured meta keys, such as IP address, or hostname, you can see additional context information around a value using the Context Hub. The additional context may include incidents, alerts, and other sources where the value was mentioned.
- The Navigate view also provides a sequential visualization of the data in a timeline. You can zoom in on a selected time period.

This figure illustrates the Navigate view.

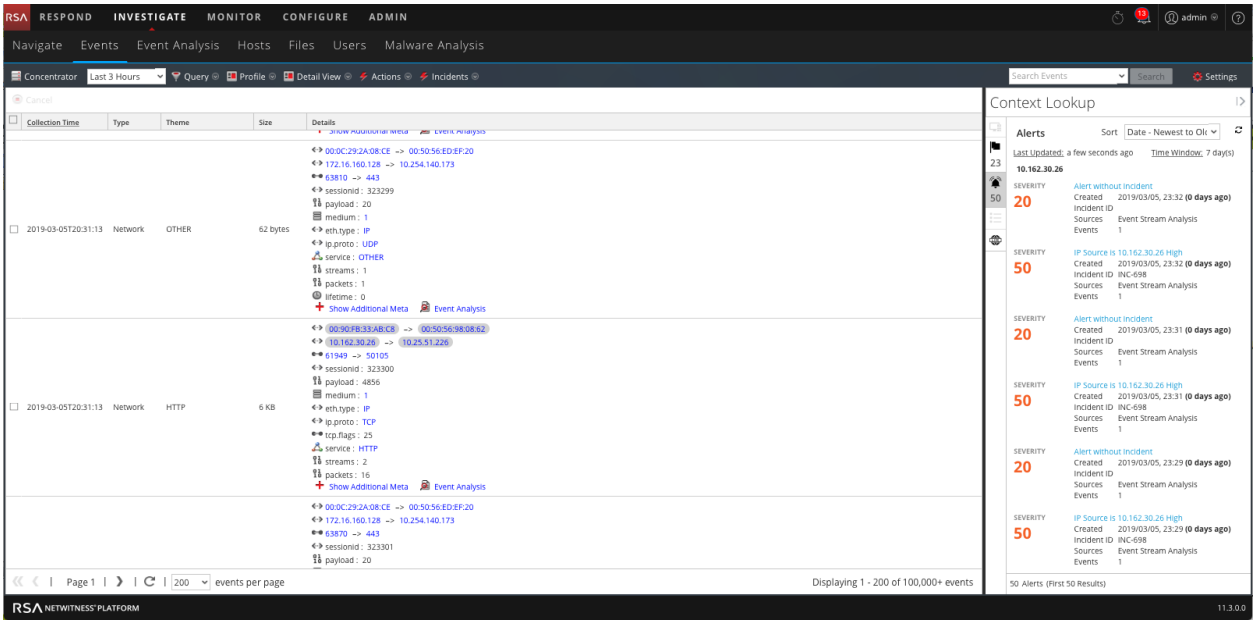


Events View

The Events view provides a view of packet, log, and endpoint events in list form so that you can view events sequentially and reconstruct events safely.

- You can open the Events view for a meta value that you see in the Navigate view.
- For analysts without sufficient privilege to navigate a service, the Events view is a standalone investigation view in which analysts can access a list of network, log, and endpoint events from a NetWitness Platform Core service without having to drill down through metadata first.
- The Events view presents event information in three standard forms, a simple list of events, a detailed listing of events, and a log view.
- For certain configured meta keys, such as IP address, or hostname, you can see additional context information around a value using the Context Hub. The additional context may include incidents, alerts, and other sources where the value was mentioned.
- You can export events and associated files, and create an incident from an event.

This figure illustrates the Events view.

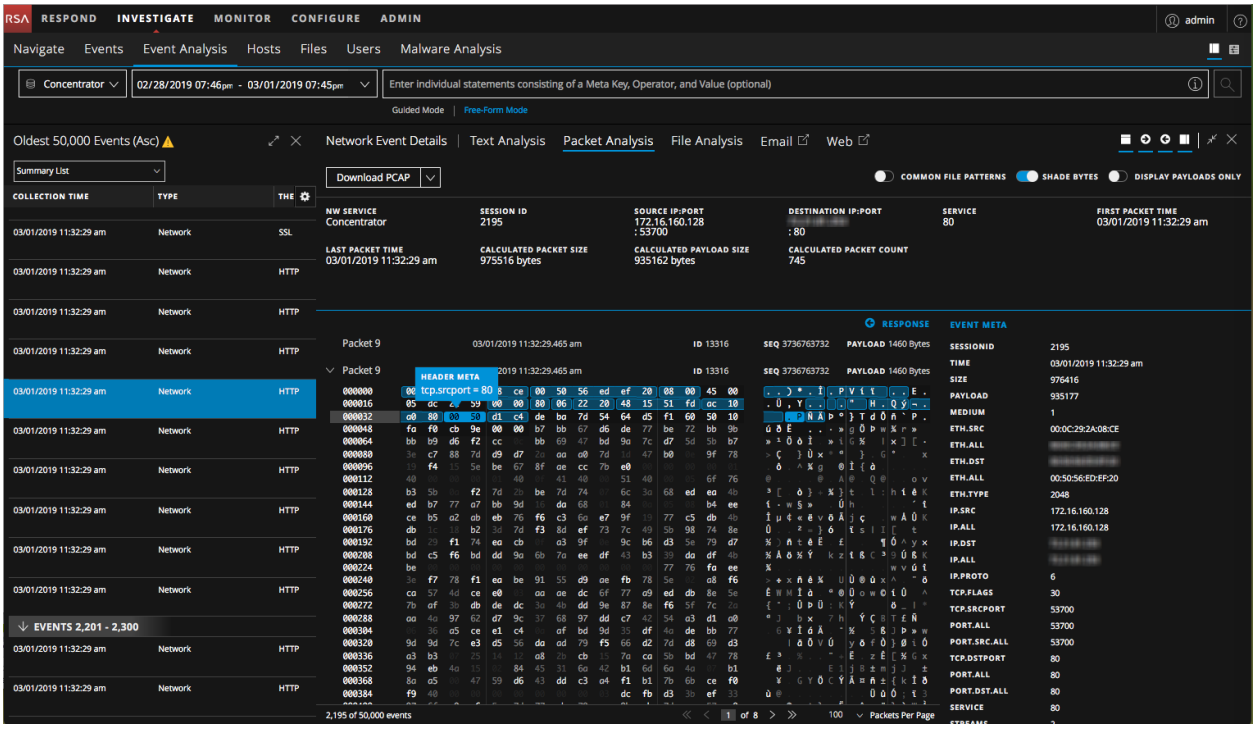


Event Analysis View

The Event Analysis view is an interactive tool to help analysts see the packets, text, or files in an event with visual cues to highlight certain types of information. Depending on the type of reconstruction different information is relevant.

- For certain configured meta keys, such as IP address, or hostname, you can search for additional context information around a value using the Context Hub. The additional context may include incidents, alerts, and other sources where the value was mentioned.
- When viewing files, you can export files in a zip archive to your local file system.
- You can download logs from the Text view, and export packets from the Packet view.

This figure is an example of the Event Analysis view.



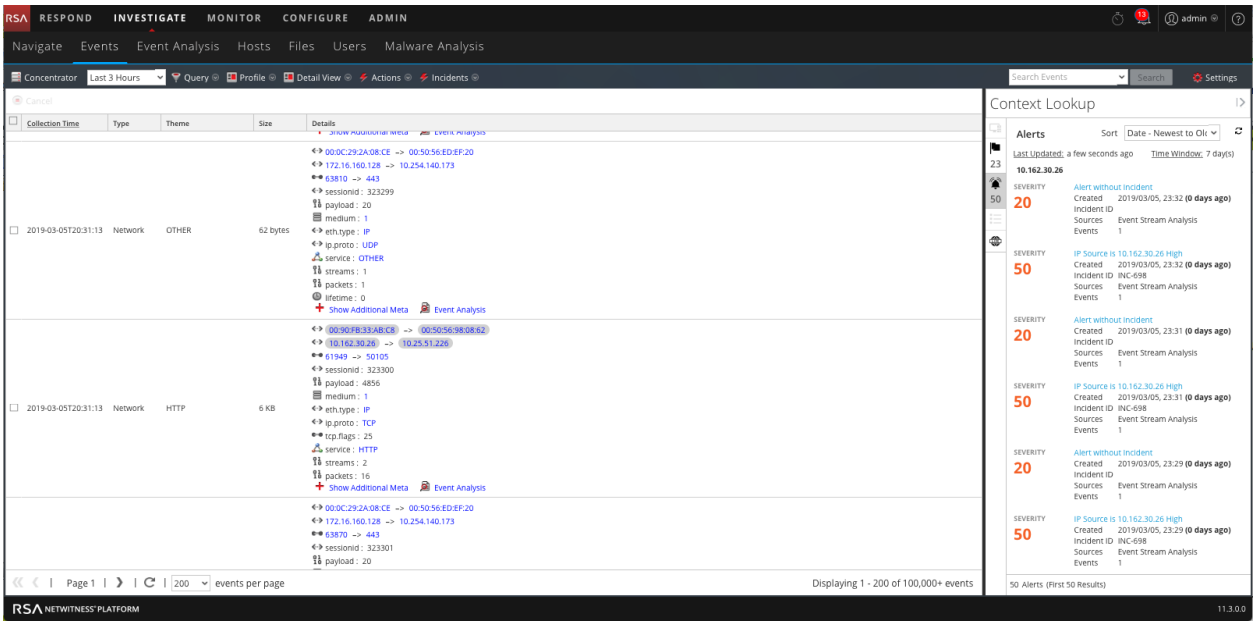
Contextual Information for an Event

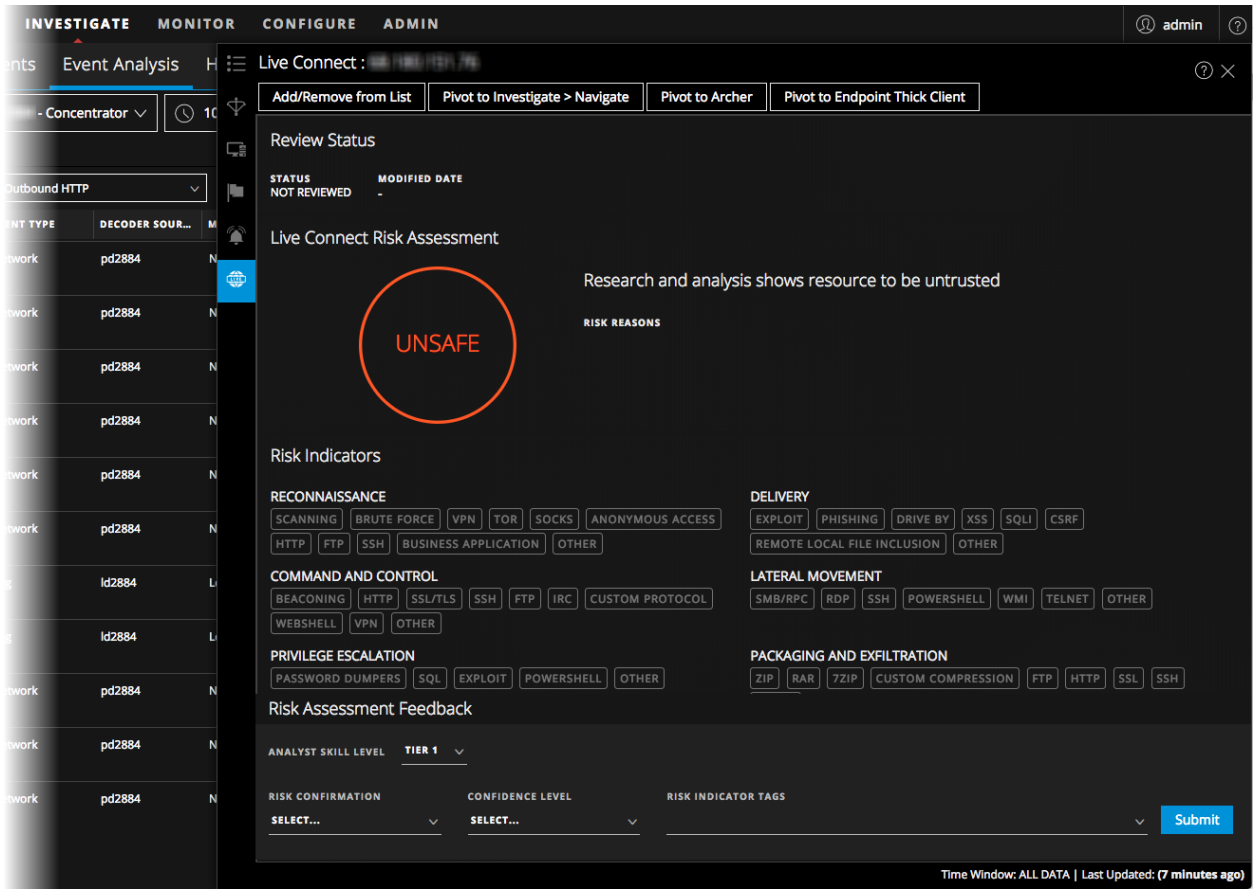
In the Navigate view, Events view, and Event Analysis view (Version 11.2 and later), the Context Lookup panel shows details about elements associated with an event (IP Address, User, Host, Domain, MAC Address, Filename, and File hash) in the Context Hub. In addition, you can right-click all meta keys except time to see additional context.

- You can interact with the elements of an event to get further insight including related incidents, alerts, custom lists, Archer assets, active directory details, and NetWitness Endpoint IIOCs.
- You can click on a data point to go to the Navigate view.

Note: Archer assets and active directory details are available in the Event Analysis view context lookup. Endpoint context lookup is available for NetWitness Endpoint 4.4.0.2 or later hosts, but not for the NetWitness Endpoint 11.1 hosts.

The following figures show the Context Lookup panel in the Events view and the Event Analysis view.

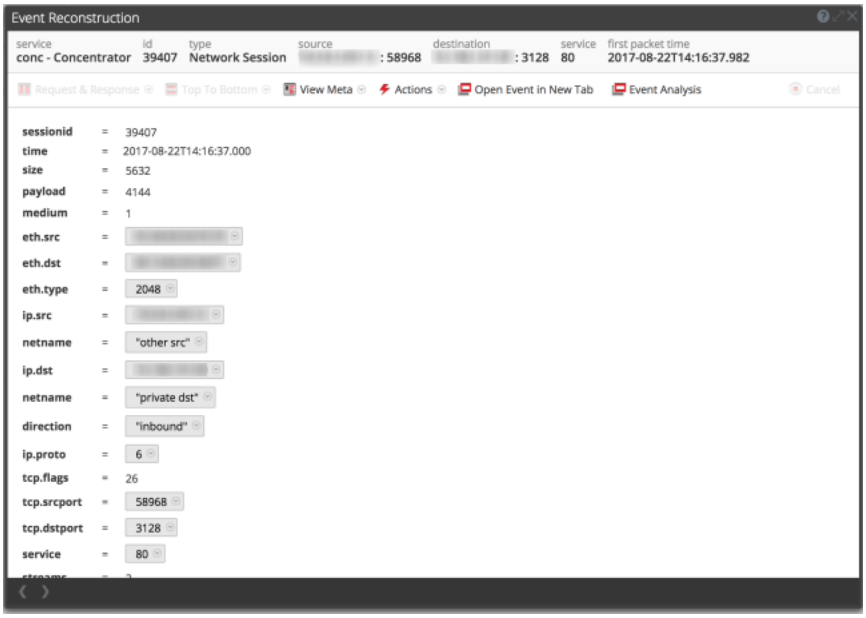

RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Navigate
Events
Event Analysis
Hosts
Files
Users
Malware Analysis
Concentrator
Last 3 Hours
Query
Profile
Detail View
Actions
Incidents
Search Events
Search
Settings
Collection Time
Type
Theme
Size
Details
2019-03-05T20:31:13
Network
OTHER
62 bytes
2019-03-05T20:31:13
Network
HTTP
6 KB
Show Additional Meta
Event Analysis
Page 1
200
events per page
Displaying 1 - 200 of 100,000+ events
Context Lookup
Alerts
Sort
Date - Newest to Ol
Last Updated: a few seconds ago
Time Window: 7 day(s)
10.162.30.26
SEVERITY
20
Alert without Incident
Created 2019/03/05, 23:32 (0 days ago)
Incident ID
Sources Event Stream Analysis
Events 1
50
IP Source is 10.162.30.26 High
Created 2019/03/05, 23:32 (0 days ago)
Incident ID INC-698
Sources Event Stream Analysis
Events 1
Created 2019/03/05, 23:31 (0 days ago)
Created 2019/03/05, 23:29 (0 days ago)
50 Alerts (First 50 Results)
RSA NETWITNESS PLATFORM
11.3.0.0


INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Event Analysis
Live Connect :
Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client
Review Status
STATUS
NOT REVIEWED
MODIFIED DATE
Live Connect Risk Assessment
UNSAFE
Research and analysis shows resource to be untrusted
RISK REASONS
Risk Indicators
RECONNAISSANCE
SCANNING
BRUTE FORCE
VPN
TOR
SOCKS
ANONYMOUS ACCESS
HTTP
FTP
SSH
BUSINESS APPLICATION
OTHER
DELIVERY
EXPLOIT
PHISHING
DRIVE BY
XSS
SQLI
CSRF
REMOTE LOCAL FILE INCLUSION
OTHER
COMMAND AND CONTROL
BEACONING
HTTP
SSL/TLS
SSH
FTP
IRC
CUSTOM PROTOCOL
WEBSHELL
VPN
OTHER
LATERAL MOVEMENT
SMB/RPC
RDP
SSH
POWERSHELL
WMI
TELNET
OTHER
PRIVILEGE ESCALATION
PASSWORD DUMPERS
SQL
EXPLOIT
POWERSHELL
OTHER
PACKAGING AND EXFILTRATION
ZIP
RAR
7ZIP
CUSTOM COMPRESSION
FTP
HTTP
SSL
SSH
Risk Assessment Feedback
ANALYST SKILL LEVEL
TIER 1
RISK CONFIRMATION
SELECT...
CONFIDENCE LEVEL
SELECT...
RISK INDICATOR TAGS
Submit
Time Window: ALL DATA | Last Updated: (7 minutes ago)

Event Reconstruction

Three NetWitness Investigate views offer the ability to reconstruct an event: Navigate view, Events view and Event Analysis view. When you discover an event that merits additional investigation, you can reconstruct an event safely in a form similar to its native form. The rendering of events restricts the use of dynamic or active code that might be contained in the event to limit any adverse outcome to your system or browser. Cache is used to improve performance when viewing previously viewed events. Each analyst has a separate cache of reconstruction data, and you can only access reconstructed events in your own cache.

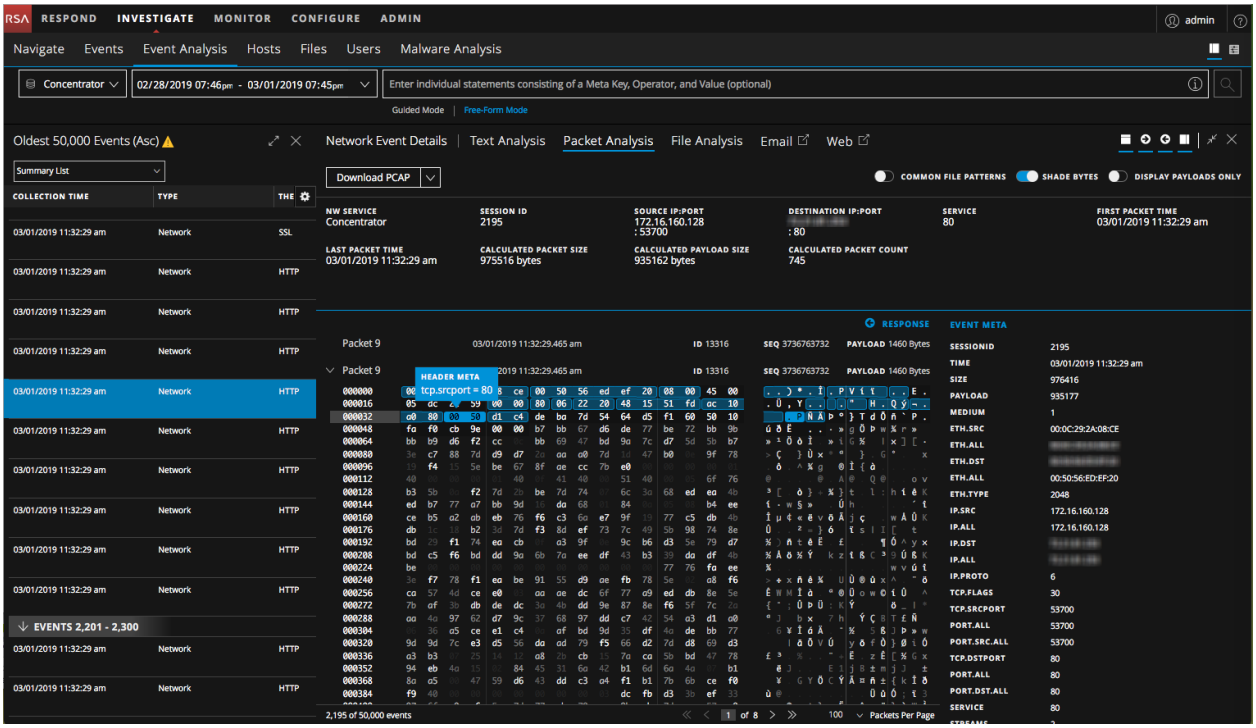
The Event Reconstruction in the Events view presents the raw data and the meta keys and meta values for an event in a list form. This figure is an example of the Event Reconstruction.



In this Event Reconstruction, you can:

- Page through the reconstruction to view the next event in this form.
- Reconstruct events using different methods to suit the type of data: metadata, text, hexadecimal, packets, web, mail, files, or the best reconstruction selected automatically.
- Export packet capture files, extract files, and export the meta values for the event.

The Event Analysis view presents an interactive event reconstruction, which includes raw data, meta keys, and values. This figure is an example of a reconstruction in the Event Analysis view.



In the Event Analysis view reconstruction, you can:

- Reconstruct an event using different methods to suit the type of data: metadata, text, hexadecimal, packets, and files.
- Understand more about highlighted information in the headers and payloads.
- View decoded and encoded payloads and see common file signatures.
- Search for locations of meta keys or values in the reconstruction.
- Export events and files.

Configuring NetWitness Investigate Views and Preferences

Analysts can configure some aspects of NetWitness Investigate views and behavior. You can customize the way that Investigate views appear, the types of information displayed, and factors that affect performance in returning results and reconstructing events. All configurable settings have default values that are effective in most deployments; however, analysts have the option to adjust these if necessary.

Analysts using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles and permissions as described in the *System Security and User Management Guide*.

These topics provide details:

- Configure the Navigate View and Events View
- Configure the Event Analysis View

Configure the Navigate View and Events View

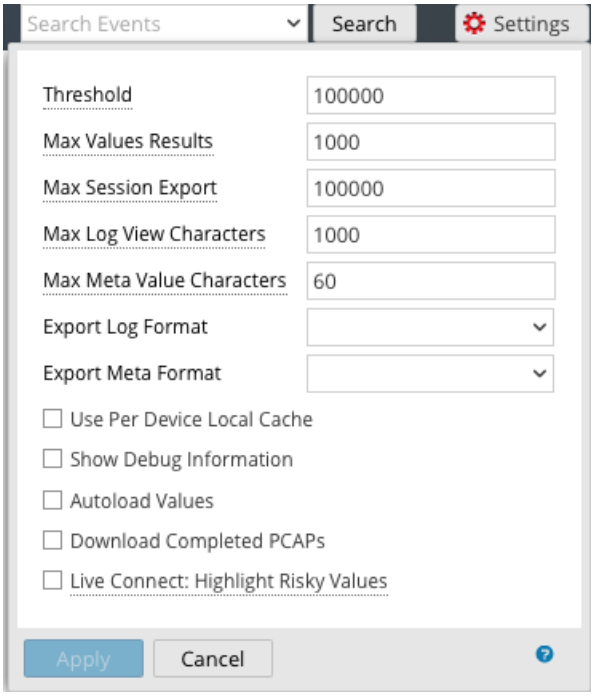
Analysts can set preferences that affect performance and behavior of NetWitness Platform when using the Navigate view and Events view. Some of the same settings are available in two places in NetWitness Platform, and changes made in either location are applied in the other view:

- Investigate view > Settings dialog for the Navigate view and the Events view.
- Profiles > Preferences panel > Investigation tab.
- Navigate view and Events view Search Options drop-down.

Access the Navigate View and Events View Settings

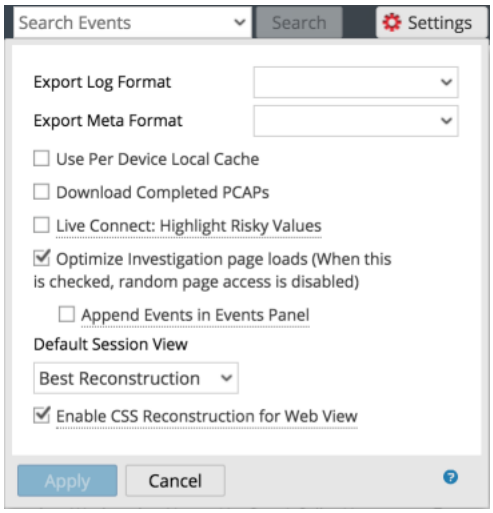
To access the settings, do one of the following:

- In the **Navigate** view toolbar, select the **Settings** option.
  The Settings dialog for the Navigate view is displayed.



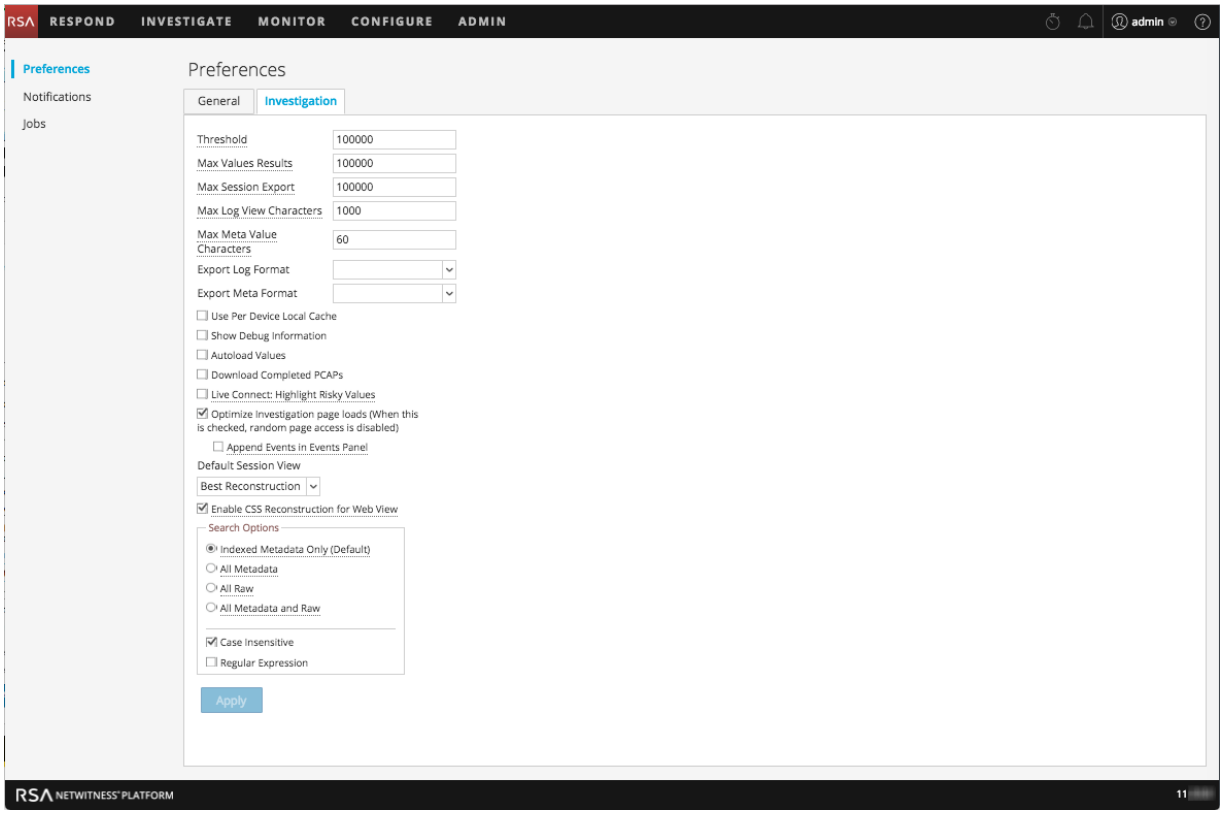
Note: Version 11.0 included a setting to Append Events in Events Panel, which was moved to the Events view settings panel in Version 11.1.

- In the **Events** view toolbar, select the **Settings** option.
  The Settings dialog for the Events view is displayed.



Note: Version 11.1 and later includes the Append Events in Events Panel setting.

- In the top right corner of NetWitness Platform, go to > , Profile, and in the **Preferences** panel click the **Investigation** tab.
  The Investigation panel is displayed. The figure below illustrates the Investigation panel.



Calibrate Navigate View Value Loading Parameters

Several settings influence the performance of NetWitness Platform when loading values in the Values panel. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations. To adjust these settings:

1. Go to the **Preferences** panel >**Investigation** tab or to the **Settings** dialog for the Navigate view.
2. Adjust the following parameters:
   - **Threshold:** Set the threshold for the maximum number of sessions loaded for a meta key value in the Values panel. A higher threshold allows accurate counts for a value, and also causes longer load times. The default value is **100000**.
   - **Max Values Results:** Set the maximum number of values to load in the Navigate view when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**.
   - **Max Session Export:** Specify the number of events that can be exported in a single PCAP or Log file.
   - **Max Log View Characters:** Set the maximum number of characters to be displayed on **Investigate > Events > Log Text**. The default value is **1000**.
   - **Max Meta Value characters:** Set the maximum number of characters in a meta value name displayed in the Navigate view Values panel. The default value is **60**.
   - **Show Debug Information:** If you want NetWitness Platform to display the `where` clause beneath the breadcrumb in the Navigate view and the elapsed load time for each aggregated service on a Broker, check this option. The default value is **Off.**
   - **Append Events in Events Panel:** This option affects paging in the Events view and is described below under "Calibrate Events View Retrieval and Default Reconstruction."
   - **Autoload Values:** If you want NetWitness Platform to automatically load values for the selected service in the Navigate view, check this option. When not selected, NetWitness Platform displays a **Load Values** button, allowing the opportunity to modify options. The default value is **Off**.
3. Click **Apply**.
   The settings become effective immediately and are visible the next time you load values.

Configure Navigate View and Events View Parameters

Several settings influence the performance of NetWitness Platform when loading values in the Navigate view and the Events view. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations. You can set these parameters separately in the Navigate view and the Events view. When configured in one view, the setting does not automatically apply to the other view. To adjust these settings:

1. Go to the **Preferences** panel > **Investigation** tab or to the **Settings** dialog for the Navigate view or the Events view.

2. Adjust the following parameters:
   - **Live Connect: Highlight Risky Values:** If you want NetWitness Platform to highlight and display only IP addresses that are considered as risky by RSA community, check this option. When not selected, NetWitness Platform displays all IP addresses. By default, this option is not selected (**Off**).
   - **Use Per Device Local Cache:** You can specify the use of locally cached data from the selected service. By default, this option is not selected **(Off)**. When unchecked, Investigate sends a fresh query to the database rather than displaying cached data in the Investigate views after the initial load. If checked, Investigate uses the data from local cache.
   - **Download Completed PCAPs:** You can automate the downloading of extracted PCAPs in the Navigate view and Events view so that the browser downloads the extracted PCAP and opens it in the default application for opening PCAP files, such as Wireshark. By default, this option is not selected (**Off**). If you are going to enable this option, ensure that an application that can open PCAPs is installed on your local file system and that the application is set as the default application to handle PCAP file formats.
   - **Live Connect: Highlight Risky Values:** If this option is unchecked, all the meta values that have context available in Live Connect are highlighted in the Navigate view Values panel. If the option is checked, among the values that have context in Live Connect, only those values deemed Risky/Suspicious/Unsafe by the community are highlighted. By default this option is unchecked (**Off**).
3. Click **Apply**.
   The settings become effective immediately.

Configure the Default Log Export Format

You can export logs from the Navigate view and the Events view as Text, XML, comma-separated values (CSV), and JSON. There is no built-in default value for the log export format. If you do not select a format here, NetWitness Platform displays a selection dialog when you invoke export of logs. To select the format for exported logs:

1. Go to the **Preferences** panel >**Investigation** tab or to the **Settings** dialog for the Navigate view or Events view.
2. Select one of the options from the **Export Log Format** drop-down menu.
3. Click **Apply**.
   The setting goes into effect immediately.

Configure the Default Meta Export Format

You can export meta values from the Navigate view and Events view as Text, CSV, tab-separated values (TSV), and JSON. There is no built-in default value for the meta export format. If you do not select a format here, NetWitness Platform displays a selection dialog when you invoke export of meta values. To select the format for exported meta values:

1. Go to the **Preferences** panel > **Investigation** tab or to the **Settings** dialog for the Navigate view or Events view.
2. Select one of the options from the **Export Meta Format** drop-down menu.
3. Click **Apply.**
   The setting goes into effect immediately.

Calibrate Events View Retrieval and Default Reconstruction

You can configure several parameters that control the how NetWitness Platform retrieves events and reconstructs events in the Events view. To adjust these paramaters:

1. Go to the **Preferences** panel > **Investigation** tab or to the **Settings** dialog for the Events view.
2. Configure the following parameters.
   - **Optimize Investigation page loads**: Set a paging option. When optimized, results are returned as quickly as possible,and you cannot go to a specific page in the event list. Unchecking this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). The default value is **enabled**.
   - **Default Session View:** Selects the default reconstruction type for the initial reconstruction in the Events view. The default value is **Best Reconstruction** in which events are reconstructed using the reconstruction method most appropriate to the event.
3. Go to the **Preferences** panel > **Investigation** tab, or to the **Settings** dialog for the Navigate view (11.1) or the Events view (11.2), and set the **Append Events in Events Panel** option. When this option is selected, the events displayed in the **Events Panel** are added incrementally. For example, each time you click the next page icon, the next increment of events is added, at first you see 1 to 25, then 1 to 50, then 1 to 75 and so on. This option is available only if the **Optimize Investigation Page Loads** option is enabled.
4. To activate the changes immediately, click **Apply**.

Enable or Disable Cascading Style Sheet Rendering in Web Content Reconstructions

Analysts can enable the use of cascading style sheets (CSS) when reconstructing web content. If enabled, the web reconstruction includes CSS styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for style sheets and images used in the target event. The option is enabled by default. Disable this option if there are problems viewing specific websites.

Note: The appearance of the reconstructed content may not match the original web page perfectly if related images and style sheets could not be found or were loaded from the web browser's cache. Also, any layout or styling that is performed dynamically through the client side javascript is not rendered in the reconstruction because all client side javascript is removed for security purposes.

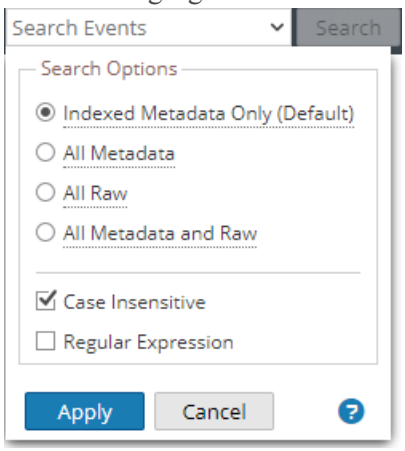
To enable or disable this option:

1. Go to the **Preferences** panel > **Investigation** tab.
2. Select the **Enable CSS Reconstruction for Web View** checkbox.
3. Click **Apply**.
   The setting becomes effective immediately and is visible in the next web content reconstruction.

Configure Search Options

You can configure search options to apply when you type a search string in the Search field. Edit the Search Options in the Profile > Preferences panel > Investigation tab or in the Navigate and Events view Search Options drop-down menu. To configure search options:

1. Navigate to the Search Options.
   The following figure illustrates the Search Options drop-down menu for Version 11.2 and later.



2. Select one or more search options to apply to the search. Search for Text Patterns provides detailed information about each option.
3. To save the search settings, click **Apply**.
   The preferences are saved and effective immediately.

Configure the Event Analysis View

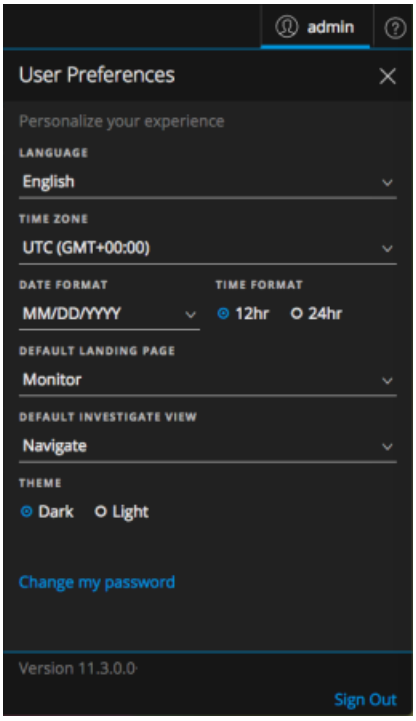
Note: The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

Analysts can set preferences that affect the behavior of NetWitness Platform when using the Investigate > Event Analysis view. In the Event Analysis view is open; these two buttons give access to preferences dialogs: and . The User menu ( ) is focused on global user preferences such as time zone, while the Event Analysis preferences menu ( ) is focused on user preferences for behavior in the Event Analysis view. The rest of this section describes both sets of preferences.

Set the Default Investigate View

You can select the default view when you open Investigate: Navigate view, Events view, Event Analysis view, Hosts view, Files view or Malware Analysis view. The default Investigate view is set in the global User Preferences dialog (in the upper right corner of the NetWitness Platform browser window, select).

The global user preferences are described in detail in the *NetWitness Platform Getting Started Guide*.

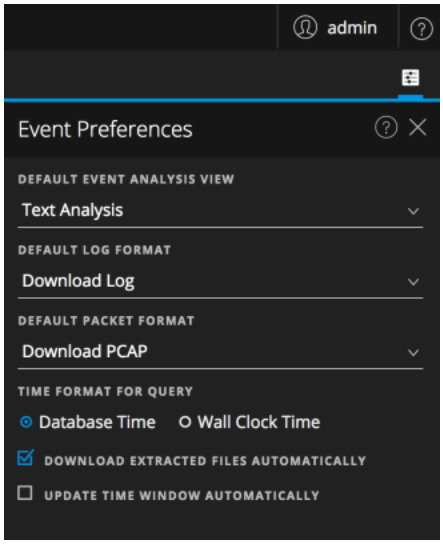


Set User Preferences for the Event Analysis View

You can set your own preferences relevant to the Event Analysis view. The preferences selected persist per user and are available whenever the specific user logs in to the application.

To set default values for working in the Event Analysis view:

1. In the Event Analysis view, click .



2. In the **Default Event Analysis View** drop-down menu, select the default reconstruction type when you open an event in the Event Analysis panel: **Text Analysis**, **Packet Analysis**, or **File Analysis**. If you have not selected a default analysis type, when you open an event, the default reconstruction type is the Packet Analysis, except for log and endpoint events, which open to the Text Analysis. If you select a default reconstruction type, the reconstruction type is the default reconstruction that you specified. In both cases, the default is the starting point, and if you change the type while you are working, the type you choose is used for the next reconstruction.
3. In the **Default Log Format** drop-down, select the download format for exporting logs: **Download Log**, **Download XML**, **Download CSV**, or **Download JSON**. If you do not select a format here, the default download format is **Download Log**. These options are also available at the time of download in a drop-down menu.
4. In the **Default Packet Format** drop-down menu, select the default format for downloading packets. These options are also available at the time of download in a drop-down menu:
   - **Download PCAP** to download the entire event as a packet capture (*.pcap) file
   - **Download All Payloads** to download the payload as a *.payload file
   - **Download Request Payload** to download the request payload as a *.payload1 file
   - **Download Response Payload** to download the response payload as a *.payload2 file
5. Under **Time Format for Query**, choose either **Database Time** or **Wall Clock Time**. The Event Analysis view can display results based on the database time or the current clock time. When you set the time format, your individual user preference is saved until changed again. The default setting for

this preference is **Database Time**, which is the same time format used to display query results in the Navigate view and Events view.

- When **Database Time** is selected, the start and end time for a query is based on the time that the event was stored.
- When **Wall Clock Time** is selected, the query is executed with the current time in accordance with the timezone set in user preferences. The current time is focused on real time ingestion of captured data rather than PCAP uploads.

6. If you want all extracted files to be downloaded automatically, select the **Download extracted files automatically** checkbox. You can go to the Jobs queue to view the extracted files.
7. (Version 11.3 and later) To automatically update the time range window in the query bar when the service is polled (at one minute intervals) and sends fresh results, select the **Update Time Window Automatically** checkbox. When the time range is updated, the (Submit Query) button is activated and you can click to get the fresh results. To keep the time range window in the query bar synchronized with the current results, clear the checkbox (this is the default value).

Beginning an Investigation

Based on the question you are attempting to answer, NetWitness Platform offers different starting points: Navigate view, Events view, Event Analysis view, Hosts view, Files view, Users view, and Malware Analysis view.

Note: Specific user roles and permissions are required for a user to conduct investigations in NetWitness Platform. If you cannot perform a task or see a view, the administrator may need to adjust the roles and permissions configured for you.
-The Hosts and Files views are available in Version 11.1 and later (refer to the *NetWitness Endpoint Quick Start Guide* and *NetWitness Endpoint User Guide* for details).
-The Users view is available in Version 11.2 and later (refer to the *NetWitness UEBA Quick Start Guide* and the *NetWitness UEBA User Guide* for details).

Focus on Metadata, Raw Events, and Event Analysis

To hunt for events that drive the incident response workflow and to do strategic analysis after another tool has generated an event, go to **INVESTIGATE > Navigate**, **INVESTIGATE > Events**, or **INVESTIGATE > Event Analysis**. You can investigate the metadata and raw events for a single Broker or Concentrator. In each of these views, you can execute a query and filter the results by narrowing the time range and querying metadata. These topics provide details about beginning an investigation:

- Begin an Investigation in the Navigate or Events View
- Begin an Investigation in the Event Analysis View

Focus on Hosts and Files

To hunt for information on hosts that have the Endpoint agent running, go to **INVESTIGATE > Hosts**. For every host, you can see processes, drivers, DLLs, files (executables), services, and autoruns that are running, and information related to logged-in users. To begin an investigation by looking at files in your deployment, go to **INVESTIGATE > Files**. (See the *NetWitness Endpoint User Guide* for detailed information.)

Focus on Risky User and Entity Behavior

To discover, investigate, and monitor risky behaviors across all users and entities in your network environment, go to **INVESTIGATE > Users** and NetWitness UEBA (User and Entity Behavior Analytics). You can detect malicious and rogue users, pinpoint, high-risk behaviors, discover attacks, and investigate emerging security threats. (See the *NetWitness UEBA User Guide* for detailed information.)

Focus on Scanning Files for Malware

To scan files for potential malware, or set up a continuous scan of a service, go to **INVESTIGATE > Malware Analysis**. Scan results are expressed as four types of analysis: network, static, community, and sandbox with an indicator of compromise (IOC) rating. There are several other ways to begin working in Malware Analysis:

- You can begin Malware Analysis from the Malware Analysis dashlets in the Monitor view to quickly see the riskiest potential threats.
- You can right-click a meta key in the Navigate view, and select **Scan for Malware**.

See the *Malware Analysis User Guide* for detailed information.

Begin an Investigation in the Navigate or Events View

The Navigate view is the default view for Investigate unless you have selected a different view as your opening view. This user preference is set on the application level as described in Configuring NetWitness Investigate Views and Preferences. In the Navigate view and Events view, you are hunting for events of interest based on a query. In the Navigate view you can also refine results by clicking on meta keys and meta values. When you find interesting events, you can take a closer look at the event in the other Investigate views.

To begin an investigation in the Navigate view or Events view, a service must be specified.

- NetWitness Platform opens the Navigate view or the Events view with the user-specified default service selected.
- If no default service is currently specified and the service id is not in the URL, NetWitness Platform presents a dialog for selecting the service or collection to investigate.
- When a service is selected manually or by default in the Navigate view or Events view, you can change the service or collection to investigate by selecting the service name in the toolbar. NetWitness Platform presents the dialog for selecting the service to investigate.

Note: The Archiver service does not appear in the Navigate view to minimize user experience of slow performance when performing investigations. The Archiver is available in the Events view for log exports and enhanced search capabilities.

With a service or collection selected, NetWitness Platform is ready to load data for the service or collection. It is recommended that you also select a time range so that results load faster. Several settings in the Navigate View and Events View Settings dialog or the Profiles > Preferences panel > Investigations tab affect the loading process: Threshold, Max Values Results, Show Debug Information, Autoload Values, and Optimize Investigation page loads (see Configuring NetWitness Investigate Views and Preferences).

Note: In the Events view data loads automatically. If you specified Autoload Values in the Navigate view preferences, NetWitness Platform populates the data automatically. Otherwise, you must select Load Values . NetWitness Platform populates the meta data in the Navigate view Values panel and results become visible almost immediately.

The rest of this topic provides instructions for beginning the investigation of data on a service.

Note: Only users with the administrator role can create a collection, and only the creator of the collection is able to investigate a collection.

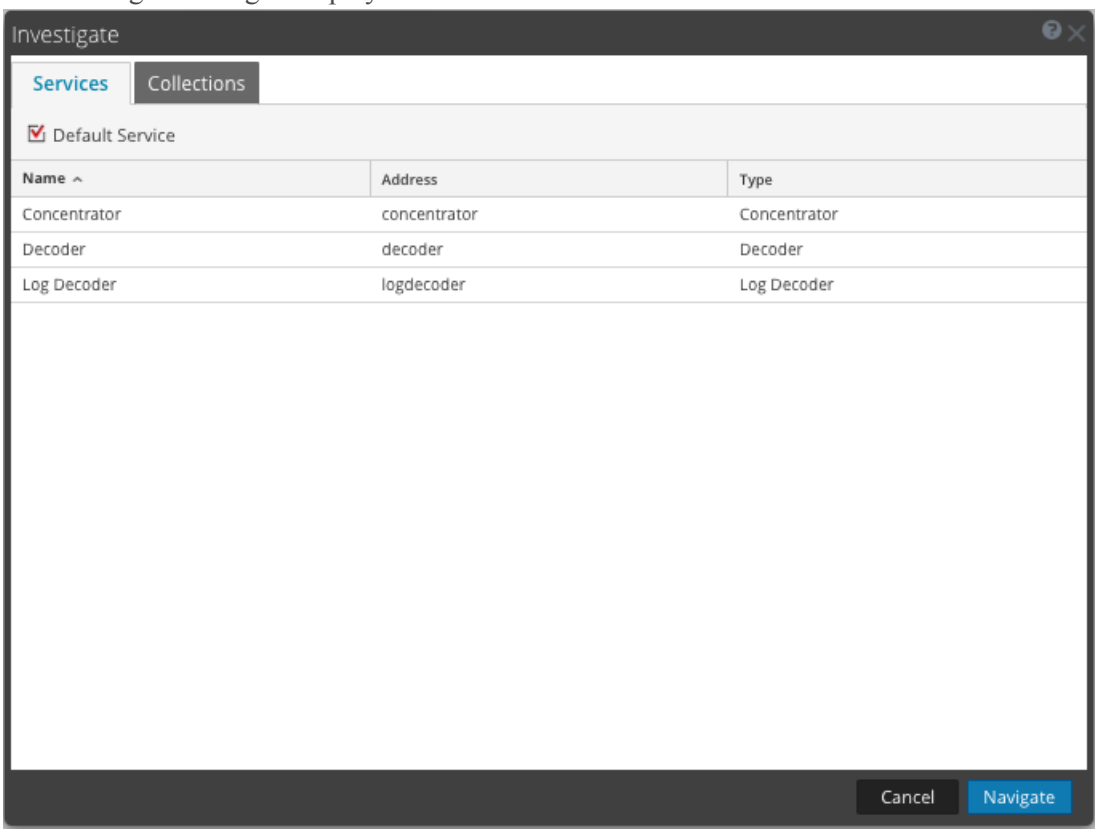
After loading data in the Navigate or the Events view:

1. Refine results, visualize data, and act on a drill point (see Investigating Metadata in the Navigate View) and Examining Raw Events in the Events View). For example, you can Look Up Additional Context for a Data Point, Launch a Malware Analysis Scan from the Navigate View, or Add Events to an Incident for Response.

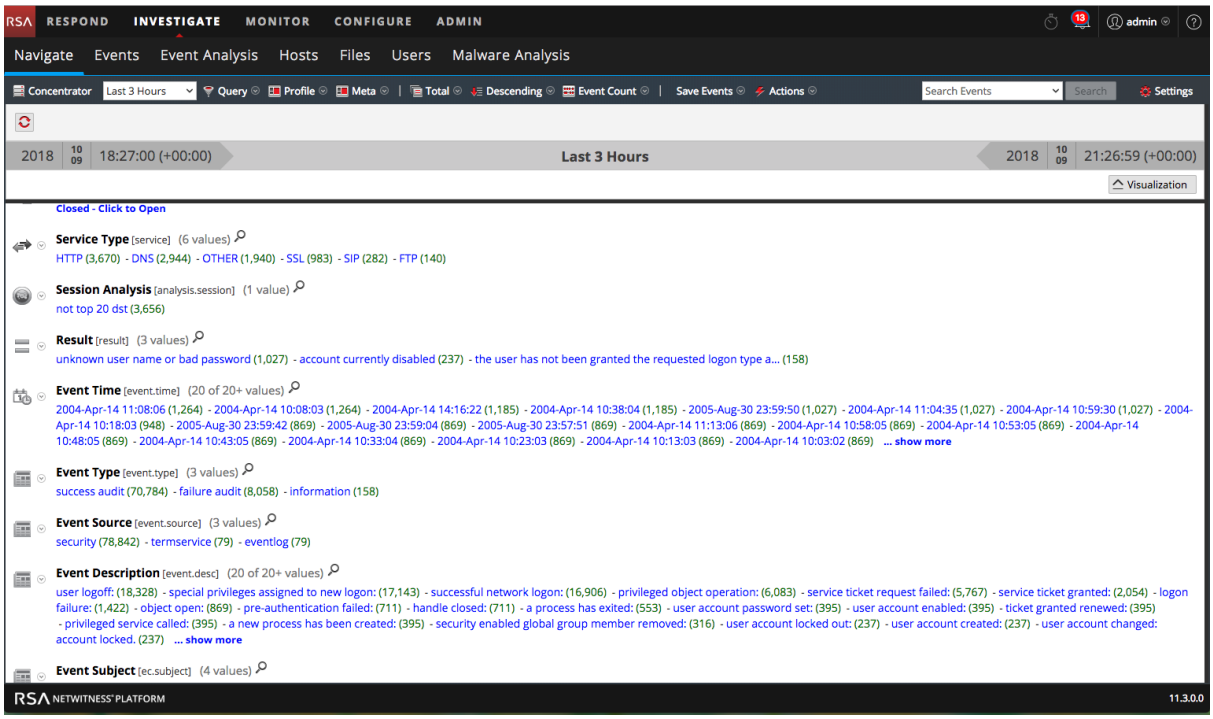
2. Reconstruct an event (see Reconstruct an Event) or view the interactive Event Analysis of an event (see Begin an Investigation in the Event Analysis View).

Begin an Investigation (No Default Service)

1. Go to **INVESTIGATE > Navigate** or **Events**.
   The Investigate dialog is displayed.



2. Double-click a service or select a service, usually a Concentrator, and click **Navigate**.
   The data loads automatically in the Events view. If you are working in the Navigate view, the resulting panel displays the activity for the selected service, but the data is not loaded automatically.
3. (Recommended) Select a specific time range so that results load faster.
4. If you want to modify investigation options before loading, you can create or modify a custom profile, apply a different time range, create or apply a meta group, and perform a custom query as described in Querying and Acting on Data in the Navigate and Events Views. You can also modify options at any time during the investigation.
5. To load data in the Navigate view, click Load Values.
   The data for the selected service begins loading.

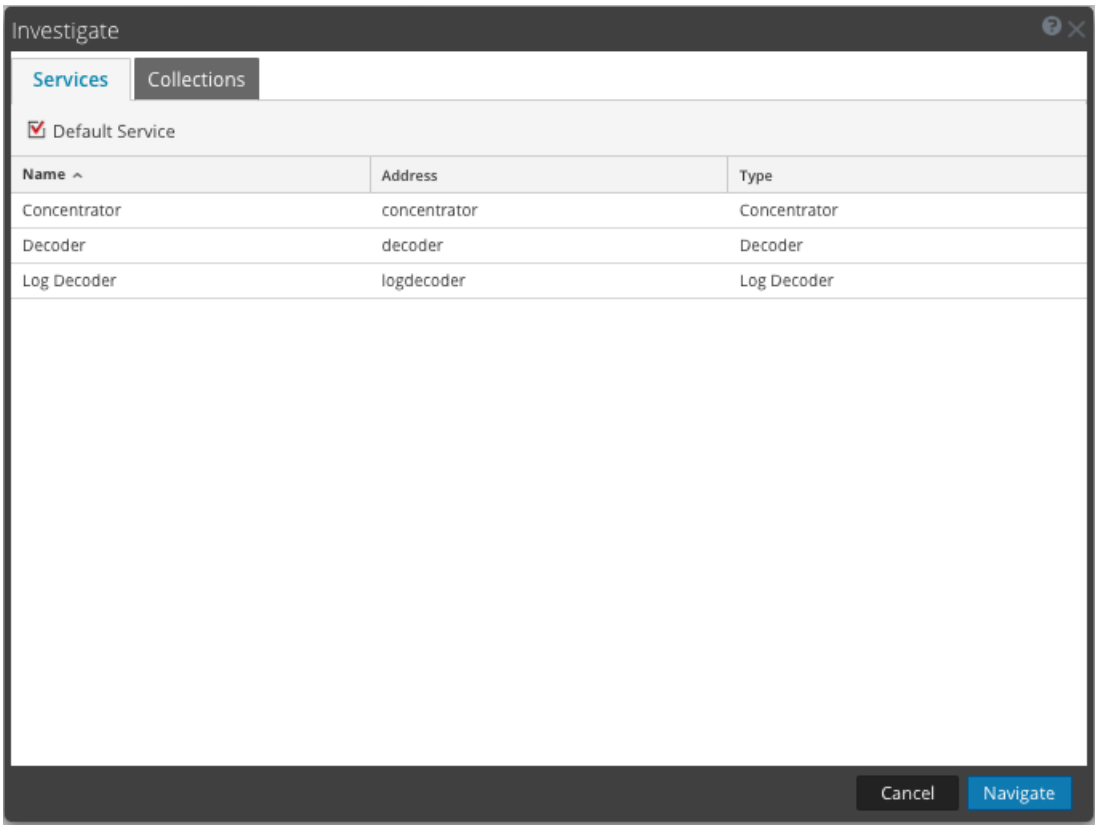


With the service selected and data loaded, you are ready to begin analyzing the data.

Set or Clear the Default Service

You can set the default service and clear the default service in the Investigate a Service dialog.

1. Click the service name in the toolbar.
   The Investigate dialog is displayed.



2. Select a service on the **Services** grid, and click Default Service.
   The service becomes the default, (indicated by **Default** in parentheses after the service name).

3. To clear the default service, select the default service in the grid, click Default Service, and click **Cancel** to close the dialog.
   No default service is set.

> **Note:** Clicking cancel does not cancel your selection of the default service. It closes the dialog without navigating to the currently selected service in the grid. Setting a default service that is different from the service currently being investigated, does not refresh the Navigate view. You must explicitly select and navigate to a different service.

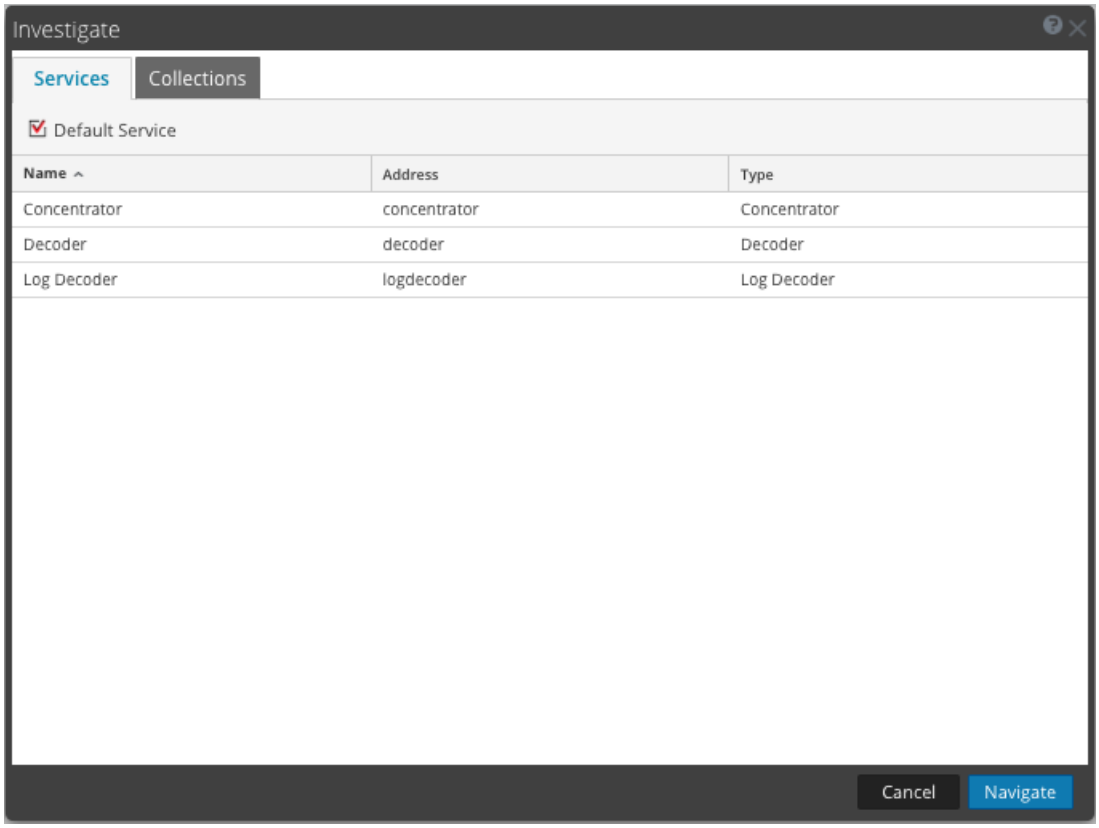
Begin an Investigation (Default Service Specified)

1. Go to **INVESTIGATE > Navigate** or **Events**.
   If the Autoload Values setting is set to off, the Navigate view is displayed with the default service selected, and ready to load data. If the Autoload Values setting is on, the values are loaded as shown in Step 3. In the Events view, the data is loaded automatically.
2. If you want to modify investigation options in the Navigate view before loading, you can create or modify a custom profile, apply a different time range, create or apply a meta group, and perform a custom query.

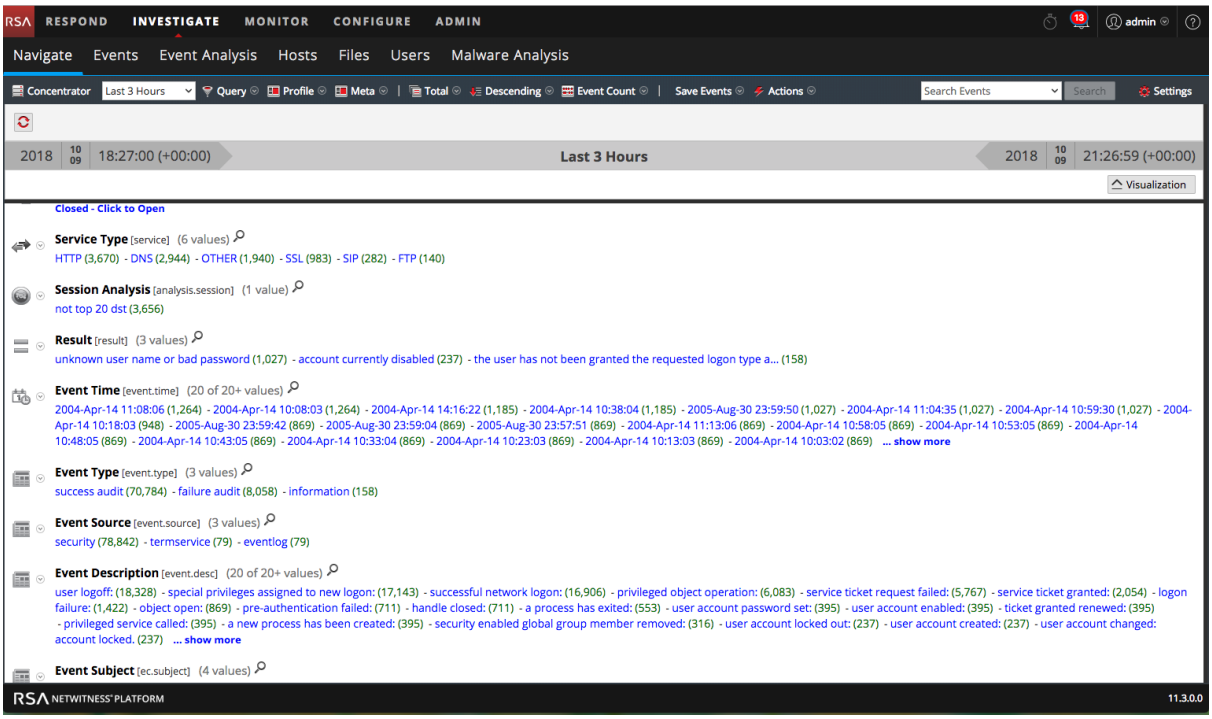
3. When ready, click Load Values.
   The values for the service are loaded in accordance with the selected options. With the service selected and data loaded you are ready to begin analyzing the data.

Change the Service or Collection to Investigate

1. In the Navigate view or the Events view, click the service name at the top of the options panel.
   The Investigate dialog is displayed.



2. Double-click a service or select a service and click **Navigate**. The resulting panel displays the activity for the selected service.
   If the Autoload Values setting is on, the values are loaded as shown in Step 3. Otherwise, the Navigate view is displayed with the default service selected, and data ready to load. In the Events view the data is loaded automatically.
3. When ready, click Load Values.
   The values for the service begin loading in accordance with the selected options.



With the service selected and data loaded you are ready to begin analyzing the data.

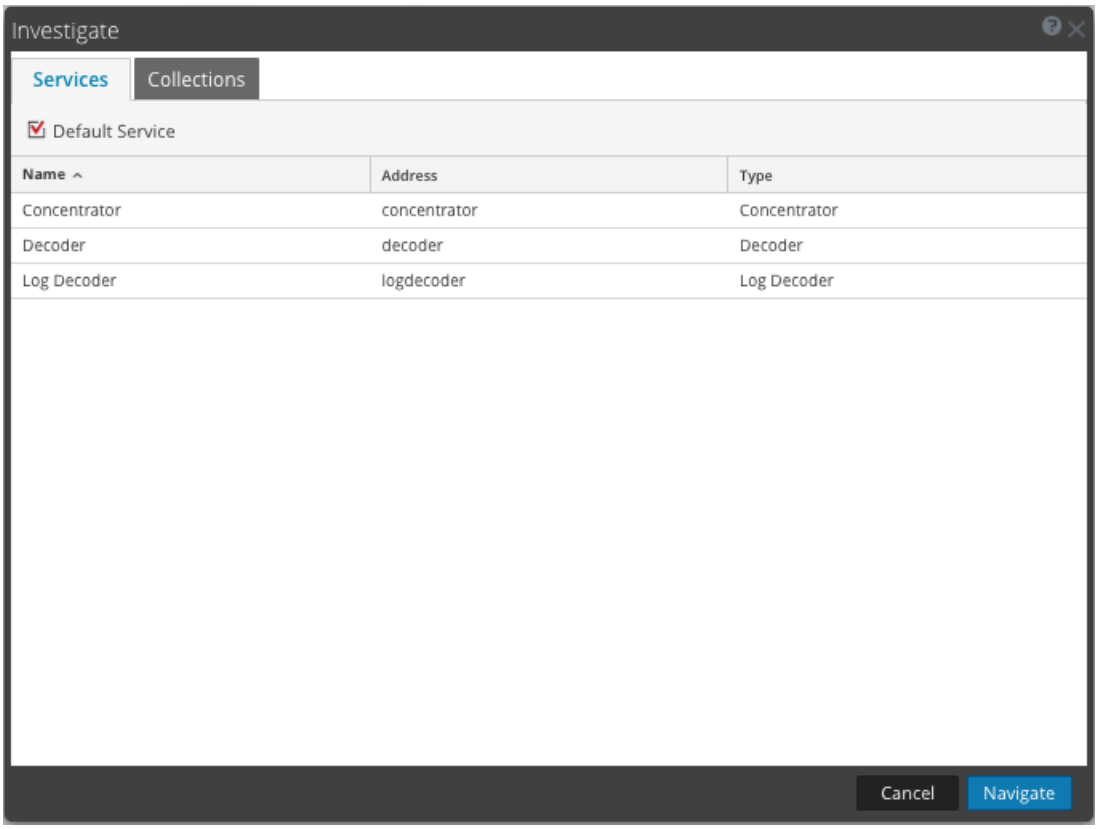
Investigate Workbench Restoration Collections

This procedure enables administrators to select content from an existing collection to reprocess for further investigation. This applies to Decoders that use Workbench services.

Note: Only a user with administrative privileges can create a collection, and you can view only those collections that you created.

To reprocess data for further investigation:

1. Go to **INVESTIGATE > Navigate** or **Events**.
   The Investigate dialog is displayed.



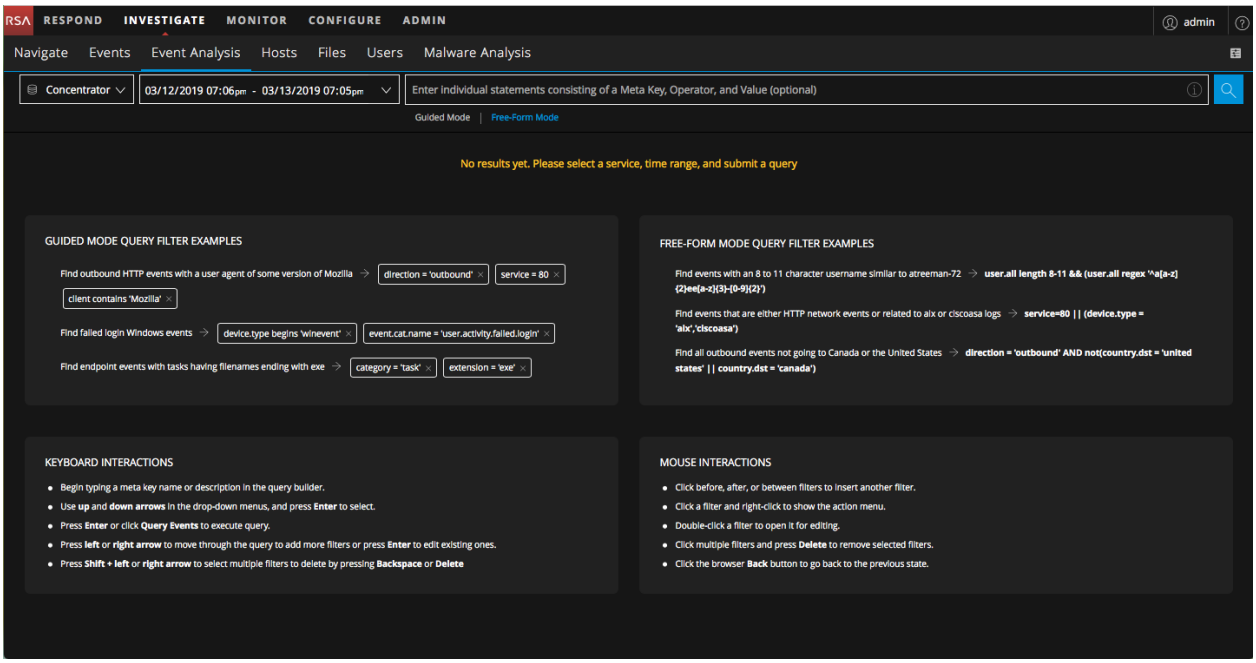
2. Select a workbench service and workbench name that you want to investigate.
3. Click **Navigate** to perform an investigation on your selected workbench service.
   Click **Cancel** to select a different workbench service to investigate.
   The Investigation view is displayed. With the collection selected and data loaded you are ready to begin analyzing the data.

Begin an Investigation in the Event Analysis View

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

The Event Analysis view offers most of the features that are available in both the Navigate view and the Events view. Similar to the Navigate view, there is a view into meta keys and meta values for logs, endpoints, and packets. Like the Events view, an events list shows events listed in the order by time, and you can view the raw event, related meta data, and a reconstruction of an event. The Event Analysis reconstruction has some helpful cues to identify points of interest in a reconstruction. See Analyzing Raw Events and Metadata in the Event Analysis View

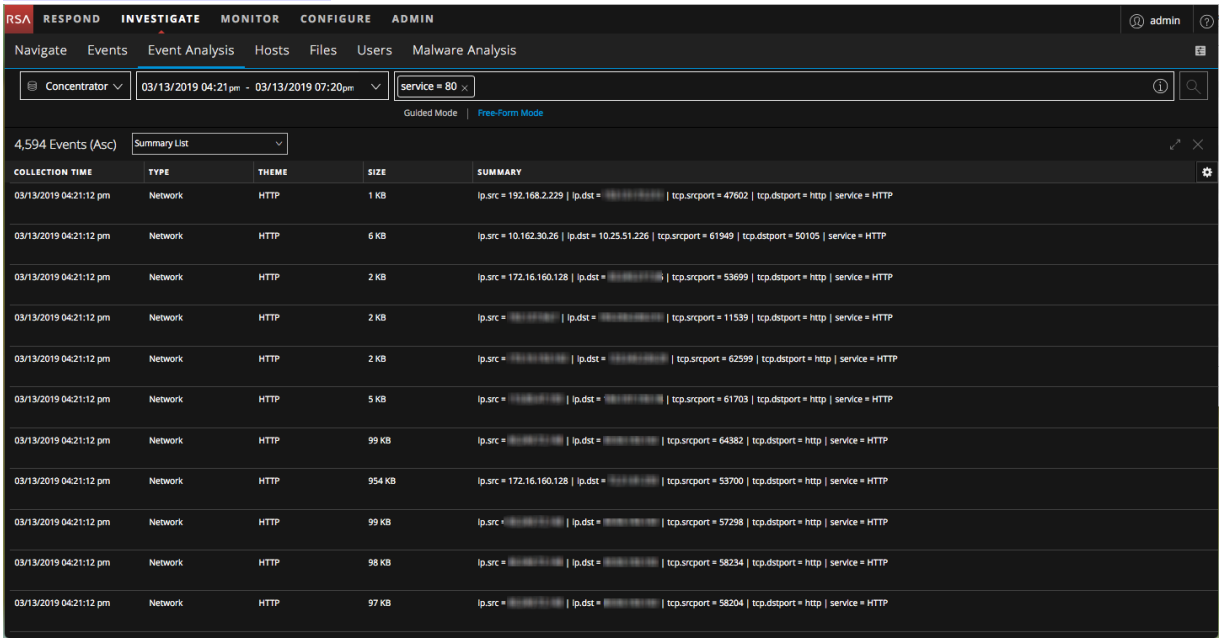
The following figure shows the initial Event Analysis view with a section that provides examples of queries.



Access the Event Analysis View (Version 11.1 and Later)

Several ways to access the Event Analysis view are available in Version 11.1.

- Use the **Actions > Go to event in Event Analysis** option in the Navigate view, and enter an event ID. The Event Analysis view opens the single event as a reconstruction. You can begin working as described in Analyzing Raw Events and Metadata in the Event Analysis View.
- Hover over a count (the green number after a meta value) in the Navigate view and Control-click **Open Event Analysis in new tab**. The Event Analysis view opens with the list of events for the selected drill point, and you can begin working as described in Analyzing Raw Events and Metadata in the Event Analysis View. The following figure is an example of the list of events.

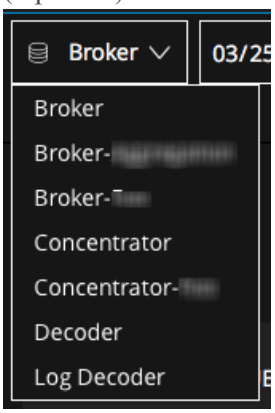


- Go to **INVESTIGATE > Event Analysis** or select the **INVESTIGATE** option in the main menu if you have made the Event Analysis view your opening Investigate view. The following procedure provides detailed steps.

To begin an investigation in the Event Analysis view using direct access:

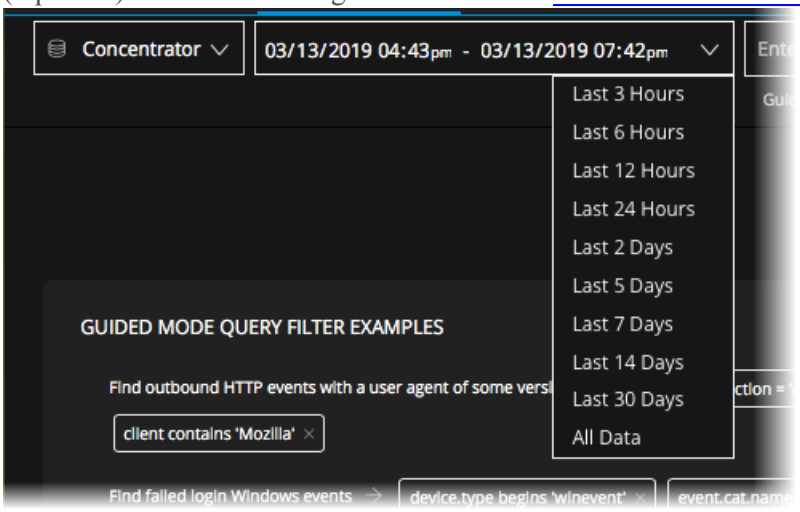
1. Go to **INVESTIGATE** > **Event Analysis**.
   The Event Analysis view opens with a service selected and no data displayed. A drop-down list offers a list of available services in alphabetical order. The **Select a service** field is populated with the first service in the list or the most recently selected service. By default the list of available services is retrieved every twelve hours and cached on the NetWitness server. If a service is added or removed from the NetWitness server before the next time to retrieve, the cache is updated with the latest list of services. An icon provides the status of the service.
   - and selected service name= the service is selected.
   - = Investigate is attempting to connect to the selected service.
   - = There was an error connecting to the selected service or there is no data in the selected service. In this state, the service selector control also turns red, and a tooltip explains why the connection attempt failed and advises you to choose another service.

2. (Optional) Select a service, usually a Broker or Concentrator, from the drop-down list.



The time range selector shows either the default time range of 24 hours, or the time range that you last selected for this service. The or Query Events button becomes active and you can create filters. If you launch a query without creating filters, the selected time is used.

3. (Optional) Edit the time range as described in Filter Results in the Event Analysis View.



The selected time range is stored in your browser for this service; you can set different time ranges for different services.

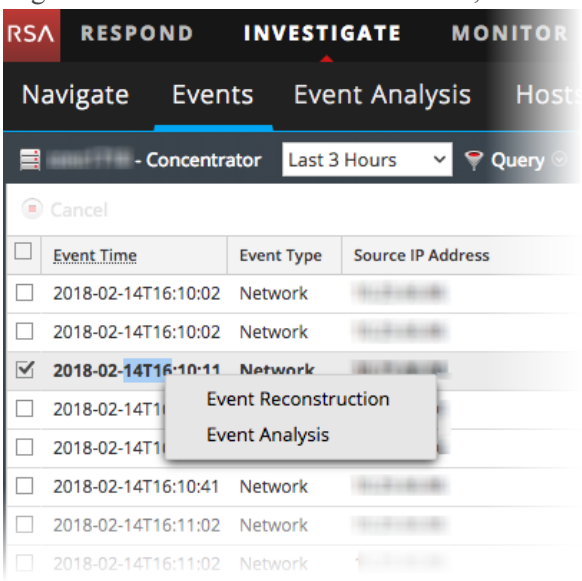
4. Create a query that consists of one or more filters that contain a meta key, operator, and optional value. See Filter Results in the Event Analysis View for details on creating queries.

5. When ready to submit the query, click or **Query Events**.
The Event Analysis view displays the data for the selected service, time range, and query, in accordance with permissions assigned to your role by the administrator. You are ready to begin analyzing the data. Refer to Analyzing Raw Events and Metadata in the Event Analysis View to learn how to work in the Event Analysis view.

Access the Event Analysis View (Version 11.0)

To open an event in the Event Analysis view:

1. Go to **INVESTIGATE** > **Events**.
2. Do one of the following:
   a. Right-click an event in the listed events, and select **Event Analysis**.



   b. Right-click an event in the listed events and select **Event Reconstruction**. Then click the **Event Analysis** button in the reconstruction.

Refer to Analyzing Raw Events and Metadata in the Event Analysis View to learn how to work in the Event Analysis view.

Investigating Metadata in the Navigate View

When conducting an investigation in the Navigate view, analysts have multiple methods, specific to the Navigate view, to refine the results, visualize data, and act on data.

- Filter Results in the Navigate View
- Manage Meta Groups
- Visualize Metadata as Parallel Coordinates
- Open an Event in the Events List
- Export or Print a Drill Point
- Launch an External Lookup of a Meta Key
- Launch a Malware Analysis Scan from the Navigate View
- Visualize the Current Drill Point in Informer

In addition, you can use these methods of querying data and acting on results that are common to the Navigate view and the Events view.

- Use Profiles to Encapsulate Common Areas for Investigation
- Search for Text Patterns
- Create a Custom Query
- View and Modify Queries Using URL Integration
- Manage Context Hub Lists and List Values in the Navigate and Events Views
- Look Up Additional Context for a Data Point
- Reconstruct an Event

Filter Results in the Navigate View

When conducting an investigation in the Navigate view, there are several methods available to refine the results displayed when meta key values are loaded in the Navigate view. The rest of this topic is focused on the basic methods of filtering data:

- Set the Time Range
- Set the Quantification Method and Sort Sequence of Meta Key Results
- Manage and Apply Default Meta Keys in an Investigation
- Drill into Data in the Navigate View Time Chart
- Drill into Data in the Values Panel

If you don't know where to begin, you can use built-in meta groups and profiles to investigate groups of meta keys that are tuned to a specific area of investigation. For example, you can select a profile to look into meta keys commonly associated with email or web activity. A separate topic describes each of these methods.

- Use Profiles to Encapsulate Common Areas for Investigation
- Manage Meta Groups
- Visualize Metadata as Parallel Coordinates

Set the Time Range

When conducting an investigation in the Navigate view, the time range options limit the results returned. You can select:

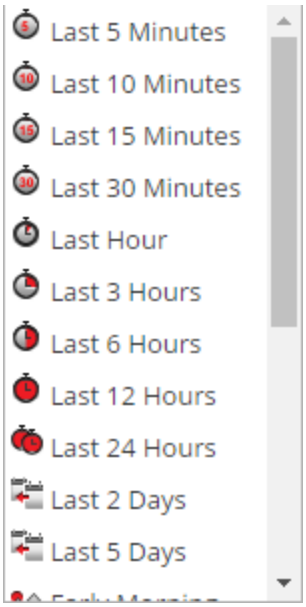
- A time range relative to the collection. Ranges relative to the collection are based on the last collection time for data.
- A time range relative to the calendar.
- A custom date range.
- All data.

The selected Date Range is shown in the Navigate view tool bar as the Time Range label. By default the label is **Last 3 Hours**. The Time Range displayed in the timeline banner shows the first and last timestamp for the date range being used for the metadata.

Note: Time range is based on the Time Zone configured in the Profile Preferences panel as described in "Setting User Preferences" in the *RSA NetWitness PlatformGetting Started Guide*.

To select a built-in time range:

1. Click the **Time Range** option in the Navigate view toolbar. The default time range is for the **Last 3 Hours**, but a different value from the selection list, for example, **All Data** or **Last Hour,** may already be selected and used as the label in the options panel.
   The Time Range selection list is displayed.



2. Do one of the following:
   - If you want to see all data, select **All Data**.
   - If you want to set a time range in minutes, hours, or days that is relative to the collection, select a value such as **Last 10 minutes**, **Last 3 Hours**, or **Last 5 days**.
   - If you want to set a time range relative to today, select **Yesterday**, **This Week**(Version 11.1), **Last Week** (Version 11.1), **All Day**, or a part of the day such as **Early Morning**, **Morning**, **Afternoon**, or **Evening**.
   - If you want to set a unique date range, select **Custom** in the **Time Range** menu and follow the procedure below.
     The selected time range is applied to the current results in the Values panel.

To specify a custom time range:

1. Select **Custom** in the **Time Range** menu.
   Date selection options are displayed in the toolbar.

2. Within the time **Start Date** and **End Date** fields, do the following to specify the date and time:
   a. Click a date from the calendar.
   b. (Optional) Select the time from the Hour and minute fields or click **Now**. The time selection defaults to the current time of day.

Note: The value for start time in seconds always defaults to :00, and the value for end time in seconds always defaults to :59. For example, if you are using time to drill down into an issue, the drill time is interpreted as "HH:MM:00 - HH:MM:59."

3. To apply the range, click **Go**.
   The selected time range is applied to the current results in the Values panel.

Set the Quantification Method and Sort Sequence of Meta Key Results

You can select the way results for each meta key are quantified and sequenced in the Navigate view.

Note: If meta entities (Version 11.1 and later) are used in meta groups, the results will show the top 20 values that matched any of the meta keys contained in the meta entity.

Each meta key section in the Navigate view contains an ordered list of values showing each meta key value (Value) and its count (Total). You can specify whether:

- The results in each meta key section are sorted based on Value or Total.
- The results are sorted in ascending or descending order.
- The values shown for each meta key are quantified by number of packets (Packet Count), number of sessions or logs (Quantify by Event Count) or by the size of events (Quantify by Event Size).

Note: If you have both a log decoder and a packet decoder for which you are viewing the metadata, the calculation of what is actually being counted is dependent on the type of key. If you select to Quantify by Packet Count and are looking at logs, the Navigate view output is the same output as if you had selected Quantify by Event Count (see Navigate View for details).

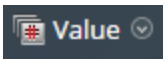
This image shows the `Event Type` meta key presented in order by **Total** in **Descending** order. The value with the greatest count of matches is presented first. The value `failure audit` has 71 matches and is listed first. The value `logon` has only one match and is presented last. The quantification method is **Event Count**.

This image shows the `Event Type` meta keys presented in order by **Value** in **Descending** order. The value names are presented in alphabetical order starting at the end of the alphabet. The value `success audit` is listed first. The value `connect` is presented last. The quantification method is **Event Count**.

To select the quantification method of meta key count and ordering of meta key results displayed in the Navigate view:

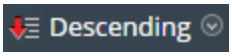
1. In the toolbar, select **Event Count**, **Event Size**, or **Packet Count** and choose one of the quantification options in the drop-down menu. The label for the menu displays the selected option.

   The current view is reloaded according to your selection.
2. In the toolbar, select **Total** or **Value** and choose one of the ordering methods in the drop-down menu. The label for the menu displays the selected option.



The current view is reloaded according to your selection.

3. In the toolbar, select **Ascending** or **Descending** and choose one of the sort order options in the drop-down menu. The label for the menu displays the selected option.
   The current view is reloaded according to your selection.



Manage and Apply Default Meta Keys in an Investigation

When analysts are conducting an investigation of captured data in Investigate, a default set of meta keys is loaded and displayed in a default sequence in the Navigate view > Values panel. The default content and sequence is based on the meta keys for the service being investigated. Analysts can specify the meta keys to display during navigation by selecting the default meta keys or by selecting a user-defined group of meta keys, which provides great flexibility to define meta keys. This can help to drill down more directly to the desired data and to reduce the load time by preventing the loading of meta that is not of interest in the current investigation.

Note: In Version 11.1 and later, wherever meta keys are used, you can also use configured meta entities.

If no custom meta groups are in effect, the Navigate view is displayed with the meta key visibility specified in the Default Meta Keys dialog. To optimize loading of meta keys in the Navigate view > Values panel, NetWitness Platform does not open non-indexed meta keys by default. When you open a non-indexed meta key in the Values view, NetWitness Platform begins loading values for that meta key. If the load time is excessive, the load of the meta key times out with a message. Title, values, and counts for non-indexed meta keys are not drillable in the Values panel. Additional labeling in Investigation identifies the non-indexed meta keys.

To select the meta keys to apply to your investigation, you can:

- Select the default meta keys.
- Select a set of meta keys, called a meta group.

Note: Investigate has built-in meta groups and user-defined meta groups. Once created, user-defined meta groups can be edited, deleted, exported for use on other services, and imported to the service you are investigating. All of these procedures are provided in a separate topic: Manage Meta Groups.

The Default Meta Keys dialog allows you to specify the default view and display sequence for meta keys during navigation in the Investigate > Navigate view for a specific service. For each key or for all keys, you can set the default view to:

- Hidden: Results for default meta key are hidden and are not available to load.
- Open: Results for default meta key are open with all values and counts displayed.
- Close: Results for default meta key are closed with only the meta name visible.
- Auto: The loading of default meta keys is controlled by the index level, which must be Indexed By Value.

When using the default meta keys, be aware that these can be modified for different services, and you may not be seeing the same set of default meta keys when navigating to a drill point on different services. If you do not see the expected data, you may need to change the initial view of the default meta keys.

When you change the initial state of default meta keys from within the Navigate view, the change persists for that service. When new keys are added to the custom index file for a Core service (for example, `concentrator-custom-index.xml` or `decoder-custom-index.xml`), the new keys are added to the default meta keys list. The changes made in the Navigate view apply only to the current service.

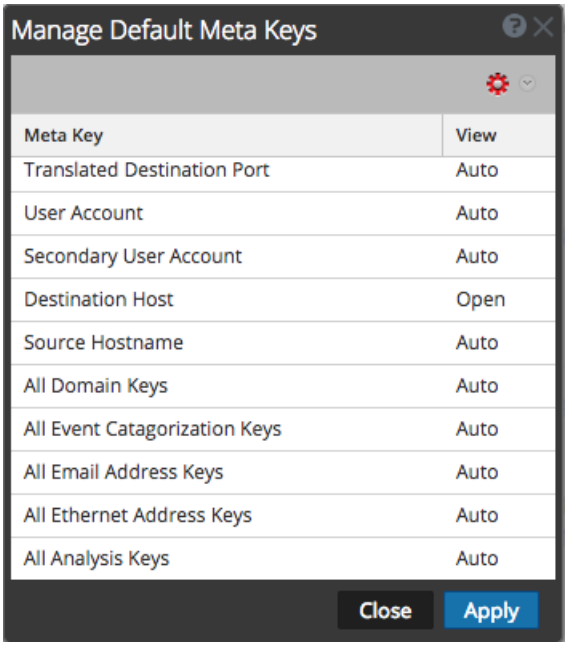
To specify that the initial Navigate view opens using default meta keys:

1. Go to **INVESTIGATE** > **Navigate**.
2. Select a service and select **Navigate**.
3. In the **Meta** menu, select **Use Default Meta Keys**.
   If an investigation is already in progress, the data is reloaded in the current view and an icon highlights the selected option. If no data is loaded yet, the default meta keys are used for the next load.

Configure Default Meta Keys

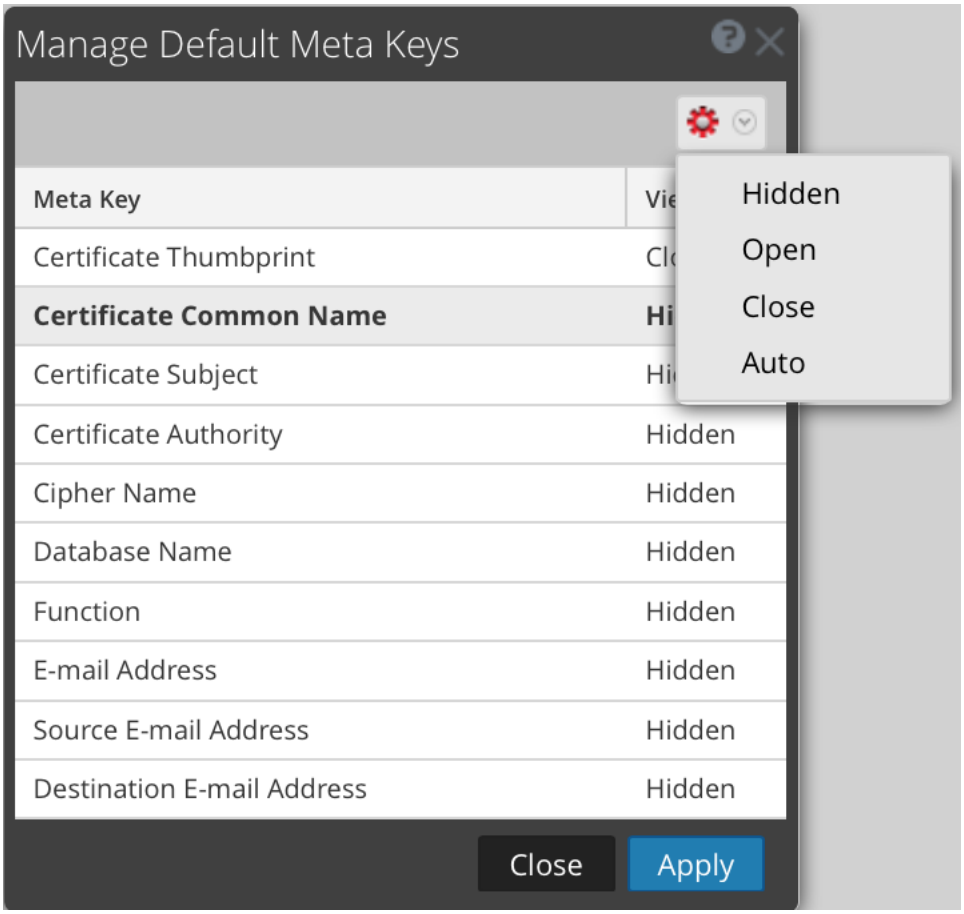
To configure the default view of default meta keys in the Navigate view:

1. In the **Navigate** view toolbar, select **Meta** > **Manage Default Meta Keys**.
   The Manage Default Meta Keys dialog is displayed with the list of available meta keys for the service.



2. (Optional) To change the order of the keys, select one or more keys, and drag the values up or down through the list of keys.

3. Do one of the following:
   - (Optional) To change the default view for all meta keys, make sure that no keys are selected and in the toolbar, select .
   - (Optional) To change the default view for one or more keys, select the keys and in the toolbar, select .
     A drop-down menu of possible initial views for all default meta keys is displayed.



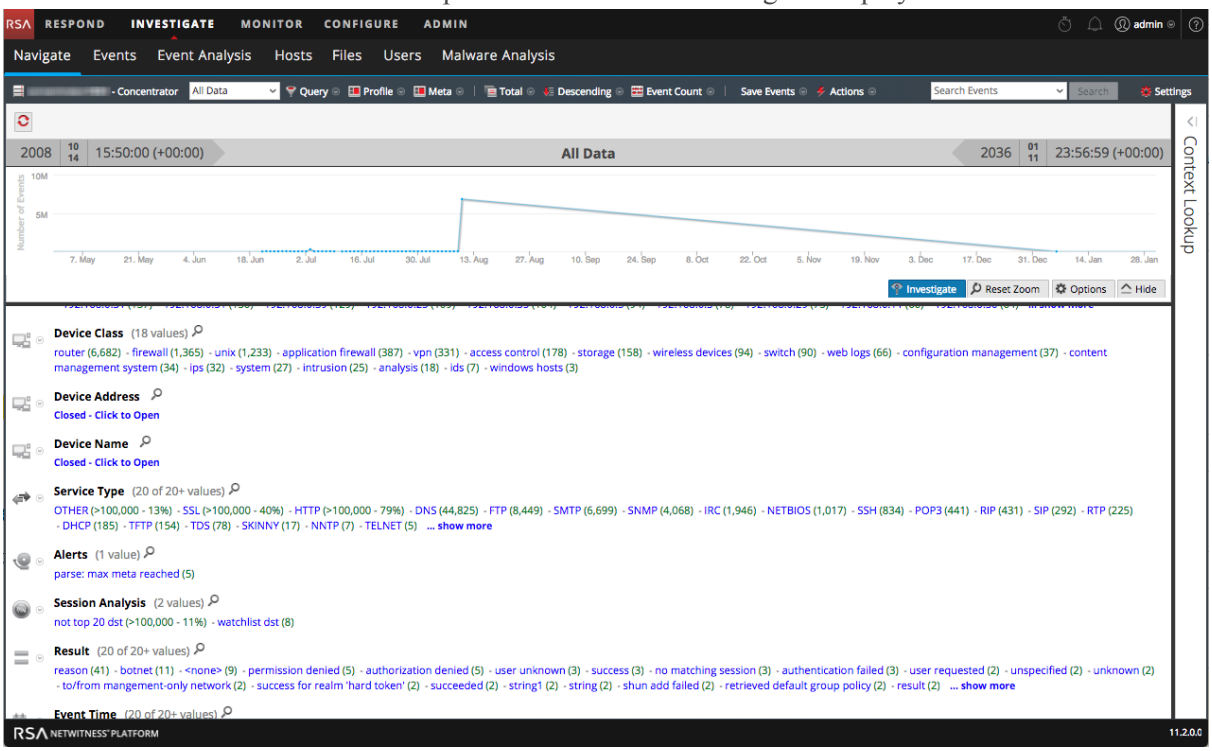
   - (Optional) To revert to the default view for meta keys as specified in the service index file, make sure that no keys are selected and in the toolbar, select > **Auto**.
     When you modify the default view for a non-indexed meta key, you cannot set the key to OPEN. If you change the default view for a group of meta keys to OPEN and some of the meta keys are non-indexed, the non-indexed meta keys revert to AUTO. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are CLOSED until opened manually.
4. Select one of the views.
5. To save the changes, click **Apply**.
   The meta keys displayed in the Navigate view are set to your specifications. If the default meta keys are hidden, values for the meta keys are not shown in the investigation at all. If the default meta keys

are closed, the values for the meta keys are not loaded by default, but you can load individual meta keys manually in the Navigate view.

Drill into Data in the Navigate View Time Chart

The Time Chart visualization allows analysts to visualize activity over time. You can zoom into the data by selecting a time window then selecting the Investigate option. You can then reset the navigation to the time range that was in effect before zooming.

1. Go to **INVESTIGATE > Navigate**.
   The Time Chart for the current drill point and selected time range is displayed.



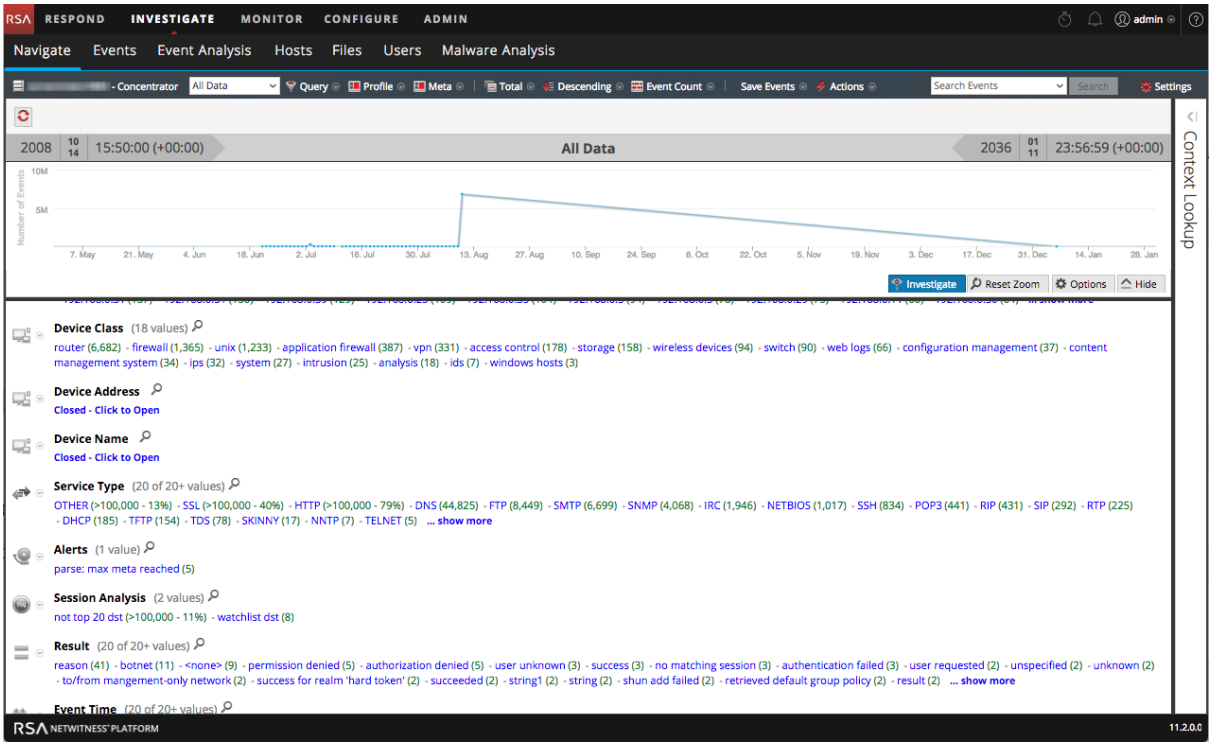
2. To highlight a period of time on the Time Chart, click over the desired time period and drag the mouse.
   The Time Chart is redrawn for the selected time range; however, the meta values are unchanged.
3. To drill into the data for the selected time range, click **Investigate**.
   The URL is updated to reflect the time range override, and the Investigation options panel is updated to reflect the custom time range. The Time Chart is redrawn and the meta values are loaded for the selected time range.
4. To reset the Time Chart to the original time range, click **Reset Zoom**.
   The URL is updated to reflect the original URL prior to zooming into the data, and the Investigation options panel is updated to reflect the time range selected before zoom. The Time Chart is redrawn for the selected time range and the meta values are loaded for that time range.

Drill into Data in the Values Panel

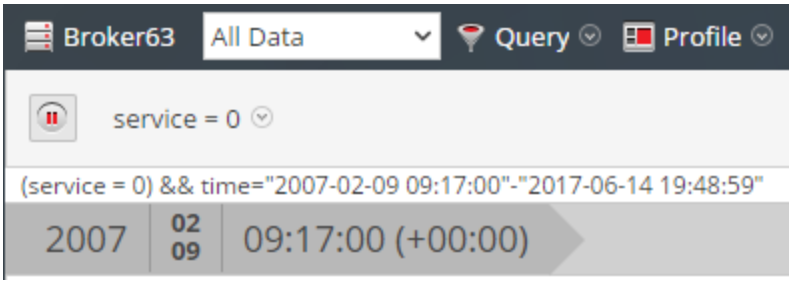
NetWitness Platform displays the activity and values for the selected service in the Investigation > Navigate view. To investigate data, analysts drill into data by clicking on a meta key or a meta value, which is treaty as a query. In the Values panel, each query is added to the breadcrumb data in the Values panel. This results in a breadcrumb at the top with a crumb for each query. You can edit the breadcrumb to insert or remove a query.

To drill into a subset of the metadata:

1. Begin an investigation so that metadata is displayed in the Navigate view.

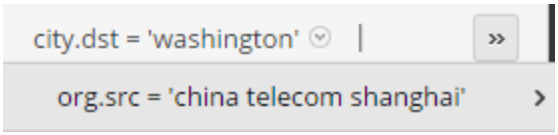


2. To drill down into the metadata, do any combination of the following:
   a. Click a **meta key**, for example, **Service Type**.
   b. Click a **meta value**, the blue text in the results. For example, **OTHER**.
      Each time you click a meta key or meta value, the investigation query pivots to a narrowed focal point, or drill point, in the data. At each drill point, the Values panel is updated and the new drill point is displayed in the breadcrumb. Below is an example of the first breadcrumb.



      This is an example of a long breadcrumb that does not fit in the toolbar. The last query that fits is

followed by a drop-down menu that lists additional queries. To select a drill point within the overflow, click the overflow icon and a query in the drop-down list.

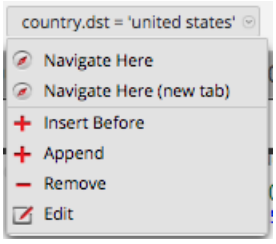


To add a query in the breadcrumb:

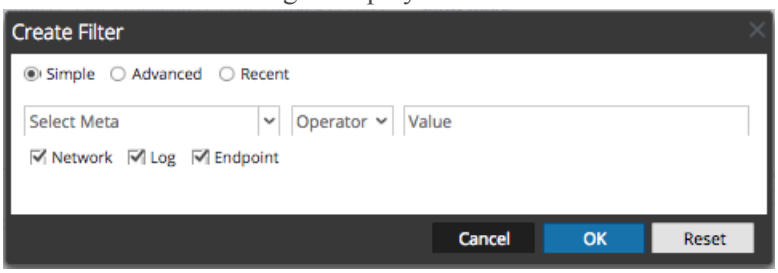
In the breadcrumb, you can click any of the crumbs to display the Query menu. You can insert a new query before a crumb, and append a new query to the end of breadcrumb. After each edit in the breadcrumb, NetWitness Platform refreshes the results.

To add a query in the breadcrumb:

1. Click a crumb.
   The Breadcrumb menu is displayed.



2. To add a query in the breadcrumb, select **Append** or **Insert Before**.
   The Create Filter dialog is displayed.



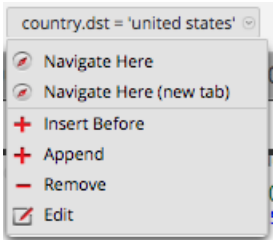
3. Create the Query as described in Create a Custom Query.

To edit a query in the breadcrumb:

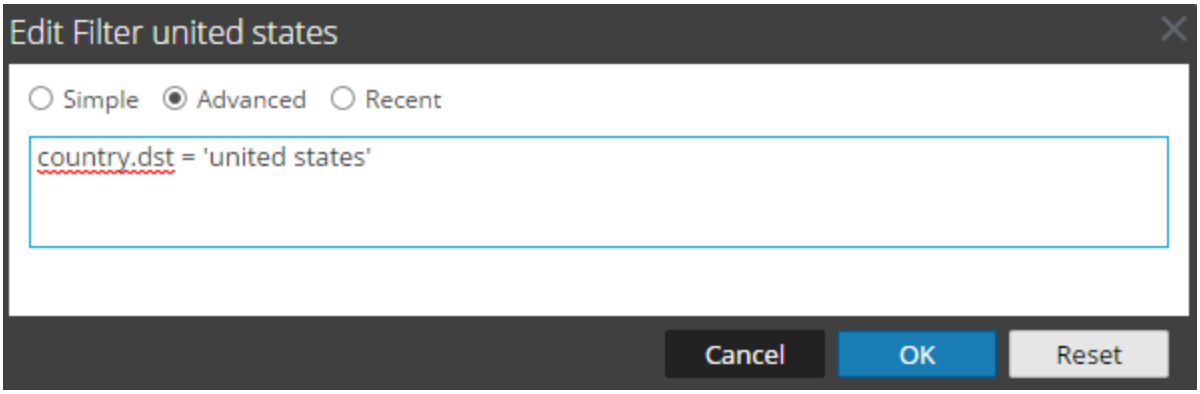
In the breadcrumb, you can click any of the crumbs to display the Query menu. You can delete a crumb and edit a query in a crumb. After each edit in the breadcrumb, NetWitness Platform refreshes the results.

To work with queries in the breadcrumb:

1. Click a crumb.
   The Breadcrumb menu is displayed.



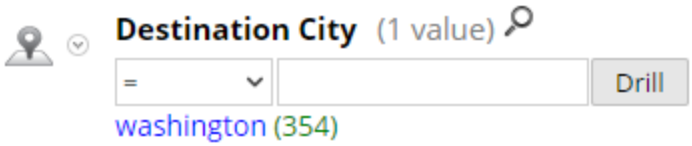
2. To edit a query in the breadcrumb, select **Edit**.
   The Create dialog is displayed with the selected query open for editing.



3. Edit the fields as described in Create a Custom Query.

To quick search within a meta key:

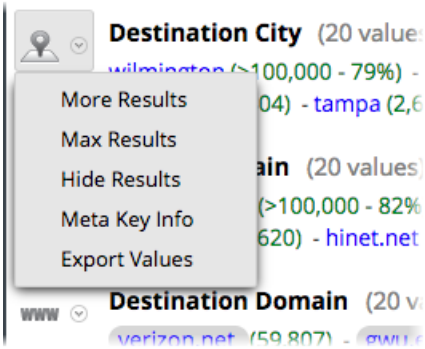
1. Move the mouse over a meta key section and click the magnifying glass.
   The Quick Search form, which contains a comparator and an optional operand for the search, is displayed.



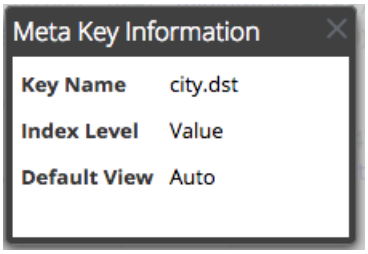
2. (Optional) If you want to close the search form, click the magnifying glass again.
3. Select the operation from the drop-down list on the left and type the text value to search for. Then click **Drill** to perform the execution.
   The metadata for that meta key is used to drill down in the current metadata.

To view meta key information and copy meta values for a meta key:

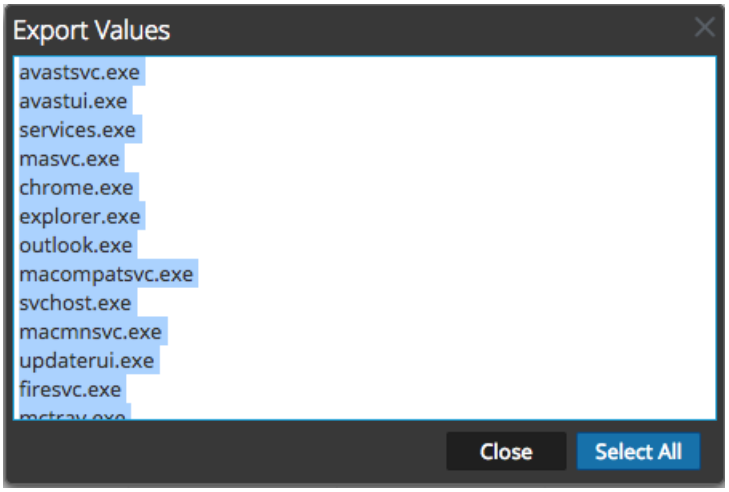
1. To view the key name, index level set for displaying the meta key, and the default view set for the meta key, click the drop-down menu next to the meta key. This figure shows the drop-down menu for Version 11.1 and later.



2. Select **Meta Key Info**.
   The Meta Key Info dialog is displayed.

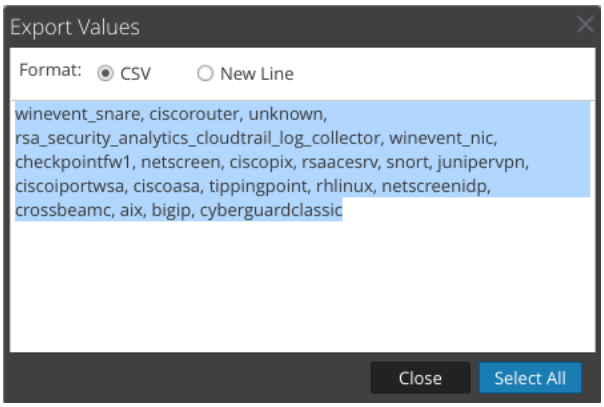


3. When finished viewing, click ■.
4. (Optional for Version 11.1 and later) To view meta values found for a meta key in a simple list that you can copy, click the drop-down menu next to the meta key.
   The Export Values dialog is displayed.
   The Version 11.1 dialog displays a list of values with one value per line.



   The Version 11.3 dialog allows you to select the method of separating values: either New Line or

CSV.



5. Select the values that you want to copy, and click **Export Values**.
   The values are copied to the local clipboard and you can paste them into a file to save or share them.
6. To close the dialog, click **Close**.
7. (Optional) If you want to hide the results for the meta key in the current drill point, click the drop-down menu next to the meta key and click **Hide Results**.

To display events associated with a meta value:

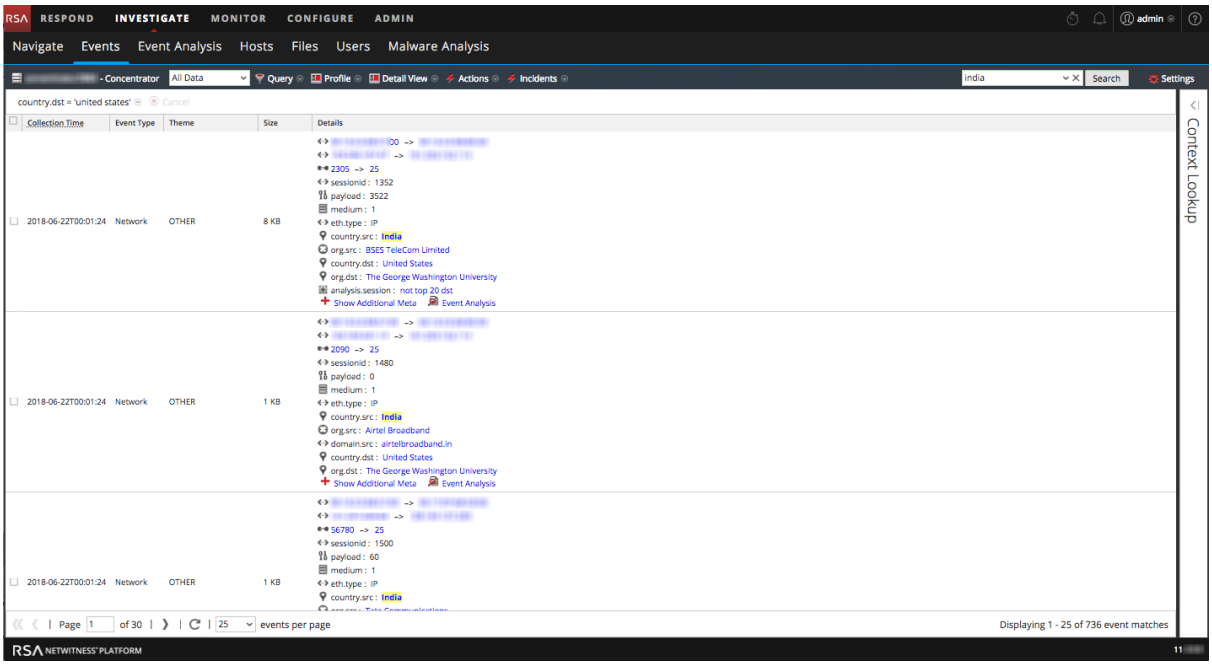
The Events view provides additional details for an event in two different views: Events List and Detail View.

1. In the Navigate view, drill into metadata that is the focus of your investigation.
2. Click the count (the number in green) next to a blue meta value.
   The Events view corresponding to the current drill point is displayed.
   The operations that you can perform in the events view are described in Examining Raw Events in the Events View.

To search for specific events associated with a meta value:

1. In the Navigate view, drill into metadata that is the focus of your investigation (click a meta value or add a query).
2. Type a search string in the Search box and press **Enter** or click **Search**.
   You can also select and set search mode preferences. See Search for Text Patterns for detailed search information.
   The Events view opens in a new tab and shows the search results. If you do not see the search term highlighted, click **Show Additional Meta**. Your time range selection and drills (queries) carry

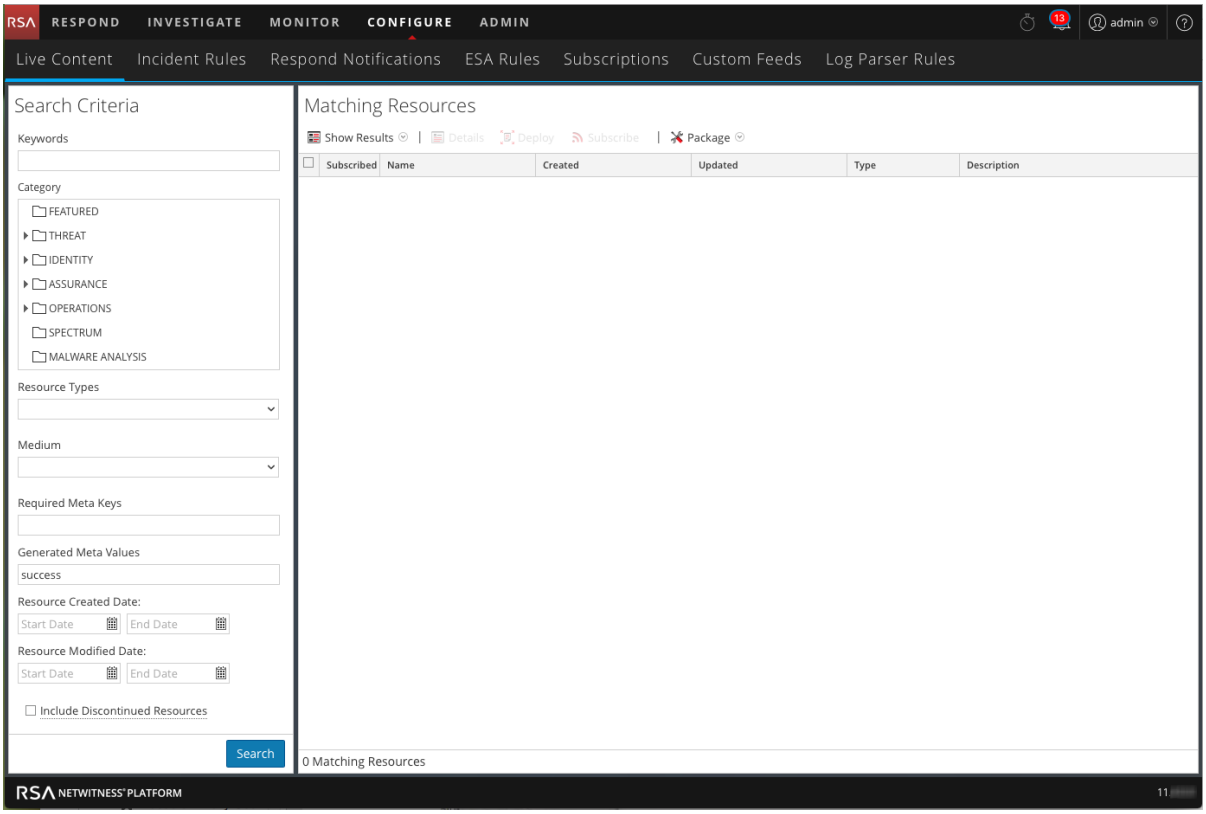
forward to the Events view.



To view a selected meta value in RSA Live:

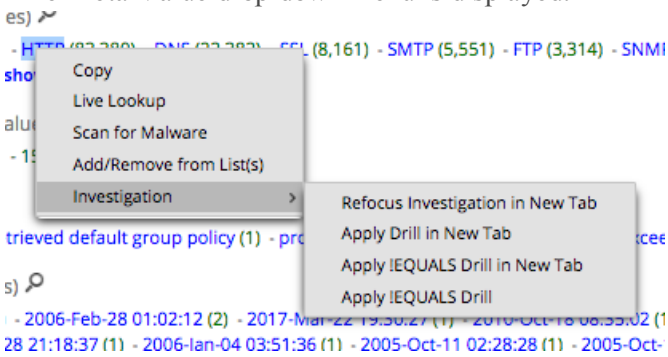
1. In the Navigate view, drill into metadata that is the focus of your investigation.
2. Right-click a meta value (the text in blue).
   The Meta Value drop-down menu is displayed.
3. To look up the meta value in RSA Live, select **Live Lookup**.
   The Live Search view is displayed with the meta value entered in the Generated Meta Value(s)

field, and ready for a search.



To refocus the investigation in a drill point:

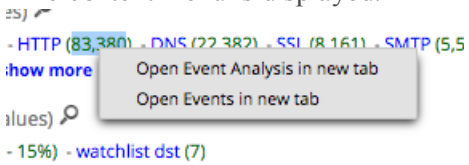
1. Right-click a meta value (the text in blue).
   The Meta Value drop-down menu is displayed.



2. Choose one of the refocus options.
   The drill is refocused according to your choice.

To look at a specific count in a new tab:

To view a count for a meta value in the Events view or the Event Analysis view, right-click a count for a meta value (the green number following the blue meta value).
The context menu is displayed.



Manage Meta Groups

A meta group combines selected meta keys and meta entities into a group to show only data in which the meta keys and meta entities were found. In the Navigate view, you can use meta groups to filter data displayed in the Values panel. A fresh installation of NetWitness Platform includes out-of-the-box (OOTB) meta groups to help you find interesting data sets in Investigate. The OOTB meta group names are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted. You can create your own groups, and you can duplicate and edit an OOTB group to create a custom group.

With a meta group in effect during an investigation, the information in the Values panel shows only the meta keys in the selected group. When you open a Parallel Coordinates visualization, the meta keys and meta entities in a group appear as axes from left to right. It may be useful to create two versions of each custom meta group; one for analysis of meta values and one for creating a parallel coordinates chart focusing on a smaller subset of the same use case.

Custom meta groups are visible to all users of a service and may be exported for import to any service, limited by the available meta keys for that service.

Note: When an administrator adds custom meta groups manually by editing the custom index file for a service, the new groups become available to Investigate after the service is restarted.

This section describes how to add, edit, import, export, and delete custom meta groups to be used during navigation on a specific service.

Out-of-the-Box Meta Groups

Out-of-the-box meta groups are built in to RSA NetWitness Platform. The OOTB meta groups are useful to focus an investigation on common use cases and to support threat detection using the RSA Hunting Pack. These are the OOTB meta groups:

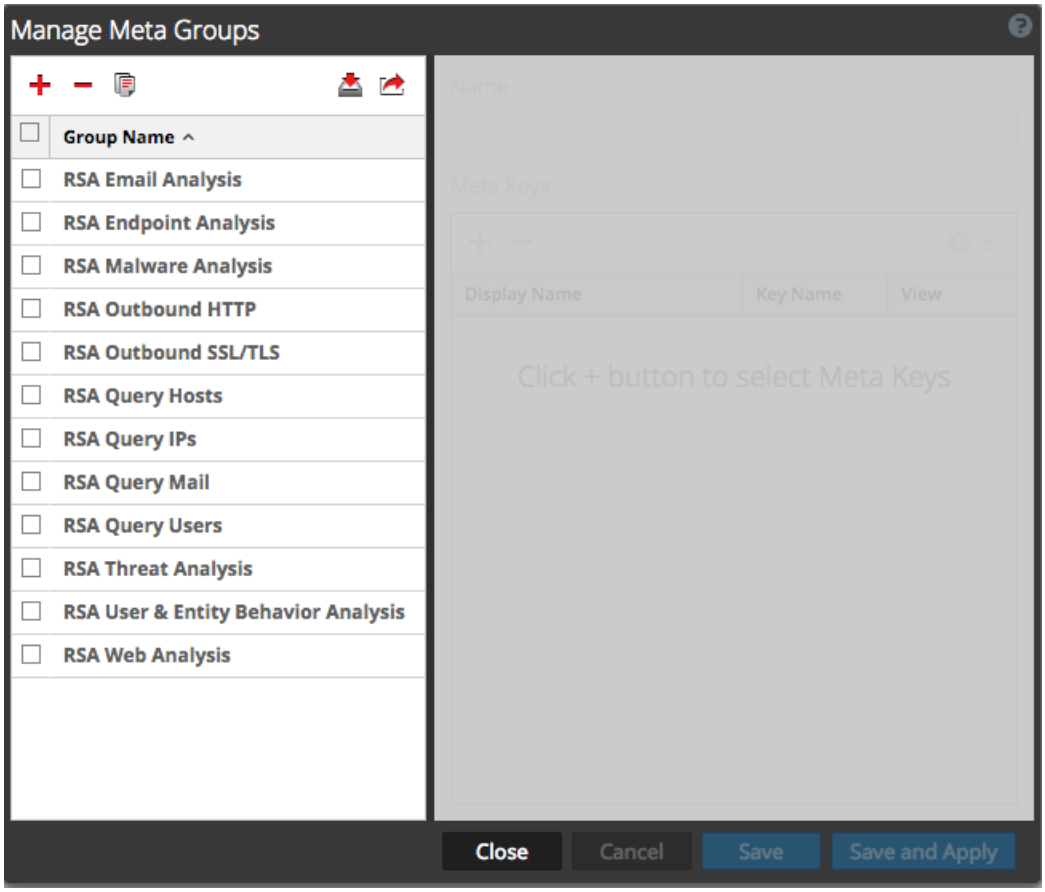
- RSA Email Analysis includes meta keys that outline email interactions.
- RSA Endpoint Analysis contains meta keys that provide insight on processes, files, users, and connections from NetWitness Endpoint (NWE) hosts.
- RSA Malware Analysis includes meta keys that mark indicators of compromise in files contained in events.
- RSA Outbound HTTP includes meta keys that provide insight into outbound web traffic.
- RSA Outbound SSL/TLS includes meta keys that focus on encrypted web traffic.
- RSA Query Hosts includes a meta keys that encompass all the meta keys to find hosts.
- RSA Query IPs includes meta keys that encompass all the meta keys to find IP addresses.
- RSA Query Mail includes meta keys that encompass all the meta keys to find email.
- RSA Query Users includes meta keys that encompass all the meta keys to find users.
- RSA Threat Analysis includes meta keys that mark potential threats in the data set.
- RSA User and Entity Behavior Analysis includes meta keys that encompass all the meta keys to

analyze user and entity behavior.

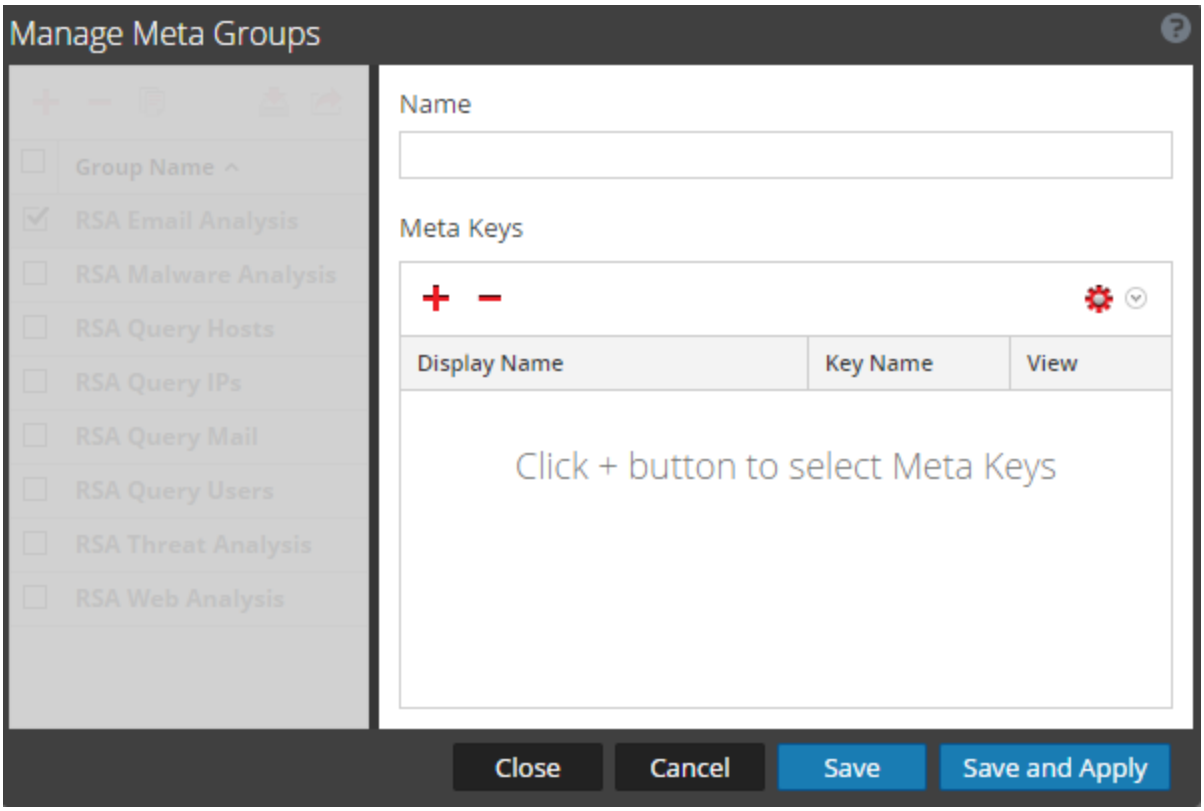
- RSA Web Analysis includes meta keys that mark anomalies in web traffic.

Create a Meta Group and Add Meta Keys

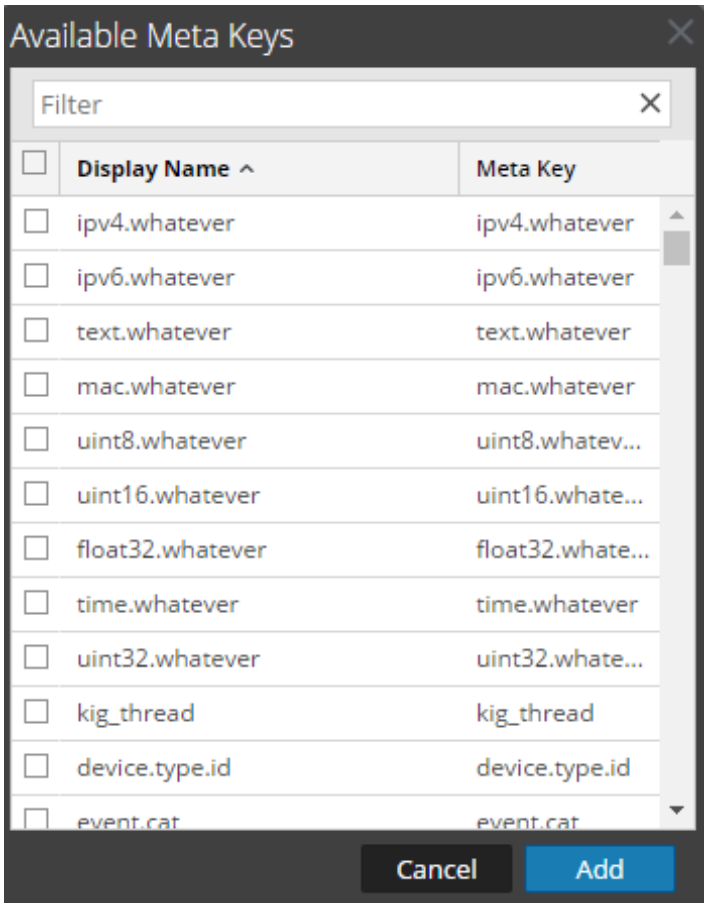
1. While investigating a service in the **Navigate** view, select **Meta > Manage Meta Groups** in the toolbar.
   The Manage Meta Groups dialog is displayed. Initially only OOTB groups are configured for a service and listed under Group Name. If other custom groups have been configured, they are also listed under Group Name.



2. In the toolbar at the top of the Meta Groups list, click +.
   A new row is inserted at the top of the Meta Groups list.
3. Type a name for the new meta group, and press **Enter**.
   The form to the right opens for editing.



4. (Optional) If you want to change the name of meta group, type a new value in the **Name** field.
5. In the **Meta Keys** toolbar, click +.
   The Available Meta Keys dialog is displayed, with keys in alphabetical order.

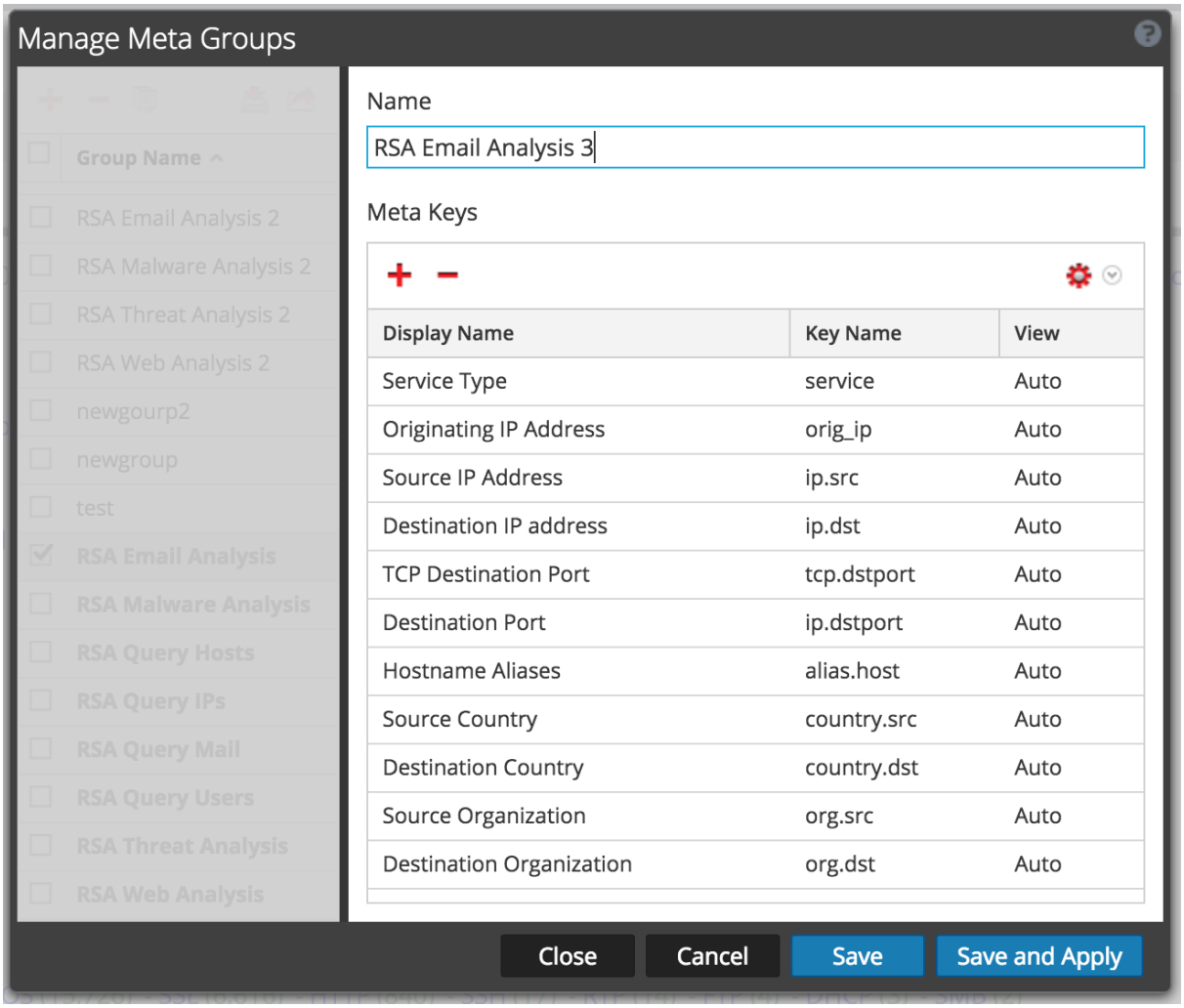


6. To filter the list of meta keys, type a word or phrase in the **Filter** field and select **Enter**.
   The list displays matching meta keys based on a case-insensitive search. Delete the filter text and press **Enter** to remove the filter.
7. To select individual meta keys to include in the meta group, select the checkboxes. To select all meta keys, select the checkbox in the title bar and click **Add**.
   The selected meta keys are added to the meta keys list.
8. (Optional) If you want to change the order in which the meta keys load and are listed in an investigation, click and drag one or more meta keys to a new position.
9. To finish creating the meta group do one of the following:
   a. To save the meta group, click **Save**.
      The group is created and available for use.
   b. To save and apply the meta group to the current Investigation view, click **Save and Apply**.
      The group is created and applied immediately to the current Investigation view.
10. Click **Close**.

Duplicate and Edit an Out-of-the-Box Meta Group

If you want to customize an OOTB meta group, you need to duplicate the group and then edit the duplicate.

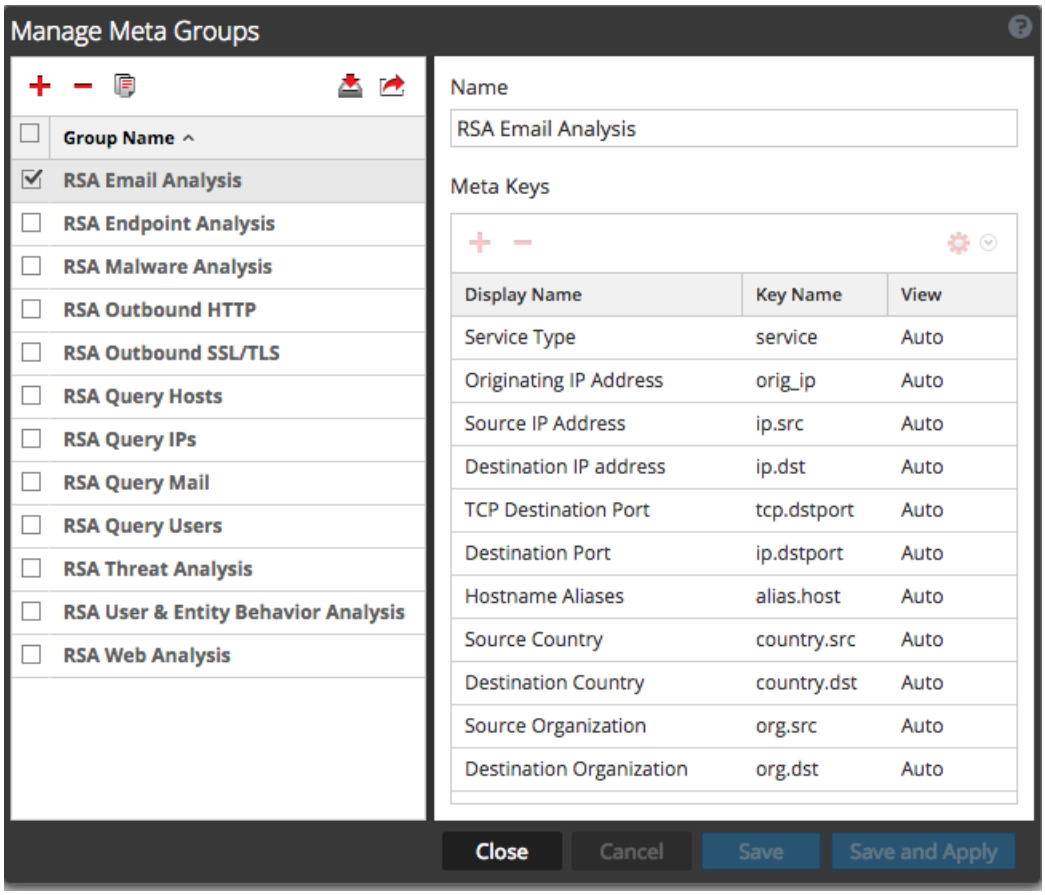
1. Select an OOTB meta group from the Manage Meta Groups list and click .
   The form to the right opens for editing with all of the meta keys as they are in the OOTB group.



2. Enter a name for the new group and continue editing as described in "Edit a Meta Group" below.

Edit a Meta Group

1. Select a group from the **Meta Groups** list.
   The form to the right opens for editing.



2. (Optional) Edit the Name of the group.
3. (Optional) Add new meta keys, as described above in "Create a Meta Group and Add Meta Keys."
4. (Optional) To set the order for the keys, drag and drop one or more keys.
5. (Optional) To change the initial view of a meta key, click and choose one of the possible views. When you modify the meta group, you cannot set the key to OPEN. If you change the default view for a group of meta keys to OPEN and some of the meta keys are non-indexed, the non-indexed meta keys revert to AUTO. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are CLOSED until opened manually.
   The value for the initial view is displayed in the View column.
6. To save, the changes, click **Save**.
7. To apply the changes to the current Navigate view, click **Save and Apply**.

Delete a Meta Group

1. In the **Meta Groups** list, select the group to be removed.
2. Click .
   A confirmation dialog provides an opportunity to cancel or complete the request.

3. Click **OK**.
   The meta group is deleted. When you close the window, if the deleted group was the currently applied meta group, it is removed and the default meta keys are used to build the view.

Export a Meta Group

User-defined meta groups are created on individual services. To make meta groups available to another service, you must export them to your local file system. To export one or more meta groups:

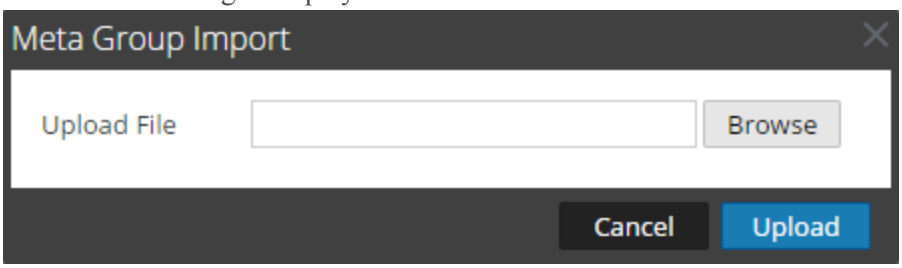
1. In the **Meta Groups** list, select one or more groups to be exported.
2. Click .
   The selected groups are downloaded to your local file system as a **MetaGroups.jsn file**. Every download of meta groups has the same name with a numeral appended to avoid overwriting previous downloads.

Import a Meta Group

To make user-defined meta groups from another service available to the currently investigated service, you must import the `MetaGroups.jsn` file from the local file system. When you import meta groups, an error message is displayed if any of the groups are already present. To import a group that is a duplicate, you must first delete the existing group. If you want to delete a meta group, it cannot be in use by a profile.

To import meta groups:

1. In the **Meta Groups** list, select a file to import and click .
   The selection dialog is displayed.



2. Click **Browse** and navigate to the directory on your local file system where the downloaded `MetaGroups.jsn` files are stored. Select a file and click **Open**.
   The filename is displayed in the Upload File field.
3. Click **Upload**.
   The upload process begins, and a message indicates that the upload was successful. The meta groups are added to Meta Group list. If the file is a duplicate of an existing meta group, a dialog tells you that the meta group already exists.

Visualize Metadata as Parallel Coordinates

Analysts can use the parallel coordinates visualization in the Navigate view to focus the investigation on combinations of meta keys and meta entities, and values that may indicate events are abnormal and worth investigation. The parallel coordinates chart is a way of visualizing the current drill point in Investigate to examine more than two meta keys simultaneously. Visualizing multiple meta keys simultaneously can help in identifying security issues associated with multivariate patterns and comparisons, such as when individual meta keys and values may not be of concern, but combining them together may bring an abnormal pattern or relationship to light. Meta groups (see Manage Meta Groups) can be used effectively to define a collection of meta keys that you want to visualize as parallel coordinates.

Best Practices for Effective Parallel Coordinates Charts

To create effective parallel coordinates charts, follow these recommendations:

- Use the RSA out-of-the-box (OOTB) meta groups that are included in a new installation.
- Start from a drill point rather than attempting to visualize all data.
- Limit the time range if necessary.
- Choose the smallest useful set of meta keys to display as axes.
- Specify the sequence of axes to highlight anomalies between the meta values as you follow a line across the chart.
- When you can identify a useful set of meta keys and sequence, create a custom meta group to use for future investigations. For example, you can create a custom meta group for Windows executable file types.
- Reuse and share custom meta groups by importing and exporting groups as `.jsn` files.
- It may be useful to create two versions of each custom meta group. One for analysis of meta values and one for creating a parallel coordinates chart focusing on a smaller subset of the same use case.

Note: When you import meta groups, an error message is displayed if any group is already present. To import a group that is a duplicate, you must first delete the existing group. If you want to delete a meta group, it cannot be in use by a profile.

To help build better parallel coordinates charts, several optimizations are included in NetWitness Platform.

- Analysts can specify that only sessions in which all meta keys exist are rendered in the chart.
- The administrator can increase the number of meta values rendered in the Parallel Coordinates Settings in the ADMIN > System > Investigation panel > Navigate tab.

RSA Meta Groups for Parallel Coordinates Use Cases

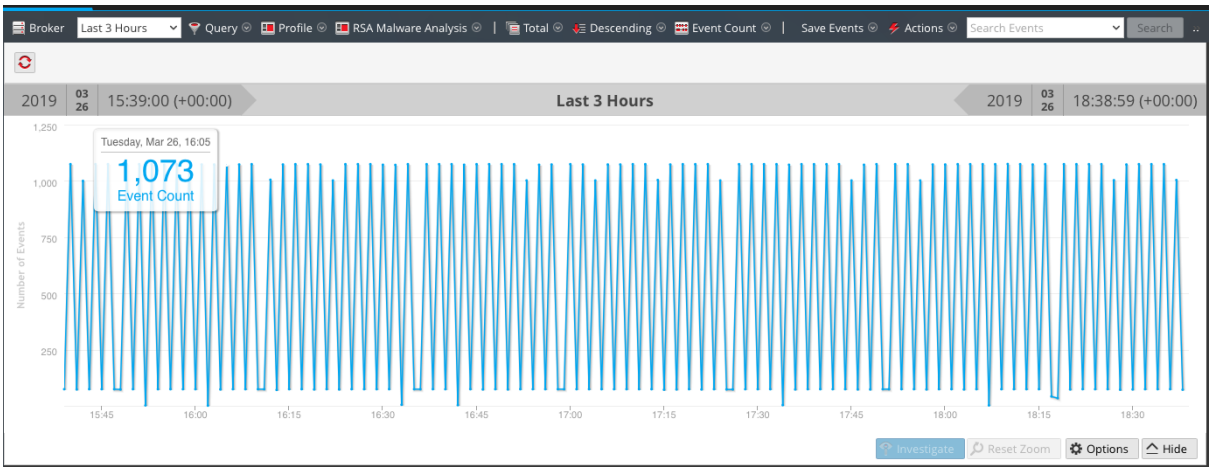
A set of predefined meta groups is included with NetWitness Platform. If you want to get the latest version, you can import the meta groups file, `MetaGroups_ootb_w_query.jsn`, in the Manage Meta Groups dialog. Some of the targeted activities that lend themselves well to Parallel Coordinates visualizations are:

- Botnet Beaconing
- Covert Channels
- Email
- Encrypted Sessions
- Endpoint Analysis
- File Analysis
- Malware Analysis
- Outbound HTTP
- Outbound SSL/TLS
- SQL Injection Attacks
- Threat Analysis
- Web Analysis

View a Parallel Coordinates Visualization

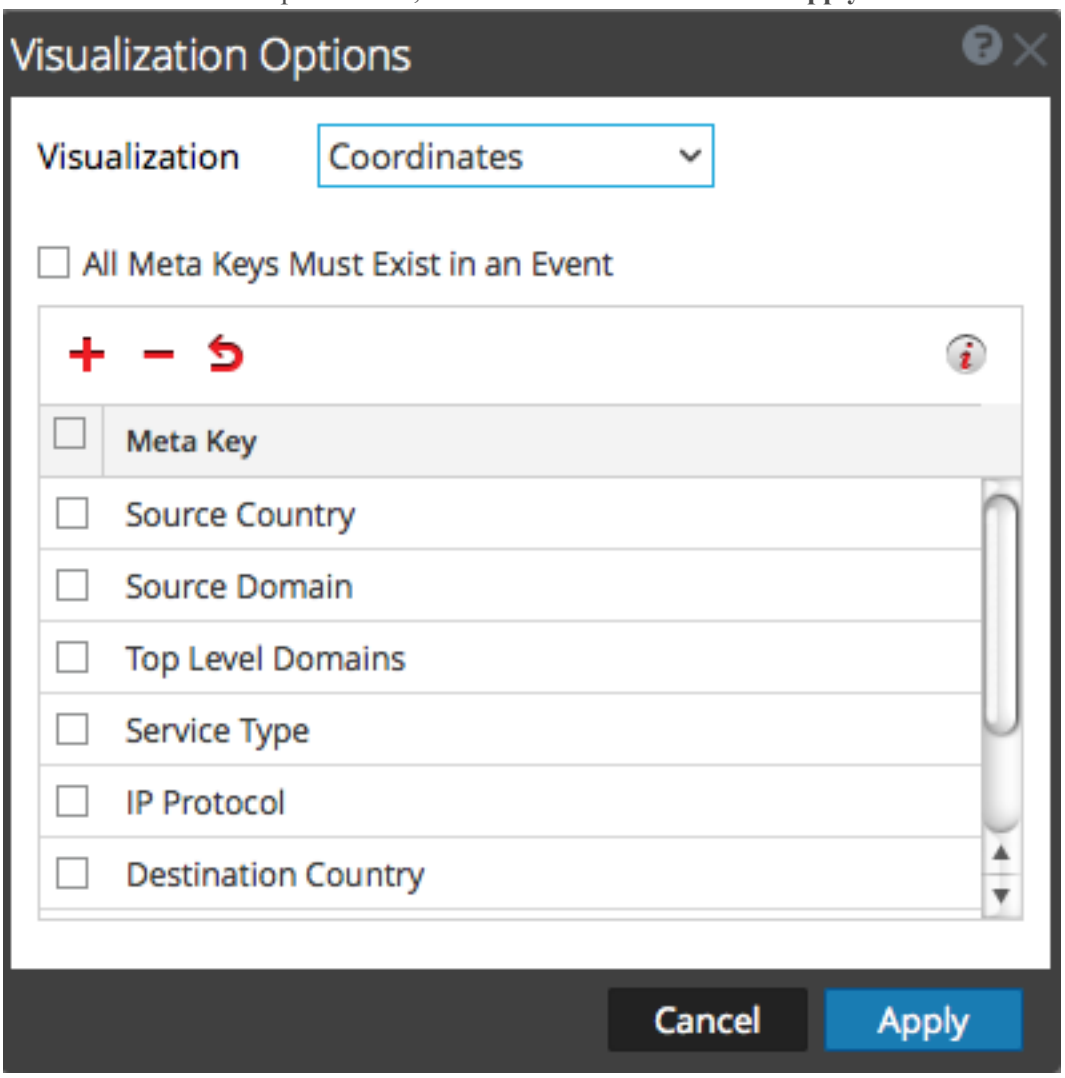
From an investigation in the Investigate > Navigate view:

1. If the Visualization panel above the Values panel is closed, select **Visualization**.
2. In the toolbar, select **Meta** > **Use Meta Group > RSA Malware Analysis**.
3. A default visualization for the current drill point is displayed as a timeline.

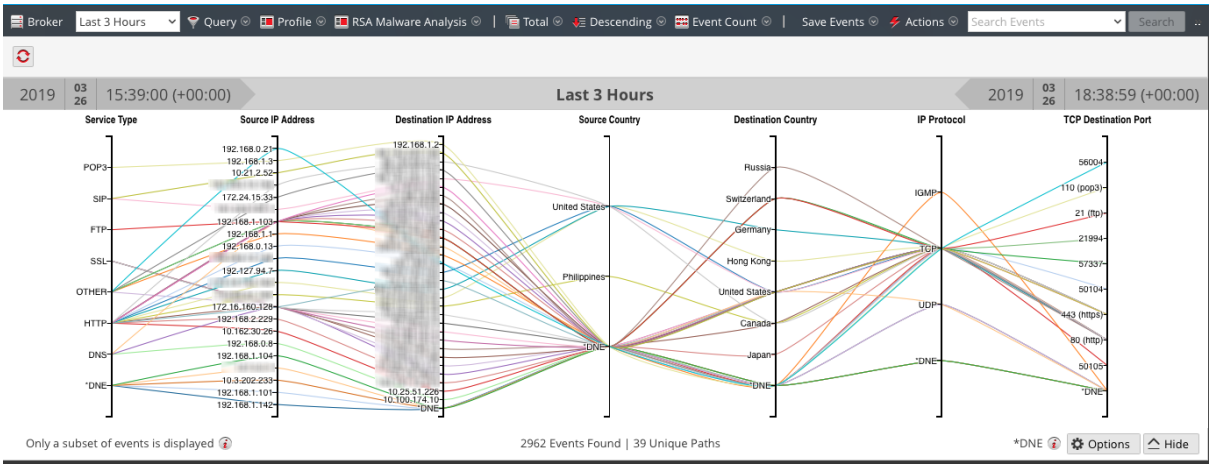


4. In the **Visualization** panel, select **Options**.
   The Visualization Options dialog is displayed.

5. In the **Visualization** drop-down list, select **Coordinates** and click **Apply**.



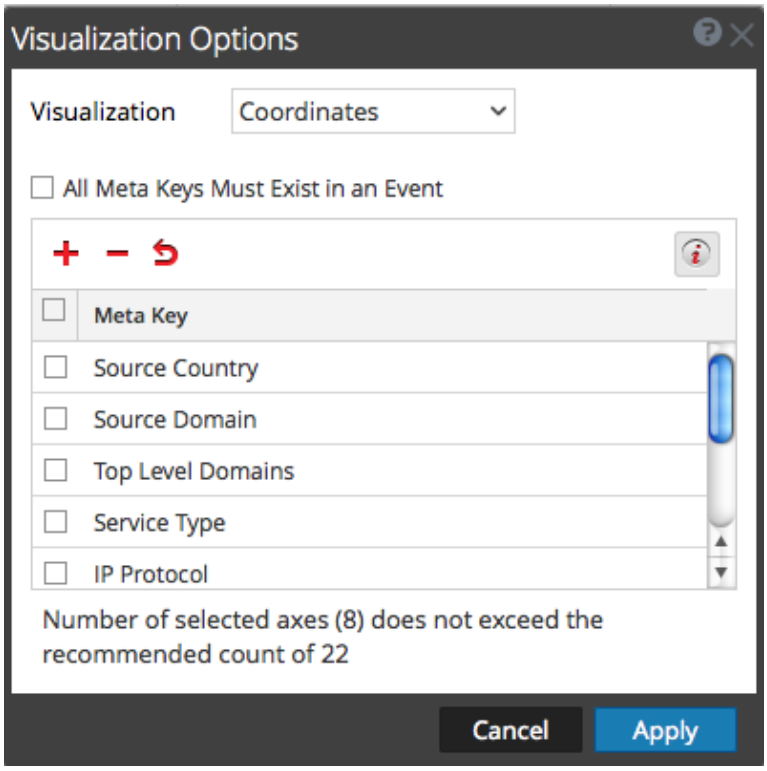
The visualization is loaded. In this example, 2962 events are found and 39 unique paths are visualized.



Select Meta Keys for a Parallel Coordinates Visualization

With a Parallel Coordinates visualization open, do the following:

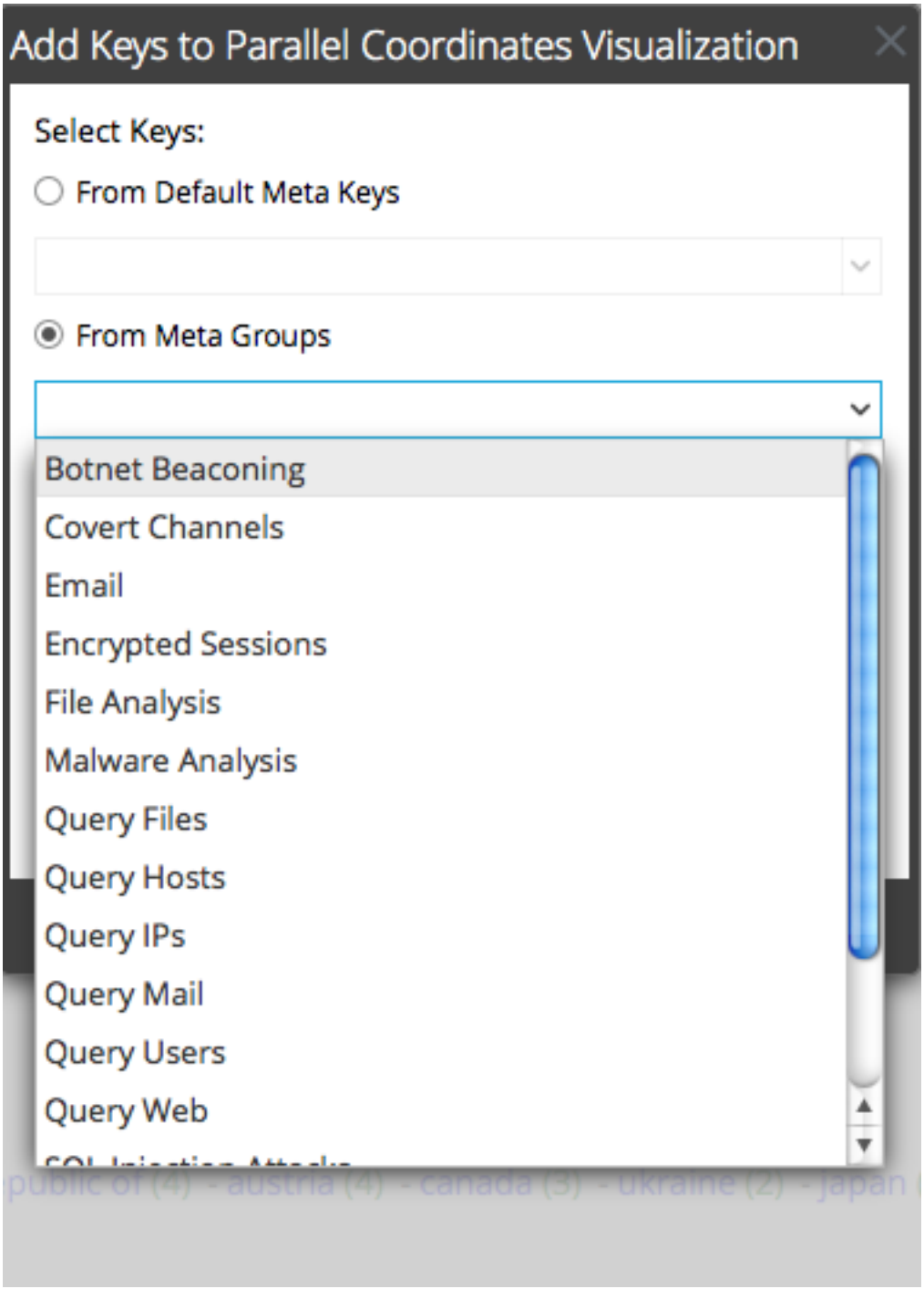
1. In the Visualization panel, select **Options**.
   The Visualization Options dialog is displayed. In the toolbar, click to display the recommended number of axes for a readable visualization. When a recommended count of keys is displayed, the count changes based on the browser size. If you make the browser window larger, the recommended count is increased.



2. If you want to change the sequence of the meta keys, drag meta keys up or down to the desired sequence.
3. If you want to delete any meta keys, click in the selection box, and click .
   The meta keys are removed, but the change has not been applied.
4. If you want to revert to the previous state, click .
   Any meta keys you have deleted are restored and any changes that you made are removed.
5. If you want to select individual meta keys, click , select **From Default keys**, and in the drop-down list, select the meta keys.

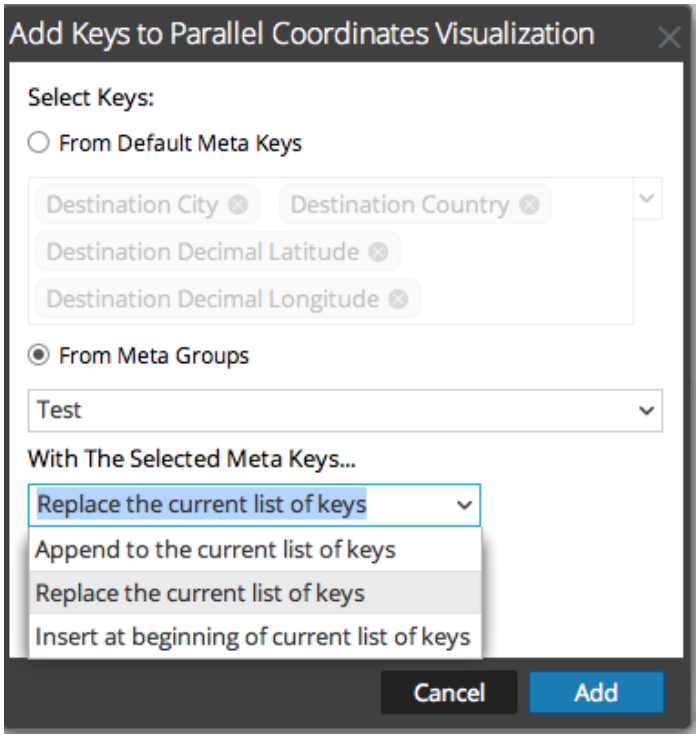
   The selected keys are listed.

6. If you want to add all the keys in a meta group, you cannot add individual meta keys. Select **From Meta Groups**, and select a group from the drop-down list.



The selected meta groups are listed in the field.

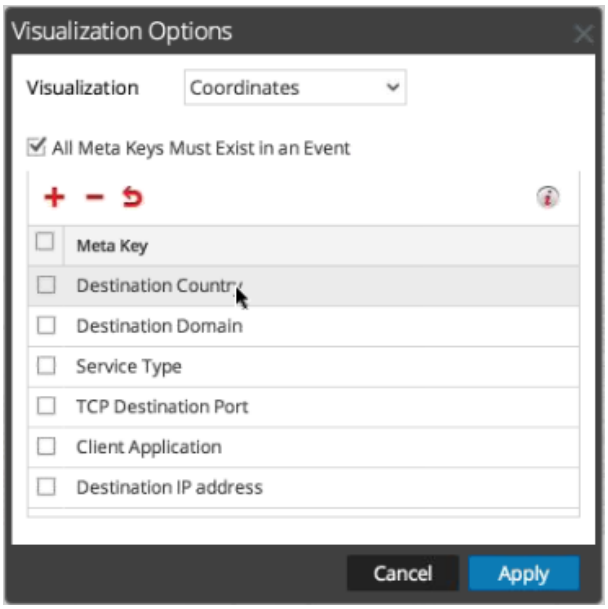
7. Select the method of adding the keys or groups: **Replace the current list of keys**, **Append to the current list of keys** (at the end), or **Insert at the beginning of current list of keys.**



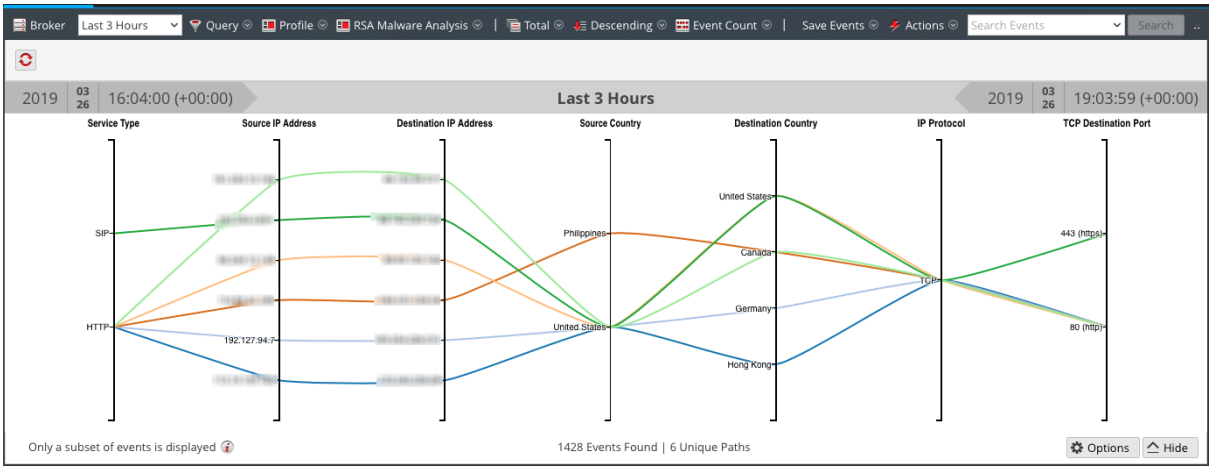
8. To complete the procedure, click **Add**.
   The Visualization Options dialog is displayed with the meta keys or groups you selected.
9. To display the new visualization chart, click **Apply**

Optimize a Parallel Coordinates Visualization

1. To optimize the visualization by removing events in which not all meta keys exist, select **Options.**

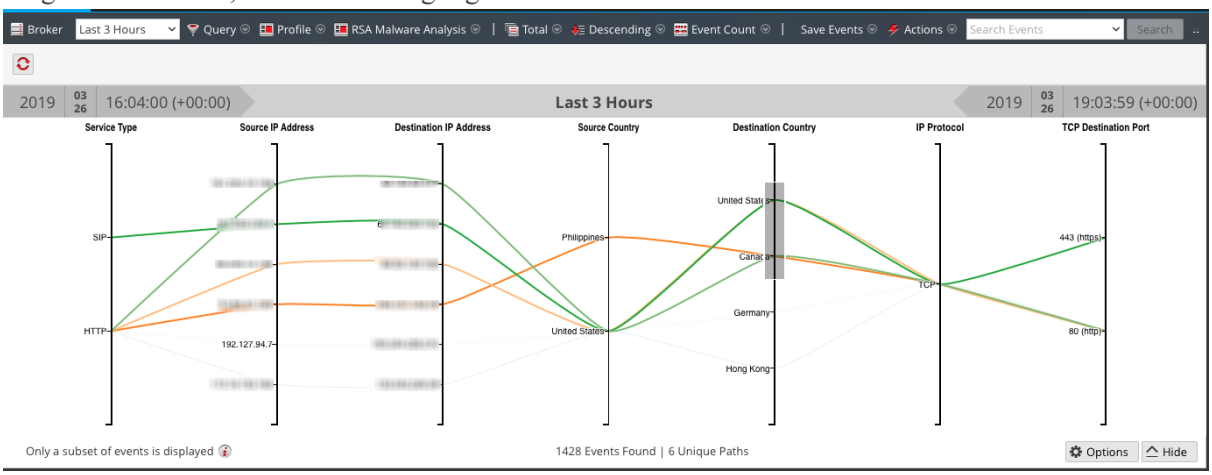


2. In the Visualization Options dialog, select **All Meta Keys Must Exist in an Event**. Click **Apply**. The resulting graph is more readable and useful and has fewer unique paths.



3. If you want to highlight a small set of points to see the path of the line from right to left, click on an axis. The cursor changes to cross hairs, which you can drag to select one or more values. When you

let go of the mouse, the lines are highlighted.



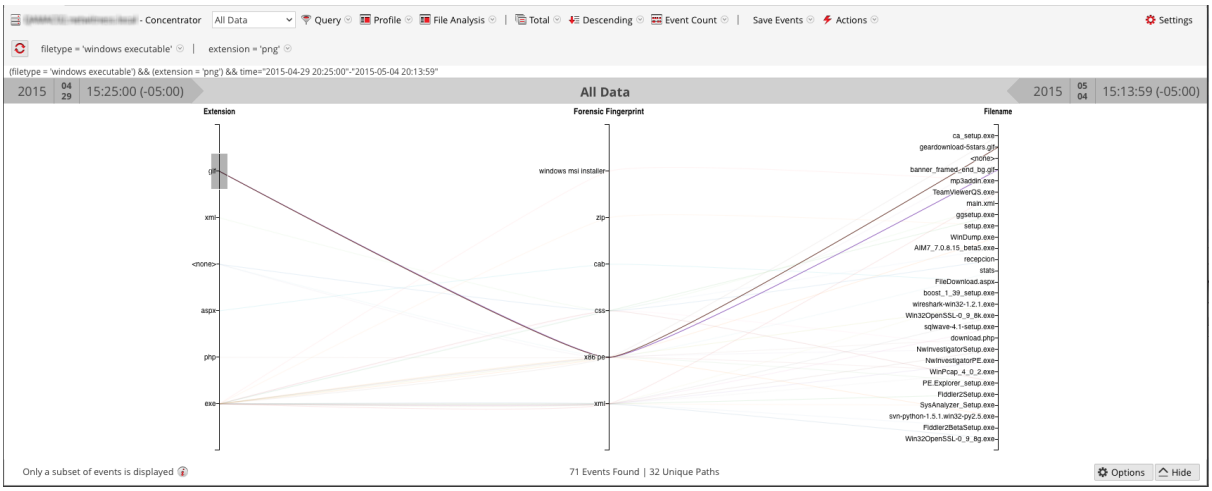
4. If you want to enlarge the visualization, drag the bottom edge of the panel down and drag the right edge of the browser window wider.

Sample Use Case

Below is an example of a parallel coordinates visualization of meta keys representing file metadata in a session. There are three meta keys or axes from left to right: Extensions, Forensic Fingerprint, and Filename with values listed along each axis. Values on the Extension axis show the file extension, and values on the Forensic fingerprint axis are windows executables. Normally the file type matches the expected forensics fingerprint; however, it is abnormal for a `gif` file type to be combined with the Windows executable fingerprint. The `gif` file type is selected to highlight the correlations of that file type, `x86pe` , and two filenames in the third axis so that an analyst can quickly identify the files that merit investigation.

To reach this view:

1. Order by Value and Sort in Ascending order.
2. Apply two filters (file type = 'windows executable' and extension = 'gif') in the Navigate view to limit the amount of data.
3. Configure a parallel coordinates chart by choosing three axes: `file extension`, `forensic fingerprint`, and `filename`.

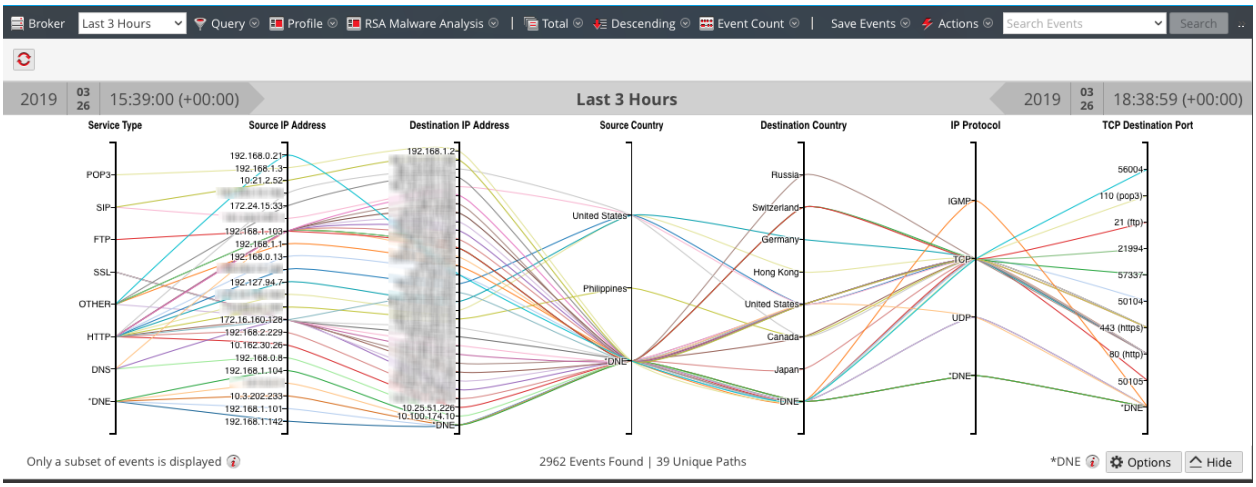


Sample Visualization of a Large Data Set

This example of a parallel coordinates visualization applied to a larger set of data illustrates several messages that help analysts to understand what has been charted.

- To create a chart, NetWitness Platform begins scanning meta values and returning results. A typical time range could have up to 10,000,000 meta values. When the number of meta values returned reaches the Meta Values Result Limit, the chart is rendered even if NetWitness Platform has not scanned a number of meta values equal to the Meta Values Scan Limit.
- There is a fixed limit on the amount of data that can be rendered as a parallel coordinates chart.The administrator configures parallel coordinates limits as part of the Investigation settings In the ADMIN > System view.

With a larger set of data, the parallel coordinates chart takes longer to process than the smaller set of data and meta keys. To preserve performance, NetWitness Platform renders the meta values from the Values panel below until the limits set by the Administrator are reached. An informational message tells you: **Only a subset of events is displayed.**



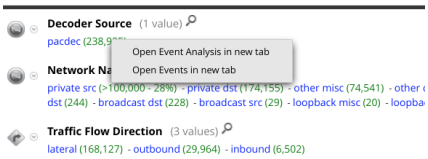
Of all the data visualized for 2962 events, there were only 39 unique parallel coordinates paths. Some events are included though they do not include some of the meta keys; these are labeled **DNE** because the metadata does not exist in the event.

Open an Event in the Events List

Analysts can view a list of events associated with a session in the Events view or in the Event Analysis view.

To display an event in the Events view do one of the following:

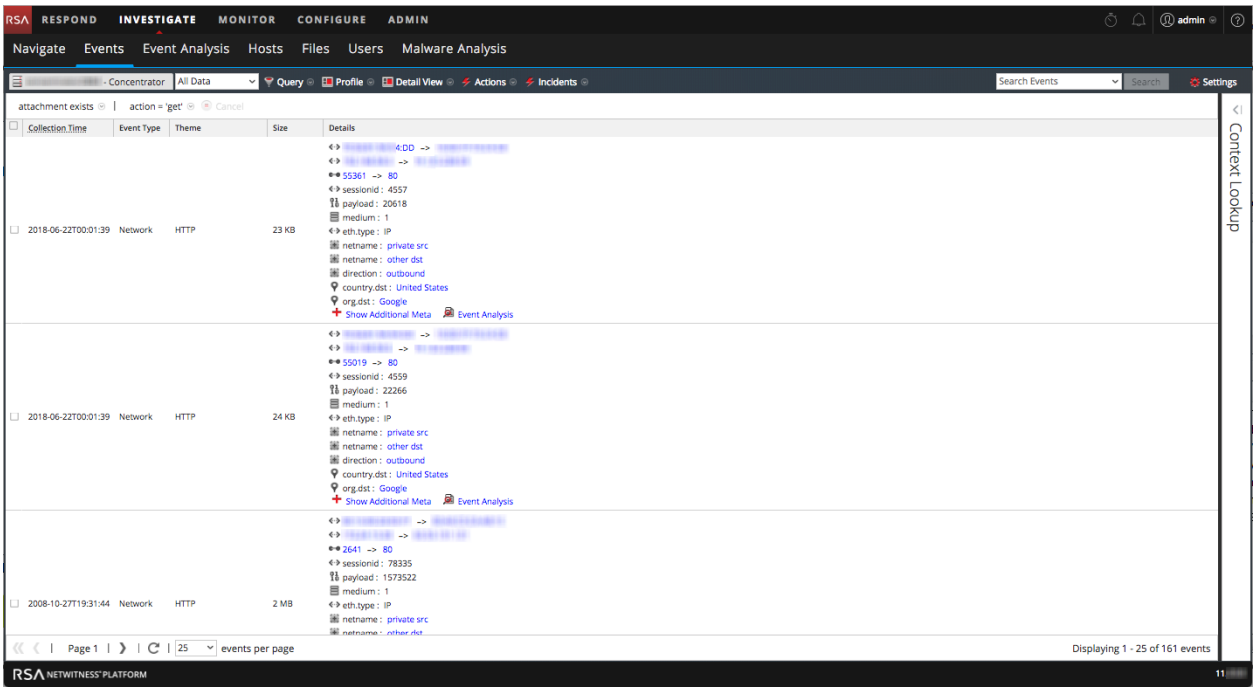
1. To use the default query for the default service, go to **INVESTIGATE** > **Events**.
   NetWitness Platform runs a default query on the last three hours for the default service (if one is set) or displays a dialog in which you can select a service and then runs the default query. The default query selects all events and the Events view displays events on the selected service, with the oldest events first.
2. To view events for a specific meta value, go to **INVESTIGATE > Navigate** and when events are loaded in the Values panel, click a meta count (the meta count is in green text). You can also right-click the meta count for a meta value . When the context menu is displayed, click **Open Events in new tab**.



   The Events view displays the events for the selected meta value.

The Events view provides three built-in presentations of event data: the Detail view, the List view, and the Log view.

This figure is an example of the Detail view.

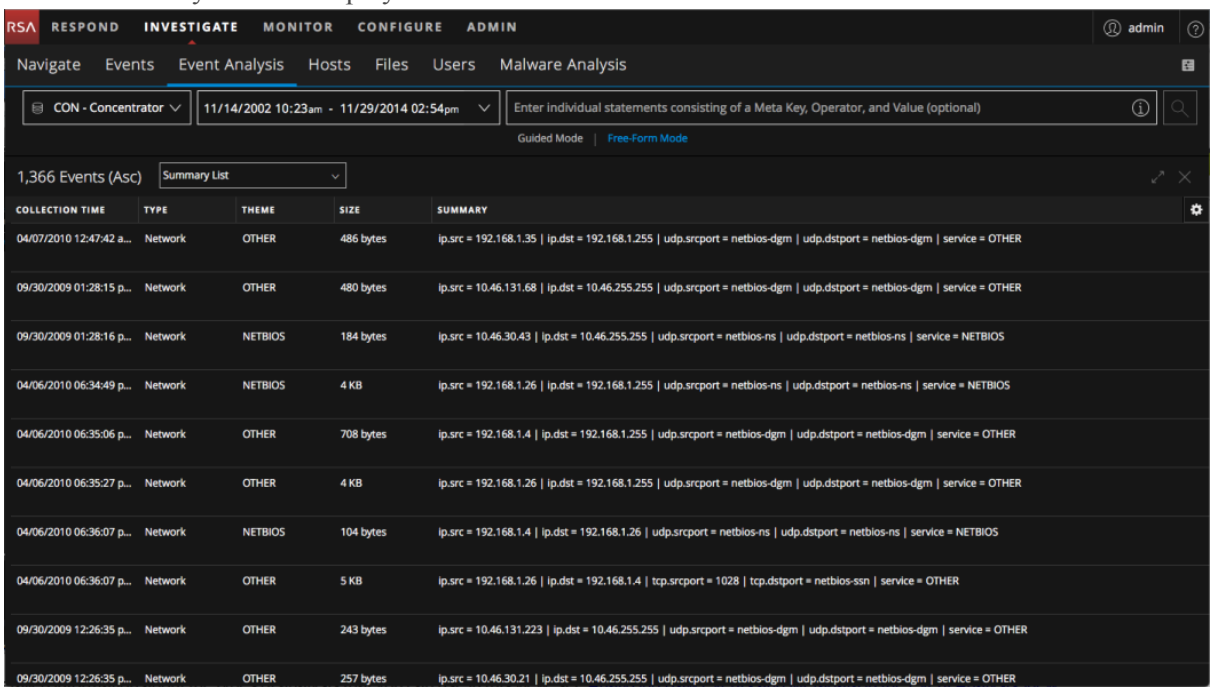


You can use queries, the time range setting, and profiles to filter the events listed in the Events view. From any view type in Events view, you can extract files, export events, export logs, and open the Event Reconstruction panel by double-clicking an event. See Examining Raw Events in the Events View for detailed information about these capabilities.

To display events in the Event Analysis view, do one of the following:

1. Go to **INVESTIGATE > Navigate**, right-click the meta count for a meta value (the meta count is in green text). When the context menu is displayed, select **Open Event Analysis in new tab**.

The Event Analysis view displays the events for the selected meta value.



For detailed information about the types of analysis that you can use in this view, see Analyzing Raw Events and Metadata in the Event Analysis View.

Export or Print a Drill Point

In NetWitness Investigate, when the data for a drill point is displayed in the Navigate view, you can:

- Extract files from a session and choose the type of files to extract: archives, audio BitTorrent, documents, executable, images, other, video, and web.
- Export the drill point as a packet capture (PCAP) file, a log file, or a metadata file.
- Print the drill point.

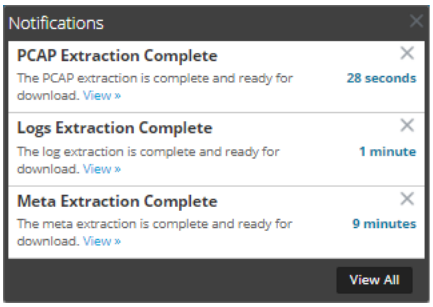
The details being exported are affected by both the time range and drill point at the time of exporting.

Note: When you export the drill point as a log file, only the log sessions are exported. The job queue message refers to the total number of sessions in the drill point rather than the number of logs. For example, if the drill point has 505 sessions and only five log sessions, the job queue message states that NetWitness Platform is extracting logs for 505 sessions.

To export a drill point from the Navigate view:

1. Conduct an investigation until you reach the desired drill point.
2. For Version 11.0, In the toolbar, select **Actions > Export** and select one of the export options: **PCAP**, **Logs**, or **Meta**.
   The drill point is extracted, and a message advises that the job is scheduled. You can check the jobs page for the status.

3. For Version 11.1, in the toolbar, select **Save Events** > and select one of the export options: **PCAP**, **Logs**, **Files**, or **Meta**.
   A dialog gives you an opportunity to edit the default filename for the file. The default filename is in the form `investigation-Feb-21-15-44-33`. When you are exporting a PCAP, the file is exported with no choice of formats. If you are using one of the other export options, a dialog is displayed.
4. In the dialog, select:
   - The export log format: **Text**, **XML**, **CSV**, or **JSON**.
   - The file types to export: Archives, Audio, BitTorrent, Documents, Executables, Images, Other, Video, and Web.
   - The Meta format: **Text**, **CSV**, **TSV**, **JSON**.
5. When the scheduled file extraction is complete, it is displayed in the Job Notifications tray.



6. Click the **View** link in the Jobs tray and download the specific extraction file requested.

To print the current drill point:

In the Navigate view, you can display the contents of the current drill point in printer friendly format in the browser window.

To display the current drill point in a print view:

1. With a drill point open in the **Navigate** view, select **Actions** > **Print** in the toolbar.
   A new tab is created with the print view of the current drill point.

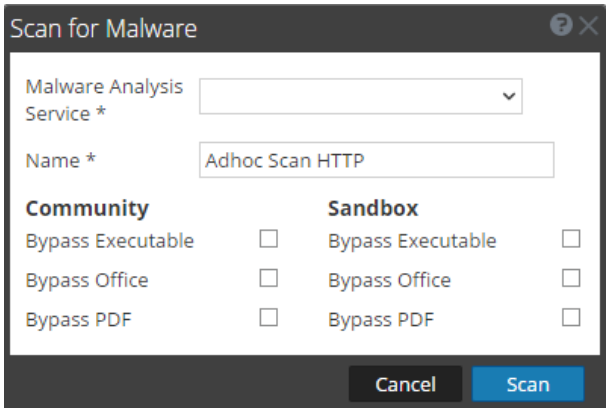
2. Use the print option in your browser to send the printable view to the printer.

Launch a Malware Analysis Scan from the Navigate View

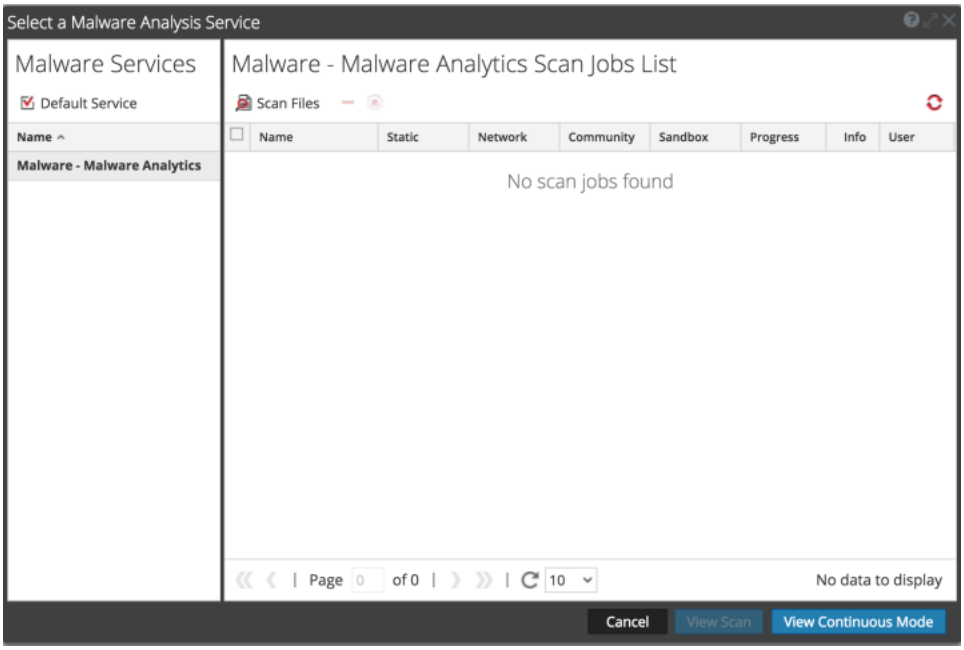
From within Investigate, analysts can launch an on-demand Malware Analysis scan by selecting a service and meta value, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis.

To launch a Malware Analysis scan of data from the INVESTIGATE > Navigate view:

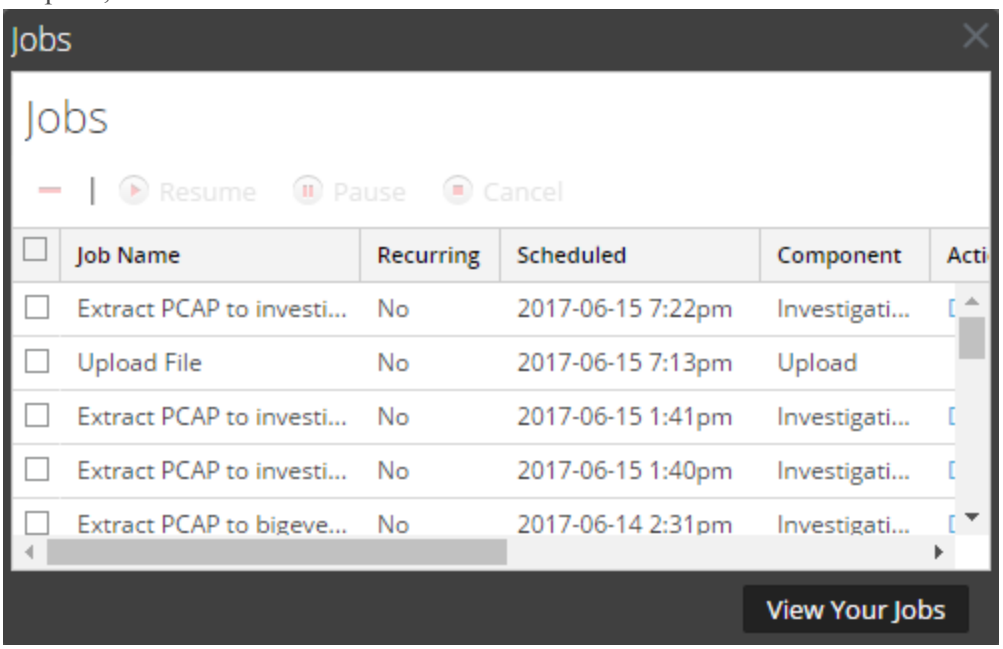
1. Right-click a meta value (for example, OTHER, DNS, or FTP) and select **Scan for Malware** in the context menu.
   The Scan for Malware dialog is displayed with a suggested name for the on-demand scan and no service selected.
2. In the Scan for Malware dialog, select a service to perform the scan, edit the name, and select the types of files to bypass under community and sandbox.



3. Click **Scan**.
   The scan request is added to the Scan Jobs List dashlet and the Jobs Tray. The bypass settings in this dialog override the default settings in the basic Malware Analysis configuration settings.
4. To view the jobs, do one of the following:
   a. Go to the Scan Jobs List in the Malware Analysis view or in the Unified dashboard. Double-click a scan to view the scan.



   b. To view the job in the Jobs tray, click in the NetWitness Platform toolbar. When the job is complete, scroll to the left and click **View**.



The Malware Summary of Events for the selected scan is displayed. The scan is also added to the list of available scans in the dialog for selecting scans in the Investigation > Malware tab.

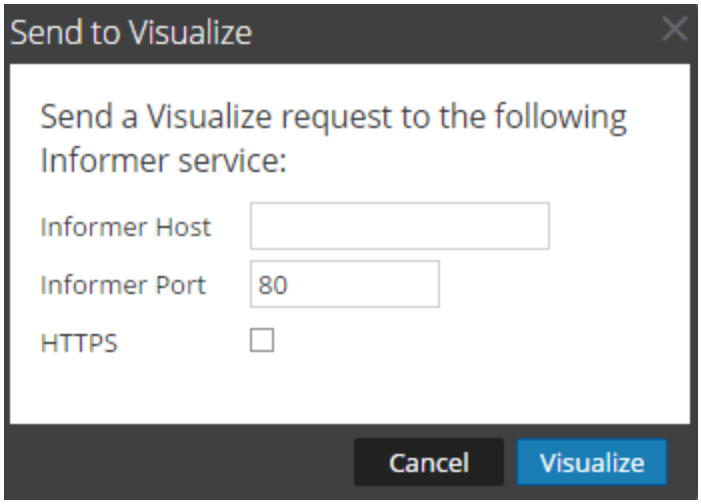
Visualize the Current Drill Point in Informer

This topic provides instructions for sending a drill point in the Navigate view to an Informer visualization.

Informer must be installed in your network and accessible by the service being investigated. You need to supply the host name and the port used on the Informer host to communicate with NetWitness Platform.

To display a visualization in Informer of the current drill point:

1. With a drill point open in the Navigate view, click **Actions > Visualize**.
   The Send to Visualize dialog is displayed.



2. Type the Informer hostname or IP address, and verify the NetWitness Platform server port used to communicate with the Informer host.
3. (Optional) Select the HTTPS option if the Informer host uses secured communications.
4. Click **Visualize**.
   The visualization is displayed in a new tab.

Examining Raw Events in the Events View

Analysts can view and reconstruct events associated with a session in Investigate.

- If you have the appropriate system roles and permissions set up for your user accounts, you can go from a Navigate view drill point to the Events view.
- If you do not have access to the Navigate view or want to go directly to the Events view, you can open sessions and examine the events that make up the session in the Events view.
- You can select queries from your query history.

These topics describe methods of working in the Events view:

- Add Events to an Incident for Response
- Manage Column Groups in the Events View
- Export Events in the Events View
- Add Events to an Incident for Response
- Combine Events from Split Sessions

You can also use these methods of querying data and acting on results that are common to the Navigate view and the Events view.

- Use Profiles to Encapsulate Common Areas for Investigation
- Search for Text Patterns
- Create a Custom Query
- View and Modify Queries Using URL Integration
- Manage Context Hub Lists and List Values in the Navigate and Events Views
- Look Up Additional Context for a Data Point
- Reconstruct an Event

Filter and Search Results in the Events View

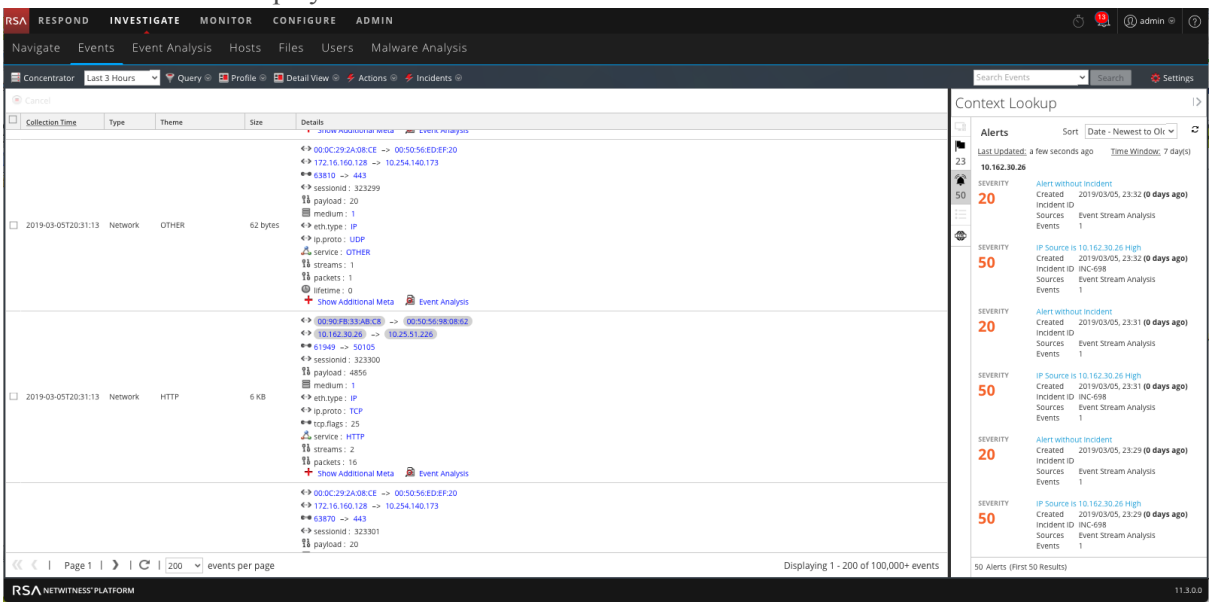
Analysts can filter events in the Events view by searching for events or selecting the service, setting the time range, and querying the metadata. If you opened the Events view from a Navigate view drill point, the view opens to the Detail view of events by default. Analysts who do not have permissions to use the Navigate view can query services directly from the Events view.

Note: When an Archiver is the currently selected service in the Events view and you are searching against a Broker or Concentrator, the search is slower than if searching against a Broker or Concentrator because the data on the Archiver is compressed and there is typically more data.

Filter Events Displayed in the Events View

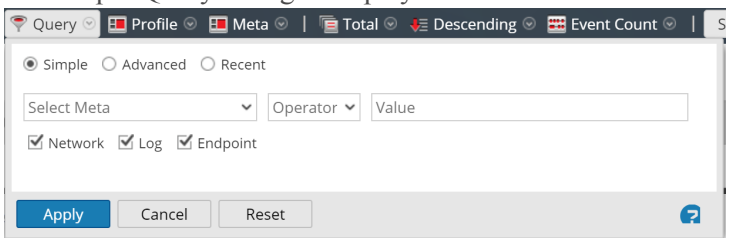
To filter the data displayed in the Events view:

1. Go to **INVESTIGATE** > **Events**.
   The Events view is displayed.

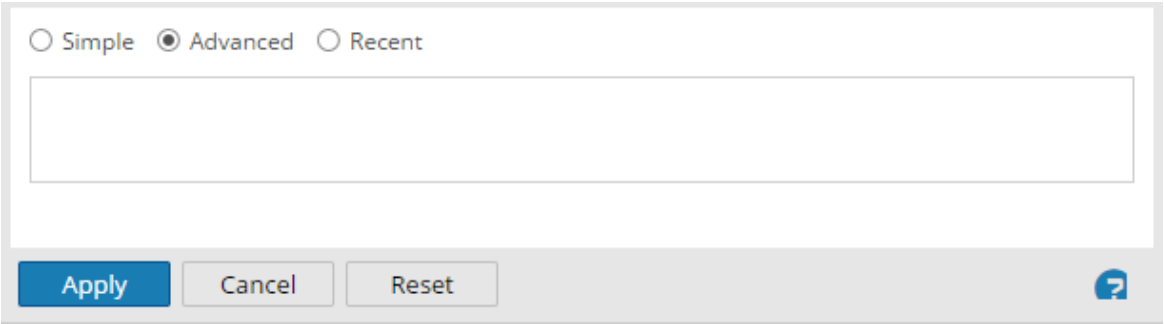


2. To select a time range other than the default (**Last 3 Hours**), in the toolbar, click the time range field and select a value. For example, **Last Hour**.
   The Events view is refreshed with the selected time range.

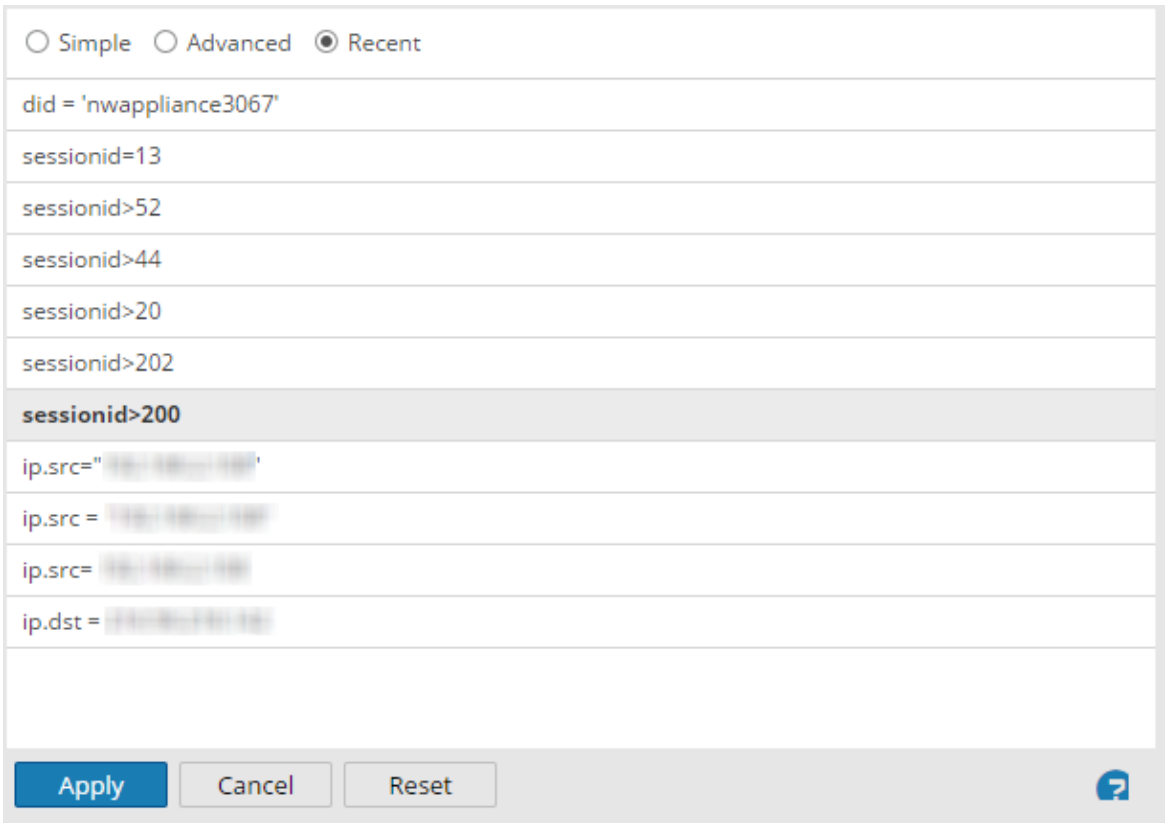
3. To enter a query for the selected service and time range, in the toolbar, click **Query**.
   The Simple Query dialog is displayed.



4. If you want to enter a simple query using the auto-complete feature to select meta and operators, do one of the following:
   a. Click in the **Select Meta** field and select a meta key from the drop-down list.
   b. Select an operator from the drop-down list in the **Operator** field.
   c. Type a value to match in the **Value** field.
   d. Select **Network, Log**, or **Endpoint** data, and click **Apply**.
      The matching data is displayed in the Events view.
5. If you want to enter a more complex query based on your knowledge of the meta keys and operators:
   a. Click **Advanced**.
      The Advanced Query dialog is displayed.



   b. Type a query. As you type the query, beginning with the meta key, drop-down lists of available meta keys and operators are displayed. When finished, click **Apply**.
6. If you want to select a query from a list of recent queries:
   a. Select **Recent**.
      The Recent Query dialog is displayed.



b. Select a query and click **Apply**.
The matching results for the query are displayed in the Detail View in the Events view. The breadcrumb reflects the query.

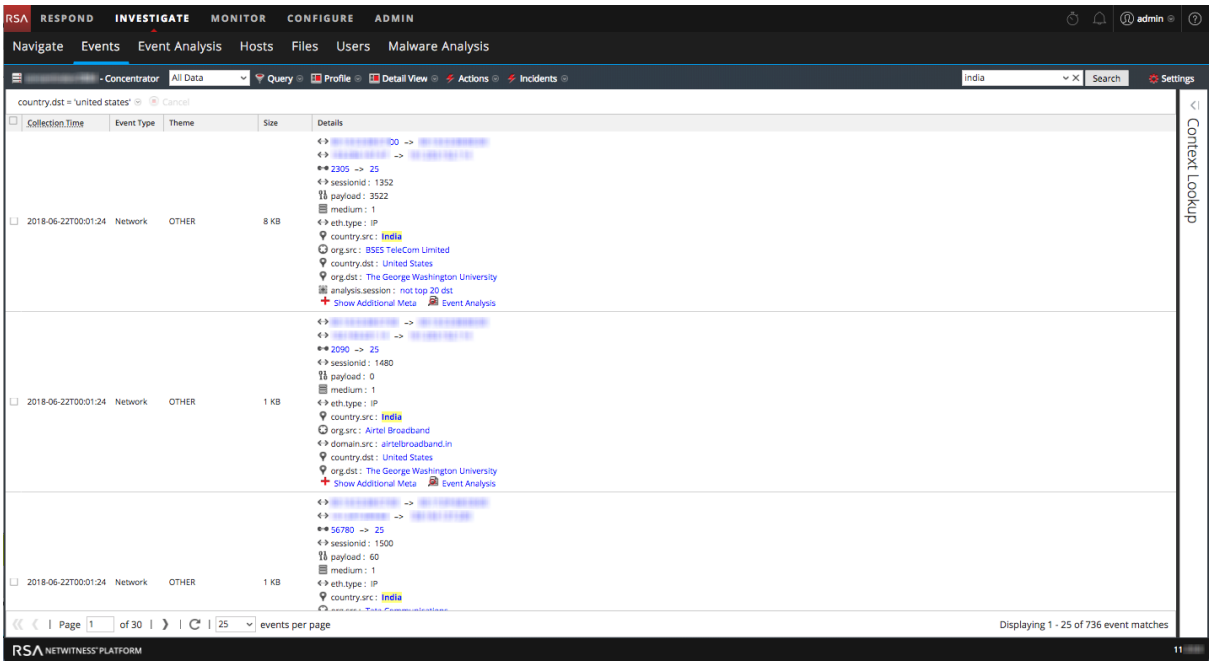
c. In the breadcrumb, you can click any of the crumbs to display the Query menu. You can insert a new query before a crumb, and append a new query to the end of breadcrumb. After each edit in the breadcrumb, the results are refreshed.

Search for Events in the Events View

You can search the currently displayed data in the Events view by entering a search string in the Search field. The search string can be a `regex` (Regular Expression) or it can be a simple text search. provides detailed information on these search types.

To search within the currently displayed data in the Events view:

1. Place the cursor in the **Search** box, type a search string, and press **Enter** or click **Search**.
The search results are displayed in the Events view. Events that match the search criteria are displayed. In the Details view and List view, matches are highlighted in the Details column. In addition, when searching RAW, matches are highlighted in the Log view Logs column. Below is an example of the search results for the search term **India** in the Events Detail view. (Search matches are not highlighted in any Event Reconstruction.)



2. If you want to narrow the search, change the query and time as described above in #Filter.
3. If you want to stop the search and return to the Events view, click **Cancel**.
   Any results that are displayed remain.
4. To clear the search box and return to the normal Events view, click **X** in the search box.

Page Through Events in the Events View

Pagination controls allow more flexibility in paging through a list of Events in the List View, Logs View, or Details View. You can select the number of events to display per page, and your selection is saved across logins to the NetWitness application. When a control is unavailable, the control is dimmed; for example, when you are viewing page 1, the ❮ and ❮❮ controls are dimmed.

To use pagination controls:

1. With results displayed in the Events view, click the current number of events per page (**10**, **25**, **50**, **100**, or **200**), and select the new number of events per page from the drop-down menu.
2. To page forward or back, use the page control icons:
   Click ❯ to go to the next page.
   Click ❯❯ to go to the last page.
   Click ❮ to go the previous page.
   Click❮❮ to go to the first page.
3. To go to a specific page, type a page number in the page number field | 3 | Page 3 |.

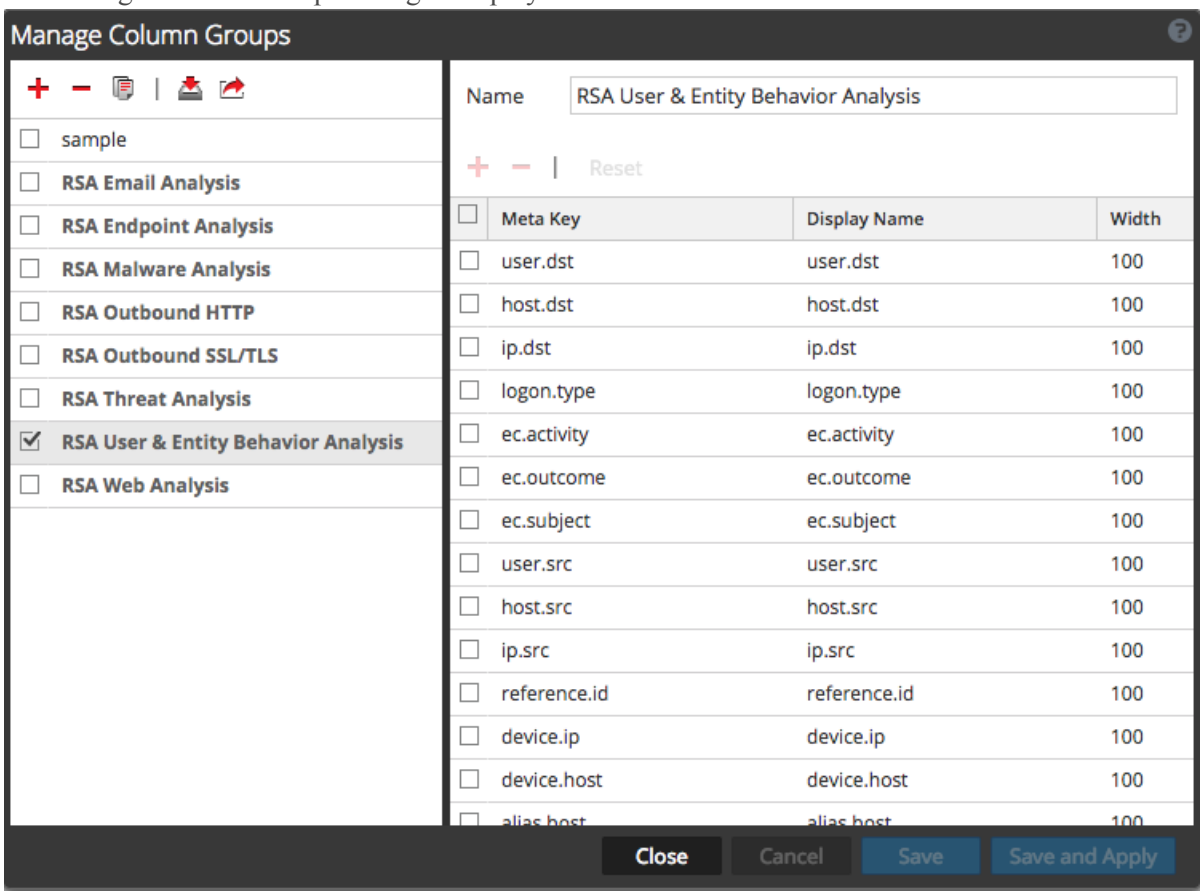
Manage Column Groups in the Events View

When viewing a list of events in Events view, you can customize the way data is displayed by defining the meta key or meta entity to display in a column, the position of the column in the list, and the default width of the column.

Note: Investigate profiles can include custom column groups. If a custom column group is used in a profile and you are viewing events in the Events view using a custom column group, you cannot change the view type (Detail, List, or Log).

Create Custom Column Group

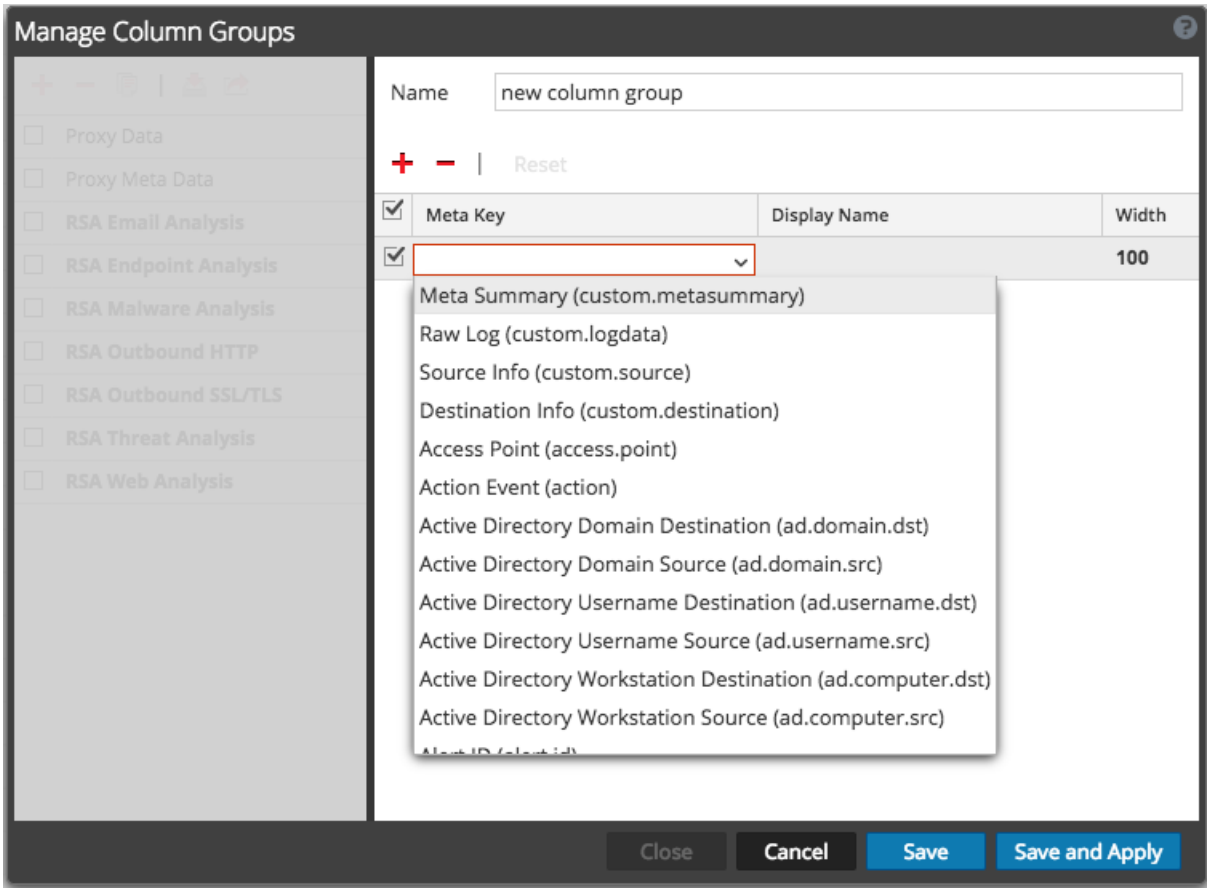
1. Go to **NAVIGATE > Events**.
2. Select **Manage Column Groups** in the **View** drop-down menu. The View option is named for the current value, for example, Detail View, List View, Log View, or the currently selected column group.
   The Manage Column Groups dialog is displayed.



3. To add a new column group in the column group panel, click + and type the name of the new group in the resulting field.

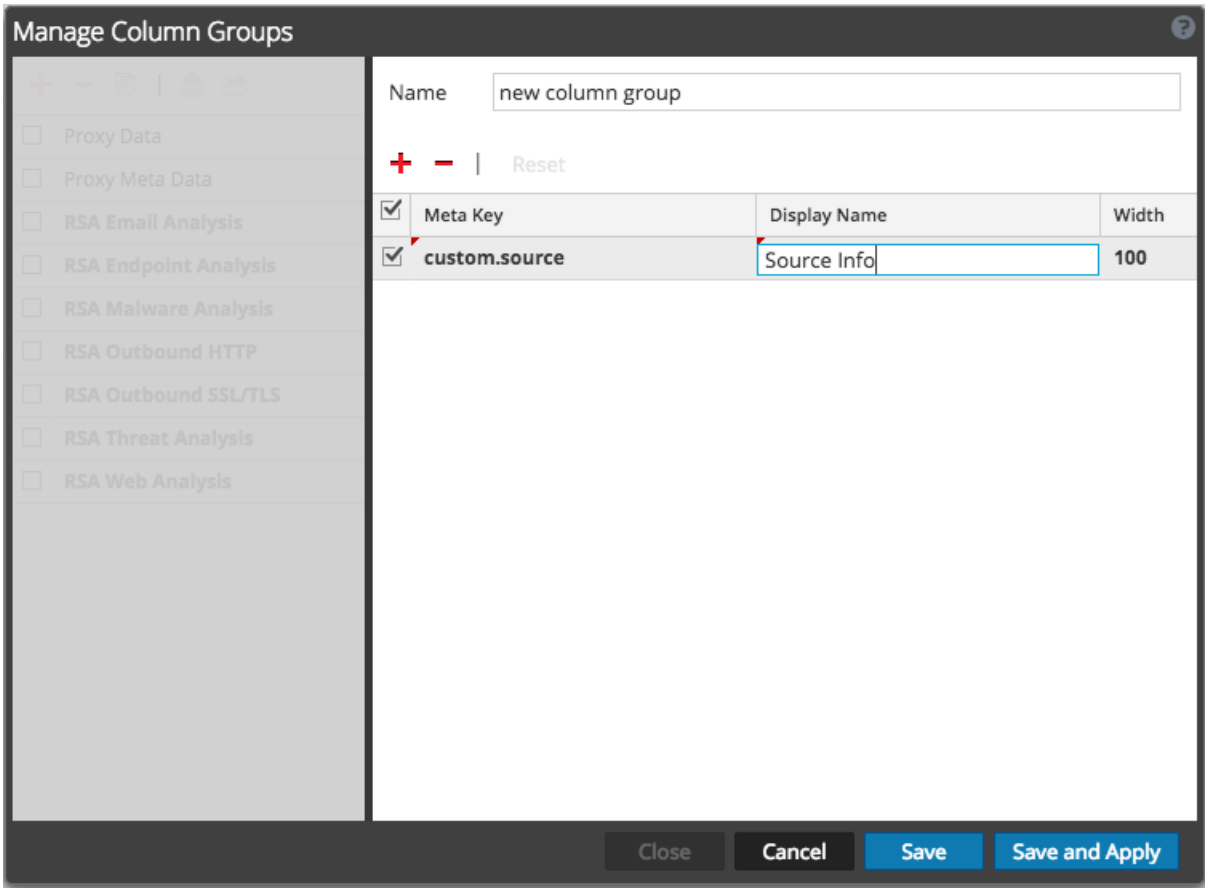
The column definition panel opens on the right with the group name filled in. You can edit the group name.

4. To add a column to the group, click +, and click in the empty **Meta Key** field to display the **Meta Key** drop-down list. Select a meta key field from the list, and repeat this step until the column set is complete.



5. (Optional) To delete a meta key from the column group, click −.
6. (Optional) To rearrange the sequence in which the columns appear in the Events list, drag meta keys to the desired position.

7. (Optional) To set the default width for a column, click in the corresponding value in the **Width** column, and type a new column width.

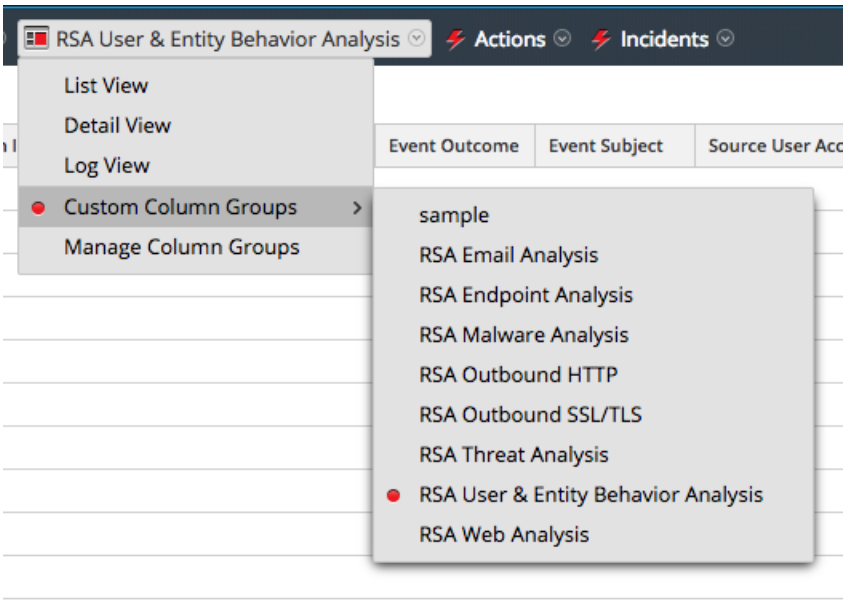


8. (Optional) To revert to the previous settings for the column group, and undo all of your changes, click **Reset**.
9. When ready to save, do one of the following:
   a. To save the edited column group and refresh the Events view with the column group settings, click **Save and Apply**.
   b. To save the edited column group without refreshing the Events view, click **Save**.

Select a Column Group

To select a column group:

1. With the Events view open, select **Custom Column Groups** in the **View** drop-down menu. The option name is the default value (Detail View or the current value).



2. Select one of the column groups from the submenu.
   The Events view is refreshed to reflect the custom column group. In Version 11.2 and later, any preQuery in the column group is displayed in the breadcrumb.

Export Events in the Events View

In the Events view, the Actions menu has an option to export events from the event being viewed to an archive.

Note: You can only export files that you have permission to view or access.

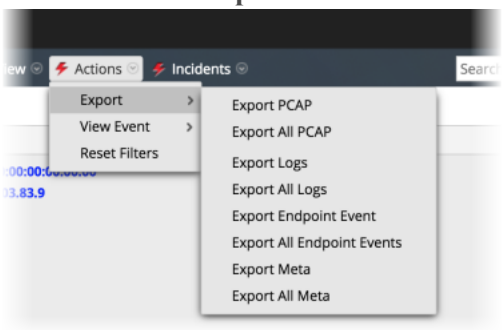
The export function queries the service for all sessions inside the selected time range and drill point to extract the content of each session. The details being exported are affected by both the time range and drill point at the time of exporting. In the File Extraction dialog, you can choose to export:

- PCAPs
- Logs
- NetWitness Endpoint events
- Meta values

The format of the exported archive: ZIP or GZIP file. After you send the request, a job is scheduled and you can track the job in in the Jobs tray. If there is an error retrieving the log or PCAP from the service, an error notification is displayed.

To extract files from an event:

1. While in the **Event view**, click an event.
2. Click **Actions > Export.**.



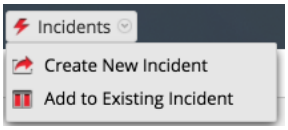
3. Select the export option.
   A message informs you that the PCAP is being downloaded.

Add Events to an Incident for Response

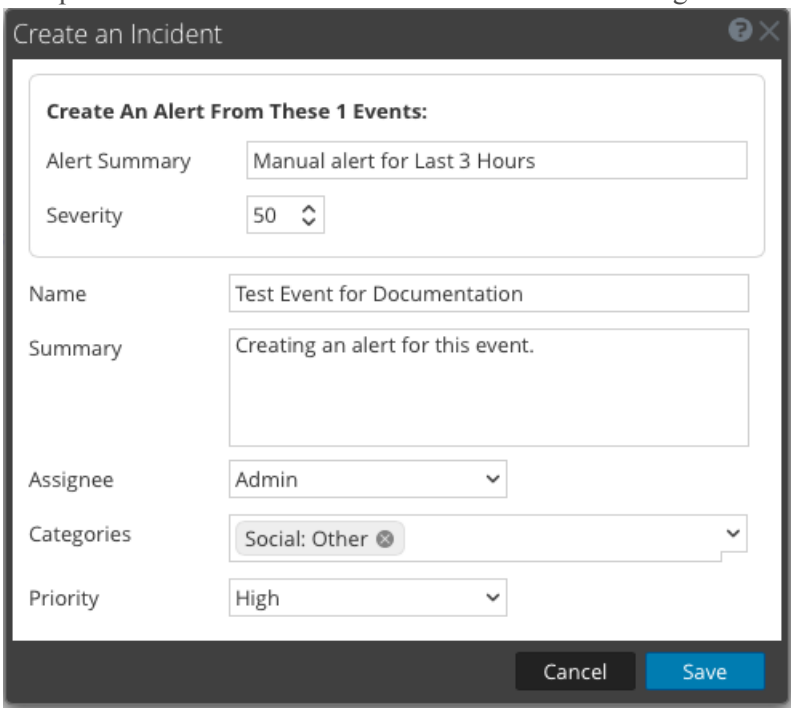
When conducting an investigation in the Events view, you can select one or more events and create an incident that is available for incident responders in Respond. You can also add events to an existing incident in Respond to which you have access.

Note: An administrator must configure the required roles and permissions as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

1. Go to **INVESTIGATE > Events**.
2. In the Events view, select one or more events, and then **Incidents > Create New Incident**.



3. Complete the information in the Create an Incident dialog.



   a. Select the severity, an integer between 1 and 100, with 100 being the most severe.
   b. Type a name for the incident and describe the incident in the **Summary** field.
   c. Select an assignee for the incident from the drop-down list. This list includes the built-in roles that have access to Respond as well as any custom roles that have been added to your system. For example, this list might include roles for admin, analyst, dpo, operator and roles for incident responsers.

d. From the **Categories** drop-down list, select one of more categories of alerts that apply to this incident.

e. From the **Priorities** drop-down list, select a category for the incident. For example, an incident may be critical, high, medium, or low priority.

f. Click **Save**.
The new incident is created and is available immediately in the incident queues for the selected role in Respond.

4. To add one or more events to an incident, select one or more events, and then **Incidents > Add to Existing Incident**.

5. In the Add Events to an Incident dialog, select the severity, and select one or more incidents to which the events will be added. You can Search for an existing incident by Incident-ID or Incident Name. When ready, click **Add to Incident**.
The events are added to the selected incidents and updated in Respond.

Combine Events from Split Sessions

Analysts can identify sessions that have been split due to session size in the Events view, and combine the fragmented sessions so that the complete session is viewable as a single query result in the Events view. When split sessions are recombined, a single packet export of the session in the Events view includes all of the session fragments.

Version 10.4 and earlier Decoders are configured with a default session size of 32 MB. When a session exceeds the 32 MB limit, the Decoder splits the session and all subsequent packets become part of a new session, fragmenting the actual network session across multiple Decoder sessions. Split sessions are parsed without the context that it is a fragment of the larger network session, sometimes resulting in session fragments with source and destination addresses and ports reversed and with unidentified application protocols. Another result of split sessions can be difficulty viewing all of the session fragments as a single query result or creating a single packet export of all the session fragments.

Decoder enhancements in NetWitness Platform 10.5 provide improved processing of fragmented sessions:

- Contextual fragment parsing.
- Session fragments highlighting.
- Finding session fragments.
- Exporting all packets to a single PCAP.

Contextual Fragment Parsing

In NetWitness Platform 10.5 and later, the Decoder completes session parsing before splitting the session based on the configured maximum session size (32 MB) or the configured timeout (60 seconds). When parsing is complete, the parsed results include the proper address directionality and application protocol, which are propagated to each subsequent session fragment to ensure consistency with the logical network session they represent.

Note: All of the necessary Decoder configuration changes are made when upgrading to 10.5. However, Find Session Fragments requires that the tcp and udp source port meta keys (tcp.srcport and udp.srcport) be fully indexed, which was not the default configuration prior to 10.5. This functionally limits the ability to find session fragments to sessions captured after the Decoder was upgraded to 10.5.

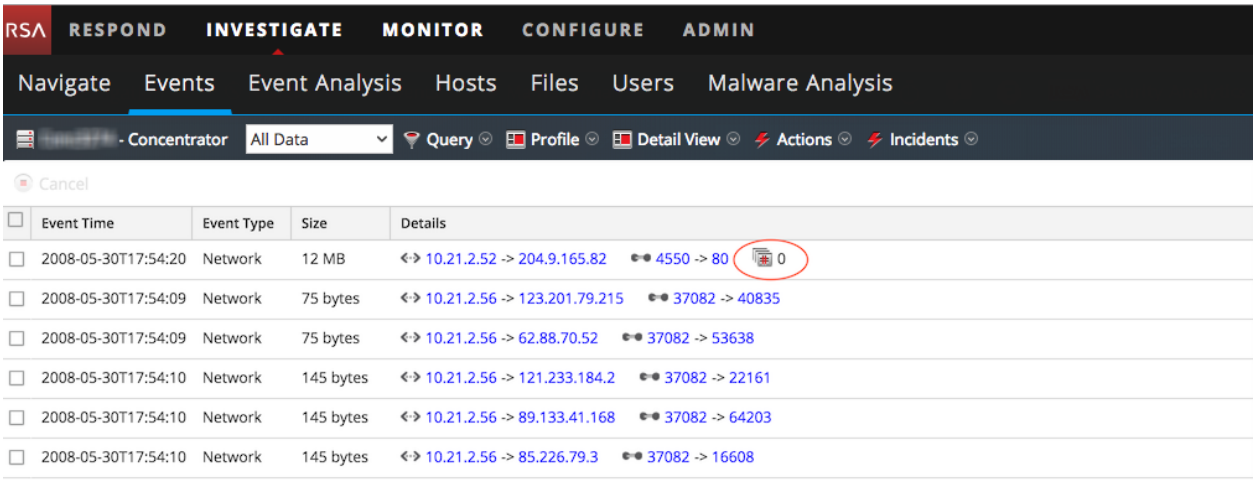
Session Fragments Highlighting

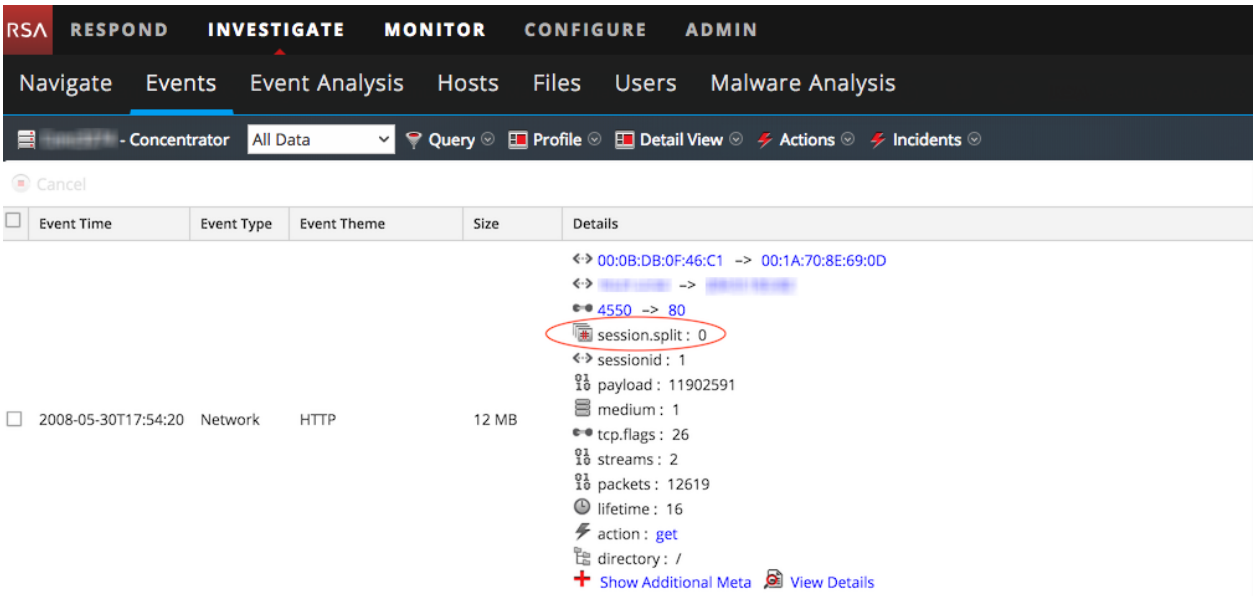
Each session fragment has an additional meta, `session.split`. The value of the `session.split` meta for a particular session fragment indicates how many fragments precede that fragment. When viewing sessions in the Events view, the `session.split` meta clearly identifies sessions that are fragments in the Events List view and the Events Detail view.

The session split happens when the configured Decoder `assembler.size.max` or `assembler.timeout.session` (latency between sessions) is reached. The earliest fragment is session 0 and sessions with a later time stamp are incrementally numbered 1, 2, 3, and so on. The `session.split` meta indicates the number of preceding sessions fragments; however, it does not always indicate that there are subsequent session fragments, even with a value of 0. It is also possible for the first fragment of the session to not have `session.split` meta if the session is parsed before exceeding the maximum session size.

Once you view the session fragments, you can determine the maximum session size or session timeout necessary for parsing to combine the split sessions into one again. For example, if you have four fragments at 32 MB, you need to configure your test Decoder (usually a virtual machine set up separate from main production service) with a maximum session size greater than 128 MB. The steps are the same to find all fragments based on a session timeout. The figures below show the Events List view and the Events Detail view with fragmented session information highlighted.

Note: A maximum session size of 12 MB was configured at the time the screen captures below were created.





The `session.split` metadata is always displayed immediately following the address and port metadata in the details view. It is never hidden as additional metadata. These enhancements make it possible to quickly:

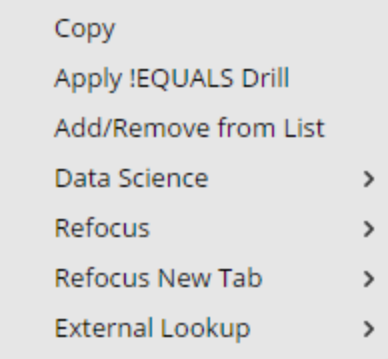
- Identify sessions that are fragments of a network sessions.
- View all of the session fragments of a network session given a single session fragment.
- Export the packets for the entire network session as a single PCAP file.

Find and Combine Fragments

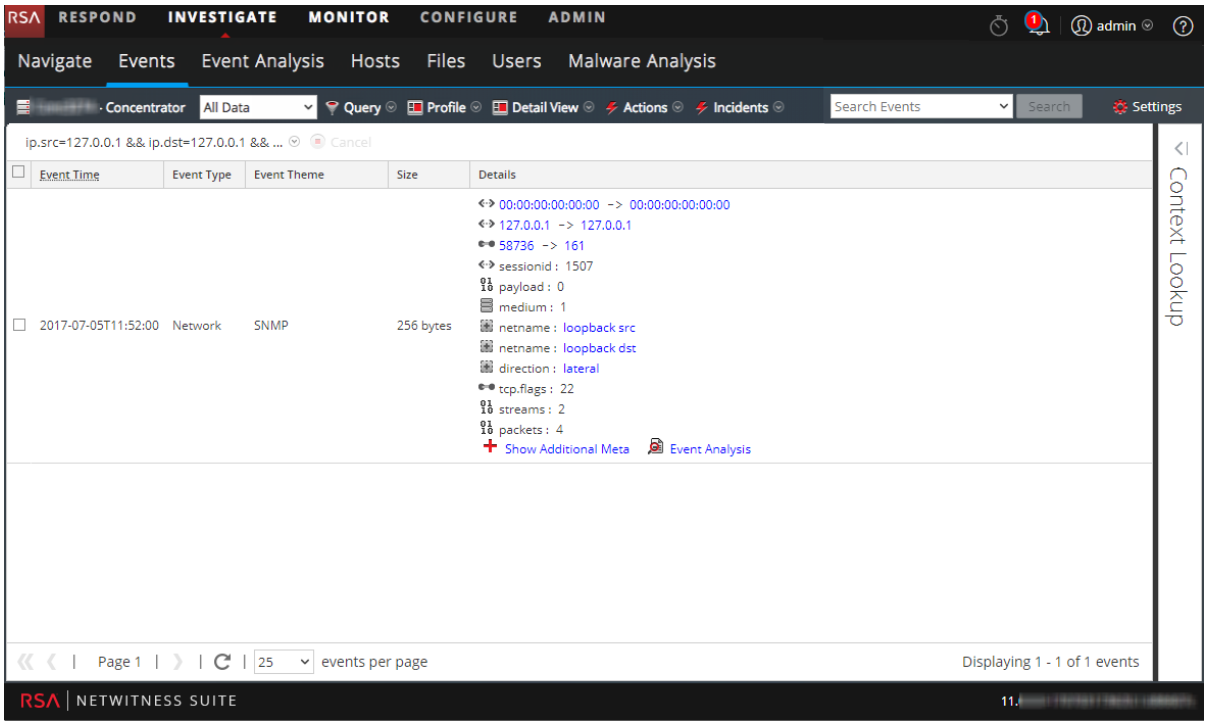
From within the Events view, you can find fragments of a session using the Refocus > Find Session Fragments context menu option. NetWitness Platform composes a query using the source and destination addresses and ports of the selected session and displays all sessions that match that query within the current time window.

To find session fragments:

1. In the **Events** view, right-click any of the source and destination address and port values: `ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport`, and `udp.dstport`) as well as `session.split` values.
   The context menu is displayed.



2. Select **Refocus > Find Session Fragments** or **Refocus New Tab > Find Session Fragments**.
   NetWitness Platform repopulates the Events list with session fragments for a single session within the current time range. Depending on the option you selected, the refocus replaces the current view or opens in a new tab. (All data is used in these examples but is not recommended on production systems).



3. If necessary, adjust the time range to include any session fragments that may precede or follow the current time window. You can tell that the time range needs to be expanded if the fragments occur near the time boundary, especially if the first visible fragment does not have a split value of 0 (or none). Alternately, inspecting the packets of the last visible session may lead you to believe that the session continues. Here is an example:

   a. If you are looking at fragments that are obviously not the first fragment, for example, 1, 2, 3, and 4 in time range 10:30 to 10:35, there should be a fragment 0. You can increase the time range to start earlier (for this example, 10:25) to find the additional fragment.

   b. If the session size of last fragment is close to maximum session size (12 MB in this example), look for additional fragments by increasing the time window to include a later time (for this example, 10:40).
   When all of the session fragments of a network session are included within a single Events list, the list can span multiple pages.

4. (Optional) To export the packets for every session fragment to a single PCAP file, select **Actions > Export All PCAP**.
   A message informs you that the PCAP is being downloaded. When download is complete, PCAP file includes the entire network session that was fragmented.

Querying and Acting on Data in the Navigate and Events Views

This topic describes methods of querying data and acting on results that are common to the Navigate view and the Events view. Analysts can:

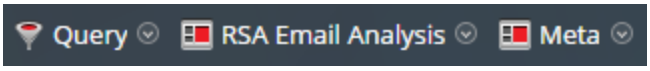
- Use Profiles to Encapsulate Common Areas for Investigation
- Create a Custom Query
- Search for Text Patterns
- View and Modify Queries Using URL Integration
- Launch an External Lookup of a Meta Key
- Look Up Additional Context for a Data Point
- Manage Context Hub Lists and List Values in the Navigate and Events Views
- Reconstruct an Event

Use Profiles to Encapsulate Common Areas for Investigation

Using profiles is a quick and easy way to determine which data is displayed in the Navigate view and the Events view. In the Manage Profiles dialog, you can use a profile to specify which meta groups and column groups are displayed by default, to append queries to an investigation, and to import or export profiles. Built-in profiles make it easier for you to focus on a specific area of interest; for example, selecting the built-in RSA Email Analysis profile automatically selects the meta keys, meta groups, and meta columns that are most useful for investigating email activity. As you become more familiar with the meta keys, you can create your own custom profiles.

Note: Profiles are shared across users in the same NetWitness Platform network. If one user modifies or deletes a profile it has an affect on what is available to the other users.

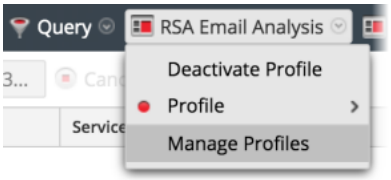
The following figure illustrates the RSA Email Analysis profile selected in the Navigate view or Events view. The profile name is displayed to the right of the Query option. When a profile is currently active, the title of the Profile menu is replaced with the profile name.



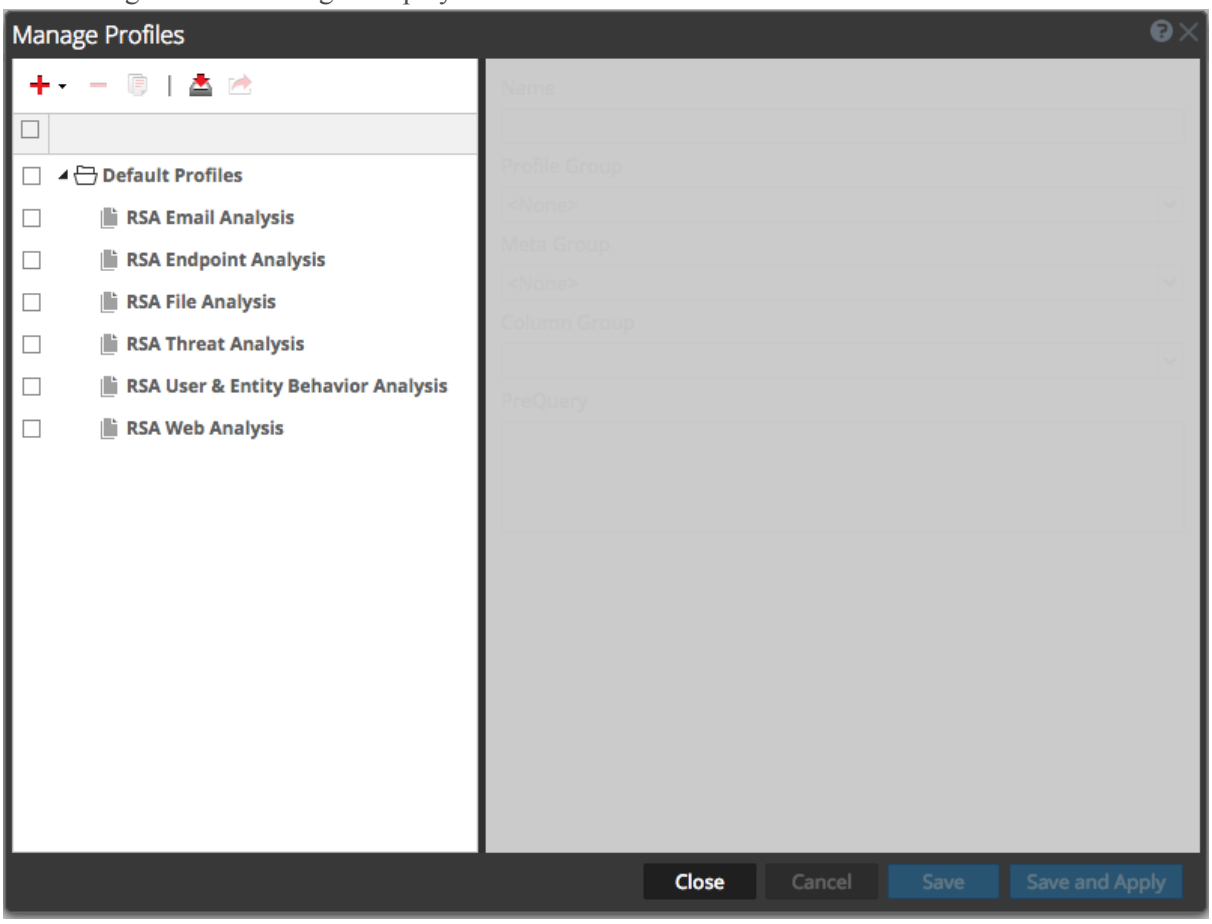
Beginning with Version 11.2, profiles are organized into profile groups. The built-in profiles are in the Default Profiles group, which cannot be edited. Analysts can create new profile groups, which anyone can use. Once created, you can edit a profile group to add profiles, remove profiles, or move profiles from one group to another. When you create a profile, it is not added to any profile group by default.

Navigate to the Manage Profiles Dialog

1. Go to INVESTIGATE > **Events** or **INVESTIGATE > Navigate**. (If the **Investigate** dialog is displayed, select a service and click **Navigate**.)
2. In the toolbar, select **Profile > Manage Profiles**.



The Manage Profiles dialog is displayed.



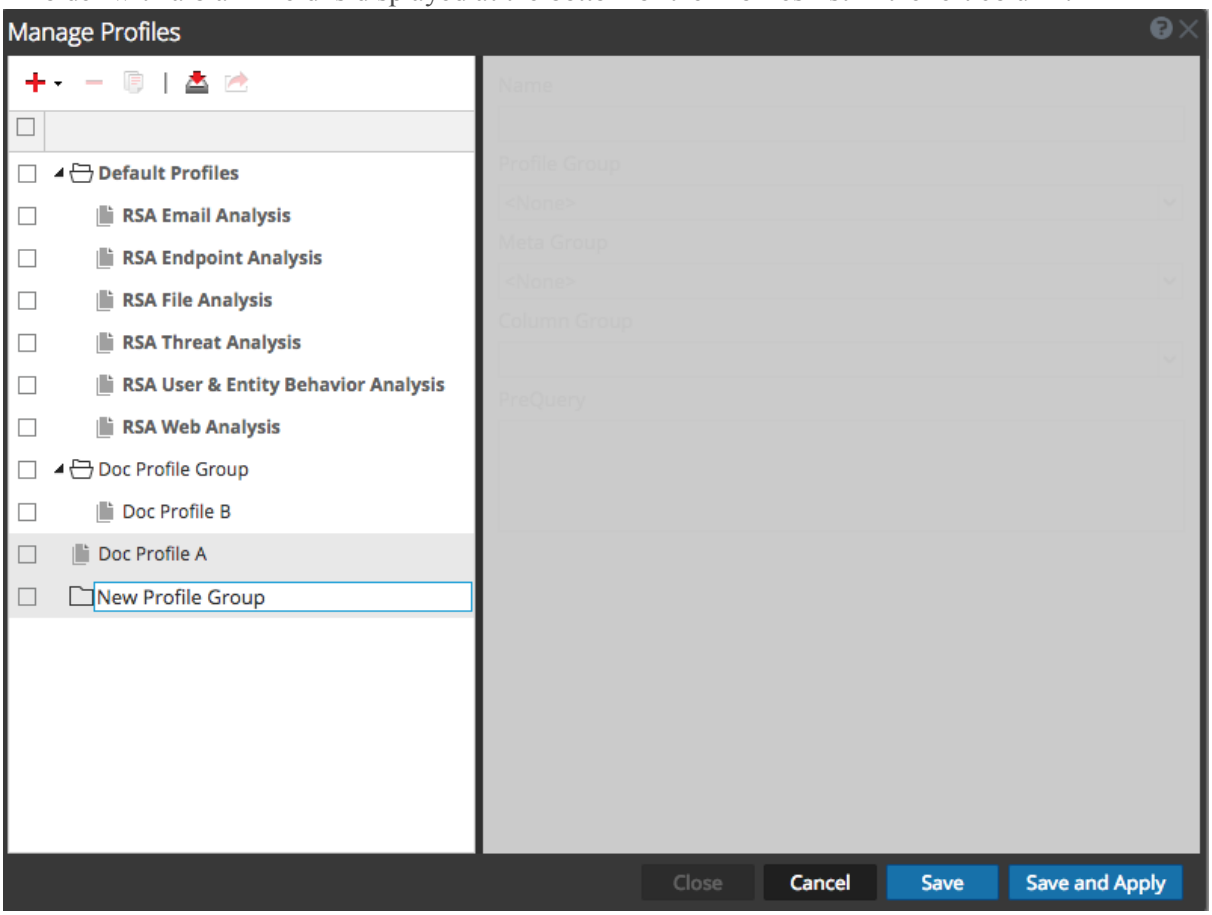
Create, Edit, or Delete a Profile Group (Version 11.2 and Later)

You can create a custom profile group to organize different profiles. Once created, the only edit you can make directly to a profile group is to edit the name of the profile group. To add or remove a profile in a group, edit the profile and assign it to a different profile group as described in Create and Edit Profiles.

1. In the **Manage Profiles** dialog, do one of the following:
   - To select an existing profile group to edit, double-click the profile group.
   - To add a new profile group, click + and select **Add New Profile Group**.

Note: If you want to edit one of the built-in profile groups, click to make an editable copy.

A folder with a blank field is displayed at the bottom of the Profiles list in the left column.



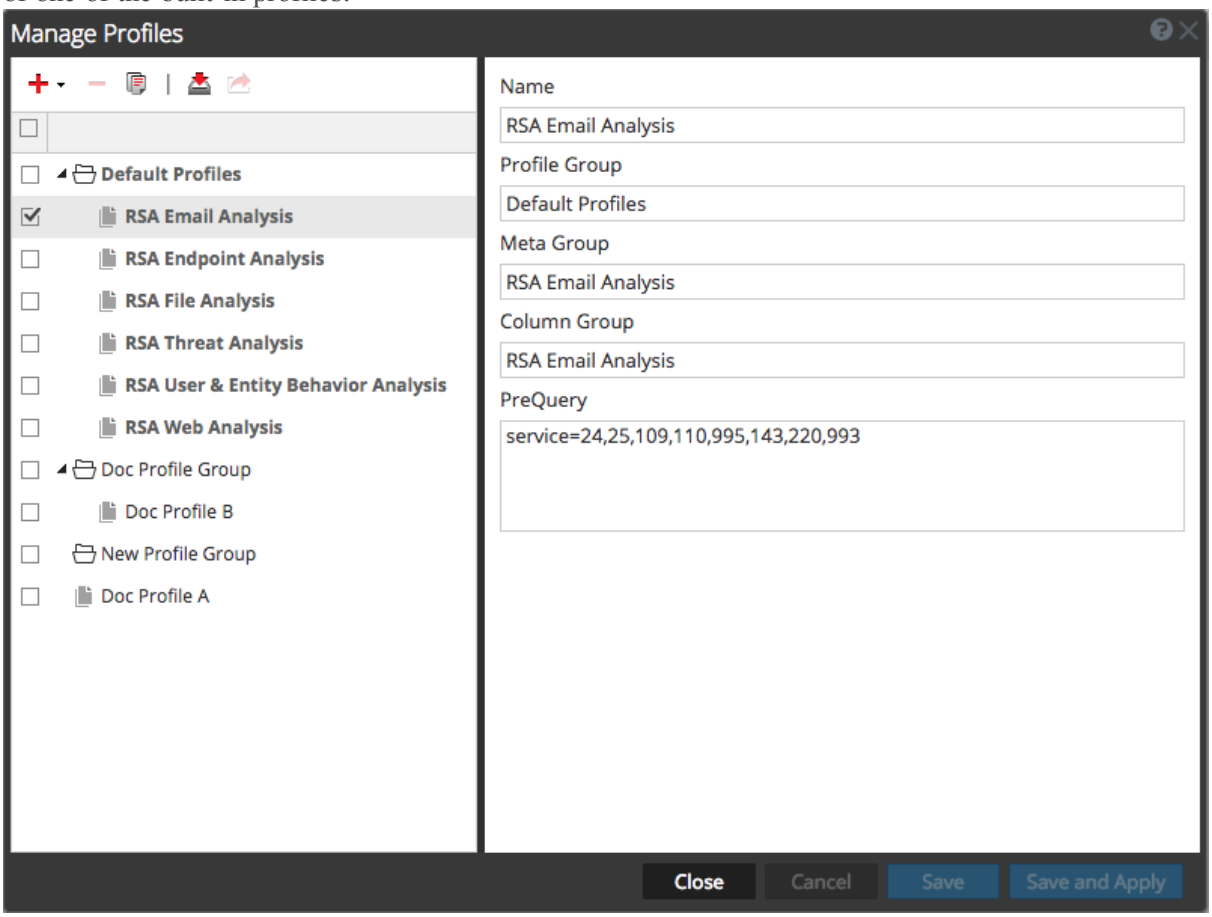
2. To edit or enter the name of the profile group, double-click the Profile Group and type in the entry field. The name must be between 2 and 80 characters.
   The profile group name is applied to a new profile group or to the profile group you edited. The profile group is now available when configuring a profile.
3. To delete a profile group do one of the following:
   - If you want to delete a profile group but keep the profiles, click the checkbox to select the group, uncheck the profiles in the group, and click delete.
   - If you want to delete a profile group and the profiles that the group contains, click the checkbox to select the group, and leave the profiles that you want to delete checked.
     A dialog asks for confirmation that you want to delete the group. If you left the mark in the checkbox next to the profiles, the group and the profiles in the group are deleted. If you unchecked the profiles, only the profile group is deleted and the profiles are moved out of the group and available to add to another profile group.

Create and Edit Profiles

1. In the **Manage Profiles** dialog, do one of the following:
   - To select an existing profile to edit, click the checkbox beside the name.
   - To add a new profile in Version 11.2 and later, click + or click the down arrow next to + and select **Add New Profile**.
   - To create a new profile in versions prior to 11.2, click +.

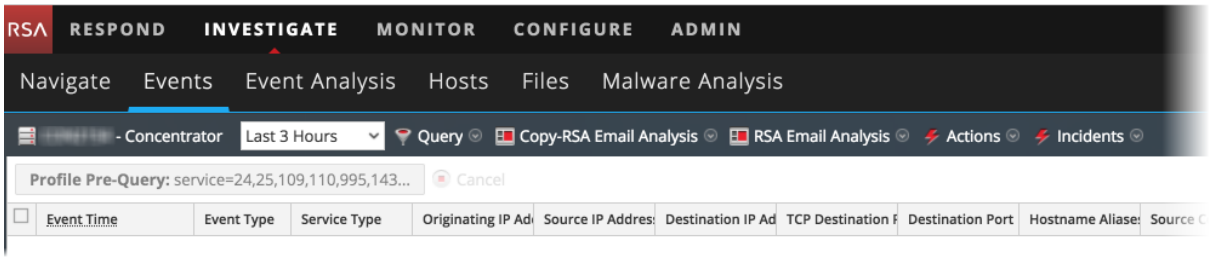
   Note: If you want to edit one of the built-in profiles, click to create a copy, and edit the copy.

   The definition of the profile is available to edit in the right panel. This figure illustrates the definition of one of the built-in profiles.



2. Edit or enter the profile name by typing in the **Name** field. The name must be between 2 and 80 characters.
3. (Optional for Version 11.2 and later) If you want to add the profile to a profile group, select a profile group from the **Profile Group** drop-down list.
   If you select a profile group, the profile is added to the group when you save the changes. If you do not select a profile group, the profile is not part of a group.

4. Select a meta group from the **Meta Group** drop-down list. You can add custom meta groups as described in Manage Meta Groups.
5. Select a column group for the **Column Group** drop-down list. You can add custom column groups as described in Manage Column Groups in the Events View.
6. Type queries to filter results in the **PreQuery** field. PreQuery follows the same syntax as the Query builder. The PreQuery in the figure uses a meta group called **service = 24,25,109,110,995,143,220,993**.
7. Click **Save** to save the profile without using it, or click **Save and Apply** to save the profile and use it immediately.
   If you click **Save and Apply**, a confirmation dialog is displayed before applying the selected profile. For Version 11.2 and later, the PreQuery that you entered in the Manage Profiles dialog is displayed in the breadcrumb.



Delete a Profile

1. In the **Manage Profiles** dialog, select a profile by clicking the checkbox beside the name.

   Note: You cannot delete any of the built-in profiles.

2. Click −.
   A prompt requests confirmation that you want to delete the profile, and the profile is deleted. The option name in the toolbar reverts to **Profile** to show that no profile is in effect.

Change the Active Profile

If you do not see enough results or the right results in the Navigate or Events views, you may have an active profile that is applying a PreQuery. If you do not want to use any profiles, you can click **Deactivate Profile** in the **Profile** drop-down menu.

To use a different profile:

1. In the **Navigate** or **Events** view toolbar, open the **Profiles** drop-down menu.
2. Hover over the **Profile** option to display a drop-down list of available profiles.
3. Select the profile you want to use.
   The profile settings are applied immediately.

If you want to change the active profile from the Manage Profile dialog:

1. In the **Navigate** or **Events** view toolbar, select **Profiles > Manage Profiles**.
   The Manage Profiles dialog is displayed.

2. Select a profile from the left panel and click **Save and Apply**.
   A confirmation dialog is displayed.
3. Click **Yes**.
   The profile settings are applied immediately.

Import Profiles

You can upload or import .jsn files that have been downloaded from another service. When profile groups are exported and then imported, the grouping of profiles is maintained.

1. In the **Manage Profiles** dialog, click in the left panel toolbar.
   The Profile Import dialog is displayed.
2. Click **Browse** or the **Upload File** field to select a file from your computer.
3. When the file is selected, click **Upload**.
   The profile is displayed in the left panel.

Download Profiles

Profiles are downloaded as .jsn files.

1. In the **Manage Profiles** dialog, select one or more profiles from the left panel.
2. In the left panel toolbar, click .
   The download begins immediately.

Create a Custom Query

In the Navigate view or the Events view, you can create a query using dialogs for that offer syntax help with drop-down lists of applicable meta keys or meta entities and operators.

When viewing the drop-down list, you can expand and collapse each meta group to view or hide the individual meta keys in that group. When you select a meta group, NetWitness Platform generates the complex query equal to a query with all of the meta keys in that group ORed together. So if a meta group contains `ip.src` and `ip.dst`, the query generated is `ip.src = <value> OR ip.dst = <value>`. If the meta group contains meta keys that have different meta value types, the value input is disabled and the query uses `exists` statements. For example, a meta group that contains `ip.src`, `ip.dst`, and `alias.host` includes meta keys that have different value types; `ip.src` and `ip.dst` are ip addresses and `alias.host` is text. The generated query is `ip.src exists OR ip.dst exists OR alias.host exists`.

A basic query is in the following form:

```
<metakey> <operator> [<metavalue>]
```

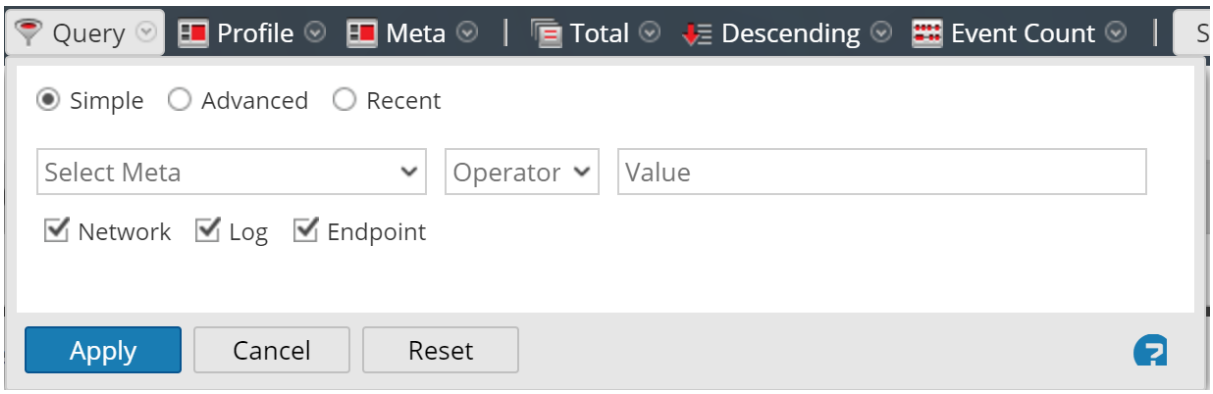
These are a few examples:

```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Create a Query Using the Basic Method

When you create a query using the basic method, drop-down lists of meta keys and operators are displayed.

1. In the **Navigate view** or the Events view toolbar, select **Query.**
   The Query dialog is displayed, with the Simple option selected.

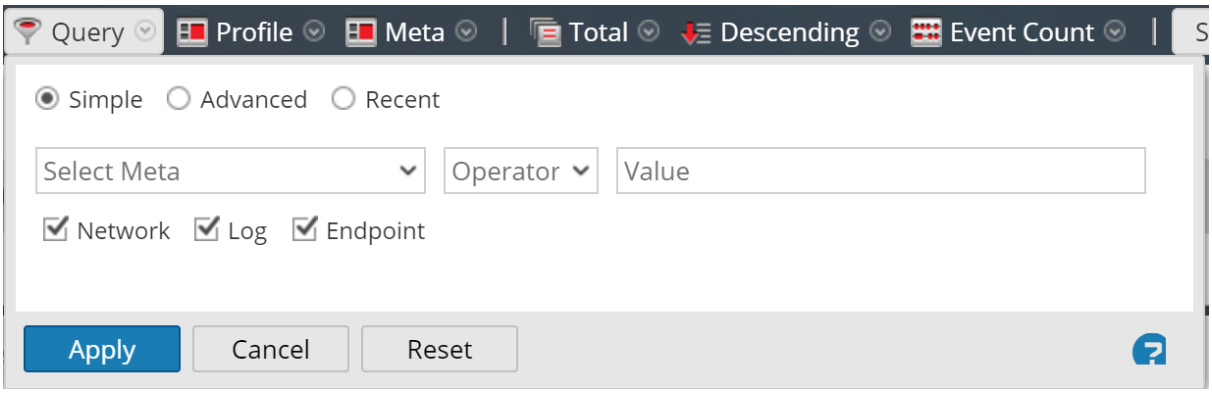


2. In the **Select Meta** field, click to display the drop-down list. The drop-down list has two sections: Meta Groups and All Meta.
3. Select a single meta key under **All Meta** or select a meta group under **Meta Groups**. You can also type in a meta key or meta group in the field.
4. In the **Operator** field, type an operator or click on the drop-down list to select a valid operator.

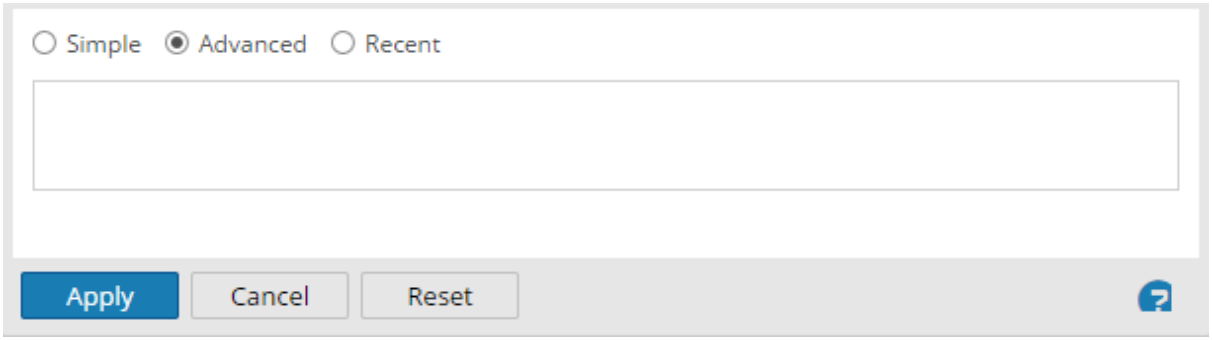
5. (Optional) If you selected an operator that requires a value, for example, =, in the third field type the value for the meta key.
6. In the Network, Log, and Endpoint checkboxes, choose the type of data to query. Do one of the following:
   a. To limit the query to packets select **Network** and de-select **Log** and **Endpoint**.
   b. To limit the query to logs, select **Log** and de-select **Network** and **Endpoint**.
   c. To limit the query to endpoint events, select **Endpoint** and de-select **Network** and **Log**.
   d. To apply the query to packets, logs, and endpoints, select **Network**, **Log**, and **Endpoint**.
7. Do one of the following:
   a. Click **Apply**.
      The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   b. Click **Cancel**.
      The window is closed and no changes are made to the view or current query.

Create a Query Using the Advanced Method

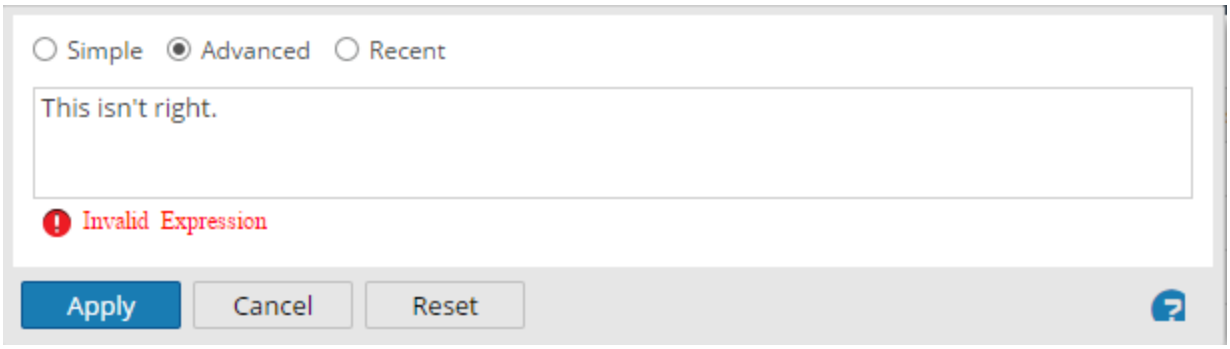
1. In the **Navigate view** or the **Events view** toolbar, select **Query.**
   The Query dialog is displayed.



2. Select **Advanced**.
   The advanced query field is displayed.



3. In the field, create a query, which can include the meta key, operator, and value. When you begin typing a meta key in the field a drop-down list of available meta keys for the selected service is displayed.
4. Select the meta key for your query.
   The display is updated. If the expression is not yet complete, the status indicates that the query is invalid.
5. Continue with an operator, from the drop-down list, then a value if necessary. The display is updated as you continue to enter the query. If you enter an operator, such as **exists** or **!exists**, which does not use the value field, the value field is disabled and the invalid status is cleared. If you enter an operator, such as =, which requires the value field, the invalid status remains until you enter a value. When the query is valid the invalid status is no longer displayed.

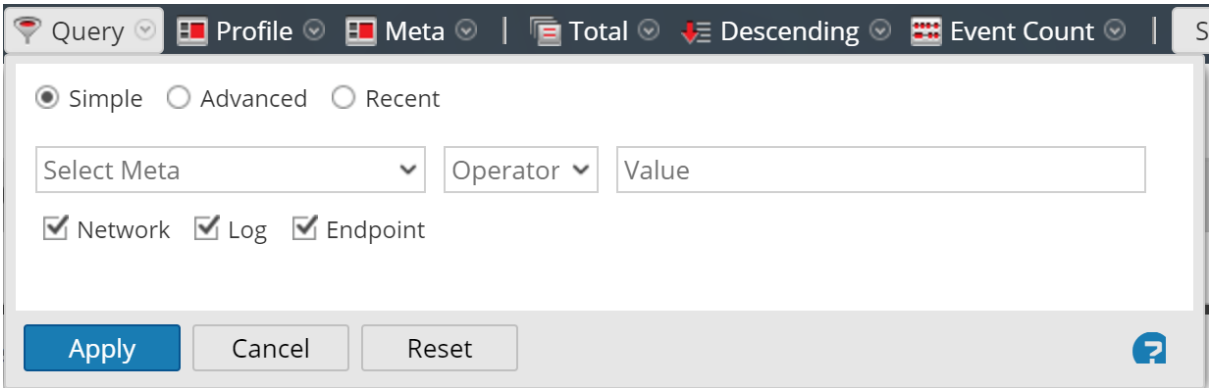


6. Do one of the following:
   - Click **Apply**.
     The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   - Click **Cancel**.
     The window is closed and no changes are made to the view or current query.

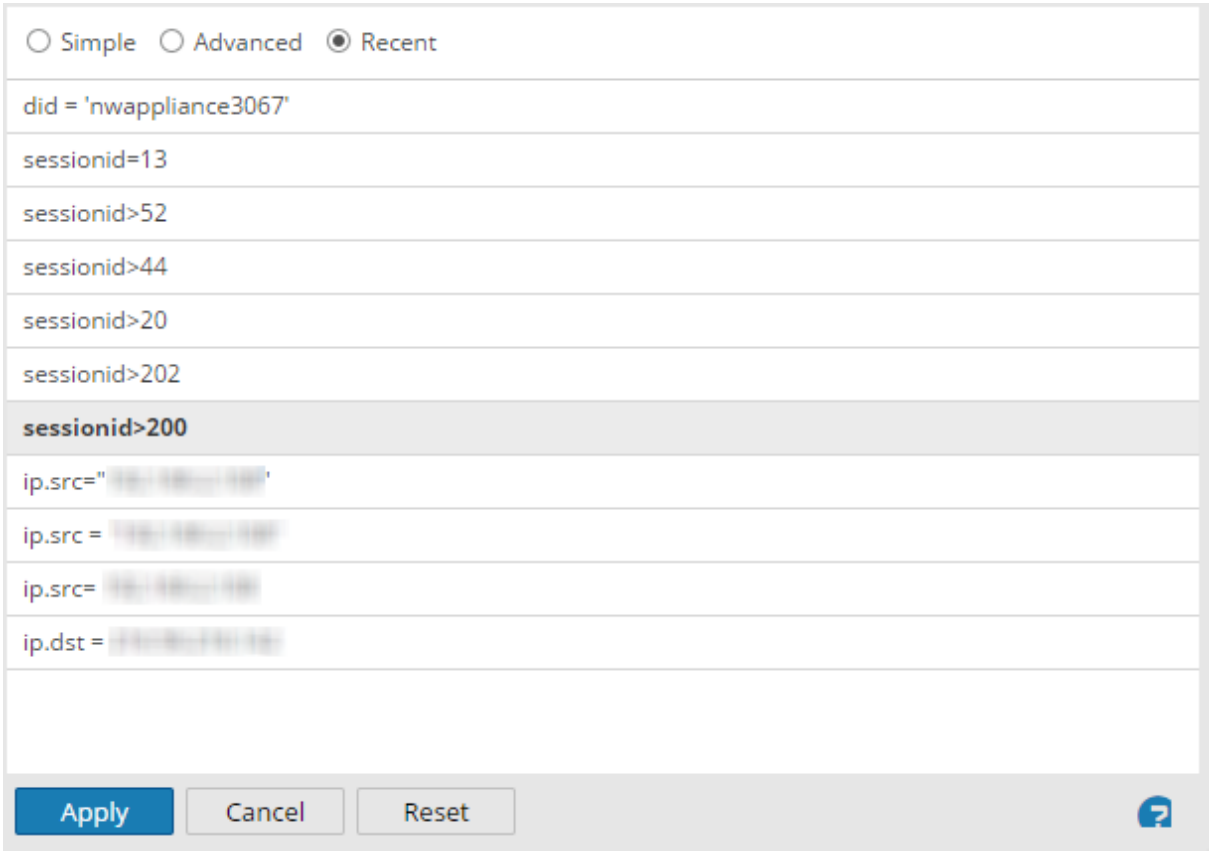
Apply a Recent Query

You can view recent queries and select one to apply to the current service being investigated. To select a recent query:

1. In the **Navigate view** or the Events view toolbar, select **Query.**
   The Query dialog is displayed, with the Simple option selected.



2. Select the **Recent** option.
   The list of recent queries is displayed in the bottom portion of the dialog.



3. In the list of recent queries, click to select a query.
4. Do one of the following:
   - Double-click a query.
   - Select a query and click **Apply**.
     The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   - Click **Cancel**.
     The window is closed and no changes are made to the view or current query.

Search for Text Patterns

You can search for text patterns within the current set of events in both the Navigate view and the Events view. You can perform a keyword text search or do regex (Regular Expression) matching. In the Navigate view, you can click a meta value, such as HTTP, to drill into the data and then enter a search string in the Search field to search for events within that subset of data. The search opens a tab in the Events view, brings your drill and time range forward, and shows your search results. You can also drill into the data using queries before starting a search. To execute the search, enter a search string in the Search box, and press **Enter** or click **Search**.

Note: By default search results are only for exact matches found in indexed data. Only meta values shown as blue links in the Events Detail view are indexed. The regex option must be selected if the value contains a space. To broaden the search change the options in the Search Events drop-down menu.

Keyword Text Search

The text search provides these capabilities:

- Each white space delimited word is ANDed, so that every word must be found, but the order or location position in relation to the other words is irrelevant. For example, if you search on `Mark Albert`, both Mark and Albert must be found in the session, but they need not be together or in any specific order.
- The word OR is special. If you search `Mark OR Albert`, either Mark or Albert must be found in the session to match; both are not required.
- You can mix or match implicit ANDs and ORs together in the search string. The explicit OR has higher precedence than the implicit (whitespace) AND. The following examples make the same logical statement, which requires that both the terms cheese and dumplings be present in a match and one of toaster bread:

```
cheese toast OR bread dumplings
cheese AND (toast OR bread) AND dumplings
```

- You can exclude words from search results using the - operator. For example, searching for `cheese -toast` would return any result that has the word cheese, unless the word toast is also present.
- The keyword search can match metadata stored in the following patterns:
  - **IPv4 and IPv6 addresses**. Any term that can be recognized as an IP address will be converted to the native metadata format so that it can be found in indexed metadata.
  - **IPv4 CIDR ranges**. You can use CIDR notation to locate IPv4 addresses within a range.
  - **Timestamps**. Timestamps are matched against the native time meta, and any additional time meta fields stored with the Time type.
  - **Numbers**. The search function will attempt to automatically identify decimal search terms and match them against numeric meta data fields.

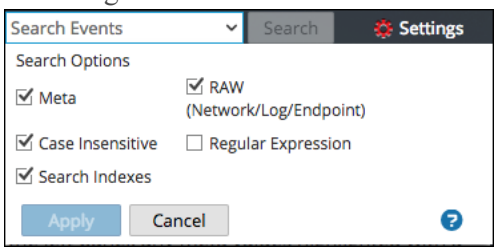
Options Controlling Search Behavior

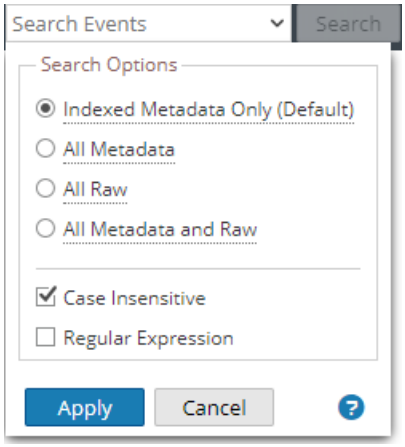
To access the Search box and search options in the Navigate or Events views:

1. You can see the Search Events field in the toolbar.

> **Note:** If you cannot see the Search Events field in the toolbar, click ·· on the right side of the toolbar.

2. Click in the Search field to view the Search Options drop-down menu. In Version 11.2 and later, the menu options are slightly different. The first figure illustrates the menu for 11.1 and below; the second figure illustrates the menu for Version 11.2 and above.





The options selected in this box change how the search is executed. The default search mode is to search indexed metadata and raw data only.

> **Note:** Because the Index or Indexed Metadata Only (default) checkbox is selected by default, the search returns results based on data that is indexed. If you want to search for a complete set of metadata or raw data, select those checkboxes and clear the Index or Indexed Metadata Only (default) checkbox. This type of search takes longer, but it contains a more complete set of data.

The following table describes the Investigation search options.

Feature	Description
Indexed Metadata Only (default) checkbox (Version 11.2 and later) **Index** radio button (Version 11.1)	This search only returns results on indexed data. Searching the index is the fastest way to locate keywords within a large data set. The index search uses any relevant indexes present within your data collection. **Caution:** Substring matches are not located by index searches. If you require substring matches, clear this checkbox and use a non-index search mode.
All Metadata radio button (Version 11.2) **Meta** checkbox (Version 11.1)	Searches the metadata. Your keyword or regex pattern is matched against any parsed metadata.
All Raw radio button (Version 11.2 and later) **RAW** (Network/Log/Endpoint) checkbox (Version 11.1)	Searches the network, log, and endpoint event text. Every event is decoded and content is searched for matches on the keyword or regex pattern. If you select all data with no filters on an Archiver, execution time may be excessive and a warning may be displayed. **Caution:** Searching raw network sessions causes sessions to be decoded, which is very time intensive. You may want to disable raw searches when looking at network-only collections.
All Metadata and Raw radio button (Version 11.2)	Searches the metadata and the log or event text. This option is a combination of two options in Version 11.1: Meta and RAW (Network/Log/Endpoint), which you could select together. In Version 11.2, you can select only one radio button.
Case Insensitive	Ignores case when searching.
Regular Expression	Searches using a Perl regular expression, rather than text. By default executes a text search. To execute a regular expression search, select the Regular Expression option. **Caution:** - Regular expression searches can be very slow. - When combining regular expressions and index search options, the regular expression pattern is matched against unique index values instead of meta values. This produces results faster, but it is not an exhaustive search of all the meta data or raw data.
Apply	Sets the default search options to apply to a search in the Navigate and Events views. This also updates your Investigation preferences in your Profile (Profile > Preferences > Investigation tab). The preferences are saved and effective immediately. You can select search options to use for a particular search without changing your default search preferences.

Regular Expression Search Syntax

A regular expression search uses Perl regular expression syntax, which is documented in detail in http://perldoc.perl.org/perlre.html.

Raw Text Keyword Search

The Log Decoder has the capability to create a raw text index for unparsed log events. This functionality creates metadata items that form a full-text index on downstream services such as Concentrators and Archivers. When you enable the Search Indexes option in your search preferences, your search automatically uses the text index. Note that the text index produces meta items that have a coarse granularity. For example, the default text indexer configuration truncates text terms. By comparing the index matches against raw data, the search engine will find accurate results for your search. However, you can improve search times by disabling the raw search checkbox. If you do so, results will be returned faster, but you may see false positive hits in your search results.

Search Examples

The following examples show searches from the Navigate and Events views.

Search in the Navigate View

To search within the currently displayed data in the Navigate view:

1. Type a search string in the Search field and press **Enter** or click **Search**.
2. To clear the search box and return to the previous Navigate view with results unfiltered by the search, click the **X** in the search box.

Search in the Events View

To search within the currently displayed data in the Events view:

1. Type a search string in the Search box, and press **Enter** or click **Search**.
   The search results are displayed in the Events view. Events that match the search criteria are displayed in the events list. In the Details view and List view, matches are highlighted in the Details column. In addition, when searching RAW, matches are highlighted in the Log view Logs column.
2. If you want to narrow the search, change the query and time.
3. If you want to stop the search and return to the Events view, click **Cancel**.
   Any results that are displayed remain.
4. To clear the search box and return to the normal Events view, click **X** in the search box.

View and Modify Queries Using URL Integration

NetWitness Investigate includes an External URL Integration that facilitates integration with third-party products by allowing a search against the NetWitness Platform architecture. By using a query in a URI, you can pivot directly from any product that allows custom links, into a specific drill point in the Investigate view. This integration provides an internal presentation of the user's query.

URL Integration allows the user to identify the service either by the host id or by the service and port, as defined in NetWitness Platform. If NetWitness Platform is unable to resolve the service, the analyst is redirected to the Navigate view, showing the Service selection dialog. Once the service is selected, the Navigate view is loaded with the drill point, defined by the query.

Service Id Known

When the ID of the service to use for an investigation is known, the format for entering a URI using a URL-encoded query is:

```
http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

where

- `<sa host: port>` is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is needed only if access is configured over a non-standard port through a proxy.
- `<deviceId>` is the internal Service ID in the NetWitness Platform instance for the service to query against. The service ID can be represented only as an integer. You can see the relevant service ID from the URL when accessing the Investigation view within NetWitness Platform. This value changes based on the service being connected to for analysis.
- `<encoded query>` is the URL-encoded NetWitness Platform query. The length of query is limited by the HTML URL limitations.
- `<start date>` and `<end date>` define the date range for the query. The format is `<yyyy-mm-dd>T<hh:mm:ss>Z`. The start and end dates are required. If no date is provided then the user defaults for that service are used. Relative ranges (for example, Last Hour) are not supported. All times are run as UTC.
  For example:
  `http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Host and Port Known

When the host and port of the service to use for investigation is known, the format for entering a URI using a URL-encoded query is:

```
http://<sa host:port>/investigation/<device host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

where

- <sa host: port> is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is needed only if access is configured over a non-standard port through a proxy.
- <device host:port> is the host and port of a service defined in NetWitness Platform instance for the service to query against. NetWitness Platform attempts to resolve the host and port as a service ID defined in NetWitness Platform.
- <encoded query> is the URL-encoded NetWitness Platform query. The length of query is limited by the HTML URL limitations.
- <start date> and <end date> define the date range for the query. The format is <yyyy-mm-dd>T<hh:mm:ss>Z. The start and end dates are required. If no date is provided then the user defaults for that service are used. Relative ranges (for example, Last Hour) are not supported in this version. All times are run as UTC.
  For example:
  `http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Examples

These are query examples where the NetWitness Server is 192.168.1.10 and the deviceID is identified as 2.

All activity on 03/12/2013 between 5:00 and 6:00 AM with a hostname registered

- Custom Pivot: `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

All activity on 3/12/2013 between 5:00 and 5:10 PM with http traffic to and from IP address 10.10.10.3

- Custom Pivot: `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Encoded Pivot Dissected:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z`

Additional Notes

Some values may not need to be encoded as part of the query. For example, commonly the IP src and dst is used for this integration point. If leveraging a third-party application for integration of this feature, it is possible to reference those without encoding applied.

Launch an External Lookup of a Meta Key

This topic provides instructions for using out-of-the-box Investigate plugins to launch an external lookup of specific meta keys using tools external to NetWitness Platform while investigating data in the Navigate view or Events view.

Analysts can use out-of-the-box external lookups to save time during investigations. The out-of-the-box lookups are available by right-clicking one of the these meta keys: IP address (`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`), `host (alias-host, domain.dst)`, `client`, and `file-hash`.

For all `ip` and `host` meta keys, the following lookups are built in to NetWitness Platform:

- Google Malware: Opens a Google Malware search in a new tab.
- SANS IP History: Opens a SANS IP History search in a new tab.
- McAfee SiteAdvisor: Opens a McAfee SiteAdvisor search in a new tab.
- Endpoint Thick Client Lookup: Opens a search in the NetWitness Endpoint Thick Client in a new tab.
- BFK Passive DNS Collection: Opens a BFK Passive DNS collection search in a new tab.
- CentralOps Whois for IPs and Hostnames: Opens a CentralOps Whois search for IPs and hostnames in a new tab.
- Malwaredomainlist.com Search: Opens a Malwaredomainlist.com search in a new tab
- Robtex IP Search: Opens a RobtexIP search in a new tab.
- ThreatExpert Search: Opens a ThreatExpert search in a new tab
- IPVoid Search: Opens a UrlVoid Search in a new tab n a new tab

For the `file-hash` and `alias-host` meta keys, the Google lookup opens a Google search in a new tab.

For the `client` meta key, the NetWitness Endpoint Lookup option opens an Endpoint Thick Client in a new tab if the client is installed on the same system on which the browser is being used.

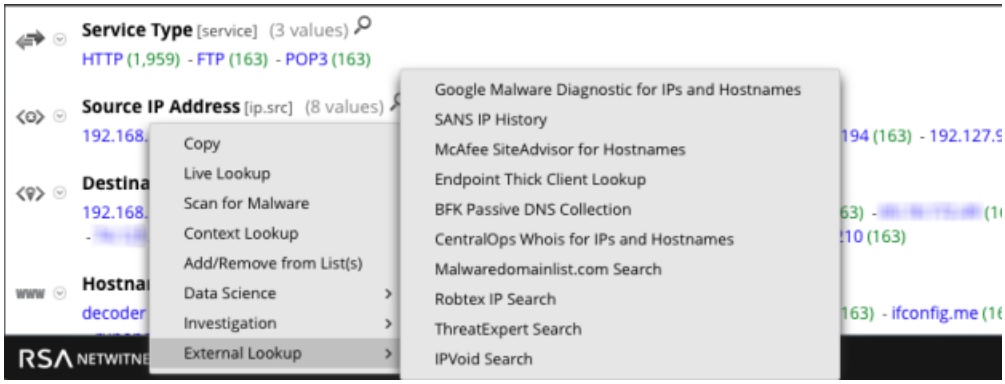
Administrators can add additional external lookups and other custom actions as described in "Add Custom Context Menu Actions" in the *System Configuration Guide*.

Launch an Endpoint Thick Client Lookup

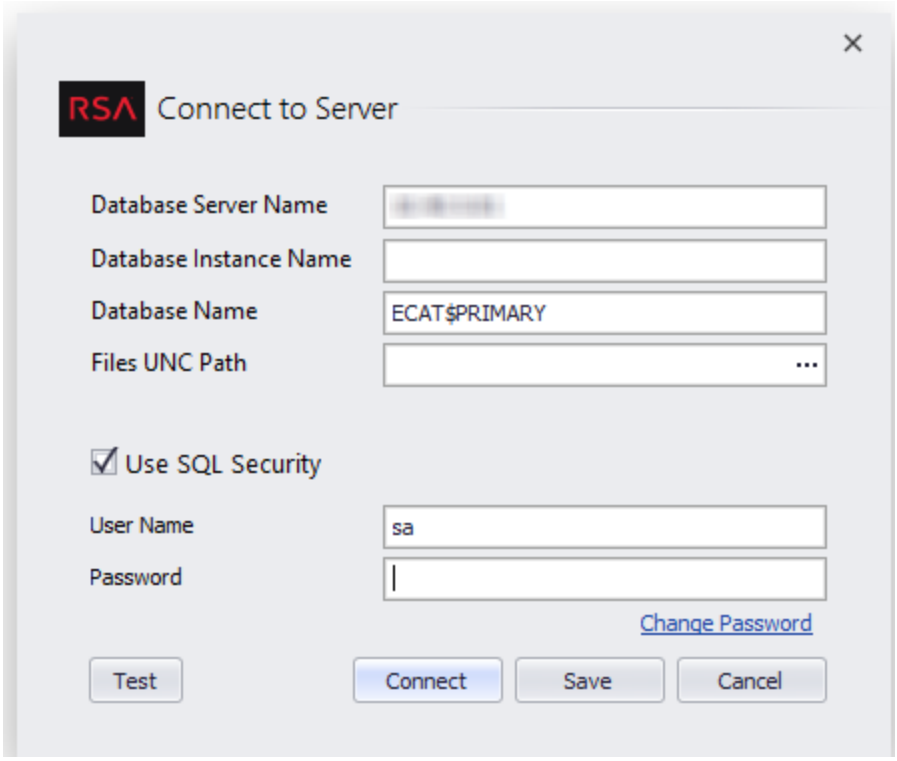
To launch an Endpoint Thick Client lookup of data from the Navigate view:

1. Right-click a meta value for one of the following meta keys: `ip-src, ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`, `alias-host`, `domain.dst`, or `client`.

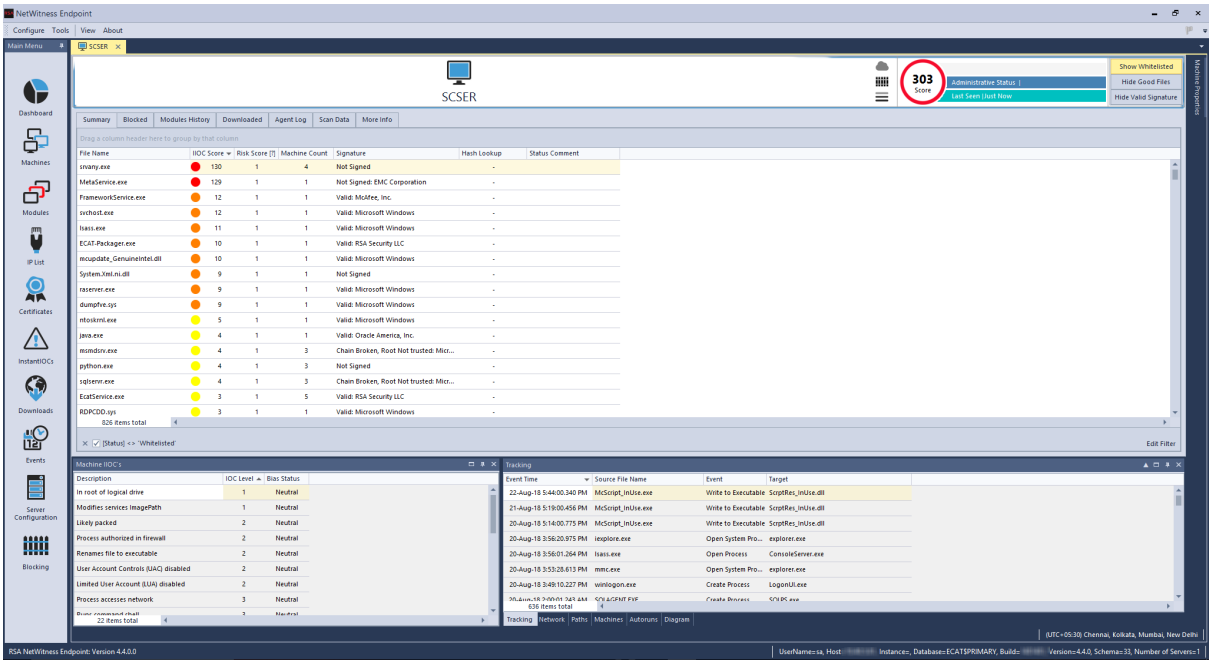
2. Select **External Lookup** in the context menu.
   A submenu of external lookup options is displayed.



3. Select **Endpoint Thick Client Lookup**.
   The Connect to Server dialog is displayed.



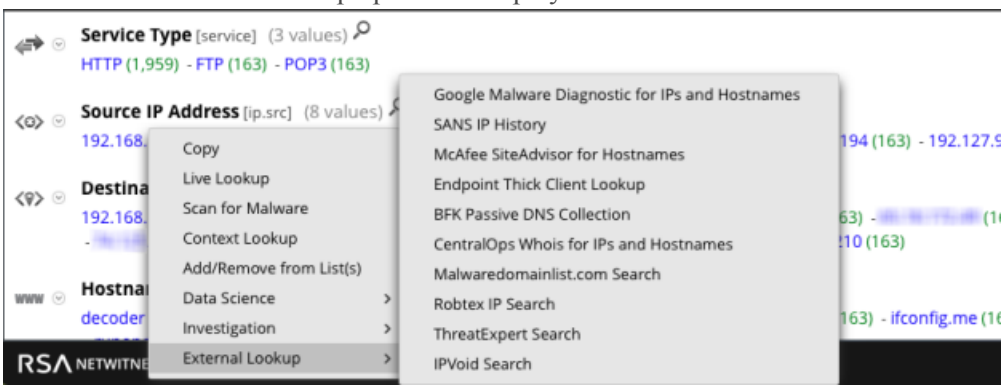
4. Enter the user name and password required to log in to the Endpoint Thick Client, and click **Connect.**
   The drill point opens in NetWitness Endpoint.



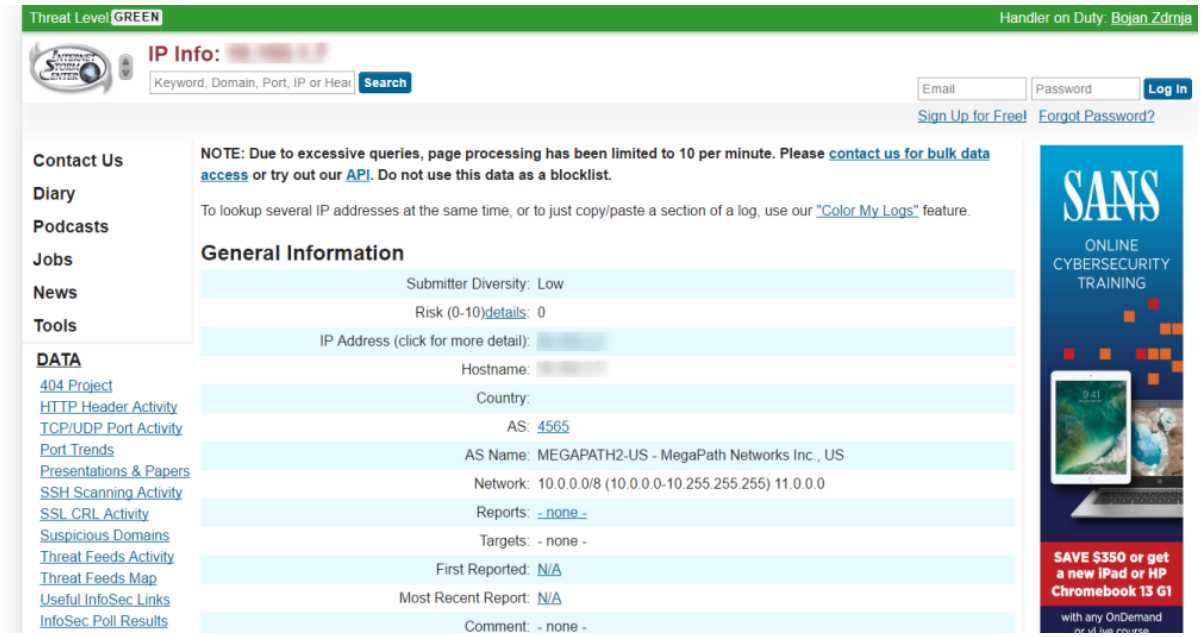
Launch Other External Lookups

To launch an external lookup of data from the Navigate view (other than NetWitness Endpoint Thick Client Lookup):

1. Right-click a meta value for one of the following meta keys: `ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`, `alias-host`, `domain.dst`, or `client`.
2. Select **External Lookup** in the context menu.
   A submenu of external lookup options is displayed.



3. Select one of the lookup options.
   The selected meta value opens in the selected lookup, for example, if you selected SANS IP History, the drill point information is displayed in SANS Internet Storm Center.



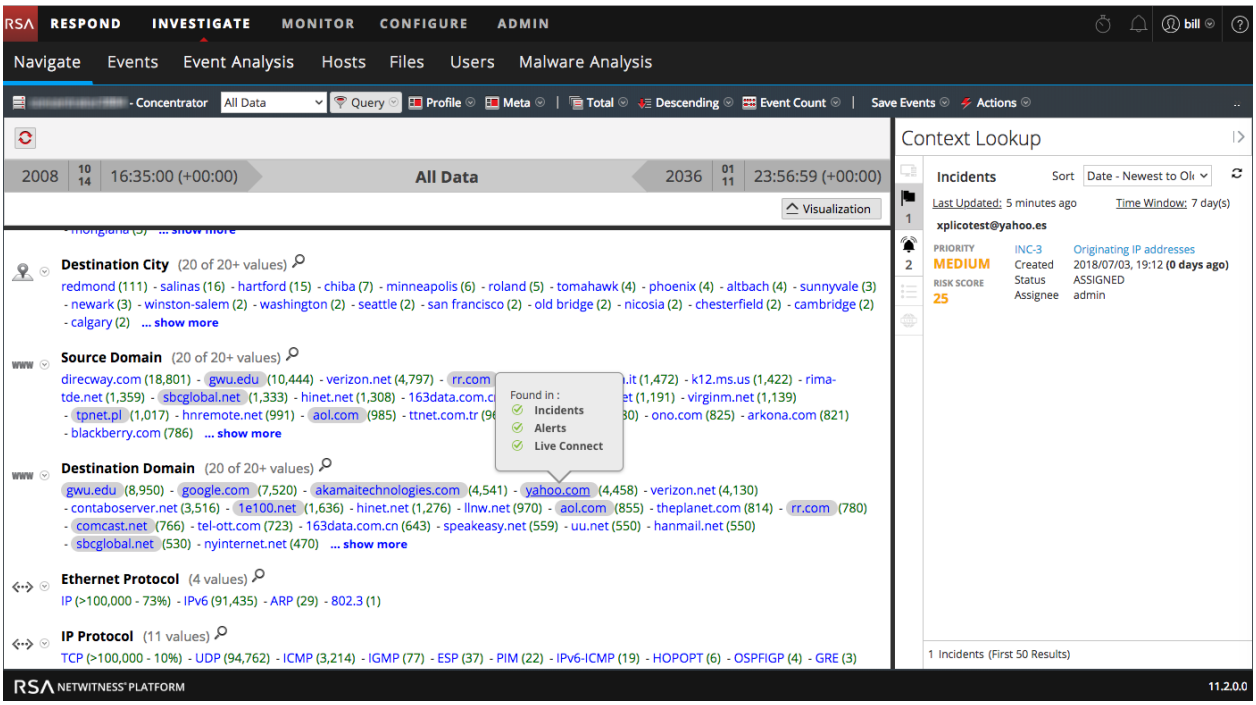
Look Up Additional Context for a Data Point

From the Events view and the Navigate view, you can look up details and intelligence about elements associated with an event in the Context Hub. (In Version 11.2 and later, you can also look up additional context in the Event Analysis view as described in Look Up Additional Context in the Event Analysis View.) These elements, or entities, are identifiers, such as an IP address, a user name, a host name, a domain name, a file name, or a file hash. The data from configured sources, such as RSA NetWitness Endpoint, can help you understand what is happening.

Note: To enable viewing of contextual information, your administrator must add the Context Hub service in RSA NetWitness Platform and configure data sources for the Context Hub service as described in the *Context Hub Configuration Guide*. Analysts also need a role with the permission `Context Lookup` as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

The Context Hub is a centralized service that aggregates data about entities from multiple configurable data sources. This data can extend your investigation with additional context beyond the immediate results of a specific query. For example, the Context Hub can tell you if a given entity has been mentioned in any incidents, alerts, feeds, or community intelligence publications.

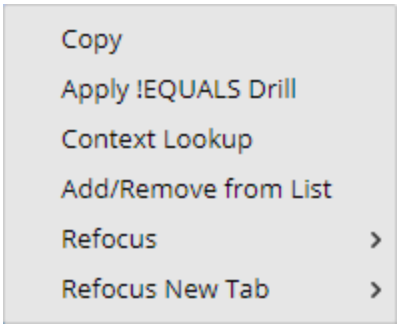
In the Navigate view and Events view, entities that have associated context data available are highlighted with a gray background; hovering over an entity displays a hover box giving a summary of the available data. When you right-click the entity, the Context Hub queries the configured data sources for relevant information, and the Context Lookup panel opens from the right side of the browser window. The Context Lookup panel is populated with the information from the Context Hub as it becomes available. You can perform another lookup by right-clicking on another entity, and the Context Lookup panel is updated with that entity's information.



In the Context Lookup panel, you can view and explore individual data sources for further investigation. For a detailed description of the information displayed for each data source, see Context Lookup Panel.

To view information in the Context Lookup panel in the Navigate view or the Events view:

1. Hover over different meta values to see the data sources for which data is available.
   A hover box displays a list of the data sources that have context data available for meta value. These are the possible data sources: NetWitness Endpoint, Incidents, Alerts, Hosts, Files, Feeds, and Live Connect.
2. Right-click a meta value, and click **Context Lookup** in the drop-down menu to open the Context Lookup panel.

   The Context Lookup panel opens from the right side of the browser window. The Context Lookup panel is populated with the information from the Context Hub as it becomes available.
3. To perform actions from the Context Lookup panel, right-click an entity such as IP address.
   The following options are available: Open Link in New tab, Query in Investigate, Copy Link, Paste, Google Lookup, Virus Total Lookup, and Query in Endpoint.
4. To close the Context Lookup panel, click ✉ in the panel.

Manage Context Hub Lists and List Values in the Navigate and Events Views

Analysts can add lists and list values for Context Hub enrichment in the Navigate view and the Events view. (In Version 11.2 and later, analysts can add lists and lists values in the Event Analysis view as described in Look Up Additional Context in the Event Analysis View.)

When the Context Hub service is enabled and configured, NetWitness Platform provides enrichment data from NetWitness Respond, custom lists, and NetWitness Endpoint directly in the Navigate view and Events view. A visual cue highlights meta values for which enrichment data is available in the Investigate views, and you can click on the highlighted value to look up the contextual information and intelligence.

In addition, from the Values panel in the Navigate view and from the Events view, you can view lists, edit meta values in an existing list, or create a new list. When you add meta values to a list, you can investigate the meta values using the context lookup option.

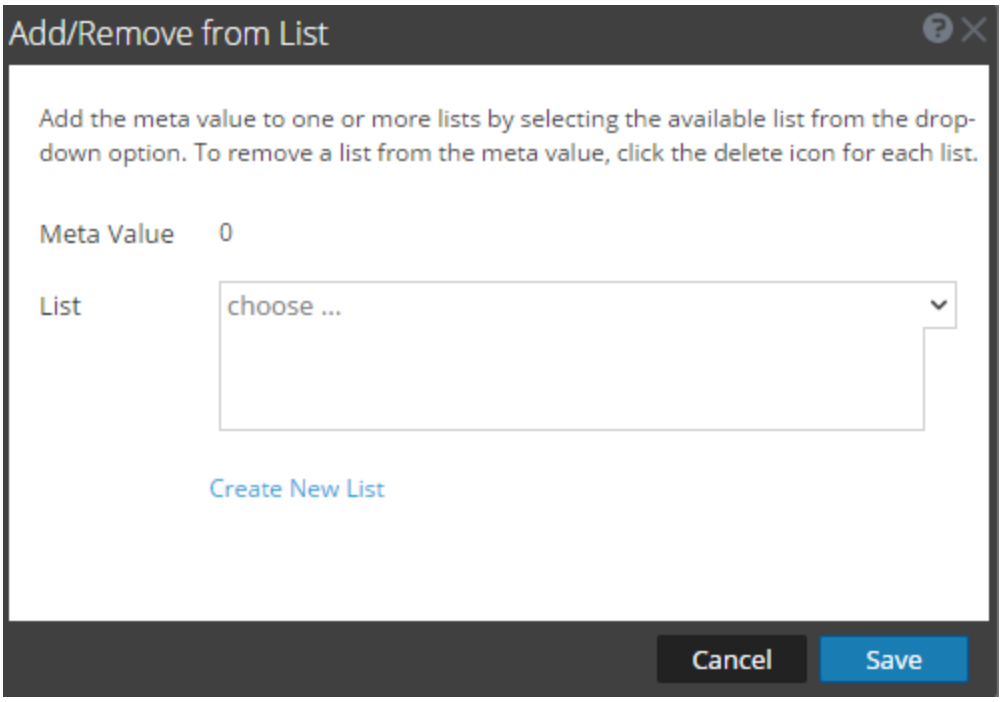
For an analyst to manage lists in Investigate, the administrator must:

- Enable the Context Hub service.
- Assign an analyst role with permission `Manage List from Investigation` to the user who will perform Context Lookup from Investigation views.
- Configure appropriate roles and permissions as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Add Meta Values to an Existing List

To add a meta value to an existing list in Context Hub:

1. While investigating a service in the **Navigate** view or the **Events** view, right-click a meta value (for example, values under Source IP, Destination IP, or Username) and select **Add/Remove from List** in the context menu.
   The Add/Remove from List dialog is displayed.



2. In the **List** field, select one or more lists from the drop-down option to which the meta value must be added.
3. Click **Save**.
   The meta value is added to the selected lists.

Remove a Meta Value from a Context Hub List

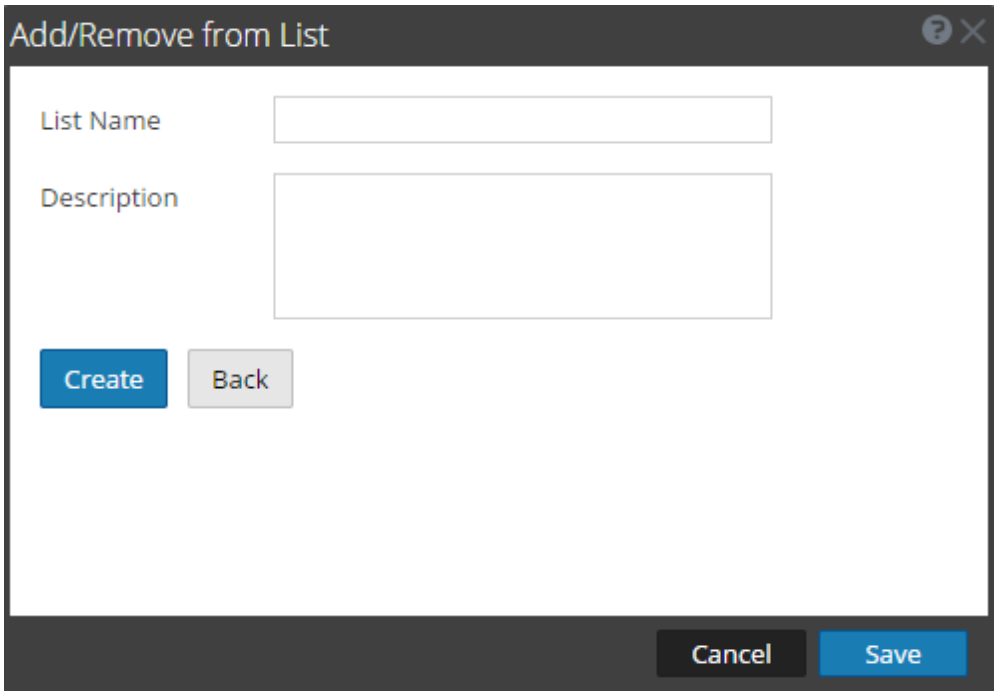
To remove a meta value from list:

1. In the **Add/Remove from List** dialog, in the **List** field, view the lists which include the meta value.
2. Click the delete icon (x) for each list that should not include the meta value.
3. Click **Save**.
   The meta value is removed from the deleted list.

Create a New List

To create a Context Hub list in Investigate:

1. In the **Add/Remove from List** dialog, click **Create New List**.



2. In the **List Name** field, enter an unique name for the list.
3. In the **Description** field, enter the description of the list.
4. Click **Create** to create the list.
5. Click **Save** to add the meta value to the created list.
   These lists are considered as data sources for retrieving context information.

Reconstruct an Event

When viewing a list of events in Events view, you can safely create a reconstruction of the event in a readable form that matches the original. By default, the initial view of a reconstructed event is the most suitable format (Best Reconstruction); for example, web content is reconstructed as a web page; an IM conversation is displayed with both parts of the conversation. Each user can select a different default reconstruction in the Profile > Preferences view.

You can also open a reconstruction from the Navigate view if you know the Event ID of the event.

In the reconstruction, you can:

- Select event information to view. Possible values are: request data, response data, both request and response data.
- Select the reconstruction type: details, text, hex, packets, web, mail, or IM.
- Export raw logs.
- Export the event as a PCAP file.
- Extract any files available in the event.
- Extract all the meta data associated with the event.

  Caution: Be careful when clicking a link to a file in the Reconstruction. If your system has an application associated with the file, or the browser is capable of opening them, and the attachments are malicious, they can negatively affect your system.

- Display the event in a separate window or tab (depending on your browser configuration).
- If you are viewing the reconstruction as a preview in the current view, you can page forward to the next event and back to the previous using the navigation buttons in the bottom left corner.

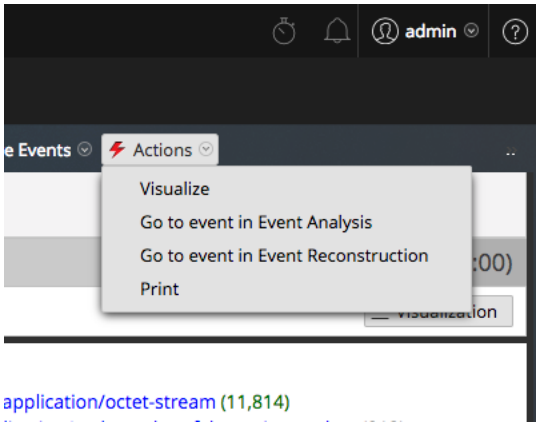
Note: Reconstruction Settings and Reconstruction Cache Settings allow an administrator to manage application performance for Investigation. As analysts reconstruct sessions that they are investigating, two situations can affect performance and results.
-Some events can be very large and contain many thousands of source packets. Reconstructing these types of sessions can degrade application performance.
- In some cases, the reconstruction cache can present incorrect content; for this reason, NetWitness Platform cleans cache that is older than a day every 24 hours. Between the daily cache cleanings, certain actions my result in stale cache being used for a reconstruction, and if the need arises, administrators can manually clear cache for one or more services that are connected to the current NetWitness Server.

Reconstruct an Event from the Navigate View

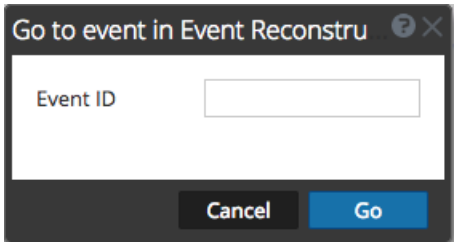
You can reconstruct an event directly from the Navigate view given a known Event ID. You can use this option without executing a query as you usually do when beginning an investigation. A service and time range must be selected to be able to jump directly to an event using just its `eventid`.

To view a reconstruction or event analysis directly from the Navigate view:

1. Go to **INVESTIGATE > Navigate** and select **Actions > Go to event in Event Analysis** or **Go to event in Event Reconstruction**.



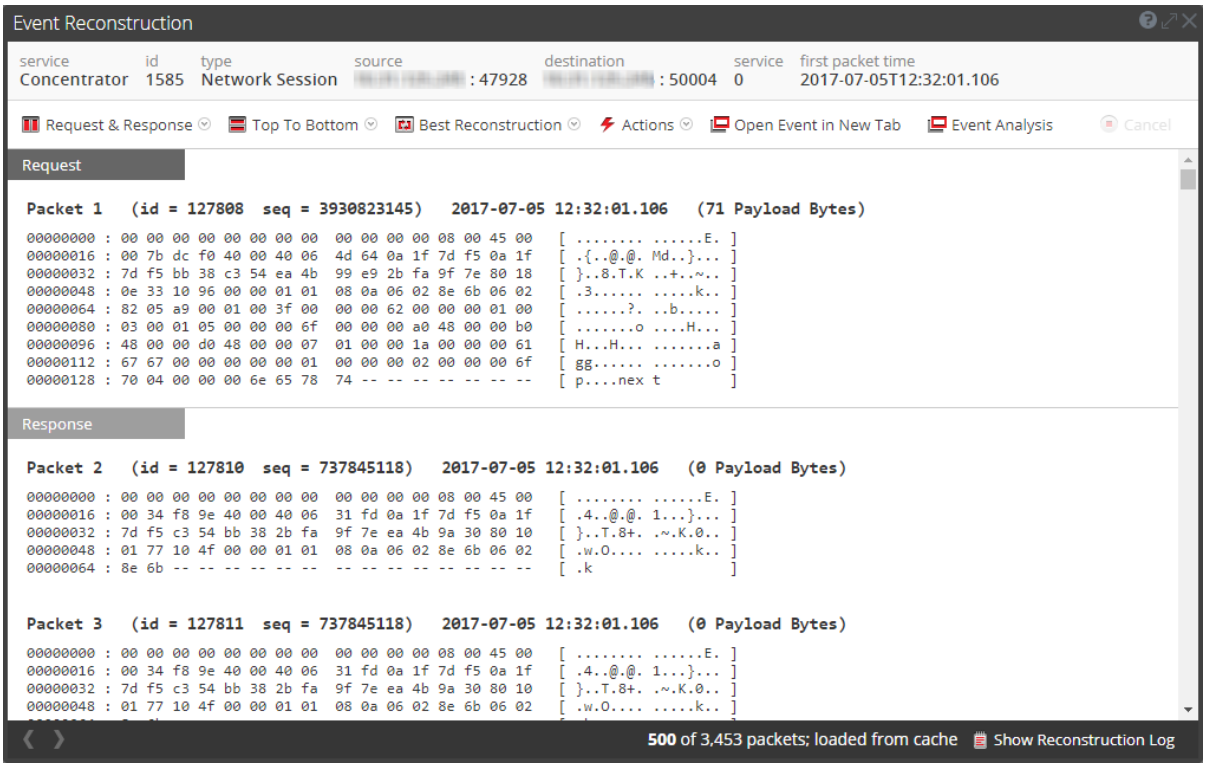
The Go to event dialog is displayed. There are two dialogs, one for Event Analysis and one for Event reconstruction. Both ask for the Event ID.



2. In the **Event ID** field, type the ID and click **Go**.
   The specified event is reconstructed in the Event Reconstruction view or the Event Analysis view.

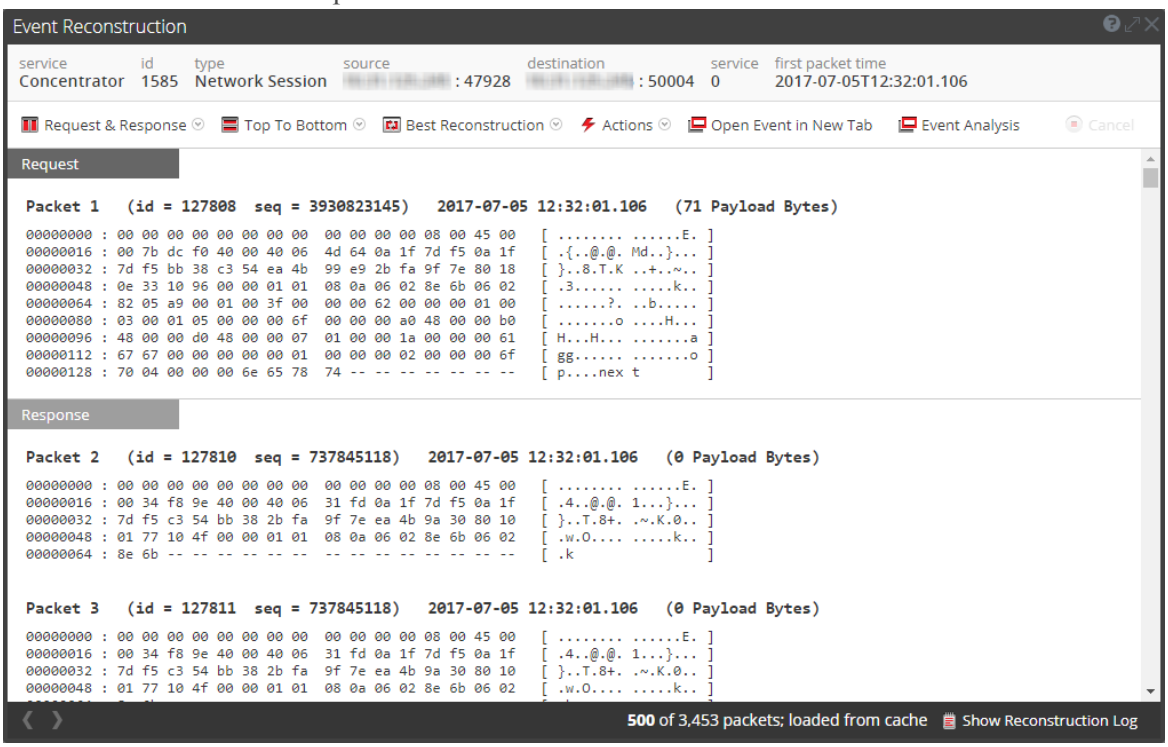
Reconstruct an Event

1. Click the count (the green number following a value) for a value in the Navigate view to open a drill point in the **Events** view.
2. To show all meta data, click + Show Additional Meta .
3. To open an event reconstruction in the Events view, select an event to reconstruct and select **Actions > View Event > Preview Inline**.
   The Event Reconstruction opens in a popup window in the same view. By default, NetWitness Platform displays the best reconstruction for the event determined by the event content or the reconstruction that you have selected in the Default Session View setting for Investigation. You can use the options in the Event Reconstruction toolbar to change the reconstruction method, view side-by-side results, export an event, open an email attachment, extract files, and open the event in a new tab. The toolbar options vary depending on the type of event being reconstructed (network event, log event, or endpoint event). This is an example of the reconstruction for a network event.



4. To preview a reconstruction of the next event, click in the lower left corner of the reconstruction or to preview a reconstruction of the previous event, click .
5. To open an event reconstruction in a new tab, do one of the following:
   a. In the **Events** view, select an event to reconstruct and select **Actions > View Event> Open in New Tab**.
   b. In the **Event Reconstruction** toolbar of previewed reconstruction, click **Open Event in New Tab** in the toolbar.

The Event Reconstruction opens in a new tab.



View Side by Side or Top to Bottom

To select the way requests and responses for an event are displayed:

1. In the **Event Reconstruction** toolbar, click **Top to Bottom** or **Side by Side**.
2. In the drop-down menu, select the information you want to see in the event: **Side by Side** or **Top to Bottom.**
   The reconstruction is refreshed with the selected information.

Select Event Information to View

To select what event information to view:

1. In the **Event Reconstruction** toolbar, click **Request & Response**.
2. In the drop-down menu, select the information you want to see in the event: **Request & Response**, **Request**, or **Response**.
   The reconstruction is refreshed with the selected information.

Select Event Reconstruction Type

To select the reconstruction type for an event:

1. In the **Event Reconstruction** toolbar, click **Best Reconstruction**.
2. In the drop-down menu, select the reconstruction type to view: **meta**, **text**, **hex**, **packets**, **web**, **mail**, or **files**.
   The reconstruction is refreshed with the selected reconstruction type.

Open or Download an Email Attachment

When viewing a reconstruction of an email that has attachments, you can open supported file types or download the files to the local system.

Caution: Be careful when selecting file attachments. If your system has an application associated with the file attachments, or the browser is capable of opening them, and the attachments are malicious, they can negatively affect your system.

To open or download email attachments:

1. In the **Event Reconstruction** toolbar, select the **View** drop-down and select **View Mail**.
   The Event Reconstruction is displayed.
2. In the **Event Reconstruction** section of the email, click the Attachment.
   If the file type is supported by the browser, the attachment will open in a new tab.
   If the file type is not supported, the Download dialog is displayed so that you can download the attachment.

Export an Event as a PCAP File

The PCAP export option downloads the sessions for the current time range and drill point to a PCAP file. To export an event as a pcap file:

1. In the **Event Reconstruction** toolbar, click **Actions**.
2. Click **Export PCAP**.
3. A confirmation dialog is displayed.
4. Click **OK**.
   The job is scheduled and when complete the PCAP is downloaded to the local file system. In the Profile > Jobs tab, you can download the PCAP.

Extract Files from a Reconstructed Event

The Extract Files option extracts and downloads the files associated with the event. To extract files:

1. In the **Event Reconstruction** toolbar, click **Actions**.
2. Click **Extract Files**.
   The File Extraction dialog is displayed.
3. Select the types of files to extract, and click **OK**.
4. The job is scheduled and when complete the selected file types are downloaded to the local file system. In the Profile > Jobs tab, you can download the files.

Analyzing Raw Events and Metadata in the Event Analysis View

Analyzing raw events and data in the same view is possible when working in the Event Analysis view. After you understand Reconstruction Types in the Event Analysis View, you can:

- Filter Results in the Event Analysis View
- Examine Events in the Event Analysis View
- Download Data in the Event Analysis View
- Act on Data in the Event Analysis View

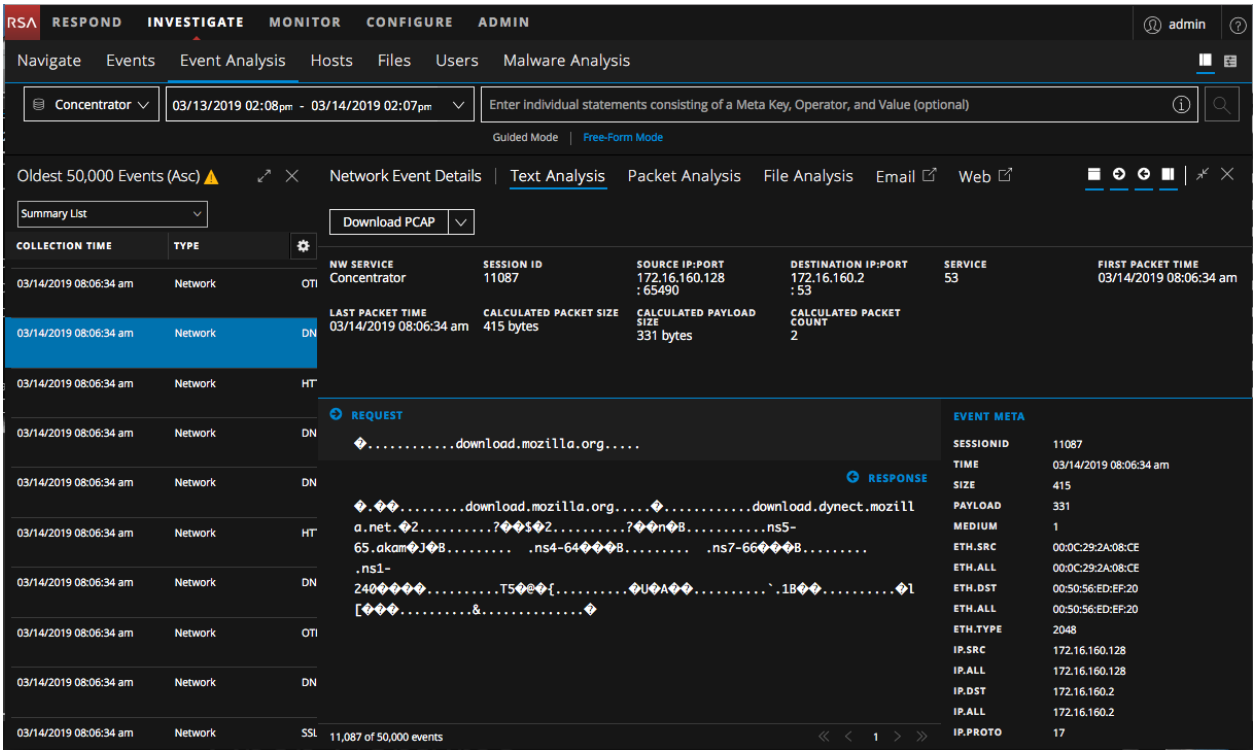
Reconstruction Types in the Event Analysis View

When hunting for possible threats in captured network data, you can drill into different points of interest in the data. If a particular session contains suspicious events, you can examine the list of events for the session and you can also safely view a reconstruction of the event with features that help to identify patterns.

Note: If you are analyzing events on a 10.6.x service from an 11.3 NetWitness Server, the download behavior in the Event Analysis view varies for files, PCAPs, logs, payloads, and meta values. You may see an event payload on a 10.6.x service to which you do not have permission, but you will not be able to download files or payloads.

In the Event Analysis view, you can select the format for the reconstruction: Packet Analysis, File Analysis, or Text Analysis, Email, and Web. For a log event or endpoint event , only the Text Analysis is available. The default reconstruction for network events is Text Analysis; however, for a network event the last reconstruction format that was open overrides the default. The Email and Web reconstructions open the event in the Events view and are described in Reconstruct an Event.

This figure is an example of the Network Event Details: Text Analysis panel in a web browser window.



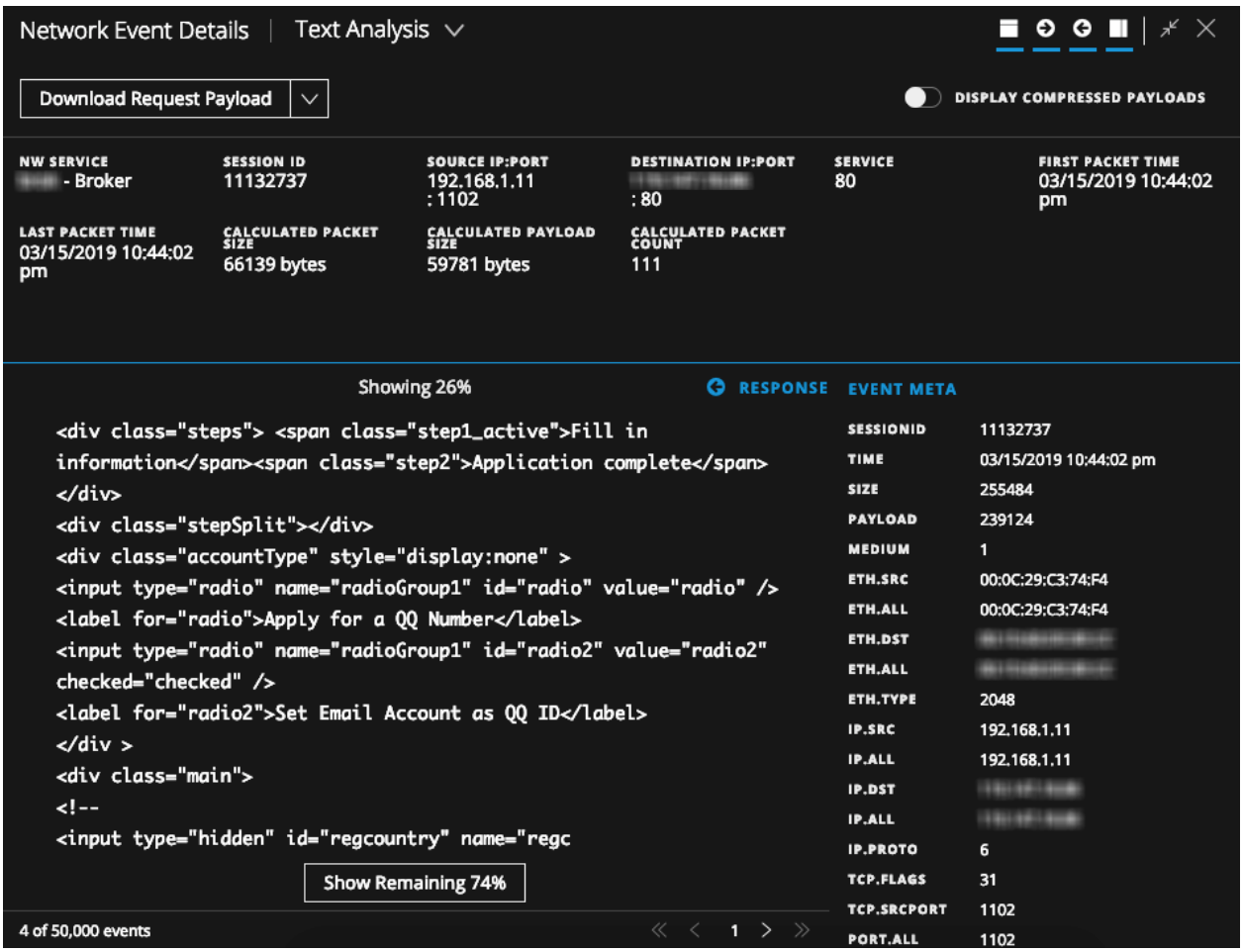
Within each type of analysis, settings are available to enhance your analysis. If you change a setting, the setting is preserved between browser refreshes and logins within the same browser. These are the preserved settings:

- The currently selected reconstruction: Text Analysis, Packet Analysis, or File Analysis.
- Whether the Event Meta panel is open or closed.

- Whether the Event header is open or closed.
- Whether the Request or Response, or both are displayed.
- Whether packet payloads are displayed in the Packet Analysis panel.
- Whether shaded bytes are displayed in the Packet Analysis panel.
- Whether other common file types are highlighted in the Packet Analysis panel.
- The number of packets per page in the Packet Analysis panel.
- Whether compressed or uncompressed text is displayed in the Text Analysis panel.

The Text Analysis Panel

You can view all types of events (network events, log events, and endpoint events) in their original text format in the Text Analysis panel. The Text Analysis panel for some network events can be quite large. To ensure the best rendering, an excessively large payload is truncated to fit. If a single reconstructed request or response in the reconstructed event exceeds the maximum number of bytes, the header indicates what percentage of bytes is shown. Pagination controls add flexibility when paging through the reconstructed text of an event. This figure illustrates a single response that has been truncated because it exceeds the maximum number of bytes (Version 11.2 and later).



Version 11.1 handles large payloads differently; the payload for a single event is limited to 2500 packets. When the packet limit is reached, a warning in the footer advises the limit has been reached and provides the total number of packets in the event. This figure shows the tooltip displayed when you hover over the warning.

Note: The Show More option is still available for messages that are truncated; however, the entire text of the message is not visible without downloading the raw payload.

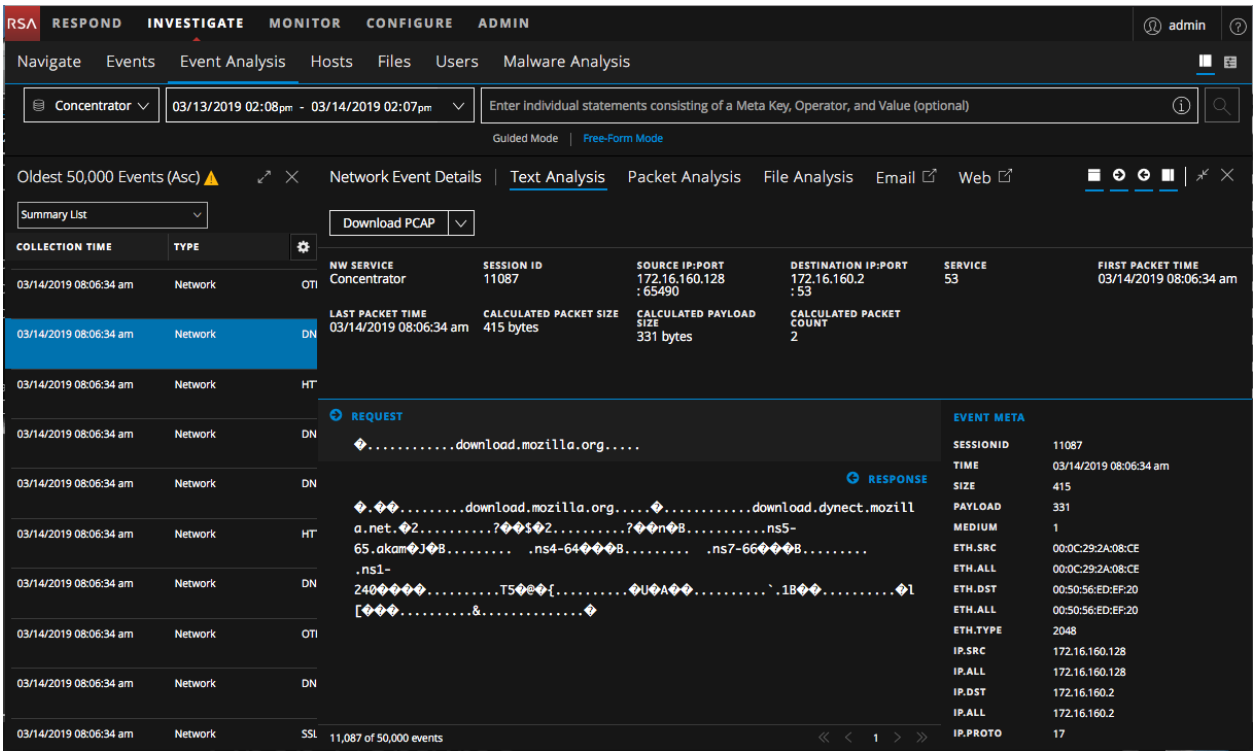
In the Text Analysis panel, network events, log events, and endpoint events are presented differently.

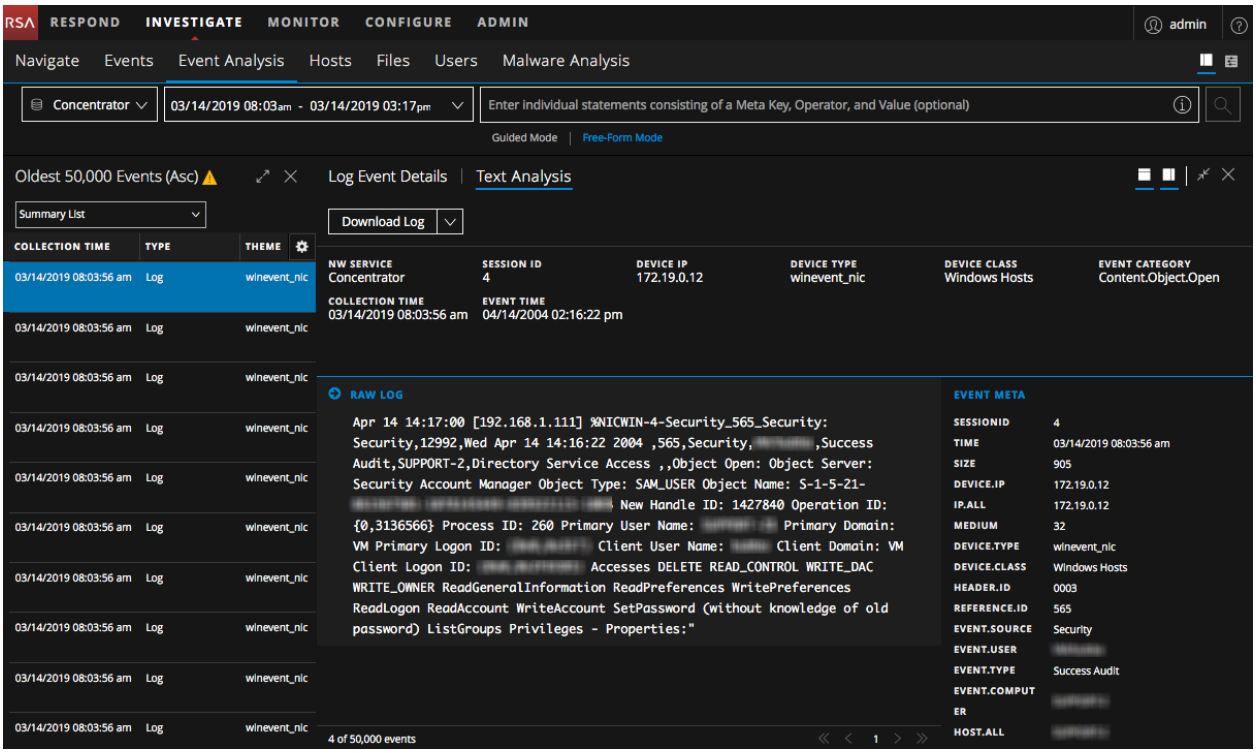
- For network events, Investigate provides the direction of the packet (Request or Response) and contents of each packet in text format. If you are reconstructing a network event, the Text Analysis panel is scrollable. When you scroll, the text identification information and the Request and Response labels remain visible rather than scrolling out of view.
- Log events and endpoint events have no request or response; only the raw event is displayed in the Text Analysis panel.

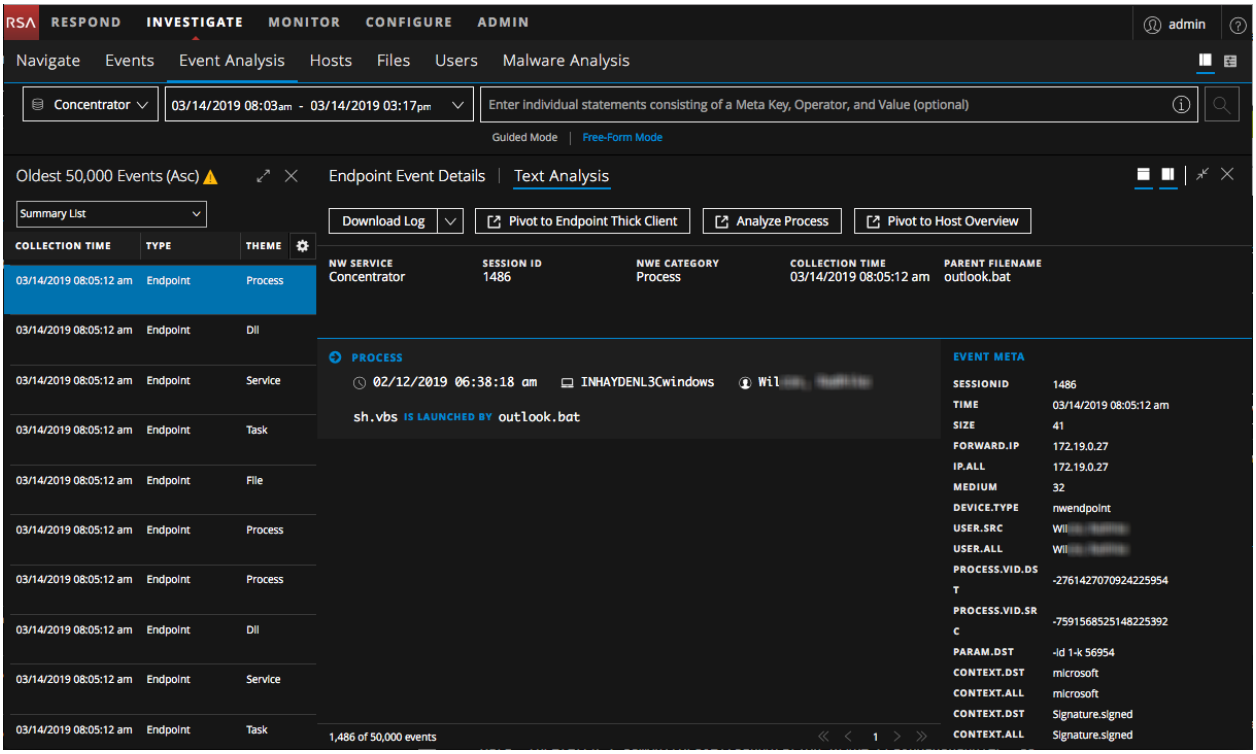
For each type of event (network, log, or endpoint), there are several differences:

- The Event header includes information relevant to each type of event.
- There are different options for exporting.

Below is an example of the Text Analysis panel for each type of event, a network event, a log event, and an endpoint event.





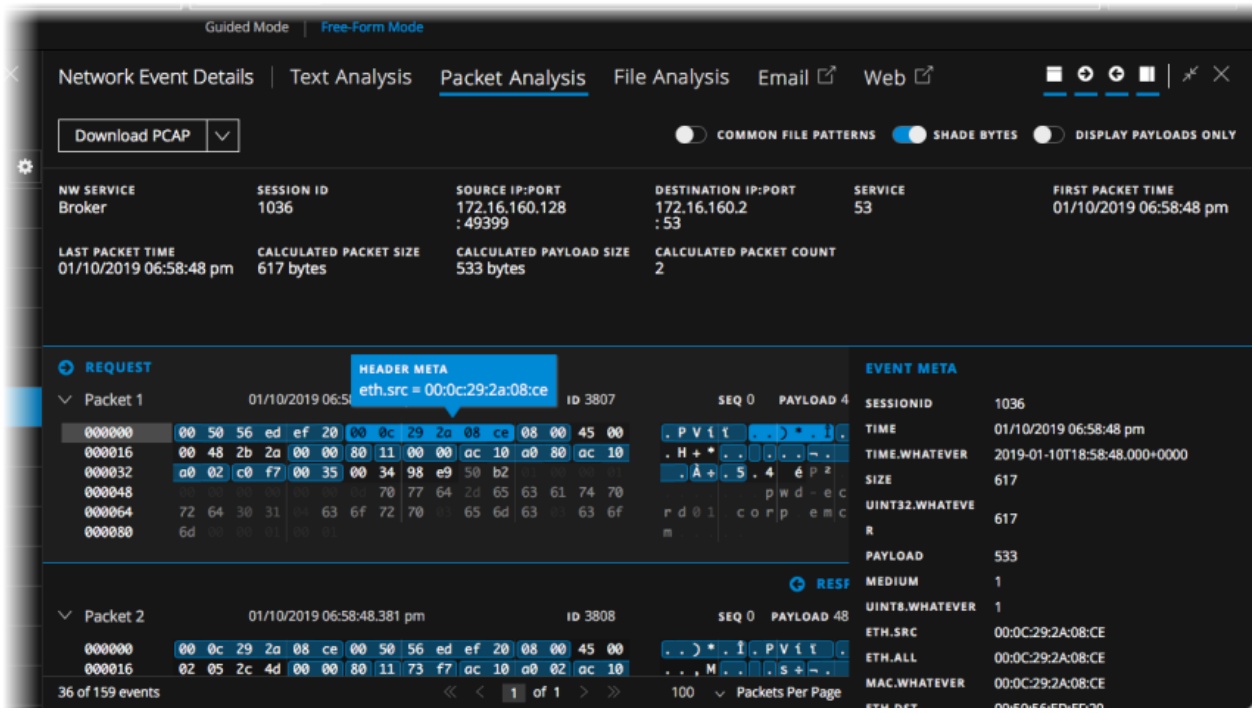


Note: The calculated packet count, calculated packet size, and calculated payload size in the Event header may be different than the same statistics in the Event Meta panel because the metadata is sometimes written before event parsing completes and may include packet duplicates.

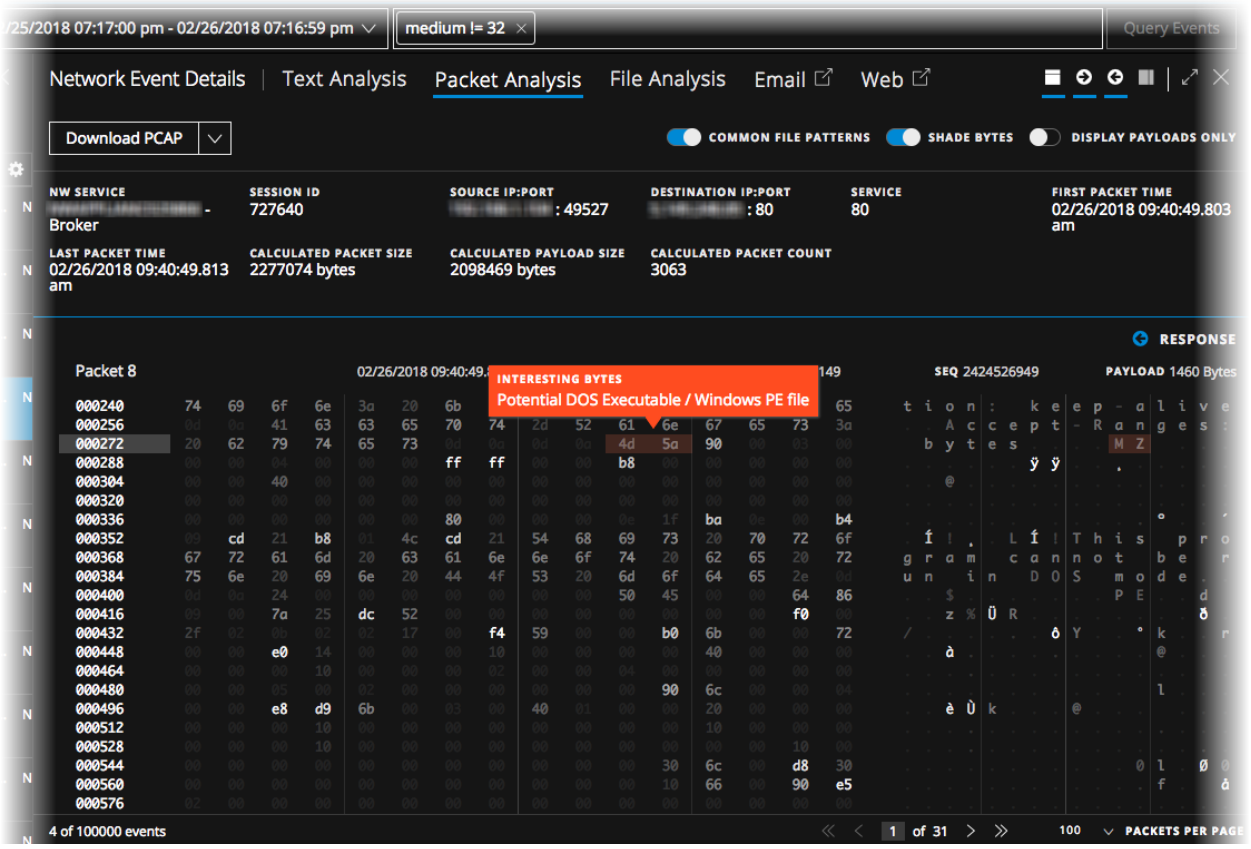
The Packet Analysis Panel

The Packet Analysis panel is for network events. The panel is scrollable, and the packet identification information and the Request and Response labels remain visible rather than scrolling out of view. In the Packet Analysis panel, the headings provide the direction of the packet (Request or Response), the packet number, the packet start time, the packet ID and the sequence, and the payload size. All packets begin with a header, and some packets have a footer. Pagination controls add flexibility when paging through packets.

The metadata in the hexadecimal and ASCII data is highlighted in blue; when you place the cursor over the highlighted metadata, the meta key/meta value information is displayed in a hover box.

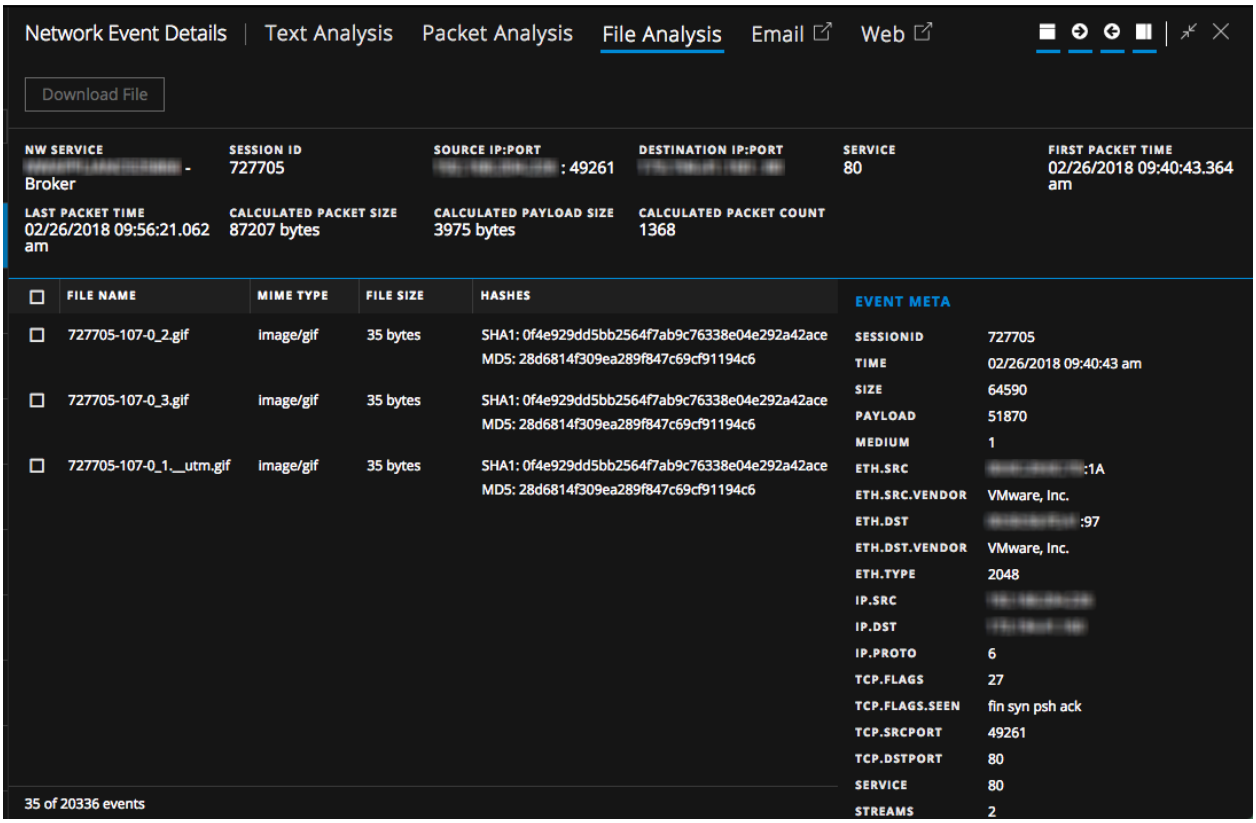


Common file signatures are highlighted with an orange background. When you place the cursor over the highlighted text, the description of the file type is displayed in a hover box.

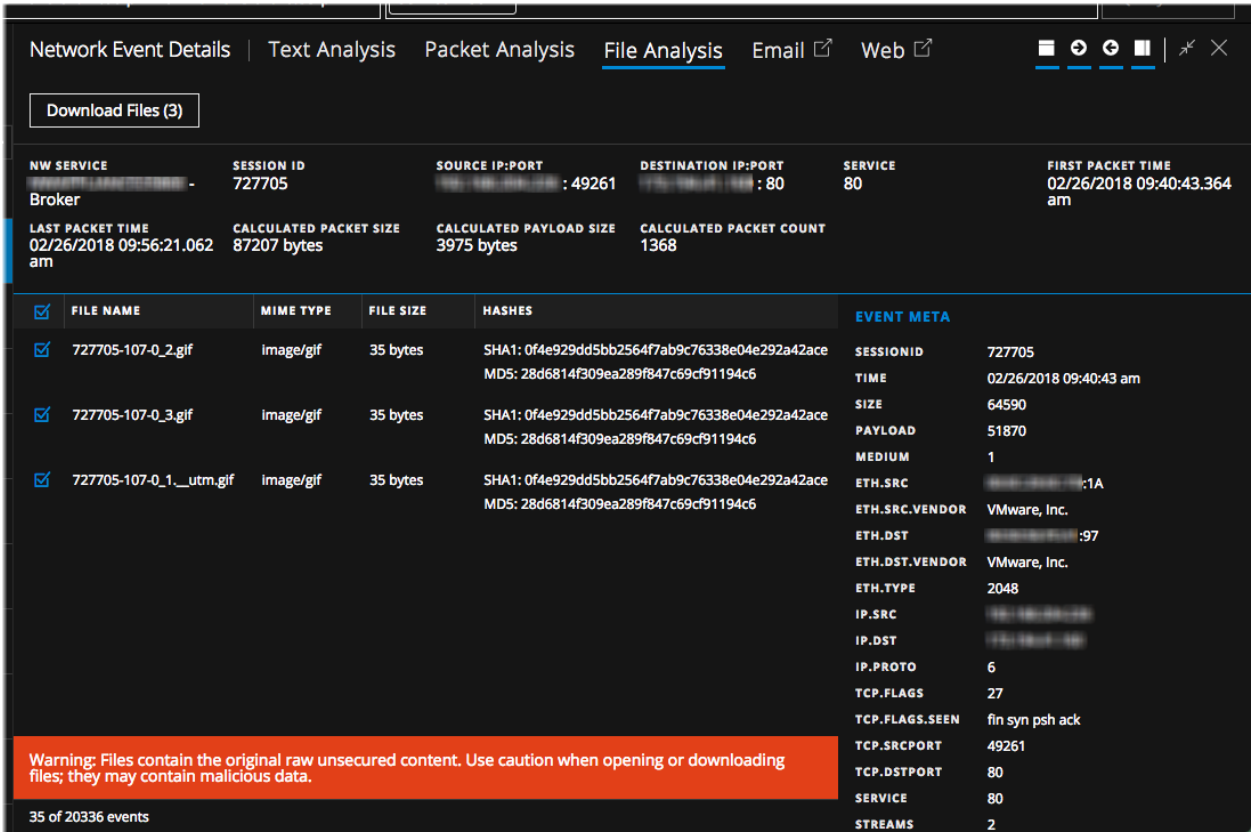

/25/2018 07:17:00 pm - 02/26/2018 07:16:59 pm
medium != 32
Query Events
Network Event Details
Text Analysis
Packet Analysis
File Analysis
Email
Web
Download PCAP
COMMON FILE PATTERNS
SHADE BYTES
DISPLAY PAYLOADS ONLY
NW SERVICE
Broker
SESSION ID
727640
SOURCE IP:PORT
: 49527
DESTINATION IP:PORT
: 80
SERVICE
80
FIRST PACKET TIME
02/26/2018 09:40:49.803 am
LAST PACKET TIME
02/26/2018 09:40:49.813 am
CALCULATED PACKET SIZE
2277074 bytes
CALCULATED PAYLOAD SIZE
2098469 bytes
CALCULATED PACKET COUNT
3063
RESPONSE
Packet 8
INTERESTING BYTES
Potential DOS Executable / Windows PE file
SEQ 2424526949
PAYLOAD 1460 Bytes
4 of 100000 events
1 of 31
100
PACKETS PER PAGE

The File Analysis Panel

The File Analysis panel shows a list of files associated with the selected network event. This is an example of the File Analysis panel.



You can select one or more files, or all files, to export to your local file system. When files are selected, Export Files becomes active and reflects the number of files selected.



Caution: Caution is advised when unzipping and opening files that are associated with a default application; for example, an Excel spreadsheet may automatically open in Excel before you have a chance to verify it is safe.

Analytical Tools for Each Type of Event Analysis

The analytical tools in the Event Analysis view help analysts find the relevant information for different types of events (network event, log event, and endpoint event). This table lists the actions you can take by event type. The rest of this section provides procedures for performing the actions.

Action	Network Event	Log Event	Endpoint Event
View the Text Analysis panel	✓	✓	✓
View the File Analysis panel	✓		
View the Packet Analysis panel	✓		
Open, close, and adjust the size of panels	✓	✓	✓
Adjust the display of requests and responses	✓		
Show or hide the Event Header in the Text Analysis panel	✓	✓	✓

Action	Network Event	Log Event	Endpoint Event
Expand truncated text entries in the Text Analysis panel	✓		
Switch between a compressed and decompressed view of payloads in the Text Analysis panel	✓		
View highlighted bytes in the Packet Analysis panel	✓		
Highlight common file types in the Packet Analysis panel	✓		
Display only the payload in the Packet Analysis panel	✓		
Shade bytes in the Packet Analysis panel when viewing payload only	✓		
Perform URL and Base64 encoding and decoding in the Text Analysis panel	✓		
View decompressed text for an HTTP network session in the Text Analysis panel	✓		
View event metadata for an event in the Text Analysis panel	✓	✓	✓
Download a network event (as a PCAP file, payload only, request only, or response only) in the Packet Analysis panel or the Text Analysis panel	✓		
Export files from a network event in the File Analysis panel	✓		
Download the file for a log event in the Text Analysis panel		✓	
Download the file for an endpoint event in the Text Analysis panel			✓
Open the current endpoint event in Text Analysis panel			✓

Filter Results in the Event Analysis View

You can filter events in the Event Analysis view using the query bar to select a service and time range and then querying the service being investigated. Filtering events helps to narrow the focus of an investigation to a smaller, relevant set of events.

Note: This section applies to version 11.1 and later.

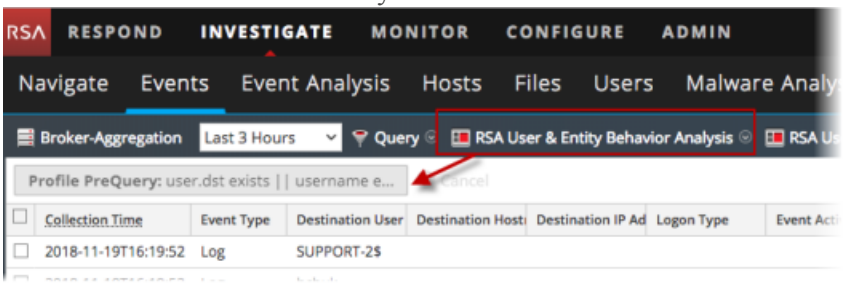
Initial View

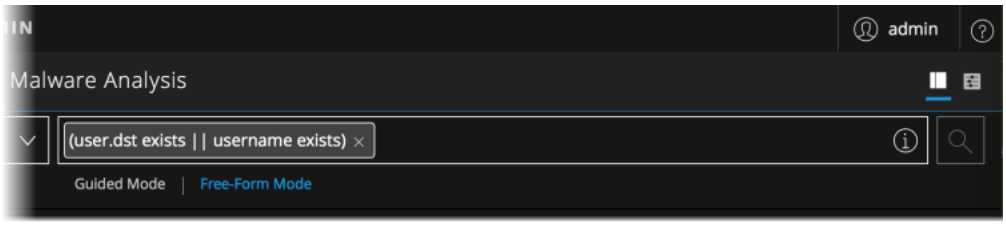
When you go to INVESTIGATE > Event Analysis to open the Event Analysis view, the service and time range selectors are displayed in the query bar.

- By default, the first service is automatically selected (unless you previously selected a service and the selected service is in browser cache).
- If you do not select a time range, the default time range (24 hours) is used.
- The query builder field is an empty field to the right of the time range selector.

When you go to the Event Analysis view from the Events view or the Navigate view, the service, time range, and any filters that were selected in the Events view or Navigate view are displayed in the query bar. The service, time range, and individual filters can be modified.

If a profile is selected in the Events view when you right-click or double-click an event and go to the Event Analysis view, the filters from the profile (preQuery) are added to the query builder field as an editable filter. The following figures show a preQuery in the Events view, and the same query added as the first filter in the Event Analysis view.





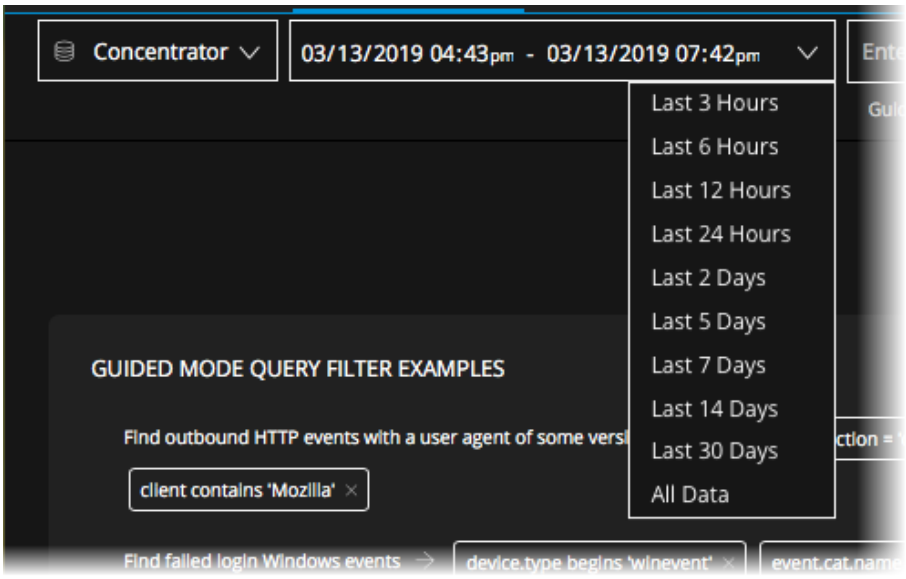
Select a Time Range

The Time Range selector limits the events returned in the Event Analysis view to a specific time range. The time range is displayed in the format `Start Time - End Time`, showing the date, hours, and minutes in your current timezone based on timezone settings configured for your profile. You can choose a time range relative to the current collection time or create a custom time range (Version 11.3 and later). The time and date format is based on preferences set for the Event Analysis view in the User Preferences dialog (select > **Profile**).

- By default, the date format is MM/DD/YYYY. You can change the format to DD/MM/YYYY, or YYYY/MM/DD in the User Preferences dialog.
- Start time and end time are in the format of HH:MM. Although seconds are not displayed, the value for start time always defaults to HH:MM:00 seconds, and the value for end time always defaults to HH:MM:59 seconds. As an example, a time range of 6:45 pm - 7:45 pm is interpreted as 06:45:00 - 07:45:59 pm.
- The default time range is the 24-hour clock; you can change it to 12-hour periods.
- The time format can be either database time or wall clock time. When Database Time is selected, the start and end time for a query is based on the time that the event was captured (collection time). When Wall Clock Time is selected, the query is executed using the end time based on the current browser time; the start time is calculated based on that end time and the time range.

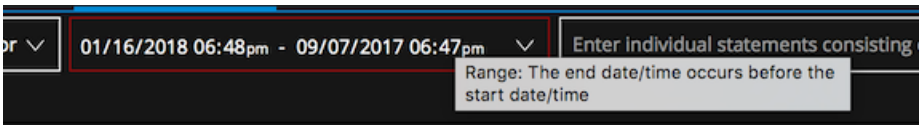
To edit the time range, do one of the following:

1. Click the drop-down arrow inside the **Time Range** selector and select a time range from the list. Options are in minutes, hours, days, or all data.

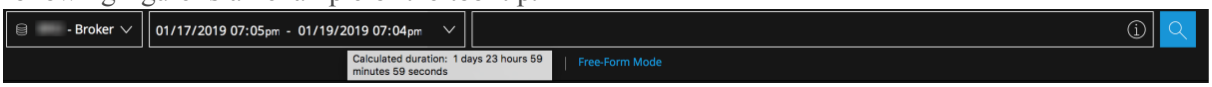


2. (Version 11.3 and later) Edit the time range directly by clicking the year, month, day, hour, or minute displayed in the query bar. When a value is highlighted, type a new value for either the start or end time. If your time format preferences are set to 12-hour periods, click **am** or **pm** to toggle between the two options.

If the time range is invalid (for example, the start time is later than the end time), a red border appears around the Time Range selector. The button is disabled because the query is no longer possible, and a tool top shows an error message explaining what you need to change. The following figure shows an invalid time range.



The selected time range is stored in your browser for the service being queried; you can set different time ranges for different services. A tool tip shows the calculated duration of the query. The following figure is an example of the tool tip.



Create Filters in the Query Bar

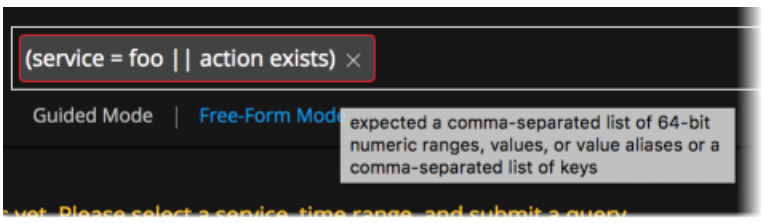
The query bar allows you to reduce the number of events to an interesting set by creating filters.

- Simple filters are in the form `<meta key><operator><meta value>`.
- Complex filters have one of these operators, `||`,`&&`, `()`, `REGEX`, or `LENGTH`. (If you open an event from the Events view or Navigate view and the filter has one of these operators, the complex filter is added as a single filter in the Event Analysis query bar.)

In the query bar, each filter becomes an editable field. Filters line up from left to right, representing the sequence in which the filters were created. As more filters are added and exceed the length of a single line, they wrap to another line and the input area expands vertically so that all filters are visible without scrolling to the right.

In Guided Mode, you are guided with suggestions for auto-complete that show only valid meta keys and operators in the drop-down menu. You can type or select from the drop-down menu. In the drop-down menu, operators that take more time to execute are marked by a stopwatch icon. As you create simple filters, the syntax of each filter is validated and invalid filters are marked by a red outline. If you hover the mouse over the filter, a message that explains the error is displayed.

In Version 11.3 and later, complex filters are validated on the server side, which may take additional time. If you submit the query before the server has returned filter validation results, the is replaced by a spinner. When server validation returns, a query with no invalid filters begins execution. If the query contains an invalid filter, execution is terminated and the invalid filter is outlined in red. This is an example of an invalid query.



In Free-Form Mode, you can type or paste a complex query. There is no auto-suggestion, and validation is performed on the server side when you submit the query. If an error is found, the query does not execute.

Note: The button has a different label in versions earlier than Version 11.3. It was previously named **Query Events**.

The button on the right side of the query bar is active as needed to submit a query. When you click , all of the filters are AND'd to generate results and the button becomes inactive. The button becomes active again in these conditions:

- If you change the service in the query bar or change the column group in the Events panel, a network call for data for reconstructions or the Events panel continues to use the previous service, time range, and metadata filters until you submit the new query. The button becomes active as an indicator that the data in the view is stale.
- If more than a minute has passed and the original query's time range would no longer generate the same result set, the button becomes active as an indicator that results may be stale. In Version 11.3 and later, a setting in the Event Analysis view preferences determines this behavior by enabling or disabling the Update Relative Time Window Automatically option (see Configure the Event Analysis View.)

Versions 11.2 and 11.3 have more capability than the original 11.1 query bar. The following table summarizes the differences.

Version	Features
11.1	• The query bar guides you as you create and edit each simple `<meta key> <operator> <meta value>` filter. The query bar supports only simple filters. If you open an event from the Events view or Navigate view and the filter has more than one operator, `||`,`&&`, `()`, `REGEX`, or `LENGTH`, the filter is added, but editing is not supported in the Event Analysis view.
11.2	• The query bar guides you as you create and edit each simple `<meta key> <operator> <meta value>` filter (called Guided Mode). The default mode is Guided Mode, which includes auto-suggest and validation options. • You can enter a complex query in Free-Form Mode. In Free-Form Mode validation is performed when you run the query.

Version	Features
11.3	• When you go to the Event Analysis view from the Navigate view or Events view, with a preQuery in effect for a profile, the preQuery that was displayed in the breadcrumb is available in the Event Analysis view query bar as an editable filter. • You can create a free-form (complex) filter while in Guided mode. The auto-suggest drop-down lists are augmented with an Advanced Options section that allows for the creation of a free-form filter. Free-Form Mode is still useful for pasting an entire complex query. • Visual cues identify the filter that is the focus of some type of action among multiple selected filters. • You can cancel a query while it is executing. • Detailed status information about the query being executed is available in the query console.

Switch Between Guided Mode and Free-Form Mode

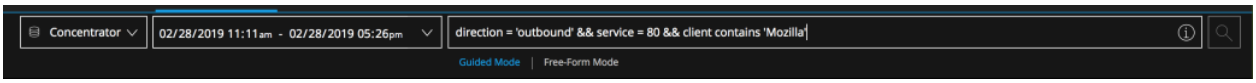
Two options switch between the modes. If you selected Free-Form Mode the last time you logged in, this choice is in effect the next time you log in.

- When you switch from Guided Mode to Free-Form Mode, filters that you created in Guided Mode are transformed to a text query in the Free-Form field.
- When you switch from Free-Form Mode to Guided Mode, the query you were typing is added to the query bar as a single uneditable filter.

> **Note:** Beginning with Version 11.3, a Free-Form filter can be edited but it does not include auto-suggest options.

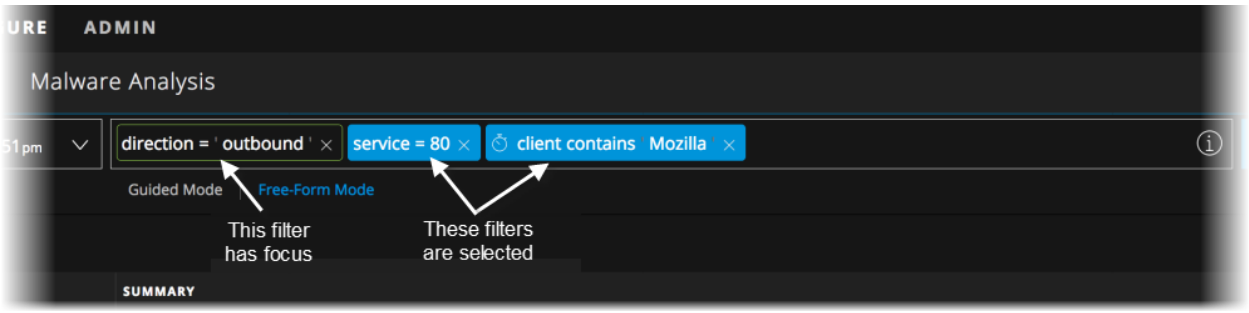
The following figure is an example of the Event Analysis view with the Guided Mode query builder in use.

The following figure is an example of the Free-Form query builder in use.

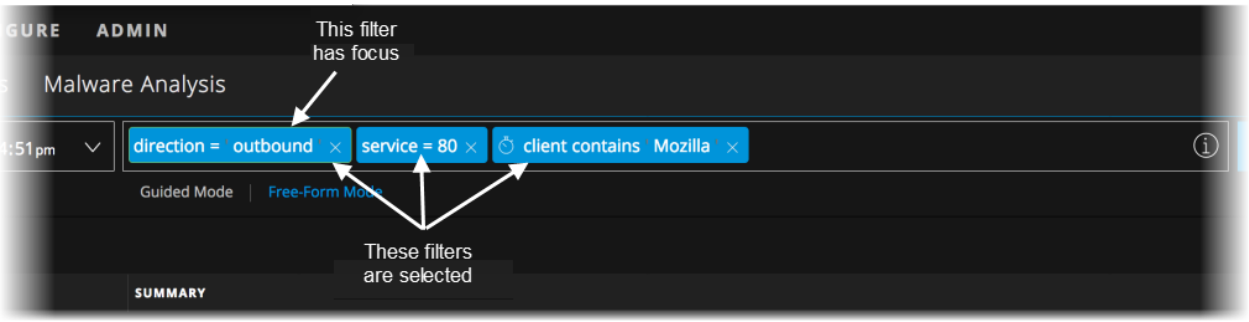


Work with Multiple Filters

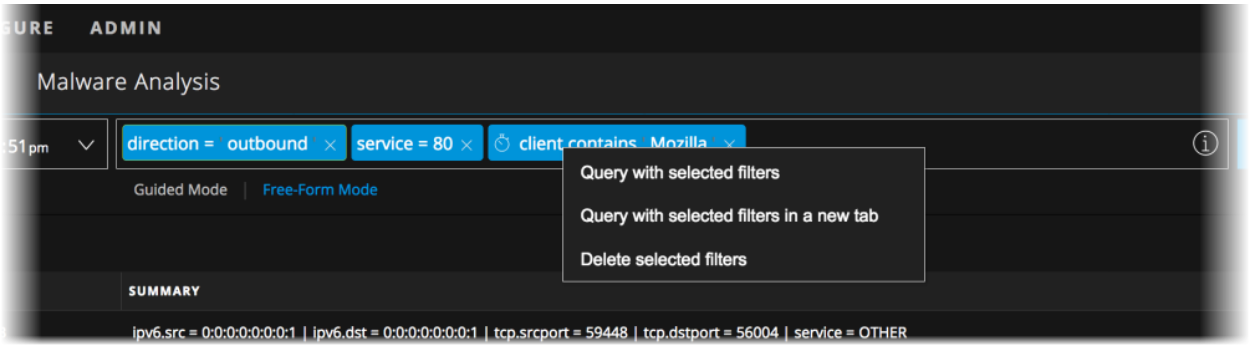
As you work in the query bar, you can see when a filter has focus for editing (a green outline) and which filters are selected (blue background). This is useful because you can have multiple filters selected for right-click actions, but only one can be edited at a time. The figure below shows the green outline marking a filter that has focus and the blue background indicating that two filters are selected.



This figure illustrates the same set of filters with all filters selected (blue background) and one filter that has focus (blue background and green outline).



A right-click action from the drop-down menu applies to all selected filters as shown in this figure.



These are a few basic concepts that explain how to work in the query bar:

- You can select multiple filters, but only one can have focus and the last selected filter is the one with active focus at any point in time.
- To select a filter and give it focus, click the filter. To deselect the filter and remove focus, click the filter again, press **Esc**, or click anywhere else on the page.
- To add a filter, click before or after an existing filter. To create a new filter before or after the filter in focus, press the right or left arrow key.
- To open a filter for editing, double-click the filter or click it and press **Enter**. To exit without saving changes and leave the filter in focus, press **Esc**.
- To delete a filter, click the filter and press **Delete** or click **X** on the filter.

Cancel Execution of a Query

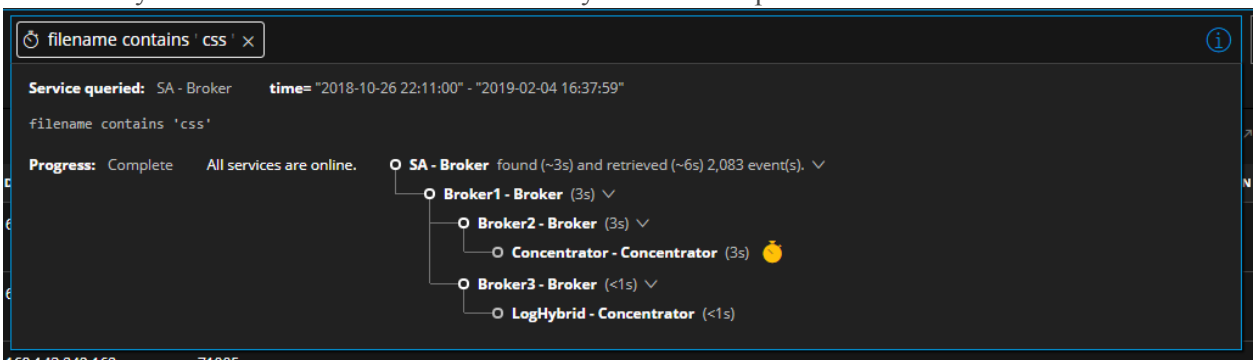
After you click to submit a query, the button changes to (the stop query option). The stop query option remains until all the events are loaded in the Events panel. To cancel the query, click .

If the query is canceled before all results have been returned, the following message is displayed at the end of results in the Events list: "Because the query was canceled, only partial results are displayed."

View Status of a Query

After a query is submitted, you can click the information icon ( ) in the query bar to open the query console. In the query console, you can see which service, time range, and metadata was queried as well as real-time information about the status of the query and the services being queried. The time range displayed in the Query console always shows each date as YYYY-MM-DD. Here is an example range from the Query Console: `"2014-09-20 20:57:00"-"2018-11-02 18:57:59"`.)

The following figure is an example of the information in the Query Console when a query executes successfully and the slowest service is marked by an amber stopwatch.



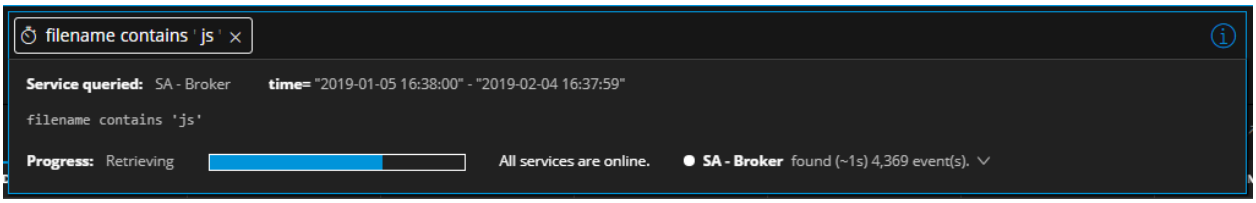
While a query is executing, a progress bar indicates the query's completion percentage at the bottom of the console. The status lets you know details about what is happening; for example, you can tell when the query is executing, queued, reading the index file for the queried service, retrieving events, and complete. All statuses and non-fatal messages are displayed as they come in, and the border color of the query bar changes to amber if a non-fatal error occurs.

Icons provide additional information about individual services.

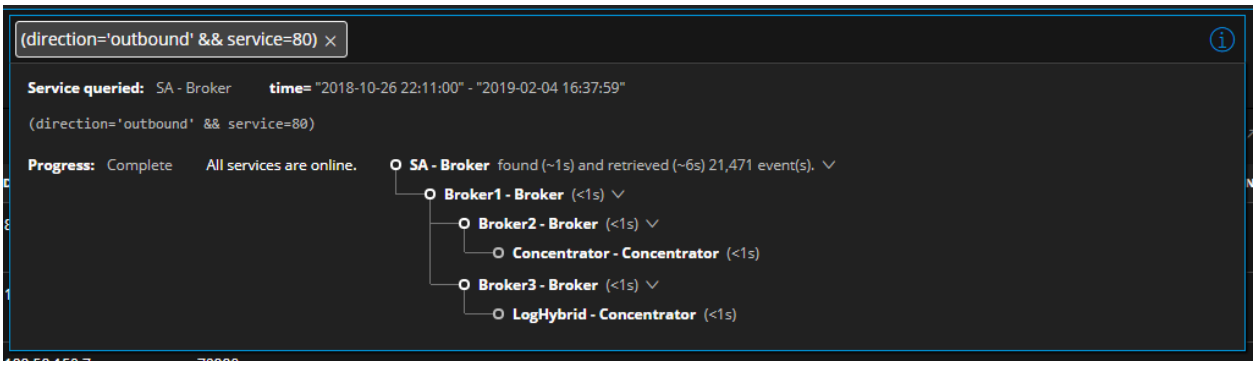
- An amber stopwatch marks the slowest service.
- An amber triangle indicates a warning was received.
- A red triangle shows that an error was received when trying to query the service.

Executing and Reading the Index File to Find Events. The first stage of a query is complete when the queried services have found results. The query console provides a nested hierarchical listing of all the services being queried with indicators showing which are online or offline, and the time in seconds that the service took to find results.

Retrieving Events and Loading in the Events Panel. While the found events are being retrieved and loading in the Events panel, the progress bar shows a visual indicator and text description of what is happening. In the figure below, results were found and are being retrieved.

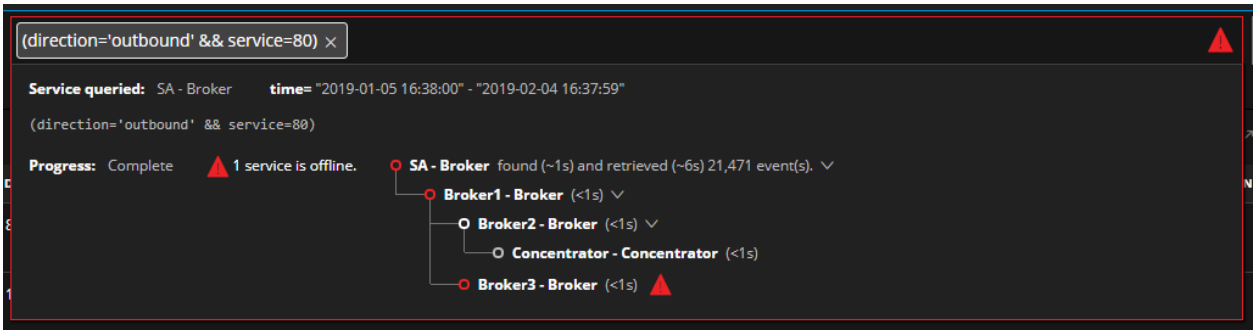


Request Complete. If there are no errors or warnings when loading is complete, the query console is outlined in blue and the button is disabled as an indicator that the data in the view is fresh. The following figure is an example of the query console for a completed query with no errors or warnings.

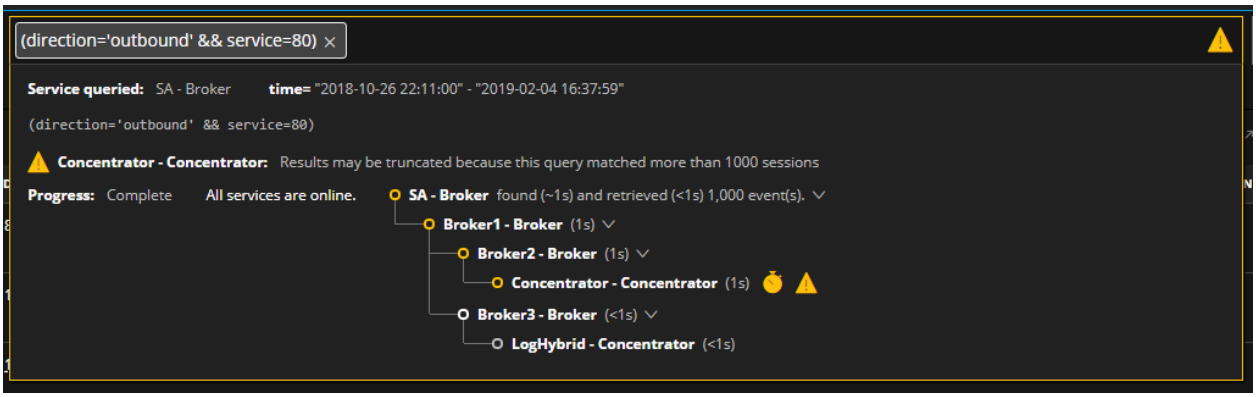


Errors and Warnings. A fatal error such as a syntax error in the query, or the queried service being offline, stops execution of the query. A red triangle is displayed in the upper right corner of the query console, and the console is outlined in red to indicate that the query failed. If the queried service is offline, only the queried service with no hierarchy of services is listed in the query console and marked by a red triangle.

A non-fatal error does not prevent a query from executing. The query is executed and events are loaded, but a red triangle is displayed in the upper right corner of the query console, and the console is outlined in red as a warning. The following figure shows the appearance of the query console when the queried service proxies to another service that is offline.

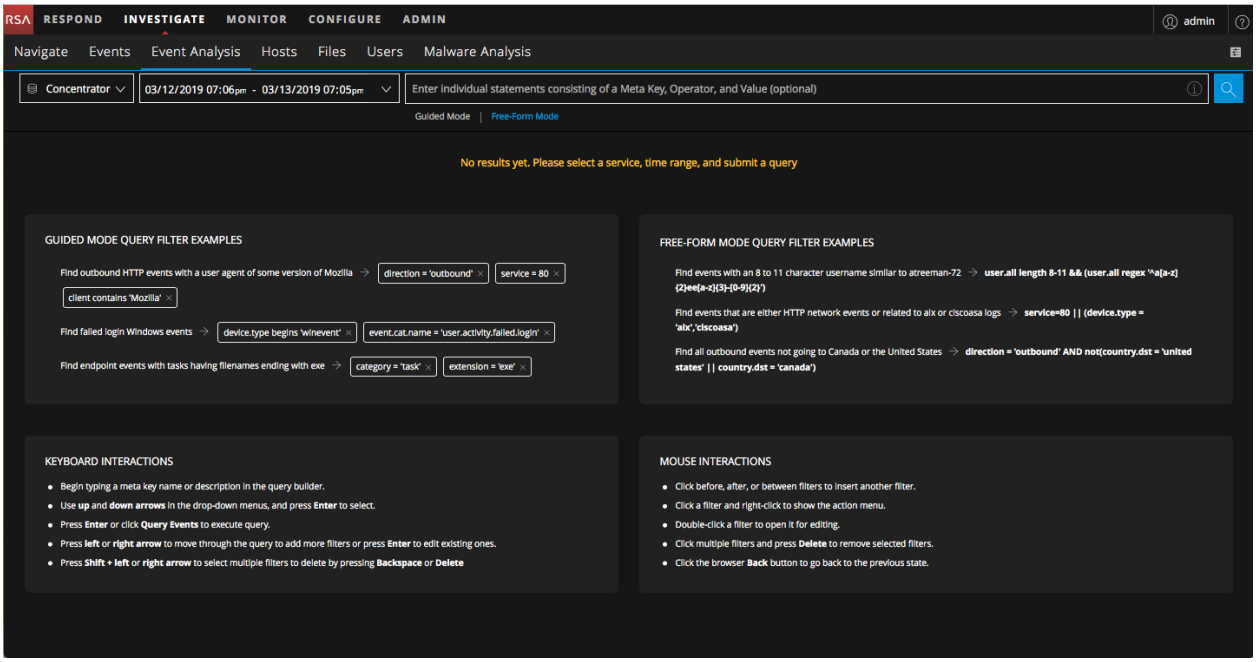


A warning does not prevent a query from executing. The query is executed and events are loaded, but an amber triangle is displayed in the upper right corner of the query console, and the console is outlined in amber. The following figure shows the appearance of the query console when there was a warning that results may be truncated on one of the services in the service hierarchy, but the request completed.



Build a Query in Guided Mode

Guided Mode is the easiest way to create a query with features to help analysts enter valid queries. The following figure illustrates the initial Event Analysis view with Guided Mode in effect in the query bar.



Note: Guided Mode in Version 11.2 supports only simple filters in the form `<meta key><operator><meta value>`. If the Events view or Navigate view has a filter with more than one operator, `not`, `>`, `<`, `<=`, `>=`, `||`, `&&`, `()`, `REGEX`, or `LENGTH`, the filter is added, but editing is not supported in the Event Analysis view. The same is true for a filter created with Free-Form mode in effect and then viewed in Guided Mode. In Version 11.3, you can enter and edit a complex filter in Guided Mode, but Free-Form Mode is still better for pasting an entire complex query.

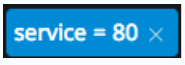
Keyboard Actions to Use in Guided Mode

In Guided Mode, the query builder allows entry, editing, and deletion of filters using the key strokes without having to use a pointer. Although you can use the pointer, you have the option to keep your fingers on the keyboard. This table identifies the available keyboard actions in Guided Mode when the cursor is located in the query bar; these do not apply to the service selector and time range.

Action	Keyboard Entry
Submit a query.	With focus on the query bar and no pending filters, press **Enter.**
Select the filter to the immediate left if one exists.	With no selection in the query bar, press the **Left Arrow** key.
Select the filter to the immediate right if one exists.	With no selection in the query bar, press the **Right Arrow** key
Insert a new filter to the immediate left of the selected filter.	With a filter selected, press the **Left Arrow** key.
Insert a new filter to the immediate right of the selected filter.	With a filter selected, press the **Right Arrow** key.
Insert a new filter to the immediate left of the selected filter, and open for editing.	With a filter selected, press the **Shift + Left Arrow** keys.
Insert a new filter to the immediate left of the selected filter, and open for editing.	With a filter selected, press the **Shift + Right Arrow** keys.
Select all filters to the right of the current filter.	With a filter selected, press the **Shift + Down Arrow** keys.
Select all filters to the left of the current filter.	With a filter selected, press the **Shift + Up Arrow** keys.
Edit a selected filter	With a single filter selected, press the **Enter** key.
Deselect all filters.	With a filter selected, press the **ESC** key.
Delete all selected filters.	With filters selected, choose the **right-click > Delete selected filters** option, press **Delete**, or press **Backspace**.
Update query with only the selected filters.	With filters selected, choose the **right-click > query with selected filters** option.
Open a new tab with the selected filters.	With filters selected, choose the **right-click > query with selected filters in a new tab** option.

Visual Feedback in Guided Mode

Guided Mode provides visual feedback during query construction. This table identifies and describes the possible feedback.

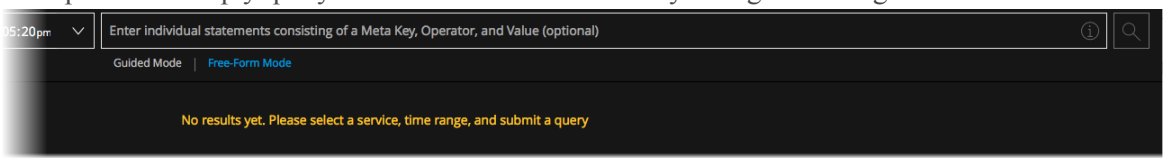
Feedback	Icon	Description
Blue Background on a Filter		Indicates that a filter is selected.

Feedback	Icon	Description
Green Circle		The cursor has been placed in between two existing filters. Clicking inserts a new filter at this location.
Green Outline on a Filter		Marks the single filter that has focus.
Red Filter Outline		Value-type is not valid for the selected meta key. A tool tip that explains the error is displayed. For example, a string value for a meta key that expects an integer.
Loading Spinner		The query is currently being processed. The **Query Events** button is disabled while this occurs.
Query Events button		The Query Events button has three possible states: Ready to submit a query using filters in the Query Builder. Waiting for server validation to complete before executing the query. The query is executing, click to cancel execution.
Slow Service Icon		This service took the longest time to load results from the query.
Stopwatch		The selected meta key/operator combination requires extra time to process. While the query is still executable, a more efficient meta key or operator is recommended.

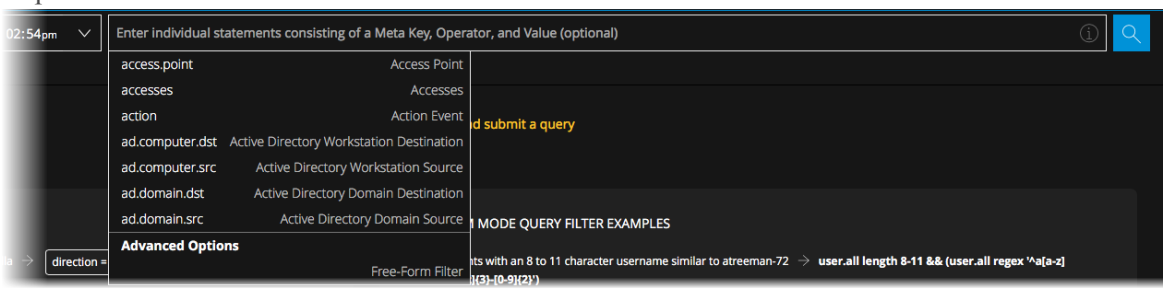
Add a Simple Filter in Guided Mode

To create a simple filter in the Event Analysis view in Guided Mode:

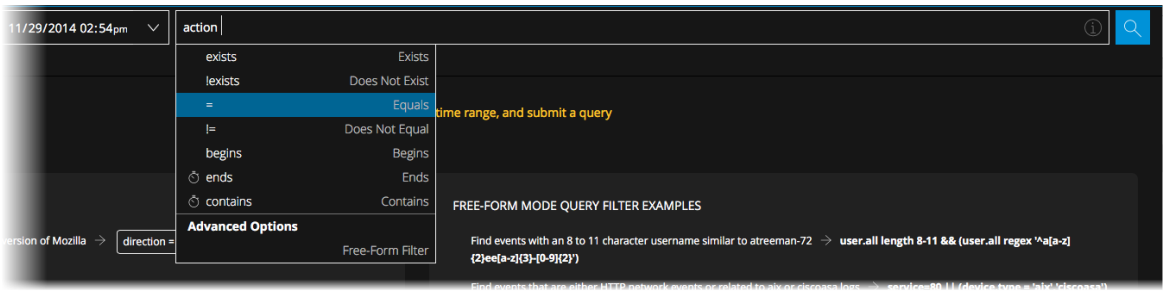
1. Go to the **Event Analysis** view and do one of the following:
   a. (Version 11.2 and later) Select **Guided Mode** below the query bar and click in the query builder field.
   b. (Version 11.1) Click in the query builder field, or before or after an existing filter. This is an example of the empty query bar in Guided Mode before you begin entering a filter.



   If the insertion point is between two filters, a green circle marks the insertion point. If the insertion point is at the end of the query bar, the filter entry field opens with a blinking cursor at the entry point. A drop-down menu lists available meta keys passed from the service being investigated in alphabetical order. Meta keys that require more time to process are marked by a stopwatch icon.



2. To select a meta key do one of the following:
   a. If there is only one option in the drop-down menu, press the **Enter**.
   b. If there are two or more options in the drop-down menu, click on the meta key or use the up/down arrow and press **Enter**.
   c. Start typing the meta key. As you type the meta key, the list is further updated. To select the meta key, press **Enter**.
   d. If you want to edit or delete the meta key, press **Backspace** or **Delete**.
   As you backspace and delete a character, the meta key drop-down menu is filtered to include meta keys that begin with those characters. To select a meta key, press **Enter**.
   The meta key is added to the query bar, a list of valid operators for the selected meta key is displayed. Operations that require more time to process are marked by a stopwatch icon. This figure shows the stopwatch icon.



3. To select an operator, do one of the following:
   a. If there is only one option in the drop-down menu, press **Enter** to select it.
   b. If there are two or more options in the drop-down menu, click on the operator or use the up/down arrow and press **Enter**.
   c. Type the operator and press **Enter**.
4. (Optional) Type a value and press **Enter**.
5. To create the filter, press **Enter**. If you click anywhere outside the box before pressing **Enter**, the filter is not created.
   The new filter is inserted, and the blinking cursor is refocused after the last filter, the meta keys drop-down is displayed. If there is an error in the filter, it is outlined in red. You can hover over the filter to see a tool tip explaining the error. This figure shows a query being created with no errors.

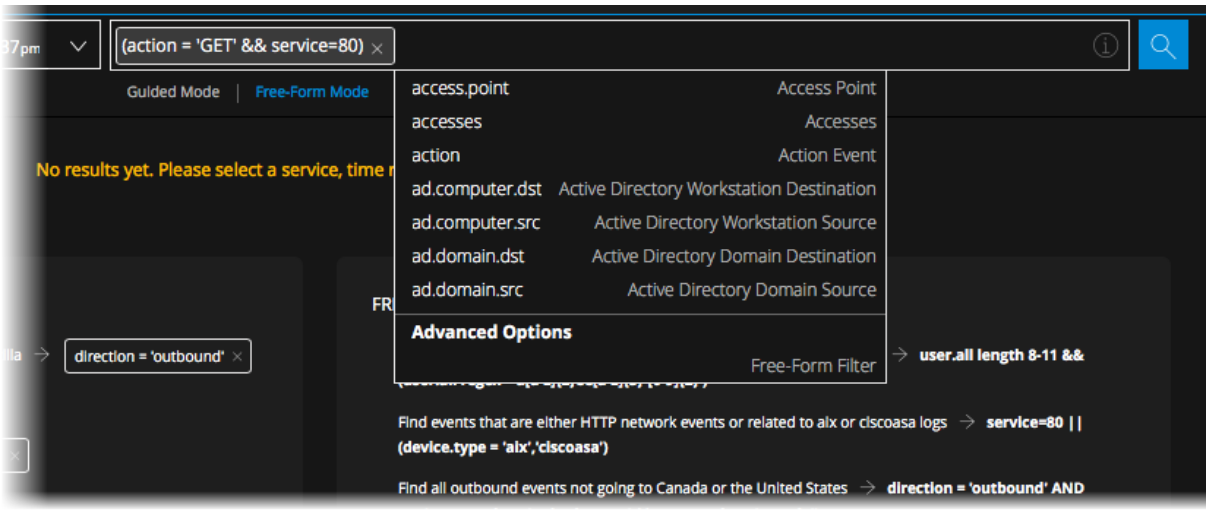
6. If the filters have no errors, you are ready to execute the query in the query bar. Click .
   The results are returned and loaded in the Events panel. The first 50,000 events that match the query begin loading in the Events panel. As the events are loaded, a status bar at the top tracks progress and you can scroll to the bottom of the list to see the completion status.
7. (Optional in Version 11.3 and later) If you want to see detailed status in the Query Console, click the information icon .
8. (Optional in Version 11.3 and later) If you want to cancel the query before it finishes executing, click .
   The query stops executing and a notification that the query has been canceled is displayed.

Add a Free-Form Filter in Guided Mode (Version 11.3 and Later)

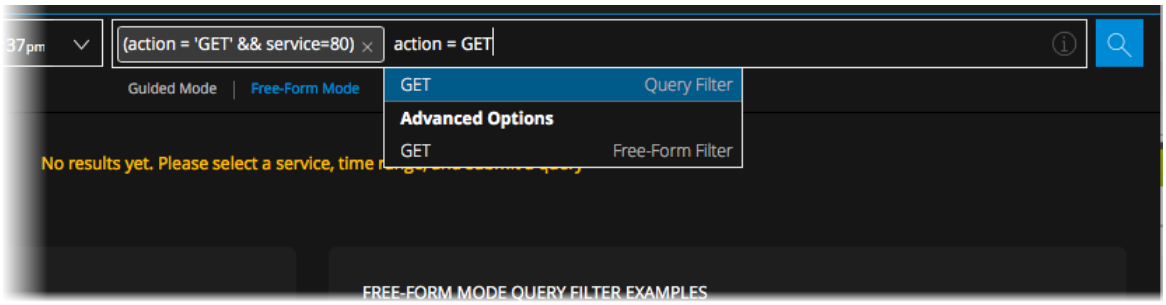
To filter the data displayed in the Event Analysis view using a free-form filter in Guided Mode:

1. Go to the **Event Analysis** view, select **Guided Mode** below the query bar, and click in the query builder field.
   If the insertion point is between two filters, a green circle marks the insertion point. If the insertion point is at the end of the query bar, the filter entry field opens with a blinking cursor at the entry point. A drop-down menu lists available meta keys passed from the service being investigated in

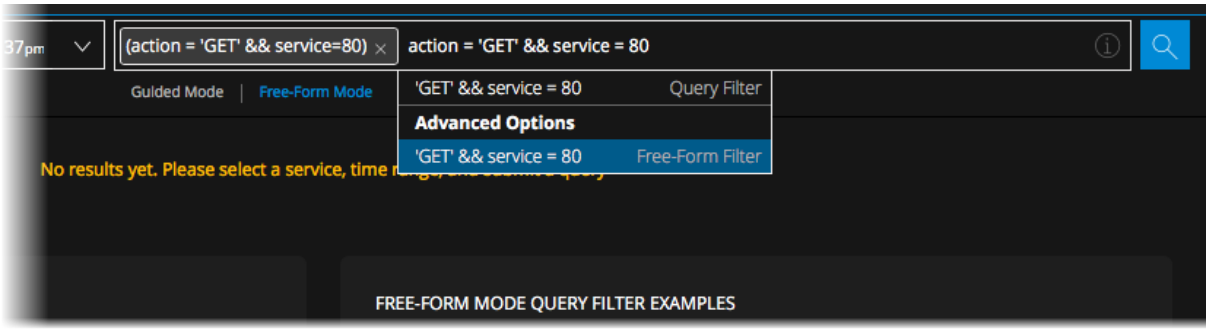
alphabetical order. Meta keys that require more time to process are marked by a stopwatch icon.



2. Do one of the following:
   a. Place the cursor in the **Free-Form Filter** field and begin typing the query.
   b. Begin typing the filter as usual beginning with a meta key.
      When no matching meta keys or operators are available in the drop-down menu, the Free-Form Filter option becomes available, and the text you typed is available in the **Free-Form Filter** field.



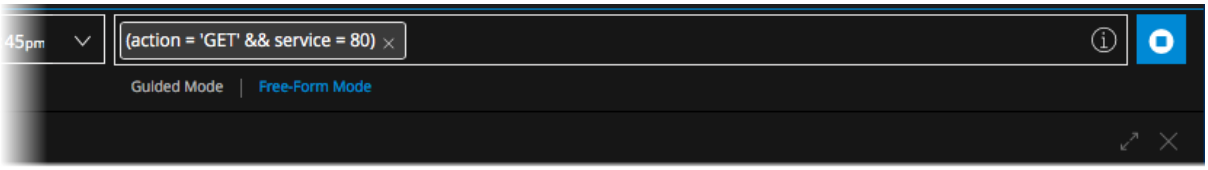
3. Continue typing the entire expression and press **Enter**.
   (If you click anywhere outside the box before pressing **Enter**, the filter is not created.) This figure shows a complex expression created by continuing to type after the value GET.



   The new filter is inserted, and the blinking cursor is refocused after the last filter, the meta keys

drop-down menu is displayed. If there is an error in the filter, it is outlined in red. You can hover over the filter to see a tool tip explaining the error.

4. To execute the query, click . While the query is executing, the button changes to .



5. If you want to cancel the query before it finishes executing, click .
   If you do not cancel the query, you can click to view the status of query execution. When the query is finished executing, the Events panel displays appropriate results for the query.

Edit a Filter in Guided Mode

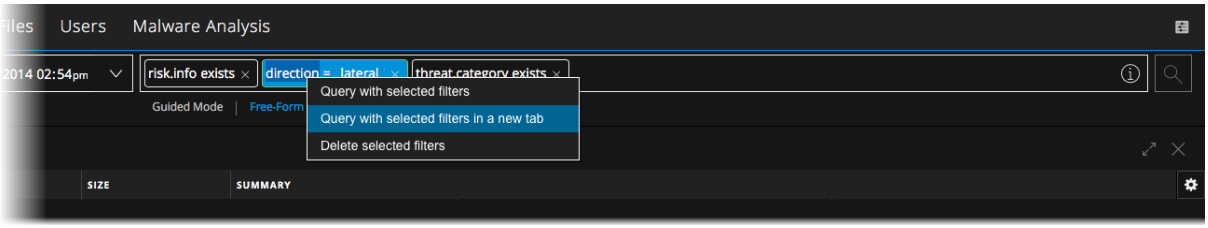
With a query in the Guided Mode query bar, you can edit a filter. To edit a filter:

1. Double-click the filter, or click the filter and press **Enter**.
2. Edit the filter. When finished editing, press **Enter** to update the filter.
3. If you want to execute the query again, click .
   The Events panel displays results for the updated filter.

Query Using Selected Filters in Guided Mode

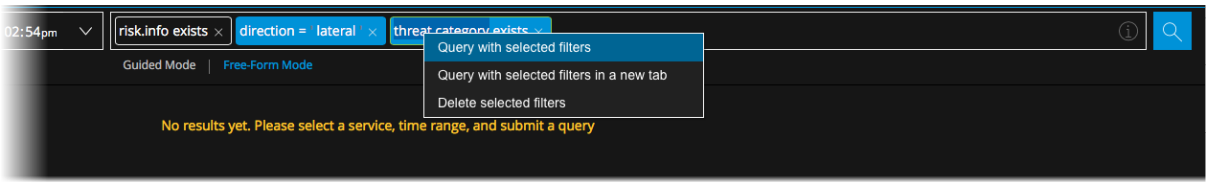
With one or more filters in the query bar in Guided Mode, you can refocus the same query to include only selected filters. The results are displayed in the current browser tab or a new browser tab. To update the query using only selected filters:

1. Begin with a Guided Mode query that includes one or more filters, for example a query has three filters: `risk.info exists`, `direction ='lateral'`, and `threat.category exists`.
2. To open a new tab with the selected filters, select `direction = 'lateral'`, right-click the filter and select **Query with selected filters in a new tab** in the drop-down menu.



   A new tab opens with the results for the selected filter and the original query is left intact on the previous tab.

3. To query the selected filters in the same tab, select `direction = "lateral"` and `threat.category exists`. Then right-click and select **Query with selected filters** in the drop-down menu.



A query with only the selected filters is submitted and all remaining filters are removed.

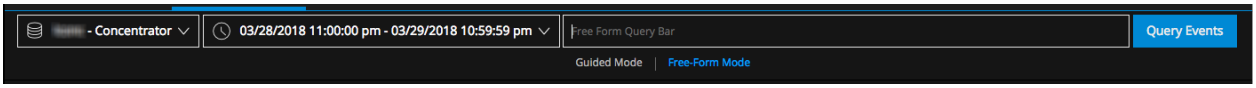
Delete a Filter in Guided Mode

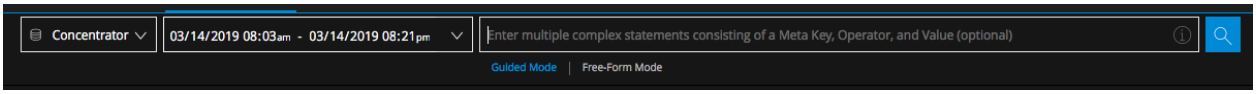
To delete a filter:

1. Click **X** in a filter, click the filter to select it and press **Delete**, or right-click one or more filters and select **Delete selected filters** in the drop-down menu.
2. If you want to execute the query again, click .
   The selected filter is deleted and the Events List is refreshed.

Create a Query in the Free-Form Mode

Free-form queries are most useful when you have a complex query saved that you want to paste, or if you have one in mind that you want to enter quickly, and you know the meta keys, valid operators, and valid syntax for entering values. The following figure illustrates the initial Event Analysis view with the empty Free-Form query builder field. The first example is Version 11.2 and the second example is Version 11.3.





The blinking cursor indicates that you can enter a query. You can enter free text here. As more expressions are added and they cannot be displayed in a single line, they wrap to another line and the input area expands vertically so that all filters are visible without scrolling to the right.

These are some examples of queries that you can enter in Free-Form mode:

To find events with an 8- to 11- character username similar to atreeman-72:

```
user.all length 8-11 && (user.all regex '^a[a-z]{2}ee[a-z]{3}-[0-9]{2}')
```

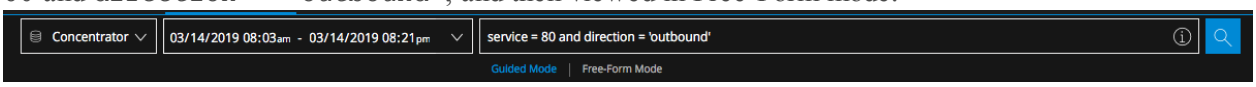
To find events that are either HTTP network events or related to aix or ciscoasa logs:

```
service=80 || (device.type = 'aix','ciscoasa')
```

To find all outbound events not going to Canada or the United States:

```
direction = 'outbound' AND not(country.dst = 'united states' || country.dst = 'canada')
```

If you have a submitted query in Guided Mode, the query is transformed into text when you click switch to Free-Form mode. This is an example of a query submitted in Guided Mode as two filters, `service = 80` and `direction = 'outbound'`, and then viewed in Free-Form mode.



The button on the right side of the query builder is visible as needed to input a query. The query is applied when you click s. At that time the query is validated to show syntax and logic errors.

Operations that require more processing time are not highlighted as they are in Guided Mode, but this table provides a summary of expensive operations for reference.

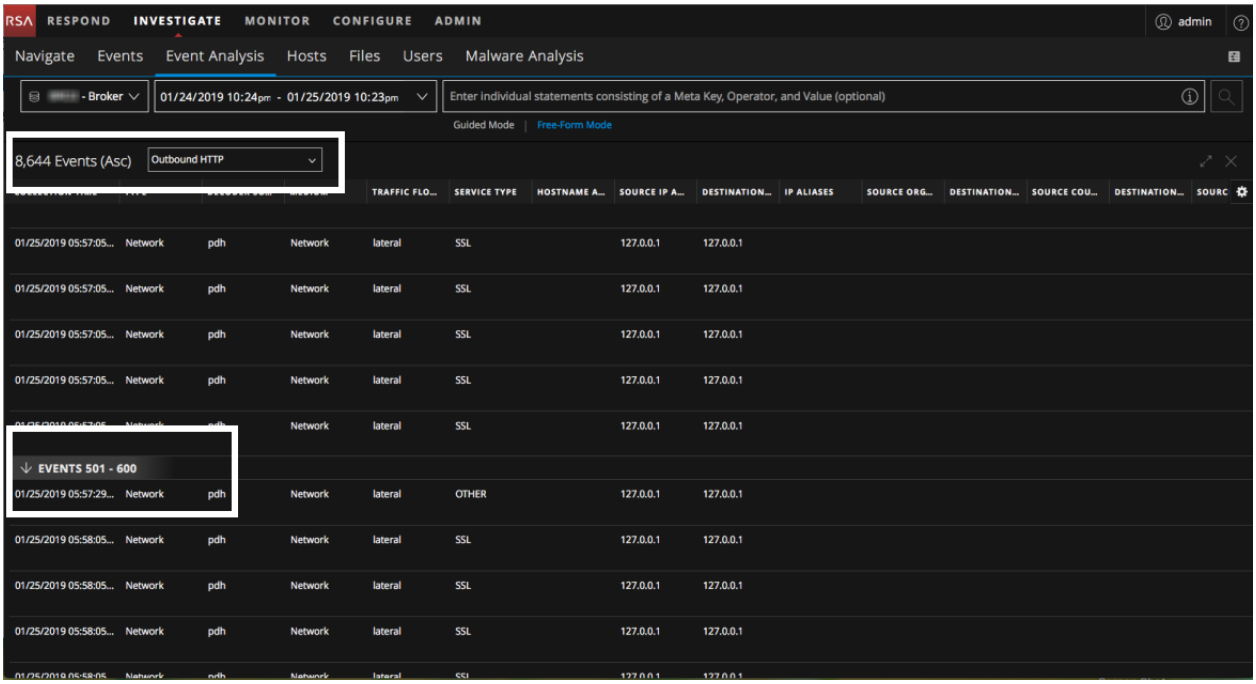
Index Method	Non-Text Value	Text Value	Regular Operations	Expensive Operations
By Key	✓		`exists`, `!exists`	`eq`, `!eq`
By Key		✓	`exists`, `!exists`	`eq`, `!eq`, `begins`, `ends`, `contains`
By Value	✓		`exists`, `!exists`, `eq`, `!eq`	no expensive operators
By Value		✓	`exists`, `!exists`, `eq`, `!eq`, `begins`	`ends`, `contains`
By None	special case for `sessionid`		`exist`, `!exits`, `eq`, `!eq`	no expensive operators

Examine Events in the Event Analysis View

After a query is submitted in the Event Analysis view, the Events panel opens; you can select an event to analyze in the Events panel. The events listed here meet two conditions:

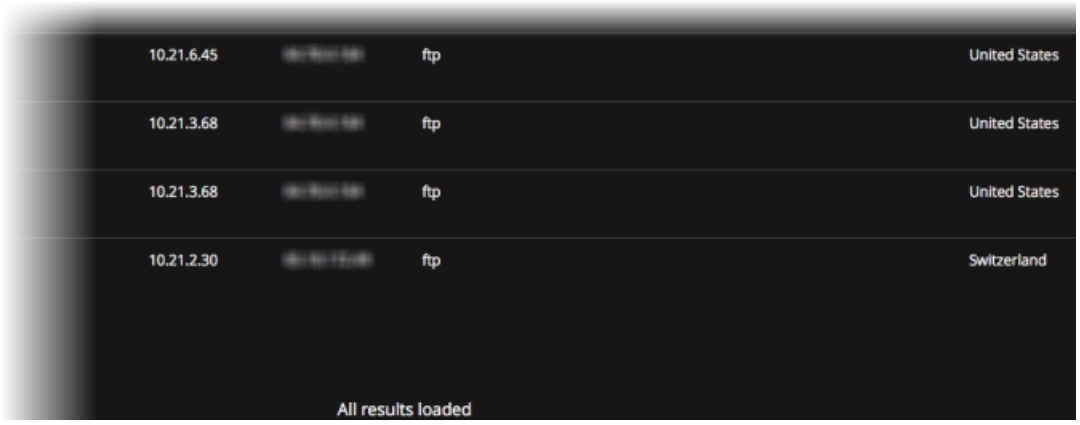
- They match the submitted query.
- They include a value for one or more meta keys required by the selected column group. (If you change the column group while viewing the Events list, the original query with the new column group is resubmitted. Any unsubmitted query changes made to service, time range, or filter, are ignored.)

There is a fixed limit of 50,000 on the number of events that can be loaded. The events begin loading into the Events panel; a progress bar at the top of the list tracks progress while events are loaded. Events with the earliest collection time are loaded first and a row number indicator of the form " EVENTS xxx - xxx" is inserted in the list after every group of 100 events as shown in the following figure.



If you scroll to the bottom of the list as the events are loading, a spinner is displayed. When all events have loaded, one of these messages is added to the bottom of the list:

- "All events loaded"
- "Reached the 50,000 event limit. Consider refining your query."
- "Retrieved 44,000 of 50,000 events prior to query cancellation."



If the number of events that match the query exceeds the limit of 50,000 events, the oldest 50,000 events in the time window are loaded in ascending order. For example, if 300,000 events match your query, the oldest 50,000 events are loaded.

A message at the top of the list indicates the total number of events loaded and if the 50,000 event limit has been reached:

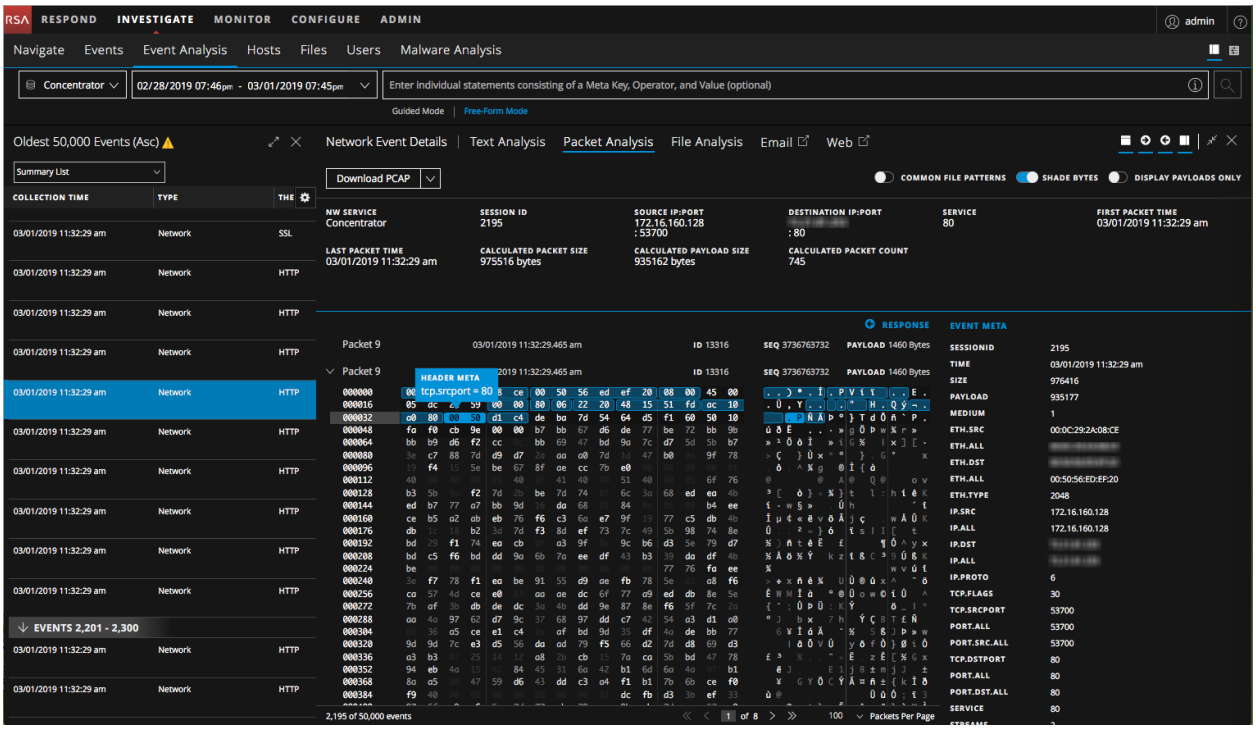
- The message when less than 50,000 events are listed is: "xx,xxx Events (Asc)"
- The message when more than 50,000 events are listed is: "Oldest 50,000 Events (Asc)"

When you select an event, the Network Event Details, Log Event Details, or Endpoint Event Details panel opens on the right. The selected event in the Events panel is highlighted and pinned to the top of the list. You can make simple adjustments in the visibility and size of the panels.

You can choose different reconstruction formats (Packet Analysis, Text Analysis, File Analysis, Web, and Email). Within the Packet Analysis panel and the Text Analysis panel, you can use additional features to adjust the way the reconstruction is displayed and bring interesting data into focus.

Open, Close, and Adjust the Size of the Panels in the Event Analysis View

Initially, the Network Event Details, Log Event Details, or Endpoint Event Details panel occupies 75% of the window width by default.

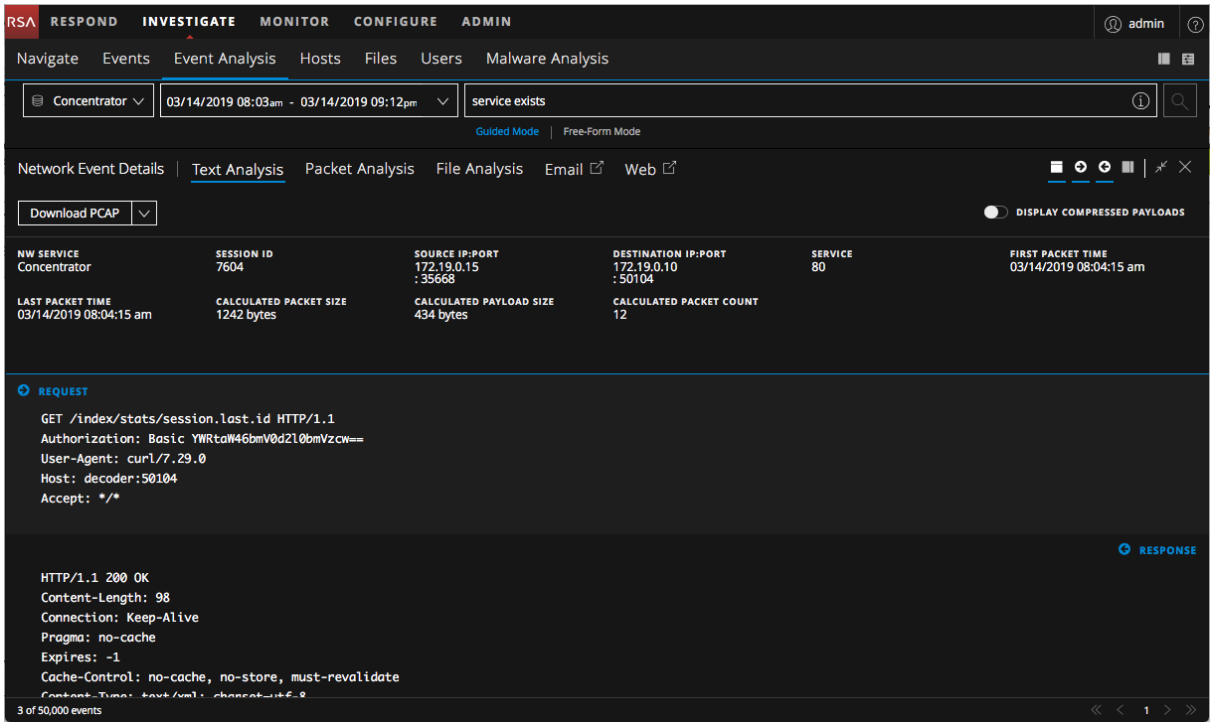


You can adjust the size ratio of the Events panel in relation to the details panels to improve readability by expanding one of the panels, contracting one of the panels, and closing one of the panels. After closing either panel you can reopen it. The ratio you select persists until you change it or refresh the browser.

To optimize your view:

1. To adjust the size ratio of the two panels, do any of the following:
   a. Click ◪ in the tool bar of the panel that you want to expand.
   b. Click ◪ in the tool bar of the panel that you want to contract.

2. To close either panel, restoring the open panel to its full width, click ■.
   This is an example of the reconstruction displayed using the full width of the browser window.



3. To reopen the Events panel after closing, click ◫ in the top right corner of the Event Analysis view. The Events panel opens to the last state (25%-75% or 50%-50%).
4. To reopen the Event Details panel, click an event in the Events panel.

Select a Column Group and Columns in Event Analysis

In Version 11.1 and later, you can use built-in or custom column groups in the Events panel. The column groups are created and managed in the Events view (see Manage Column Groups in the Events View); these groups are reflected in the Event Analysis view. When you change the column group, the changes you make to a column group are for the current view only. When you navigate away and come back to the Event Analysis view, the column changes do not persist in the Events panel.

These are the built-in column groups.

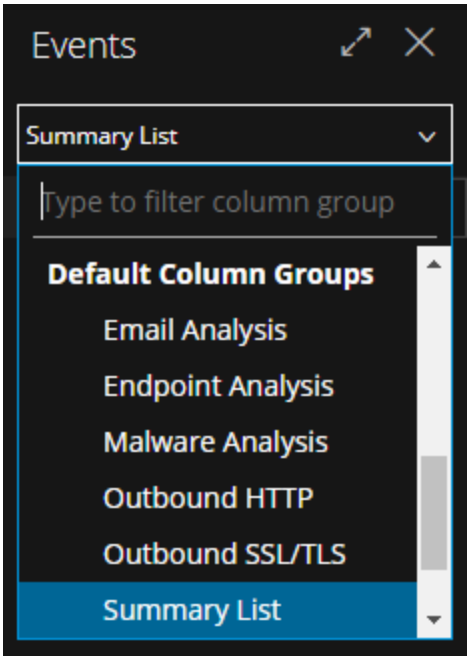
- **Email Analysis**: Includes meta keys that are useful when investigating email-related metadata.
- **Endpoint Analysis**: Includes meta keys that are useful when investigating endpoint-related metadata.
- **Malware Analysis**: Includes meta keys that are useful when investigating malware-related metadata.
- **Outbound HTTP**: Includes meta keys that are useful when investigating Outbound HTTP- related metadata.
- **Outbound SSL/TLS**: Includes meta keys that are useful when investigating Outbound SSL/TTS analysis-related metadata.

- **Summary List**: Includes meta keys that are useful in a general investigation. This is the default column group.
- **Threat Analysis**: Includes meta keys that mark potential threats in the data set.
- **User and Entity Behavior Analysis**: Includes meta keys that are useful when investigating UEBA data.
- **Web Analysis**: Includes meta keys that mark anomalies in web traffic.

A column group may contain more columns that are only visible when you scroll to the right. The order of the columns reflects the order in the Events view of the default column group. By default, the first 15 columns are displayed when you select a column group. For optimized viewing, view only 15 columns at a time; however, you can select additional columns to display and remove columns displayed.

To select a column group:

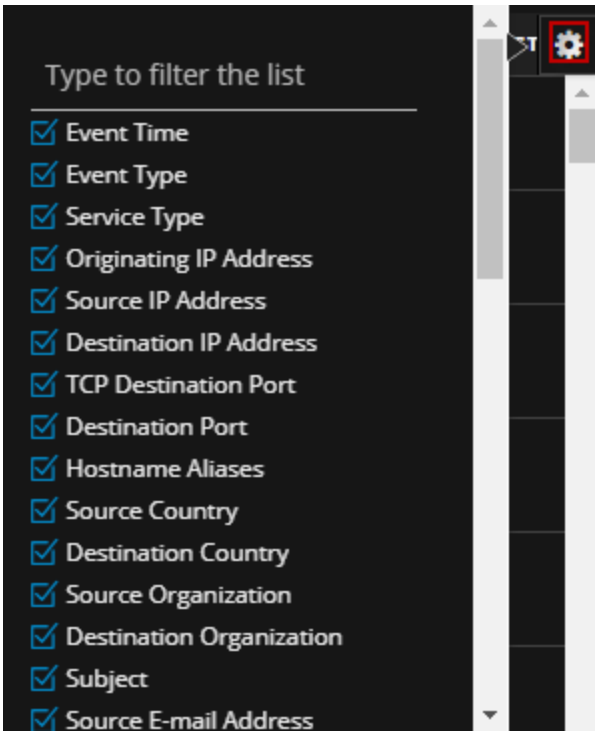
1. From the drop-down menu next to Events, select a column group (for example, **Summary List**). You can also start typing the name of the column group and select a group as the groups appear in the drop-down menu.



   The Events panel displays data in the columns that belong to the selected column group.

To select columns to display:

1. While working in the Event Analysis view, with a column group selected, click ⚙ to display the column selector.



2. Select the meta keys or enter the name of a meta key that you want to display in additional columns.
3. If you do not want to see a meta key displayed in a column, deselect the meta key.
   The data is redisplayed using the selected columns.

Select the Event Analysis Type

To select the event analysis type for an event, do one of the following:

1. In the **Event Analysis view** toolbar, click the analysis type in the toolbar.
2. In the drop-down menu, select the analysis type: **File Analysis**, **Text Analysis**, **Packet Analysis**, **Email** , or **Web**.
   If you chose **File Analysis**, **Text Analysis**, or **Packet Analysis**, the data is displayed in the selected panel.
   If you chose **Email** or **Web**, the Events view email or web recontruction of the single event opens in a new tab. This is the same reconstruction of an email or web session used in the Events view. The Events view provides more functionality when viewing an email or web reconstruction, allowing you to page through events in that view instead of viewing only one event (see Reconstruct an Event).

Note: The Packet Analysis panel is only available for network events.

Adjust the Display of Requests and Responses

For Event types that have requests and responses, you can make several adjustments.

Note: If the analysis type does not have requests and responses, the option is not selectable. The File Analysis panel is an example of a reconstruction type without requests and responses. A reconstructed log event in the Text View is another example.

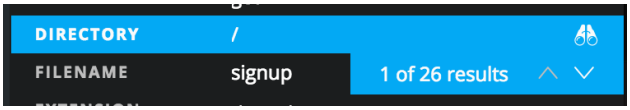
To select which side of the conversation to show, Request, Response, or both, click one or both of the direction icons. The reconstruction is refreshed with the selected information.

Note: If you do not see any data, you may have deselected both Request and Response. You must select one of the two to see data displayed.

View Event Metadata for an Event

When examining events in the Text Analysis panel, Packet Analysis panel, or File Analysis panel, you can click to show the associated metadata in an adjacent panel, the Event Meta panel.

When viewing Text Analysis and the Event Meta panel, hovering over the meta key/meta value pairs reveals a pair of binoculars if the meta value is searchable in the raw text. This is an example of the binoculars icon when hovering over the **Directory** and / meta key/meta value pair.

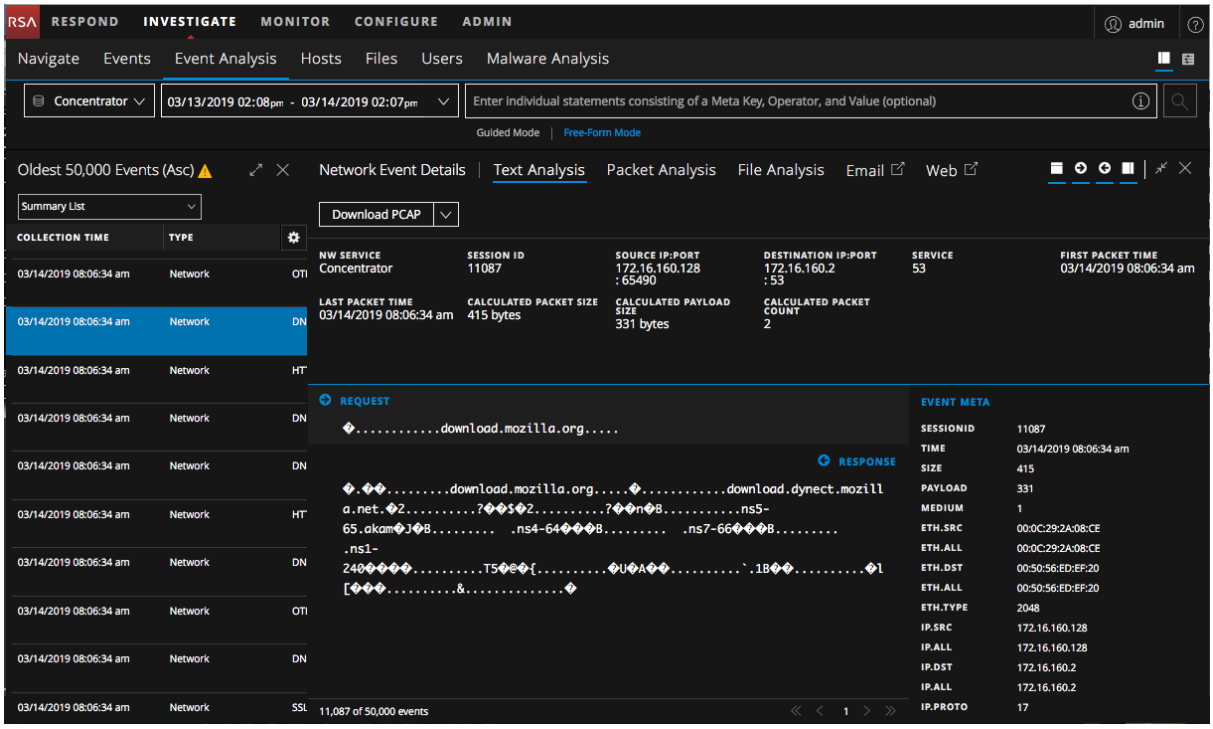


Clicking the icon triggers a search for the meta key/meta value pair (case-insensitive) in the Text Analysis panel and each instance is highlighted. In the Event Meta panel, the highlighted row has a count of the results and a scroller that you can use to quickly find each result in the Text Analysis panel. You can view each highlighted location of the data that triggered generation of the meta key, going forward to view the next, and back to view the previous.

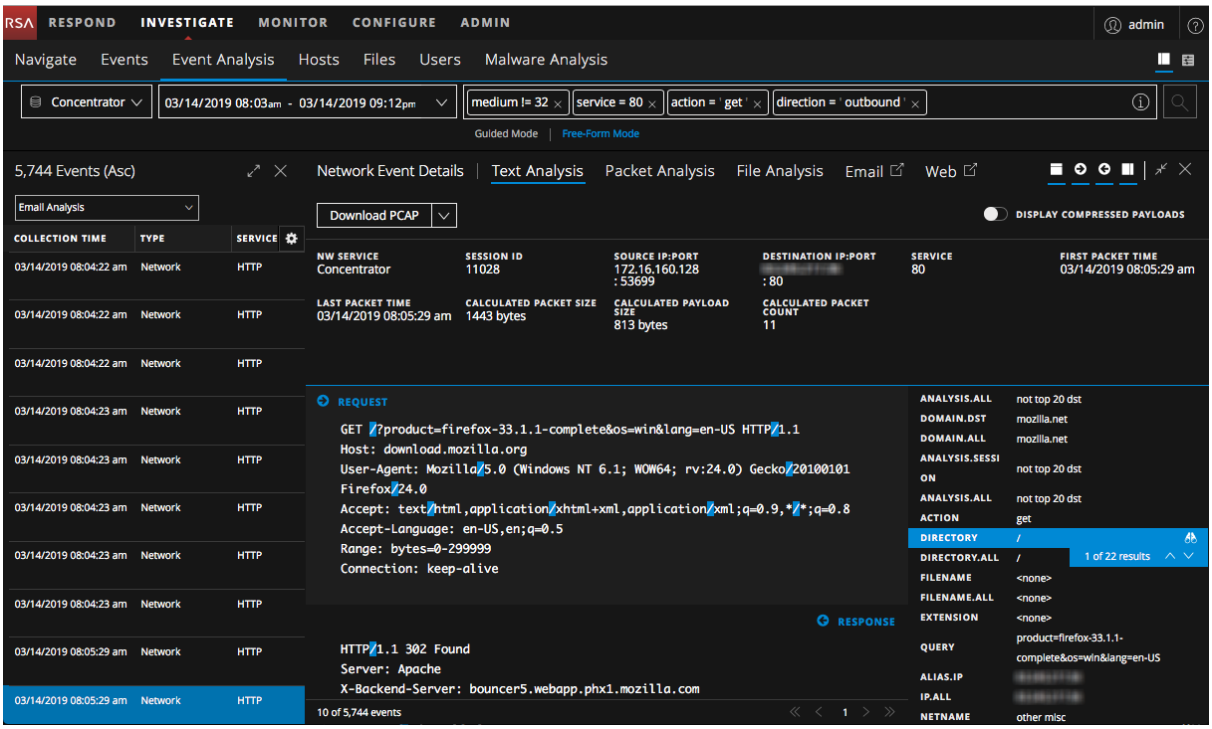
Only meta keys that have relevant values inside the RAW text are searchable. You can search only one meta key at a time. If the value is currently hidden due to truncation of a text entry with more than 3000 characters, the text entry is expanded to reveal the found meta value.

To search the raw text for meta values that triggered a meta key:

1. Open a network event in the Text Analysis panel.



2. In the toolbar, click to open the Event Meta panel. As you hover over the meta key:value pairs in the list, a binoculars icon identifies values that are searchable in the Text Analysis panel.
3. To search for the value in the raw text, click a row that has the binoculars icon, indicating it is searchable.
   If no relevant occurrence of the value is in the text, the value that you are searching for is highlighted in the Event Meta panel and nothing is highlighted in the Text Analysis panel.
   If one or more relevant instances of the value is found in the Text Analysis panel, each occurrence is highlighted. The value that you are searching for is highlighted in the Event Meta panel and the scroller is visible.



4. To remove the highlighting, close the Event Meta panel, click the same meta key/meta value pair in the Event Meta panel, or click a different meta key/meta value pair in the Event Meta panel. The highlighting is removed from the raw text.

Note: When a meta key value is more than 255 characters, you can hover over that meta key to view the complete value.

Show or Hide the Event Header

To hide the Event Header in the Packet Analysis panel, Text Analysis panel, or File Analysis panel, providing more vertical space for the data, click .

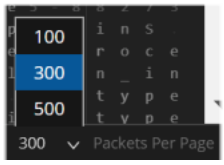
Page Through Events in the Packet and Text Analysis Panels

Pagination controls allow more flexibility in paging through a list of packets or text. In the Packet Analysis panel, you can select the number of packets to display per page, and your selection is saved across logins to the NetWitness application. When a control is unavailable, the control is dimmed; for example, when you are viewing page 1, the and controls are dimmed.

Note: For Text Analysis, pagination controls are available in Version 11.2 and later.

To use pagination controls:

1. (Packet Analysis only) With an event open in the Event Analysis view, click the current number of packets per page (**100**, **300**, or **500**), and select the new number of packets per page from the drop-down menu.

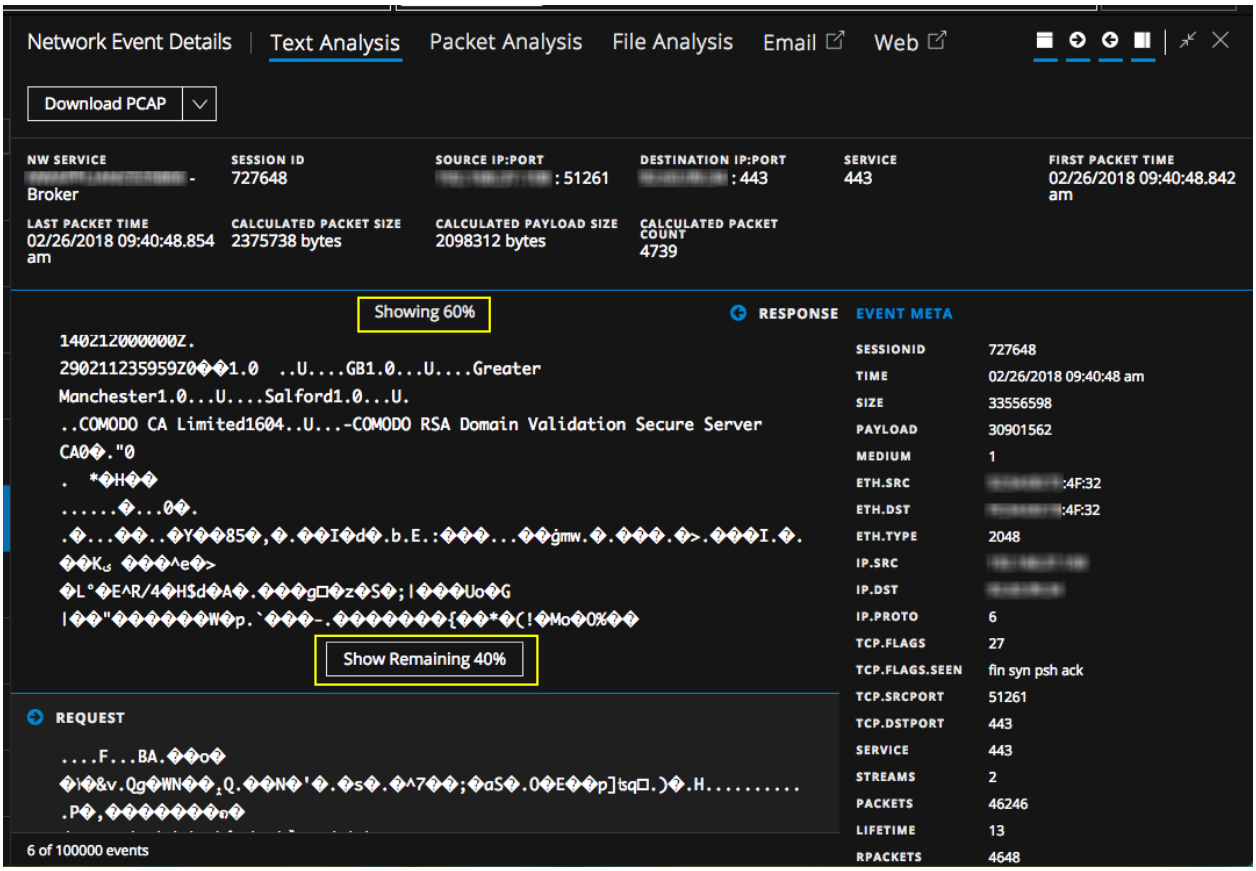


2. To page forward or back, use the page control icons:
   Click ▶ to go to the next page.
   Click ⏭ to go to the last page.
   Click ◀ to go the previous page.
   Click ⏮ to go to the first page.
3. (Packet Analysis only) To go to a specific page, type a page number in the page number field

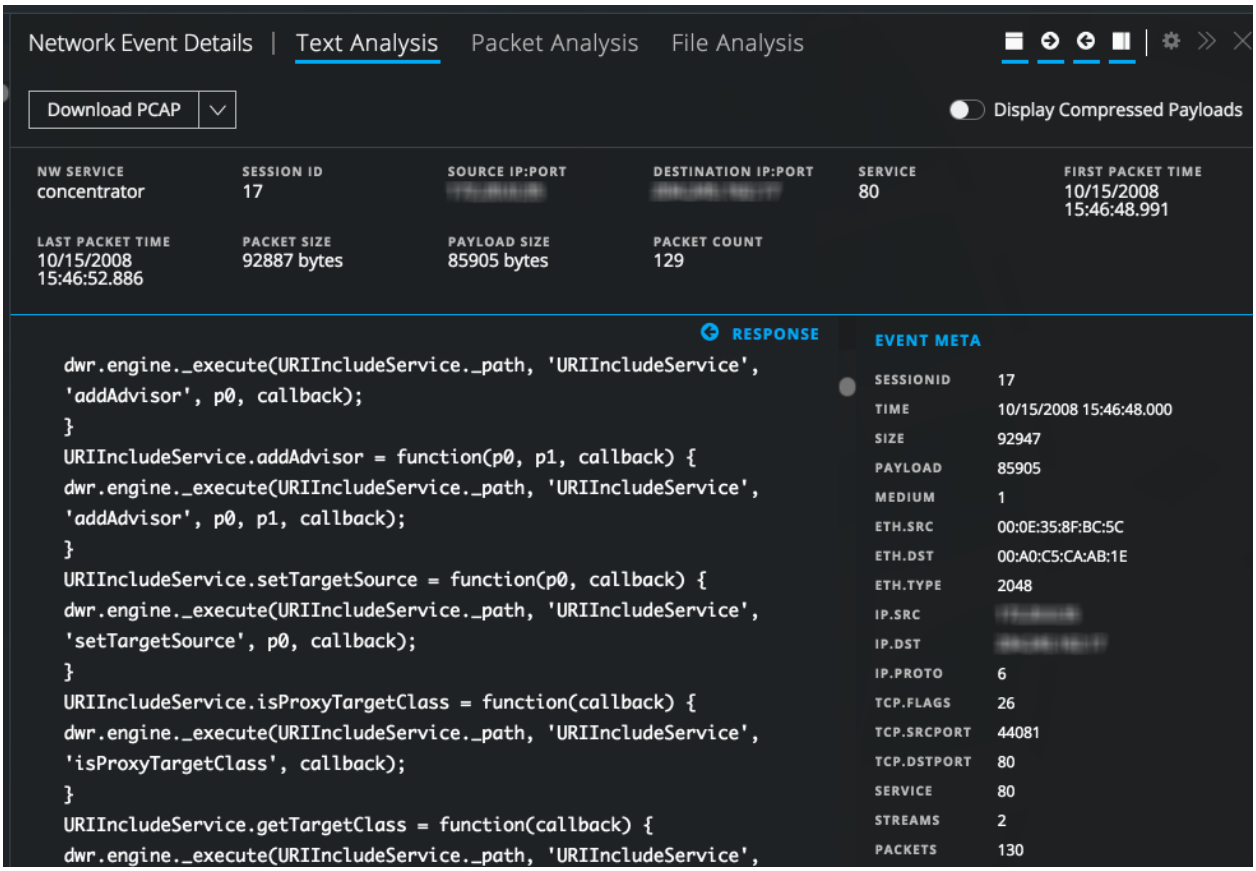
Note: When in the Text Analysis panel, you must navigate manually to the last page before the last page control icon is available.

Expand Truncated Text Entries in the Text Analysis Panel

A reconstruction of a network event in the Text Analysis panel may include requests and responses of many hundred thousands of characters and scrolling through a long entry of more than 6000 characters that is not of interest can waste time. To improve the experience for analysts, all text entries that have more than 6000 characters are truncated to show only the first 2000 characters. This example shows an entry that has more than 2000 characters and a message in the header indicates the percentage of total characters that is being displayed.



You can see that 60% of the characters (the first 2000) are displayed, and click **Show Remaining 40%** to reveal the rest of the entry.



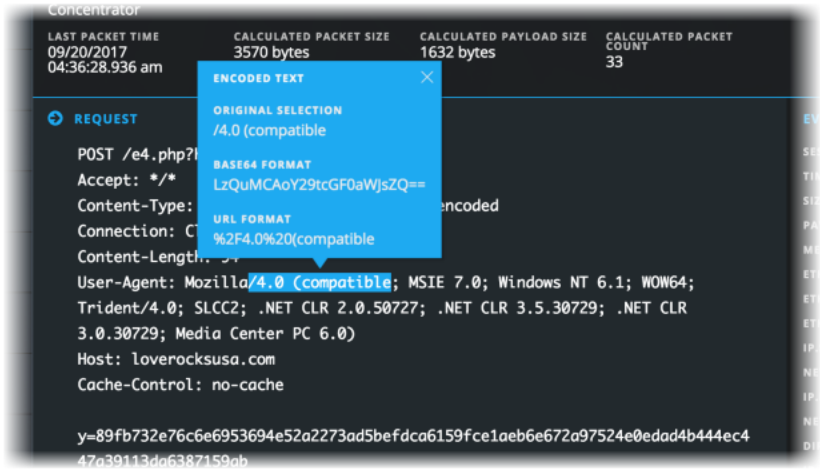
If you search for metadata seen in the Event Meta panel while text is truncated in the Text Analysis panel, the truncated text is searched. If the metadata exists inside hidden text, the text entry expands to reveal the text with the found metadata.

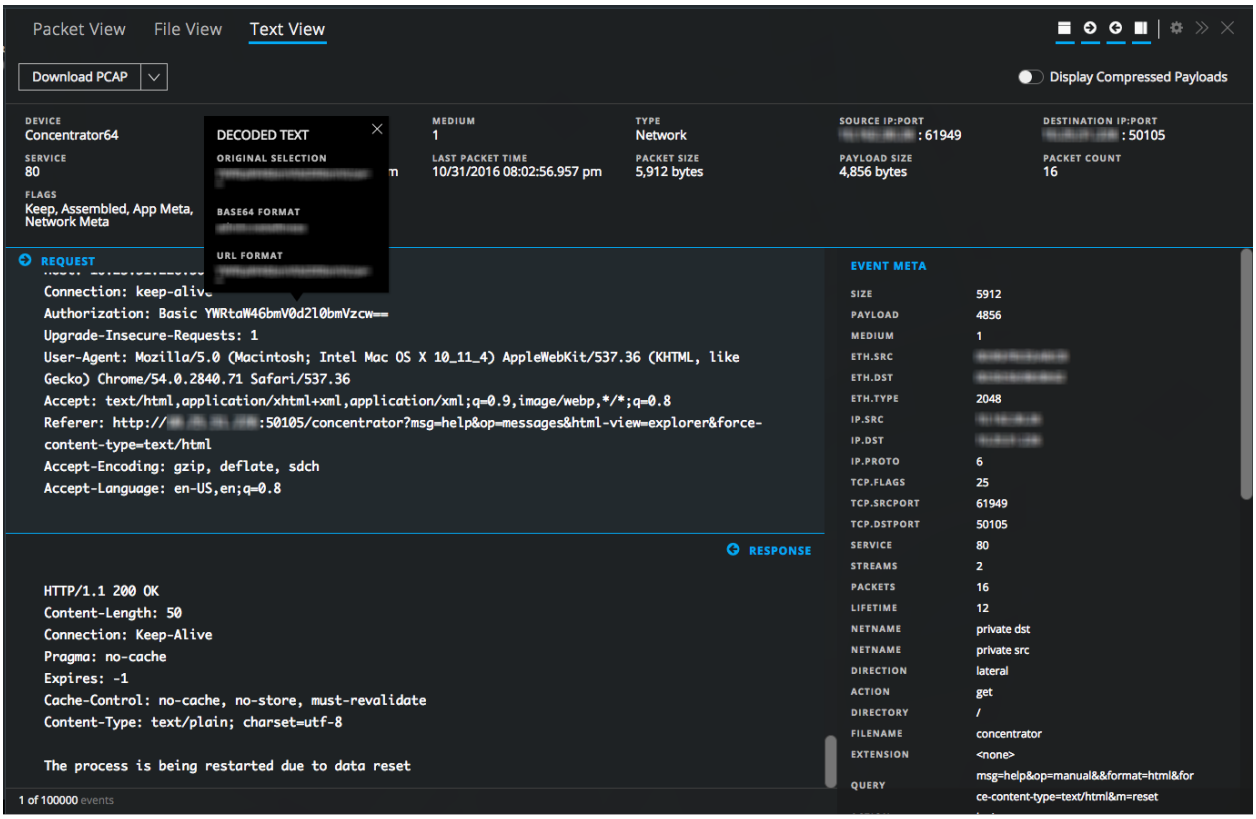
Perform URL and Base64 Encoding and Decoding in the Text Analysis Panel

If a network session being reconstructed in the Text Analysis panel contains Base64 or URL encoded strings, you can decode a string to better understand the session. If the session contains decoded strings for Base64 or URL, you can view a string in its encoded form in order to search for additional instances of the encoded text in other sessions.

When viewing any network session that contains encoded text in the Text Analysis panel, you can select a subset of the text within a single Request or Response to view in either encoded or decoded form. Depending on the content loaded on the Decoder, there may be additional metadata outlining that Base64 or URL encoded data is contained within the session.

Below are examples of a hover box that is displaying URL encoding and Base 64 encoded text.

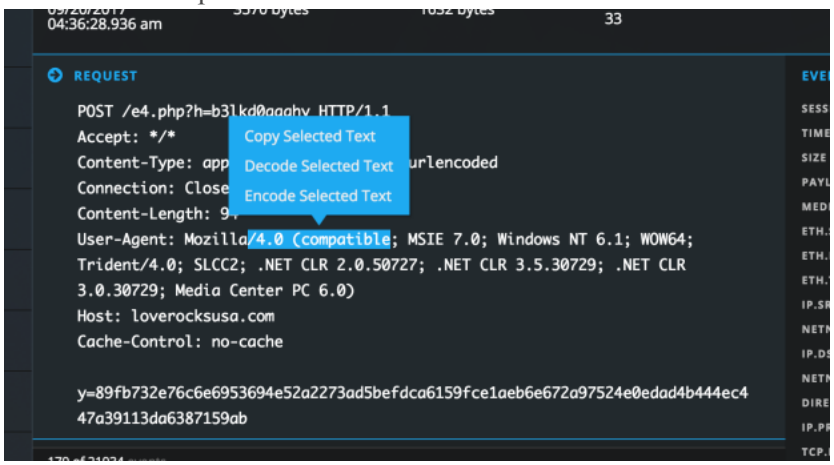




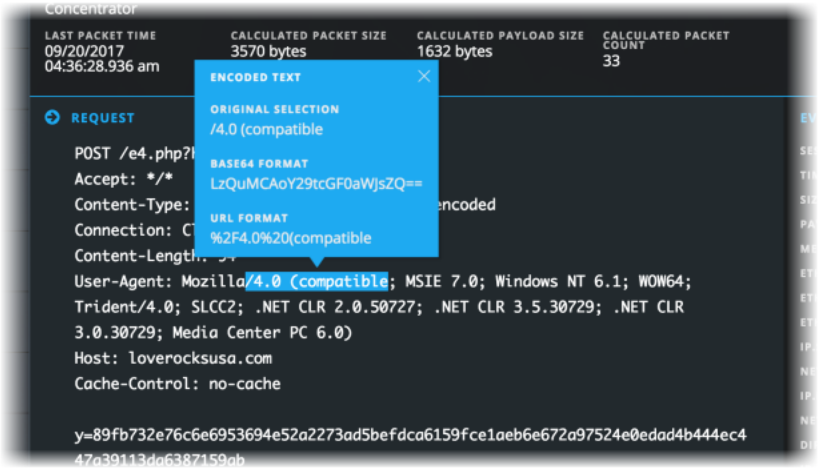
To perform encoding and decoding in the Text Analysis panel:

1. In the **Event Analysis view**, go to the Text Analysis panel of a session that contains encoded or decoded content.
2. To view some decoded text in encoded form, drag to select the text within a single Request or Response.

A menu offers options to encode and decode.



3. Click **Encode Selected Text.**
   The encoded text is displayed in a hover box, which remains in place until you click ■, select different text in the Text Analysis panel, close the Events panel, select another event for reconstruction, or switch to a different reconstruction view.

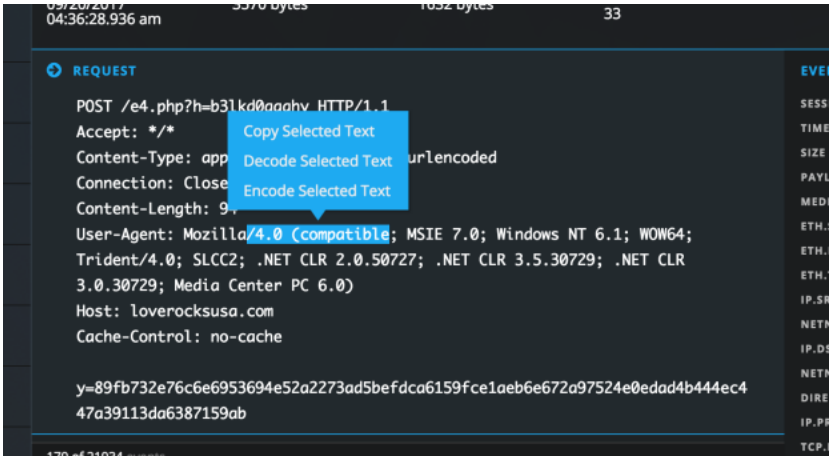


   When a longer text is selected, the hover box is scrollable and large enough to fit the entire selected text and the decoded text.

4. If the session contains encoded text that you want to see in decoded form, drag to select the text within a single Request or Response.
   A menu offers options to encode and decode.

5. Click **Decode Selected Text.**
   The decoded text is displayed in a hover box, which remains in place until you click ■, select different text in the Text Analysis panel, close the Events panel, select another event for reconstruction, or switch to a different reconstruction view.

6. If you want to copy some text from the text reconstruction, do one of the following:
   a. Drag to select some text, right-click, and select **Copy Selected Text** from the popup menu.



   b. Drag to select some text, then select either **Decode Selected Text** or **Encode Selected Text**.
   Within the popup, select the desired text and type **Control-C**.
   The selected text is copied to the clipboard and available to paste in a query.

7. When finished, click ✖ to close the hover box.

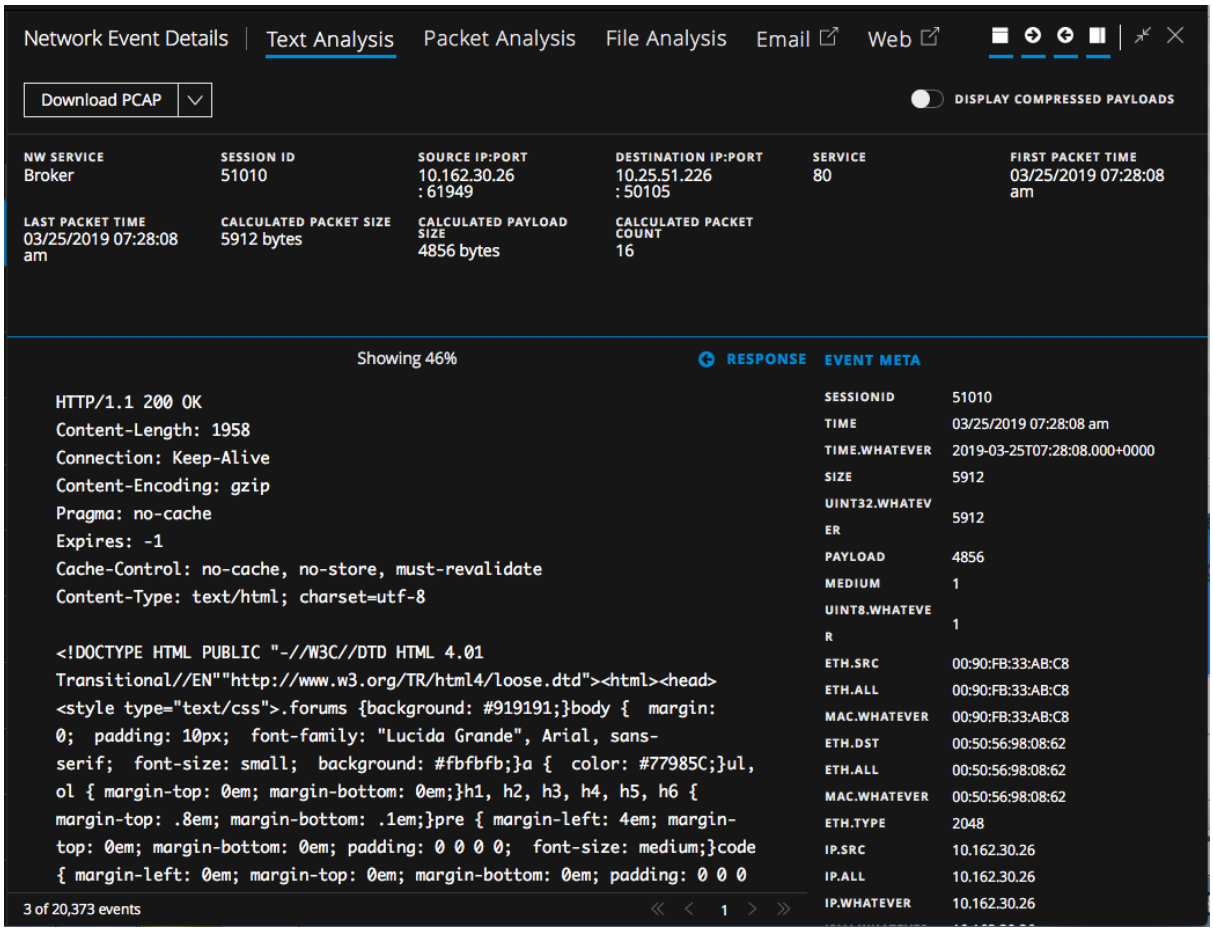
View Decompressed Text in an HTTP Network Session in the Text Analysis Panel

When the content of an HTTP network session is compressed and you are viewing the Text Analysis panel, NetWitness Platform displays decompressed content by default. This helps you to determine if there are any patterns and view the readable characters. You can switch between a compressed and decompressed view of compressed text.

Note: Decompressed text is not available for the Packet Analysis panel, the File Analysis panel, non-HTTP network sessions, and log data.

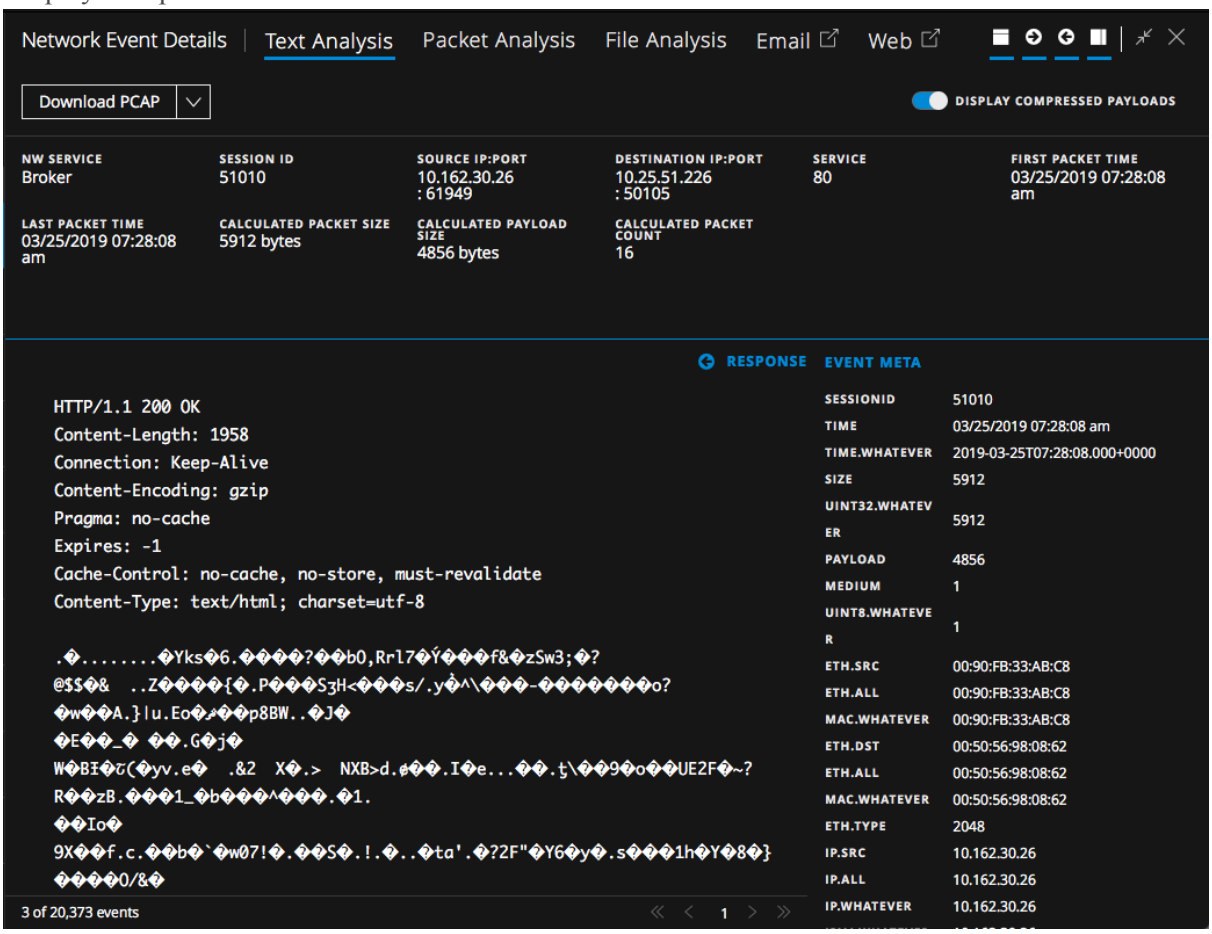
The toggle for changing between compressed and decompressed text is only displayed in the Text Analysis panel, and is enabled only if there is compressed text content.

1. Open the Text Analysis panel of an HTTP session that contains compressed content.
   By default the session is reconstructed with the text decompressed, and above the reconstruction, is the **Display Compressed Payloads** toggle switch.



2. To view the same text in its compressed form, click the toggle switch.
   The view changes so that the compressed text is no longer readable, and the switch indicates the

Display Compressed Packets is on.



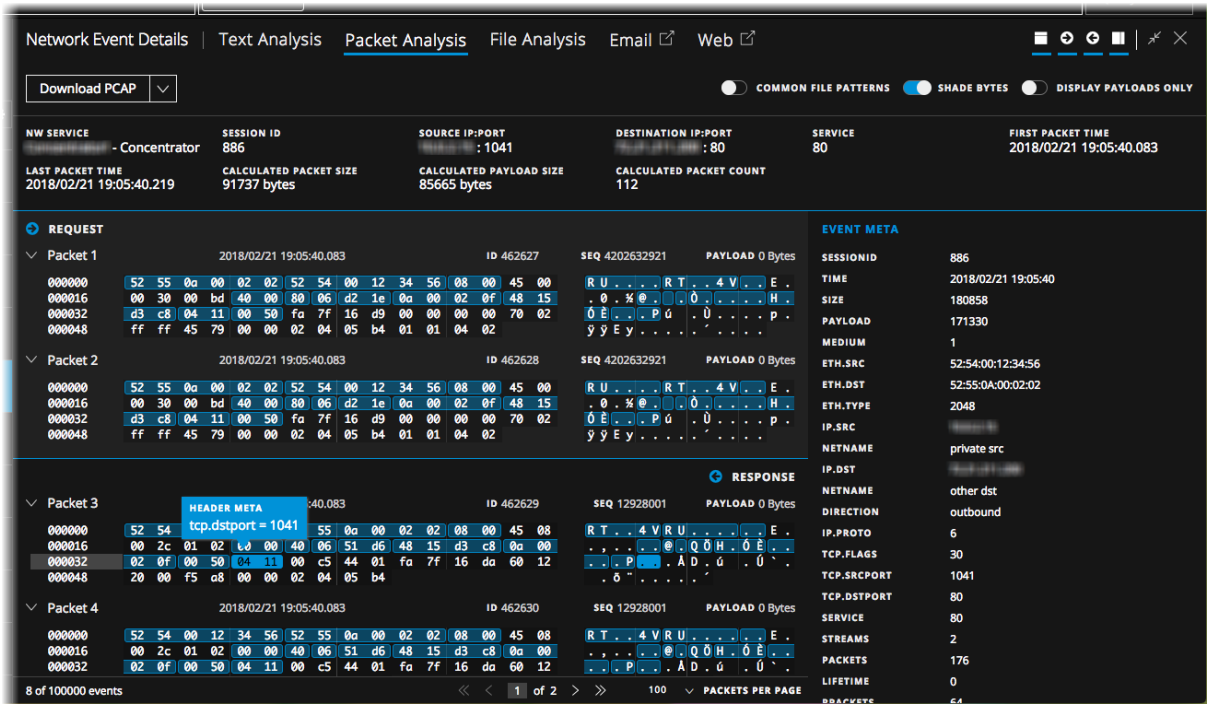
3. To return to the view of decompressed text, click the switch again.

Use the Payload Only Option in the Packet Analysis Panel of a Network Session

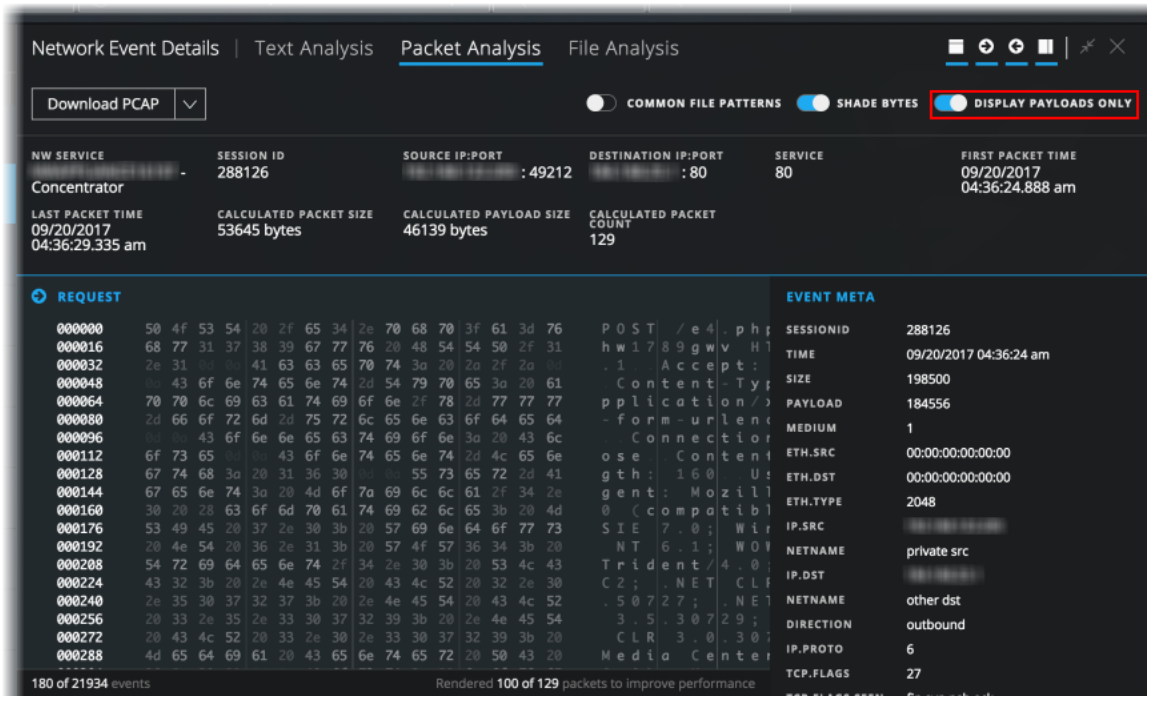
When viewing a reconstruction of a network session in the Packet Analysis panel, you can choose to view only the main payload for each packet. By default, packet header and footer bytes are displayed for each packet. You can hide these by clicking the Display Payloads Only toggle switch. If you are viewing only the payload bytes, you can revert to the default setting by setting the Display Payloads Only toggle switch to on. This setting persists until you change it or refresh the browser.

- With the Display Payloads Only option off, the number of packets, packet header, packet footer, and payload are displayed.
- With the Display Payloads Only option on, no packet header and footer bytes are displayed. Only the packet content of 16 hexadecimal bytes per line and the corresponding ASCII per line is displayed.

1. In the **Event Analysis** view, go to the Packet Analysis panel of a network session.
   By default the session is reconstructed with the packet header, footer, and payload displayed.

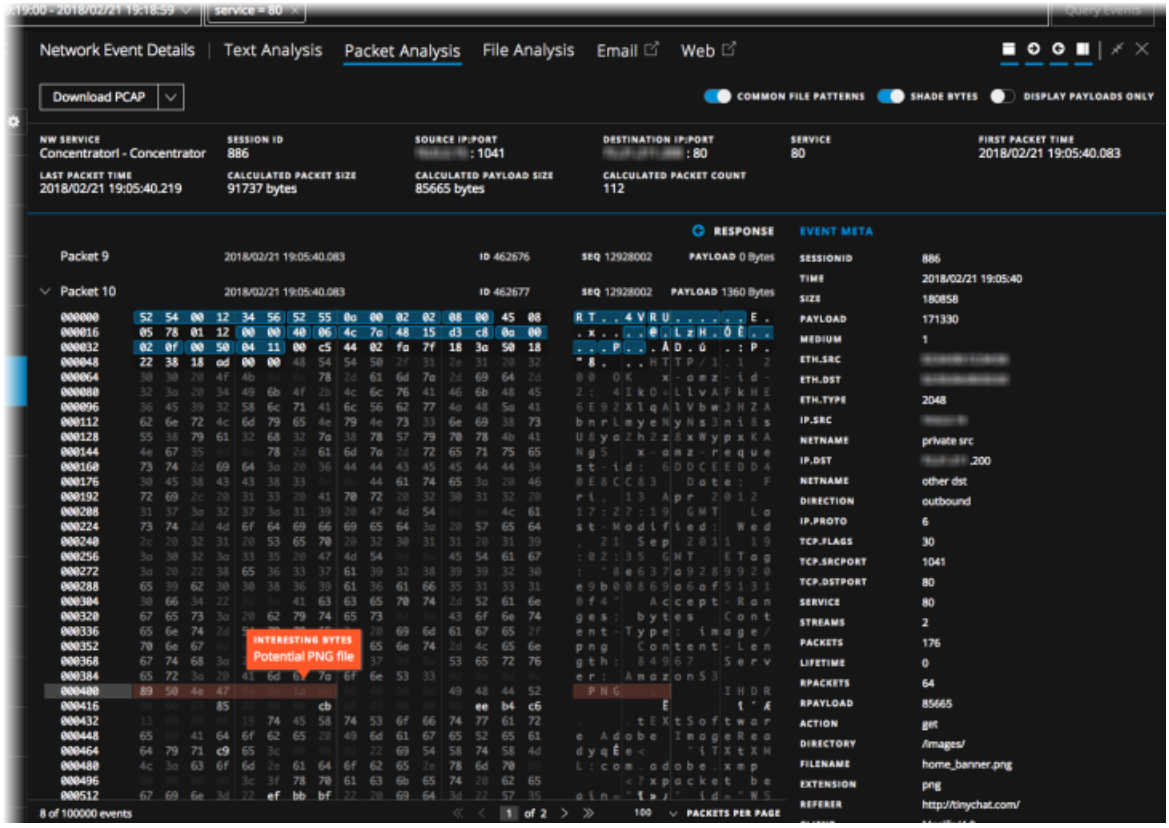


2. To change the view to show only the payload for each packet, click the **Display Payloads Only** toggle switch.
   The view changes to that only the payload is visible and contiguous same-side packets are concatenated together to make the payload more readable and understandable.

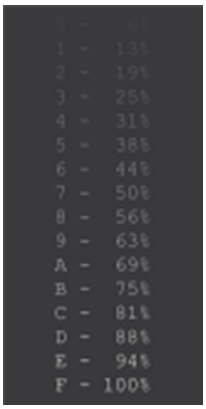


View Highlighted Bytes in the Packet Analysis Panel

When you first open a reconstruction in the Packet Analysis panel, the significant header bytes in each packet are highlighted in blue, and the payload bytes are distinguished using shading to help you understand the contents of the packet. This figure shows the default Packet Analysis with highlighting and byte shading.



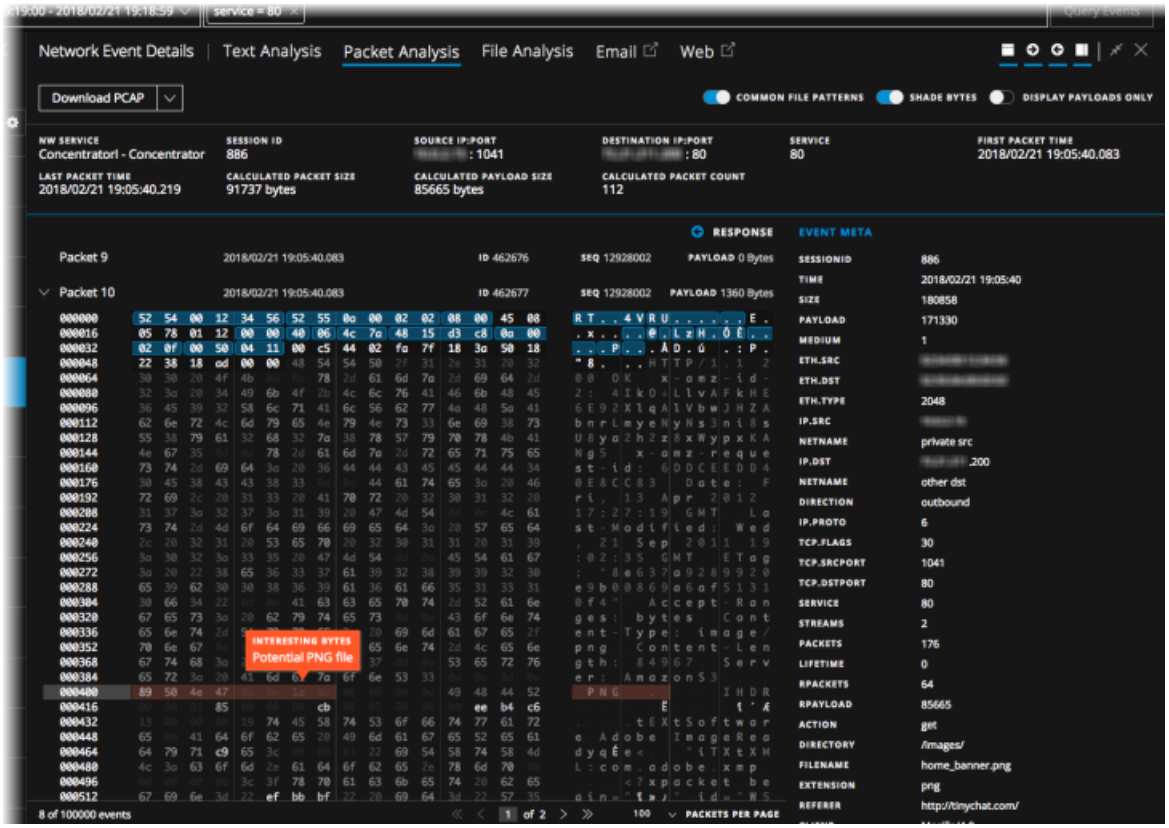
The Shade Bytes option adds shading to identify the different hexadecimal bytes (00 to FF) using degrees of highlighting. Bytes near the lower range are more transparent, and bytes near 255 are more opaque. Both hexadecimal and ASCII bytes are shaded. This is an example of the shading applied to each hexadecimal byte.



The Shade Bytes switch controls the shading of bytes. When you set Shade Bytes on or off, your setting persists until you change it or refresh the browser.

Highlight Common File Types in the Packet Analysis Panel

In the Packet Analysis panel, analysts can show or hide highlighting of certain common file types based on the file signature. When the Common File Patterns feature is turned on, the magic number bytes in the file signature are highlighted in the payload and you can hover over the highlighting to see the potential type of file. In this example, `89 50 4e 47` is highlighted in the hexadecimal payload and `PNG` is highlighted in the ASCII payload. When you hover over the highlighted bytes, the potential file type associated with the magic number is provided in a hover box.



These are the file types and corresponding magic numbers that are highlighted if present in the payload:

File Type	Hexadecimal Signature	ASCII Encoding
DOS Executable / Windows PE	4D 5A	MZ
Portable Network Graphics (PNG)	89 50 4E 47 0D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/Exif	45 78 69 66	Exif

File Type	Hexadecimal Signature	ASCII Encoding
GIF	47 49 46 38 37 61	GIF87a
GIF	47 49 46 38 39 61	GIF89a
Non-portable Executable	5A 4D	ZM
BMP	42 4D	BM
PDF	25 50 44 46	%PDF
Old Office Document (doc, xls, ppt, msg, and other)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
ZIP file formats and formats based on it, such as JAR, ODF, OOXML	50 4B	PK..
7-Zip File Format (7z)	37 7A BC AF 27 1C	7z¼¯'
Java Class File, Mach-O Fat Binary	CA FE BA BE	Êþº¾
Postscript	25 21 50 53	%!PS
Unix/Linux Shell script	23 21	#!
Executable and Linkable Format (ELF) executables	7F 45 4C 46	.ELF

To view common file signatures in the Packet Analysis panel:

1. Go to the Packet Analysis panel, and turn on the **Common File Patterns** option.
   If there is more then one highlight in view, all are shown.
2. To view the hover box, place the cursor over the highlighting.

Look Up Additional Context in the Event Analysis View

The information in this topic applies to RSA NetWitness® Platform Version 11.2 and later. In earlier versions, you can look up additional context in the Navigate view or the Events view as described in Look Up Additional Context for a Data Point.

From the Event Analysis view, you can look up details and intelligence about elements associated with an event in the Context Hub. These elements, or entities, are identifiers, such as an IP address, a user name, a host name, a domain name, a file name, or file hash. The data from configured sources, such as RSA NetWitness Endpoint, can help you understand what is happening.

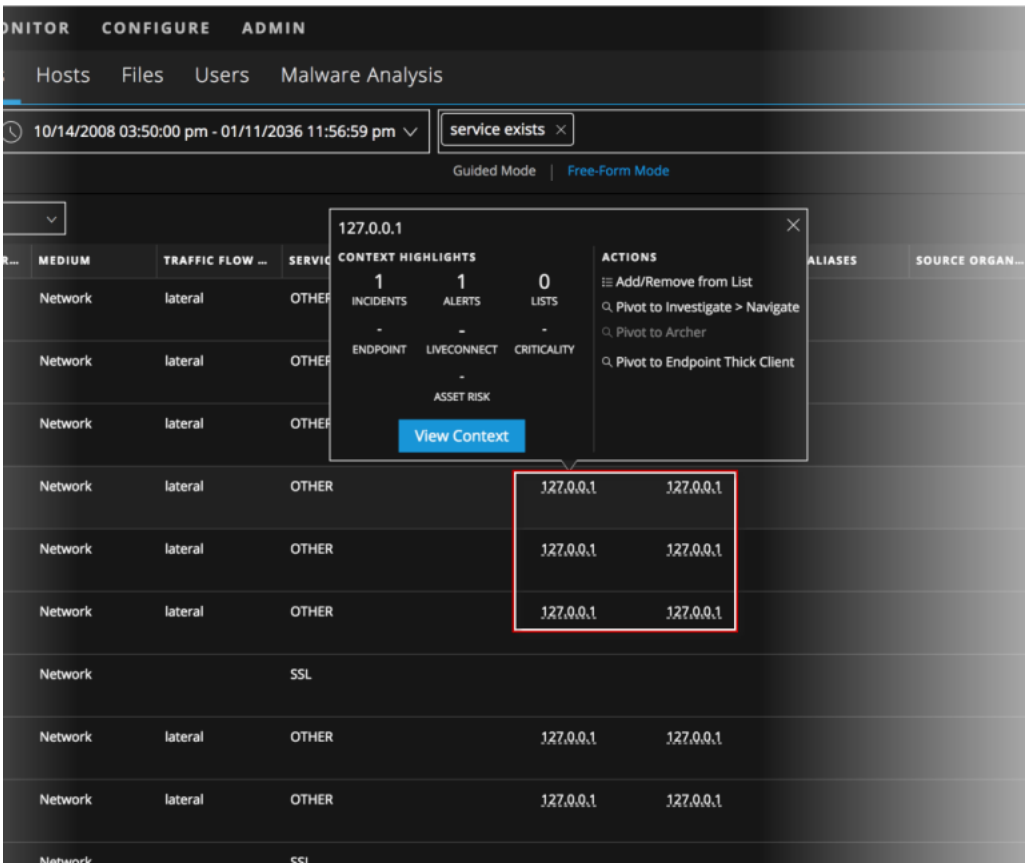
Note: To enable viewing of contextual information, your administrator must add the Context Hub service in RSA NetWitness Platform and configure data sources for the Context Hub service as described in the *Context Hub Configuration Guide*. Analysts also need a role with the permission `Context Lookup` as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

The Context Hub is a centralized service that aggregates data about entities from multiple configurable data sources. This data can extend your investigation with additional context beyond the immediate results of a specific query. For example, the Context Hub can tell you if a given entity has been mentioned in any incidents, alerts, feeds, or community intelligence publications.

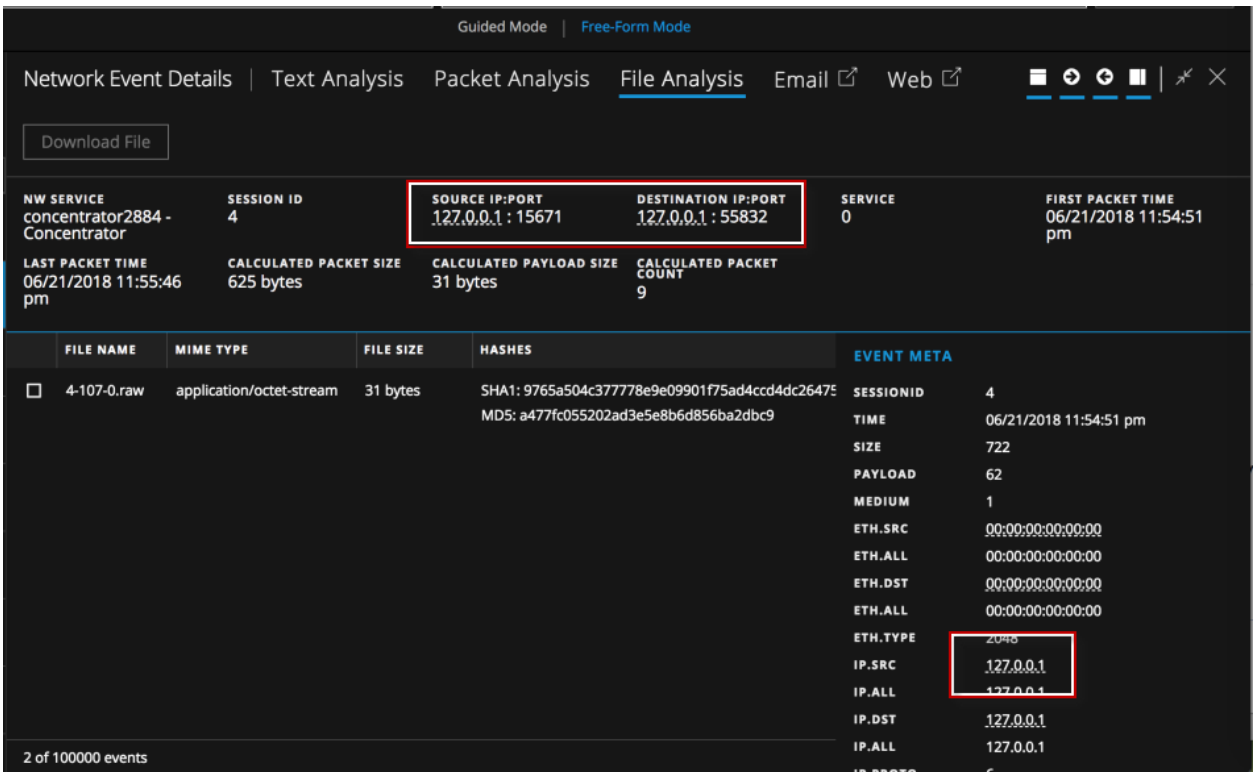
In the Events panel, the Event Header, or the Event Meta panel, you can see underlined entities. If an entity is underlined, NetWitness Platform is populating information about that entity type in the Context Hub. There may be additional information available about that entity in the Context Hub.

The following figure shows underlined entities in the Events panel with the context tooltip open. The context tooltip has two sections: Context Highlights and Actions.

- The information in the Context Highlights section helps you to determine the actions that you would like to take. It can show related data for Incidents, Alerts, Lists, Endpoint, Live Connect, Criticality and Asset Risk. Depending on your data, you may be able to click these items for more information.
- The **Actions** section lists the available actions. In the example, the Add/Remove from List, Pivot to Investigate > Navigate, Pivot to Archer, and Pivot to Endpoint Thick Client options are available.



The following figure shows underlined entities in the Event Header and the Event Meta panel.



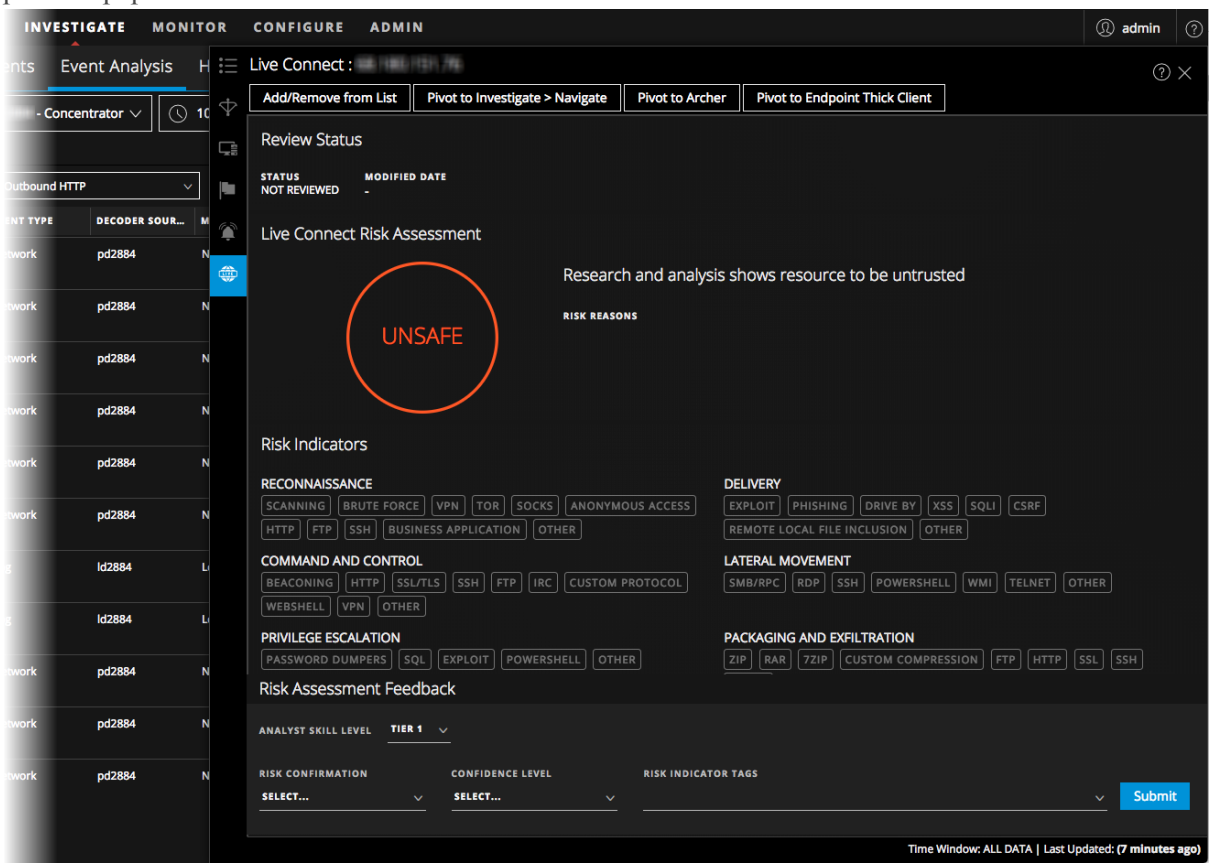
When you click View Context in the context tooltip, the Context Hub queries the configured data sources for relevant information, and the Context Lookup panel opens from the right side of the browser window. The Context Lookup panel is populated with the information from the Context Hub as it becomes available. You can perform another lookup by using the View Context option on another entity, and the Context Lookup panel is updated with that entity's information.

In the Context Lookup panel, you can view and explore individual data sources for further investigation. For a detailed description of the information displayed for each data source on the Context Lookup panel, see Context Lookup Panel.

You can also take any available action in the Actions section.

To view information in the Context Lookup panel in the Event Analysis view:

1. Hover over different meta values to see the data sources for which data is available.
   A context tooltip displays a list of the context data available for the selected meta value.
2. Click **View Context** in the context tooltip to open the Context Lookup panel.
   The Context Lookup panel opens from the right side of the browser window. The Context Lookup panel is populated with the information from the Context Hub as it becomes available.



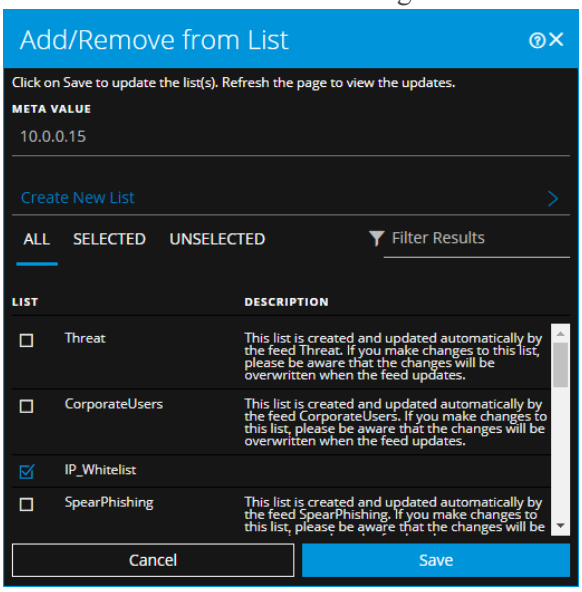
3. To perform actions on an entity, select one of the available actions in the context tooltip: Add /Remove from List, Pivot to Investigate > Navigate, Pivot to Archer, Pivot to Endpoint Thick Client. For more information, see Pivot to Investigate > Navigate, Pivot to Archer, Pivot to NetWitness Endpoint Thick Client, and Add an Entity to a Whitelist.

Note: The Pivot to Archer link is disabled when Archer data is not available or when the Archer data source is not responding. Check that the RSA Archer configuration is enabled and configured properly.

Add an Entity to a Whitelist

You can add any underlined entity to a list, such as a Whitelist or Blacklist, from a context tooltip. For example, to reduce false positives, you may want to whitelist an underlined domain to exclude it from the related entities.

1. In the Events panel, the Event Header, or the Event Meta panel, hover over the underlined entity that you would like to add to a Context Hub list.
   A context tooltip showing the available actions is displayed.
2. In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.
   The Add/Remove from List dialog shows the available lists.



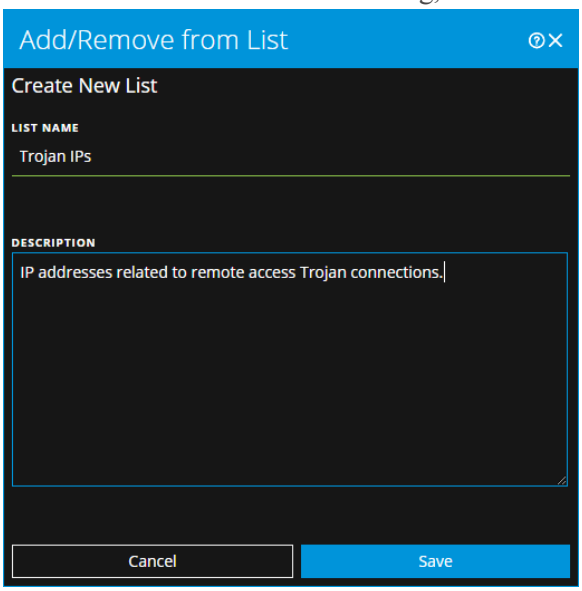
3. Select one or more lists and click **Save**.
   The entity is added to the selected lists. Add/Remove from List Dialog provides additional information.

Create a List

You can create lists in Context Hub from the Event Analysis view. In addition to using lists to whitelist and blacklist entities, you can use lists to monitor entities for abnormal behavior. For example, to improve the visibility of a suspicious IP address and Domain under investigation, you may want to include them in two separate lists. One list could be for domains suspected of being related to command and control connections, and another list could be for IP addresses related to remote access Trojan connections. You can then identify indicators of compromise using these lists.

To create a list in Context Hub:

1. In the Events panel, the Event Header, or the Event Meta panel, hover over the underlined entity that you would like to add to a Context Hub list.
   A context tooltip showing the available actions is displayed.
2. In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.
3. In the Add/Remove from List dialog, click **Create New List**.



4. Type a unique **List NAME** for the list. The list name is not case sensitive.
5. (Optional) Type a **DESCRIPTION** for the list.
   Analysts with the appropriate permissions can also export lists in CSV format to send to other analysts for further tracking and analysis. The *Context Hub Configuration Guide* provides additional information.

Pivot to Investigate > Navigate

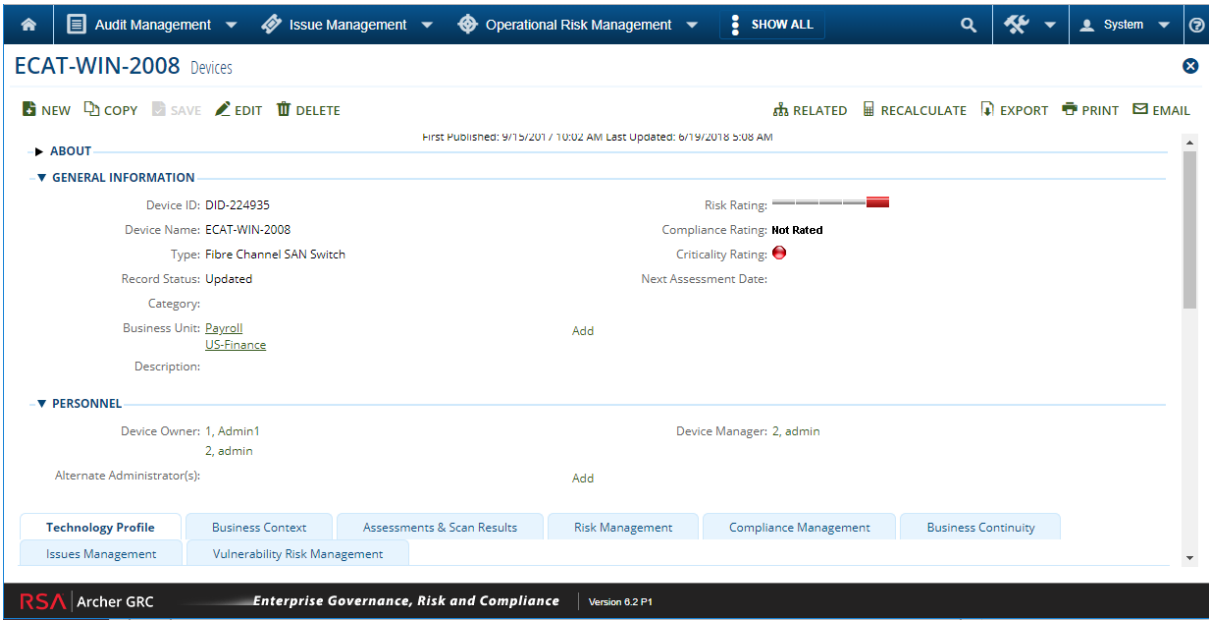
For a more thorough investigation of an entity, you can open the the Navigate view.

1. In the Events panel, the Event Header, or the Event Meta panel, hover over any underlined entity.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate > Navigate**.
   The Navigate view opens, enabling you to perform a deeper dive investigation. For more information, see Investigating Metadata in the Navigate View.

Pivot to Archer

For viewing more details about the device in RSA Archer® Cyber Incident & Breach Response, you can pivot to the device details page. This information is displayed only for IP address, host, and Mac address.

1. In the Events panel, the Event Header, or the Event Meta panel, hover over any underlined entity (IP address, host, and Mac address).
2. In the **ACTIONS** section of the context tooltip, select **Pivot to Archer**.
3. The device details page in **RSA Archer Cyber Incident & Breach Response** opens if you are logged in to the application, otherwise the login screen is displayed.



Note: The Pivot to Archer link is disabled when Archer data is not available or when the Archer Datasource is not responding. Check that the RSA Archer configuration is enabled and configured properly.

For more information, see the *Archer Integration Guide*.

Pivot to NetWitness Endpoint Thick Client

If you have the NetWitness Endpoint thick client application installed, you can launch it through the context tooltip. From there, you can further investigate a suspicious IP address, Host, or MAC address.

1. In the Events panel, the Event Header, or the Event Meta panel, hover over any underlined entity.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint Thick Client**.
   The NetWitness Endpoint thick client application opens outside of your web browser.

For more information on the thick client, see the *NetWitness Endpoint User Guide*.

Download Data in the Event Analysis View

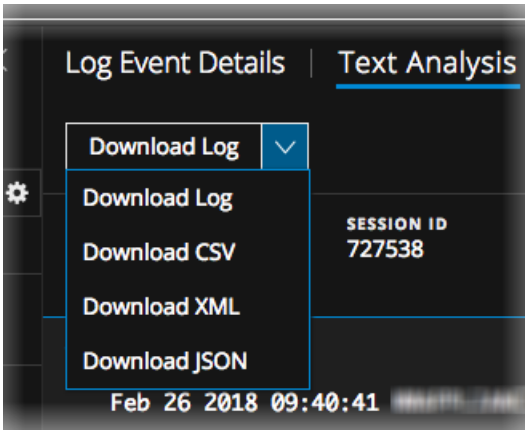
In the Event Analysis view, you can download events, logs, and files.

Download a Log in the Text Analysis Panel

When viewing a log reconstruction in the Text Analysis panel, you can download a log file in the following formats using options in the Download Log drop-down menu:

- Raw log (log) using the **Download Log** option
- Comma-separated values (CSV) using the **Download CSV** option
- Extensible Markup Language (XML) using the **Download XML** option
- JavaScript Object Notation (JSON) using the **Download JSON** option

This is an example of a log reconstruction with the Download Log menu options displayed.



Note: The Download Log option is applicable only for endpoint events that have at least one meta value exceeding 256 characters. For an endpoint event, the raw log is populated only when the meta value exceeds 256 characters. Long running or historically downloaded files are not downloadable. For example, the meta values like launch arguments can exceed 256 characters. In this case, 256 characters are available as meta value while the full value is available in the raw log to view.

The downloaded log file contains the log and is named to help identify the service on which the log was collected, the session ID, and the file type. This is an example of the filename for a raw log: **Concentrator_SID2.log**. The exported log file is named using the following convention:

`<service-ID or host name>_SID<n>.<filetype>`

where:

- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved.
- `SID<n>` is the session ID number.

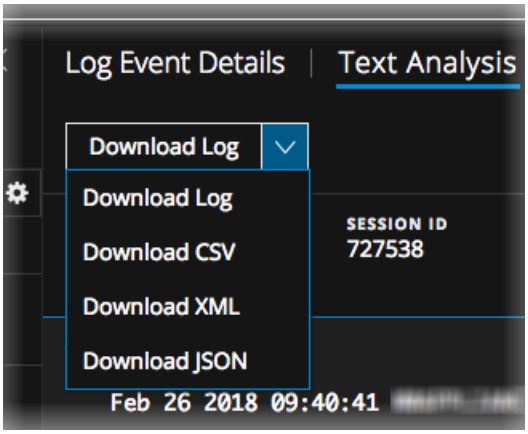
- `<filetype>` identifies the format of the downloaded log. These are the possible log types: raw log, CSV, XML, and JSON. By default, the format is a raw log.

Note: Some formats do not have time stamps or the device IP where the event was generated, so a log downloaded in CSV, XML, or JSON format has an extra value called `timestamp` along with the raw log content. The additional information inside the log is in this form: `Log timestamp="1490824512" source="10.12.35.65".`

To download the log for a session:

In the Text Analysis panel of a log event, select one of the file formats for the downloaded log.

- To download the log as a raw log (the default format), click **Download Log**.
- To download the log in one of the other formats, click the downward arrow on the **Download Log** button, and select one of the file formats for the downloaded log.



The log file is downloaded to your local file system in the format specified. If you initiate a download and move away from the view while the log is being extracted and before the log starts to download, the log is not downloaded in your browser. A message notifies you that you can find the downloaded log in the job queue.

Download Network Event Data in the Text Analysis Panel or the Packet Analysis Panel

When viewing a reconstructed network event in the Packet Analysis panel or the Text Analysis panel, you can export network data files for further analysis. The download includes events for the current time range and drill point. You can download the data in these forms:

- The entire event as a packet capture (`*.pcap`) file using the **Download PCAP** option.
- The payload as a `*.payload` file using the **Download All Payloads** option.
- The request payload as a `*.payload1` file using the **Download Request Payload** option.
- The response payload as a `*.payload2` file using the **Download Response Payload** option.

This is an example of the filename for a PCAP file: `C01 - Concentrator_SID1697309.pcap`. The exported network data file is named using the following convention:

<service-ID or host name>_SID<n>.<filetype>

where:

- <service-ID or host name> is the name of the service (for example a Concentrator or Broker) where the session was saved.
- SID<n> is the session ID number.
- <filetype> is pcap, payload, payload1, or payload2.

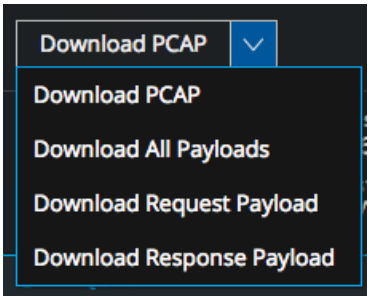
The network data is downloaded directly into your browser if the download is quick. If the download takes longer due to network factors or file size, the file is downloaded in the background and the task is tracked in the Jobs queue. In this case, you can check your jobs in the queue and get the file when the download is complete.

Note: If you initiate a download and move away from the view while the file is being extracted and before the file starts to download, the file is not downloaded in your browser. A message notifies you that you can find the downloaded document in the job queue.

To export an event as a network data file:

Go to the Packet Analysis panel of a network event, and select one of the file formats for the downloaded file.

- To download the event as a PCAP file (the default format), click **Download PCAP**.
- To download the event in one of the other formats, click the downward arrow on the **Download PCAP** button, and select one of the file formats for the downloaded event data.



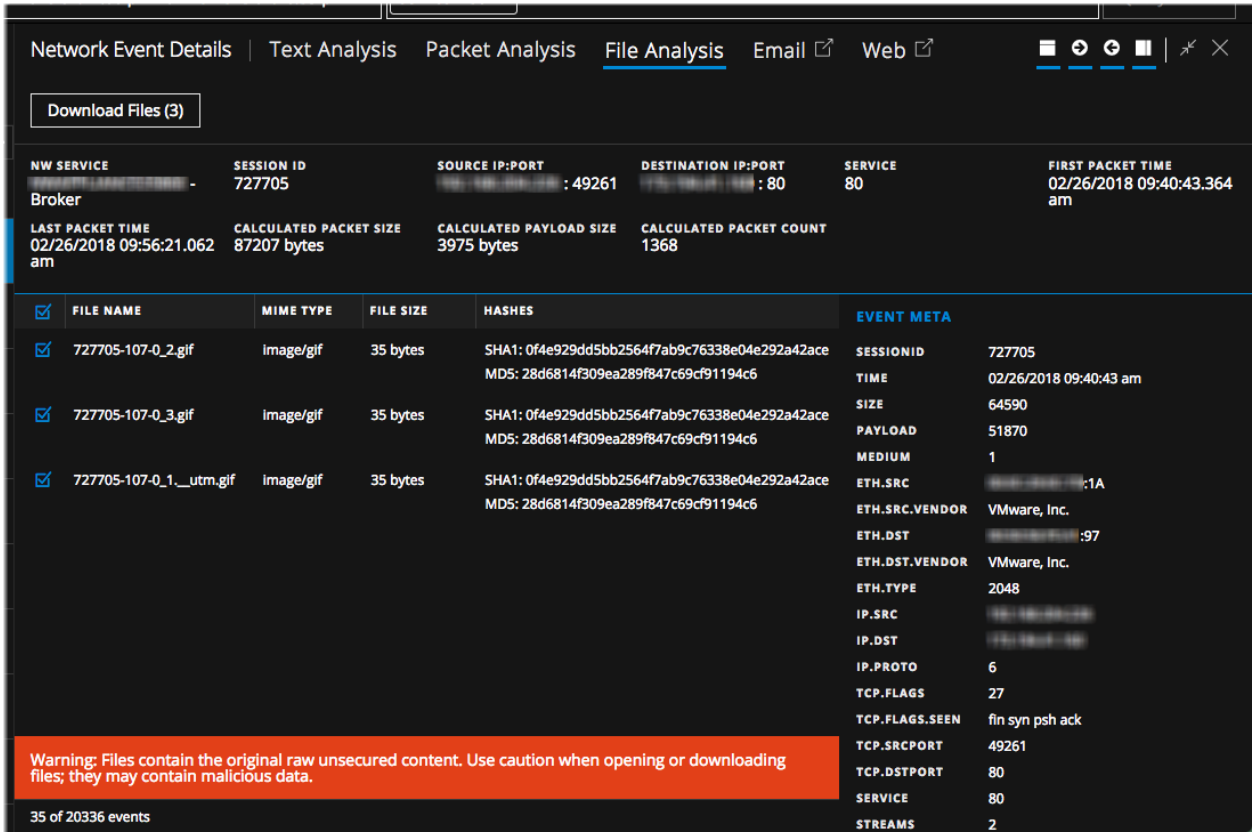
The network data file is downloaded to your local file system in the format specified.

Download Files from a Network Event in the File Analysis Panel

When viewing reconstructed network events that contain files in the File Analysis panel, you can select one or more files, or all files, to download to your local file system.

Note: If you initiate a download and move away from the view while the file is being extracted and before the file starts to download, the file is not downloaded in your browser. A message notifies you that you can find the downloaded file in the job queue.

When files are selected, the Download Files button becomes active and reflects the number of files selected.



Clicking Download Files exports the selected files as a password-protected zip archive. The password to open the exported archive is `netwitness`. Exporting the files in this form ensures that:

- The archive is not quarantined by antivirus software.
- Potentially malicious files are not automatically opened by the default application and executed.

This is an example of the filename for an archive: `C01 - Concentrator_SID1697309_FC1.zip`. The exported archive is named using the following convention:

`<service-ID or host name>_SID<n>_FC<n>.zip`

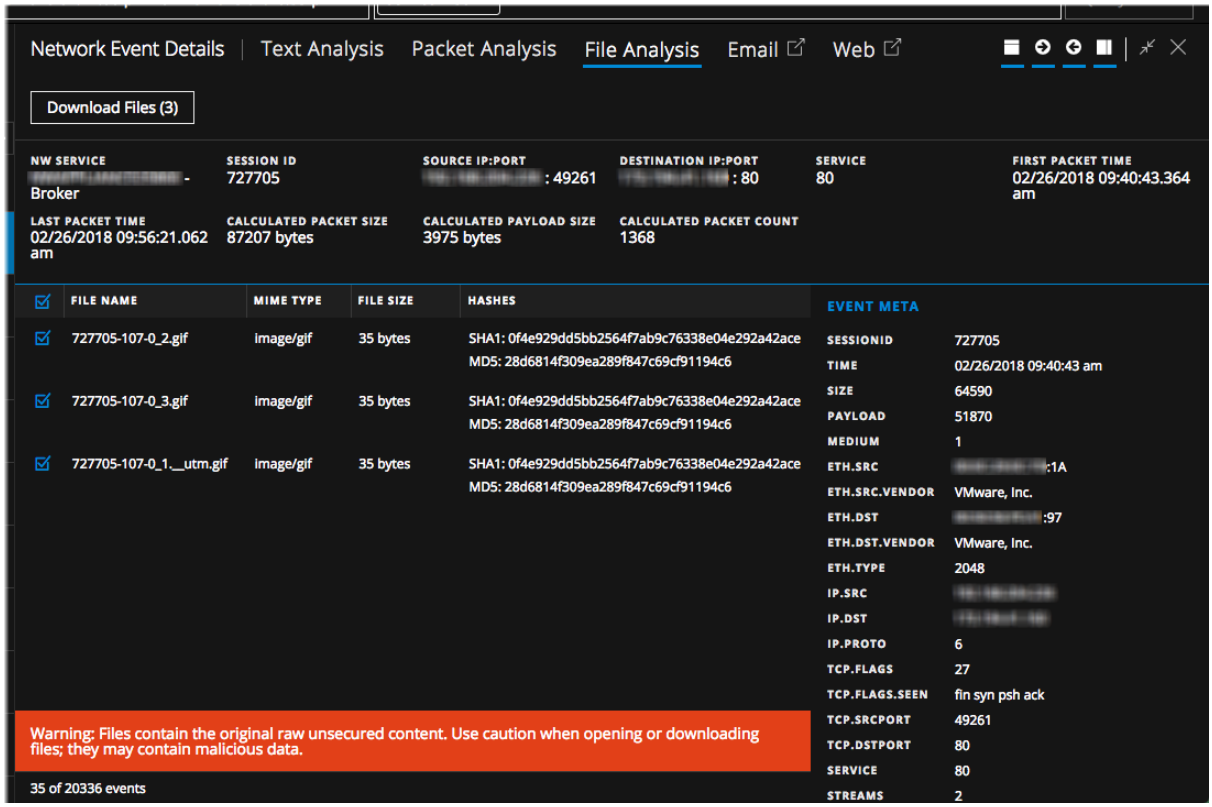
where:

- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved.
- `SID<n>` is the session ID number.
- `FC<n>` is the file count or number of files in the archive.

Caution: Caution is advised when unzipping and opening files that are associated with a default application; for example, an Excel spreadsheet may automatically open in Excel before you have a chance to verify it is safe.

To export files in a reconstructed event:

1. In the **Event Analysis** view, go to the File Analysis panel of an event that contains files.



2. Click one or more files that you want to extract, and click **Download File** or **Download Files**.
   The job is scheduled and when complete the selected file are downloaded, in the form of a password-protected zip archive, to the local file system.
3. To open the archive on your local file system, enter the following password when prompted: `netwitness`.

Act on Data in the Event Analysis View

When you have found data of interest in the Event Analysis view, you can do internal lookups to NetWitness Endpoint and RSA Live, as well as external lookups of meta values in community resources such as SANS IP History and ThreatExpert Search.

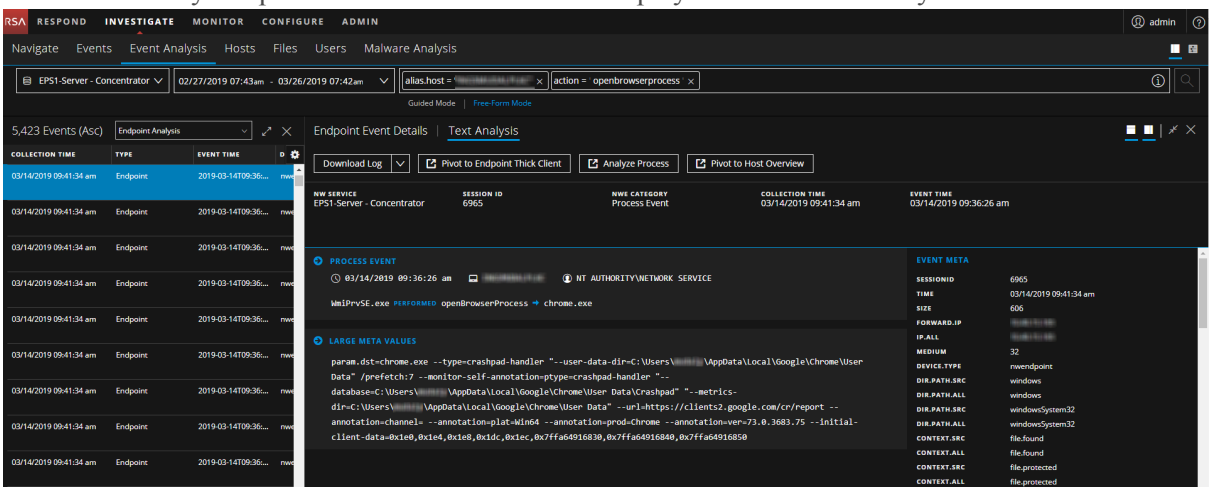
Open an Endpoint Event in the NetWitness Endpoint Thick Client

When viewing an endpoint event in the Text Analysis panel, you can pivot to analyze the same event in NetWitness Endpoint.

Note: Version 4.4.0.x of the NetWitness Endpoint (NWE) thick client must be installed on the same server, the NWE meta keys must exist in the `table-map.xml` file on the Log Decoder, and the NWE meta keys must exist in the `index-concentrator-custom.xml` file. The NWE thick client is a Windows only application. Complete setup instructions are provided in the *NetWitness Endpoint User Guide* for Version 4.4.

To open an event in NetWitness Endpoint:

1. Starting from the Navigate view:
   a. In the **Query** drop-down, select **Advanced**, and enter one of the following queries:
   `nwe.callback_id exists` or `device.type='nwendpoint'`
   Endpoint data is displayed in the Values panel.
   b. Right-click an event, and select **Event Analysis** in the menu.
2. (Version 11.1 and later) Go to **INVESTIGATE > Events Analysis**. In the **Query** drop-down, select **Advanced**, and enter one of the following queries: `nwe.callback_id exists` or `device.type='nwendpoint'`
   Endpoint data is displayed in the Events panel.
3. Select an event.
   The Event Analysis opens with the selected event displayed in the Text Analysis.



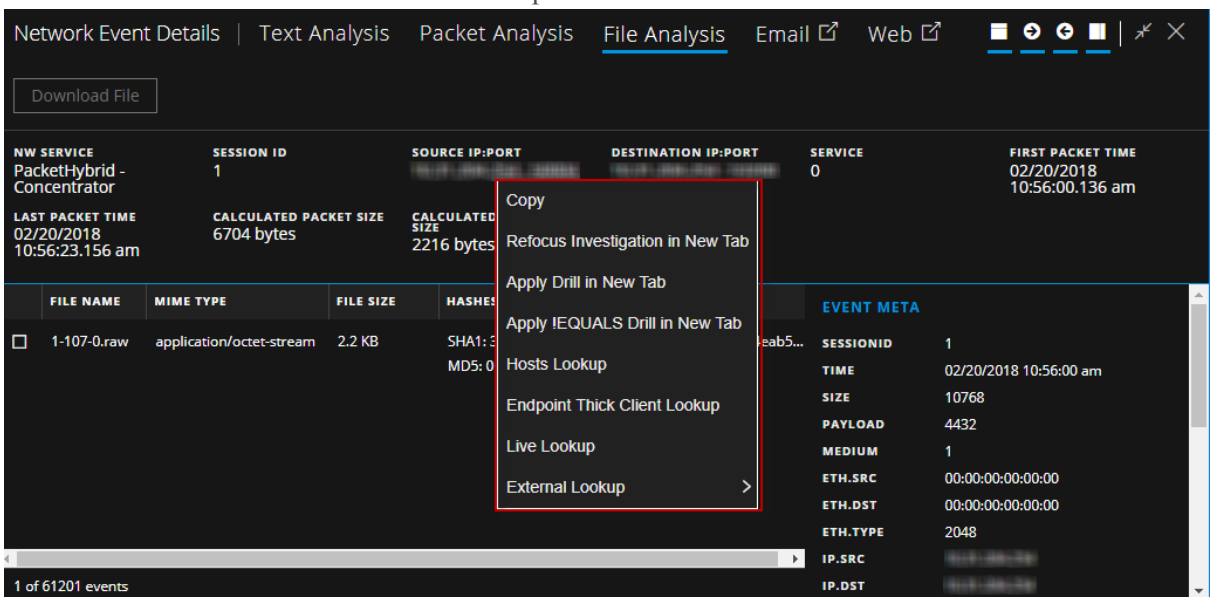
4. In the Event Header click **Pivot to Endpoint.**
   A new browser tab with the url `ecatui://<id>` opens and the NWE Thick Client is launched. If

the NetWitness Endpoint Thick Client is not installed, no data is displayed and the following message is displayed: `Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

Perform Lookups of Meta Values in Event Analysis

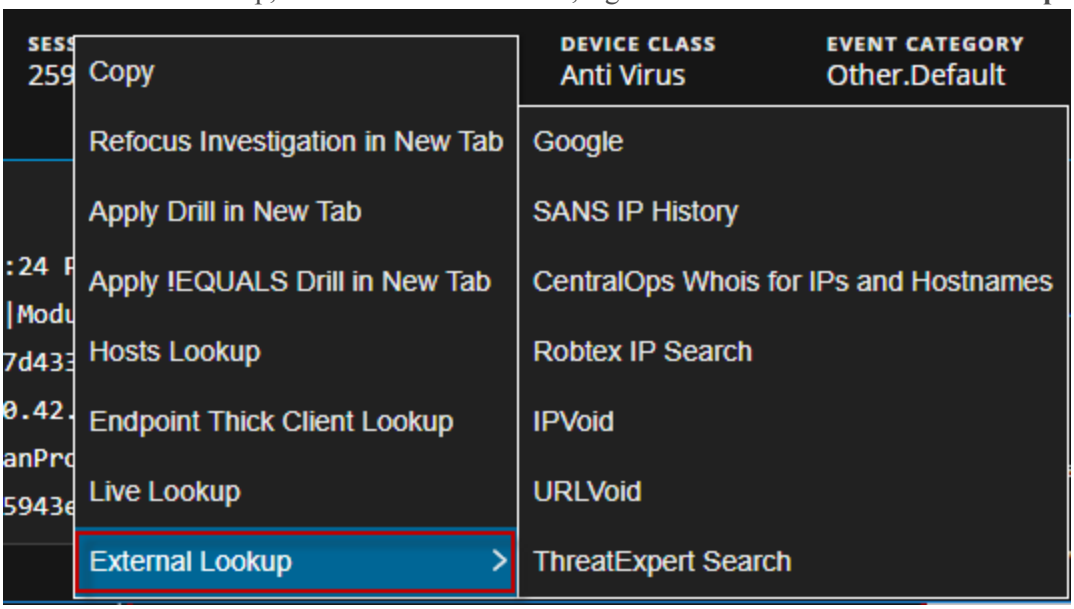
In the Event Analysis view, you can further investigate meta values in an event by right-clicking certain meta values and using the options in a drop-down menu. Not all fields have right-click actions. To perform internal and external lookups:

1. In the Event Analysis view, right-click a meta value in the Events List, the Event Meta panel, or the Event Header. Some meta values have a drop-down menu.



2. Select one of the following internal lookups:
   - **Copy**: Copies the meta value to the clipboard.
   - **Refocus Investigation in New tab**: Launches the another investigation in a new tab with the focus on the selected meta value.
   - **Apply Drill in New Tab**: Applies the drill and launches it in a new tab to drill the data in Navigate view.
   - **Apply !EQUALS Drill in New Tab**: Applies (!EQUALS) to the meta and launches a new tab, effectively excluding the meta value from the results.
   - **Hosts Lookup**: Looks up the value in the Investigate > Hosts view.
   - **Endpoint Thick Client Lookup**: Analyzes the meta value in the Endpoint Thick Client (for clients which have Endpoint Agent).
   - **Live Lookup**: Looks up a meta value on Live for further analysis.

3. For an external lookup, hover over a meta value, right-click and select **External Lookup**.



4. In the submenu select one of the available external lookups:
   - **Google**: Looks up a meta value on Google.com
   - **SANS IP History**: Looks up a meta value on SANS IP History, domain = http://isc.sans.org/ipinfo.html?ip=ipaddress
   - **CentralOps Whois for IPs and Hostnames**: Looks up a meta value on CentralOps Whois for IPs and Hostnames, domain = http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true
   - **Robtex IP Search**: Looks up a meta value on Robtext IP Search, domain = https://www.robtex.com/cidr/domain.ipaddress
   - **IPVoid**: Looks up a meta value on IPVoid, domain = http://www.ipvoid.com/scan/domain/
   - **URLVoid**: Looks up a meta value on URLVoid, domain = http://www.urlvoid.com/scan/ipaddress/
   - **ThreatExpert Search**: Looks up an IP meta value on ThreatExpert Search, domain = http://www.threatexpert.com/reports.aspx?find=IP address

Troubleshooting NetWitness Investigate

This section provides information about possible issues when using NetWitness Investigate.

Navigate View and Events View Issues

Message	`Not indexed; will experience longer than usual load times.` in the Manage Meta Groups dialog.
Issue	Meta keys in the Manage Meta Groups dialog are marked by a red exclamation point, and the error message is displayed. This can occur when investigating a Broker or Decoder while adding a meta group with meta keys that are not indexed in the index file or the custom index file for the service. For a Broker, it could mean that the Broker has not begun aggregating data from a Concentrator. In this case the Broker will not have the contents of the custom index file from the aggregate services and the keys will not be indexed. For a Decoder, it means that the meta keys are not indexed in the Decoder index or custom index file.
Explanation	To fix the issue on a Broker, log out, log in, and restart the Broker service so that it can aggregate the meta key information from connected Concentrators. To fix the issue on a Decoder, edit the custom index file to index the meta keys, log out, log in, and restart the Decoder service.

Behavior	When downloaded from the Event Reconstruction view, logs and metadata are always in text format irrespective of the format selected in the Events view.
Issue	When you download metadata or a log in the Event Reconstruction view, the format that you selected in the Events view is not used. The exported data is always in text format.
Explanation	Download metadata and logs from the Events view if you want to use a format other than text format.

Event Analysis View Issues

Message	`Investigation Profiles/OOTB column groups are not present in Event Analysis`
Issue	Post upgrade to RSA NetWitness v11.1, the default column groups - Endpoint Analysis, Outbound SSL and Outbound Http are not added under column groups. Also, few of the

Explanation	Investigation Profiles are missing post upgrade.
	It is observed that this issue occurs only when you have created a custom column group with the name which is same as one of the new 11.1 OOTB custom column group name. For example, if you create a custom column group in 11.0 with name **RSA Endpoint Analysis** then after upgrade to 11.1. Due to the same name already existing in 11.1, OOTB column groups and OOTB profiles will not be available in the UI. To fix this, change the name of custom column group to something other than one of the OOTB column groups and restart the jetty server by using the following command on the NetWitness server: `systemctl restart jetty`

Message	`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`
Issue	When you click **Pivot to Endpoint** in the Event Analysis view, no data is displayed and the message is displayed.
Explanation	Version 4.4 of the NetWitness Endpoint Thick Client must be installed on the same server, the NWE meta keys must exist in the `table-map.xml` file on the Log Decoder, and the `index-concentrator-custom.xml` file on the Concentrator. The NWE Thick Client is a Windows only application. Complete setup instructions are provided in the *NetWitness Endpoint User Guide* for Version 4.4.

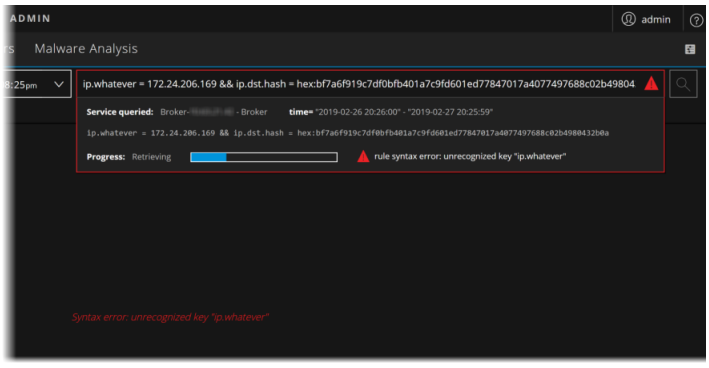
Message	`Event Analysis requires all core services to be NetWitness 11.1. Connecting prior versions of services to the 11.1 NetWitness Server results in limited functionality (see "Investigate in Mixed Mode" in the Physical Host Upgrade Guide).`
Issue	When attempting to investigate a service that has not been updated to Version 11.1 in the Event Analysis view, the informational message is displayed.
Explanation	When an analyst opens the Event Analysis view in mixed mode (that is, some services are upgraded to 11.1 and later, and some are still on 11.0.0.x or 10.6.x), Role-Based Access (RBAC) is not applied uniformly. This affects viewing and downloading content, and validation of filters in the interactive breadcrumb. You will see this informational message when you open Event Analysis. As you select a service, services that are not up to date are displayed in a red box, with the message that the service is not up to date. When your administrator has upgraded all connected services to 11.1 and later, these features work as expected.

Message	`Forbidden. You cannot access the requested page.`
Issue	When attempting to access the Event Analysis view, the view opens with the message.
Explanation	Your administrator has prevented access to the Event Analysis view using role and permissions.

Message	`Insufficient permissions for the requested data.`
Issue	While attempting to access an event in Event Analysis, the message is displayed.
Explanation	You have entered an event ID for an event that you do not have permission to view. The administrator may have placed some restrictions to limit access by role and permissions.

Message	`Invalid session ID: <<eventId>>`
Issue	No `sessionId` matches the `sessionId` that you queried.
Explanation	The reason for an invalid session ID can vary. Perhaps you edited the session ID manually, and no such session exists. Another case may be when you query a Broker, and the aggregated data has not been refreshed, you may see this error for a session that no longer exists.

Message	`No text data was generated during content reconstruction. This could mean that the event data was corrupt/invalid, or that an administrator has disabled the transmission of raw endpoint events in the Endpoint server configuration. Check the other reconstruction views.`
Issue	When you reconstruct an event as text in the Event Analysis view, no data is displayed and the message is displayed.
Explanation	If you do not see the raw text in other Event Analysis views or Events view reconstructions, and you believe the data is not corrupted or invalid, your administrator has likely disabled transmission of raw endpoint events on the NetWitness Endpoint server. Contact your administrator for additional information.

Message	`Rule Syntax error: Unrecognized key "<meta key or meta entity name>"` `Syntax error: Unrecognized key "<meta key or meta entity name>"`
Issue	While querying a service, the matching events are not listed and the message is displayed in the query console and the Event Analysis view. 
Explanation	The query you entered is querying a meta entity that is not configured properly. All

	upstream devices connected to the Broker being queries should have the same entity configuration. This error indicates that the Broker is operating with mismatched entity definitions. Ask your administrator to review the configuration described in "Index Customization" in the *Core Database Tuning Guide*.

Message	`Session is unavailable for viewing.`
Issue	While querying an event ID, the reconstruction is not displayed and the message is displayed.
Explanation	The query you entered is trying to look at restricted data, for example, if you are allowed to see only log data and you are using a link to network data .

Message	`The session id is too large to be handled:<<eventId>`
Issue	The session id that you typed in, or got from the Events view or Navigate view is too large.
Explanation	If you manually typed the sessionId or edited a sessionId in the Event Analysis view, you may have created an integer that is too large for Event Analysis to process.

Investigate Reference Materials

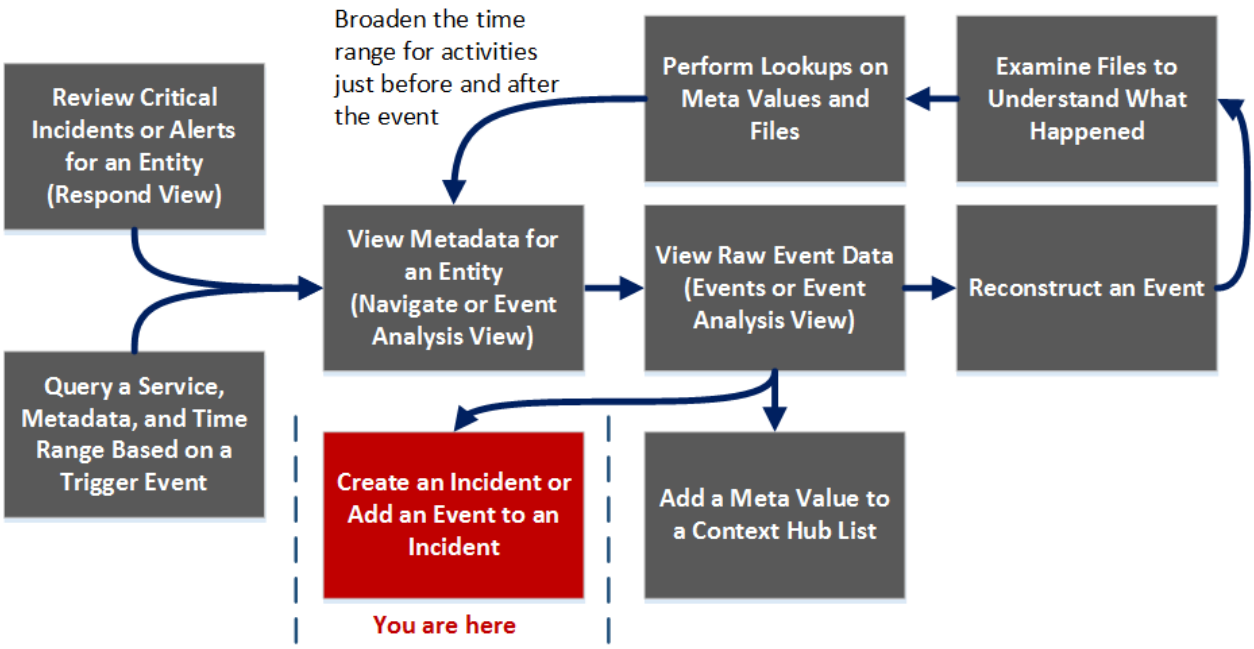
This section provides is intended to help you understand the purpose and application of NetWitness Investigate views. For each view, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition some of the reference materials include workflows and Quick Looks to highlight important features in the user interface.

- Investigate View
- Navigate View
- Events View
- Event Analysis View
- Add/Remove from List Dialog
- Add Events to an Incident Dialog
- Context Lookup Panel
- Create an Incident Dialog
- Event Analysis View - Text Analysis Panel
- Event Analysis View - Packet Analysis Panel
- Event Analysis View - File Analysis Panel
- Event Reconstruction View
- Investigate Dialog
- Investigation Tab - User Preferences Panel
- Manage Default Meta Keys Dialog
- Manage Column Groups Dialog
- Manage Profiles Dialog
- Navigate View
- Query Dialog
- Settings Dialogs for Investigate Views

Add Events to an Incident Dialog

In the Add Events to an Incident dialog, analysts can add alerts to an existing incident so that incident responders look at the associated events as part of an incident response. To access this dialog while investigating a service in the Events view, select **Incidents > Add to Existing Incident** from the toolbar.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View

User Role	I want to ...	Show me how
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

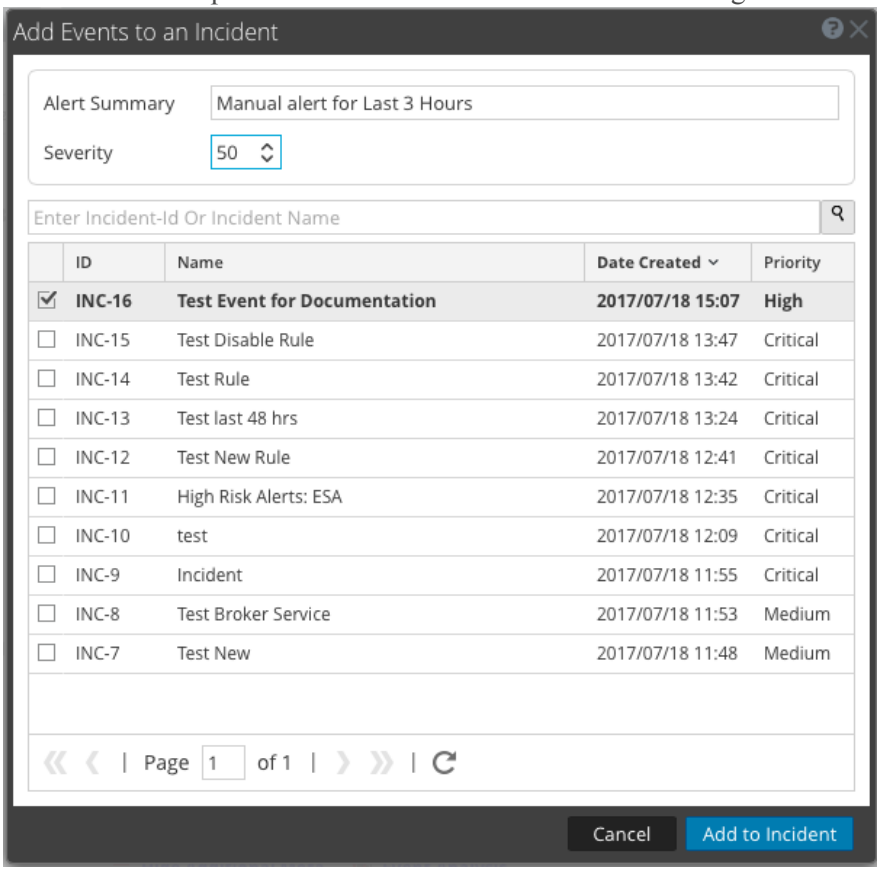
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View

Quick Look

The following figure is an example of the Add Events to an Incident dialog. The table describes the information and options in the Add Alerts to an Incident dialog .



Feature	Description
Alert Summary	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.
Search	Allows you to search for an existing event.
ID	The ID of the incident. You can sort IDs in ascending or descending order.
Name	The incident name. You can sort the Name in ascending or descending order.
Date Created	Displays the date and time the incident was created. You can sort the dates in ascending or descending order.
Priority	Displays the priority of the incident: either low or critical.
Cancel	Closes the dialog without saving changes.
Add to Incident	Adds the alerts to the incident. A dialog confirms that alerts are successfully added

Add/Remove from List Dialog

The Add/Remove from List dialog allows you to add an entity or meta value to an existing Context Hub list, remove an entity or meta value, or create a new Context Hub list containing the entity or meta value. When you look up an IP address or other entity and you find it suspicious or interesting, you can add it to a list that has been added as a data source. An example of a commonly used list is a white list or black list. This improves the visibility of the suspicious IP addresses and reduces false positives that do not need further investigation.

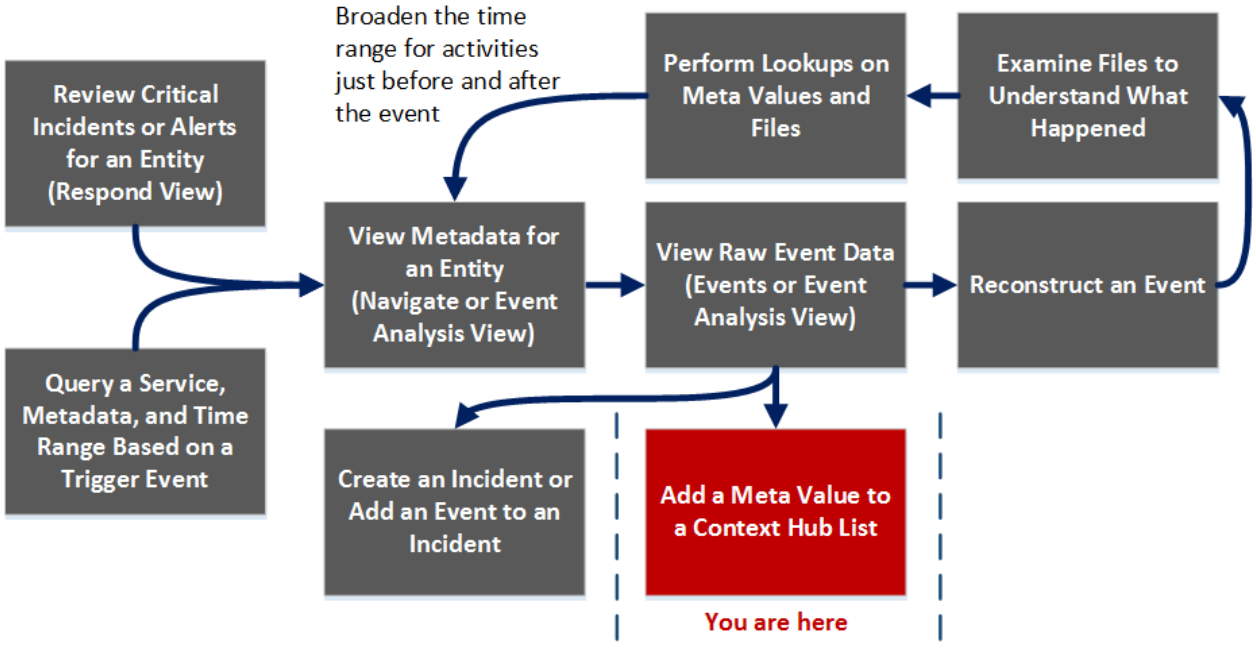
You can add entities or meta values to more than one list. For example, you can add them to one list for suspected domains related to command and control connections and to another list for Trojan connection IP addresses related to remote access. If a list is not available, you can create a list.

The dialog is available in NetWitness Investigate and in NetWitness Respond. When working in Investigate, in the Navigate view, Events view, or Event Analysis view (Version 11.2), you can add meta values for the `Source IP`, `Destination IP`, or `Username` meta keys to an existing context hub list or you can create a new list containing the meta values. When you add meta values to a list, you can look up additional context on those meta values.

- To display the dialog in the Navigate view or the Events view, right-click a meta value under `Source IP`, `Destination IP`, or `Username`) and select **Add/Remove from List** in the context menu.
- To display the dialog in the Event Analysis view, hover over a value and select **Add/Remove from List** in the Actions section of the context tooltip.

Workflow

The following workflow diagram shows the workflow for an investigation with the location of the Add to List task highlighted.



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

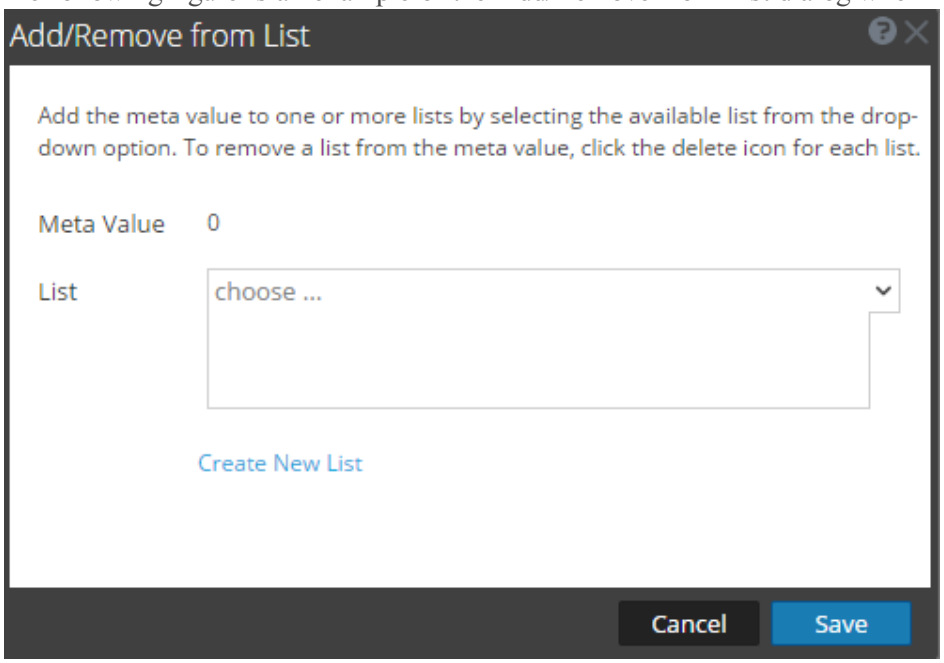
*You can perform this task in the current view.

Related Topics

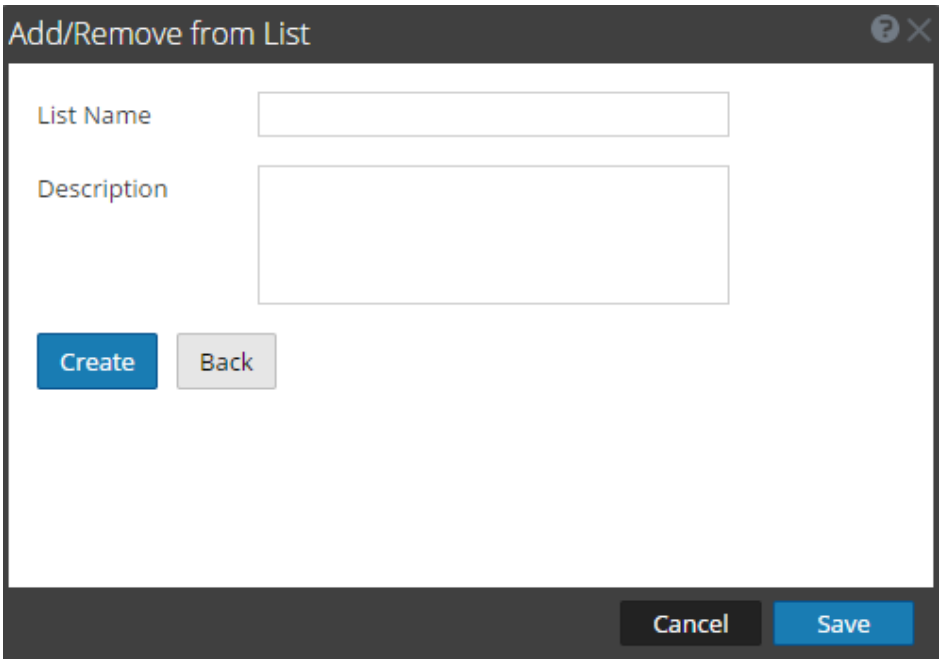
- Look Up Additional Context for a Data Point
- Navigate View
- Events View
- Event Analysis View

Quick Look in the Navigate and Events Views

The following figure is an example of the Add/Remove from List dialog when initially opened.



The following figure shows the dialog when you select Create New List.

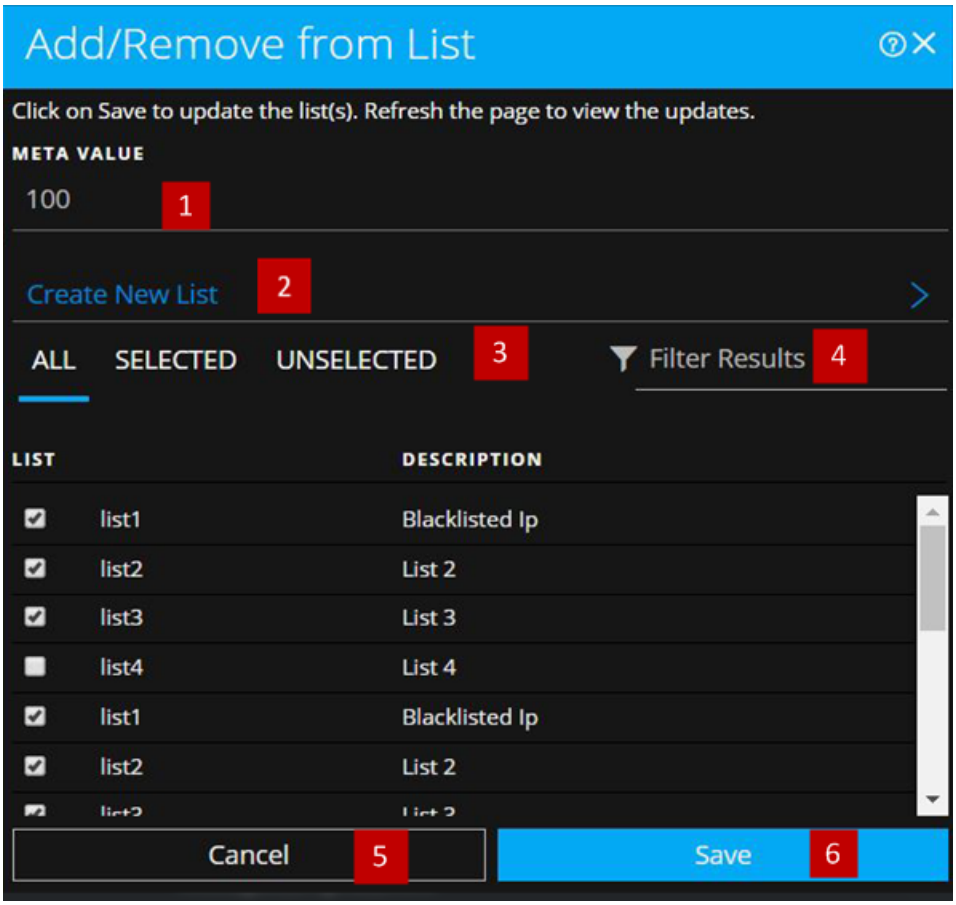


The following table describes the features of the Add/Remove from List and Create New List dialogs.

Feature	Description
Meta Value	The selected meta value to be added to the existing or new list.
List	The list to which the selected meta value must be added. A drop-down menu provides a list of available lists to which you can add the meta value.
Create New List	Opens a new dialog in which you can create a new list for the selected meta value.
List Name	The name of the new list.
Description	The description of the new list.
Create	Creates a new list after entering the required fields.
Back	In the new list mode, cancels the new list creation and returns to the original dialog.
Cancel	Cancels the addition of the meta value to a list and closes the dialog.
Save	Saves the changes made to the lists and closes the dialog.

Quick Look in the Event Analysis View (Version 11.2 and Later)

The following is an example of the **Add/Remove from List** dialog in the Event Analysis view.



1 Entities or meta values to be added or removed.
2 Create a new list using the selected meta.
3 Select any of the tabs: All, Selected, or Unselected.
4 Search using the list name or description.
5 Cancel the action.
6 Save to update lists or create a new list.

The following table shows the options in the Add/Remove from List dialog.

Option	Description
META VALUE	Displays the selected entity or meta value that needs to be added to or removed from one or more lists. You can also a create a new list using the selected value.
Create New List	Displays a dialog to create a new list using the selected meta value.
ALL	Shows all of the available Context Hub lists. The lists that contain the selected entity or meta value are selected. Select a checkbox to add an entity or meta value to a list. Clear a checkbox to remove it from the list.
SELECTED	Shows only the lists that contain the selected entity or meta value. (All lists are selected.)

Option	Description
UNSELECTED	Shows only the lists that do not contain the selected entity or meta value. (All lists are unselected.)
Filter Results	Enter the name or description of a specific list to search from multiple lists.
LIST	Displays the name of all the lists.
DESCRIPTION	Displays information about the selected list. The description that you provide when creating a list appears in this dialog. For example: This list contains all of the blacklisted IP addresses.
Cancel	Cancels the operation.
Save	Saves the changes.

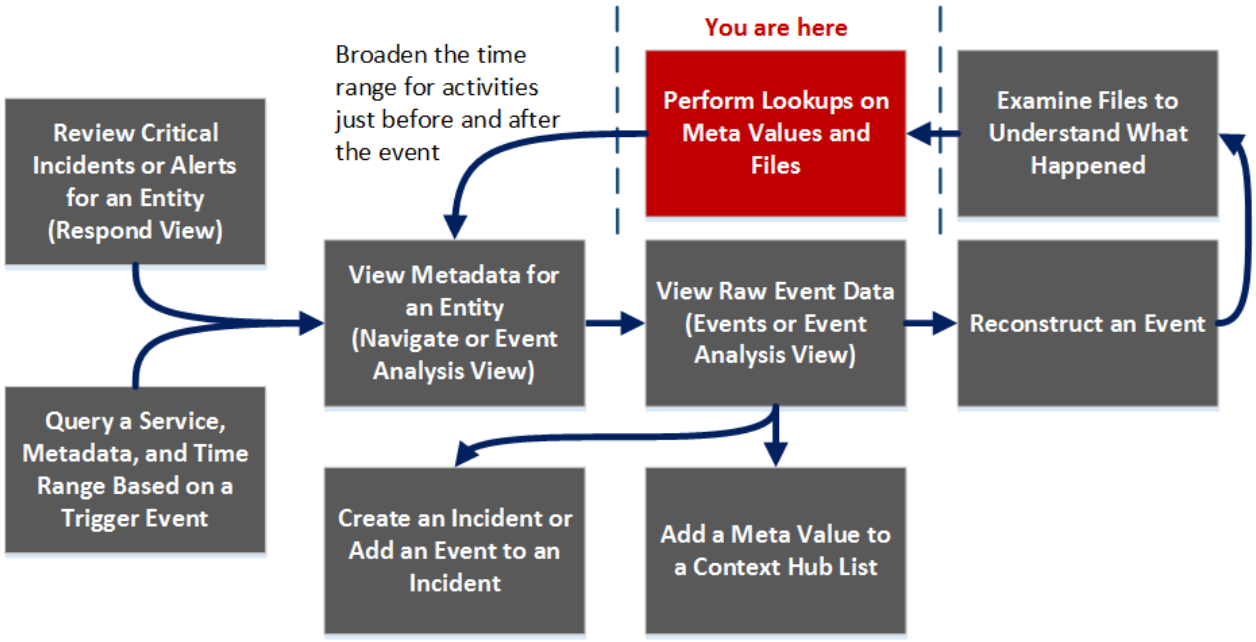
Context Lookup Panel

After an administrator configures the Context Hub service, you can view the contextual information for the meta values in the Navigate view, Events view, and Event Analysis view (Version 11.2 and later). The Context Hub service is pre-configured with a default meta type and meta key mapping. For information about mapping of the context hub meta value with investigation meta key, see "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*.

The Context Lookup panel is displayed on the right side of the Navigate view, Events view, or Event Analysis view. Meta values that have been added to a Context Hub list are highlighted in gray in the Navigate view or Events view results. In the Event Analysis view, they are marked by an underscore. When you right-click a highlighted value and select **Context Lookup** in the resulting context menu, the lookup results are displayed in the Context Lookup panel for configured sources for the selected meta value. You can select a source in the Context Lookup panel icon bar to view the contextual information.

There are some differences between the appearance and contents of the Context Lookup panel when open in the Navigate view or Events view and when open in the Event Analysis view.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*

User Role	I want to ...	Show me how
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups*	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

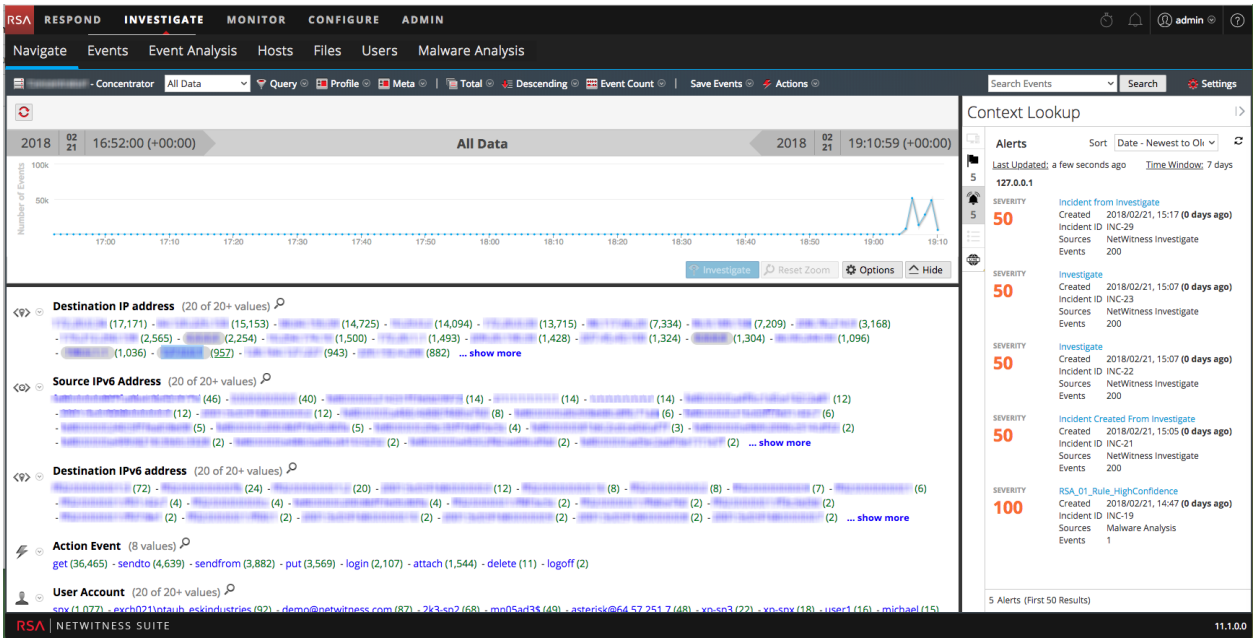
Related Topics

- How NetWitness Investigate Works
- Events View
- Navigate View

- Event Analysis View
- "NetWitness Feedback and Data Sharing" in the *Live Services Management Guide*

Quick Look (in the Navigate and Events Views)

The following figure is an example of the Context Lookup panel as it appears in the Navigate view and Events view. Controls and features are described in the table.



Feature	Description
Source Options Bar	Displays the icons for the available sources: Endpoint, Incidents, Alerts, and Lists.
Source Name	Displays the source name based on the selected icon: • Endpoint • Incidents • Alerts • Lists • Live Connect
Sort	Provides a drop-down of sort options for the listed context information. Possible sort options are Severity - High to Low, Severity Low to High, Date - Oldest to Newest. and Date - Newest to Oldest. The sorting options vary by source type.
	Refreshes the lookup results.

Feature	Description
<n items> (First <n> Results)	The footer provides a count of results currently displayed and the total number of results. For example, 5 Alerts (First 50 Results).

Incidents

Incidents are displayed based on time first (Newest to Oldest) and then priority status. The following information is displayed for incident lookups:

- Incident Name and ID
- Priority status of the incidents
- Risk Score value of the incidents
- Date when the incident was created
- Status of the incident
- Assignee for the incident
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Time window: This is based on the value that is set for the "Query Last (Days)" field in the Configure Respond window. For details, see the "Configure Respond as a Data Source" topic in the *Context Hub Configuration Guide*.
- Sort: This drop-down field provides options to change the sorting of result based on time or priority.

Alerts

Alerts are displayed based on the Severity. ;The following information is displayed for alert lookups:

- Alert Name
- Severity value of the alerts
- Date when the alert was created
- Incident ID: This is the ID of the incident that the alert is associated with (If any).
- Sources: Event source name
- Number of events associated with the alert.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Time window: This is based on the value that is set for the "Query Last (Days)" field in the Configure Respond window. For details, see the "Configure Respond as a Data Source" topic in the *Context Hub Configuration Guide*
- Sort: This drop-down field provides option to change the sorting of result based on time or priority.

Lists

The following information is displayed for list lookups.

- List Name
- Owner who created the list
- Created Date
- Last Updated Date
- Description of the list

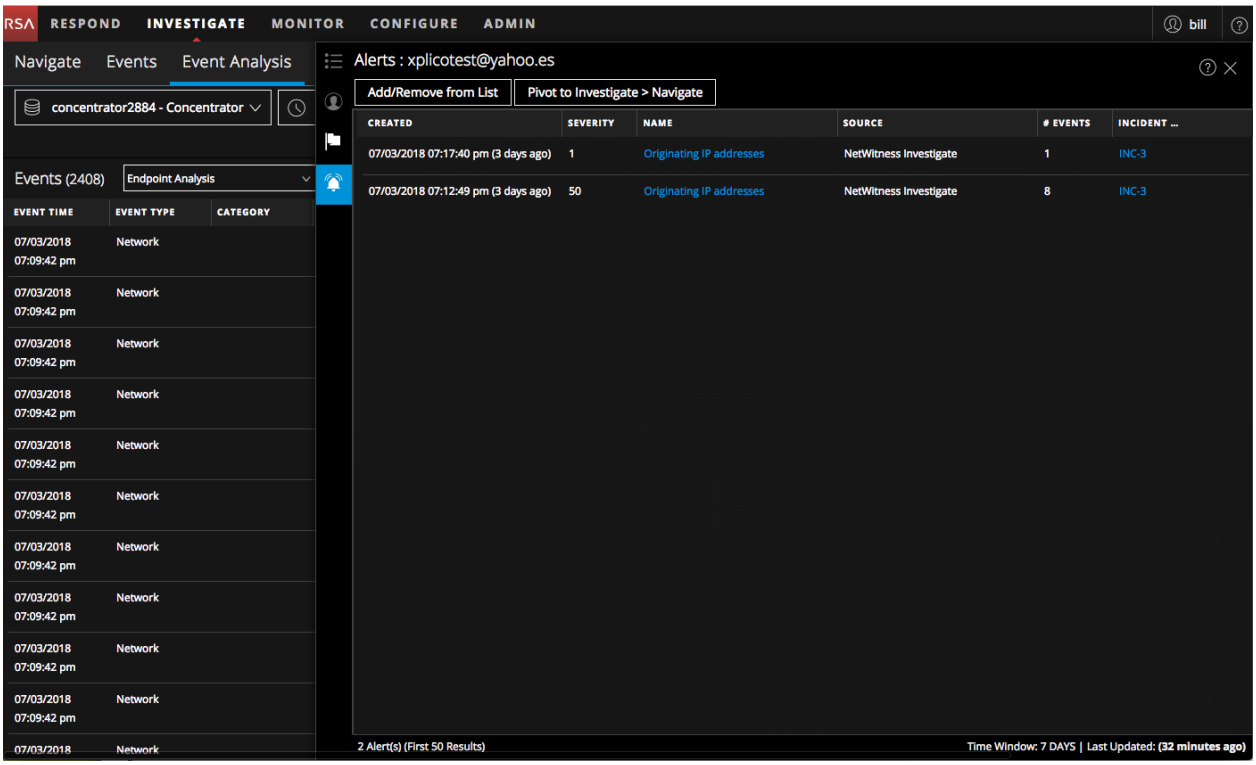
Endpoint

The following information is displayed for Endpoint lookups.

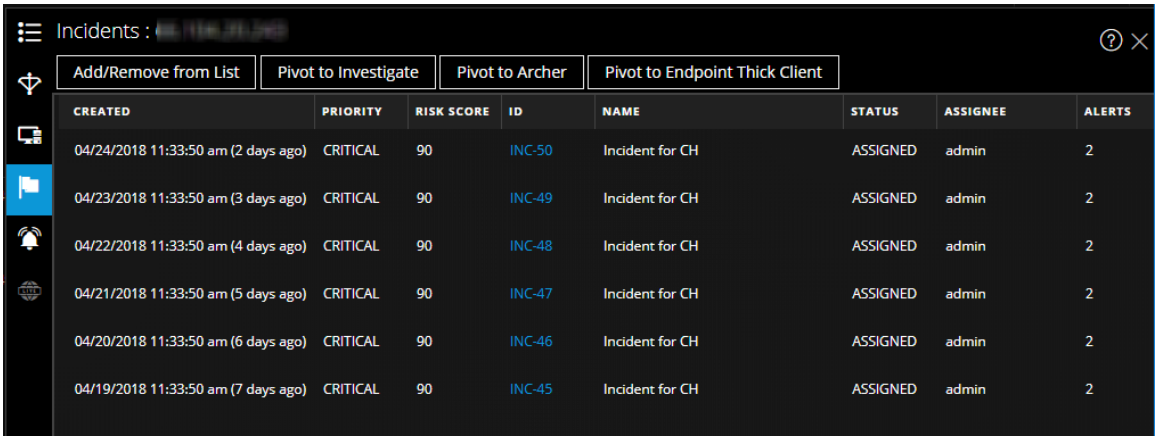
- Machine name and IP address of the machine.
  By clicking on the IP or Endpoint machine name, you will be navigated to Endpoint UI to perform further investigation.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Machine Score: A machine IIOC score is aggregated based on the module scores.
- Number of modules: Number of active files for the selected machine.
- Last Updated: Indicates when the scan results were last updated in Endpoint database.
- Last Login User
- Machine MAC Address
- Operating System Version
- Admin Notes (if any)
- Admin Status (if any)
- Top Suspicious Modules (Modules that have an IIOC score > 500). This is based on the value set for "Minimum IIOC Score" field in the Configure Endpoint window. The default value for "Minimum IIOC Score" is 500.
- Machine IIOC Levels

Quick Look in the Event Analysis View (Version 11.2 and Later)

The following figure is an example of the Context Lookup panel as it appears in the Event Analysis view.



The contextual information or query results displayed in the Context Lookup panel depends on the selected entity and the associated data sources. The Context Lookup panel has separate tabs for each of the data sources. The tabs are: List data source, Archer, Active Directory, Endpoint, Incidents, Alerts, and Live Connect. The following figure shows the Context Lookup panel for a selected entity in the Incident Details view with the Incidents tab in view.



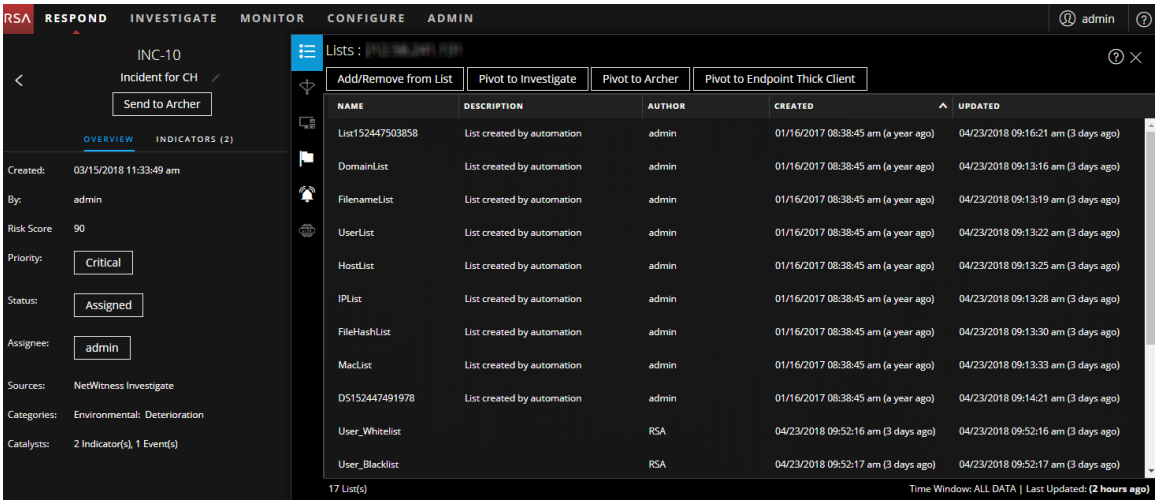
The following table describes the data available on each tab and the supported entities.

Tab	Description	Supported Entities
(Lists)	Displays all of the list data associated with the selected entity or meta value. The result is sorted by the last updated list.	All entities

Tab	Description	Supported Entities
(Archer)	Displays asset information along with criticality ratings using the Archer data source.	IP, Host, and Mac
(Active Directory)	Displays all user information for the selected user.	User
(NetWitness Endpoint)	Displays the NetWitness Endpoint data source information for the selected entity or meta value, which includes the Machines, Modules, and IIOC levels. Modules are by highest IOC score to lowest IIOC score and IIOC levels are sorted by highest IOC levels to lowest IOC levels.	IP, MAC address, and Host
(Incidents)	Displays the list of incidents associated with the selected entity or meta value. The result is sorted by newest incidents to oldest incidents.	All entities
(Alerts)	Displays the list of alerts associated with the selected entity or meta value. The result is sorted by newest alerts to oldest alerts.	All entities
(Live Connect)	Displays information related to Live Connect.	IP, Domain, and Filehash
(File Reputation)	Displays file reputation status for Filehash entities.	Filehash entities

Lists Tab

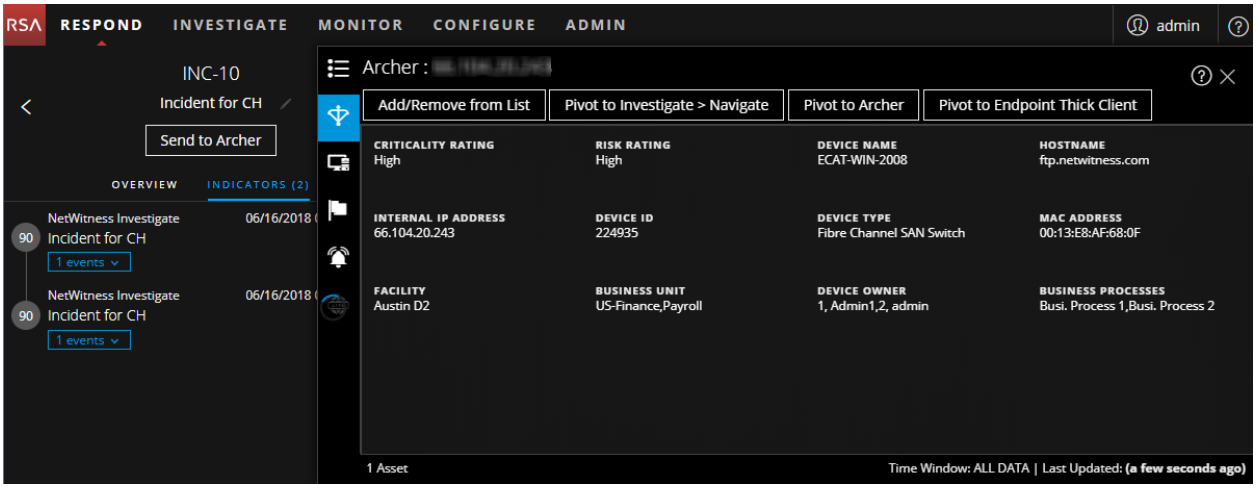
The Context Lookup panel for Lists shows one or more lists associated with the selected entity or meta value. The following figure is an example of the Context Panel for Lists, and the table describes the fields.



Field	Description
Name	The name of the list (defined while creating the list).
Description	The description of the list (defined while creating the list).
Author	The owner who created the list.
Created	The date when the list was created.
Updated	The date when the list was last updated or modifed.
Count	The number of lists in which the selected entity or meta value is available.
Time Window	The time window based on the value set for the "Query Last" field in the Configure Responses dialog. By default, all Lists data is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

Archer Tab

The Context Lookup panel for Archer displays asset information along with criticality ratings using the Archer data source for IP, Host, and Mac entities. The following figure is an example of the Context Lookup panel for Archer, and the table describes each field.



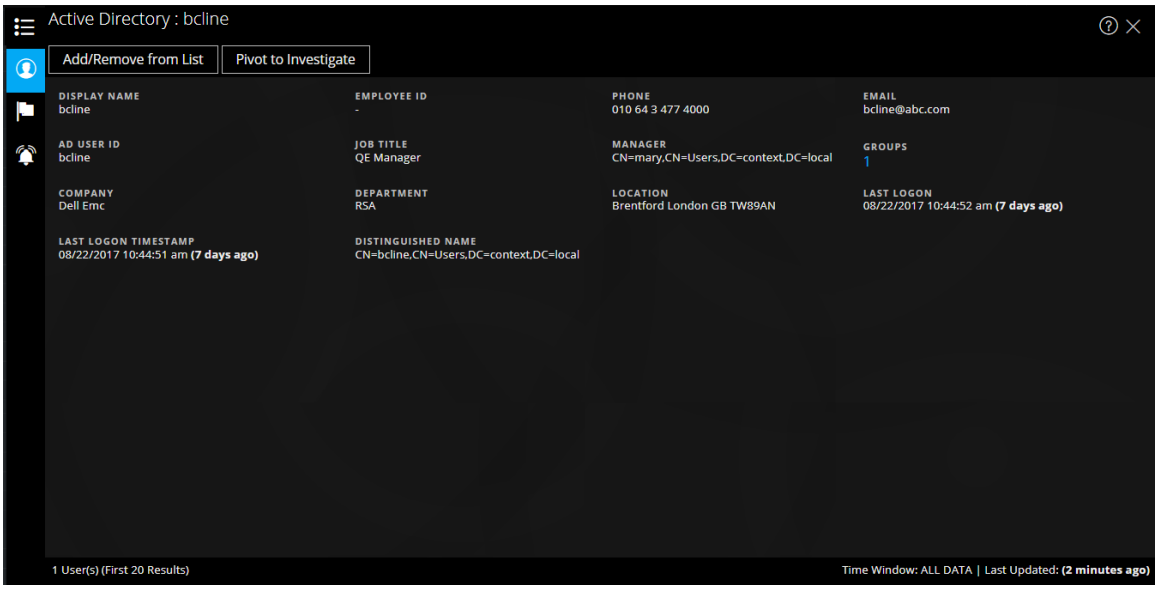
Field	Description
Criticality Rating	The device operational criticality based on the applications it supports. The criticality ratings can be set as Not Rated, Low, Medium-Low, Medium, Medium-High, or High.
Risk Rating	The calculated risk rating for the device based on the most recent assessment and the average risk rating of facilities using the device. The risk rating can be set as Severe, High, Medium, Low, or Minimal.
Device Name	The unique name of the device.
Host Name	The host name of the device.
IP Address	The primary internal IP address of the device.
Device ID	The automatically populated value that uniquely identifies the record across all applications within the system.
Type	The device type, for example, server, laptop, desktop, and others.
Facilities	Links to records in the Facilities application that are related to this device.
Business Unit	Links to records in the Business Unit application that are related to this device. For more than three business unit values, you can hover over the field to view the values.
Device Owner	The person who is responsible for the device and receives read and update rights of the record.
Count	The number of assets available.

Field	Description
Time Window	The time window based on the value that is set for the "Query Last" field in the Configure Responses dialog. By default, all data for Archer is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

Note: In the localized versions, only these twelve fields are displayed: Criticality Rating, Risk Rating, Device Owner, Business Unit, Host Name, MAC Address, Facilities, IP Address, Type, Device ID, Device Name, and Business Processes.

Active Directory Tab

The following figure is an example of a Context Lookup panel for Active Directory.



The Context Lookup panel for Active Directory displays all the related information, incidents, and alerts for a user. You can perform a look up using the following formats:

- userPrincipalName
- Domain\UserName
- sAMAccountName

If the user exists in multi-domain or multi-forest, all the related context information is displayed for the specific user.

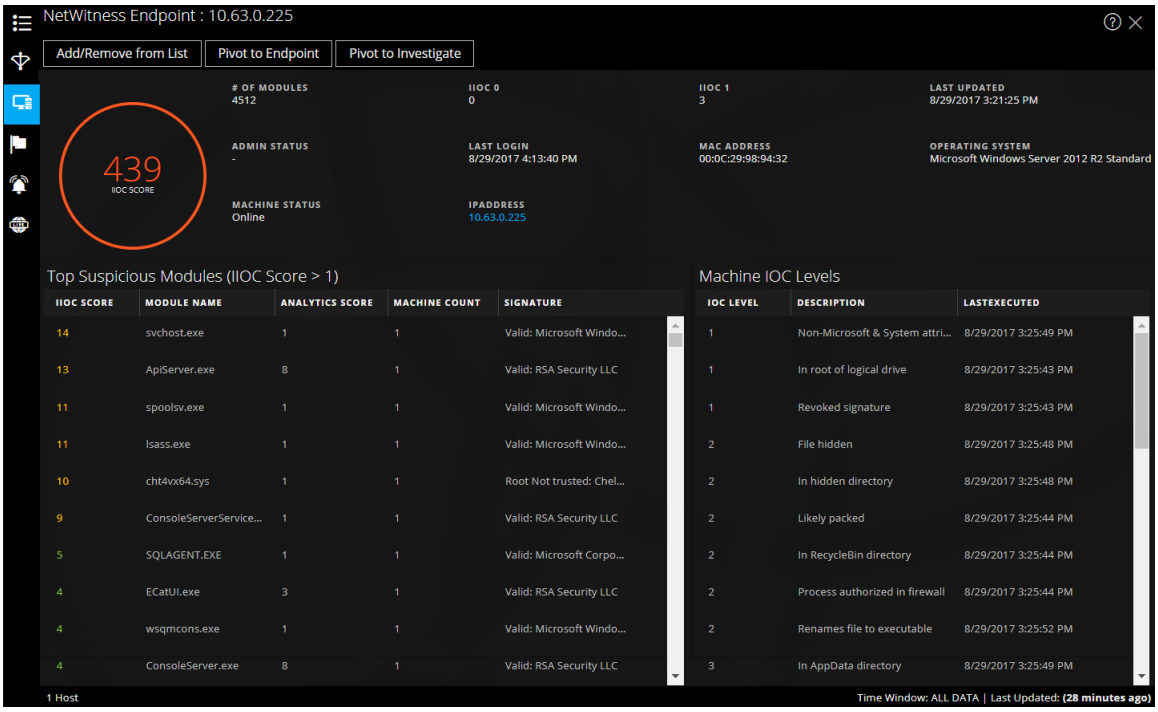
The following information is displayed for Active Directory.

Field	Description
Display Name	The name of the user.
Employee ID	The employee ID of the user.
Phone	The phone number of the user.
Email	The email ID of the user.
AD User ID	The unique identification of the user within an organization.
Job Title	The designation of the user.
Manager	The name of the user's manager.
Groups	The list of groups of which the user is a member.
Company	The name of the user's company.

Field	Description
Department	The department name to which the user belongs within the organization.
Location	The location of the user.
Last Logon	The time when the user logged into the system, only if the Global Catalogue is defined.
Last Logon TimeStamp	The time when the user logged into the system.
Distinguished Name	The unique name assigned to the user.
Count	The number of users.
Time Window	The time window based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, all data for Active Directory is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

NetWitness Endpoint Tab

The following figure is an example of the Context Lookup panel for NetWitness Endpoint.



The following information displayed for IIOCs.

Field	Description
# Of Modules	The number modules that are looked up.

Field	Description
Admin Status	The admin status (if any).
Last Updated	The time when the data was last refreshed.
Last Login	The time when the user last logged in.
MAC Address	The Machine MAC Address.
Operating System	The Version of the Operating System used by the NetWitness Endpoint machine.
Machine Status	The state of the module being viewed: Online, Offline, Active, or Inactive.
IP Address	The IP address of the specific module.

The following information is displayed for modules.

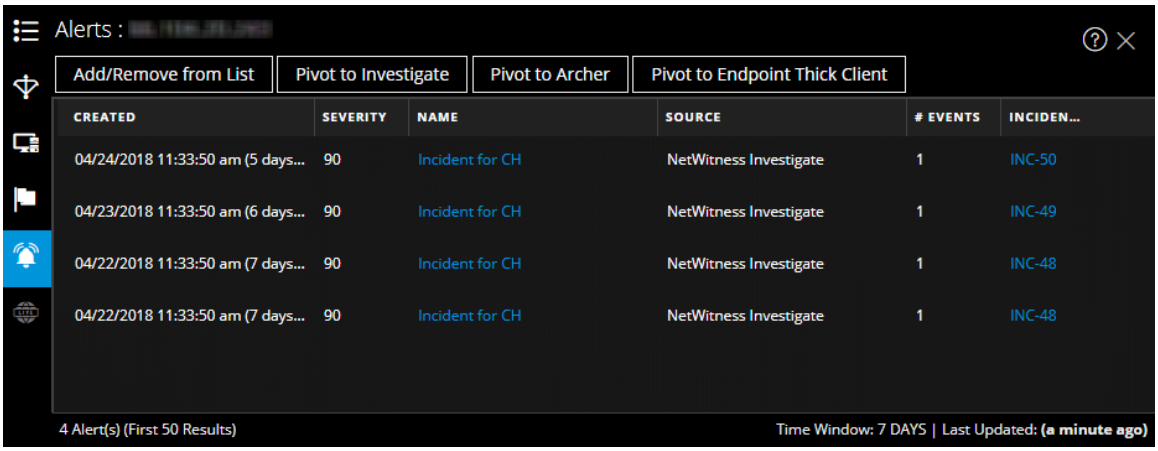
Field	Description
IIOC Score	A machine IIOC score is an aggregated score based on the module scores. This is based on the value set for Minimum IIOC Score field in the Context Hub Data Source Settings dialog. The default value for Minimum IIOC Score is 500. See "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.
Module Name	The name of the module that is being looked up.
Analystic Score	The number of active files for the selected machine.
Machine Count	The number of machines on which that particular IOC got triggered.
Signature	Indicator of whether the file is signed or unsigned, valid or invalid, and signatory information. For example, Google, Apple, and so on.

The following information is displayed for machines.

Field	Description
IOC Levels	The IOC levels.
Description	The description for he IOC level if available.
Last executed	The time when the action was executed.
Count	The number of hosts that are being looked up.
Time Window	The time window based on the value set for the Query Last field in the Configure Data Source Settings dialog. By default, all data for NetWitness Endpoint is fetched.
Last Updated	The time when scan results were last updated in NetWitness Endpoint database.

Alerts Tab

The following figure is an example of Context Panel for Alerts that is displayed based on time first (Newest to Oldest) and then severity.

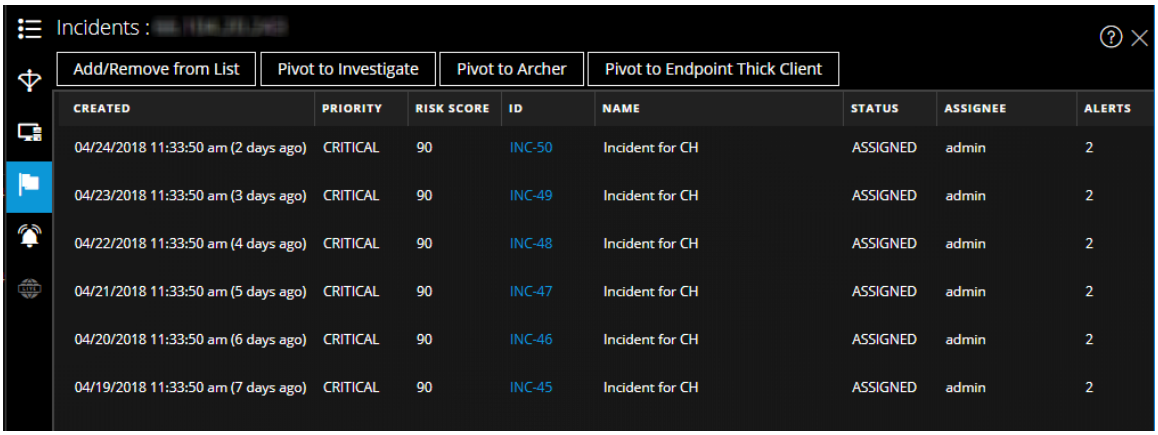


The following information is displayed in the Context Lookup panel for Alerts.

Field	Description
Created	The date and time when the alert was created.
Severity	The severity value of the alerts.
Name	The name of the alert. You can click the name to view the details of a specific alert.
Source	The alert source name from which the alert is triggered.
#Events	The number of events associated with the alert.
Incident ID	The ID of the incident (if any) with which the alert is associated. You can click the ID to view the details of a specific alert.
Count	The number of alerts. By default only the first 100 alerts are displayed. For more information on how to configure the settings, see "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.
Time Window	The time window based on the value set for the Query Last field in the Configure Data Source Settings dialog. By default, the alert data for last 7 days is fetched.
Last Updated	The time when contextual data was last fetched from data source.

Incidents Tab

The following figure is an example of the Context Panel for Incidents, which is based on time first (Newest to Oldest) and then priority status.

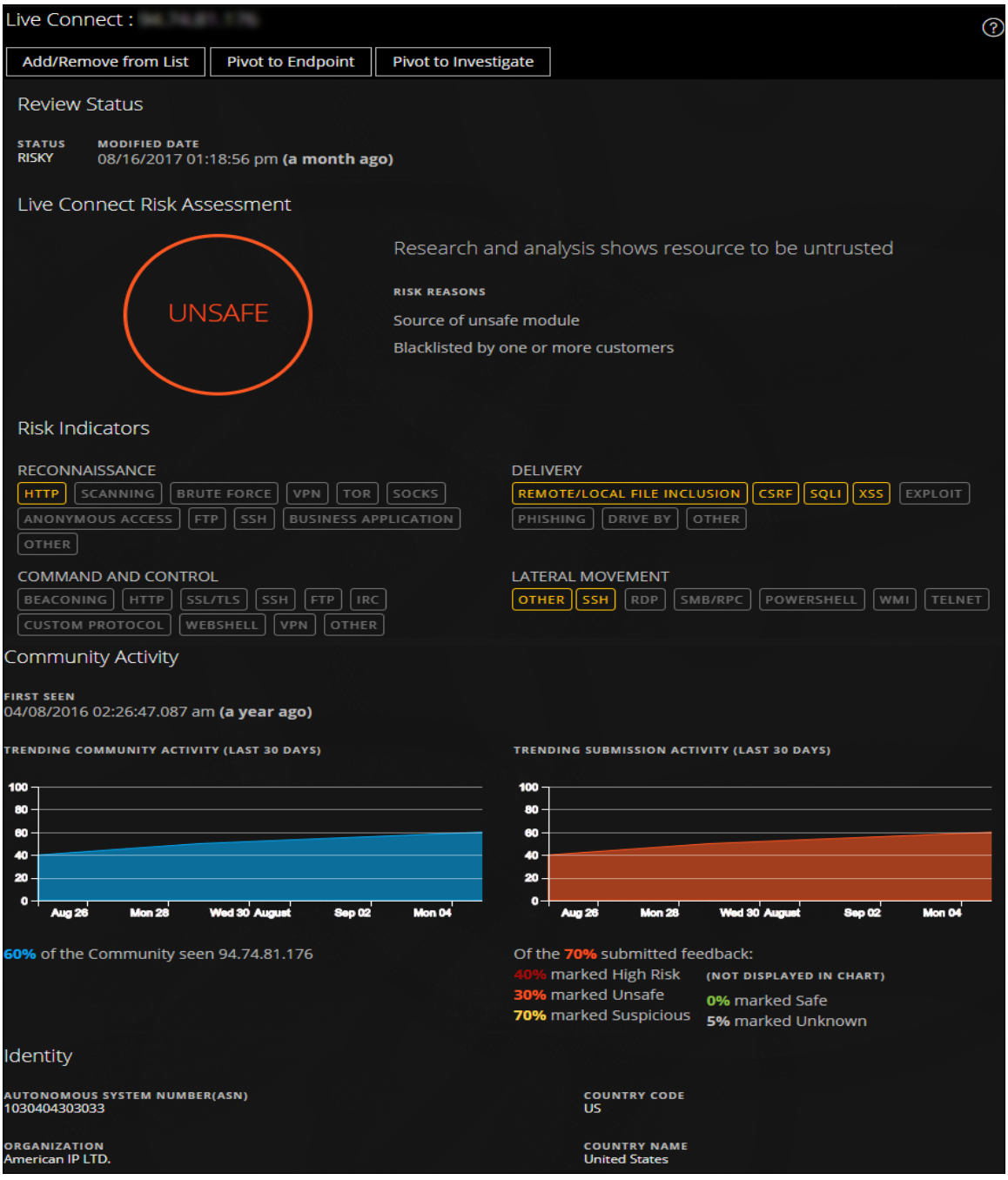


The following information is displayed in the Context Lookup panel for Incidents.

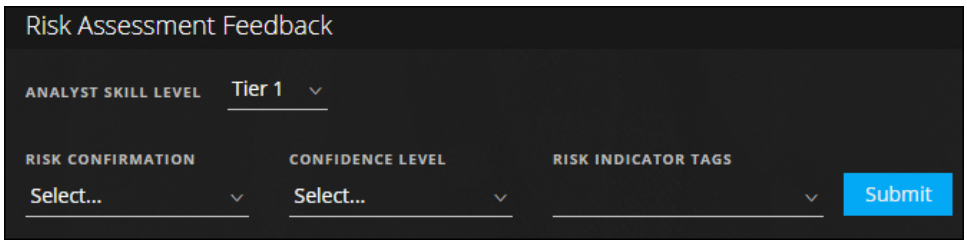
Field	Description
Created	The date when the incident was created.
Priority	The priority status of the incidents.
Risk Score	The risk score of the incidents.
ID	The Incident ID of the incident. You can click on the ID to display further details about the incident.
Name	The incident name.
Status	The status of the incident
Assignee	The current owner of the incident.
Alerts	The number of alerts associated with the incident.
Count	The number of incidents. By default only the first 100 incidents are displayed. For more information on how configure the settings, see "Configure Context Hub Data Source Settings" in the *Context Hub Configuration Guide*.
Time Window	The time window based on the value set for the Query Last field in the Configure Data Source Settings dialog. By default, the alert data for last 7 days is fetched.
Last Updated	The time when contextual data was last fetched from data source.

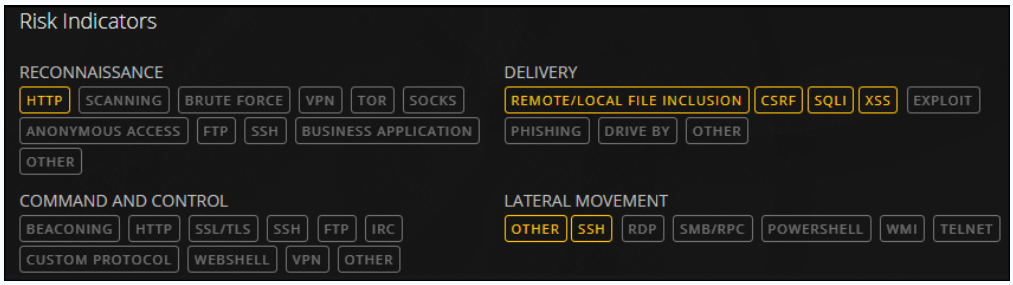
Live Connect Tab

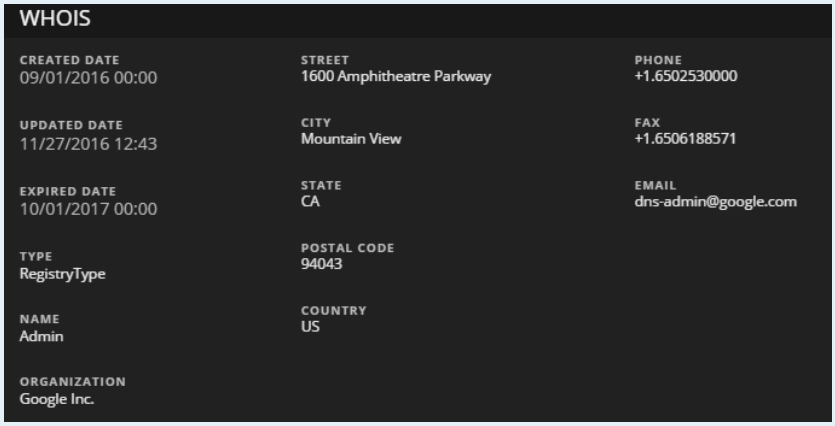
The following figure is an example of a Context Panel for Live Connect, and the table describes the information displayed.

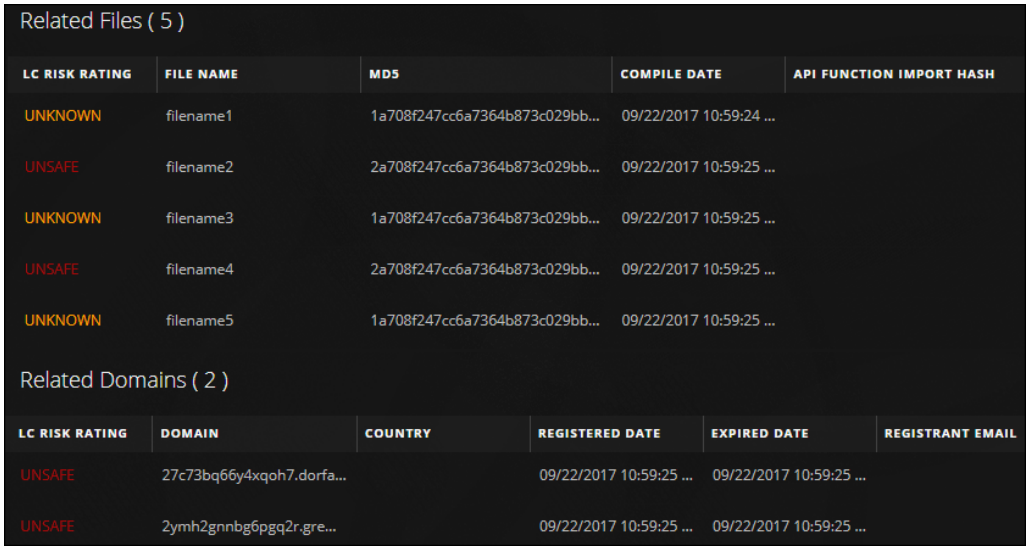


Field	Description
Review Status	The review status of the selected Live Connect entity (IP, file, or domain) based on the analyst activity. This gives the visibility of the analyst activity within an organization. **Status** Below are the types of status: • **New:** Lookup results for an IP address are viewed for the first time within the organization. • **Viewed:** Any analyst within the organization has already viewed the lookup results for an IP address. • **Marked as Safe:** Any analyst within the organization has already viewed the lookup results and marked the IP address as safe. • **Marked as Risky:** Any analyst within the organization has already viewed the lookup results and marked the IP address as risky.
Risk Assessment	The risk assessment for the selected Live Connect entity (IP, file, or domain) based on the Live Connect analysis and analyst feedback. The Risk Assessment categories are: • **Safe:** The Live Connect entity is considered to be safe. • **Unknown:** Live Connect does not have enough information about this entity to calculate the risk. • **High Risk**: Marked as high risk based on the analysis and risk reasons provided by the community. Entities marked as high risk require immediate attention. • **Suspicious**: Marked as suspicious based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action. • **Unsafe:** Marked as unsafe based on the analysis and risk reasons provided by the community. The entity is rated as High Risk, Suspicious, or Unsafe and displays the associated risk reasons accordingly.

Field	Description
Risk Assessment Feedback	 Risk Assessment Feedback allows the analyst to submit threat intelligence feedback about an entity to the Live Connect server. • **Analyst Skill Level** Below are the Analyst skill level options: ◦ **Tier 1** - Analysts at this level define procedures for remediation, and decide if an incident should be escalated to other areas in a Security Operation center (SOC). This is the default value. ◦ **Tier 2** - Analysts who investigate incidents and capture intelligence from an investigation to feed back into the various workflows in a SOC. ◦ **Tier 3** - Analysts who share the investigation results to the SOC organization. They generally manage incidents and have a wide breadth and depth of skills and tools necessary for incident response. **Note:** While creating a new user for NetWitness Platform (Analyst), an administrator should be able to identify the user as Tier 1, Tier 2, or Tier 3 Analyst. • **Risk Confirmation** - The risk confirmation for the selected Live Connect entity (IP, file, or domain). The Risk confirmation categories are: ◦ **Safe**: The Live Connect entity is considered to be safe. ◦ **Unknown**: The analyst does not have enough information to provide a risk confirmation ◦ **High Risk**: Marked as high risk based on the analysis and risk reasons provided by the community. Entities marked as high risk require immediate attention. ◦ **Suspicious**: Marked as suspicious based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action. ◦ **Unsafe**: Marked as unsafe based on the analysis and risk reasons provided by the community. • **Confidence Level** - The confidence level of an analyst in providing feedback for the Live Connect entity. The confidence level categories are: High, Medium, and Low. • **Risk Indicator Tags** - Allows you to select a tag category based on the analysis.

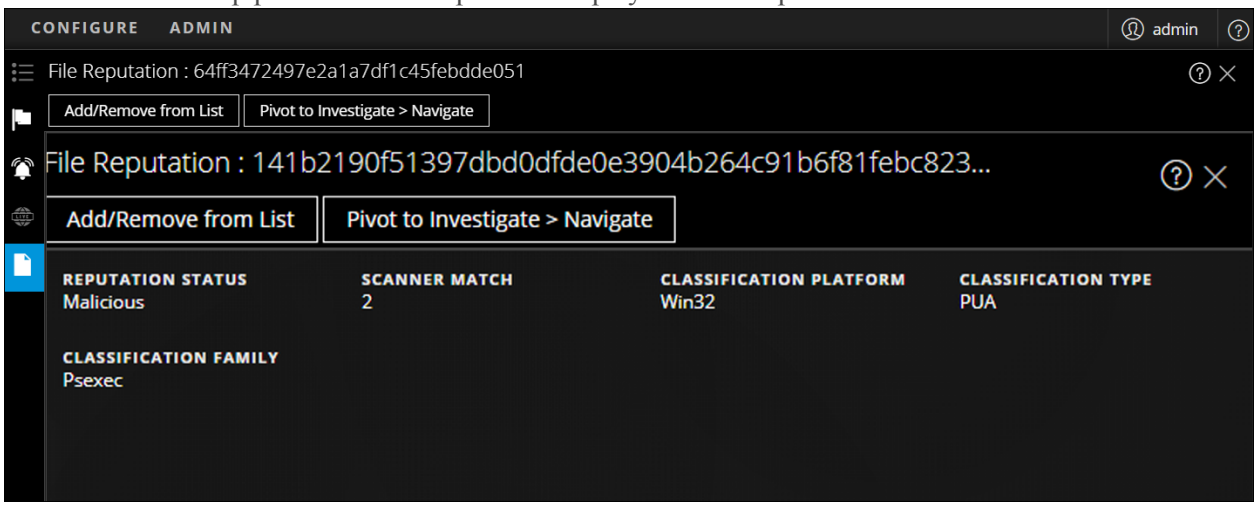
Field	Description
Community Activity	Community activities such as: • Date first seen in the community. • Time since the IP/File/Domain was seen for the first time (Current time - First seen time). **Trending Community Activity:** If the IP address is known within the RSA community, a graphical representation of the community activity trend is displayed for the following: • Users (in %) who have viewed the IP address in the Live Connect community over time. • Users (in %) who submitted feedback for the IP address. • Users (in %) who marked the IP address as unsafe over time.
Risk Indicators	 Risk indicators are highlighted based on the tags that are assigned by the community to the entities (IPs, Files, or Domains). The tags are categorized as follows: Reconnaissance, Delivery, Command and Control, Lateral Movement, Privilege Escalation, and Packaging and Exfiltration. These tags are samples and vary based on the inputs received from the community on the Live Connect server. The analyst can choose the appropriate risk indicator tags while providing the review feedback. A highlighted tag indicates that the selected entity is associated with that particular category and tag. Clicking a highlighted tag displays the description of the tag.
Identity	Provides the following identity information for the selected entity or meta value: For IP address: Autonomous System Number (ASN), Prefix, Country Code and Country Name, Registrant (Organization), and Date. For File Hash: File Name, File Size, MD5, SH1, SH256, Compile Time, and Mime Type. For Domain: Domain Name and Associated IP Address.
Certificate Information	Provides the following certificate information for the selected file hash: Certificate Issuer, Validity of the Certificate, Signature Algorithm, and Certificate Serial Number.

Field	Description
WHO IS Information	 The **WHO IS** information provides the ownership details for a given domain. The following information about the domain owner is displayed: Created Date, Updated Date, Expired Date, Type (Registration Type), Name, Organization, Address with Postal code, Country, Phone, Fax, and Email.
Related Files	Related Files are displayed for entity types IP and Domain. A list of known associated files is displayed along with the following information: Live Connect Risk Rating (Safe, Risky, or Unknown), File Name, MD5, Compile Time and Date, API Function, Import Hash, and Mime Type.
Related Domains	Related Domains are displayed for entity types IP and Files. A list of known associated domains is displayed along with the following information: Live Connect Risk Rating (Safe, Risky, or Unknown), Domain Name, Country Name, Registered Date, Expired Date, and Registrant Email address.

Field	Description
Related IPs	 Related IPs are displayed for entity types Domain and Files. A list of known associated IPs is displayed along with the following information: Live Connect Risk Rating (Safe, Risky, or Unknown), IP Address, Domain Name, Country Code and Country Name, Country Name, Registered Date, Expired Date, and Registrant Email address.

File Reputation Tab

The Context Lookup panel for File Reputation displays the file reputation status of a file.



Field	Description
Reputation Status	Reputation Status of filehash. For more information about reputation status, see *"View Reputation of files"* in the Investigate User Guide.

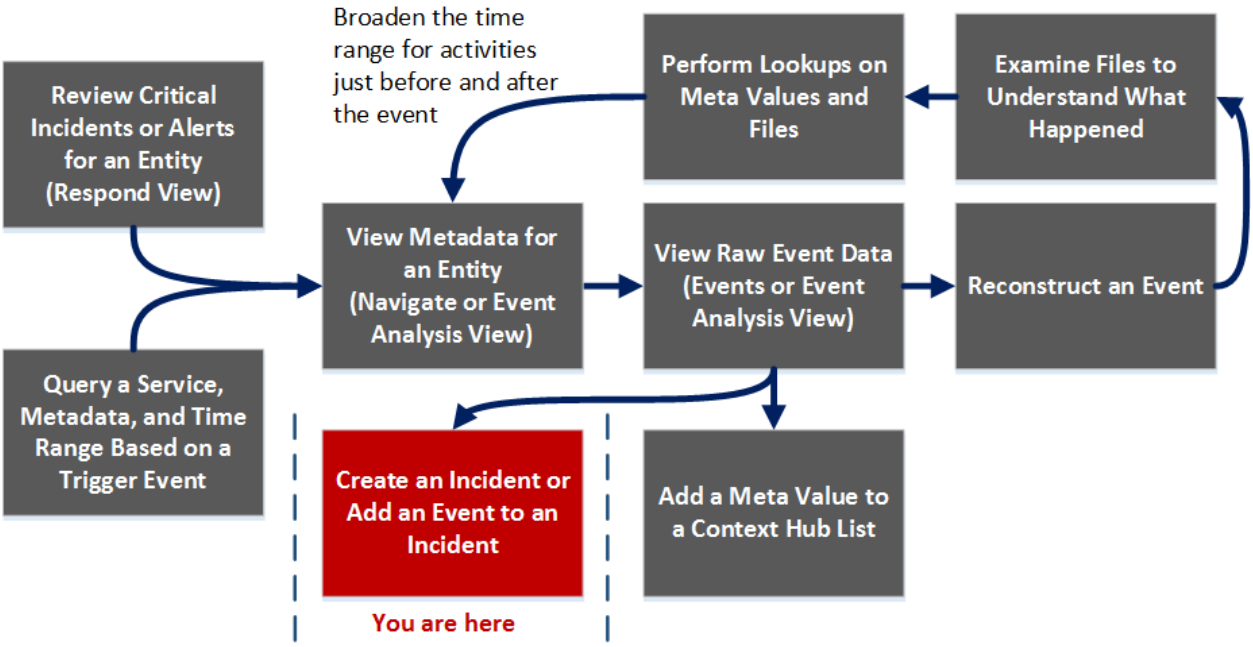
Field	Description
Scanner Match	Number of scanners that detected malware or suspicious activity in the last scan.
Classification Platform	Classification for the queried filehash based on the platform. For example, the platform can be Win 32.
Classification Type	Classification for the queried filehash based on the type.
Classification Family	Classification for the queried filehash based on the malware family name.

Create an Incident Dialog

In the Create an Incident dialog, analysts can create an incident from selected events in the Events view. The incident is then available to incident responders working in Respond.

To access this dialog, while investigating a service in the Investigation > Events view, select **Incidents > Create New Incident** from the toolbar.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View

User Role	I want to ...	Show me how
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

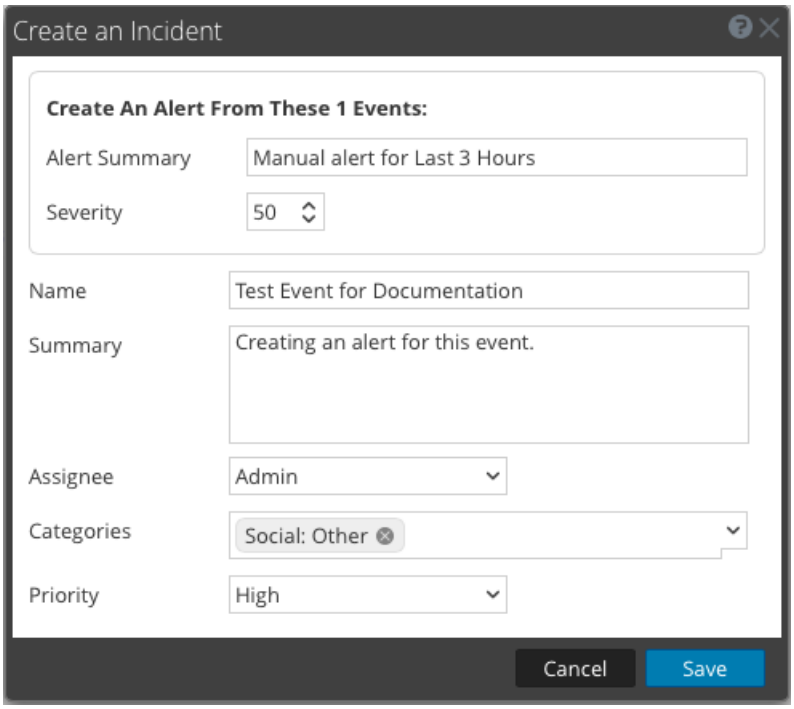
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

The following figure is an example of the Create an Incident Dialog, and the features are described in the table.



Feature	Description
Create Summary from These Events	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.
Name	(Required) Specifies a name to identify the incident. In the example, the name is Sample Incident. You can provide a name that clearly identifies the nature of events that will be added to this incident
Summary	(Optional) Specifies a description for the incident. A good summary clearly identifies the incident for other analysts and responders.
Assignee	(Optional) Assigns the incident to a user in the SOC. Clicking Assignee opens a drop-down list showing the user names of SOC personnel who respond to incidents.
Categories	(Optional) Identifies categories of incidents. Clicking Categories, opens a drop-down list of Incident categories and subcategories. You can select one or more categories to which the incident belongs. Categories fall into these major groups: Environmental, Error, Hacking, Malware, Misuse, and Social.
Priority	Identifies the priority for the incident. Clicking Priority opens a drop-down list of priorities: Critical, High, Medium, or Low displayed in the drop-down list.
Cancel	Closes the dialog without saving changes.
Save	Saves the incident and closes the dialog. A message confirms that the incident was created successfully.

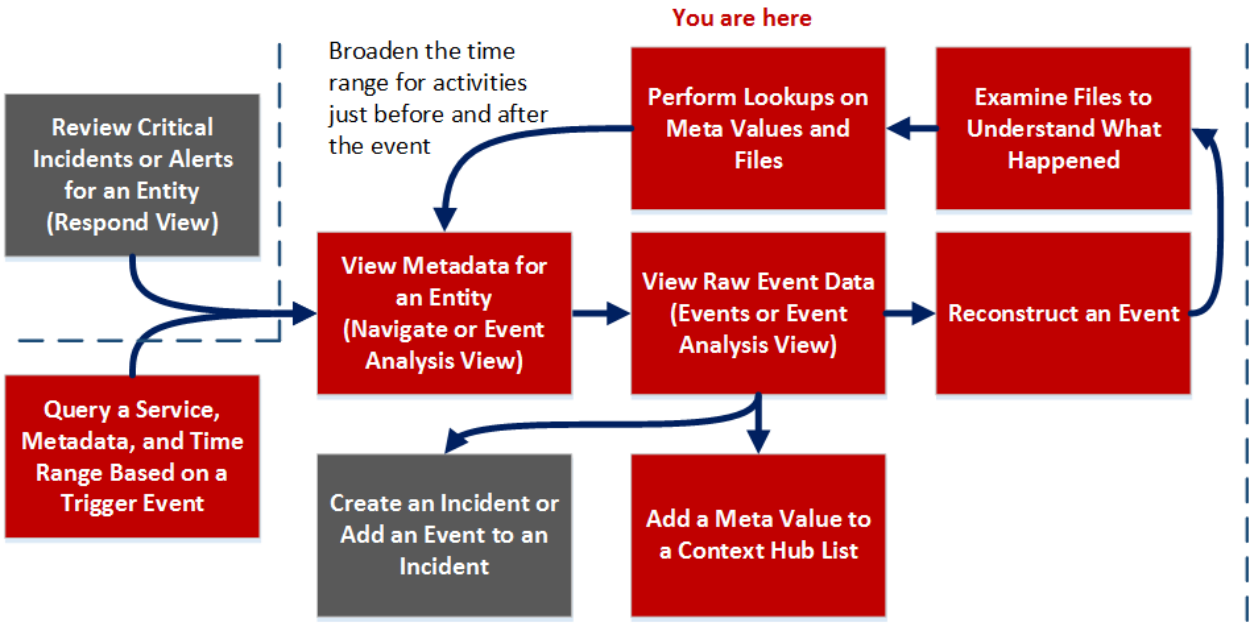
Event Analysis View

In the Event Analysis view analysts can view a list of events, select an event for analysis, and view the raw event and metadata with interactive features that enhance the ability to see meaningful patterns in the data. This is an alternative to the static Events view and Event Reconstruction view. You can view network, log, and endpoint events in the Event Analysis view. The Event Analysis view offers packet, text, and log reconstruction. It does not support email and web reconstruction directly; however, you can open an email or web reconstruction of the current results in the Events view email or web reconstruction.

Note: The administrator sets permission for analysts to access this view. If your administrator has not given you access, and you navigate to the Event Analysis view by any means, the following message is displayed: `Forbidden. You cannot access the requested page.` For example, if you are viewing a reconstruction from the Events view and attempt to view the same reconstruction in the Event Analysis view, you will see the `Forbidden` message.

Workflow

The following figure is a high-level workflow illustrating the tasks you can do in NetWitness Investigate, with the Event Analysis view tasks highlighted in red.



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*

User Role	I want to ...	Show me how
Threat Hunter	query a service, metadata, and time range*	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata*	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data*	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event*	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups*	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View - Packet Analysis Panel
- Event Analysis View - Text Analysis Panel
- Event Analysis View - File Analysis Panel

Quick Look

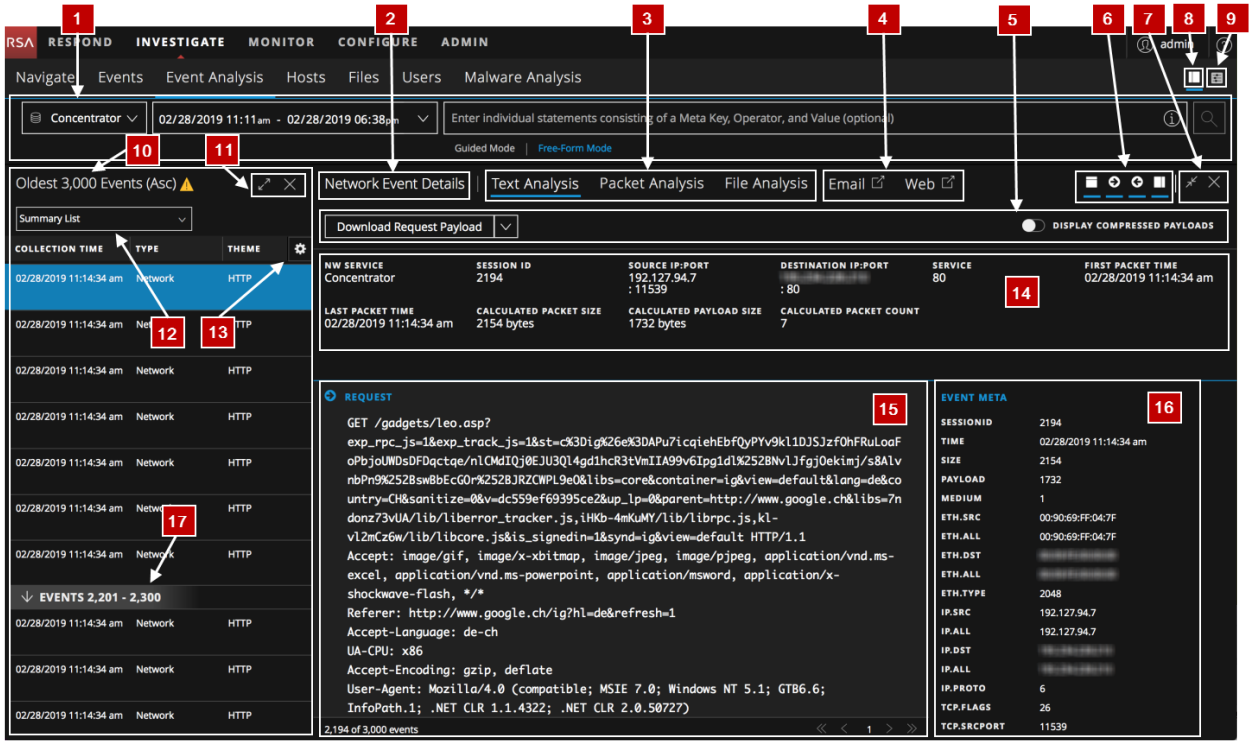
There are multiple access points to this view, which are described in Begin an Investigation in the Event Analysis View. If you access Event Analysis from the Respond view, you can see the analysis for a selected event in an incident. The options are a subset of the options available when you open an event from within the Investigate view. To get complete functionality and examine other events, you can go to the Event Analysis view directly (INVESTIGATE > Event Analysis).

The Event Analysis view lists events in ascending order by time in the Events panel. The events displayed can be results for the drill point in the Navigate view or Events view, or results for a query entered in the Event Analysis view breadcrumb.

Input fields for a query are displayed so that you can select a service and time range, and type an optional query. When you submit a query, the service being investigated counts the results up to a limit of 50,000 events, and 50,000 network, log, and endpoint events are loaded in the Events panel. Different columns are displayed, depending on the selected column group. You can rearrange and resize the columns, choose a built-in or custom column group, and choose individual columns that you want to see. When you find an event of interest, clicking the event opens the reconstruction in a new panel (Packet Analysis, Text Analysis, or File Analysis).

Note: For versions earlier than 11.3, the first 100 events are loaded. You can scroll through the list and click **Show Next 100 Events** at the bottom of the list. If the next page contains fewer than 100 events, the button changes to reflect the number of remaining events.

The following figure highlights the major features of the Event Analysis view for Versions 11.3 and later.



1 **Query Bar**: When a service is selected, displays the service selector, time range selector, and the queries you have entered. You can select a service as described in Begin an Investigation in the Event Analysis View and refine the query as described in

	Filter Results in the Event Analysis View. Clicking submits the query and sends a request to the selected service to load the data. In Version 11.3, clicking the (console icon) opens the query console, where detailed status of the query is provided (see Query Console below).
2	The type of event being analyzed is reflected in the heading: **Network Event Details**, **Log Event Details**, or **Endpoint Event Details**. For details, see Reconstruction Types in the Event Analysis View.
3	The types of analysis available for the event type. Network events can use all types of analysis: text, packet, and file. Log and endpoint events use only text analysis.
4	The Email and Web analysis types open the current event as an email or web reconstruction in the Events view.
5	These options vary for the different types of analysis. For details, see Examine Events in the Event Analysis View.
6	Controls to show or hide the Event Header, show or hide requests and responses, and open the Event Meta panel (16). For details, see Examine Events in the Event Analysis View.
7, 11	Controls to change the size of the panel and close the panel. For details, see Examine Events in the Event Analysis View.
8	Reopens the Events panel or the Event Meta panel if you have closed it. For details, see Examine Events in the Event Analysis View.
9	Sets preferences for the Event Analysis view (see Configure the Event Analysis View.
10	The Events panel title. In Version 11.3 and later, the Events panel title is slightly different than the title in prior versions, and a row number indicator has been added. The title lists the number of events and sort order; for example, **24,000 Events (Asc)** means that 24,000 events were found and they are listed in ascending order by time. If more than 50,000 events are found, only the oldest 50,000 events are displayed in ascending order, and an amber triangle highlights the fact that not all events were loaded. This may indicate that you need to refine the query.(For more information about refining the events listed here, see Filter Results in the Event Analysis View. Versions prior to 11.3 simply list the number of events found, and you can load 100 of them at a time. .
12	The Column Group drop-down lists built-in and custom column groups that you can apply to the Events panel. Built-in column groups are sometimes updated between one version and the next. Some examples of built-in column groups are Email Analysis, Endpoint Analysis, Malware Analysis, Outbound HTTP, Outbound SSL/TLS, and Summary List. Summary List is the default column group.
13	Settings to select the individual columns displayed in the Events panel.
14	The Event Header provides summary information about the event you are currently analyzing. The selected event is highlighted in the Events panel with a blue background. The summary information is different for the different event types (packet, log, and endpoint).
15	The event data for the event you are currently analyzing. • For a packet, the data is called a payload and is displayed in the form of a request and response. • For a log event, the data is a line of text from the raw log. • For an endpoint event, the event data is relevant to data from the NetWitness Endpoint Insights Agents running on hosts in the network. It may be a single process, driver, DLL, file (executable), service, or autorun, and information related to logged-in users. (See the *NetWitness Endpoint User Guide* for complete information about endpoint

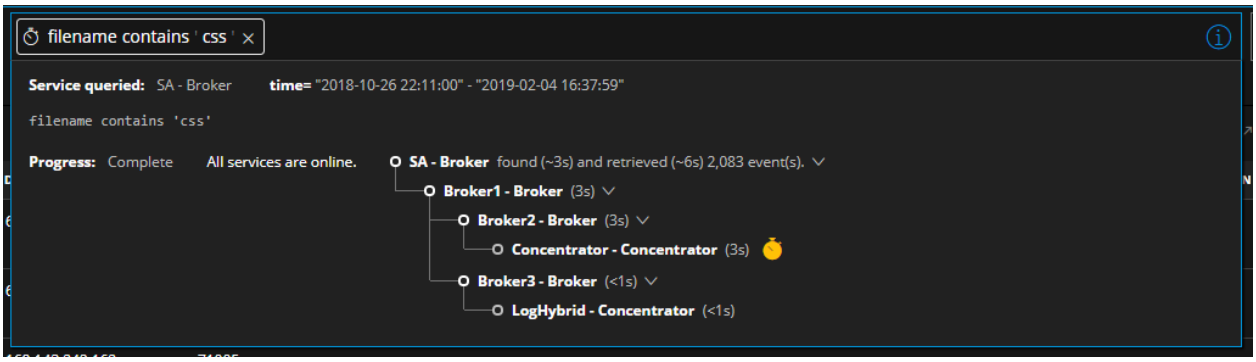
event data.)

16 The Event Meta panel lists the meta keys and values found in the data. Some metadata are searchable; they have a binoculars icon, which you can click to see the associated data highlighted in the event data (see Examine Events in the Event Analysis View).

17 (Version 11.3) Because the number of events can be up to 50,000, a row number indicator appears at the beginning of every hundred events, beginning with 200.

Query Console

Clicking (the console icon) opens the query console, where detailed status of the query is provided.



In the query console, you can see which service, time range, and metadata was queried as well as real-time information about the status of the query and the services being queried. A progress bar indicates the query's completion percentage at the bottom of the console. The statuses let you know details about what is happening; for example, you can tell when the query is executing, queued, reading the index file for the queried service, retrieving events, and complete. All statuses and non-fatal messages are displayed as they come in, and the border color changes if a non-fatal error occurs. View Status of a Query provides additional details on this subject.

Several messages that may be displayed in the query console require additional explanation.

Message: Maximum value limit (`valueMax`) of %1% reached on meta key %2% in index slice %3%

Explanation: The `valueMax` property on the specified meta key has been reached in the index being queried. An administrator configures this inside the index files available in `ADMIN > Services > [Service Name] > Files > index-[service type].xml` or `index-[service type]-custom.xml`. As an example, the statement below from the index file states the meta key called `client` has a limit of 250,000 values by default.

```
<key description="Client Application" level="IndexValues" name="client"
format="Text" valueMax="250000" />
```

Message: The query on channel %2% was auto-canceled by the system for exceeding time usage limits. Check timeout values.

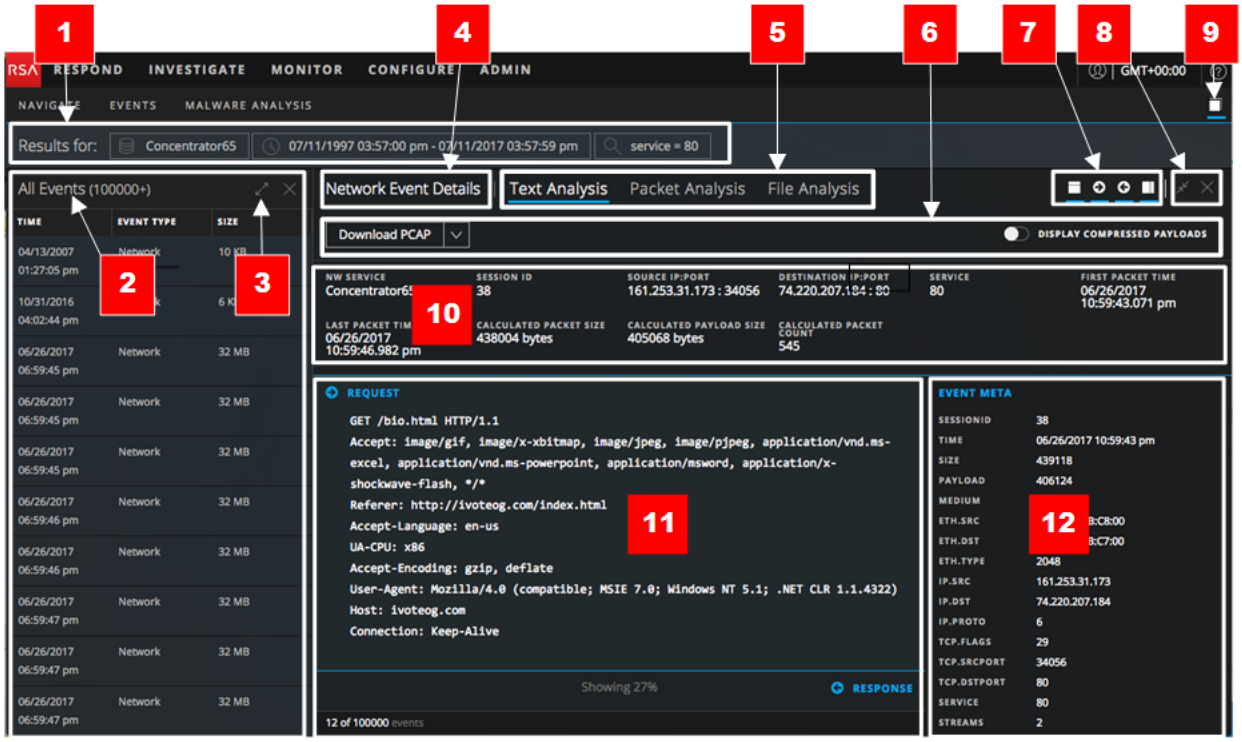
The server has a per-operation limit on execution time, and the requested operation exceeded the limit. To avoid this error, split the operation into smaller pieces, such as smaller time ranges.

Memory limit of %1% reached, controlled by setting max.query.memory

The server has a per-operation limit on memory utilization, and the requested operation exceeded the limit. The limit is related to the amount of memory in the server, which an administrator can adjust in **ADMIN > Services > [Service Name] > sdk > config**. To avoid this error, split the operation into smaller pieces, such as smaller time ranges.

Quick Look for Version 11.0.0.x (End-Of-Life)

The following figure highlights the major features of the Event Analysis view for Version 11.0.0.x.



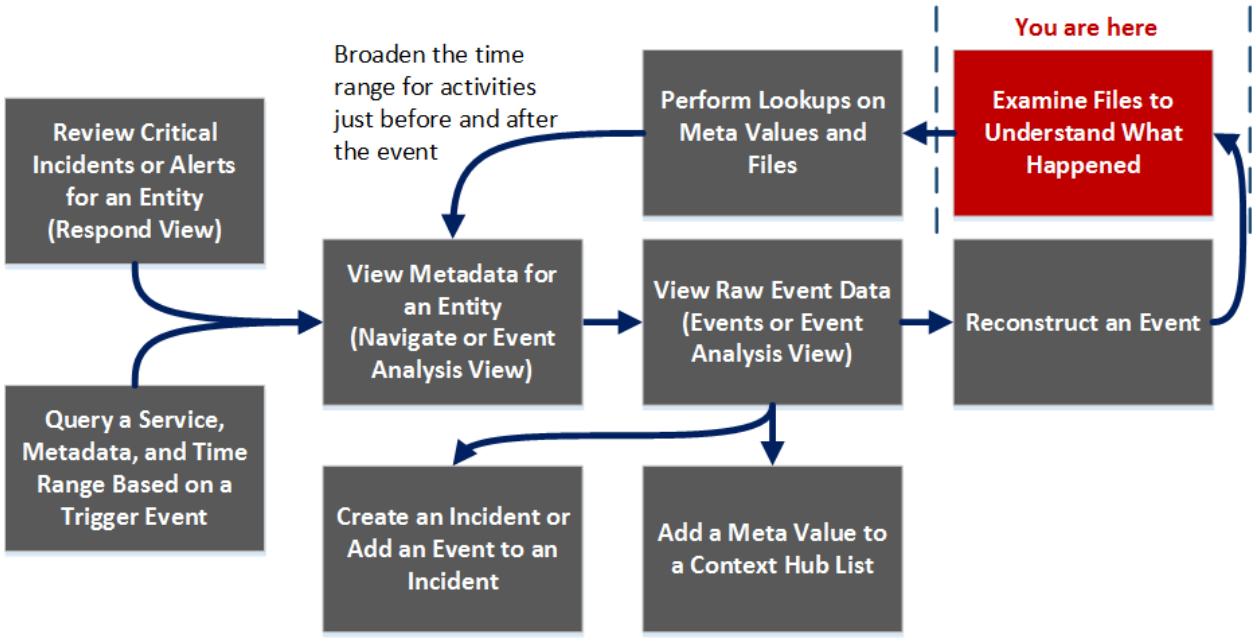
1	The read-only breadcrumb displays the selected service, time range, and query entered in the Navigate view or Events view.
2	This is a read-only list of events based on the query made in the Navigate or Events view. The Events panel includes a count of the events. You can rearrange and resize columns. You can scroll to the bottom of the list, and load more events (see Examine Events in the Event Analysis View).
3, 8	Controls to change the size of the panel and close the panel.
4	The type of event being analyzed is reflected in the heading: Network Event Details, Log Event Details, or Endpoint Event Details. Each view is discussed in detail in Examine Events in the Event Analysis View.
5	The types of analysis available for the event type. Network events can use all three types of analysis: text, packet, and file. Log and endpoint events use only text analysis.
6	These options vary for the different types of analysis. They are discussed in detail in Examine Events in the Event Analysis View.
7	Controls to show or hide the Event Header, show or hide requests and responses, and open the Event Meta panel (12). These controls are described in Examine Events in the Event Analysis View.

9	Reopens the Events panel or the Event Meta panel if you have closed it.
10	The Event Header provides summary information about the event. This information is different for the different event types (packet, log, and endpoint).
11	The event data (sometimes called a payload for packets). The event data for a log event or endpoint event is typically a line of text from the raw log rather than request and response shown for a packet.
12	The Event Meta panel lists the meta keys and values found in the data. Some meta data are searchable; they have a binoculars icon, which you can click to see the associated data highlighted in the event data (see Examine Events in the Event Analysis View.

Event Analysis View - File Analysis Panel

In the File Analysis panel (**Event Analysis** > **File Analysis),** you can safely view a list of files and download one or more files in an event.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View

User Role	I want to ...	Show me how
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

Related Topics

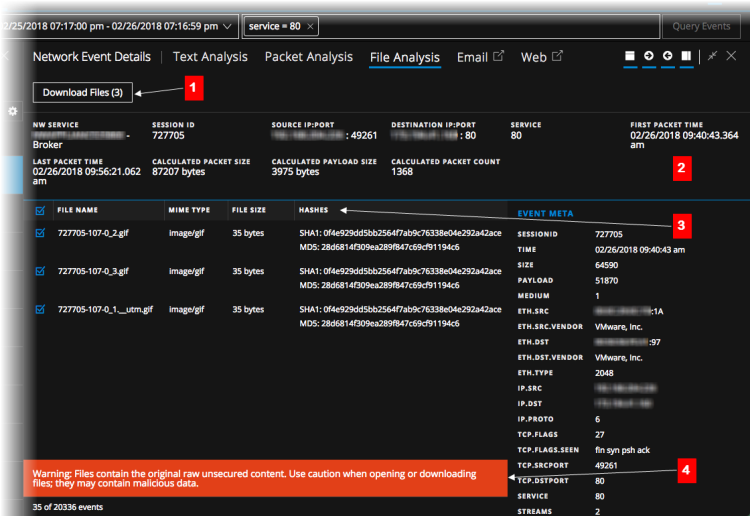
- How NetWitness Investigate Works
- Event Analysis View
- Event Analysis View - Text Analysis Panel
- Event Analysis View - Packet Analysis Panel

Quick Look

The File Analysis panel displays a list of files associated with a network event. You can download files in this view.

Below is an example of the File Analysis panel with labeled features.

Note: The Email and Web reconstruction types at the top of the figure are available in Version 11.1 and later.

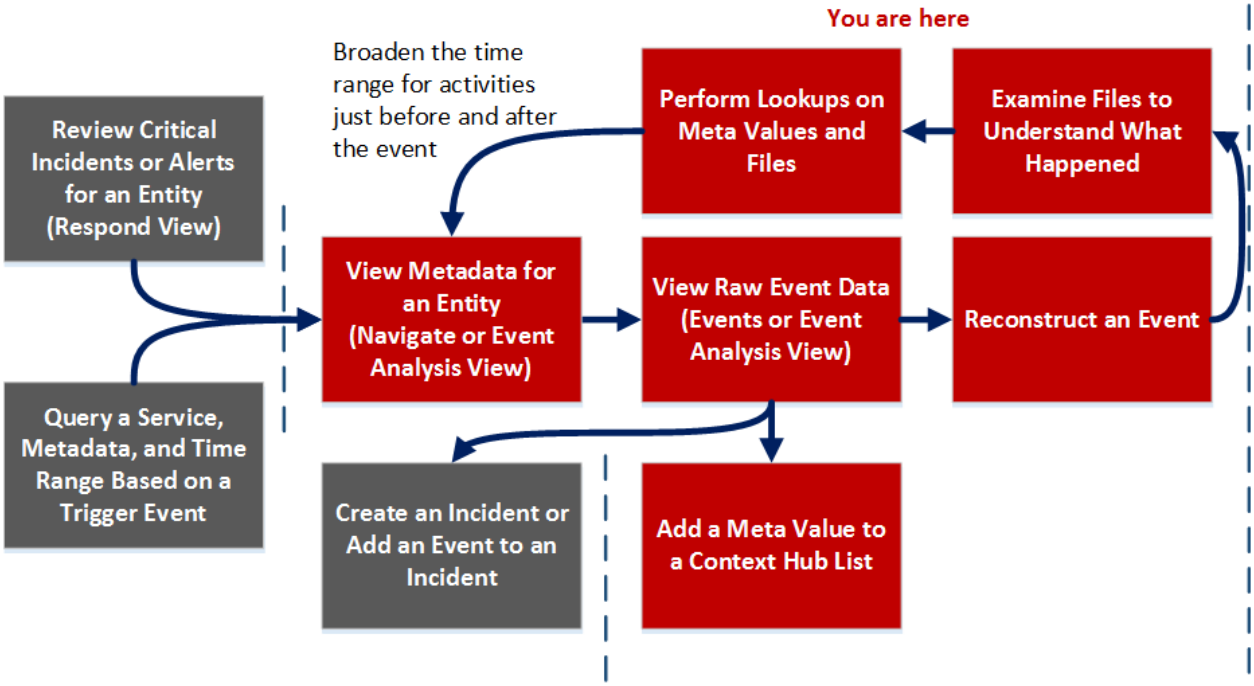


1 Click to download one or more selected files.
2 The Event Header displays summary information for the network event that contains the files.
3 Scrollable list of associated files that you can select and download.
4 Reminder that caution is necessary when downloading potentially malicious files.

Event Analysis View - Packet Analysis Panel

In the Packet Analysis panel (**Event Analysis > Packet Analysis),** you can safely view and interactively analyze the packets and payload of an event.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata*	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View

User Role	I want to ...	Show me how
Threat Hunter	view raw event data*	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event*	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups*	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View
- Event Analysis View - Text Analysis Panel
- Event Analysis View - File Analysis Panel

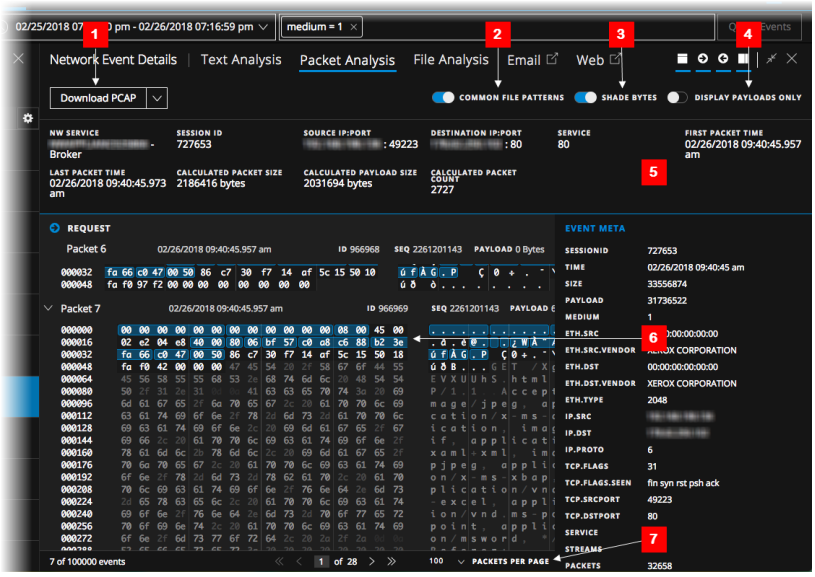
Quick Look

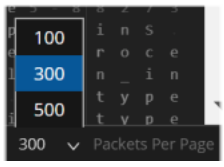
Only network events can be analyzed in the Packet Analysis panel. The Packet Analysis panel lists each packet in the event. The list of packets is scrollable. When you scroll, the packet or text identification information as well as the Request and Response labels remain visible rather than scrolling out of view.

In Version 11.1 and later, you can use pagination controls to go backward and forward through the pages, go to a specific page, and select the number of packets to display per page (100, 300, or 500).

Each packet is displayed with shading and highlighting to help identify common file patterns: significant header and payload bytes, hexadecimal and ascii bytes, and common file signatures. In addition, you can adjust the request/response display, and display or hide the packet summary.

Below is an example of the Packet Analysis panel with labels to identify features. For details and examples of each feature, see Examine Events in the Event Analysis View.

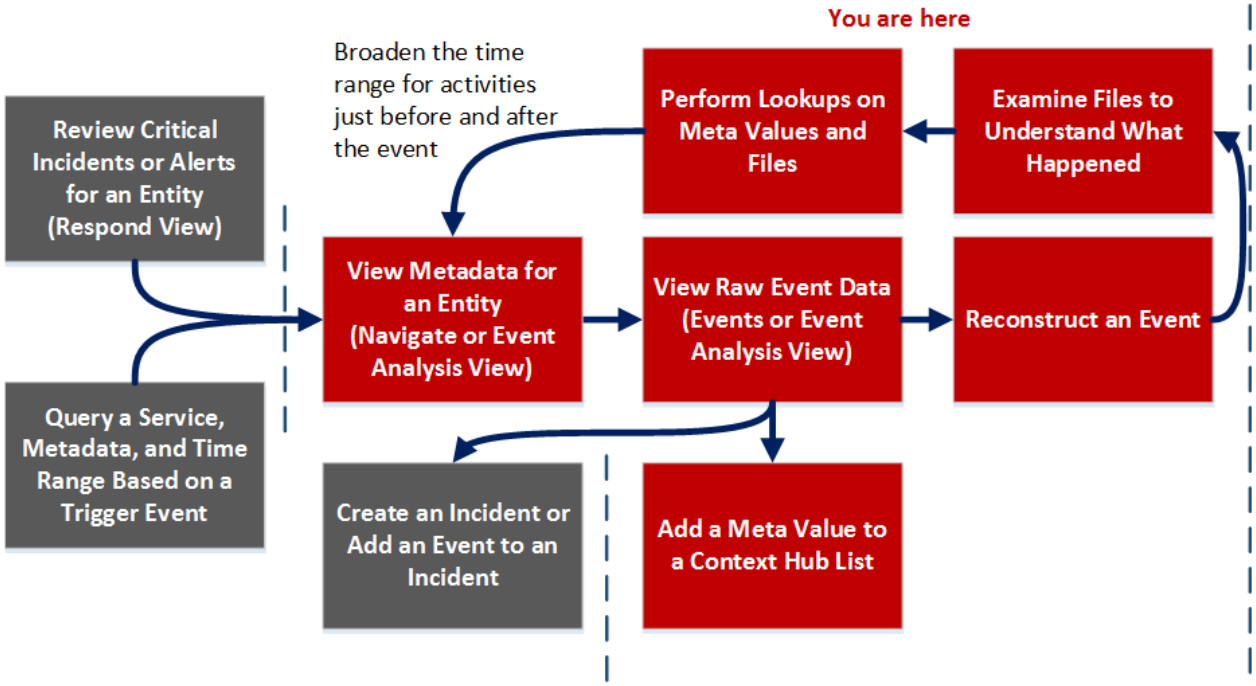


1	Options for exporting a network event. You can export a PCAP, all payloads, request payloads, or response payloads for deeper analysis and to share with others.
2	The option to identify common file signatures is activated by default. Common file signatures are highlighted in orange; hovering over the highlight reveals the file type.
3	The Shade Bytes option adds shading to identify the different hexadecimal bytes (00 to FF) using degrees of highlighting.
4	The option to display payloads only hides the packet headers, leaving more space for the payload.
5	The Event Header.
6	Significant bytes are highlighted in a blue background; as you move the cursor over the highlighting the meta data is displayed in a hover box.
7	(Version 11.1 and later) Packet pagination controls allow more flexibility in paging through a list of packets. When a control is unavailable, the image is dimmed; for example, when you are viewing page 1, the ⟪ and ⟨ controls are dimmed. ⟪ - Go to the first page ⟨ - Go to the previous page 1 of 206 - Go to a specific page ⟩ - Go to the next page ⟫ - Go to the last page  - Select the number of packets per page

Event Analysis View - Text Analysis Panel

In the Text Analysis panel (**Event Analysis > Text Analysis),** you can safely view and analyze the raw text payload of an event. The Text Analysis panel includes features that can show decompressed or compressed text, expand truncated entries, perform URL and Base64 encoding and decoding, and download network events, logs, and endpoint events. The Text Analysis panel is available for all types of events: network, log, and endpoint.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata*	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View

User Role	I want to ...	Show me how
Threat Hunter	view raw event data*	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event*	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups*	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

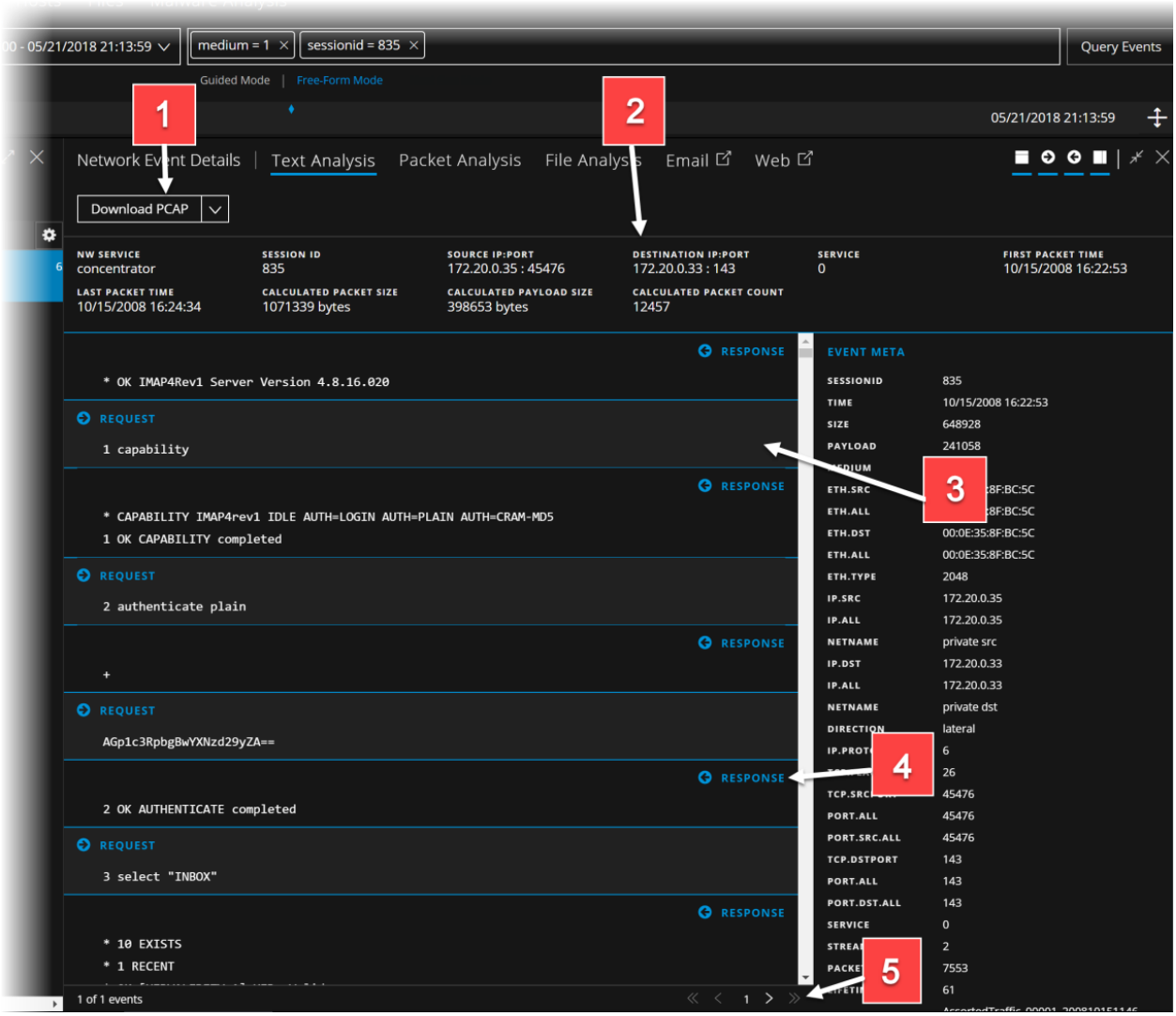
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View
- Event Analysis View - Packet Analysis Panel
- Event Analysis View - File Analysis Panel

Quick Look

The Event Analysis view displays the text of a single event in the Text Analysis panel. When you click an event in the Event list panel, the adjacent panel shows the Text Analysis. Only the raw log for log events and endpoint events is shown in the Text Analysis panel. For network events, the direction of the packet (Request or Response) and contents of each packet are provided in text format. For more examples of the Text Analysis, see Analyzing Raw Events and Metadata in the Event Analysis View. For detailed procedures, see Examine Events in the Event Analysis View.



1	Options for exporting a log, a PCAP, or files for deeper analysis and to share with others. This download menu is for network data.
2	The event header information.
3	The payload for a network event includes requests and responses. This is the request side of the packet.
4	This is the response side of the packet.
5	(Version 11.2 and later) Event pagination controls allow more flexibility in paging through a list of events. When a control is unavailable, the image is dimmed; for example, when you are viewing page 1, the ⟪ and ⟨ controls are dimmed. ⟪ - Go to the first page ⟨ - Go to the previous page ⟩ - Go to the next page ⟫ - Go to last page (Only available after last page has already been navigated to)

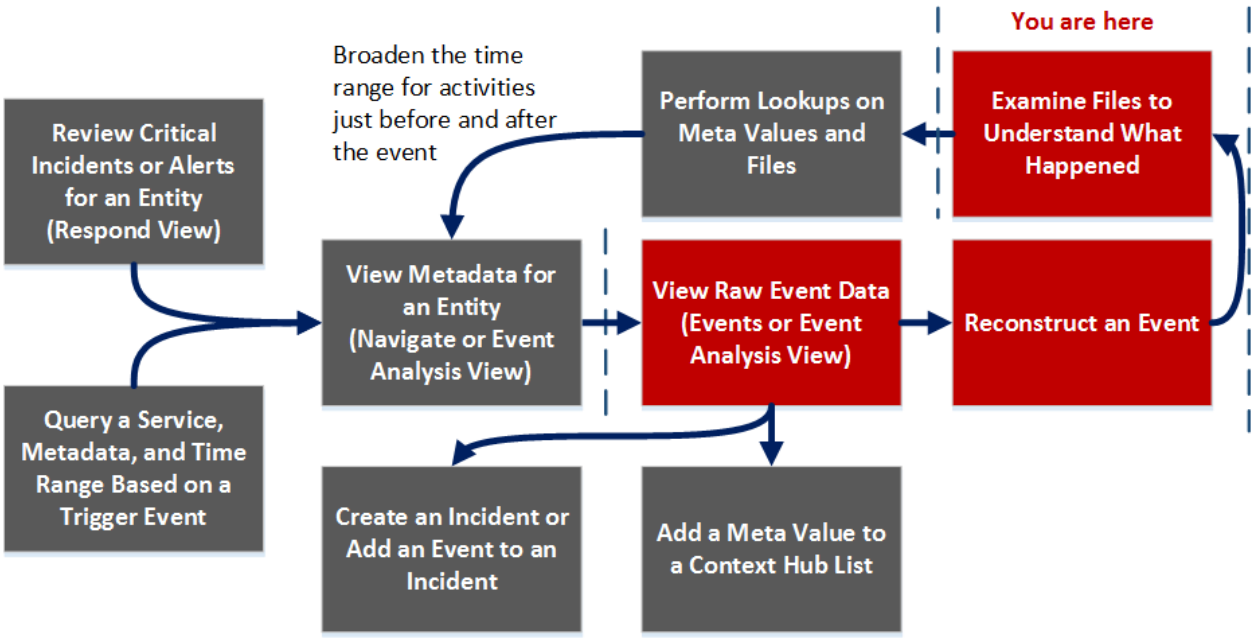
Event Reconstruction View

The Event Reconstruction view provides a reconstruction of a selected event from the Events view. By default, NetWitness Platform displays the best reconstruction for the event determined by the event content, or the default reconstruction that you have selected in the Default Session View setting for Investigate. You can use the options in the Event Reconstruction toolbar to change the reconstruction method, view top-to-bottom or side-by-side results, select request and response views, export an event, export meta values, extract files, open an email attachment, and open the event in a new tab.

To access this view, do one of the following:

- In any Events view, double-click an event.
- In the Events view with Detail View selected, right-click **Event Analysis** at the end of the event, and select **Event Reconstruction.**
- In the Event Reconstruction toolbar of previewed reconstruction, click **Open Event in New Tab**.
- In the Navigate view, select **Actions > Go to event in Event Reconstruction**, and enter an event ID.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*

User Role	I want to ...	Show me how
Threat Hunter	query a service, metadata, and time range	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data*	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event*	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

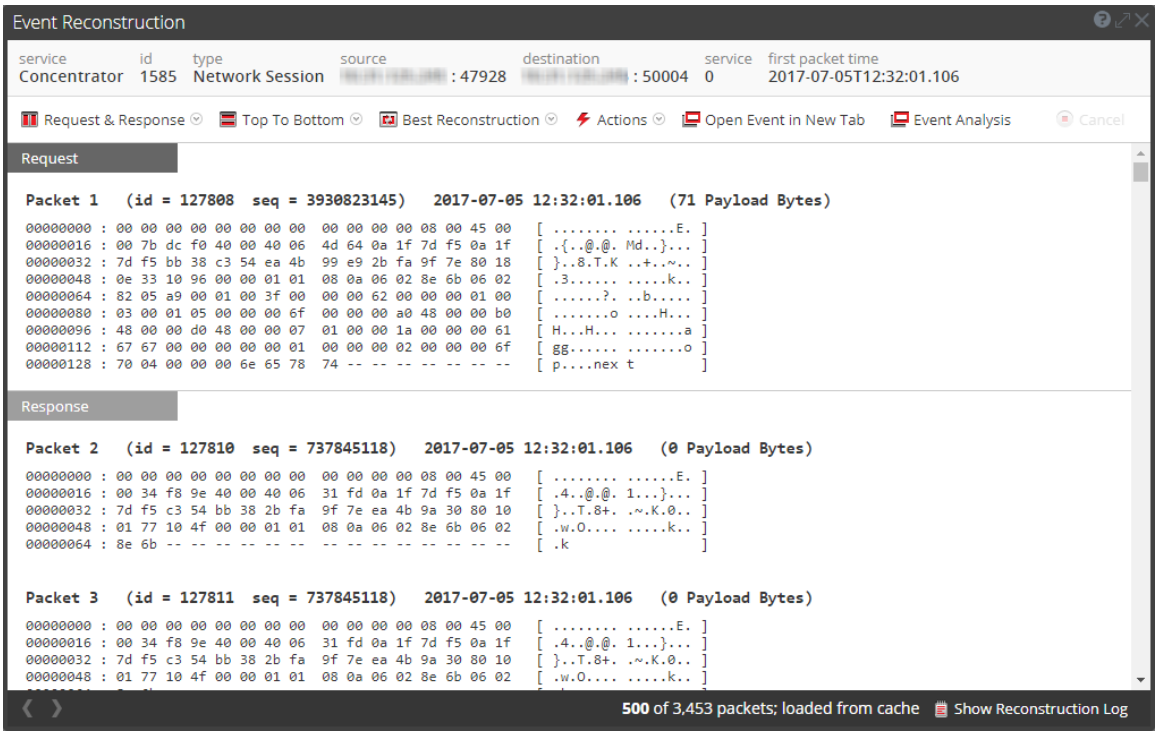
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Event Analysis View

Quick Look

This figure is an example of the Event Reconstruction view. The following table describes the toolbar options.



Feature	Description
Request & Response	Displays a drop-down menu for selecting whether the view displays: • Request & Response • Request • Response
Organization	Displays a drop-down menu for selecting whether the information is displayed top to bottom or side by side.
Reconstruction View	Displays a drop-down menu for selecting what information is displayed. By default, Best Reconstruction is selected. Other options are: • View Meta • View Text • View Hex • View Packets • View Web • View Mail • View Files
Actions	Displays a drop-down menu with the actions available in the Event Reconstruction view (Export PCAP, Extract Files, and Export Meta).

Feature	Description
Open Event in New Tab	Opens the event in a new browser tab.
Event Analysis	Open the event in the Event Analysis view.

Beneath the toolbar is a list of meta keys and values. Some of the keys offer a drop-down menu with available actions.

The bar at the bottom of the view offers several options.

Feature	Description
	Displays the previous event.
	Displays the next event.
Show Reconstruction Log	Displays the reconstruction log at the bottom of the view. Once you click this button, it changes to Hide Reconstruction Log.

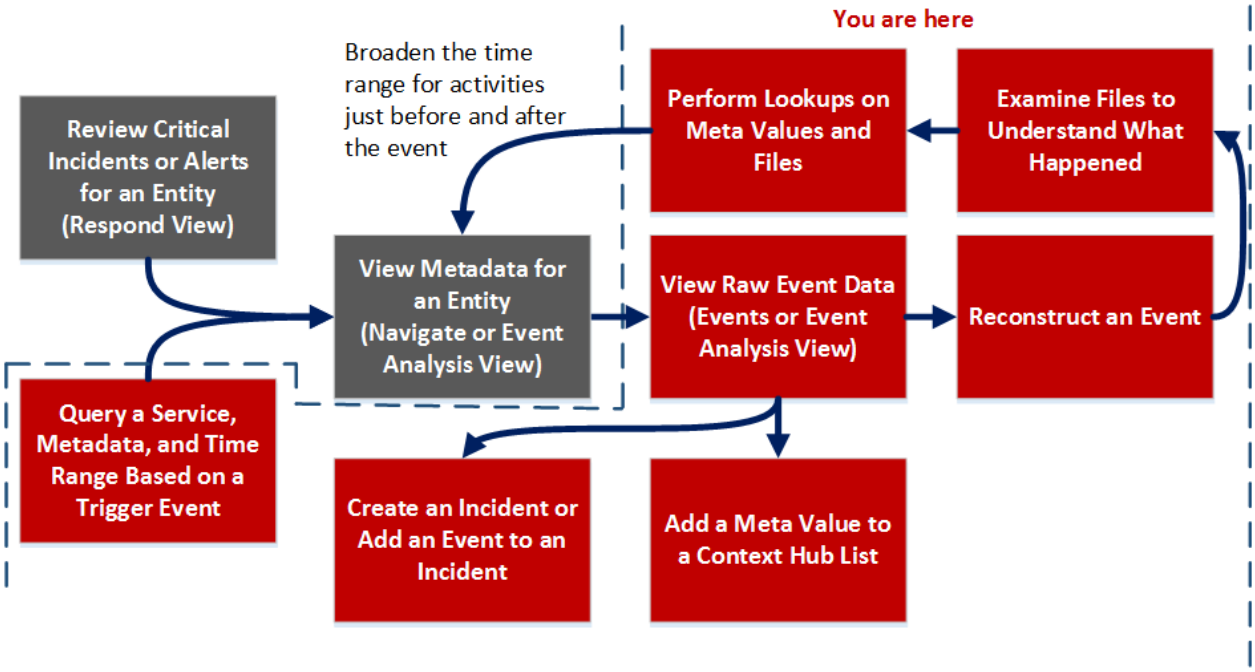
Events View

In the Events view a list of events associated with a session is available; this view is optimized for viewing raw events in sequence by time. You can display the events list in several forms, filter events, search for events, and open a reconstruction of an event.

There are two ways to display the Events view:

- Go to **INVESTIGATE > Events.** NetWitness Platform runs a default query on the last three hours for the default service (if one is set) or displays a dialog in which you can select a service and then runs the default query. The default query selects all events and the Events view displays events on the selected service, with the oldest events first.
- From within the **Navigate** view, double-click an event. The Events view displays the events on the selected service based on the drill point in the Navigate view.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*

User Role	I want to ...	Show me how
Threat Hunter	query a service, metadata, and time range*	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data*	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event*	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups*	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Examining Raw Events in the Events View
- Querying and Acting on Data in the Navigate and Events Views

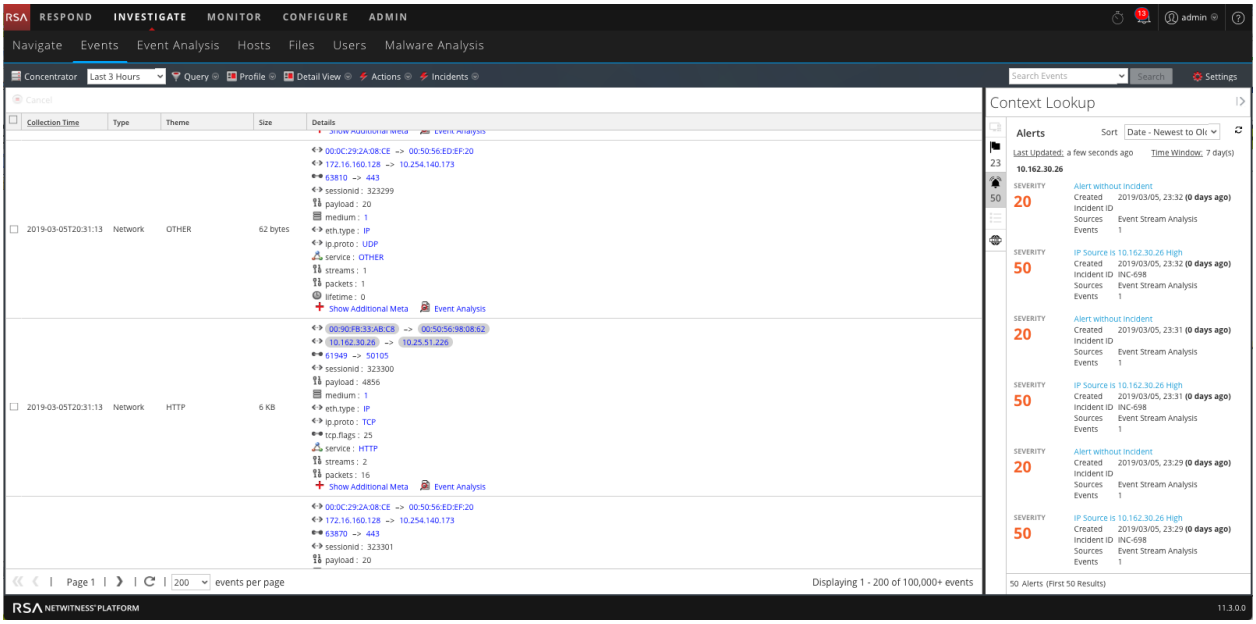
Quick Look

The Events view provides three built-in presentations of event data: the Detail view, the List view, and the Log view. The List view and Detail view provide more information for each event including the timestamp, event type, event theme, and size.

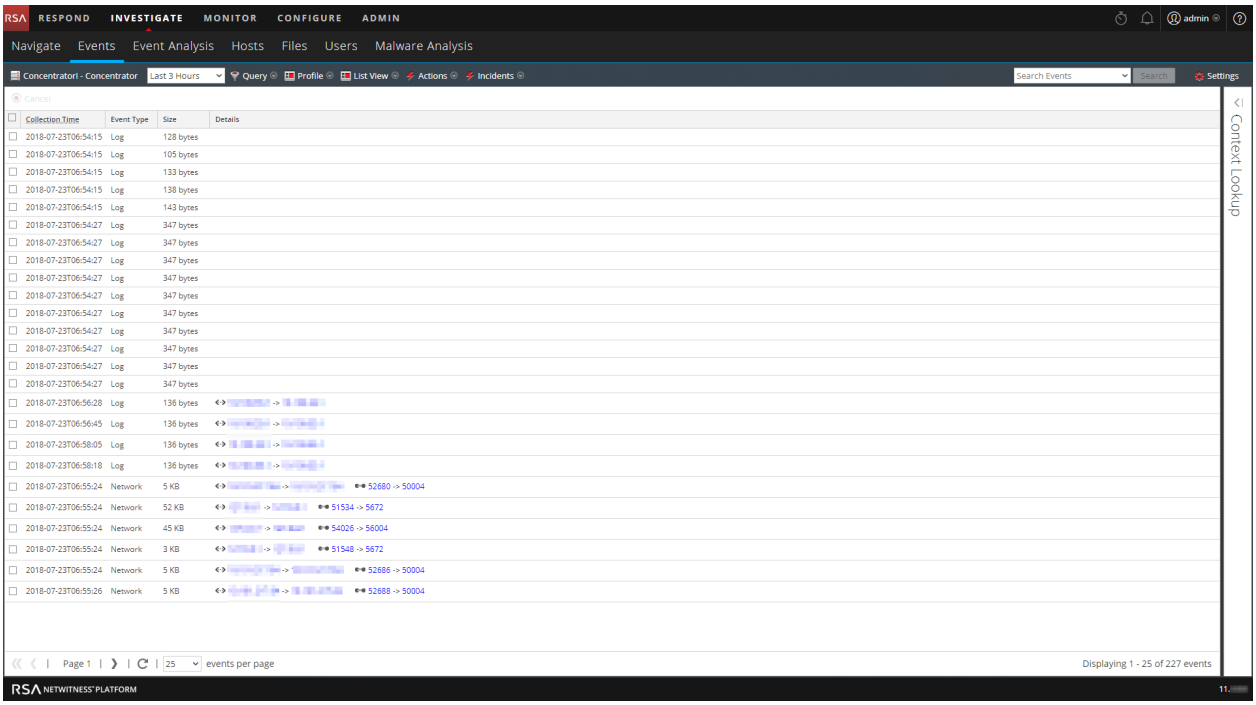
- The List View shows corresponding source and destination address and port information for events in summary form in a grid.
- The Detail View shows all metadata collected for the event in a paged view.
- The Log View is optimized for viewing log and endpoint information, and provides more information for each log including the timestamp, event type, service type, service class, and the logs.

You can use queries, the time range setting, and profiles to filter the events listed in the Events view. From any view type in Events view, you can extract files; export network events, endpoint events, logs, and meta values, and open the Event Reconstruction panel. In the Detail View you can also open the event in Event Analysis.

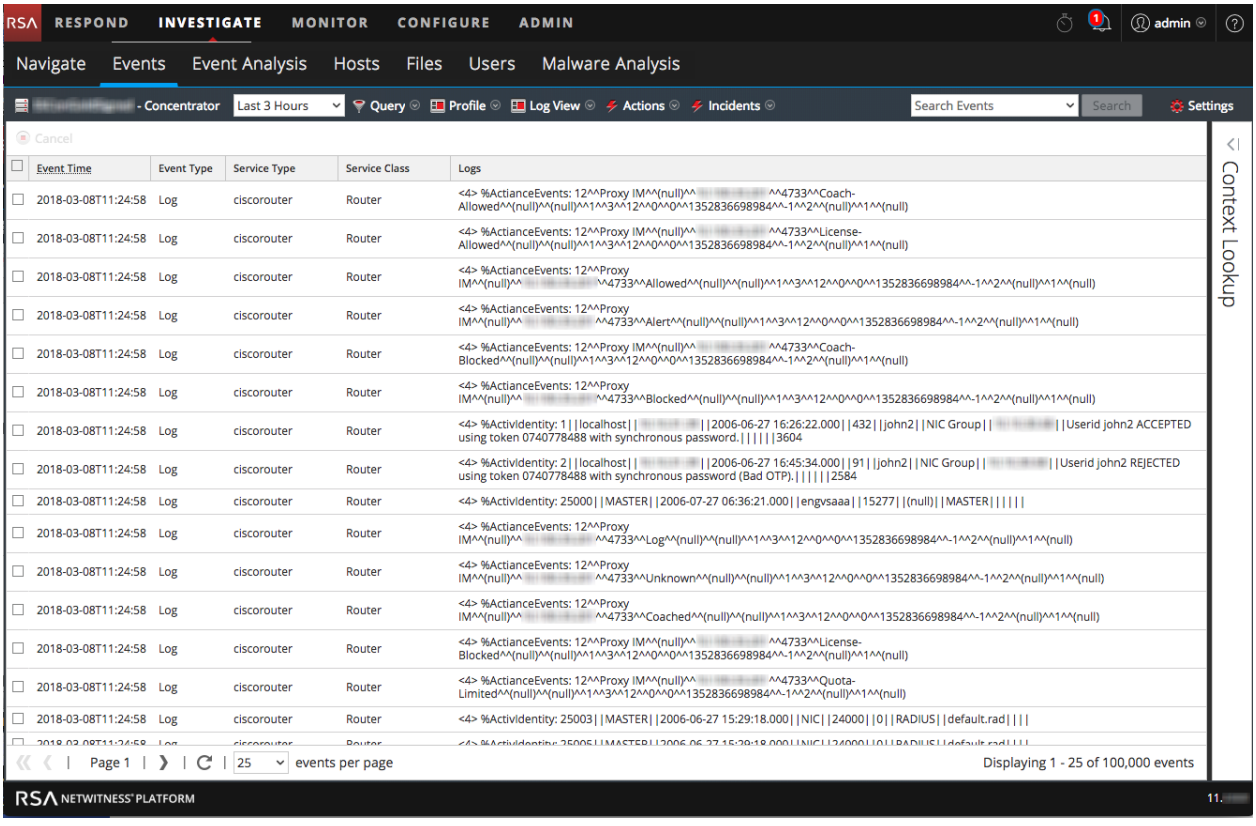
The following figure is an example of events in the Detail View. The Context Lookup panel is visible only if the Context Hub service is configured.



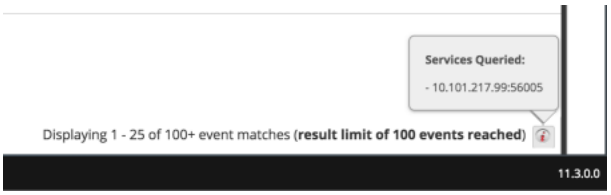
The following figure is an example of events in the List View.



The following figure is an example of the Log View.



The following figure shows the information added to the footer for Version 11.3 and later.



Detailed Description

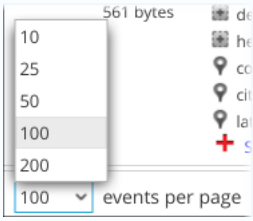
The Events view has a toolbar at the top with the following options.

Feature	Description
Select Service	Displays the selected service name next to the icon. Opens the Investigate dialog, in which you can select a service for which the event list is displayed.
Time Range	Displays a drop-down menu for selecting the time range to apply to the event list. You can choose one of the standard options or specify a custom time range.
Query	Displays the Query dialog, in which you can enter a custom query directly instead of drilling down the data (see Create a Custom Query).
Profile	Displays the Profile menu; the currently selected profile is displayed in the toolbar. The menu options include built-in (Default) profiles and custom profiles, as well as an option to manage profiles. Each profile can include a meta group, a column group, and a beginning query that is applied to the Navigate view (meta groups and queries) and the Events view (column groups and queries) as you investigate events. (see Use Profiles to Encapsulate Common Areas for Investigation).
View Type Drop-down	Displays a drop-down menu for selecting the event view type. • Detail View shows events in a paged format with detailed information for each event. • List view shows the events in table form with a summary of each event in a separate row. • Log View shows a log-oriented events grid with a summary of each log in a separate row. • Custom Column Groups displays the event list using a column group selected from a drop-down list of custom column groups. • Manage Column Groups displays the dialog for creating and editing custom column groups.

Feature	Description
Actions	Displays a drop-down menu with actions in the Events view: • Export an events as PCAP files, export logs, export endpoint events, or export meta values. • View an event reconstruction in a popup window or in a new tab. • Reset all filters in the Events view.
Incidents	Create a new incident in Respond and add the selected events, or add selected events to an existing incident in Respond.
Search	Displays the Search Events options, which allow you to specify the export log and export meta value format with additional options explained in Search for Text Patterns
Settings	Displays the Investigation settings for the Events view (which are also available in the Profile view) so that you can change Investigation settings without navigating away from the Events view. When you change a setting In the Events view, the setting is also changed in the Profile view (see Configure the Navigate View and Events View).

Other features of the Events view are described in this table.

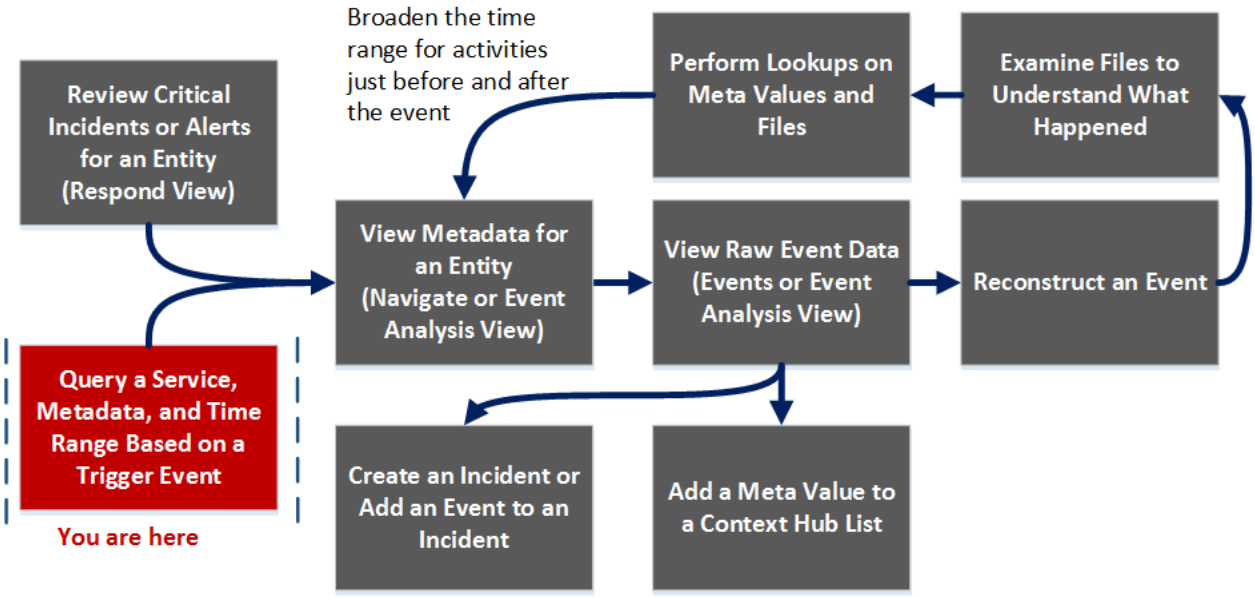
Feature	Description
Show Additional Meta (in the Detail View of an event)	Displays the rest of the metadata for the event.
Event Analysis (in the Detail View of an event)	Opens the selected event in the Event Analysis view.

Feature	Description
(in the footer)	Pagination controls allow more flexibility in paging through a list of events. When a control is unavailable, the image is dimmed; for example, when you are viewing page 1, the « and ‹ controls are dimmed. « - Go to the first page ‹ - Go to the previous page 3 Page 3 | - Go to a specific page › - Go to the next page » - Go to the last page  - Select the number of packets per page When you select a number of events per page, the setting is saved in browser cache so that you do not have to select your preferred number of events each time you log in. The setting applies to all views: Log View, List View, and Details View.
Displaying 1-100 of 100,000 events (in the footer) Displaying 1-25 of 100+ event matches (result limit of 100 events reached) (in the footer)	Displays the count of events displayed versus the total number of matching events. In Version 11.3 and later, the footer includes a notification if the results limit configured by the administrator has been reached to let you know that more results are available but not viewable. To view the additional results, you need to refine the filter to get fewer results. Clicking the information icon in the footer displays the IP address and connecting port number for all services queried.

Investigate Dialog

In the Investigate dialog, analysts can select a service or a collection to investigate. The dialog is automatically displayed when you first go to the Navigate view or Events view and have not selected a default service to investigate. To access the dialog from a current investigation, select the current service name in the toolbar.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range*	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View

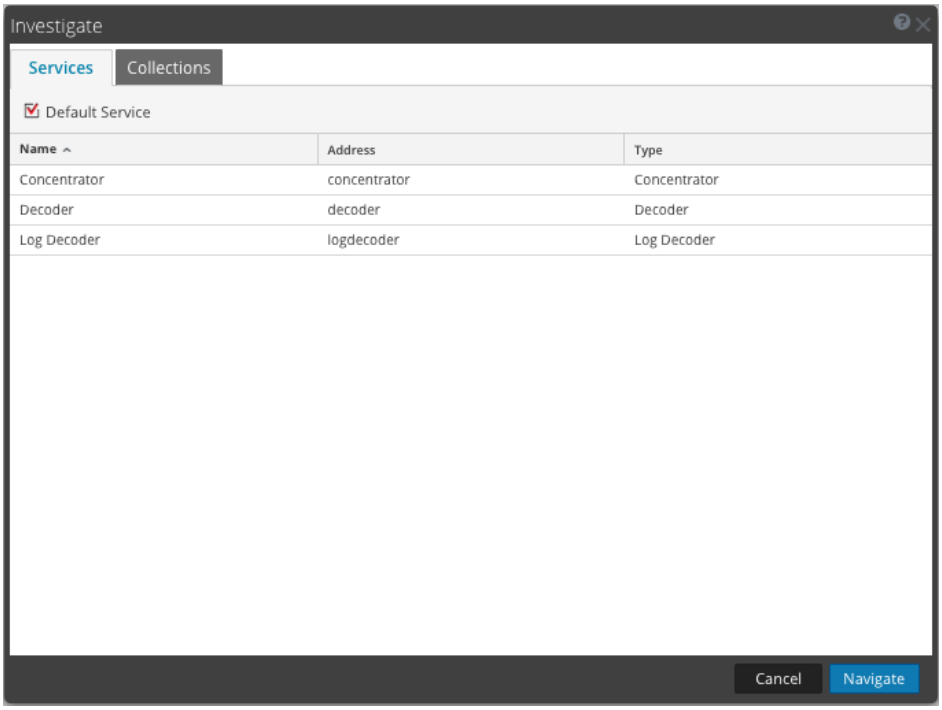
User Role	I want to ...	Show me how
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look



The Investigate dialog has two tabs: Services and Collections.

Note: Collections are also known as workbench collections. You can only view workbench collections that you have created, and only administrators can create a workbench collection.

The Services tab includes a list of services available for investigation, and three buttons. All features are described in the following table.

Feature	Description
Default Service	Clicking this button sets or clears the default service to investigate. When a service has been set as the default service, the word (Default) is appended to the service name.
Name	The name of the service.
Address	The IP address of the service.
Type	The type of service.
Cancel	Closes the dialog.
Navigate	Opens the selected service in the Navigate or Events view.

The Collections tab has two buttons and two panels: Workbench and Collections.

The Workbench panel lists available Workbench services by name. After a Workbench service is selected, you can select a collection from the Collections panel.

The Collections panel lists available collections to investigate. After a collection is selected, you can click Navigate to view the collection.

The following table describes the features of the Collections panel.

Feature	Description
Name	The name of the collection.
Type	The type of collection.
Size	The size of the collection.
Data Type	The type of data within the collection.
Date Created	The date the collection was created.

Investigation Tab - User Preferences Panel

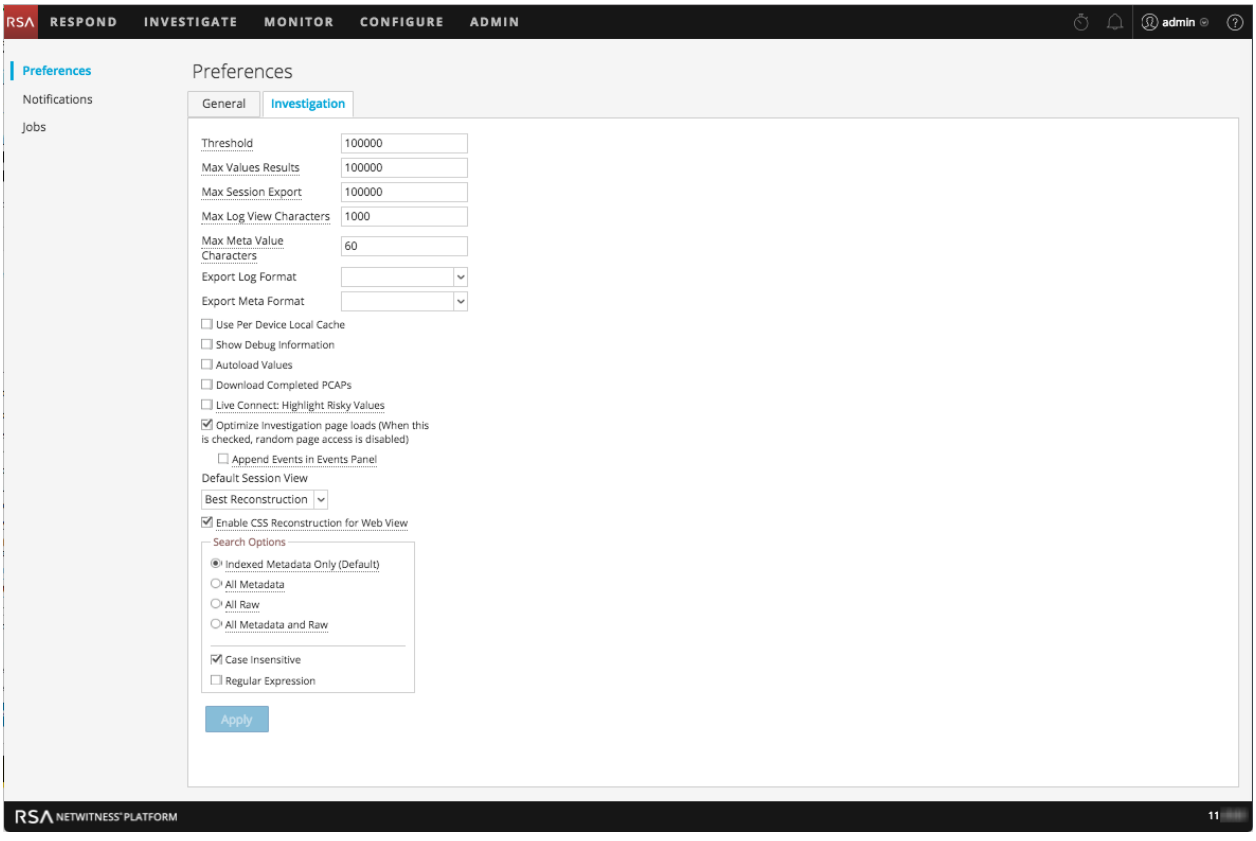
In the Profile view > Preferences panel > Investigation tab, users can set several preferences that affect the performance and behavior of NetWitness Platform when analyzing data, viewing events, and reconstructing events in NetWitness Investigate. To access this tab, select > Profile from the Navigate view or the Events view. When the Profile view is displayed, select **Preferences > Investigation**. You can change user preferences at any time when you are working in NetWitness Platform.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

This figure is an example of the Investigation tab, and the following table describes the preferences that affect Investigate. There are slight differences between the 11.1 search settings and later versions of the search settings and these are explained in Search for Text Patterns.



Feature	Description
Threshold	This setting controls the count shown for a meta key value in the Navigate view during the load. A higher threshold allows more accurate counts for a value. However, a higher threshold causes longer load times. When the threshold is reached, NetWitness Platform displays the count and the percentage of time used to reach the count in comparison to the time necessary to load all sessions with that value. For example, **(>100000 - 18%)** indicates that the threshold was set at 100000 and this load took only 18% of the time it would have taken with no threshold set. The default value is **100000**.
Max Values Results	This setting controls the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open meta key. The default value is **1000**.
Max Session Export	This setting controls the maximum number of sessions that can be exported. The default value is **100000**.
Max Log View Characters	This setting controls the maximum number of characters to be displayed on **Investigation > Events > Log Text**. The default value is **1000**.
Export Log Format	This setting specifies the default format for exporting logs from Investigation. Available options are **Text**, **XML**, **CSV**, and **JSON**. There is no default value for the log export format. If you do not select a format for logs here, NetWitness Platform displays a selection dialog when you invoke export of logs. When you select one of the options from the Export Log Format drop-down menu and click Apply, the setting goes into effect immediately.
Export Meta Format	This setting specifies the default format for exporting meta values from Investigation. Available options are Text, XML, CSV, and JSON. There is no default value for the meta export format. If you do not select a format for exporting meta values here, NetWitness Platform displays a selection dialog when you invoke export of meta values. When you select one of the options from the Export Meta Format drop-down menu and click Apply, the setting goes into effect immediately.
Use Per Device Local Cache	Allows you to specify the use of locally cached data from the selected service. By default, this checkbox is cleared (Off), which means that Investigate sends a fresh query to the database rather than displaying cached data in the Investigate views after the initial load. If the option is set, Investigate uses the data from local cache.
Show Debug Information	When this option is set, NetWitness Platform displays the `where` clause beneath the breadcrumb in the Navigate view. For each meta value load, the load time is displayed. If the service is a Broker, the elapsed time for each aggregated service is reported. The default value is **Off.**

Feature	Description
Append Events in Events Panel	When this option is set, the events displayed in the **Events Panel** are added incrementally rather than overwriting the currently displayed events. Each time you click the next page icon, the additional events are appended to the previous events; 1 -25, then 1 -50, then 1 -75 and so on. **Note:** This option is available only if the Optimize Investigation Page Loads option is enabled.
Autoload Values	When this option is set, the service values are automatically loaded in the Navigate view. When not set, NetWitness Platform displays a **Load Values** button, allowing the user the opportunity to modify the options. The default value is **Off**.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigate so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP format.
Live Connect: Highlight Risky Values	If you want NetWitness Platform to highlight and display only IP addresses that are considered to be risky by the RSA community, set this option. When not enabled, NetWitness Platform displays all IP addresses. By default, this option is cleared (Off).
Optimize Investigation Page Loads	This option is enabled by default (checked) and controls how the Events view retrieves events. When enabled, results are returned as quickly as possible, but you cannot go to a specific page in the event list. Clearing the checkbox changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). Being able to go to any page in the list costs additional overhead to determine the events in advance.
Default Session View	This setting selects the default reconstruction type for the initial reconstruction view. By default events are reconstructed using the reconstruction type most appropriate to the event.
Enable CSS Reconstruction for Web View	This setting controls how web content reconstruction is performed. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for stylesheets and images used in the target event. The option is enabled by default. Clear the checkbox if there are problems viewing specific websites. **Note:** The appearance of the reconstructed content may not match the original web page perfectly if related images and stylesheets could not be found or were loaded from the web browser's cache. Also, any layout or styling that is performed dynamically via client side javascript does not render in the reconstruction because all client side javascript is removed for security purposes.
Search Options	This setting specifies the default search options to apply to a search in the Navigate and Events views. Search for Text Patterns provides detailed information.

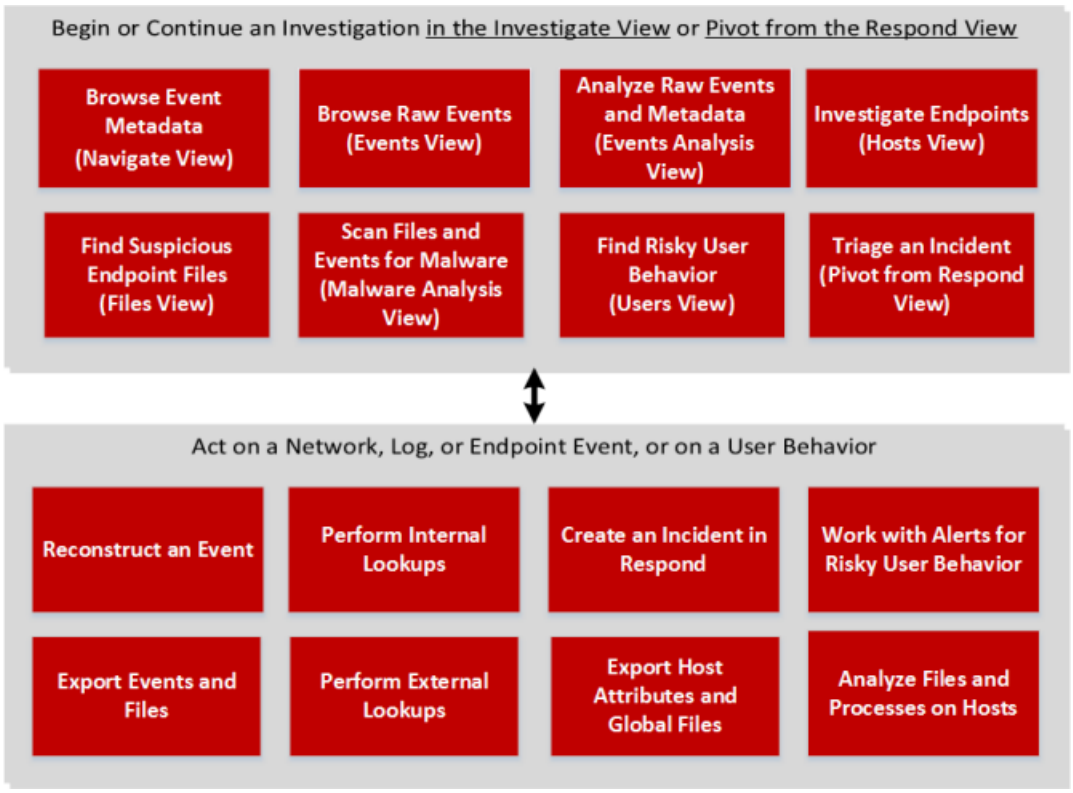
Feature	Description
Apply	Saves your preferences and puts them into effect immediately.

Investigate View

The Investigate view (INVESTIGATE) is the primary entry point to NetWitness Investigate. The Investigate view has six submenus, which open different views that allow you to analyze events from different perspectives. The submenus are: Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis.

Workflow

The figure below depicts the high-level tasks that you can perform in the Investigate view.



You can use the submenu options to move between the different views.

- The Navigate view, Events view, and Event Analysis view offer linkages to each other to look at the current results from a different perspective, which provides some continuity for the investigation as you move between views.
- The Hosts view and Files view integrate NetWitness Endpoint into Investigate, and provide a view of all hosts with a NetWitness Endpoint agent installed and a view of unique executable files found in the deployed environment.
- The Users view provides visibility into risky user behaviors across your enterprise using NetWitness UEBA. You can view a list of high-risk users and a summary of the top alerts for risky behavior for

your environment, and then select a user or an alert and view details about the risky behavior and a timeline during which the behaviors occurred.

- The Malware Analysis view provides the ability to scan files found in one of the other views or collected by continuous scanning of network traffic.

When you find an event or file of interest, you can perform different actions to continue the investigation on a deeper level: reconstruct and analyze events, export events and files, perform lookups with internal and external resources, and create incidents and alerts.

What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	browse event metadata	Begin an Investigation in the Navigate or Events View
Threat Hunter	browse raw events	Begin an Investigation in the Navigate or Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Event Analysis View
Threat Hunter	investigate endpoints (Version 11.1 and later)	*NetWitness Endpoint User Guide*
Threat Hunter	find suspicious endpoint files (Version 11.1 and later)	*NetWitness Endpoint User Guide*
Threat Hunter	find risky user behaviors	*NetWitness UEBA User Guide*
Threat Hunter	scan files and events for malware	*Malware Analysis User Guide*

Related Topics

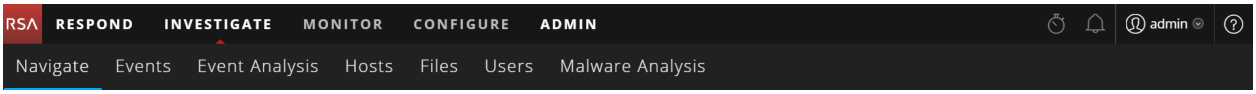
- How NetWitness Investigate Works
- Beginning an Investigation
- Configuring NetWitness Investigate Views and Preferences
- Navigate View
- Events View
- Event Analysis View
- *NetWitness Investigate Quick Start Guide*
- *NetWitness Endpoint Quick Start Guide*

- *NetWitness UEBA Quick Start Guide*
- *Malware Analysis User Guide*

Quick Look

The Investigate view consists of six views, each representing a different approach to analyzing data. By default, Investigate opens to the Navigate view. You can change the default view to one of the other views as described in Configuring NetWitness Investigate Views and Preferences. See How NetWitness Investigate Works for an introduction to the uses for each view. The following figure illustrates the submenus under INVESTIGATE.

Note: The Event Analysis, Hosts, and Files submenus are available in Version 11.1 and later. The Users menu is available in Version 11.2 and later. Configured permissions per user role and user determine which submenus are displayed.

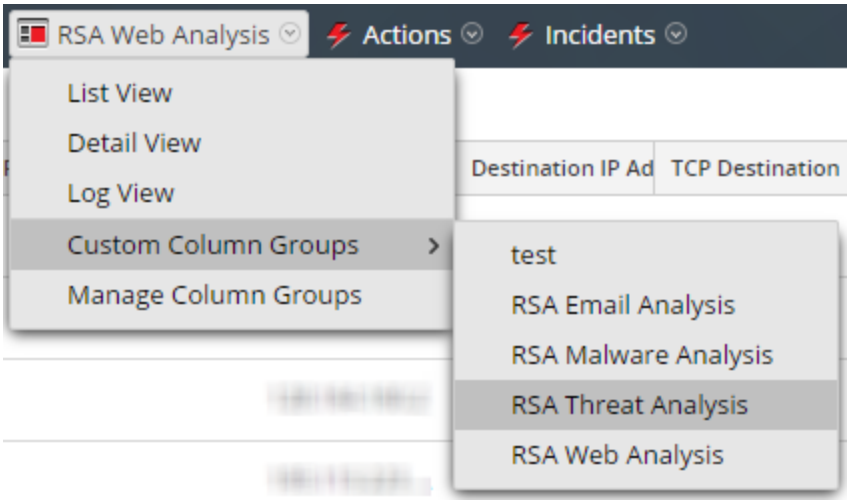


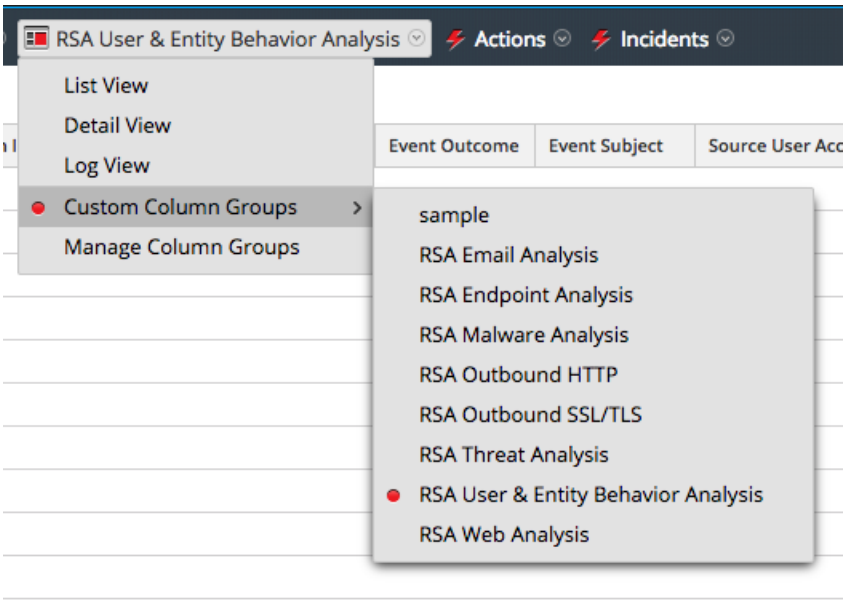
Manage Column Groups Dialog

Column groups allow you to customize the way list data is displayed in Navigate, Events, and Event Analysis views. You can define column groups in the Manage Column Groups dialog, which is accessible in the Events view (see Manage Meta Groups). The column group definition includes the meta keys to use as column titles, the position of the column in the list, and the default width of the column. You can add, delete, import, export, and edit column groups. At fresh installation, out-of-the-box (OOTB) column groups are available for use in the Manage Column Groups dialog. The OOTB column groups are prefixed with RSA and can be duplicated but cannot be edited or deleted. You can also create custom column groups.

After column groups are defined in the Manage Column Groups dialog you can use them in other Investigate views. In the Navigate view, Profiles allow you to select a column group to use when the profile is applied. In the Event Analysis view, you can select a column group to apply to the Events panel.

To access this dialog, go to **INVESTIGATE > Events** and in the **View** drop-down list select **Manage Column Groups**. The **View** option is named for the current value, for example, Detail View, List View, Log View, or the currently selected column group.

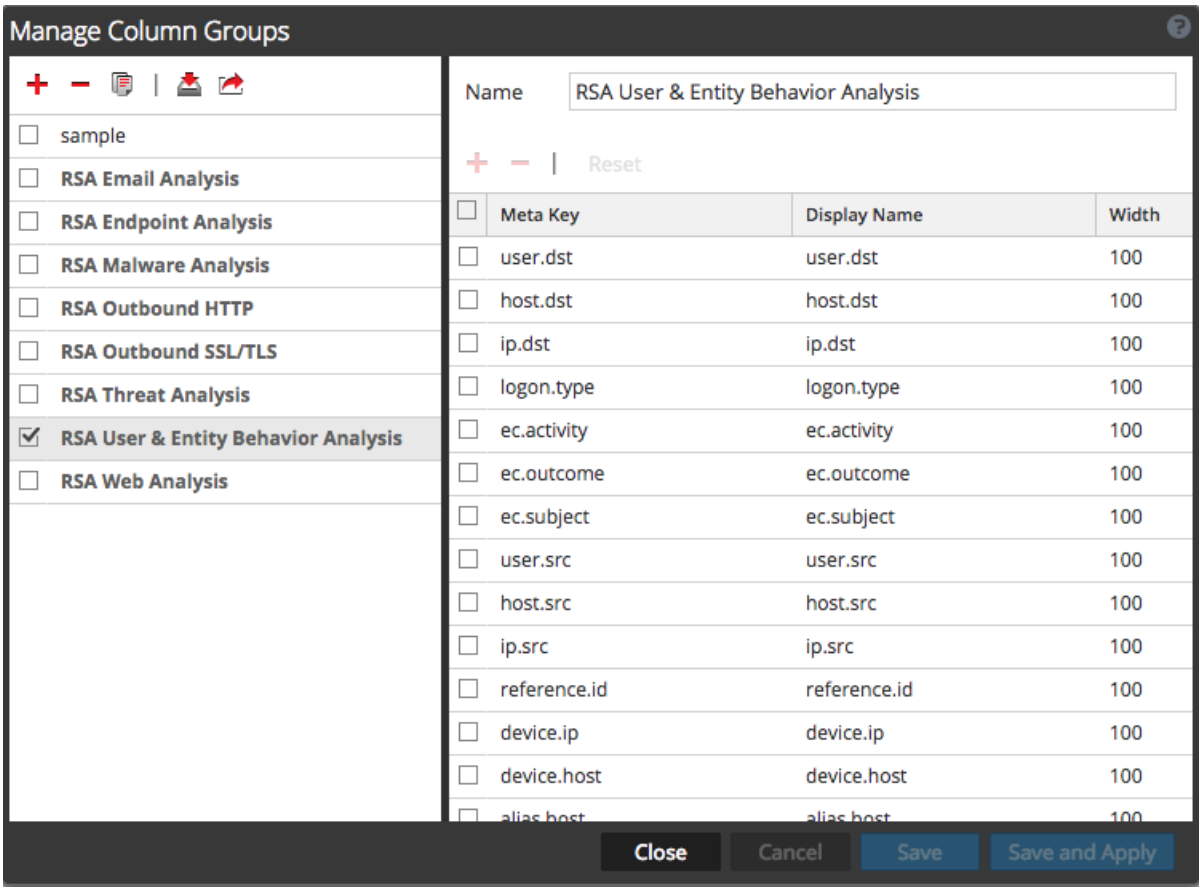




Related Topics

- How NetWitness Investigate Works
- Events View

Quick Look



The Manage Column Groups dialog has two panels: Groups and Settings. At the bottom of this dialog are four buttons: Close, Cancel, Save, and Save and Apply.

The left panel is the Groups panel. This is where you can add, delete, import, or export column groups. At the top of the panel is a toolbar. Below the toolbar is a list of added column groups, where you can select one or more groups.

The following table lists the actions in the toolbar.

Action	Description
+	Adds a column group. Clicking this button highlights the Settings panel on the right, where you can name the column group and add or delete meta keys. At least one meta key is required to add a group.
−	Deletes a column group. A confirmation dialog is displayed before the selected group is deleted. OOTB column groups cannot be deleted.
	Creates a copy of the selected column group.
	Displays the Import Column Groups dialog, where you can select a file to upload.
	Exports one or more selected groups to your local file system.

The right panel is the Settings panel. This is where you can create and edit column groups. This panel contains the Name field, a toolbar, and a list. The following table describes the features of the Settings panel.

Feature	Description
Name	The name of the selected column group.
+	Adds a new row to the list of meta keys, where you can open a drop-down menu to select a new meta key.
−	Deletes one or more selected meta keys. Displays a confirmation dialog before deleting.
Reset	Returns the column group to its most recently saved settings.
Meta Key	Lists the meta keys added to the selected column group.
Display Name	Lists the names of the meta keys as they are displayed in the Navigate, Events, and Event Analysis views.
Width	Specifies the width of each meta key's column. The width can be set between **10** and **1000**. The default width is **100**.

The following table provides descriptions of the action buttons.

Feature	Description
Close	Closes the dialog without saving.
Cancel	Cancels all unsaved changes.
Save	Saves all changes without closing the dialog.
Save and Apply	Saves and applies all changes immediately, closing the dialog.

Manage Default Meta Keys Dialog

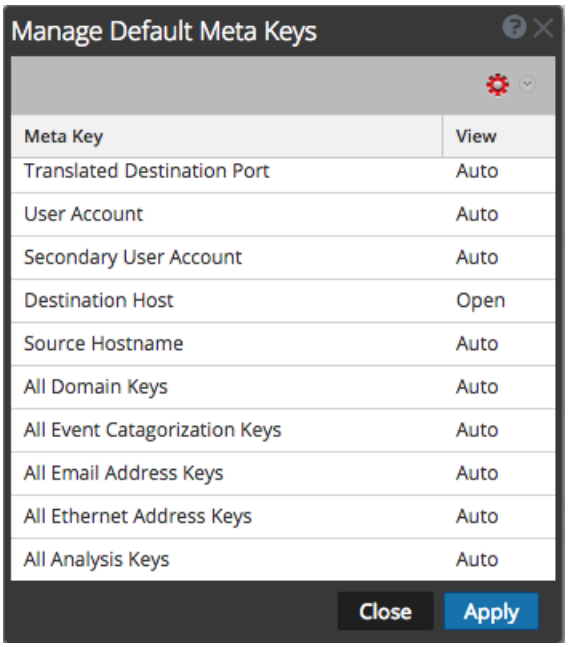
In the Manage Default Meta Keys dialog, analysts can specify the meta keys to be displayed in the Navigate view > Values panel (see Manage and Apply Default Meta Keys in an Investigation. This can help you find the desired data more quickly and prevents the loading of meta keys that are not of interest. To access this dialog, in the **Navigate View** toolbar, select **Meta > Manage Default Meta Keys**.

Related Topics

- Manage Meta Groups
- Manage Meta Groups

Quick Look

The following figure illustrates the Manage Default Meta Keys dialog, which has a list of meta keys, toolbar, Close button, and Apply button. In the list, you can view, sort, and manage default meta keys. If you click and drag meta keys, you can rearrange their order. The following table describes columns in the list.



Column	Description
Meta Key	This column displays the meta keys available for the service. In Version 11.1 and later, default meta entities are also included, for example All Domain Keys and All Email Address Keys.

Column	Description
View	This column displays the type of view assigned to each meta key. By clicking on the view in each row, you can assign the meta key a different default view. There are four views: • Auto: Reverts to the default view for meta keys as specified in the service index file. • Close: The values of this meta key are closed by default, and can be opened manually. • Hidden: These meta keys are hidden by default, and are not shown in Investigation at all. • Open: The values of this meta key are displayed by default. When you modify the default meta keys for a non-indexed meta key, you cannot set the key to **Open**. If you change the default view for a group of meta keys to **Open** and some of the meta keys are non-indexed, the non-indexed meta keys revert to **Auto**. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are **Closed** until opened manually.

The following table describes the toolbar options and buttons.

Feature	Description
	Displays a drop-down menu that allows you change the default view of all the meta keys. There are four views: • Auto: Reverts to the default view for meta keys as specified in the service index file. • Close: The values of this meta key are closed by default. • Hidden: The values of this meta key are hidden by default. • Open: The values of this meta key are displayed by default.
Close	Closes the dialog. Any unsaved changes are lost.
Apply	Applies the changes, and they become effective immediately.

Manage Meta Groups Dialog

In the Investigate > Navigate view, you can use meta groups to filter data displayed in an investigation. A fresh installation of NetWitness Platform includes out-of-the-box (OOTB) meta groups to help you find interesting data sets in Investigate. The OOTB meta groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted. You can create your own groups and you can duplicate and edit an OOTB group to create a custom group. With a meta group in effect during an investigation, the information in the Values panel shows only the meta keys in the selected group. In the Manage Meta Groups dialog, you can add, delete, import, and export meta groups (see Manage and Apply Default Meta Keys in an Investigation).

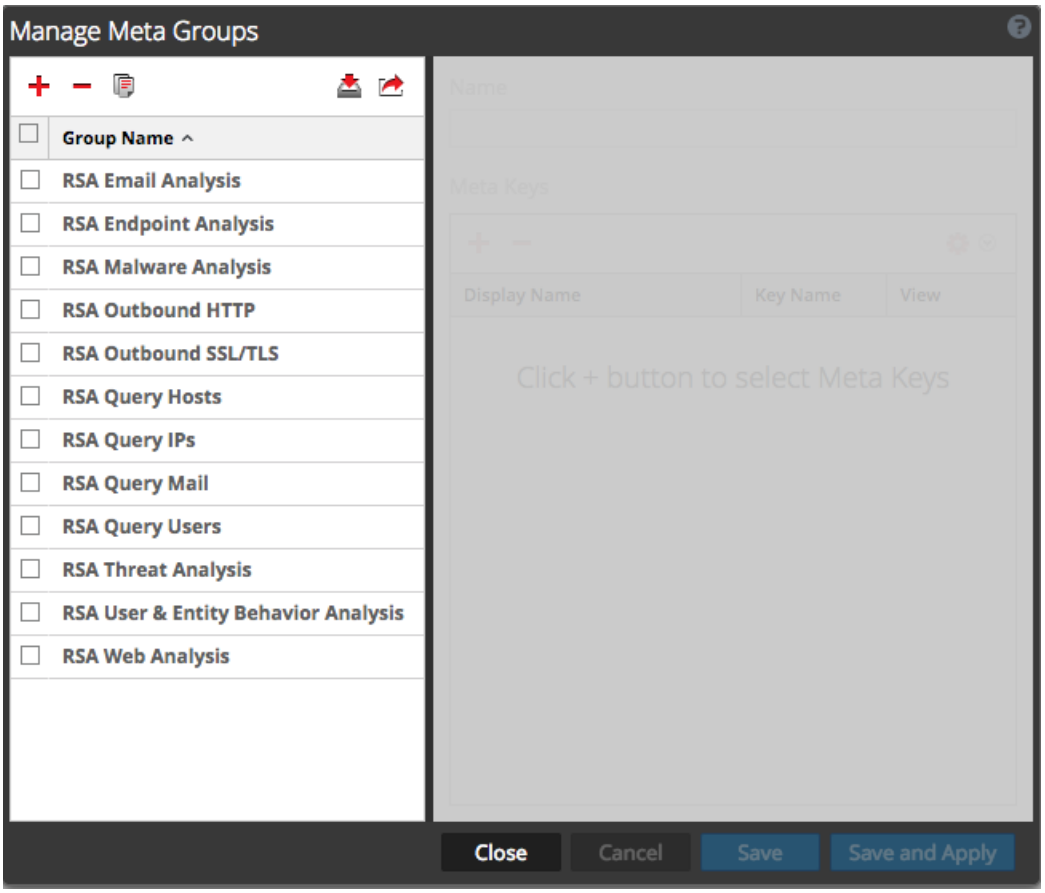
To access this dialog in the **INVESTIGATE > Navigate view** toolbar, select **Meta > Manage Meta Groups**

Related Topics

- Filter Results in the Navigate View
- How NetWitness Investigate Works

Quick Look

The following figure is an example of the Manage Meta Groups dialog.



The Meta Groups panel is on the left side of the Manage Meta Groups dialog. This is where you can add, delete, import, and export meta groups. The following table describes the features of the Meta Groups panel.

Feature	Description
+	Adds a meta group using the Settings panel on the right side of the Manage Meta Groups dialog.
−	Deletes the selected meta group. A confirmation dialog is displayed before the meta group is deleted.
	Creates a copy of the selected meta group.
	Displays the Meta Group Import dialog, where you can upload a file.
	Exports the selected meta group to your computer.
Group Name	Lists all meta group names.

The Settings panel is on the right side of the Manage Meta Groups dialog. This is where you create and edit meta groups. Below the Name field is the Meta Keys list. The following table describes the features of the Settings panel.

Feature	Description
Name	Displays the name of the selected meta group.
+	Displays the Available Meta Keys dialog, where you can select meta keys to add to the group.
−	Deletes the selected meta keys.
	Displays a drop-down menu, where you can select the view for all meta keys. There are four options based on the possible values for the `defaultAction` property used to define a key in the custom index file for the service: • Hidden: These meta keys are hidden by default, and are not shown in Investigation at all. • Open: The values of this meta key are displayed by default. • Close: The values of this meta key are closed by default, and can be opened manually. • Auto: Reverts to the default view for meta keys as specified in the service index file.
Display Name	Indicates the name that is displayed for the key in Investigate views, and is defined by the `description` property for the key in the custom index file for the service..
Key Name	Indicates the `name` of the meta key as defined in the custom index file for the service.

Feature	Description
View	Indicates the view to which the meta key is set. You can change: • Change the view for all meta keys by clicking in the View column header, then selecting a view from the drop-down menu. • Change the view for a single meta key by clicking a single meta key in the View column, then and selecting a view from the drop-down menu.

The following table describes the buttons at the bottom of the dialog.

Feature	Description
Close	Closes the dialog.
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and immediately applies all changes.

Manage Profiles Dialog

Profiles allow you to set up custom views in the Navigate view and the Events view based on a meta group, column group, and limiting query (see Use Profiles to Encapsulate Common Areas for Investigation). You can manage out-of-the-box (OOTB) profiles and custom profiles in the Manage Profiles dialog. In Version 11.2 and later, you can organize profiles into profile groups. In the Manage Profiles dialog, you can configure, add, delete, import, and export profiles and profile groups.

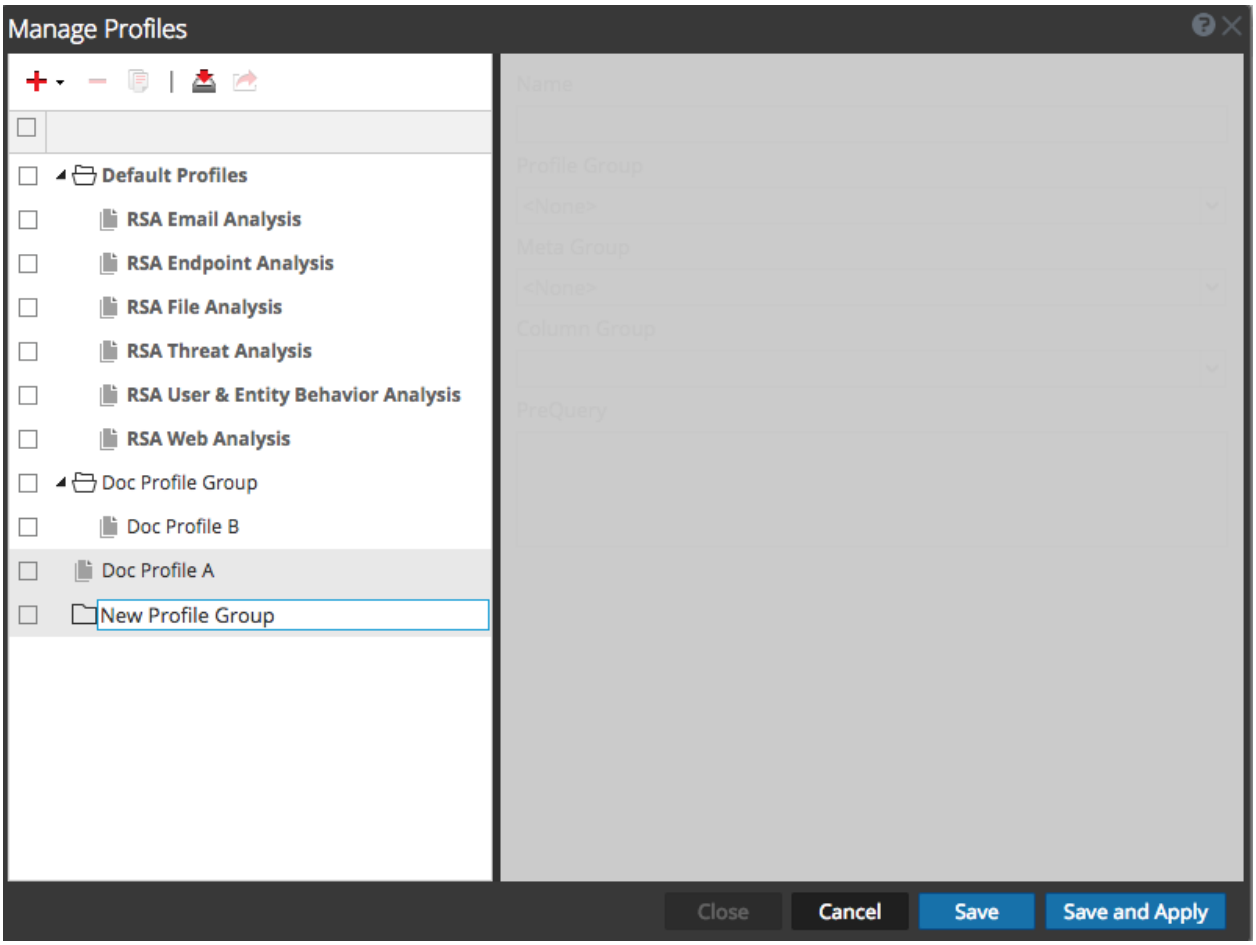
The OOTB profile names begin with the RSA prefix and are grouped under Default Profiles. You cannot edit or delete OOTB profiles, but you can copy an existing profile and edit the copy. To access this dialog, in the **Navigate** or **Events** view toolbar, select **Profile > Manage Profiles** in the **Navigate** or **Events** view toolbar.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

This is an example of the Manage Profiles dialog showing several profile groups.



The Profile panel on the left side of the dialog displays available profiles and allows you to add, delete, import, and export profiles. The following table describes the fields in the Profile panel.

Field	Description
+	Adds a new profile using the Settings panel on the right side of the Manage Profiles dialog.
−	Deletes the selected profile. A confirmation dialog is displayed before the profile is deleted.
	Creates a copy of the selected profile.
	Displays the Profile Import dialog, where you can upload a file.
	Exports the selected profile to your computer.
Profile Name	Lists all profile names.

The Settings panel on the right side of the dialog offers options to configure profiles. It can only be used when one profile is selected. The following table describes the fields in the Settings panel.

Feature	Description
Name	Displays the name of the profile.
Meta Group	Displays a drop-down menu listing available meta groups.
Column Group	Displays a drop-down menu listing available column groups. The OOTB column groups and these three groups are available by default: • List View • Detail View • Log View
PreQuery	Defines a limiting query for filtering Investigate results. This query is used when the associated profile is activated and the preQuery applies to any queries used in the Investigation Navigate and Events views. This is an example of a preQuery: `'service=80,25,110'`.

The following table describes the buttons.

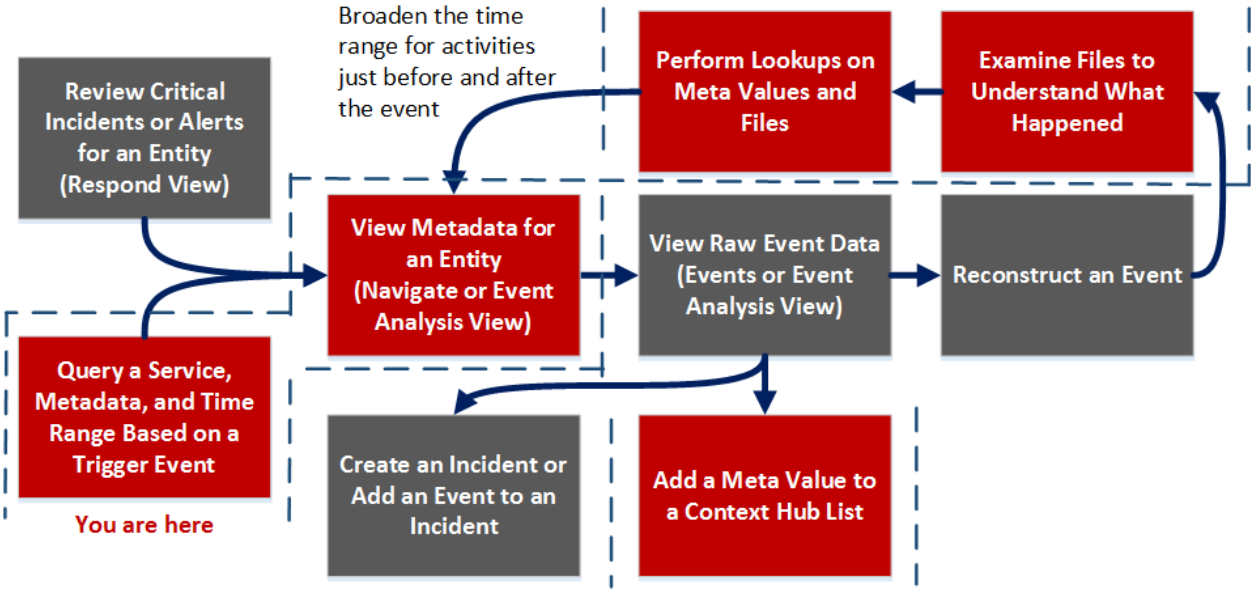
Field	Description
Close	Closes the dialog.
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and applies all changes immediately.

Navigate View

The Navigate view (**INVESTIGATE** > Navigate) displays event metadata--the meta keys and meta values-- that were found in captured data for the selected service. The data is filtered and displayed in accordance with the options you set for profile, time range, meta group, and query. You can also drill into the data by clicking meta keys and meta values. The Navigate view is the default entry point to NetWitness Investigate; you can change the default entry point to one of the other views in the Profile preferences.

Workflow

The figure below depicts the high-level workflow for investigating event metadata.



In the Navigate view, you can:

- View metadata for events in the Values panel.
- Visualize events in a timeline or parallel coordinates chart.
- Save events, go to an event using the event ID, visualize an event, and print an event.
- View additional contextual data for meta keys and values.
- Open a drill point or an event in the Events view or the Event Analysis view.

What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*

User Role	I want to ...	Show me how
Threat Hunter	query a service, metadata, and time range*	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata*	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files*	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups*	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

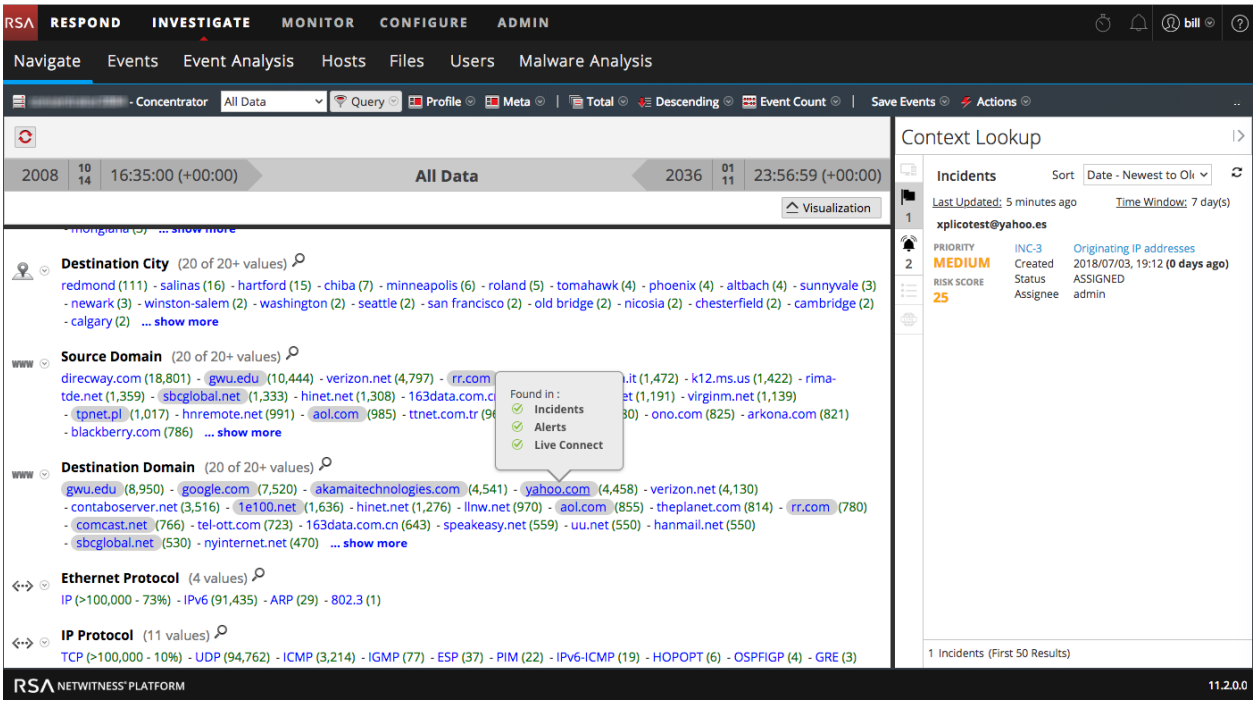
*You can perform this task in the current view.

Related Topics

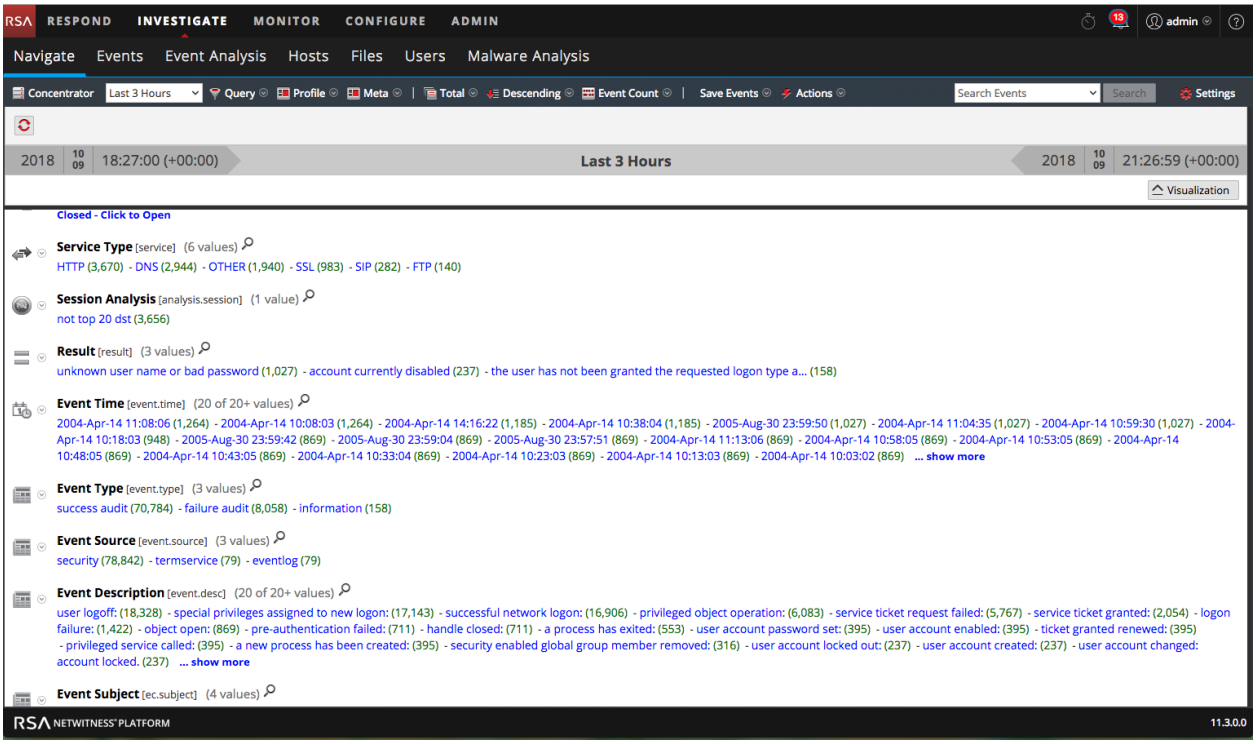
- How NetWitness Investigate Works
- Events View
- Event Analysis View

Quick Look

This figure illustrates the 11.2 Navigate view.



This figure illustrates the 11.3 Navigate view.



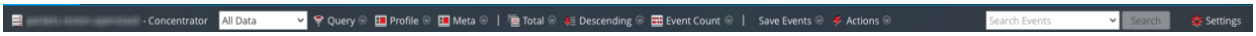
The Navigate view consists of these features:

- Toolbar
- Pause/reload button and breadcrumb
- Time banner
- Optional debug information.
- Collapsible Visualization panel
- Values panel
- Context Lookup panel
- Context menus

Toolbar

The following figure is an example of the toolbar. The toolbar provides a way to:

- Change the service being investigated.
- Control the range of data displayed: You can select use profiles, set a time range, use meta groups, and create queries to apply to the data.
- Set the quantification method and sorting method for data in the Values panel.
- Perform actions on the results. You can export and print results, open an event for which you have an event ID in the Events view or Event Analysis view, and pass a query to Informer.
- Configure Investigate settings without navigating away from the Investigate views.



Some of the toolbar options are labeled with the default value or the selected value rather than displaying the name of the option. For example, the time range option in the example above is labeled **Last 5 Minutes** to reflect the currently selected value. These are the toolbar options.

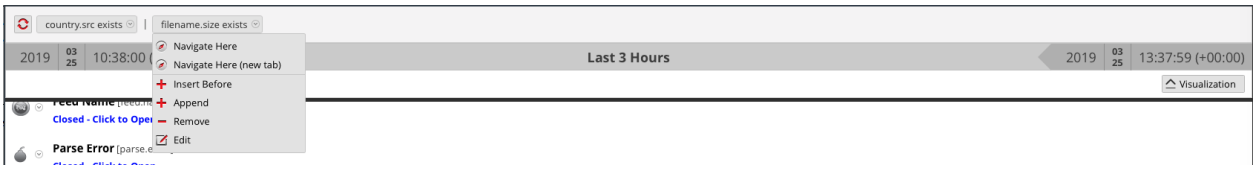
Option	Description
	Displays the selected service name next to the icon. Clicking the icon opens the Investigate a Service dialog, in which you can select a service to investigate and set the default service to investigate (see Begin an Investigation in the Navigate or Events View). Changing the service does not cause a reload of the data.

Option	Description
Time Range	Displays the Time Range options; the currently selected option is displayed in the toolbar (see Filter Results in the Navigate View). Possible choices are: • All Data • Last 5, 10, 15, or 30 Minutes • Last Hour, Last 3, 6, 12, or 24 Hours • Last 2 or 5 Days • Early Morning • Morning • Afternoon • Evening • All Day • Yesterday • This Week • Last Week • Custom **Note:** If you specify custom start or end times in seconds, the value for start time in seconds always defaults to :00, and the value for end time in seconds always defaults to :59. For example, if you are using time to drill down into an issue, the drill time will be interpreted as `HH:MM:00 - HH:MM:59`. Seconds display in this format in Investigate functions.
Query	Displays the Query dialog, in which you can enter a custom query directly instead of drilling down the data. See Query Dialog for a description of the dialog.
Profile	Displays the Profile menu; the currently selected profile is displayed in the toolbar. A profile allows you to manage and use profiles that can include custom meta groups, a default column group, and a beginning query. The Profiles apply to the Navigate view (meta groups and queries) and the Events view (column groups and queries). See Use Profiles to Encapsulate Common Areas for Investigation for more information.
Meta	Displays the Meta Group menu. You can use Default Meta Keys or a custom Meta Group. You also have the option to make changes to both group types (see Manage Meta Groups).
Sort Field	Displays the Sort Field menu; the currently selected option is displayed in the toolbar. The menu has two options: Order by Total and Order by Value. The Sort Field is a complement to the Sort Order option; the data for each meta key is ordered based on the total (green number) or the meta value (blue text) (see Filter Results in the Navigate View).

Option	Description
Sort Order	Displays the Sort Order menu; the currently selected option is displayed in the toolbar. The menu has two options: Sort in Ascending Order and Sort in Descending. The Sort Order is a complement to the Sort Field option; the selected sort field for each meta key is ordered in ascending or descending order (see Filter Results in the Navigate View).
Quantification Method	Displays the Quantification Method menu; the currently selected option is displayed in the toolbar. The Quantification Method only applies to the meta key results in the Values panel. It does not apply to the timeline. The drop-down menu contains three options for calculating the quantity (green number in parentheses) for a meta value: Quantify by Event Count, Quantify by Event Size, and Quantify by Packet Count (see Filter Results in the Navigate View). These are applied differently depending on the type of data in view. For packet data: • Quantify by Event Count shows the number of sessions. • Quantify by Event Size shows the size in bytes. • Quantify by Packet Count shows the number of packets. For log data: • Quantify by Event Count shows the number of logs. • Quantify by Event Size shows the size in bytes. • Quantify by Packet Count shows the number of logs.
Save Events	Displays the Save Events menu, in which you can use options to: extract files associated with an event, export the current drill point as a PCAP file, and export the current drill point as a log file (see Export a Drill Point).
Actions	The Actions menu includes actions that you can perform in the Navigate view (see Investigating Metadata in the Navigate View). In Version 11.1 and later, the options are Visualize, Go to event in Event Reconstruction, Go to event in Event Analysis, and Print).
Search Events	Enables you to search for text patterns within the current set of events. If you click in the Search field, it shows a drop-down menu with search options. If you click Apply, it saves the selected options and also updates the search options in the Events view and the Investigations profile (see Search for Text Patterns).
Settings	Displays the settings for the Navigate view (which are also editable in the Profile view) so that you can change Investigate settings without navigating away from the Navigate view. When you change a setting In the Navigate view the setting is also changed in the Profile view (see Configure the Navigate View and Events View).

Pause/Reload Button and Breadcrumb

The breadcrumb tracks each query as you drill down through the metadata for the service. The following figure is an example of the breadcrumb.



Each query is listed with a drop-down menu in a pipe separated string. The last point is the current point, also called the tip. The icon in front of the breadcrumb allows you to pause the loading of meta values and to reload meta values. The breadcrumb does not include the service name and appears only if a query is in effect. If too many drill points exist for display, the overflow is shown as double angle brackets, >>, at the end of the breadcrumb. Each drop-down menu in the breadcrumb is the same, with slight variation based on the position of the crumb.

The following table describes the controls and menu options in the breadcrumb.

Feature	Description
Pause	Pause and Reload button. Controls the loading of data in the view. It has three possible functions: pause loading, continue loading, and reload.
Navigate Here	Opens the selected drill point in the current Values panel.
Navigate Here (new tab)	Opens the selected drill point in a new tab.
Insert Before	Inserts a query before the current drill point. The Create Filter dialog opens and you can define a custom query to insert in the breadcrumb (see Create a Custom Query).
Append	Appends a query after the current drill point. The Create Filter dialog opens and you can define a custom query to append to the end of the breadcrumb (see Create a Custom Query).
Remove	Removes the selected drill point from the breadcrumb.
Edit	Opens the selected drill point in the Create Filter dialog so that you can edit the query.
>>	Clicking the angle brackets displays a drop-down menu of the breadcrumb overflow.

(Optional) Debug Information

If you have activated the Show Debug Information setting and the service you are navigating is a Broker, NetWitness Platform, displays the debug information beneath the breadcrumb.

The debug information is the `where` clause from the current query. The only time there is no `where` clause is when the time range is all data and there are no drill points. If the Broker has at least one aggregate service that is offline, the debug information also lists the offline service.

For example:

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)$$time='2014-05-
04 18:50:00"-"2014-05-09 18:59:59(attachment exists) && (tcp.dstport = '80')
&& (risk.info exists) && time="2014-05-04 18:50:00"-"2014-05-09 18:50:59"
```

In addition, the time taken to load is displayed at the end of each meta key in the Values panel.

Time Banner

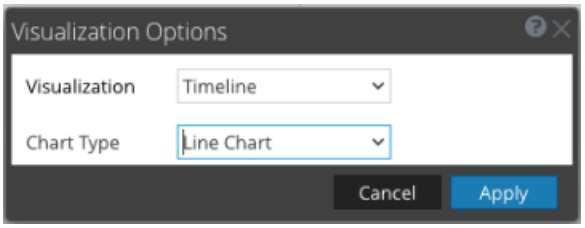
Just below the breadcrumb and debug information (if present), the time banner shows the time range used to create the chart. The following figure is an example of the time banner.

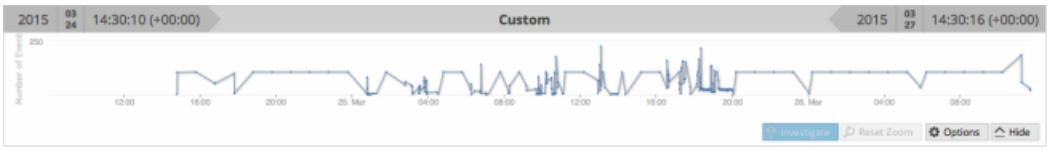
Visualizations

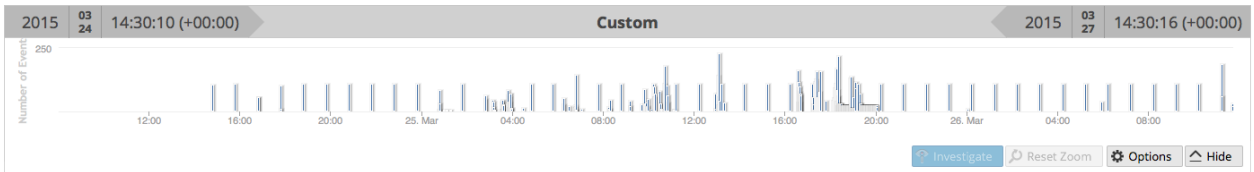
At the top of the Navigate view is a visualization of the current drill point. You can use this to drill into data from the Visualization panel (see Filter Results in the Navigate View). You can show or hide the visualization, and choose one of thevisualization options: Timeline or Coordinates. The Visualization opens initially to the last saved Visualization.

Timeline Chart

The timeline is the count of the number of events that occur at a specific instance. The timeline provides event counts so that you can see if the number of events increases drastically at a given point in time. The timeline displays activity for the specified service and time range as a line chart or a bar chart based on your choice in the Options menu. The second figure illustrates a line chart and third figure illustrates a bar chart.







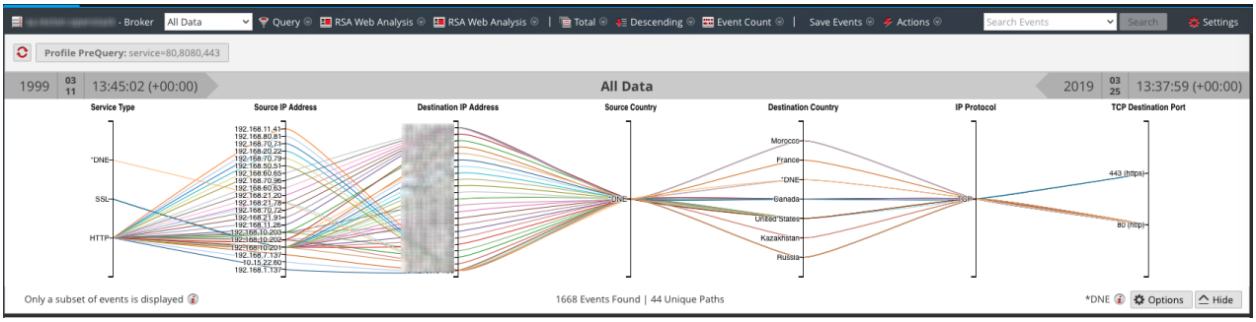
The timeline displays activity for the specified service and time range, as a line chart or a bar chart based on your choice in the Options menu.

Feature	Description
Number of Events (Timeline)	The Y axis of the chart based on thousands of events.

Feature	Description
Time Line (Timeline)	The X axis of the chart based on the time the events occurred.
Event point (Timeline)	If you want to explore a specific section, simply select the range from the chart. The new time range will be reflected in the chart.
Investigate (Timeline)	Displays the meta values for the selected subset.
Reset Zoom (Timeline)	To return to the original time range, click Reset Zoom.
Options	Displays the Visualization Options dialog. Data points can be displayed as a Line chart (default), a Bar chart, or Coordinates chart. When a chart type is select, the relevant options are displayed.
Hide	Collapses the chart.

Parallel Coordinates Chart

The Parallel Coordinates chart is one of the choices in the Options menu for visualizing the current drill point. With Coordinates selected in the Visualization Options dialog, you can select the meta data to be displayed (see Visualize Metadata as Parallel Coordinates). An easy way to view a useful Parallel Coordinates chart is to choose a profile group as shown in the following figure.



Feature	Description
Axes	Each axis is a meta key. The number of meta keys affects the load time for the chart. All meta keys are loaded, but it there the number of events per meta key is limited.
Lines	Lines represent events and they connect values on the axes to show the correlation between multiple meta keys.
Options	Displays the Visualization Options dialog. Data points can be displayed as a Line chart (default), a Bar chart, or Coordinates chart. When a chart type is select, the relevant options are displayed.
Only a subset of events is displayed.	This message is a notification that not all events in the values panel are drawn in the chart. Removing axes or filtering the data in the Values panel can help to display all events.

Feature	Description
Events Found | Unique Paths	Displays the total number of events charted versus the number of unique paths charted. Setting the All Meta Keys Must Exist in an Event option redraws the chart so that it is more targeted and legible.
DNE	Indicates that there is no values for this meta key in the event.

In the Visualization Options dialog for Coordinates, you can select the meta keys to chart.

Feature	Description
Visualization selection	Displays a drop-down list of visualization types: Timeline and Coordinates
All Meta Keys Must Exist in an Event	Limits the data represented in the visualization to only those events that include all selected meta keys. This can result in a cleaner, more targeted visualization.
	Displays the Add Keys to Parallel Coordinates Visualization dialog so that you can add axes to the visualization. This is useful if you are looking for relationships between the default meta keys and some additional ones.
	Deletes the selected keys so that they do not appear as axes in the visualization. This can help to make the visualization less cluttered and allow for more data points to be included in the visualization.
	Reverts to the default meta keys for visualization, which consist of all meta keys in the current drill point.
	Controls the display of additional information about the number of selected axes versus the recommended count. This helps to make you aware of possible performance improvements by removing axes.
Axes	Lists the meta keys selected as axes in the visualization.
Cancel	Cancels any changes made to the visualization options.
Apply	Saves the changes made to the visualization options and applies to the current visualization.

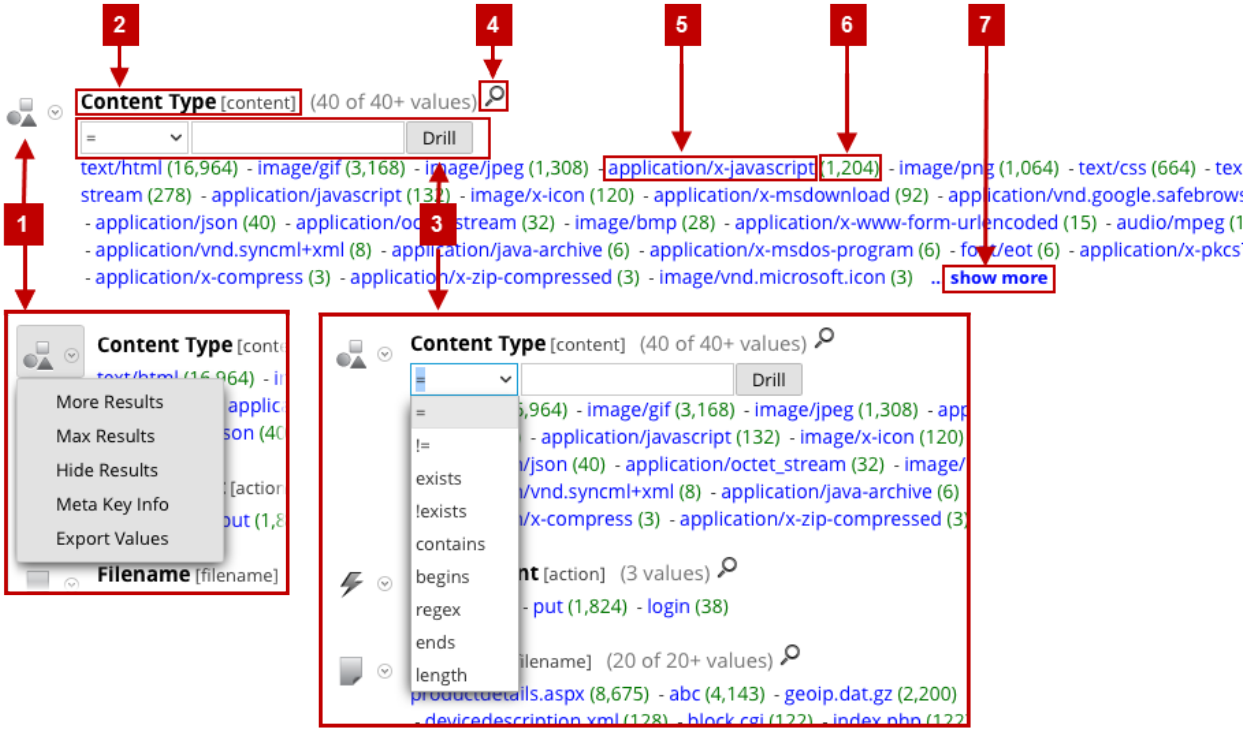
In the Add Keys to Parallel Coordinates Visualization dialog, you can select the meta keys or meta groups to use as axes the Parallel Coordinates visualization.

Feature	Description
Visualization selection	Select Keys: Two options for selecting meta keys are: • From Default Meta Keys • From Meta Groups Each option offers a drop-down list from which to select.

Feature	Description
With the Selected Meta Keys...	The options for the method of adding meta keys allow you to: • Replace the current list of keys • Append to the current list of keys • Insert at beginning of the current list of keys
Cancel	Closes the dialog and does not add any keys.
Add	Closes the dialog and adds the selected keys as specified.

Values Panel

The major feature of the Navigate view is the Values panel, which presents meta keys and meta values found in the service being investigated. Procedures for analyzing data in the Values panel are provided in Filter Results in the Navigate View.



Note: Title, values, and counts for non-indexed meta keys are not drillable; the Values and counts are shown in black.

1 The meta keys in the Values panel have drop-down menus, which offer actions that can apply to that meta key. You can use these to change the way the results for the meta key are displayed in the current view. Changes made to meta keys are displayed in the current view and persist until you refresh the page or select a new service in the Navigate view

	toolbar. See Drill into Data in the Values Panel Refresh reverts to the current view of meta keys as defined in the Manage Default Meta Keys dialog (see Manage and Apply Default Meta Keys in an Investigation). If you have never made modifications in the Manage Default Meta Keys dialog, NetWitness Platform, a refresh restores the default meta keys from the core service. • More Results • Max Results • Hide Results • Meta Key Info • Export Value
2	The name of the meta key for which values are listed. In Version 11.3 and later, the user friendly name of the meta key is displayed with the index file name of the meta key following in brackets. For example **Content Type [content]** gives the user friendly name of the `content` meta key with the index file name in parentheses. For meta groups, the name of the group is given in plain English with the meta group name following in parentheses. This is an example of a meta group name as it would appear in the Values panel: **All User Keys [users.all]**.
3 and 4	Clicking 🔍 on an indexed meta key opens the Search dialog in which you can enter a filter for the current meta key. The search function is not available for non-indexed meta keys, and is based on the actual meta value rather than the alias. Drilling in the Search dialog using aliases is not supported. NOTE: Check with your administrator to obtain a list of aliases used for a meta key in Investigation. When an alias is used, this search dialog does not provide results. Instead, you must query the meta key using the Right-click query capability or the Query dialog.
5	The meta value associated with the found meta key. These are listed in order by meta value name or by the count of events in which the meta value was found, according to your preference.
6	The number of events that include the meta value.
7	The number or values rendered is specified by the Render Threads value in the Investigation Preference settings. In the example above, the meta key is **Content Type**, and 40 of 40+ values are currently displayed. You can display additional values by clicking **...show more**. The number of instances found for a particular meta in the session.

Values Panel Loading Behavior

The default view is for the last 3 hours of collection, using the default meta keys and non-indexed meta keys closed. The meta keys within the meta groups are displayed in the order that NetWitness Platform queries the keys. As the data loads into the Values panel, NetWitness Platform is optimized to show partial results, loading progress, and service status as the data loads.

The loading behavior is determined by several configuration settings. The highest level settings are configured by the administrator for each user. These are:

- The maximum amount of time allowed for this user to run a query (Query Timeout).
- The limit at which NetWitness Platform stops counting the number of meta values in a session (Session Threshold). If a threshold is set for a session, the Navigate view shows that the threshold

was reached and the percentage of results loaded. Any session that does not show a percentage is accurate and was processed to completion. If there is a percentage, that reflects how much processing was completed. The percentage displayed is estimated by extrapolating from the value at the time processing finished, considering the amount of work remaining. Larger percentages are generally more accurate because they require less extrapolating

- The limit at which NetWitness Platform stops counting the number of meta values in a session (Session Threshold). If a threshold is set for a session, the Navigate view shows that the threshold was reached and the percentage of query time used to reach the threshold.

Note: The values for non-indexed meta keys take longer to load in the Values panel. To optimize loading, NetWitness Platform does not open non-indexed meta keys by default. Refer to Manage and Apply Default Meta Keys in an Investigation for a detailed description of non-indexed meta keys in Investigation.

When you have launched an investigation of a service, NetWitness Platform displays results in the Values panel.

1. NetWitness Platform loads meta keys and meta values in the Values panel. For each meta key load, the stages of load are:
   a. **Waiting to Be Loaded** or **Closed**. If Closed, no data for that key is loaded.
   b. **Loading**
      i. **Loading progress**: NetWitness Platform is receiving and displaying progress messages.
      ii. **Partial results**: NetWitness Platform is receiving values messages and partial results are displayed in the Values panel.
   c. **Load Complete**: All results are finished loading.
2. As each meta key load is completed, and final values are displayed, the next meta key is started. The number or values rendered for each meta key is specified by the Render Threads value in the Investigation Preference settings. Loading continues until all keys to be loaded have finished.
3. If **Show Debug Information** is active and the service you are navigating is a 10.4 or later Broker, NetWitness Platform displays load time information beneath the values for each meta key and displays additional load details for the aggregated services. NetWitness Platform also displays the debug information beneath the breadcrumb.

Iterative results

Iterative results provide feedback on the status of queries within the interfaces to provide additional context for how long the data load will take and if any service data is missing. For example, if you are querying a Broker that is aggregating from two Concentrators, NetWitness Platform starts displaying the results from the first Concentrator as soon as it is available, even if the second Concentrator is still waiting for results.

Iterative results also include a notification that service data is missing because the service is unreachable.

Partial results

When partial values from the Core service are returned but not completed, a message at the end of the meta key listing shows the progress of values loaded. For example, Currently looking at 38 ip.src values 71% indicates that loading of values for the meta key is 71% complete.

Debug Information

If the Show Debug Information setting is in effect, a field at the end of the values displays the status for the different systems against which you are querying within NetWitness Platform. For example, when you are querying against a 10.4 broker pulling from multiple concentrators, NetWitness Platform displays the status of the query on each of the Concentrators, which provides insight into the relative speed of data loading from each of the Concentrators. Each service that participated in the query is listed with the total elapsed time for the query.

Each service that participated in the query is listed with the total elasped time for the query. In the example above, two services returned in 3.207 seconds, localhost:50005 took 2 seconds to return the results. In addition, the where clause of the query is displayed below the breadcrumb. You can copy this syntax directly into an application rule or Reporting where clause of a rule.

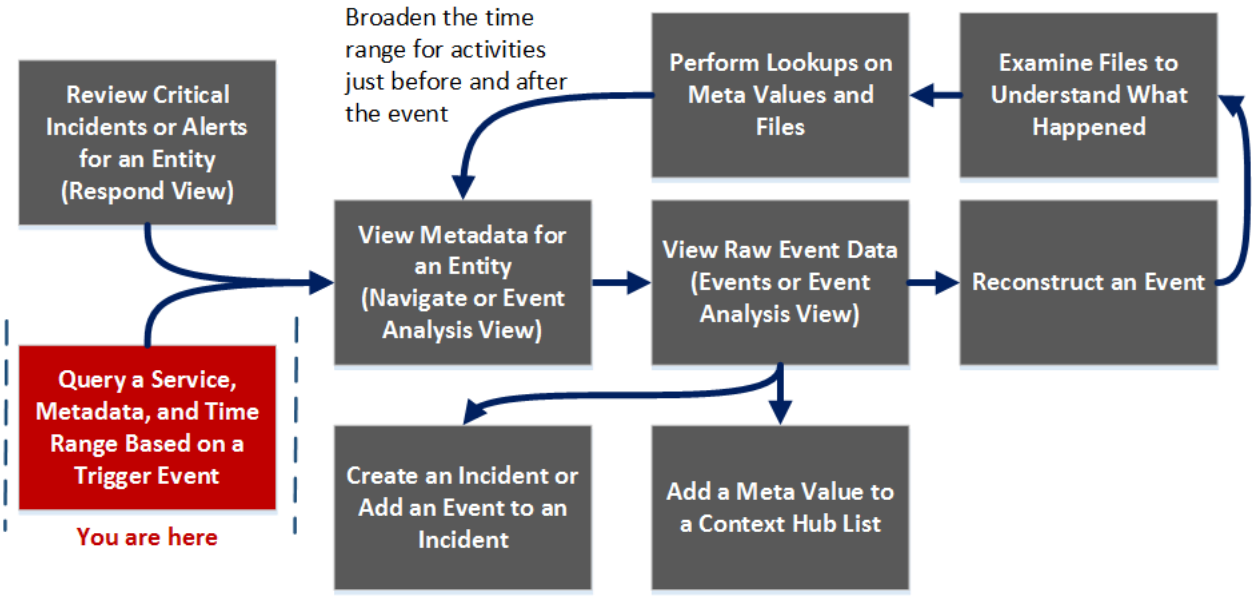
Load Complete

For each meta key, there is a list of values (blue text) and counts (green text) found in the current drill point. When you click a value to drill down into a subset of the currently selected data, the display is updated and the new drill point is recorded in the breadcrumb. You can specify the sorting and quantification methods for the values list using the option in the toolbar.

Query Dialog

In the Navigate view or Events view, you can create a query rather than clicking through the meta keys and values to drill down into the meta data. The dialogs for creating a query offer syntax help with drop-down lists of applicable meta keys and operators. To access this dialog in the **Navigate** or **Events** view toolbar, select **Query**.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Incident Responder	review critical incidents or alerts	*NetWitness Respond User Guide*
Threat Hunter	query a service, metadata, and time range*	Filter Results in the Event Analysis View Filter Results in the Navigate View Create a Custom Query Filter and Search Results in the Events View
Threat Hunter	view metadata	Examine Events in the Event Analysis View Investigating Metadata in the Navigate View
Threat Hunter	view raw event data	Examine Events in the Event Analysis View Examine Events in the Event Analysis View Examining Raw Events in the Events View

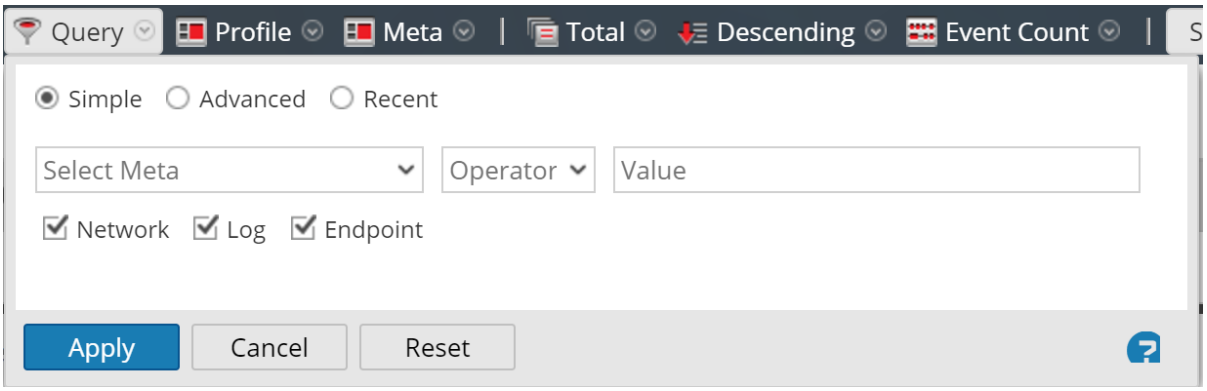
User Role	I want to ...	Show me how
Threat Hunter	reconstruct the event	Examine Events in the Event Analysis View Reconstruction Types in the Event Analysis View Reconstruct an Event
Threat Hunter	examine files	Download Data in the Event Analysis View Reconstruct an Event
Threat Hunter	perform lookups	Act on Data in the Event Analysis View Look Up Additional Context in the Event Analysis View Launch an External Lookup of a Meta Key Look Up Additional Context for a Data Point
Threat Hunter	create an incident or add to an incident	Add Events to an Incident for Response
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context in the Event Analysis View Look Up Additional Context for a Data Point Manage Context Hub Lists and List Values in the Navigate and Events Views

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View

Quick Look

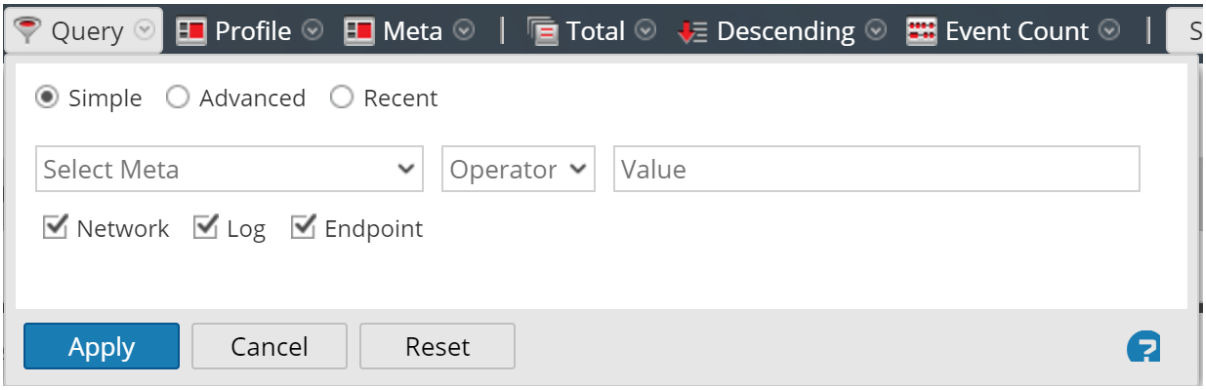


The Query dialog has three views:

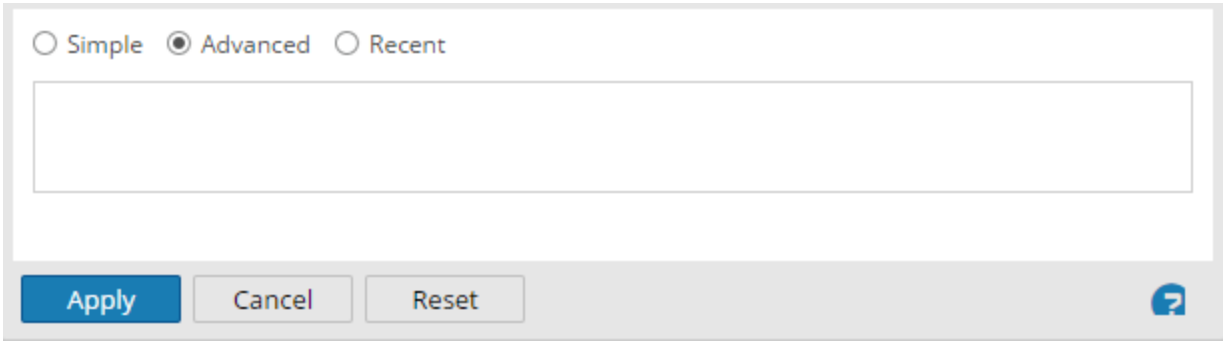
- Simple
- Advanced
- Recent

In the Simple view, you can create a query using the options displayed in the dialog. In the Advanced view, you can create a query without guidance. In the Recent view, you can select a query from a drop-down list of recent queries.

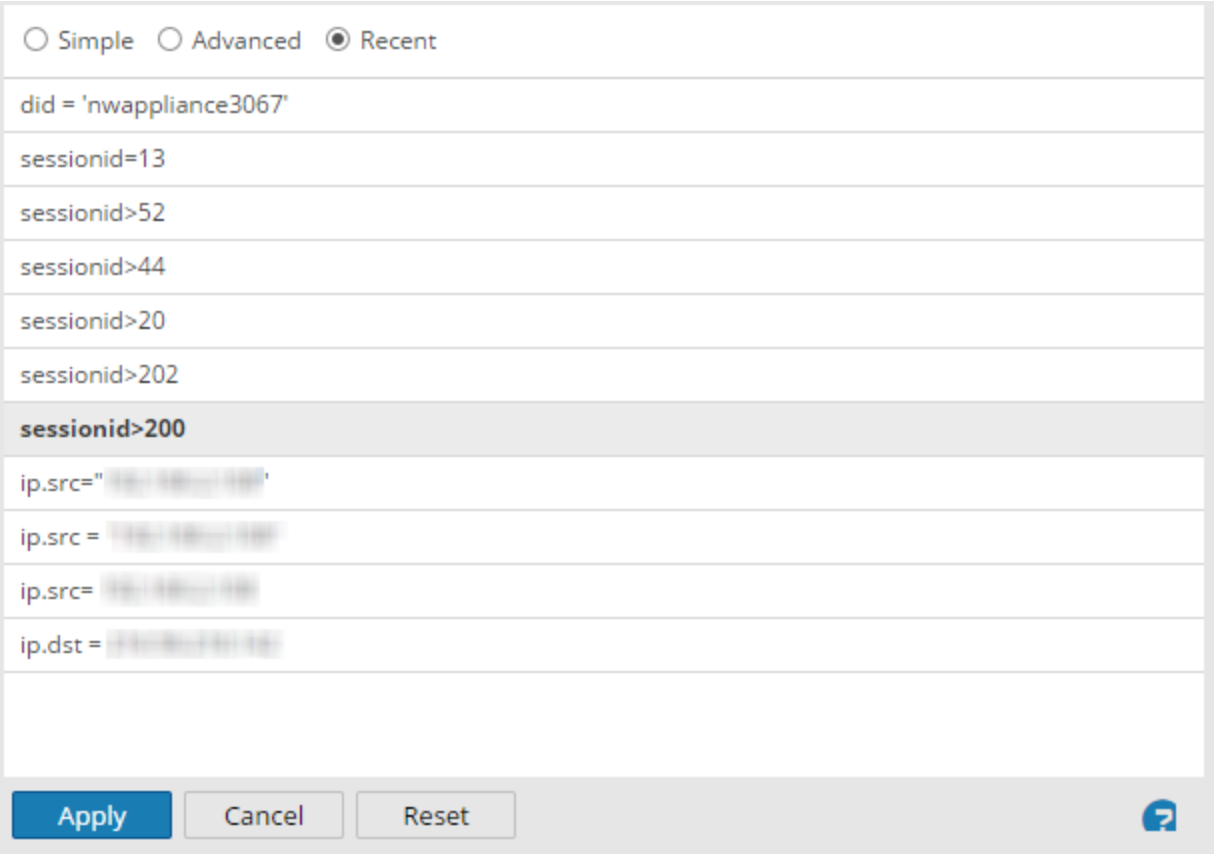
Simple View



Advanced View



Recent View



The following table describes features of the Query dialogs.

Feature	Description
Select Meta	Displays a drop-down list of meta groups.
Operator	Displays a drop-down list of operators (=,NetWitness Platform!=,NetWitness Platformexists,NetWitness Platform!exists)
Value	Allows you to enter a value to complete the query.
Network	Limits the query to packets if Log is not selected.
Log	Limits the query to logs if Network is not selected.
Query box	Allows you to enter a query in the Advanced view. When you begin typing, a drop-down list of available meta keys for the service is displayed, then a drop-down of operators is displayed as you type. If the expression currently entered in the query box is invalid, a warning appears near the box. When the query is valid, the warning is removed.
Query list	Allows you to select a query from a list of recent queries in the Recent view. Double-clicking a query automatically applies it.

Feature	Description
Apply	Applies the new query to the current Investigation view.
Cancel	Closes the dialog without applying changes.
Reset	Resets all fields.

Settings Dialogs for Investigate Views

NetWitness PlatformVersion 11.0 has two settings dialogs, one for the Navigate view and one for the Events view. With the addition of the settings dialog for the Event Analysis view in Version 11.1, Investigate has three settings dialogs.

The settings in the Navigate view and Events view Settings dialogs are a subset of the Investigation settings made in the Profiles > Preferences panel > Investigations tab. Analysts can save time by editing these settings within the Investigate view. If you change a setting here, the same setting is changed in the Profiles view, and if you change a setting in the Profiles view, the same setting is changed here.

To access this dialog, go to the **Navigate** or **Events** view, and select the **Settings** option in the toolbar.

The settings in the Event Analysis view have no corresponding settings in the Profiles > Preferences panel.

Related Topics

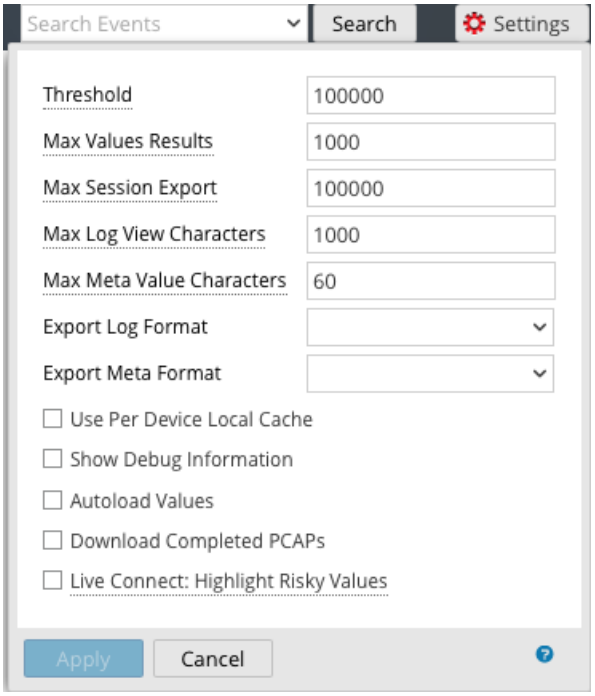
- How NetWitness Investigate Works

Quick Look

This is a quick look at the settings dialog for the Navigate view, Events view, and Event Analysis view.

Navigate View Settings Dialog

The following figure illustrates the Navigate view Settings dialog. The settings that influence performance when loading values in the Values panel have default values based on common usage, and individual analysts can adjust these settings for their own investigations. The following table describes the features.

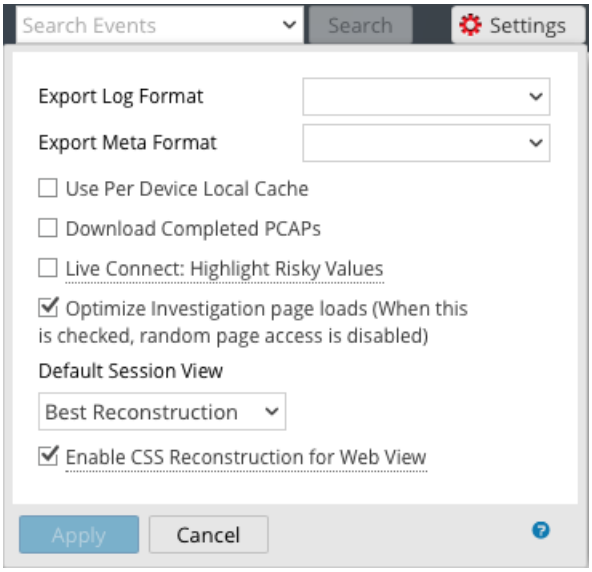


Feature	Description
Threshold	Sets the threshold for the maximum number of sessions loaded for a meta key value in the Values panel. A higher threshold allows accurate counts for a value, and also causes longer load times. The default value is **100000**.
Max Values Results	Sets the maximum number of values to load in the Navigate view when the Max Results option is selected in the Meta Key menu for an open meta key. The default value is **1000**.
Max Session Export	Sets the maximum number of sessions that can be exported. The default value is **100000**.
Export Log Format	Sets the file format of exported logs. There are four formats available: • **Text**: Raw log format. • **SML**: Structured Markup Language format. • **CSV**: Comma-separated values (CSV) format. • **JSON**: The JavaScript Object Notation (JSON) format.
Export Meta Format	Sets the file format of exported meta values. There are four formats available: • **Text**: Raw log format. • **SML**: Structured Markup Language format. • **CSV**: Comma-separated values (CSV) format. • **JSON**: The JavaScript Object Notation (JSON) format.
Use Per Device Local Cache	When the checkbox is cleared, Investigate sends a fresh query to the database rather than displaying cached data in the Investigate views after the initial load. If the checkbox is selected, Investigate uses the data from local cache.
Show Debug Information	This option controls the display of the `where` clause beneath the breadcrumb in the Navigate view and the elapsed load time for each aggregated service on a Broker. When the checkbox is selected, the debug information is displayed. The default value is **Off** (checkbox cleared).
Autoload Values	This option controls automatic loading of values for the selected service in the Navigate view. When the checkbox is selected, values are automatically loaded when you select a service to investigate. When the checkbox is cleared, Investigate displays a **Load Values** button, allowing the opportunity to modify options. The default value is **Off**.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in Investigate so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP form. When the checkbox is selected, the option is enabled. The default setting is disabled (checkbox is cleared).

Feature	Description
Live Connect: Highlight Risky IPs	If the checkbox for this option is cleared, all the meta values that have context available in Live Connect are highlighted in the Navigate view Values panel. If the checkbox is selected, among the values that have context in Live Connect, only those values deemed Risky/Suspicious/Unsafe by the community are highlighted. By default this option is disabled (checkbox cleared).
Apply	Applies the settings immediately and they are visible the next time you load values. The same changes are also applied in the Profiles view.
Cancel	Cancels the editing operation and closes the dialog, leaving the settings unchanged.

Events View Settings Dialog

The following figure is an example of the Settings dialog for the Events view, and the table describes the features.

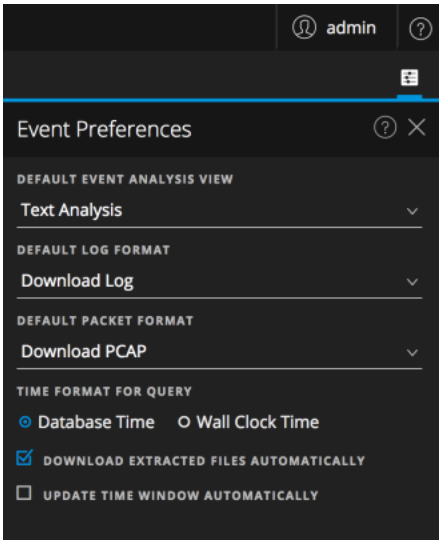


Feature	Description
Export Log Format	Sets the file format of exported logs. There are four formats available: • **Text**: Raw log format. • **SML**: Structured Markup Language format. • **CSV**: Comma-separated values (CSV) format. • **JSON**: The JavaScript Object Notation (JSON) format.

Feature	Description
Export Meta Format	Sets the file format of exported meta values. There are four formats available: • **Text**: Raw log format. • **SML**: Structured Markup Language format. • **CSV**: Comma-separated values (CSV) format. • **JSON**: The JavaScript Object Notation (JSON) format.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in Investigate so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP form.
Live Connect: Highlight Risky IPs	When the checkbox is selected, Investigate uses a filter to fetch only IP addresses that are considered as risky by RSA community. When the checkbox is cleared, NetWitness Platform displays all IP addresses. By default, this option is disabled (checkbox cleared).
Optimize Investigation page loads	Sets a paging option. When optimized, results are returned as quickly as possible, sacrificing the original ability to go to a specific page in the event list. Clearing this checkbox changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). The default value is enabled (checkbox selected).
Append Events in Event Panel	This option affects paging in the Events panel and in prior releases was located in the Navigate view settings dialog. When the checkbox is selected, the next group of events is appended to the already displayed events. When cleared, the previous page of events is replaced by the next page. The default value is Off (checkbox cleared).
Default Session View	Selects the default reconstruction type for the initial reconstruction in the Events view. The default value is **Best Reconstruction** in which events are reconstructed using the reconstruction method most appropriate to the event.
Enable CSS Reconstruction for Web View	This setting controls how web content reconstruction is performed. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for style sheets and images used in the target event. The option is enabled by default. Clear the checkbox to disable this option if there are problems viewing specific websites.
Apply	Applies the settings immediately and they are visible the next time you view events. The same changes are also applied in the Profiles view.
Cancel	Cancels the editing operation and closes the dialog, leaving the settings unchanged.

Event Analysis View Preferences Dialog

Beginning with Version 11.1, the Event Analysis view has user preferences that you can configure in the Event Analysis view > Event Preferences dialog. These settings persist so that they are applied each time you log in and go to the Event Analysis view. The following figure is an example of the dialog, and the table below describes the options.



Feature	Description
Default Event Analysis View	Selects the default event analysis view that is displayed every time you open the Event Analysis view. For example, if you select File Analysis, the File Analysis panel is highlighted and displayed every time you investigate an event in the Event Analysis view. These are following options: • **Text Analysis**: View and analyze the raw text payload of an event. • **Packet Analysis**: View and interactively analyze the packets and payload of an event. • **File Analysis**: View a list of files and download one or more files in an event.
Default Log Format	Selects the default format for downloading logs: • **Download Log**: Raw log (log) format. • **Download CSV**: Comma-separated values (CSV) format. • **Download XML**: The Extensible Markup Language (XML) format. • **Download JSON**: The JavaScript Object Notation (JSON) format.

Feature	Description
Default Packet Format	Selects the default packet format for downloading packets. • **Download PCAP**: To download the entire event as a packet capture (*.pcap) file. • **Download All Payloads**: To download the payload as a *.payload file. • **Download Request Payload**: To download the request payload as a *.payload1 file. • **Download Response Payload**: To download the response payload as a *.payload2 file.
Time Format for Query	The Event Analysis view can display results based on the database time or the current clock time. The default setting for this preference is Database Time, which is the same time format used to display query results in the Navigate view and Events view. When **Database Time** is selected, the start and end time for a query is based on the time that the event was captured (collection time). When **Wall Clock Time** is selected, the query is executed using the end time based on the current browser time; the start time is calculated based on that end time and the time range.
Download Extracted Files Automatically	Enables the automatic download of files if they are in the selected default format in the **Default Log Format** and **Default Packet format** fields set in the Event Preferences dialog. Select the checkbox to enable downloading the selected format automatically to local file system. Otherwise, the download job goes to the job queue, and you can download it manually.
Update Time Window Automatically	(Version 11.3 and later) Enables automatic update of the time range window in the breadcrumb when the service is polled (at one minute intervals) so that fresh results are sent. The default setting is disabled. When the checkbox is selected, as the time range is updated, the (Submit Query) button is activated so you can click to get the fresh results. When the checkbox is cleared, the automatic update is disabled keeping the time range window in the breadcrumb synchronized with the current results.