RSA NETWITNESS® PLATFORM

NetWitness Investigate User Guide

for RSA NetWitness® Platform 11.4

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

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

April 2020

Contents

How NetWitness Investigate Works

NetWitness Investigate provides the data analysis capabilities in RSA NetWitness® Platform. Using Investigate, analysts can examine 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 original packets captured on the network, logs forwarded by a device, and endpoint events seen by the endpoint agent.

The configured rules, parsers, and feeds on the Decoder create *metadata* that analysts can use to investigate the ingested logs, packets, and endpoint data. 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 Broker or 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 about the event without having to query each Decoder. In some special cases, analysts may query a Decoder.

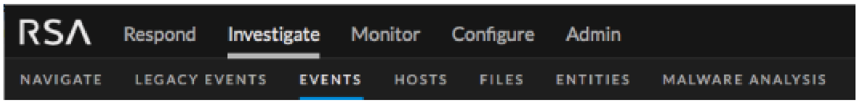
Triggers for an Investigation

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 that your SOC manager 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 Investigate > Entities > Users tab (UEBA) you can filter for that username to make sure there is no longer any activity for that user and see if that user deviated from their typical behavior prior to being let go.
- A phishing attack detected has an associated attachment, and you want to know what devices in your environment have seen that file by searching for the file hash in Investigate > Files.
- A malicious file has been automatically found in your environment, and you want to review the static and dynamic analysis done on that file along with how many systems it has been transmitted to or from. Starting in Investigate > Malware Analysis you can see the analysis results.

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 Legacy Events view, the Hosts view, the Files view, the Entities 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 11.3; the name in Version 11.4 changed to Entitites view.
- The Legacy Events view is disabled by default in Version 11.4, but can be enabled by an administrator as described in the *System Configuration Guide*.
- Specific user roles and permissions are required for a user to conduct investigations and malware analysis in NetWitness Platform. If you cannot see a view, the administrator may need to adjust the roles and permissions configured for you.

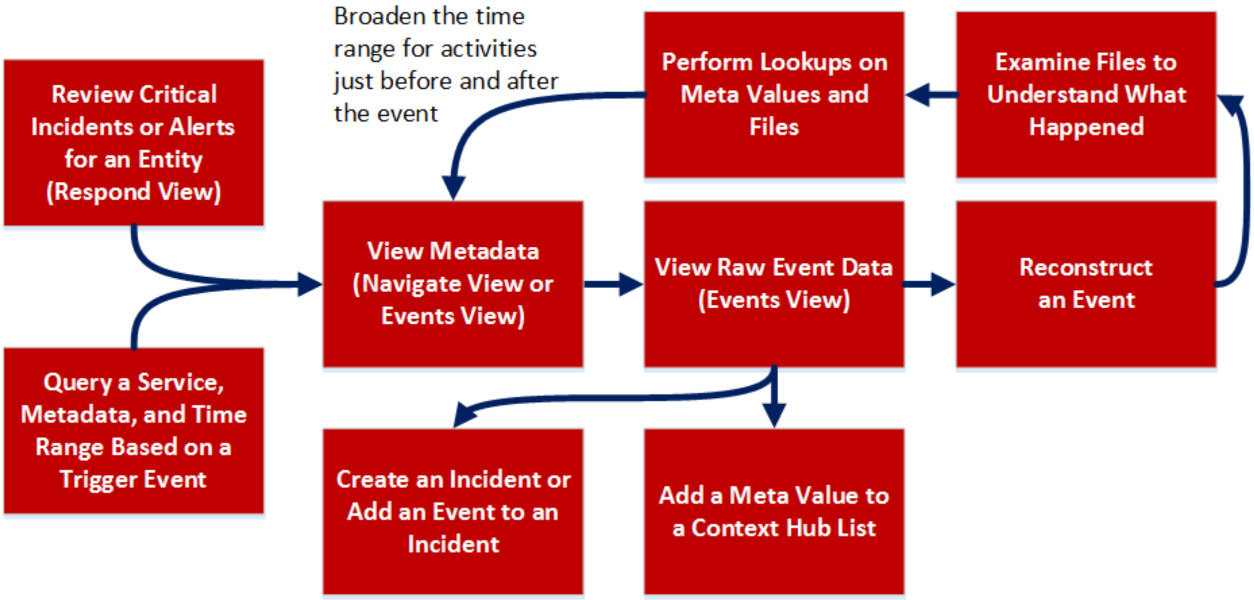
You can access each view from the Investigate submenu and from other Investigate views. You can also go directly into an Investigate view from NetWitness Respond, and go directly from NetWitness Investigate to NetWitness Respond and to standalone NetWitness Endpoint. The use case determines the starting point for your investigation. Every situation is unique in terms of the types of information you are attempting to find. Many investigations start in one view, and end in a different view as you learn something and then need to follow that result to a different line of questioning. The following table provides general guidance on the starting view for different use cases.

Go to...	Focus
Navigate view	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 look up in Malware Analysis or Live. This is the default Investigate view. (See Refining the Results Set and Downloading and Acting Upon Results.)
Events view	The default workflow for analysts interacting with events is optimized to limit the need to transition from one view to another. With major functionality added to the 11.3 Event Analysis view, it has become the default Events view. Events in the Events view are listed in order by time. You can view the raw event and related metadata, sort and search the list, view a reconstruction that offers helpful cues to identify points of interest in a reconstruction (interesting bytes, file types, and encoded data), and download events and files. You can pivot to standalone Endpoint, look up in Live, do other internal lookups, 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 Refining the Results Set, Reconstructing and Analyzing Events, and Downloading and Acting Upon Results.)
Legacy Events view	The Legacy Events view was the original Events view (11.0 to 11.3.x.x). The Legacy Events is no longer needed and it is hidden unless the administrator enables it. By default only the Events view appears in the menu, but when the Legacy Events view is enabled, both the Events view and the Legacy Events view are visible in the menu bar. You can view the raw event and related metadata, view a reconstruction, and download events and files. (See Refining the Results Set, Reconstructing and Analyzing Events, and Downloading and Acting Upon Results.)
Hosts view	Hosts on which the NetWitness Endpoint 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 pivot to the Navigate, Events, and Entities views. (See the *NetWitness Endpoint User Guide*.)
Files view	Unique files in your deployment, such as PE, Macho, and ELF, 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 Events 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*.)

Go to...	Focus
Entities view	Labeled as the Users view in Version 11.2 and 11.3. 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*.)

Focus on Metadata, Query, and Time

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


Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata (Navigate View or Events View)
View Raw Event Data (Events View)
Reconstruct an Event
Examine Files to Understand What Happened
Perform Lookups on Meta Values and Files
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

Analysts use 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 Legacy Events 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 Events 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 this meta value: `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 Respond View Incidents and Alerts

An analyst who is working on an incident or an alert in Respond can open the incident in 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 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 the Respond view, defined meta keys are queried and the captured packets, logs, and endpoint events are 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.
- From the Incident Details view Indicators panel in Respond, you can open the Events 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 Legacy Events 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:

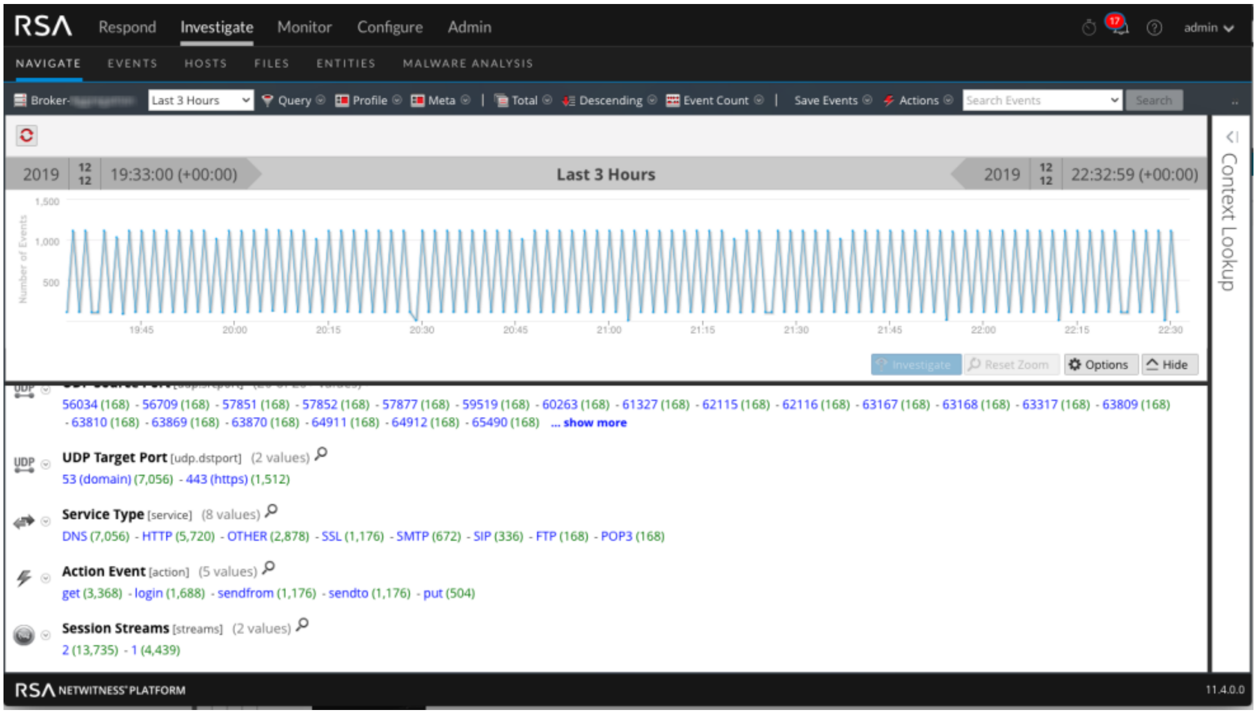
- The *NetWitness Endpoint User Guide* covers features and functions of the Hosts view and Files view.
- The *NetWitness UEBA User Guide* covers features and functions of the Entities (formerly Users) view.
- The *Malware Analysis User Guide* covers features and functions of the Malware Analysis view.

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 and a time range, 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 values, 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. This additional context is retrieved from sources other than the original data providing the analyst further perspective around the event. As an example of context, the associated incidents and alerts convey if this event or a similar one has been seen or previously worked on before. Any lists that match the metadata can help indicate if the metadata relates to a known blacklist of known adversaries or another analysts list of users they have found to be against typical usage policies.
- 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.



56034 (168) - 56709 (168) - 57851 (168) - 57852 (168) - 57877 (168) - 59519 (168) - 60263 (168) - 61327 (168) - 62115 (168) - 62116 (168) - 63167 (168) - 63168 (168) - 63317 (168) - 63809 (168) - 63810 (168) - 63869 (168) - 63870 (168) - 64911 (168) - 64912 (168) - 65490 (168) ... show more

UDP Target Port [udp.dstport] (2 values)
53 (domain) (7,056) - 443 (https) (1,512)

Service Type [service] (8 values)
DNS (7,056) - HTTP (5,720) - OTHER (2,878) - SSL (1,176) - SMTP (672) - SIP (336) - FTP (168) - POP3 (168)

Action Event [action] (5 values)
get (3,368) - login (1,688) - sendfrom (1,176) - sendto (1,176) - put (504)

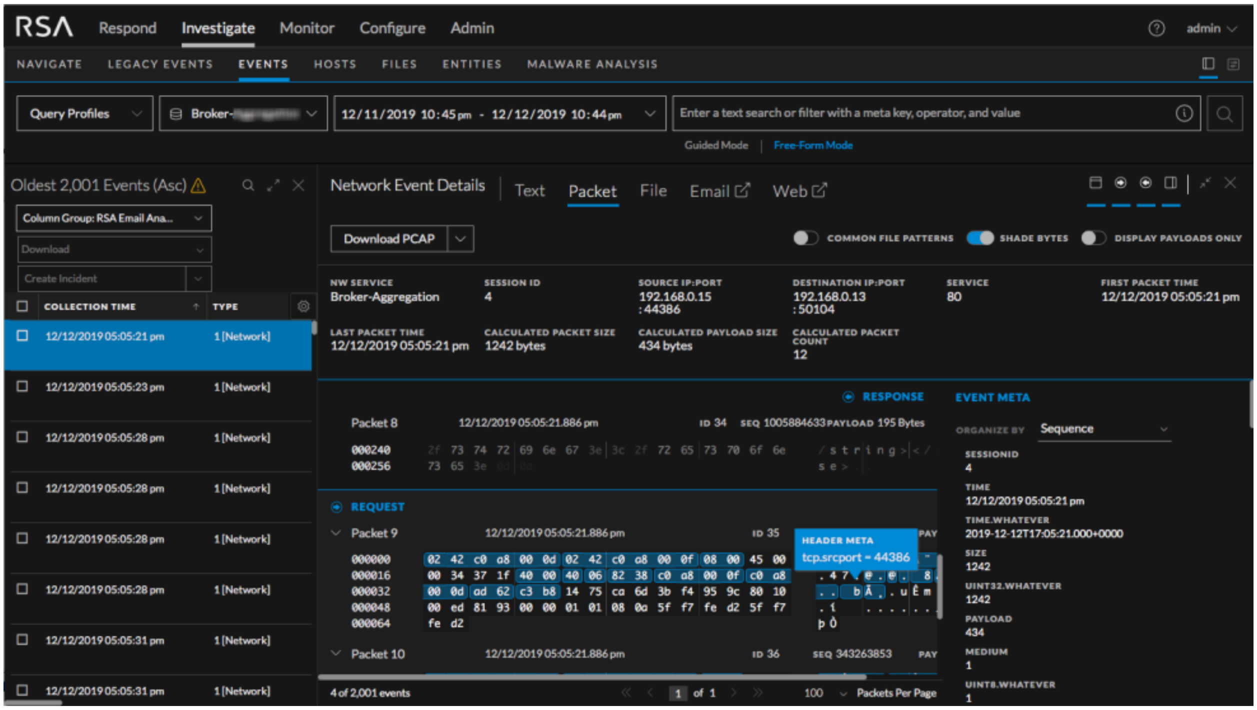
Session Streams [streams] (2 values)
2 (13,735) - 1 (4,439)

Events View

The default workflow for analysts interacting with events is optimized to limit the need to transition from one view to another. By combining capabilities (highlights spelled out further in this document) that were previously in two distinct workflows, known as Event Analysis and Events, the analyst now has a single workflow for analyzing events. By default the previous workflow is not in the Investigate menu, but an administrator can re-enable it if they desire a transitional period for existing analysts. Events are listed in order by time.

- The Events list shows the raw data for events, which you can sort and filter. You can also apply column groups to control which columns are displayed and their arrangement across the view. You can use Query profiles to apply a built-in or custom column group and a prequery in this view.
- The related metadata for results in the Events list is shown in the Event Meta panel. Analysts reviewing the metadata can change the order of the metadata to better track down what they are looking for. The items in the list of metadata can optionally be grouped by the sequence they were generated or alphabetically.
- Clicking an event opens a reconstruction of the event. Different reconstructions are available in the Events view (packets, text, files, and email) with helpful cues to identify points of interest, such as interesting bytes, file types, and encoded data. The Email panel was added to the Events view in Version 11.4.1; in earlier versions, the Email reconstruction opens in the Legacy Events view. The web reconstruction still opens in a Legacy Events view window.
- 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.
- You can pivot to standalone Endpoint, look up in Live and do other internal lookups, 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.
- 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. You can download multiple events from the Events list.

This figure is an example of the Events view with a packet reconstruction open in the right panel. The Events list is visible in the left panel.



☐	COLLECTION TIME	TYPE
☐	12/12/2019 05:05:21 pm	1 [Network]
☐	12/12/2019 05:05:23 pm	1 [Network]
☐	12/12/2019 05:05:28 pm	1 [Network]
☐	12/12/2019 05:05:28 pm	1 [Network]
☐	12/12/2019 05:05:28 pm	1 [Network]
☐	12/12/2019 05:05:28 pm	1 [Network]
☐	12/12/2019 05:05:31 pm	1 [Network]
☐	12/12/2019 05:05:31 pm	1 [Network]

NW SERVICE: Broker-Aggregation
SESSION ID: 4
SOURCE IP:PORT: 192.168.0.15 :44386
DESTINATION IP:PORT: 192.168.0.13 :50104
SERVICE: 80
FIRST PACKET TIME: 12/12/2019 05:05:21 pm
LAST PACKET TIME: 12/12/2019 05:05:21 pm
CALCULATED PACKET SIZE: 1242 bytes
CALCULATED PAYLOAD SIZE: 434 bytes
CALCULATED PACKET COUNT: 12

```
Packet 8     12/12/2019 05:05:21.886 pm     ID 34  SEQ 1005884633 PAYLOAD 195 Bytes
000240   2f 73 74 72 69 6e 67 3e 3c 2f 72 65 73 70 6f 6e    / s t r i n g > < /
000256   73 65 3e 0d 0a                                     s e > . .

Packet 9     12/12/2019 05:05:21.886 pm     ID 35
000000   02 42 c0 a8 00 0d 02 42 c0 a8 00 0f 08 00 45 00
000016   00 34 37 1f 40 00 40 06 82 38 c0 a8 00 0f c0 a8    . 4 7 . @ . @ .   8 .
000032   00 0d ad 62 c3 b8 14 75 ca 6d 3b f4 95 9c 80 10    . .   b Ã , . u Ê m
000048   00 ed 81 93 00 00 01 01 08 0a 5f f7 fe d2 5f f7    . í       . . . . . . .
000064   fe d2                                              þ Ò

Packet 10    12/12/2019 05:05:21.886 pm     ID 36  SEQ 343263853
```

HEADER META
tcp.srcport = 44386

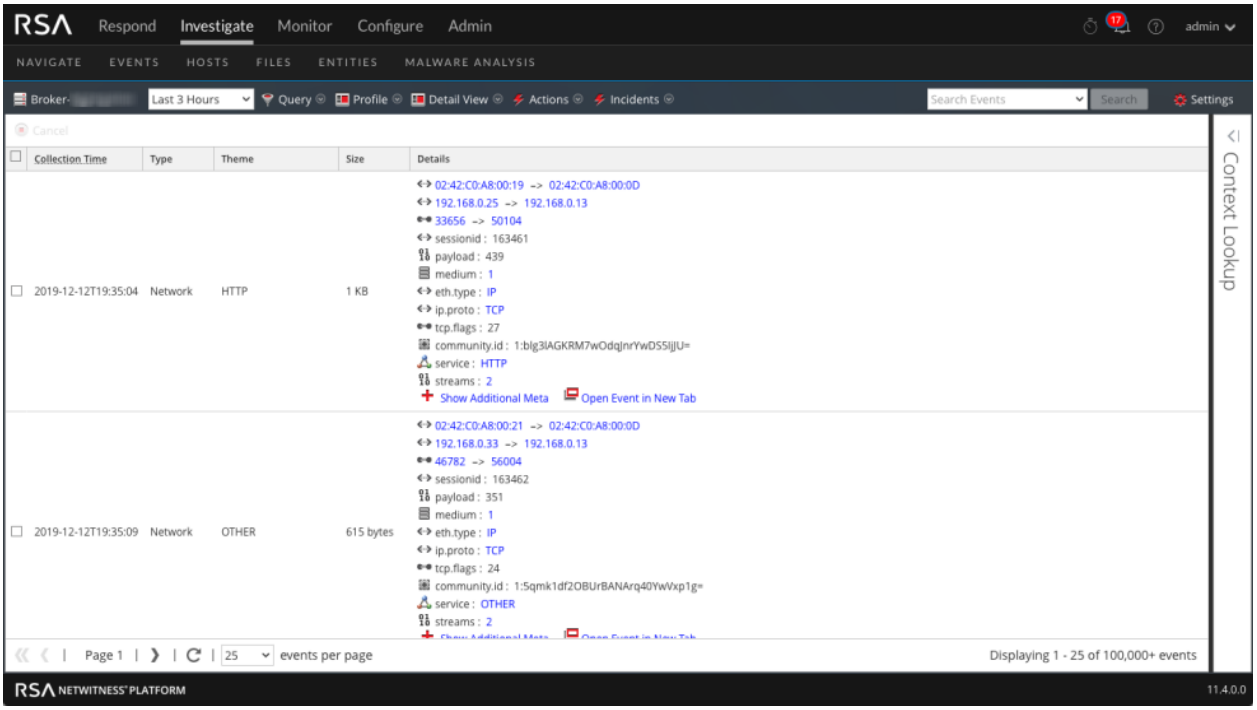
SESSIONID: 4
TIME: 12/12/2019 05:05:21 pm
TIME.WHATEVER: 2019-12-12T17:05:21.000+0000
SIZE: 1242
UINT32.WHATEVER: 1242
PAYLOAD: 434
MEDIUM: 1
UINT8.WHATEVER: 1

Legacy Events View

The Legacy Events view was the original Events view (11.0 to 11.3.x.x). The Legacy Events is no longer needed in Version 11.4, and it is hidden unless the administrator enables it as described under "Configure Investigation Settings" in the *System Configuration Guide*. The Legacy 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 Legacy Events view for a meta value that you see in the Navigate view.
- For analysts without sufficient privilege to navigate a service, the Legacy 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 Legacy 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 Legacy Events view.



☐	Collection Time	Type	Theme	Size	Details
☐	2019-12-12T19:35:04	Network	HTTP	1 KB	02:42:C0:A8:00:19 -> 02:42:C0:A8:00:0D 192.168.0.25 -> 192.168.0.13 33656 -> 50104 sessionid : 163461 payload : 439 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 27 community.id : 1:blg3lAGKRM7wOdqJnrYwDS5IjJU= service : HTTP streams : 2 + Show Additional Meta Open Event in New Tab
☐	2019-12-12T19:35:09	Network	OTHER	615 bytes	02:42:C0:A8:00:21 -> 02:42:C0:A8:00:0D 192.168.0.33 -> 192.168.0.13 46782 -> 56004 sessionid : 163462 payload : 351 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 24 community.id : 1:5qmk1df2OBUrBANArq40YwVxp1g= service : OTHER streams : 2 + Show Additional Meta Open Event in New Tab

Page 1 | 25 events per page

Displaying 1 - 25 of 100,000+ events

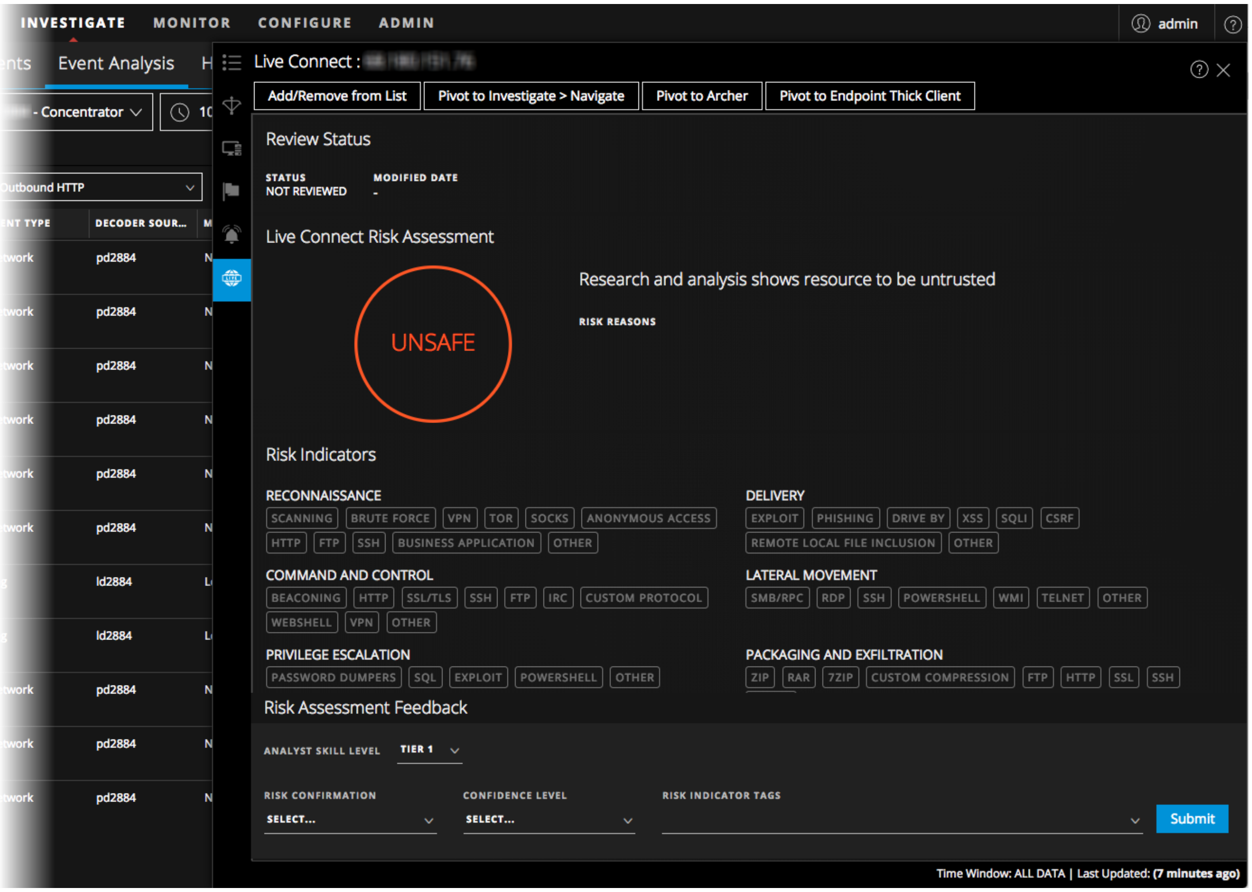
Contextual Information for an Event

In the Navigate view, Events view, and Legacy Events view, the Context Lookup panel shows details about elements associated with an event in the Context Hub for these meta types: IP Address, User, Host, Domain, MAC Address, Filename, and File hash. 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 and Legacy Events view.

> **Note:** Archer assets and active directory details are available in the Events 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 or later hosts.

The following figure shows the Context Lookup panel in the Events view.



Live Connect : [redacted]

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

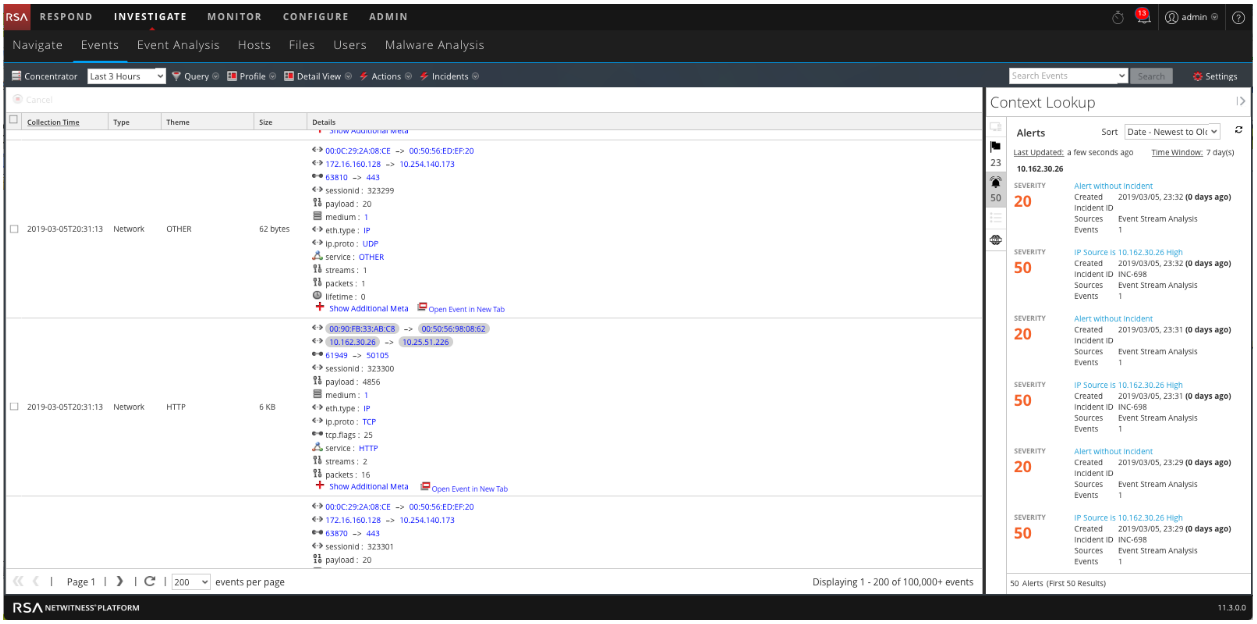
RISK CONFIRMATION: SELECT...

CONFIDENCE LEVEL: SELECT...

RISK INDICATOR TAGS

Time Window: ALL DATA | Last Updated: **(7 minutes ago)**

The following figure shows the Context Lookup panel in the Legacy Events view.



	Collection Time	Type	Theme	Size	Details
□	2019-03-05T20:31:13	Network	OTHER	62 bytes	00:0C:29:2A:08:CE -> 00:50:56:ED:EF:20 172.16.160.128 -> 10.254.140.173 63810 -> 443 sessionid : 323299 payload : 20 medium : 1 eth.type : IP ip.proto : UDP service : OTHER streams : 1 packets : 1 lifetime : 0
□	2019-03-05T20:31:13	Network	HTTP	6 KB	00:90:FB:33:AB:C8 -> 00:50:56:98:08:62 10.162.30.26 -> 10.25.51.226 61949 -> 50105 sessionid : 323300 payload : 4856 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 25 service : HTTP streams : 2 packets : 16
					00:0C:29:2A:08:CE -> 00:50:56:ED:EF:20 172.16.160.128 -> 10.254.140.173 63870 -> 443 sessionid : 323301 payload : 20

Page 1 | 200 events per page

Displaying 1 - 200 of 100,000+ events

Context Lookup

23

50

Alerts

Sort: Date - Newest to Ol

Last Updated: a few seconds ago   Time Window: 7 day(s)

10.162.30.26

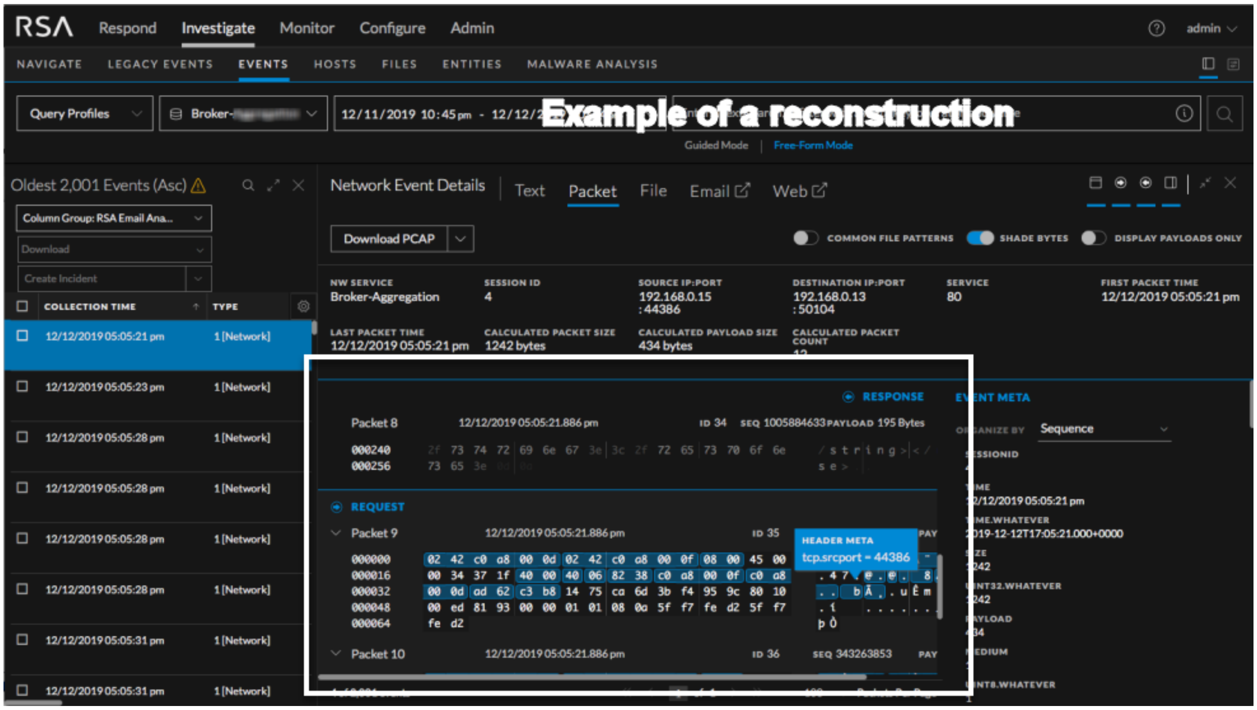
Severity	Alert	Created	Incident ID	Sources	Events
20	Alert without Incident	2019/03/05, 23:32 **(0 days ago)**		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:32 **(0 days ago)**	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:31 **(0 days ago)**		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:31 **(0 days ago)**	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:29 **(0 days ago)**		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:29 **(0 days ago)**	INC-698	Event Stream Analysis	1

50 Alerts (First 50 Results)

Event Reconstruction

Multiple views offer the ability to reconstruct an event. 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 may 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 Events view presents an interactive event reconstruction, which includes raw data, meta keys, and values. This figure is an example of a reconstruction in the Events view.



Example of a reconstruction

Broker-[redacted]

12/11/2019 10:45 pm - 12/12/

COLLECTION TIME	TYPE
12/12/2019 05:05:21 pm	1 [Network]
12/12/2019 05:05:23 pm	1 [Network]
12/12/2019 05:05:28 pm	1 [Network]
12/12/2019 05:05:28 pm	1 [Network]
12/12/2019 05:05:28 pm	1 [Network]
12/12/2019 05:05:28 pm	1 [Network]
12/12/2019 05:05:31 pm	1 [Network]
12/12/2019 05:05:31 pm	1 [Network]

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Broker-Aggregation	4	192.168.0.15 :44386	192.168.0.13 :50104	80	12/12/2019 05:05:21 pm

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
12/12/2019 05:05:21 pm	1242 bytes	434 bytes	12

```
Packet 8    12/12/2019 05:05:21.886 pm    ID 34  SEQ 1005884633 PAYLOAD 195 Bytes
000240   2f 73 74 72 69 6e 67 3e 3c 2f 72 65 73 70 6f 6e   /string></
000256   73 65 3e 0d 0a                                   se>

Packet 9    12/12/2019 05:05:21.886 pm    ID 35                          PAY
000000   02 42 c0 a8 00 0d 02 42 c0 a8 00 0f 08 00 45 00
000016   00 34 37 1f 40 00 40 06 82 38 c0 a8 00 0f c0 a8   .47.@.@.   8
000032   00 0d ad 62 c3 b8 14 75 ca 6d 3b f4 95 9c 80 10   .. bÃ .uÊm
000048   00 ed 81 93 00 00 01 01 08 0a 5f f7 fe d2 5f f7   .í   ......
000064   fe d2                                            þÒ

Packet 10   12/12/2019 05:05:21.886 pm    ID 36  SEQ 343263853           PAY
```

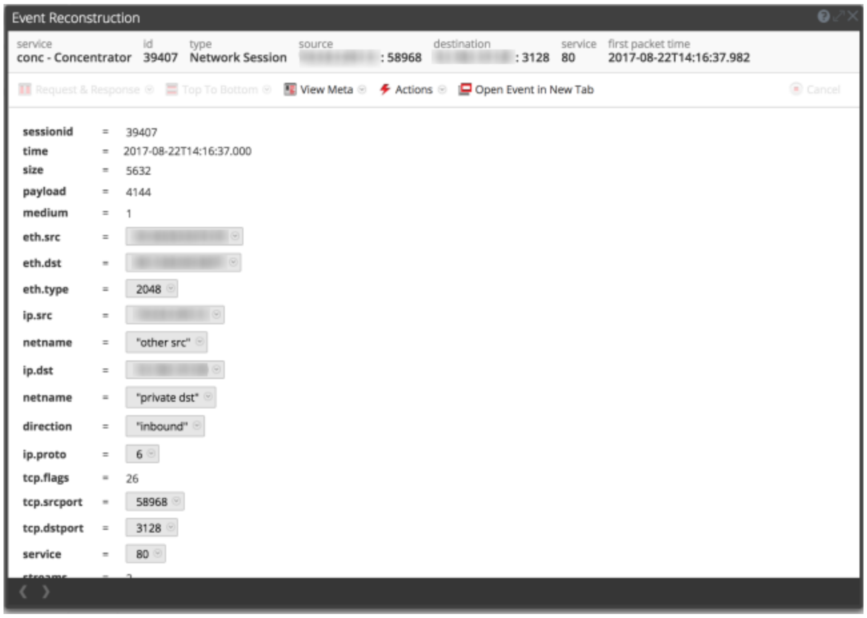
HEADER META
tcp.srcport = 44386

SESSIONID
4
TIME
12/12/2019 05:05:21 pm
TIME.WHATEVER
2019-12-12T17:05:21.000+0000
SIZE
1242
UINT32.WHATEVER
1242
PAYLOAD
434
MEDIUM
1
UINT8.WHATEVER

In the Events 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.

The Event Reconstruction in the Legacy 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.



Event Reconstruction

service	id	type	source	destination	service	first packet time
conc - Concentrator	39407	Network Session	[redacted] : 58968	[redacted] : 3128	80	2017-08-22T14:16:37.982

sessionid	=	39407
time	=	2017-08-22T14:16:37.000
size	=	5632
payload	=	4144
medium	=	1
eth.src	=	[redacted]
eth.dst	=	[redacted]
eth.type	=	2048
ip.src	=	[redacted]
netname	=	"other src"
ip.dst	=	[redacted]
netname	=	"private dst"
direction	=	"inbound"
ip.proto	=	6
tcp.flags	=	26
tcp.srcport	=	58968
tcp.dstport	=	3128
service	=	80
streams	=	2

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.

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 Legacy Events View
- Configure the Events View

Configure the Navigate View and Legacy Events View

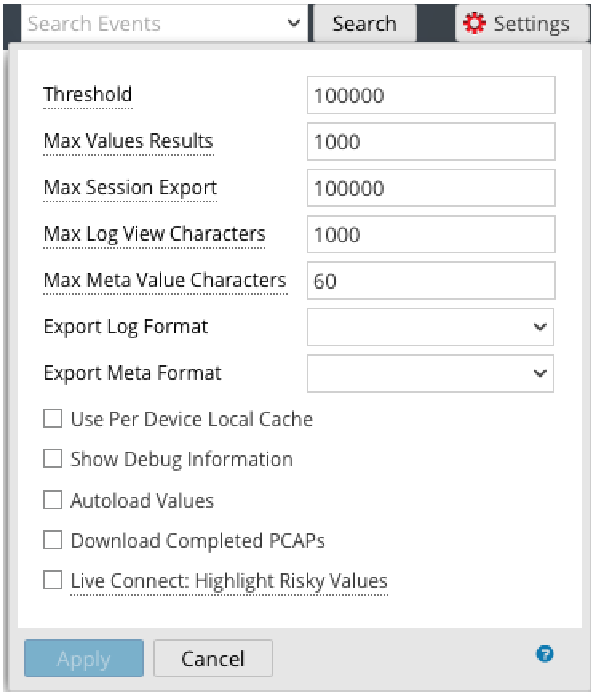
Analysts can set preferences that affect performance and behavior of NetWitness Platform when using the Navigate view and Legacy Events view. Some of the same settings are available in two places in NetWitness Platform, and changes made in either location are applied in the other view:

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

Access the Navigate View and Legacy 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.

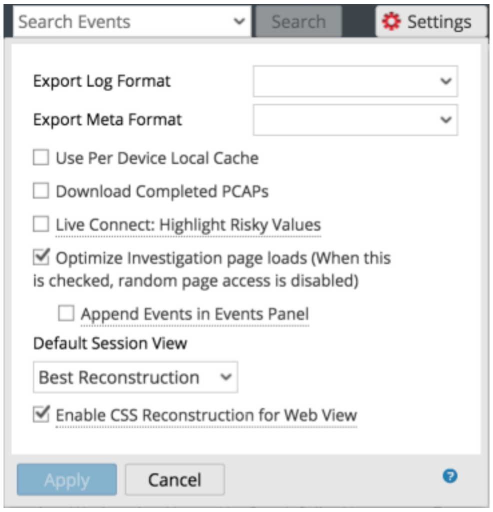


Threshold	100000
Max Values Results	1000
Max Session Export	100000
Max Log View Characters	1000
Max Meta Value Characters	60
Export Log Format	
Export Meta Format	

☐ Use Per Device Local Cache
☐ Show Debug Information
☐ Autoload Values
☐ Download Completed PCAPs
☐ Live Connect: Highlight Risky Values

> **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 **Legacy Events** view toolbar, select the **Settings** option.
  The Settings dialog for the Legacy Events view is displayed.



Export Log Format

Export Meta Format

□ Use Per Device Local Cache

□ Download Completed PCAPs

□ Live Connect: Highlight Risky Values

☑ Optimize Investigation page loads (When this is checked, random page access is disabled)

□ Append Events in Events Panel

Default Session View

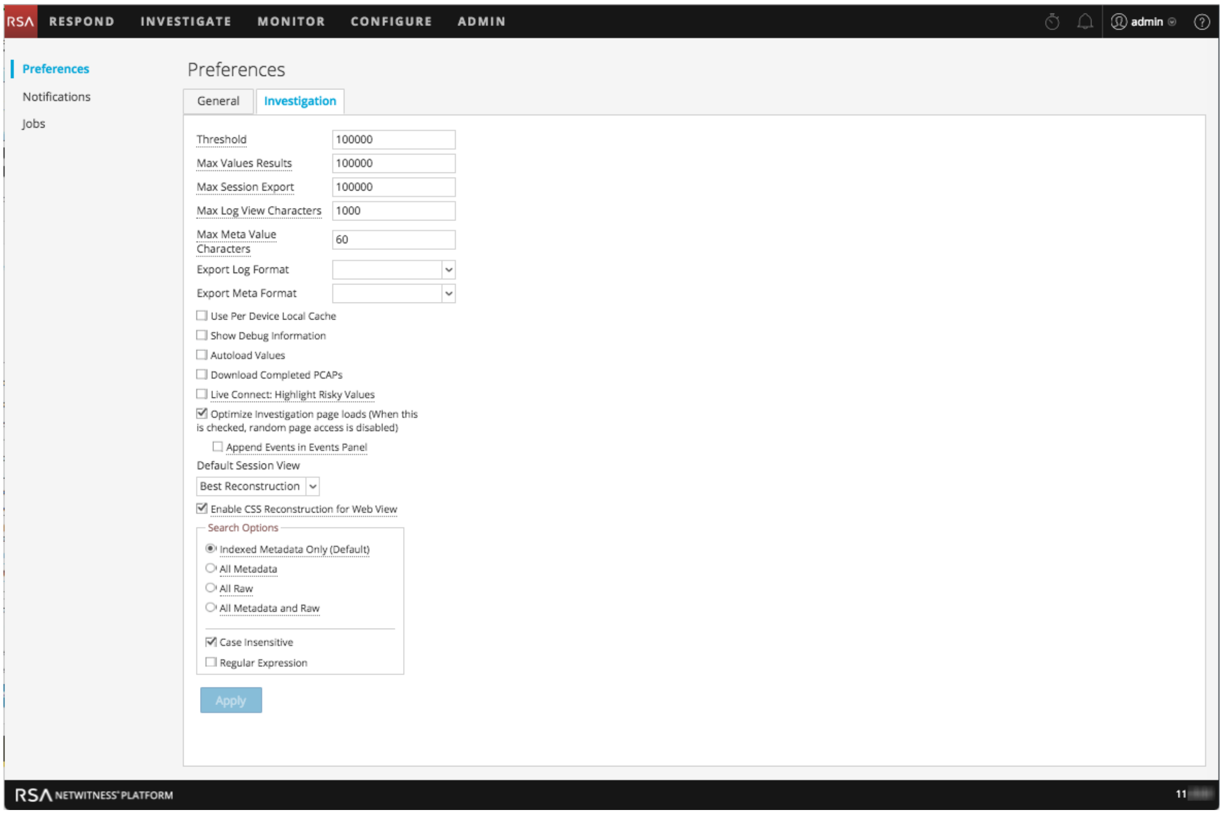
Best Reconstruction

☑ Enable CSS Reconstruction for Web View

Apply Cancel

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.



Preferences

General | Investigation

Threshold 100000

Max Values Results 100000

Max Session Export 100000

Max Log View Characters 1000

Max Meta Value Characters 60

Export Log Format

Export Meta Format

□ Use Per Device Local Cache

□ Show Debug Information

□ Autoload Values

□ Download Completed PCAPs

□ Live Connect: Highlight Risky Values

☑ Optimize Investigation page loads (When this is checked, random page access is disabled)

□ Append Events in Events Panel

Default Session View

Best Reconstruction

☑ Enable CSS Reconstruction for Web View

Search Options

● Indexed Metadata Only (Default)

○ All Metadata

○ All Raw

○ All Metadata and Raw

☑ Case Insensitive

□ Regular Expression

Apply

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 Legacy Events View Parameters

Several settings influence the performance of NetWitness Platform when loading values in the Navigate view and the Legacy 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 Legacy 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 Legacy 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 Legacy 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 Legacy 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 Legacy 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 Value Export Format

You can export meta values from the Navigate view and Legacy Events view as Text, CSV, tab-separated values (TSV), and JSON. There is no built-in default value for the meta value 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 Legacy Eventsview.
2. Select one of the options from the **Export Meta Format** drop-down menu.
3. Click **Apply.**
   The setting goes into effect immediately.

Calibrate Legacy Events View Retrieval and Default Reconstruction

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

1. Go to the **Preferences** panel > **Investigation** tab or to the **Settings** dialog for the Legacy 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 Legacy 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 Legacy Events view (11.2 and later), 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.

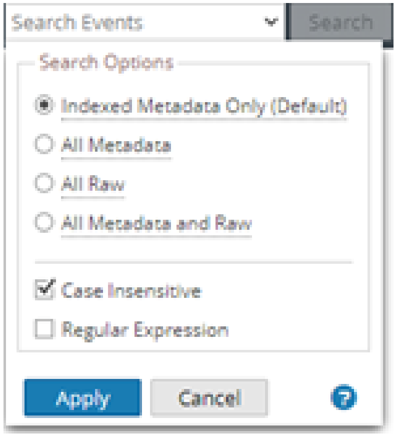
To enable or disable this option:

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 Legacy Events view Search Options drop-down menu. To configure search options:

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



Search Events

Search Options

● Indexed Metadata Only (Default)

○ All Metadata

○ All Raw

○ All Metadata and Raw

☑ Case Insensitive

□ Regular Expression

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

Configure the Events View

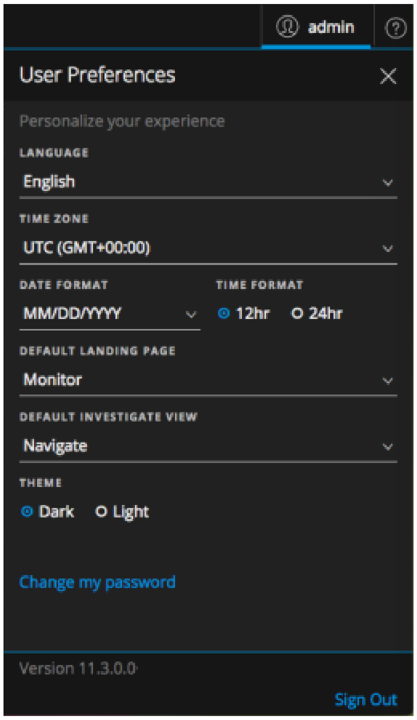
Note: The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

Analysts can set preferences that affect the behavior of NetWitness Platform when using the Investigate > Events view. If the Events 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 Events preferences menu () is focused on user preferences for behavior in the Events 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, Hosts view, Files view, Entities 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*.



Personalize your experience

LANGUAGE: English

TIME ZONE: UTC (GMT+00:00)

DATE FORMAT: MM/DD/YYYY

TIME FORMAT: ● 12hr ○ 24hr

DEFAULT LANDING PAGE: Monitor

DEFAULT INVESTIGATE VIEW: Navigate

THEME: ● Dark ○ Light

Change my password

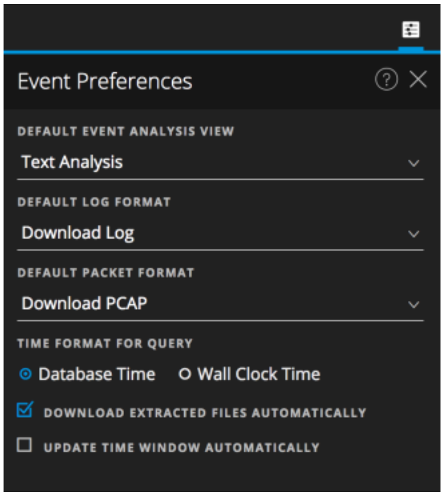
Version 11.3.0.0

Set User Preferences for the Events View

You can set your own preferences relevant to the Events 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 Events view:

1. In the **Events** view, click ☰.
   The Event Preferences dialog is displayed. The 11.3 and 11.4 versions of the dialog have some differences in labeling and available options as shown in the following figures. The first figure is an example of the Version 11.3 dialog, and the second figure shows the dialog for Version 11.4.



Event Preferences

DEFAULT EVENT ANALYSIS VIEW
Text Analysis

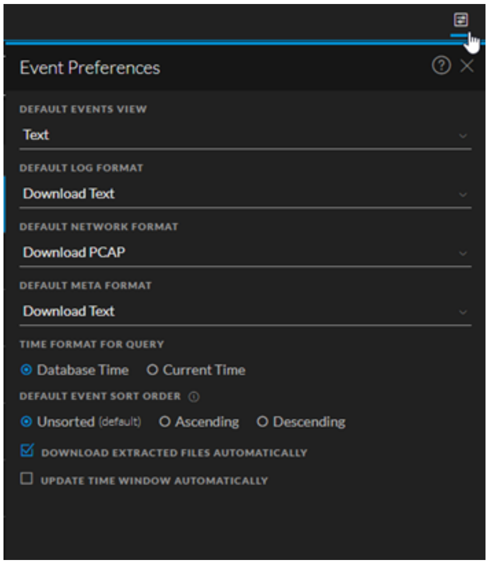
DEFAULT LOG FORMAT
Download Log

DEFAULT PACKET FORMAT
Download PCAP

TIME FORMAT FOR QUERY
● Database Time ○ Wall Clock Time

☑ DOWNLOAD EXTRACTED FILES AUTOMATICALLY

□ UPDATE TIME WINDOW AUTOMATICALLY



Event Preferences

DEFAULT EVENTS VIEW
Text

DEFAULT LOG FORMAT
Download Text

DEFAULT NETWORK FORMAT
Download PCAP

DEFAULT META FORMAT
Download Text

TIME FORMAT FOR QUERY
● Database Time ○ Current Time

DEFAULT EVENT SORT ORDER
● Unsorted (default) ○ Ascending ○ Descending

☑ DOWNLOAD EXTRACTED FILES AUTOMATICALLY

□ UPDATE TIME WINDOW AUTOMATICALLY

2. In the **Default Events View** field, select the default reconstruction type when you open an event in the Events panel: **Text**, **Packet**, **File**, or **Email** .
   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** field, select the download format for exporting logs: **Download Log** (11.3) or **Download Text** (11.4), **Download XML**, **Download CSV**, or **Download JSON**. If you do not select a format here, the default download format is **Download Text**. These options are also available at the time of download in a drop-down menu.

4. In the **Default Packet Format** (11.3) or **Default Network Format** (11.4) field, select the default format for downloading packets. If you do not select a format here, the default download format is **Download PCAP**. 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** (11.3) or **Download Payloads** (11.4) 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. (Version 11.4 and later) In the **Default Meta Format** field, select the download format for exporting metadata: **Download Text**, **Download CSV**, **Download TSV**, or **Download JSON**. If you do not select a format here, the default download format is **Download Text**.

6. Under **Time Format for Query**, choose either **Database Time** or **Current Time** (11.4). The Events 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 Legacy 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 **Current Time** (labeled **Wall Clock Time** in Version 11.3 and earlier) 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.

7. (Version 11.4 and later) To set the sort sequence by collection time for the events listed in the Events panel, select one option under **Default Event Sort Order**. After you have selected a preference, you can also interact with the table column headers to request the results again sorted differently as described in Use Columns and Column Groups in the Events List.

   - **Unsorted** (default for Version 11.4.1): To list events as processed by the Core services. Unsorted is faster because it streams back the events as soon as a match is found versus waiting for all Core services to respond and then displaying them in the chosen order.
   - **Ascending** (default for Version 11.4 and earlier): To put the events with the earliest collection time first in the list. The oldest events are displayed first if in ascending order.
   - **Descending**: To put the events with the latest collection time first in the list. The newest events are displayed first if in descending order. When investigating logs, you may want to change the sort sequence to see the latest collection time first.

   If results exceed the events limit, not all events can be loaded. The portion of returned events loaded in the Events panel matches the sort order preference: the oldest portion of events is loaded when Ascending order is selected, and newest portion of events is loaded when Descending order is selected. When Unsorted is selected, the oldest portion of events is matched and then listed unsorted. If you changed the sort order preference after events were loaded, you must refresh the view to apply the new sort order.

8. 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.

9. (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 submit a query to get 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 Investigate offers different starting points: Navigate view, Events view, Legacy Events view, Hosts view, Files view, Entities view, and Malware Analysis view.

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 Entities (formerly 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).
- The 11.4 Events view is the default view for investigating events. The default workflow for analysts interacting with events is optimized to limit the need to transition from one view to another. By combining capabilities that were previously in two distinct workflows, known as Event Analysis and Events, the analyst has a single workflow for analyzing events. With the new functionality added to the Events view, the Legacy Events view is no longer needed. By default the previous workflow is not in the Investigate menu, but an administrator can re-enable it as described in "Configure Investigation Settings" in the *System Configuration Guide*.

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** > **Legacy Events**. 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 Events View
- Begin an Investigation in the Navigate or Legacy Events 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** > **Entities** or NetWitness UEBA (User and Entity Behavior Analytics). In versions 11.3 and earlier, the menu option is **Investigate** > **Users**. 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 Legacy 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 Legacy Events, 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 Legacy Events view, a service must be specified.

- Investigate opens the Navigate view or the Legacy 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, Investigate 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 Legacy Events view, you can change the service or collection to investigate by selecting the service name in the toolbar. Investigate 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 Legacy Events view for log exports and enhanced search capabilities.

With a service or collection selected, Investigate 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 Legacy 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 Legacy Events view data loads automatically. If you specified Autoload Values in the Navigate view preferences, Investigate populates the data automatically. Otherwise, you must select Load Values. Investigate populates the metadata in the Navigate view Values panel and results become visible almost immediately.

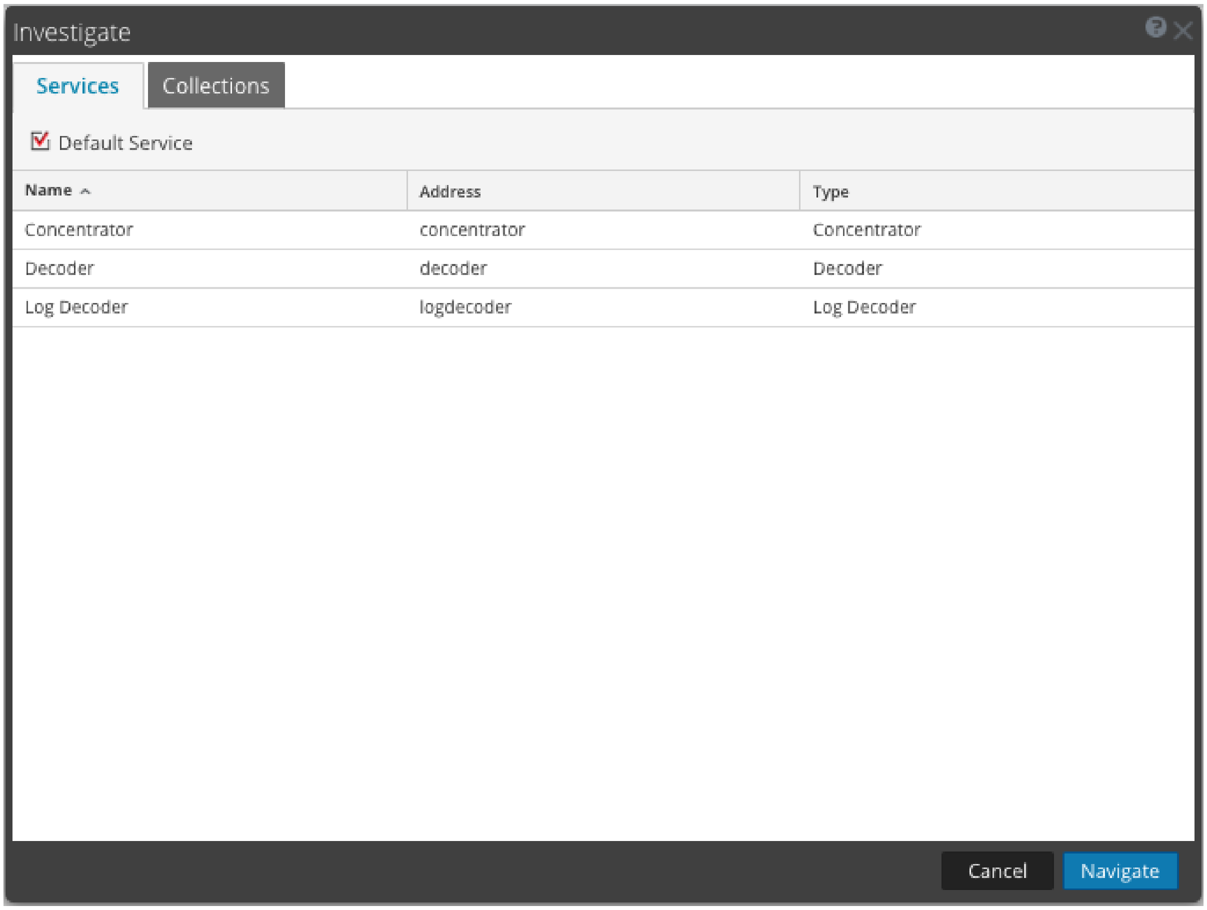
The rest of this topic provides instructions for beginning the investigation of data on a service.

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 Legacy Events view, refine results, reconstruct and analyze events, then download and act upon results (see Refining the Results Set and Reconstructing and Analyzing Events and Downloading and Acting Upon Results).

Begin an Investigation (No Default Service)

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



☑ Default Service

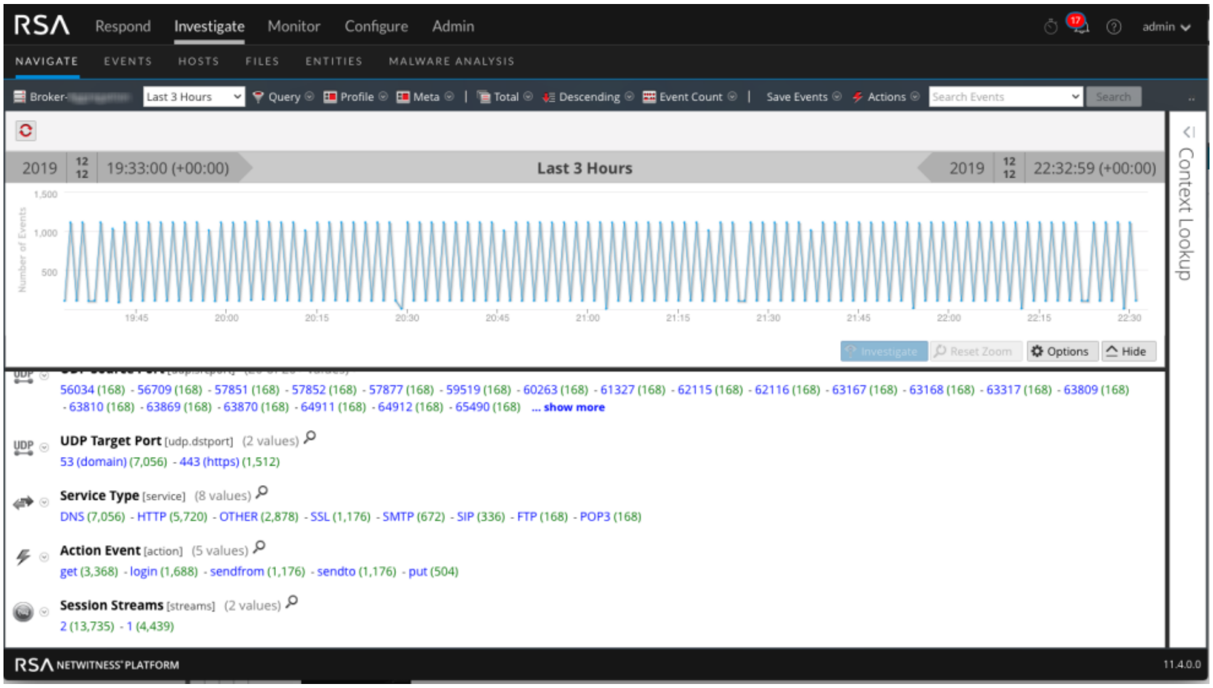
Name	Address	Type
Concentrator	concentrator	Concentrator
Decoder	decoder	Decoder
Log Decoder	logdecoder	Log Decoder

2. Double-click a service or select a service, usually a Concentrator, and click **Navigate**.
   The data loads automatically in the Legacy 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 Refining the Results Set. 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.



56034 (168) - 56709 (168) - 57851 (168) - 57852 (168) - 57877 (168) - 59519 (168) - 60263 (168) - 61327 (168) - 62115 (168) - 62116 (168) - 63167 (168) - 63168 (168) - 63317 (168) - 63809 (168) - 63810 (168) - 63869 (168) - 63870 (168) - 64911 (168) - 64912 (168) - 65490 (168) ... show more

UDP Target Port [udp.dstport] (2 values)
53 (domain) (7,056) - 443 (https) (1,512)

Service Type [service] (8 values)
DNS (7,056) - HTTP (5,720) - OTHER (2,878) - SSL (1,176) - SMTP (672) - SIP (336) - FTP (168) - POP3 (168)

Action Event [action] (5 values)
get (3,368) - login (1,688) - sendfrom (1,176) - sendto (1,176) - put (504)

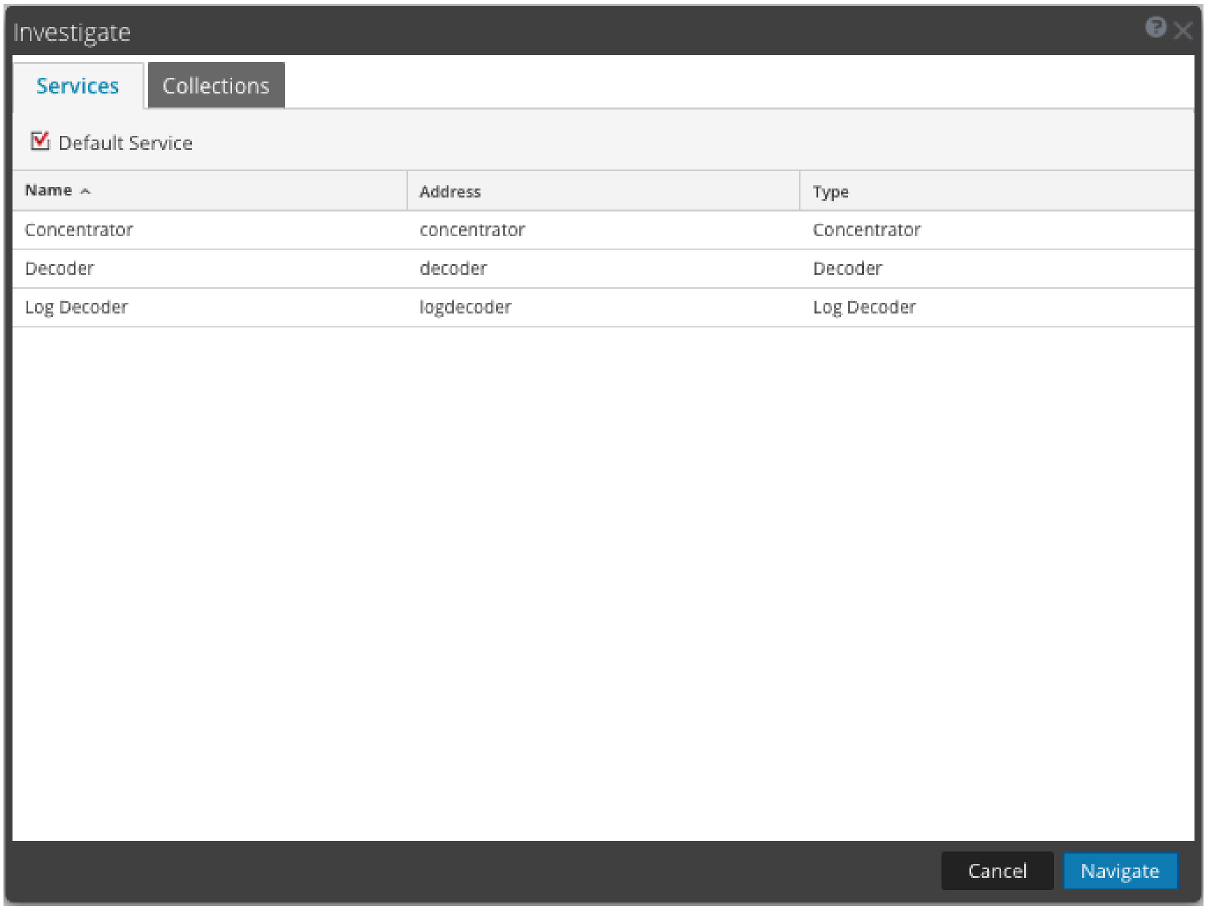
Session Streams [streams] (2 values)
2 (13,735) - 1 (4,439)

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.



Name	Address	Type
Concentrator	concentrator	Concentrator
Decoder	decoder	Decoder
Log Decoder	logdecoder	Log Decoder

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)

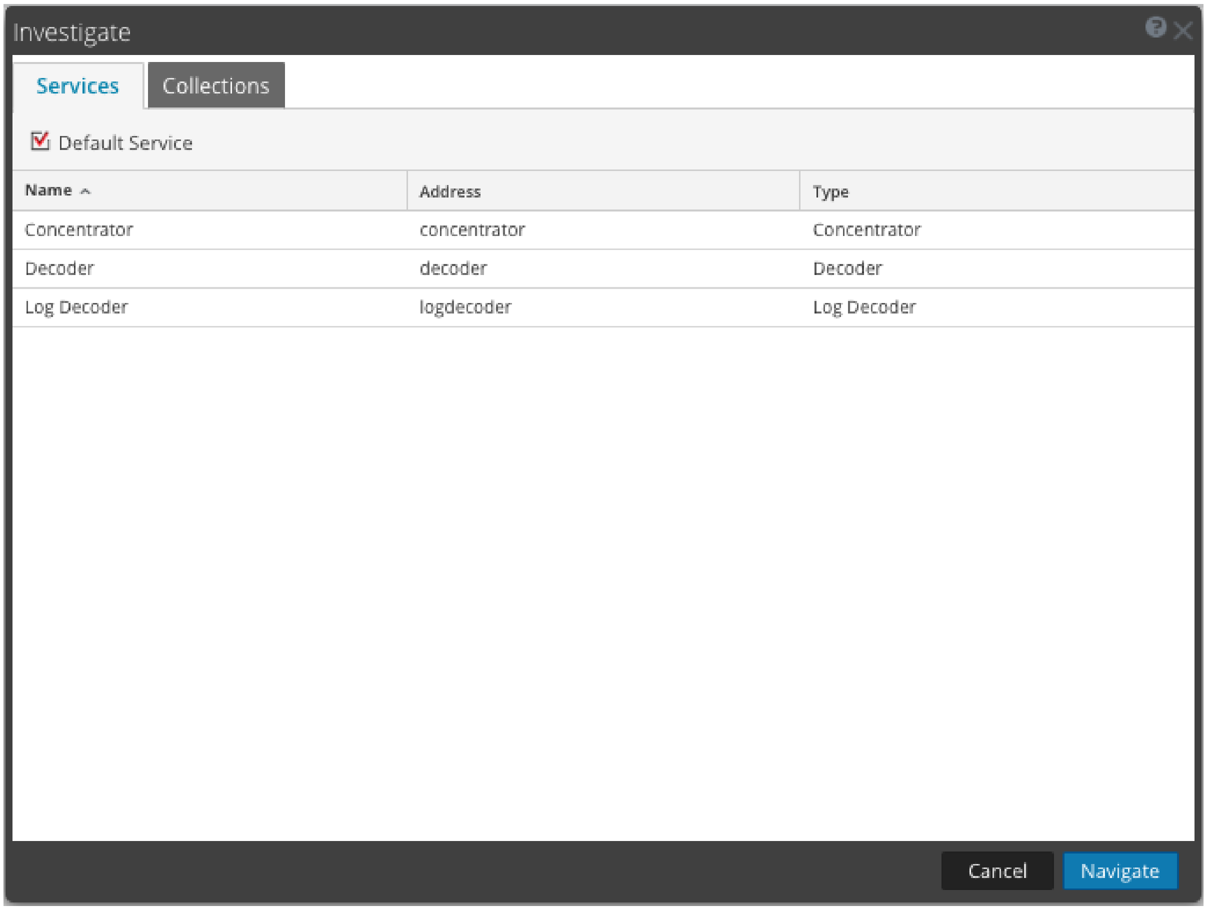
1. Go to **Investigate > Navigate** or **Legacy Events**.
   If the Autoload Values setting is set to off, the Navigate view is displayed with the default service selected, and ready to load data. If the Autoload Values setting is on, the values are loaded as shown in Step 3. In the Legacy Events view, 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 Legacy Events view, click the service name at the top of the options panel.
   The Investigate dialog is displayed.

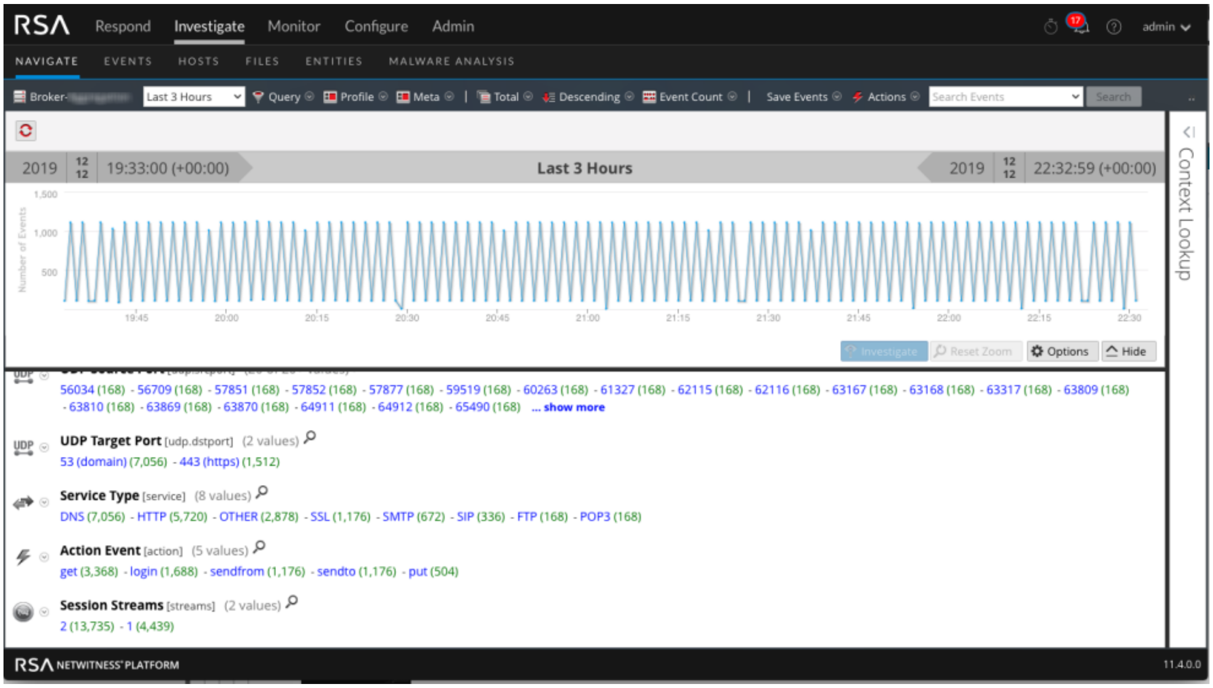


☑ Default Service

Name	Address	Type
Concentrator	concentrator	Concentrator
Decoder	decoder	Decoder
Log Decoder	logdecoder	Log Decoder

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.



56034 (168) - 56709 (168) - 57851 (168) - 57852 (168) - 57877 (168) - 59519 (168) - 60263 (168) - 61327 (168) - 62115 (168) - 62116 (168) - 63167 (168) - 63168 (168) - 63317 (168) - 63809 (168) - 63810 (168) - 63869 (168) - 63870 (168) - 64911 (168) - 64912 (168) - 65490 (168) ... show more

UDP Target Port [udp.dstport] (2 values)
53 (domain) (7,056) - 443 (https) (1,512)

Service Type [service] (8 values)
DNS (7,056) - HTTP (5,720) - OTHER (2,878) - SSL (1,176) - SMTP (672) - SIP (336) - FTP (168) - POP3 (168)

Action Event [action] (5 values)
get (3,368) - login (1,688) - sendfrom (1,176) - sendto (1,176) - put (504)

Session Streams [streams] (2 values)
2 (13,735) - 1 (4,439)

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

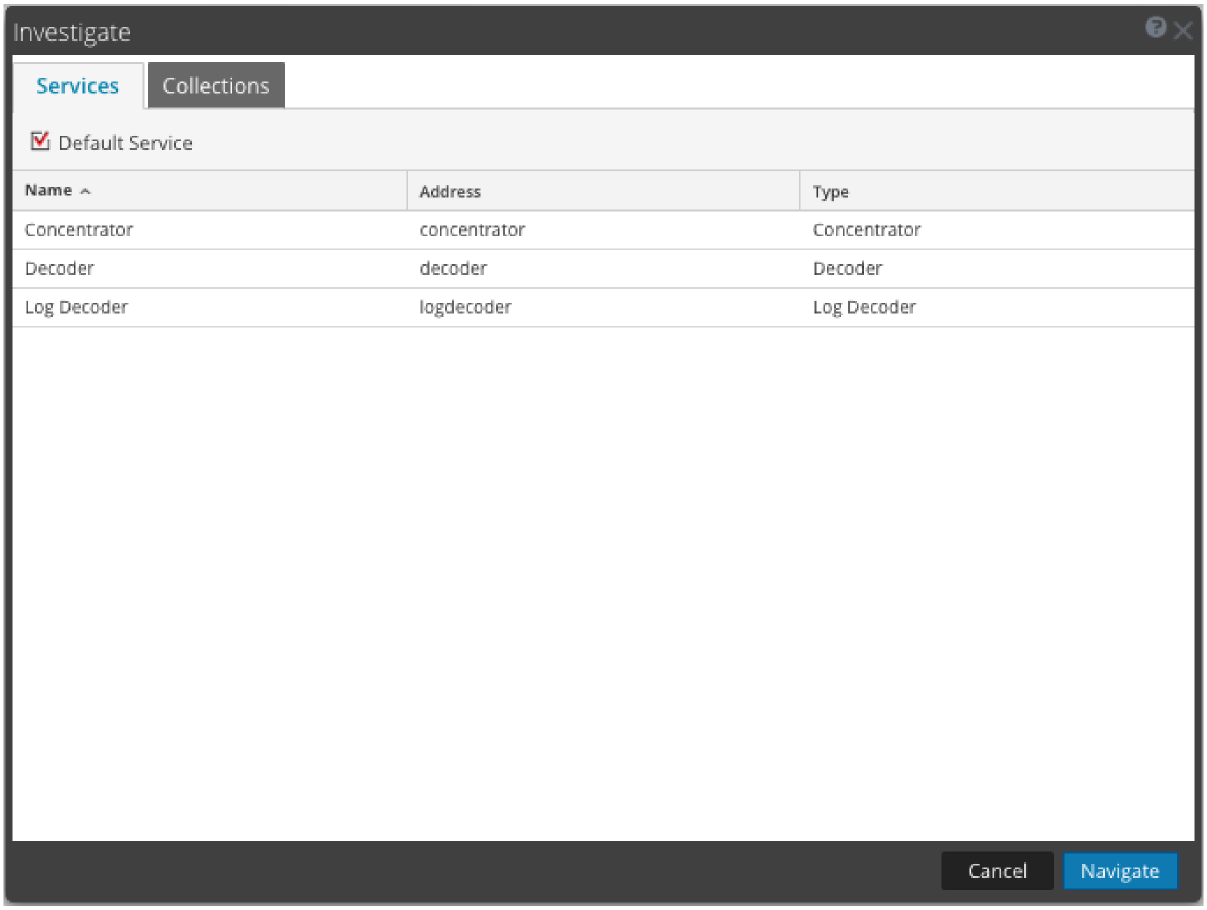
Investigate Workbench Restoration Collections

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 **Legacy Events**.
   The Investigate dialog is displayed.



☑ Default Service

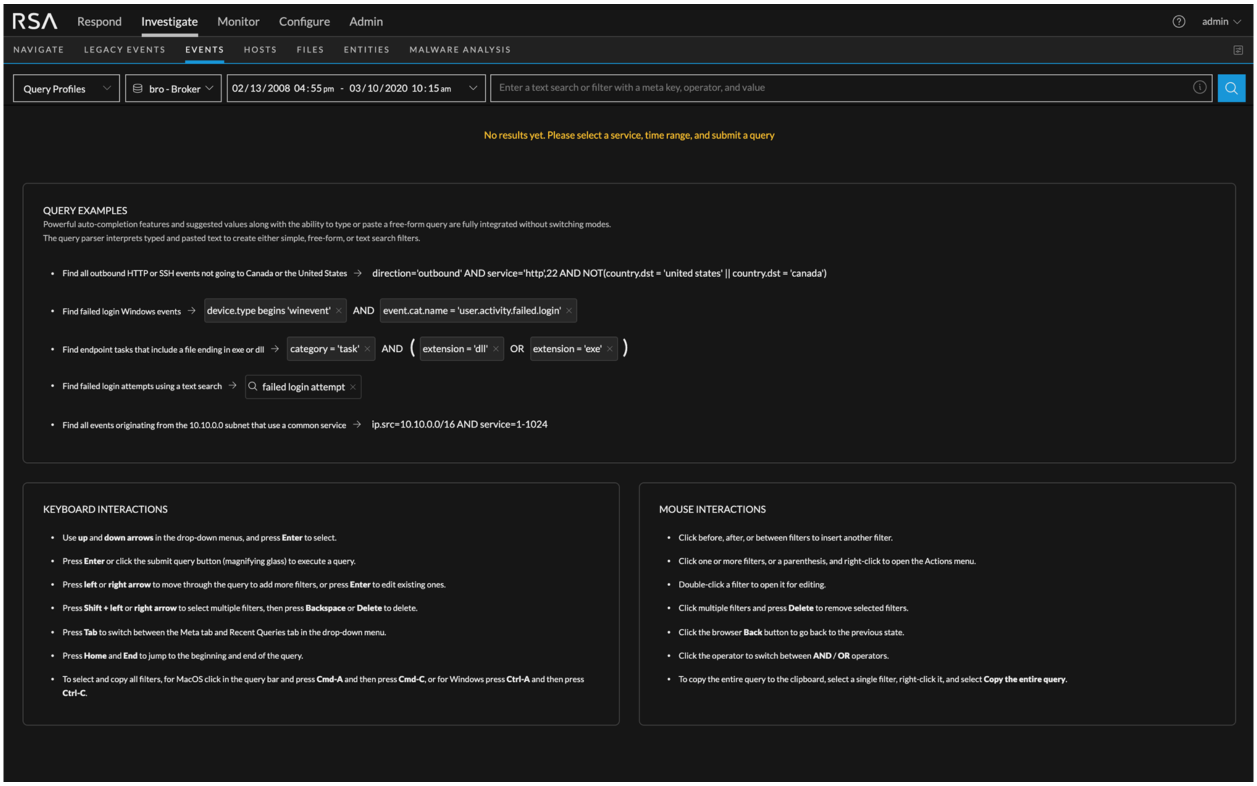
Name	Address	Type
Concentrator	concentrator	Concentrator
Decoder	decoder	Decoder
Log Decoder	logdecoder	Log Decoder

2. Select a workbench service and workbench name that you want to investigate.
3. Click **Navigate** to perform an investigation on the 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 Events View

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

The following figure shows the initial Events view with some examples of queries and information about keyboard and mouse interaction. This figure depicts the initial view in Version 11.4.1.



No results yet. Please select a service, time range, and submit a query

QUERY EXAMPLES

Powerful auto-completion features and suggested values along with the ability to type or paste a free-form query are fully integrated without switching modes.
The query parser interprets typed and pasted text to create either simple, free-form, or text search filters.

- Find all outbound HTTP or SSH events not going to Canada or the United States → direction='outbound' AND service='http',22 AND NOT(country.dst = 'united states' || country.dst = 'canada')
- Find failed login Windows events → device.type begins 'winevent' × AND event.cat.name = 'user.activity.failed.login' ×
- Find endpoint tasks that include a file ending in exe or dll → category = 'task' × AND (extension = 'dll' × OR extension = 'exe' ×)
- Find failed login attempts using a text search → failed login attempt ×
- Find all events originating from the 10.10.0.0 subnet that use a common service → ip.src=10.10.0.0/16 AND service=1-1024

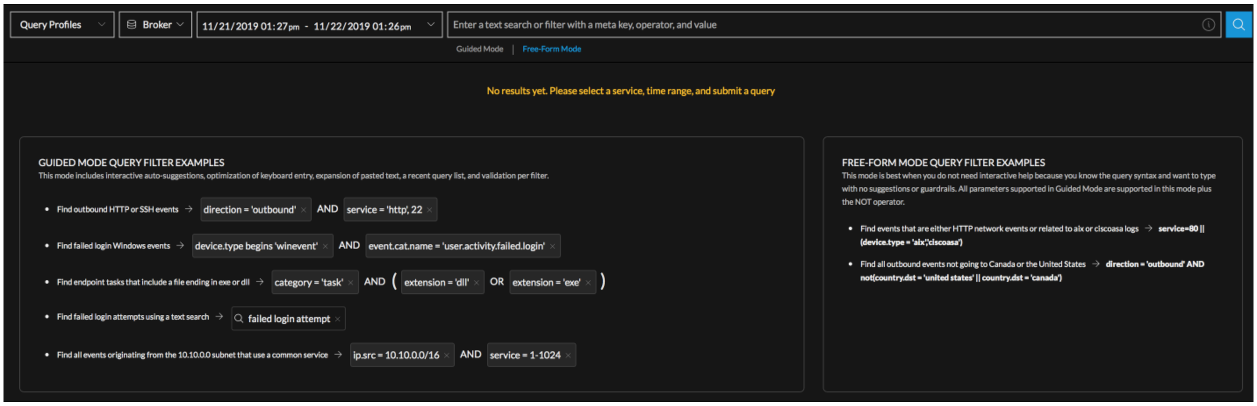
KEYBOARD INTERACTIONS

- Use **up** and **down arrows** in the drop-down menus, and press **Enter** to select.
- Press **Enter** or click the submit query button (magnifying glass) to execute a query.
- Press **left** or **right arrow** to move through the query to add more filters, or press **Enter** to edit existing ones.
- Press **Shift + left** or **right arrow** to select multiple filters, then press **Backspace** or **Delete** to delete.
- Press **Tab** to switch between the Meta tab and Recent Queries tab in the drop-down menu.
- Press **Home** and **End** to jump to the beginning and end of the query.
- To select and copy all filters, for MacOS click in the query bar and press **Cmd-A** and then press **Cmd-C**, or for Windows press **Ctrl-A** and then press **Ctrl-C**.

MOUSE INTERACTIONS

- Click before, after, or between filters to insert another filter.
- Click one or more filters, or a parenthesis, and right-click to open the Actions menu.
- Double-click a filter to open it for editing.
- Click multiple filters and press **Delete** to remove selected filters.
- Click the browser **Back** button to go back to the previous state.
- Click the operator to switch between **AND / OR** operators.
- To copy the entire query to the clipboard, select a single filter, right-click it, and select **Copy the entire query**.

This figure show the examples provided in Version 11.4, which has two modes for creating queries.


Query Profiles
Broker
11/21/2019 01:27pm - 11/22/2019 01:26pm
Enter a text search or filter with a meta key, operator, and value
Guided Mode
Free-Form Mode

No results yet. Please select a service, time range, and submit a query

GUIDED MODE QUERY FILTER EXAMPLES

This mode includes interactive auto-suggestions, optimization of keyboard entry, expansion of pasted text, a recent query list, and validation per filter.

- Find outbound HTTP or SSH events → direction = 'outbound' × AND service = 'http', 22 ×
- Find failed login Windows events → device.type begins 'winevent' × AND event.cat.name = 'user.activity.failed.login' ×
- Find endpoint tasks that include a file ending in exe or dll → category = 'task' × AND (extension = 'dll' × OR extension = 'exe' ×)
- Find failed login attempts using a text search → failed login attempt ×
- Find all events originating from the 10.10.0.0 subnet that use a common service → ip.src = 10.10.0.0/16 × AND service = 1-1024 ×

FREE-FORM MODE QUERY FILTER EXAMPLES

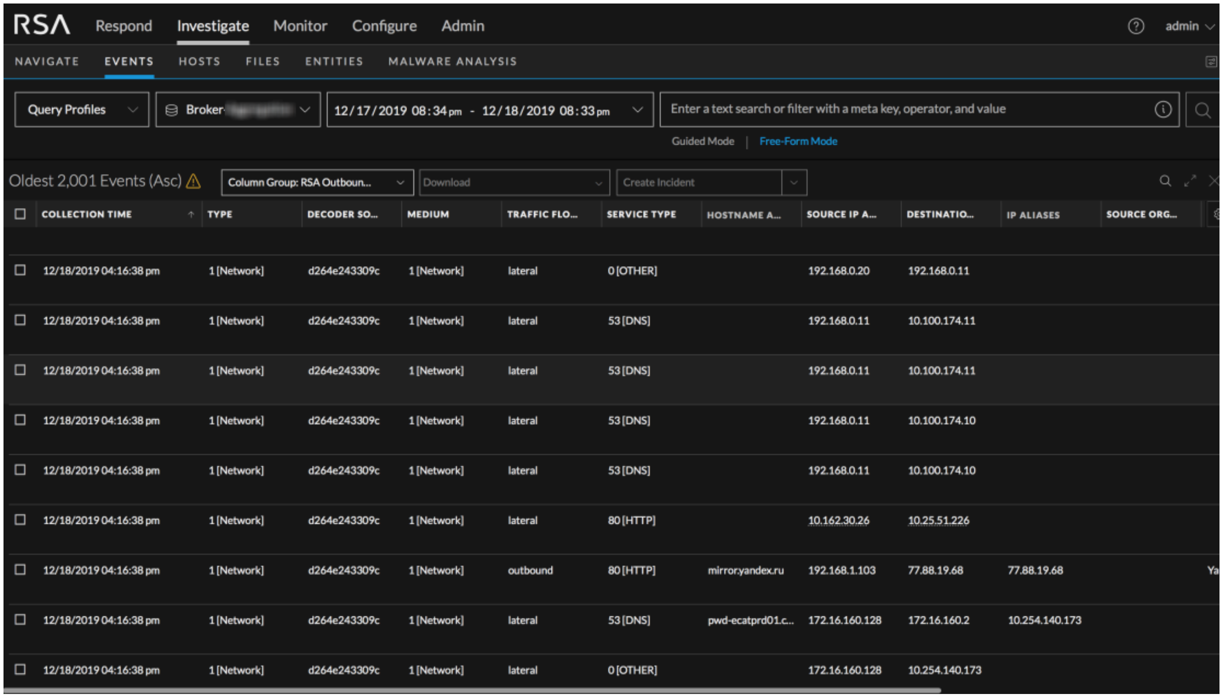
This mode is best when you do not need interactive help because you know the query syntax and want to type with no suggestions or guardrails. All parameters supported in Guided Mode are supported in this mode plus the NOT operator.

- Find events that are either HTTP network events or related to aix or ciscoasa logs → **service=80 || (device.type = 'aix','ciscoasa')**
- Find all outbound events not going to Canada or the United States → **direction = 'outbound' AND not(country.dst = 'united states' || country.dst = 'canada')**

Access the Events View

Several ways to access the Events view are available in Version 11.1 and later.

- Go to **Investigate > Events** or select the **Investigate** option in the main menu if you have made the Events view your default Investigate view. The following procedure provides detailed steps.
- Hover over and click a count (the green number after a meta value) in the Navigate view. The Events view opens with the list of events for the selected drill point, and you can begin working as described in Reconstructing and Analyzing Events.
- Hover over a count and control-click **Open Events in new tab**. The Events view opens in a new tab with the list of events for the selected drill point, and you can begin working as described in Reconstructing and Analyzing Events. The following figure is an example of the list of events.


RSA
Respond
Investigate
Monitor
Configure
Admin
admin
NAVIGATE
EVENTS
HOSTS
FILES
ENTITIES
MALWARE ANALYSIS
Query Profiles
Broker [redacted]
12/17/2019 08:34 pm - 12/18/2019 08:33 pm
Enter a text search or filter with a meta key, operator, and value
Guided Mode | Free-Form Mode
Oldest 2,001 Events (Asc)
Column Group: RSA Outboun...
Download
Create Incident

□	COLLECTION TIME	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP A...	DESTINATIO...	IP ALIASES	SOURCE ORG...
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	0 [OTHER]		192.168.0.20	192.168.0.11		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.11		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.11		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.10		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.10		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	outbound	80 [HTTP]	mirror.yandex.ru	192.168.1.103	77.88.19.68	77.88.19.68	Ya
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]	pwd-ecatprd01.c...	172.16.160.128	172.16.160.2	10.254.140.173	
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	0 [OTHER]		172.16.160.128	10.254.140.173		

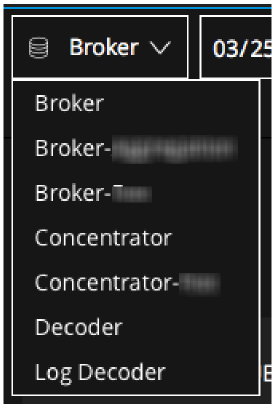
To begin an investigation in the Events view using direct access:

1. Go to **Investigate** > **Events**.

   The Events 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.

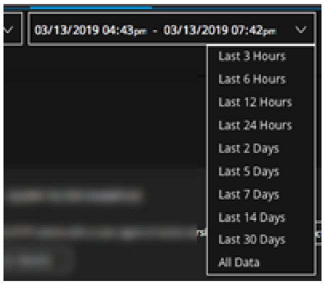
- 🗄 and selected service name = The service is selected.
- ◌ = Investigate is attempting to connect to the selected service.
- ⚠ = There was an error connecting to the selected service or there is no data in the selected service. In this state, the service selector control also turns red, and a tooltip 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 Events View.



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

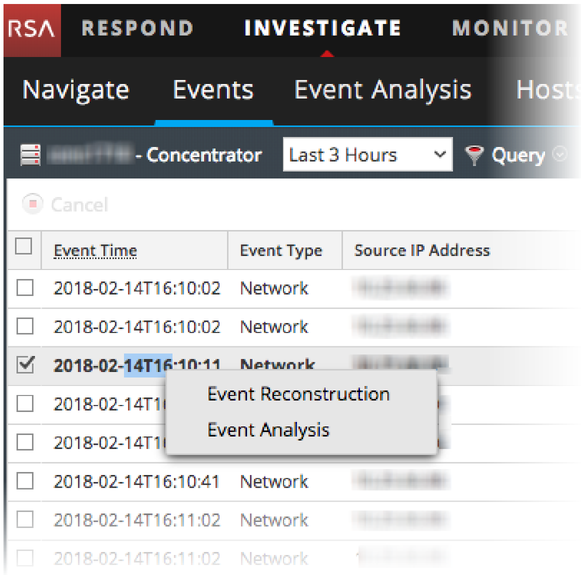
4. Create a query that consists of one or more filters that contain a meta key, operator, and optional value. See Filter Results in the Events View for details on creating queries.

5. When ready to submit the query, click 🔍 or **Query Events**.
   The Events 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 Reconstruct an Event in the Events View and Analyze Events in the Events View to learn how to work in the Events view.

Access the Events View (Version 11.0)

To open an event in the Event 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**.



□	Event Time	Event Type	Source IP Address
□	2018-02-14T16:10:02	Network	[redacted]
□	2018-02-14T16:10:02	Network	[redacted]
☑	2018-02-14T16:10:11	Network	[redacted]
□	2018-02-14T1		[redacted]
□	2018-02-14T1		[redacted]
□	2018-02-14T16:10:41	Network	[redacted]
□	2018-02-14T16:11:02	Network	[redacted]
□	2018-02-14T16:11:02	Network	[redacted]

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

Refer to Reconstruct an Event in the Events View and Analyze Events in the Events View to learn how to work in the Events view.

Refining the Results Set

When conducting an investigation, results load faster and it is easier to find what you are looking for if you refine the results to get a smaller number of results. In addition, limiting the time range and submitting a good query gives you more relevant results to answer the question at hand. Use a combination of the methods described in the rest of this section to get the information you need quickly.

- Use Meta Groups to Focus on Relevant Meta Keys
- Use Columns and Column Groups in the Events List
- Use Query Profiles to Encapsulate Common Areas for Investigation
- Filter Results in the Events View
- Filter Results in the Navigate View
- Filter Results in the Legacy Events View
- Create a Query in the Navigate and Legacy Events Views
- View and Modify Queries Using URL Integration
- Search for Text Patterns in the Navigate and Legacy Events Views

Use Meta Groups to Focus on Relevant Meta Keys

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 Navigate view Values panel. A fresh installation of NetWitness Platform includes built-in meta groups to help you find interesting data sets in Investigate. The built-in 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 a built-in 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.

Built-In Meta Groups

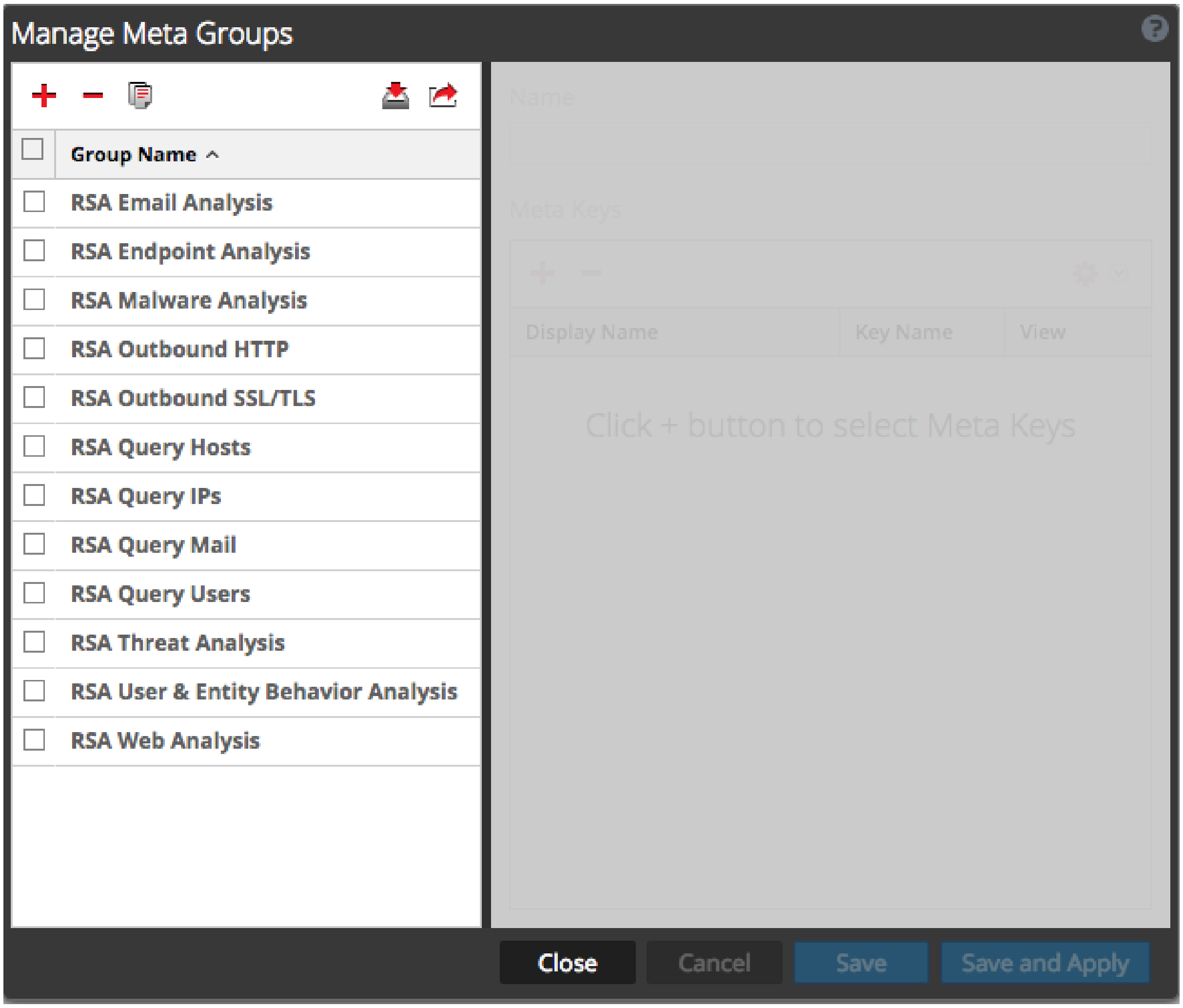
RSA NetWitness Platform has built-in meta groups that are available immediately after installation. The built-in meta groups are useful to focus an investigation on common use cases and to support threat detection using the RSA Hunting Pack. These are the built-in meta groups:

- 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 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 & 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.

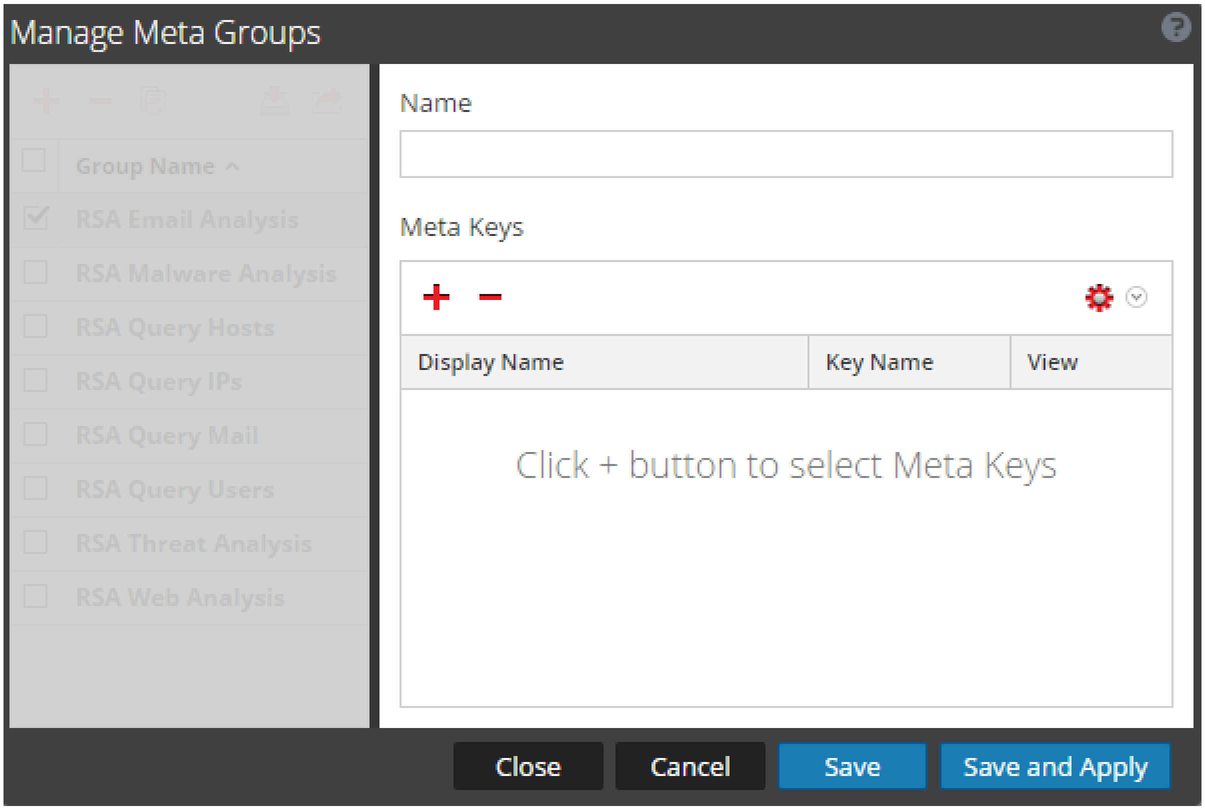
Create a Meta Group and Add Meta Keys

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 built-in 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.



□	Group Name ^
□	RSA Email Analysis
□	RSA Endpoint Analysis
□	RSA Malware Analysis
□	RSA Outbound HTTP
□	RSA Outbound SSL/TLS
□	RSA Query Hosts
□	RSA Query IPs
□	RSA Query Mail
□	RSA Query Users
□	RSA Threat Analysis
□	RSA User & Entity Behavior Analysis
□	RSA Web Analysis

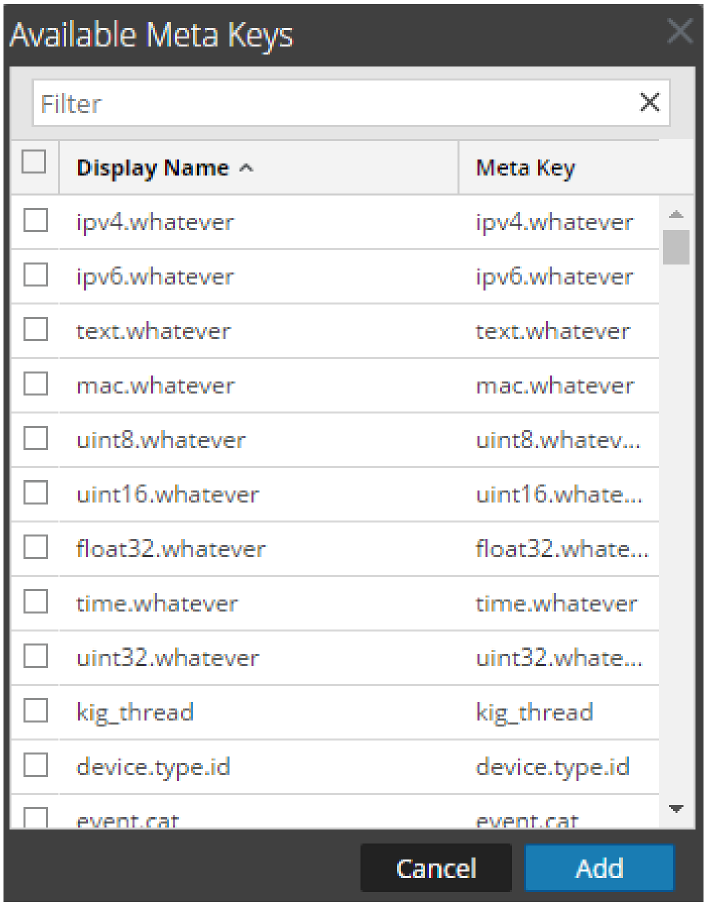
2. In the toolbar at the top of the Meta Groups list, click +.
   The form to the right opens for editing.



Click + button to select Meta Keys

3. Type a name for the new meta group in the **Name** field.

4. In the **Meta Keys** toolbar, click +.
   The Available Meta Keys dialog is displayed, with keys in alphabetical order.



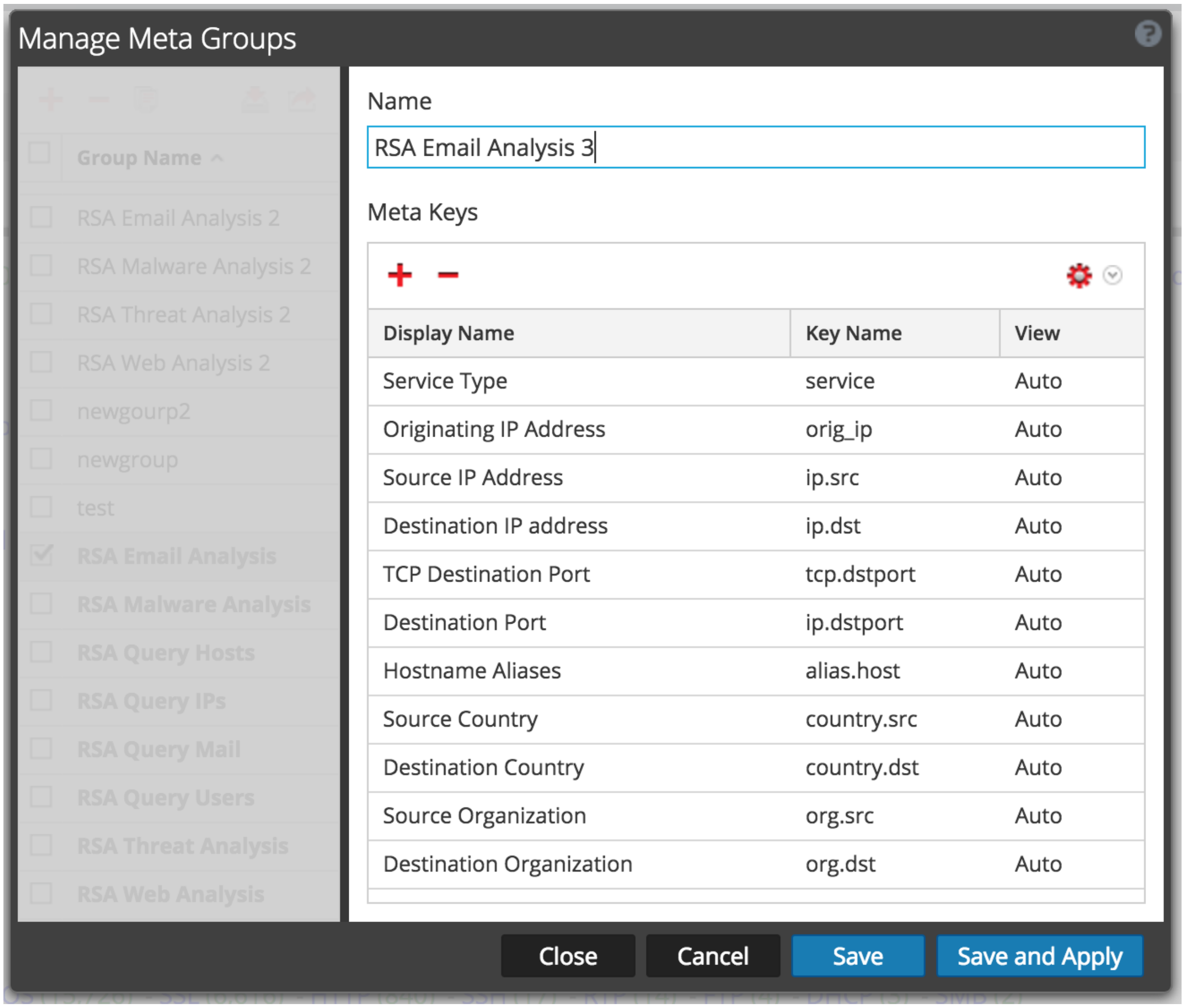
□	Display Name ^	Meta Key
□	ipv4.whatever	ipv4.whatever
□	ipv6.whatever	ipv6.whatever
□	text.whatever	text.whatever
□	mac.whatever	mac.whatever
□	uint8.whatever	uint8.whatev...
□	uint16.whatever	uint16.whate...
□	float32.whatever	float32.whate...
□	time.whatever	time.whatever
□	uint32.whatever	uint32.whate...
□	kig_thread	kig_thread
□	device.type.id	device.type.id
□	event.cat	event.cat

5. To filter the list of meta keys, type a word or phrase in the **Filter** field and press **Enter**.
   The list displays matching meta keys based on a case-insensitive search. Delete the filter text and press **Enter** to remove the filter.
6. 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.
7. (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.
8. 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.
9. Click **Close**.

Duplicate and Edit a Built-In Meta Group

If you want to customize a built-in meta group, you need to duplicate the group and then edit the duplicate.

1. Select a built-in 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 built-in group.



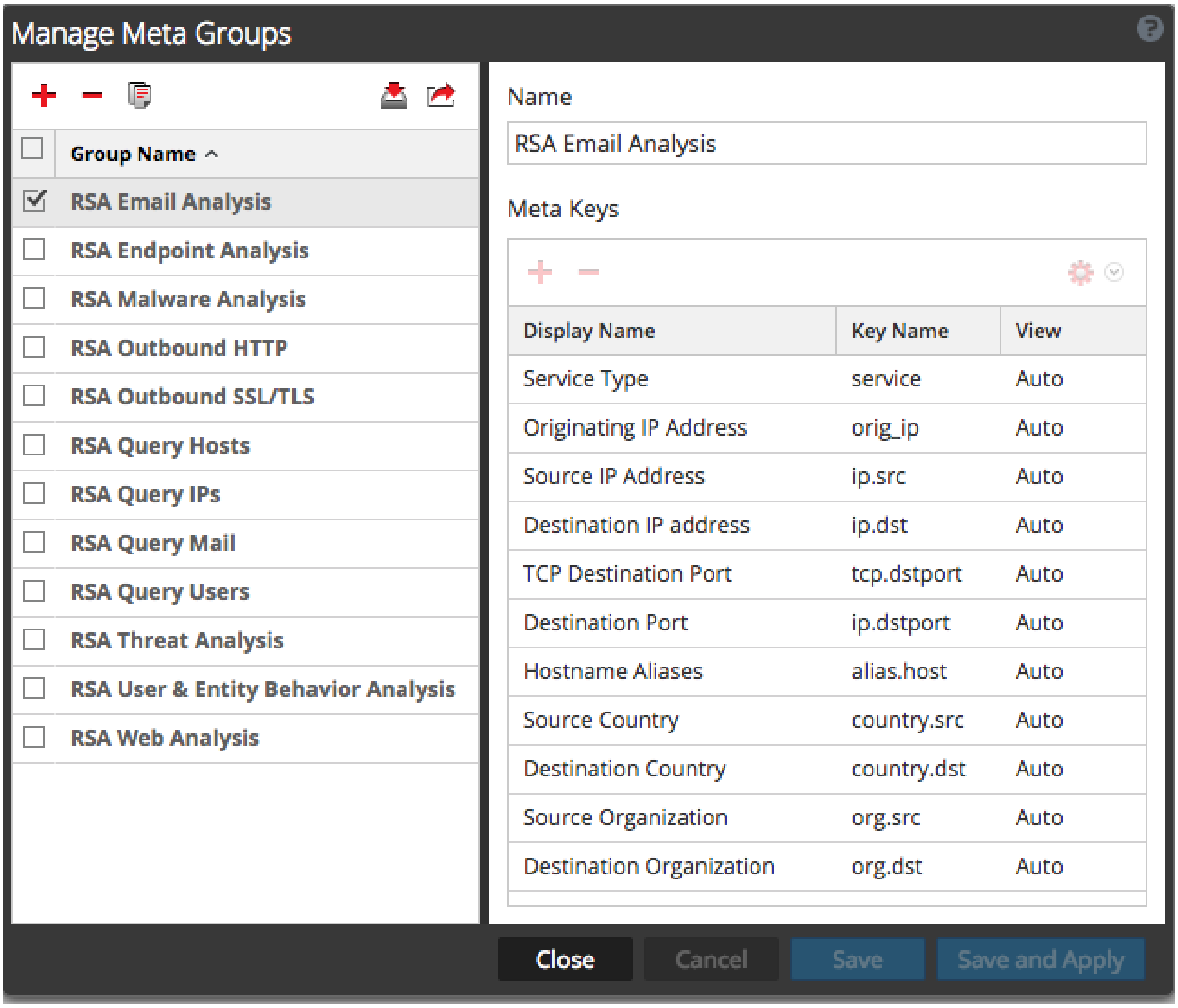
Name: RSA Email Analysis 3

Display Name	Key Name	View
Service Type	service	Auto
Originating IP Address	orig_ip	Auto
Source IP Address	ip.src	Auto
Destination IP address	ip.dst	Auto
TCP Destination Port	tcp.dstport	Auto
Destination Port	ip.dstport	Auto
Hostname Aliases	alias.host	Auto
Source Country	country.src	Auto
Destination Country	country.dst	Auto
Source Organization	org.src	Auto
Destination Organization	org.dst	Auto

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.



	Group Name ^
☑	RSA Email Analysis
□	RSA Endpoint Analysis
□	RSA Malware Analysis
□	RSA Outbound HTTP
□	RSA Outbound SSL/TLS
□	RSA Query Hosts
□	RSA Query IPs
□	RSA Query Mail
□	RSA Query Users
□	RSA Threat Analysis
□	RSA User & Entity Behavior Analysis
□	RSA Web Analysis

Name: RSA Email Analysis

Meta Keys

Display Name	Key Name	View
Service Type	service	Auto
Originating IP Address	orig_ip	Auto
Source IP Address	ip.src	Auto
Destination IP address	ip.dst	Auto
TCP Destination Port	tcp.dstport	Auto
Destination Port	ip.dstport	Auto
Hostname Aliases	alias.host	Auto
Source Country	country.src	Auto
Destination Country	country.dst	Auto
Source Organization	org.src	Auto
Destination Organization	org.dst	Auto

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 **Yes**.
   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:

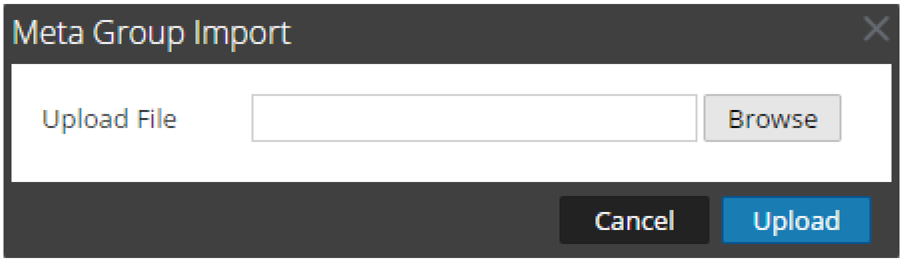
1. In the **Meta Groups** list, select one or more groups to be exported.
2. Click ↗.
   The selected groups are downloaded to your local file system as a **MetaGroups.jsn file**. Every download of meta groups has the same name with a numeral appended to avoid overwriting previous downloads.

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.

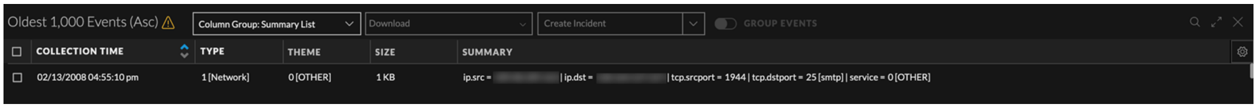


2. Click **Browse** and navigate to the directory on your local file system where the downloaded `MetaGroups.jsn` files are stored. Select a file and click **Open**.
   The filename is displayed in the Upload File field.

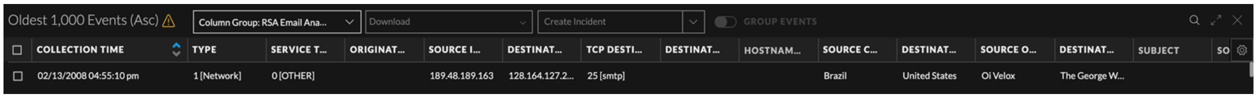
3. Click **Upload**.
   The upload process begins, and a message indicates that the upload was successful. The meta groups are added to Meta Group list. If the file is a duplicate of an existing meta group, a dialog tells you that the meta group already exists.

Use Columns and Column Groups in the Events List

When the events list in Investigate is populated with events, each column lists the values returned for a meta key. Changing the meta keys displayed in the events list is a useful method of narrowing the focus of your investigation. For example, compare these two figures showing the same set of events with different columns. The first figure has five columns, **Collection Time**, **Type**, **Theme**, **Size**, and **Summary**. These are just the basic information, not specialized in any way. The second figure has many more columns that contain information useful when investigating email; you can scroll to the right to see the additional columns.



☐	COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
☐	02/13/2008 04:55:10 pm	1 [Network]	0 [OTHER]	1 KB	ip.src = [redacted] | ip.dst = [redacted] | tcp.srcport = 1944 | tcp.dstport = 25 [smtp] | service = 0 [OTHER]



☐	COLLECTION TIME	TYPE	SERVICE T...	ORIGINAT...	SOURCE I...	DESTINAT...	TCP DESTI...	DESTINAT...	HOSTNAM...	SOURCE C...	DESTINAT...	SOURCE O...	DESTINAT...	SUBJECT	SO
☐	02/13/2008 04:55:10 pm	1 [Network]	0 [OTHER]		189.48.189.163	128.164.127.2...	25 [smtp]			Brazil	United States	Oi Velox	The George W...		

You can adjust the events list as you work, selecting different columns to be displayed, rearranging the order of the columns, changing the width of the columns, and choosing a column by which the list is sorted. Manual adjustments are easy to make if you know which meta keys are relevant, but they apply only to the current session.

To improve your ability to see relevant meta keys quickly when looking at events in the Legacy Events view and the Events view, you can change the set of meta keys displayed by applying a column group. A column group defines the meta keys or meta entities that are displayed as columns, the position of the column in the Events list, and the default width of the column. Column groups are useful in themselves, and they become even more useful when you combine them with meta groups and preQueries to define query profiles (see Use Query Profiles to Encapsulate Common Areas for Investigation).

Note: Version 11.4 has a single Events view, which was known as the Event Analysis view in prior versions. The Legacy Events view from Versions 11.3 and earlier is still available when your administrator enables the view as described in the *System Configuration Guide*. If the Legacy Events view is enabled, both views are available in the Investigate submenu.

The same column groups are shared between the Legacy Events view and the Events view and are visible globally to all users. When importing a column group, the imported group is limited to the available meta keys for the service being investigated.

Large column groups can have a performance impact when loading data because the values for each meta key are loaded in the events list. To minimize impact on performance, the Events view has a fixed limit on the number of meta keys in a column group. The maximum number of meta keys in a column group is 40. Because default keys are included you may see more than 40 displayed on the screen. A column group must have at least one column. Meta keys that are not in the selected column group are not loaded in the events list. By default we load all columns in the group, but only 15 are displayed by default.

The Legacy Events view does not have a limit on the number of meta keys in a column group, and may have more than 40 meta keys in a column group. If you apply a column group with more than 40 meta keys that was created in the Legacy Events view, all columns are loaded in the Events view. However, when you edit a column group that exceeds the limit, the number of columns must be reduced to comply with the fixed limit of 40.

Note: In Version 11.3, column groups are created and managed in the Events view and available for use in the Event Analysis view. All existing column groups, both built-in and custom, are available in the 11.4 Events view. The complete column group management functionality is available in the Legacy Events view, and all functionality except cloning, importing, and exporting column groups is available in the 11.4 Events view.

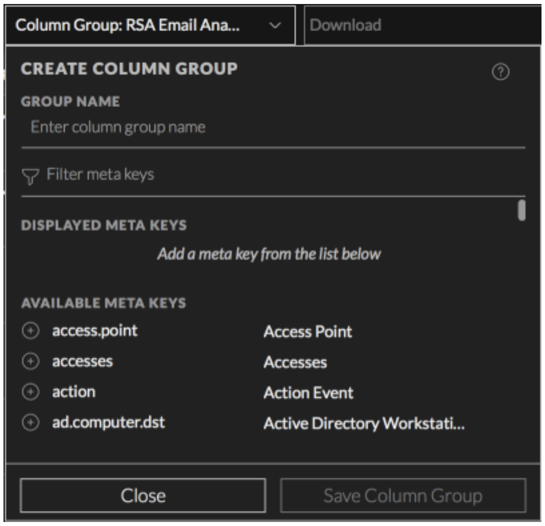
NetWitness Platform has built-in column groups that include useful meta keys for specific types of investigation. The built-in groups cannot be edited or deleted, but you can create a copy of the group and edit the copy. The column groups are listed in alphabetical order in the Column Group menu in a way that makes built-in groups distinguishable from custom groups that you imported or created. In the Legacy Events view, "RSA" precedes the name of built-in column groups. In the Events view (Version 11.4 and later), RSA precedes the name and the group is marked by the lock symbol (🔒). These are the built-in column groups.

- **RSA Email Analysis**: Includes meta keys that are useful when investigating email-related metadata.
- **RSA Endpoint Analysis**: Includes meta keys that are useful when investigating endpoint-related metadata.
- **RSA Malware Analysis**: Includes meta keys that are useful when investigation potential malware.
- **RSA Outbound HTTP**: Includes meta keys that are useful when investigating Outbound HTTP-related metadata.
- **RSA Outbound SSL/TLS**: Includes meta keys that are useful when investigating Outbound SSL/TTS analysis-related metadata.
- **RSA Threat Analysis**: Includes meta keys that mark potential threats in the data set.
- **RSA User and Entity Behavior Analysis**: Includes meta keys that are useful when investigating UEBA data.
- **RSA Web Analysis**: Includes meta keys that mark anomalies in web traffic.
- **Summary List**: Includes meta keys that are useful in a general investigation. This is the default column group.

You can create custom column groups to support scenarios that you use frequently while working in Investigate. If you edit a custom column group, your changes are applied globally. If you delete a custom column group, the group is deleted and no longer available for all analysts. 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.

Dialogs for Managing Column Groups

While the functionality of column groups is similar in the Legacy Events view and the Events view, the user interface and some of the procedures are different. The following figures illustrate the (Events view) Create Column Group dialog and the (Legacy Events view) Manage Column Groups dialog.



Column Group: RSA Email Ana... | Download

CREATE COLUMN GROUP

GROUP NAME

Enter column group name

Filter meta keys

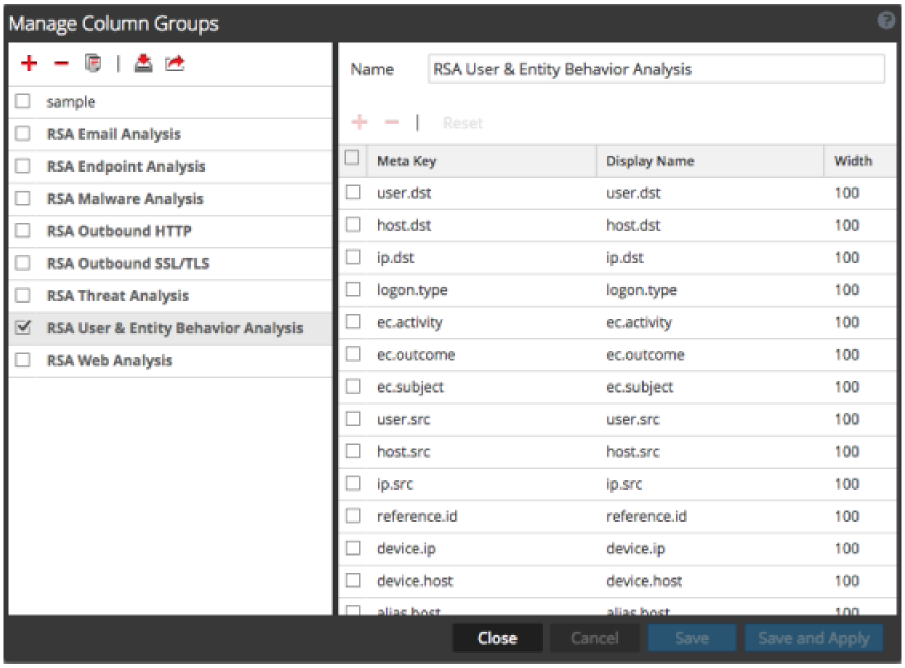
DISPLAYED META KEYS

Add a meta key from the list below

AVAILABLE META KEYS

⊕ access.point	Access Point
⊕ accesses	Accesses
⊕ action	Action Event
⊕ ad.computer.dst	Active Directory Workstati...

Close | Save Column Group



Manage Column Groups

- □ sample
- □ RSA Email Analysis
- □ RSA Endpoint Analysis
- □ RSA Malware Analysis
- □ RSA Outbound HTTP
- □ RSA Outbound SSL/TLS
- □ RSA Threat Analysis
- ☑ RSA User & Entity Behavior Analysis
- □ RSA Web Analysis

Name: RSA User & Entity Behavior Analysis

Reset

□	Meta Key	Display Name	Width
□	user.dst	user.dst	100
□	host.dst	host.dst	100
□	ip.dst	ip.dst	100
□	logon.type	logon.type	100
□	ec.activity	ec.activity	100
□	ec.outcome	ec.outcome	100
□	ec.subject	ec.subject	100
□	user.src	user.src	100
□	host.src	host.src	100
□	ip.src	ip.src	100
□	reference.id	reference.id	100
□	device.ip	device.ip	100
□	device.host	device.host	100
□	alias.host	alias.host	100

Close | Cancel | Save | Save and Apply

Using options in the Create Column Group dialog and the Column Group Details dialog, you can:

- See the details of a column group.
- Create, edit, and delete custom column groups.

Using options In the Manage Column Groups dialog, you can do all of above and these additional functions:

- Clone and edit the clone of a built-in or custom column group.
- Import and export a column group.

The rest of this topic provides instructions for working with column groups in the 11.4 Events view, the 11.3 and earlier Event Analysis view, and the Legacy Events view.

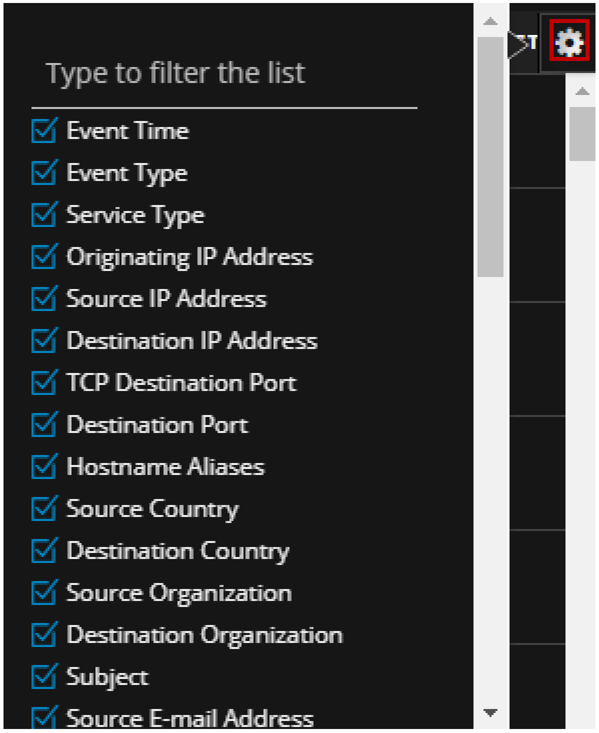
Work with Columns and Column Groups in the 11.4 Events View

After the upgrade to Version 11.4, all of the existing column groups -- both built-in and custom -- are available for management in the Events view. Unless noted, the procedures in this section are for the Events view.

Manually Select Columns to Display and Adjust Column Order and Width

> **Note:** The Column Selector was also available in the 11.3 Event Analysis view. If a column group includes a column for a meta key that your administrator has blacklisted (hidden), the data for that column cannot be displayed. The column is not available in the Column Selector and is not displayed in the Events panel.

1. With the Events list open and a column group applied, click ⚙ to display the column selector.

   Type to filter the list

   ☑ Event Time
   ☑ Event Type
   ☑ Service Type
   ☑ Originating IP Address
   ☑ Source IP Address
   ☑ Destination IP Address
   ☑ TCP Destination Port
   ☑ Destination Port
   ☑ Hostname Aliases
   ☑ Source Country
   ☑ Destination Country
   ☑ Source Organization
   ☑ Destination Organization
   ☑ Subject
   ☑ Source E-mail Address

2. Select the meta keys or enter the name of a meta key that you want to display in additional columns.
3. Deselect the meta keys that you do not want to display in a column.
   The data is redisplayed using the selected columns.
4. To change the width of the columns in the events list, hover the cursor over the column title and drag the column divider to the right or the left.
5. To rearrange the order of the columns across the top of the events list, hover the cursor over the column title and drag the column to the right or the left.
   The changes that you make in the events list are in effect during the current session and are not

retained as part of the column group. The next time the column group is applied, the original composition and order of columns is applied.

Select a Column for Sorting Events in the Events Panel

Note: You can sort events in the Events panel after results have finished loading if all connected services are updated to 11.4. or later. Sorting by column is disabled when any connected service is running an earlier version of NetWitness Platform. Version 11.4.1 has more visible sorting toggles in the column heads and the ability to view results without sorting, but otherwise it functions the same as in Version 11.4.

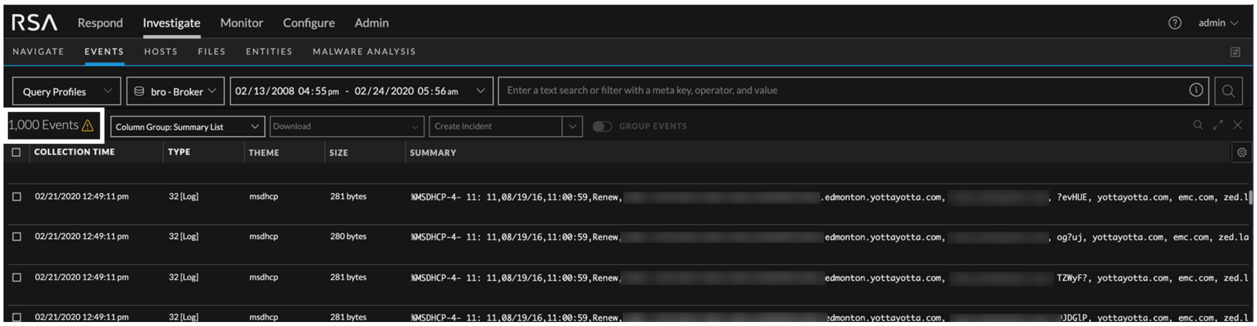
You can change the order of the events list in the Events panel based on the value for a meta key in the event. Each column title represents a meta key, and the column is populated by the values found for the meta key in the displayed events. In Version 11.4, the events in the Events panel are sorted using the method selected in the Event Preferences dialog: Ascending or Descending. If no sort method is selected, the default order is ascending (see Configure the Events View). In Version 11.4.1, the events in the Events panel are sorted only when the sort preference in the Event Preferences dialog is selected and is either Ascending or Descending. The events are not sorted if you do not have a sort preference selected under Events Preferences or if you selected Unsorted.

Sortability of a column is based on the definition of the meta key in the Broker and Concentrator index files. Columns for meta keys that are indexed by value are sortable. If the meta key is not indexed, is indexed by meta key, or has multiple values in the same event, it is not sortable.

- These are some examples of keys that are indexed by value and sortable: `time`, `eth.type`, `city.src`, `ip.src`, `ipv6.dst`, and `ipv6.src`.
- Meta entities are not sortable. For example, the meta entity `ipv6.all` is not sortable because it includes `ipv6.dst` and `ipv6.src`, and a single event has both `ipv6.dst` and `ipv6.src`.
- These are some examples of multiple value keys, which cannot be sorted: `filename`, `filetype`, and `attachment`. A single event can have more than one file and therefore more than one value for `filename`, `filetype`, and `attachment`.
- These are some examples of meta keys that cannot be sorted because they are not indexed or not indexed at the values level: `password`, `query`, and `size`.

Version 11.4.1 Sorting by Column

The initial view of the Events list with the sorting preference set to Unsorted and no column sorting has an event count in the title, with no indication of a sorting method applied to a column. In this case more than 1000 events matched the query, and only 1000 events as processed by the Core services are displayed. Clicking the amber warning triangle displays an explanation. If the event sorting preference is set to Ascending, the count label is "Oldest 1,000 Events." If the event sorting preference is set to Descending, the count label is "Newest 1,000 Events." Refer to Configure the Events View for more information about the sorting preference.



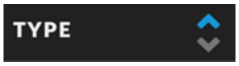
02/13/2008 04:55 pm - 02/24/2020 05:56 am

1,000 Events ⚠

□	COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
□	02/21/2020 12:49:11 pm	32 [Log]	msdhcp	281 bytes	%MSDHCP-4- 11: 11,08/19/16,11:00:59,Renew, [redacted] .edmonton.yottayotta.com, [redacted] , ?evHUE, yottayotta.com, emc.com, zed.l
□	02/21/2020 12:49:11 pm	32 [Log]	msdhcp	280 bytes	%MSDHCP-4- 11: 11,08/19/16,11:00:59,Renew, [redacted] edmonton.yottayotta.com, [redacted] , og?uj, yottayotta.com, emc.com, zed.la
□	02/21/2020 12:49:11 pm	32 [Log]	msdhcp	281 bytes	%MSDHCP-4- 11: 11,08/19/16,11:00:59,Renew, [redacted] edmonton.yottayotta.com, [redacted] TZWyF?, yottayotta.com, emc.com, zed.l
□	02/21/2020 12:49:11 pm	32 [Log]	msdhcp	281 bytes	%MSDHCP-4- 11: 11,08/19/16,11:00:59,Renew, [redacted] edmonton.yottayotta.com, [redacted] JDGlP, yottayotta.com, emc.com, zed.l

When you move the mouse over a column title, sortable columns have a pair of arrows after the column title, one pointing up for ascending and one pointing down for descending (⇅). You can choose one sort column and the direction of the sort. A blue up arrow (▲) indicates that ascending sort order is in effect; which means the earliest events or the lowest numbers, or the text strings beginning with an 'A' appear first. A blue down arrow (▼) indicates that descending sort order is in effect; which means the latest events or the highest numbers, or the text strings beginning with a 'Z' appear first.

- When a column has a blue arrow, you can click the white arrow to change the sort order. When you change the sort order, a blue progress bar is displayed in the Events list title bar to show progress. As sorting begins, there is a short segment on the left side of the window; as sorting progresses the blue color extends to the right across the entire title bar. The directional arrow does not change until the events are re-sorted in the chosen sort order.
- To change the column to unsorted, you can click the blue arrow. Both arrows are white now to show that the column is unsorted. This figure shows the Type column sorted in ascending order.

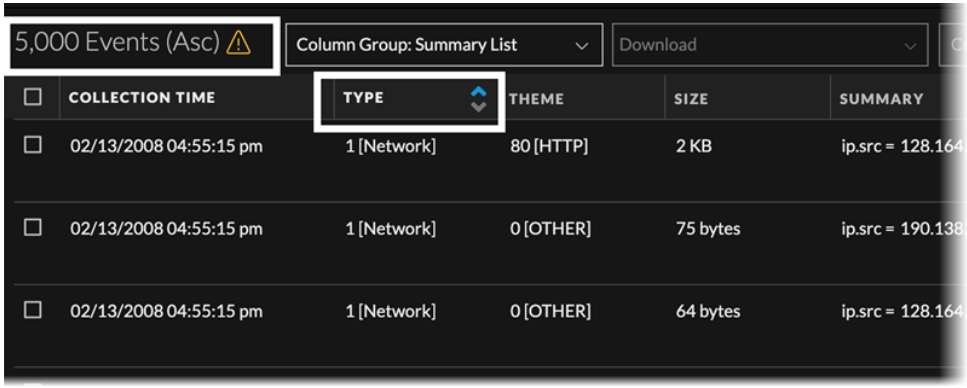
- If a column is not sortable, no arrow is displayed when you hover the mouse over the column title. Instead a tooltip explains why it is not sortable.

Sorting on a column is done on the client side without re-executing the query if the number of displayed results is less than the events limit set by the administrator. If there are more results that are not displayed because the number of results exceeded the events limit, a new query is submitted with the new sort order, and the same service, time range, and filters. The current results are removed, a spinner indicates progress, the Cancel button becomes available, the reconstruction closes, and progress is visible in the Query console.

Note: The re-sorting of events takes place in the browser when the number of results of the original query is less than the event display threshold.

To change the sort order or the sort column:

1. Move the mouse over the column titles to find a sortable column.
   If a column is not sortable, a tooltip that explains the reason is displayed.
2. To sort the list based on a column, move the mouse over a sortable column and click one of the arrows (⇅).
   The arrow turns blue and the events are reloaded in the selected order. If both arrows are white, the column is not being used to sort the events list. If one arrow is blue, the column is being used to sort the events list, and the sort order (Asc or Desc) is appended to the events count in the title bar. This figure shows a column sorted in ascending order. When a column is descending order, (Desc) is appended to the event count.



5,000 Events (Asc) ⚠ | Column Group: Summary List | Download

□	COLLECTION TIME	TYPE ⇅	THEME	SIZE	SUMMARY
□	02/13/2008 04:55:15 pm	1 [Network]	80 [HTTP]	2 KB	ip.src = 128.164
□	02/13/2008 04:55:15 pm	1 [Network]	0 [OTHER]	75 bytes	ip.src = 190.138
□	02/13/2008 04:55:15 pm	1 [Network]	0 [OTHER]	64 bytes	ip.src = 128.164

   a. Click a white arrow to sort the events list in that order.
   b. Click a blue arrow to return to unsorted order.

Version 11.4 Sorting by Column

When you move the mouse over a column title, sortable columns have an up or down arrow (↑ or ↓) after the column title. You can choose one sort column and the direction of the sort. An up arrow indicates that Ascending sort order is in effect; which means the earliest events or the lowest numbers, or the text strings beginning with an 'A' appear first. A down arrow indicates that Descending sort order is in effect; which means the latest events or the highest numbers, or the text strings beginning with a 'Z' appear first. When you select a sort column, it is sorted in descending order by default, with events having a null value for the meta key first.

- A column that is being used to sort the events list has a bright white arrow indicating the direction that you can choose for sorting: click ↑ to change to Ascending or ↓ to change to Descending order. When you click ↑ to change to Ascending sort order, the directional arrow does not change until the events are re-sorted in ascending order. The same behavior applies when you click the ↓ to change to Descending order.

- If a sortable column is not being used to sort the events list, the arrow is dimmed. If a column is not sortable, no arrow is displayed when you hover the mouse over the column title. Instead a tooltip explains why it is not sortable.
- If you click the arrow on a different column, the column is sorted in the same order as the previously active sort column. You can select a different sort order if desired.

Sorting on a column is done on the client side without re-executing the query if the number of displayed results is less than the events limit set by the administrator. If there are more results that are not displayed because the number of results exceeded the events limit, a new query is submitted with the new sort order, and the same service, time range, and filters. The current results are removed, a spinner indicates progress, the Cancel button becomes available, the reconstruction closes, and progress is visible in the Query console.

> **Note:** The re-sorting of events takes place in the browser when the number of results of the original query is less than the event display threshold. If some of those events have the exact same time, they will not change order as you might expect when you reverse the sort order.

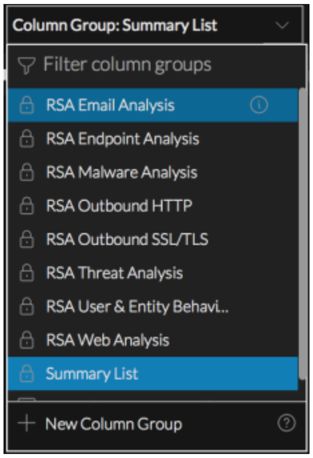
To change the sort order or the sort column:

1. Move the mouse over the column titles to find a sortable column.
   If a column is not sortable, a tooltip that explains the reason is displayed.
2. To sort the list based on a column:
   a. Move the mouse over a sortable column and click the arrow (↑ or ↓).
      The events are sorted in the correct sort order. If you hover over the column title, you can see that the arrow is no longer dimmed. A column that is being used to sort the events list has a bright white arrow that you can click to change the sorting direction.
   b. To change the sort order, click ↑ to change to Ascending or ↓ to change to Descending order.
      The direction of the arrow changes and the events are reloaded in the selected order.

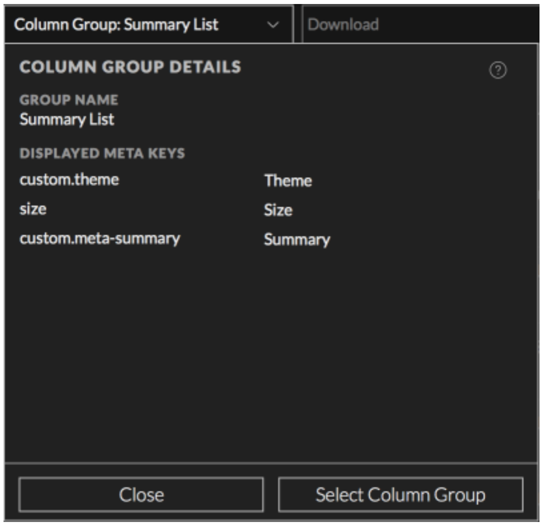
View the Meta Keys Included in a Column Group

To view details of a column group:

1. Go to **Investigate** > **Events** and click 🔍 to load events.
   The events for the default service and the default time range are loaded in the Events panel. The Summary List column group or the column group from your last session is applied to the list. The Column Group menu title includes the name of the selected column group. This figure shows the menu initially when Summary List is selected by default and the first column group in the list is highlighted.



2. Hover over the **Summary List** group and click the information icon (ⓘ) to see which columns are included in the group.
   This figure shows the columns for the Summary List. The Collection Time and Type column are always the first two columns in the Events list, but are not listed in the Column Group Details dialog.



COLUMN GROUP DETAILS

GROUP NAME
Summary List

DISPLAYED META KEYS

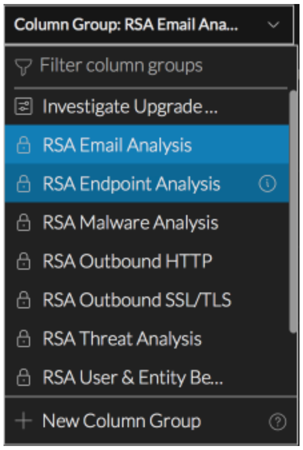
custom.theme	Theme
size	Size
custom.meta-summary	Summary

3. Do one of the following.
   a. To close the dialog, click **Close**.
   b. If you want to apply the column group, click **Select Column Group**.
      The dialog closes and the Events list is updated to reflect the selected column group.

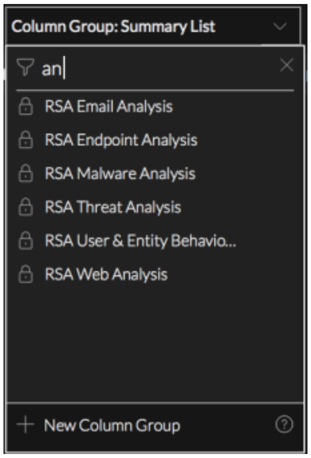
Select a Column Group

1. With the Events panel open in the 11.4 Events view, click the **Column Group** menu title.
   The menu drops down to display a list of column groups with a filtering option and a New Column Group option. The built-in column groups (except for Summary List) have an "RSA" prefix and a lock icon (🔒) to indicate that you cannot edit the groups. A custom icon (☰)precedes the name of custom column groups. The list is sorted alphabetically and the selected column group is displayed in

the menu label. The first option in the list is highlighted. The selected column group has a slightly different background color than the highlighted column group.
This figure shows the menu after RSA Endpoint Analysis was highlighted, but RSA Email Analysis is still selected. Investigate Upgrade is an example of a custom column group.



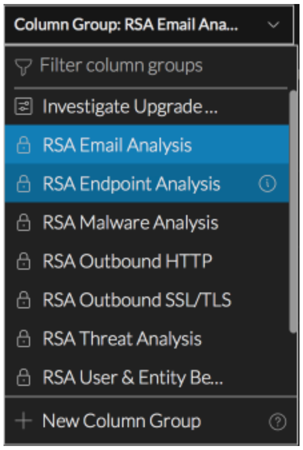
2. Do one of the following:
   a. If the highlighted group is the one you want to apply, press **ENTER**.
   b. Begin typing text in the **Filter column groups** field to search for a column group name. As you type, the list is filtered to show only the column group names that contain that string.



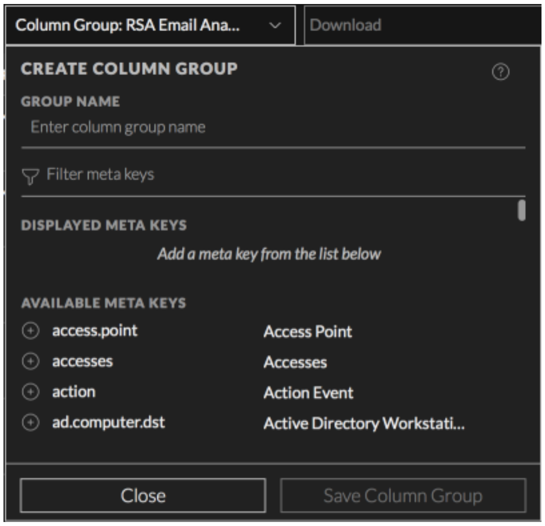
When you see the group that you want to apply, click it or use the down or up arrow to highlight it, then press **ENTER**.
The Events list is refreshed to include only columns in the selected column group, and the menu title includes the selected group name. Your selection persists when you navigate away from the Events view. The order of the columns in the Events list reflects the order of the meta keys in the column group. A column group may contain more columns that are only visible when you scroll to the right. For optimal viewing, the first 15 columns are displayed by default when you select a column group.

Create a Custom Column Group

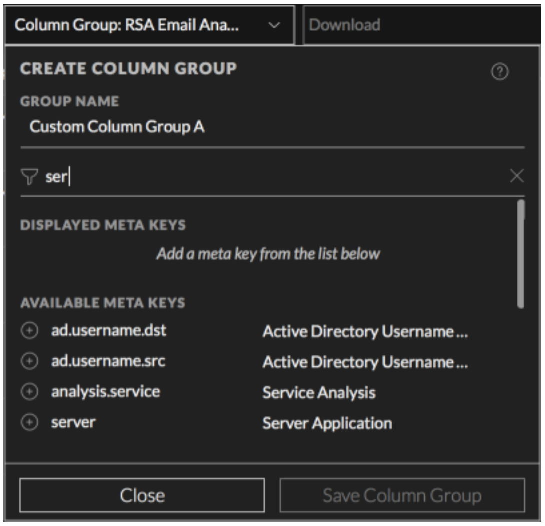
1. Go to **Investigate > Events** and submit a query to load data in the Events panel.
2. In the Events panel toolbar, click the **Column Group** menu title.
   The menu drops down to display a list of column groups with the Filter Column Groups field at the top and the + New Column Group option at the bottom. The first group in the list is highlighted. To illustrate the difference between highlighted and selected, this figure shows the menu after RSA Endpoint Analysis was highlighted, but RSA Email Analysis is still selected.

3. Select + **New Column Group**.
   The Create Column Group dialog is displayed.

4. In the **Group Name** field, type a unique name (maximum length of 256 characters) for the new column group, for example, **Custom Column Group A**.
5. To add a meta key to the column group, select and add each meta key as follows:
   a. Type a text string in the **Filter meta keys** field and look for meta keys that contain that text in the **Available Meta Keys** list.



Column Group: RSA Email Ana... | Download

CREATE COLUMN GROUP

GROUP NAME

Custom Column Group A

ser

DISPLAYED META KEYS

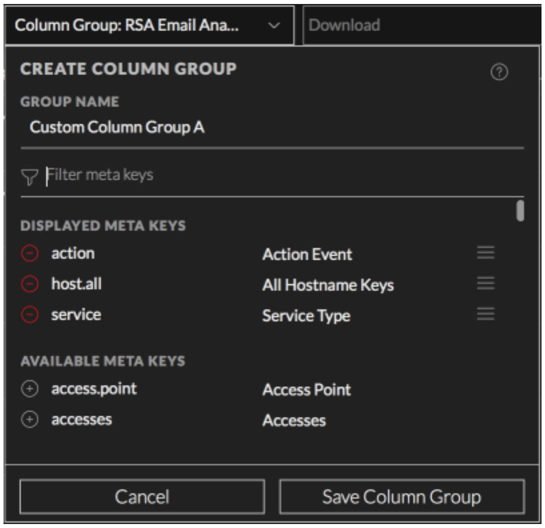
Add a meta key from the list below

AVAILABLE META KEYS

⊕ ad.username.dst	Active Directory Username ...
⊕ ad.username.src	Active Directory Username ...
⊕ analysis.service	Service Analysis
⊕ server	Server Application

Close | Save Column Group

b. When you see the meta key that you want to add, click the add icon ⊕ that precedes the meta key name.
The meta key is added to the end of the Displayed Meta Keys list. (This list is also filtered using the text you typed.) The maximum number of meta keys in a column group is 40. If you attempt to add another meta key when 40 are already included in the Displayed Meta Keys list, a message advises you that the group has the maximum number of meta keys.



Column Group: RSA Email Ana... | Download

CREATE COLUMN GROUP

GROUP NAME

Custom Column Group A

Filter meta keys

DISPLAYED META KEYS

⊖ action	Action Event	☰
⊖ host.all	All Hostname Keys	☰
⊖ service	Service Type	☰

AVAILABLE META KEYS

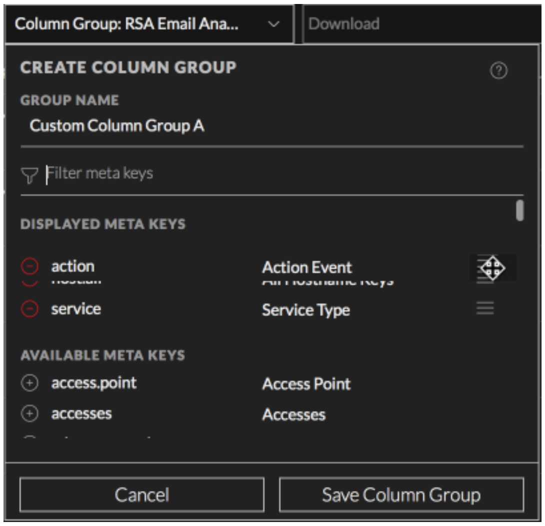
⊕ access.point	Access Point
⊕ accesses	Accesses

Cancel | Save Column Group

6. (Optional) To find and remove a meta key from the column group, type a text string in the **Filter meta keys** field and look for meta keys that contain that text in the **Dispayed Meta Keys** list. When you see the column that you want to remove, click the remove icon (⊖) that precedes the meta key name in the **Displayed Meta Keys** list.
The meta key is moved back to the Available Meta Keys list.

7. (Optional) To change the order of the displayed meta keys in the Displayed Meta Keys list, place the cursor over the list order icon (☰). When the cursor changes to the drag and drop icon (✥), drag

the meta key up or down in the list.



Custom Column Group A

action	Action Event
service	Service Type
access.point	Access Point
accesses	Accesses

8. Do one of the following:
   a. To close the dialog without creating the custom column group, click **Cancel**.
   b. To create the group, click **Save Column Group**.
   The new column group is saved and becomes available for all analysts. The buttons change to Done and Select Column Group.
9. Do one of the following:
   a. To close the dialog, click **Done**.
   b. To close the dialog and select the new column group, click **Select Column Group**.
   The new group is added to the Column Groups menu (in alphabetical order), and if you clicked Select Column Group, the Events list is updated to show the columns in the new column group.

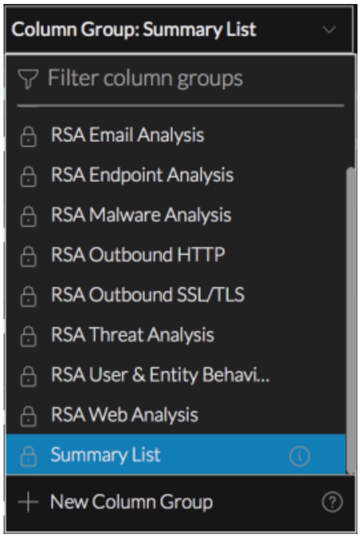
Delete a Custom Column Group

You can delete any custom column group that is not currently applied in the Events list. The built-in column groups are read only, and cannot be deleted. When you delete custom column groups, only the built-in column groups and the groups that have not been deleted, are displayed in the column group menu.

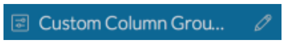
Caution: When you delete a column group, the effect is global and the group is no longer available to any analyst.

To delete a custom column group:

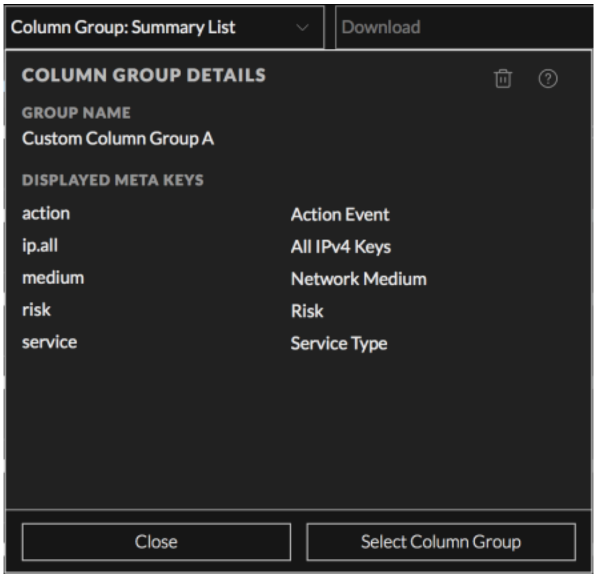
1. Go to **Investigate** > **Events** and click 🔍 to load events.
   The events for the default service and the default time range are loaded in the Events panel. The Summary List column group or the column group from your last session is applied to the list. This figure shows the initial view with the Summary List column group selected. The label on the Column Group menu includes the name of the selected column group.



2. To delete a column group, highlight a custom column group as shown in the following figure and click the edit icon (✎) to the right of the name.



3. The Column Group Details dialog opens with the details for the selected group displayed.



COLUMN GROUP DETAILS

GROUP NAME

Custom Column Group A

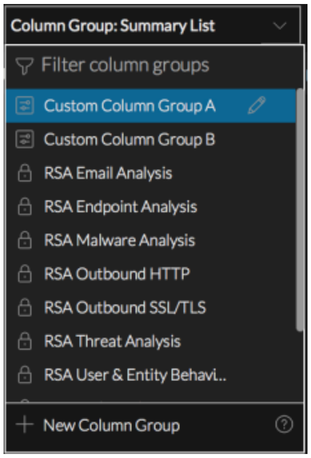
DISPLAYED META KEYS

action	Action Event
ip.all	All IPv4 Keys
medium	Network Medium
risk	Risk
service	Service Type

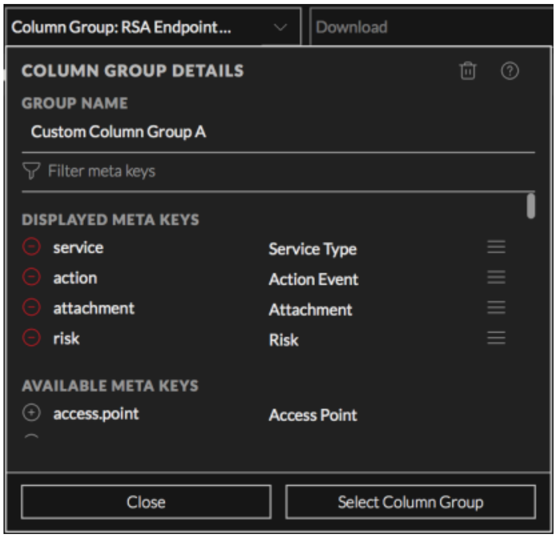
4. Click the delete group icon (🗑).
   If the column group is currently in effect, the following message is displayed: `This column group cannot be deleted because it is currently active.`
   If the column group is not in effect and is not a built-in column group, the group is deleted immediately and removed from the Column Groups menu. The column group no longer appears anywhere for any analyst working in Investigate. There is no request for confirmation before the column is deleted.

Edit a Custom Column Group

1. Go to **Investigate> Events** and submit a query to load data in the Events panel.
2. In the Events panel toolbar, click the **Column Group** menu title.
   The menu drops down to display a list of column groups with the Filter Column Groups field at the top and the + New Column Group option at the bottom. The first group on the list is highlighted, and the selected group has a light blue background.
3. Highlight the column group that you want edit. This figure shows Custom Column Group A highlighted. The edit icon is displayed to the right.



4. Click the edit icon (✎).
   The Column Group Details dialog is displayed so that you can edit the Group Name and Displayed Meta Keys. You can add or delete meta keys and rearrange the order of the meta keys in the list.



GROUP NAME
Custom Column Group A

DISPLAYED META KEYS

service	Service Type
action	Action Event
attachment	Attachment
risk	Risk

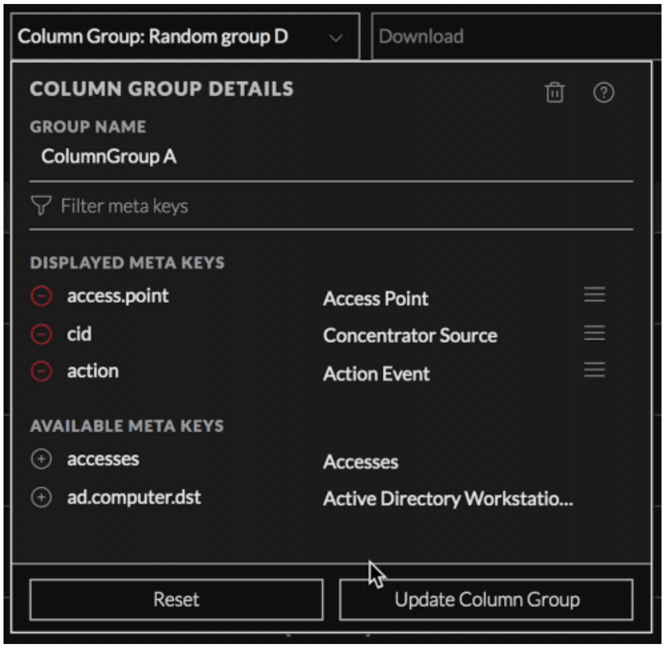
AVAILABLE META KEYS

access.point	Access Point

5. (Optional) In the **Group Name** field, edit the name of the column group.
6. (Optional) To add a meta key to the column group, select and add each meta key as follows:

a. Type a text string in the **Filter meta keys** field and look for meta keys that contain that text in the **Available Meta Keys** list. Or just scroll through the list to find the meta key.

b. When you see the meta key that you want to add, click the add icon ⊕ that precedes the meta key name.
The meta key is added to the end of the Displayed Meta Keys list. (This list is also filtered using the text you typed.) This figure shows the group name changed to Column Group C and `access.point` added to the Displayed Meta Keys list.



Column Group: Random group D

COLUMN GROUP DETAILS

GROUP NAME

ColumnGroup A

Filter meta keys

DISPLAYED META KEYS

⊖ access.point	Access Point
⊖ cid	Concentrator Source
⊖ action	Action Event

AVAILABLE META KEYS

⊕ accesses	Accesses
⊕ ad.computer.dst	Active Directory Workstatio...

7. (Optional) To find and remove a meta key from the column group, type a text string in the **Filter meta keys** field to look for meta keys that contain that text in the **Dispayed Meta Keys** list, or simply scroll through the list. When you see the column that you want to remove, click the remove icon (⊖) that precedes the meta key name in the **Displayed Meta Keys** list.
The meta key is moved back to the Available Meta Keys list.

8. (Optional) To change the order of the displayed meta keys in the Displayed Meta Keys list, place the cursor over the list order icon (☰). When the cursor changes to the drag and drop icon (✥), drag the meta key up or down in the list.

9. Do one of the following:

   a. To close the dialog without saving the changes to the custom column group, click **Reset**.

   b. To save the edits to the column group, click **Update Column Group**.
   The updated column group is saved globally for all analysts, and the buttons change to Done and Select Column Group.

10. Do one of the following:

    a. To close the dialog, click **Close**.

b. To close the dialog and select the updated column group, click **Select Column Group**.
The column group is updated, and if you clicked Select Column Group, the Events list is updated to show the columns in the new column group.

Select a Column Group and Columns (11.3 and Earlier Event Analysis View)

In the 11.3 and earlier Event Analysis view, you can select a column group to apply to the Events list. These are the built-in groups and custom column groups created in the Legacy Events view.

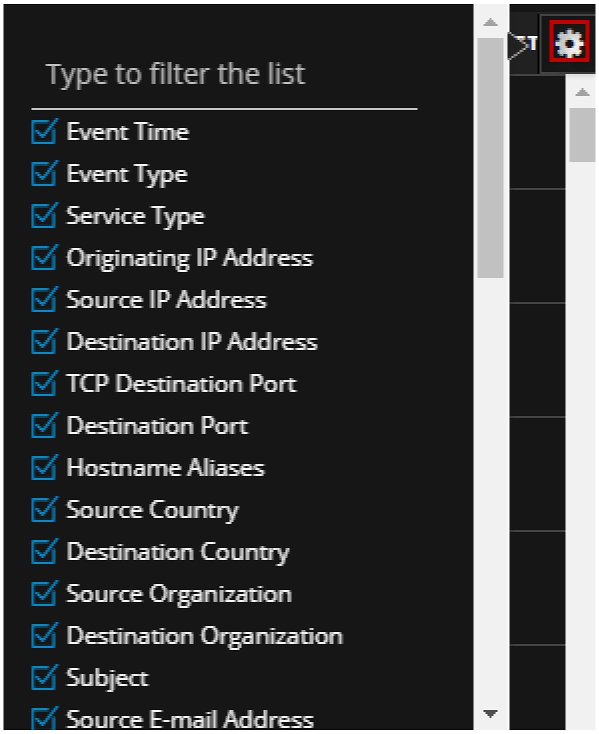
To select a column group:

Begin in the Column Group menu and do one of the following:

1. Select a column group (for example, **Summary List**).
2. To filter the list of column groups, start typing the name of the column group. Type one character and a list of column groups that contain that character is displayed; as you continue to type the list is filtered to match. When you see the column group that you want, click to select it. To clear the filter text, click **X** or delete the typed text.
The Events panel displays data in the columns that belong to the selected column group.

To select columns to display:

1. With the Events list open and a column group selected, click ⚙ to display the column selector.



Type to filter the list

☑ Event Time
☑ Event Type
☑ Service Type
☑ Originating IP Address
☑ Source IP Address
☑ Destination IP Address
☑ TCP Destination Port
☑ Destination Port
☑ Hostname Aliases
☑ Source Country
☑ Destination Country
☑ Source Organization
☑ Destination Organization
☑ Subject
☑ Source E-mail Address

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.

Work with Column Groups in the Legacy Events View

This section includes procedures for working in the 11.4 Legacy Events view (and the 11.3 Events view). Three different forms of the events list with hard-coded columns are built in and labeled as follows: Detail View, List View, Log View. You can remove columns, rearrange the order, and change the width of a column. In addition the built-in or custom column groups are available; these give you more flexibility in choosing columns.

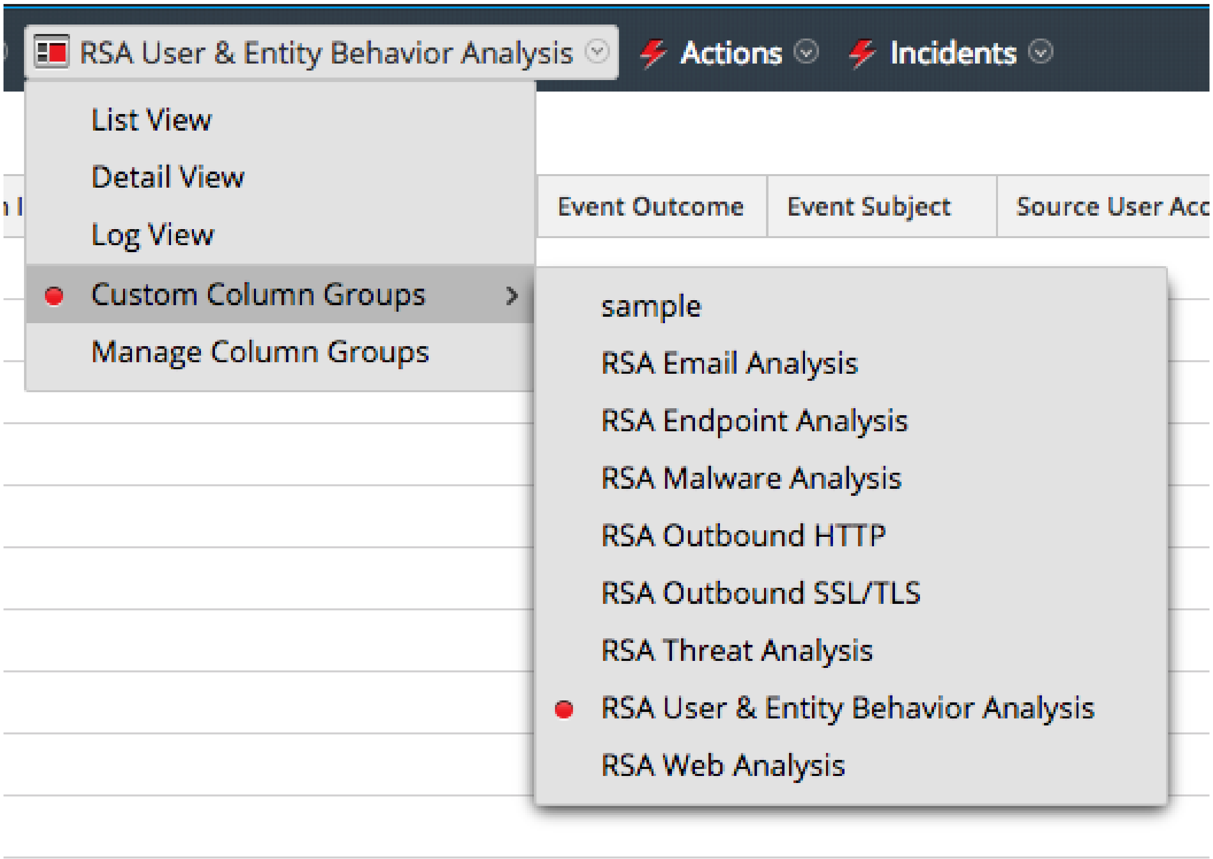
Column groups are shared globally, per service, across Investigate. Any changes you make to custom column groups are applied globally, affecting all analysts using the service. If you delete a column group, the column group is no longer available to anyone who is investigating the service.

Select a Column Group

> **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 Legacy Events view using a custom column group, you cannot change the view type (Detail, List, or Log).

To select a column group:

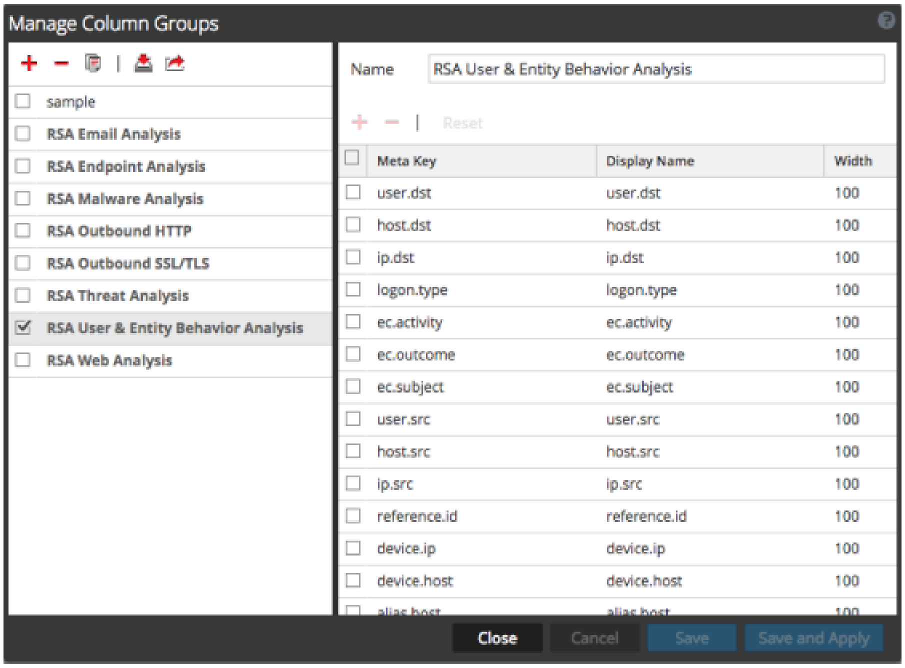
1. With the Legacy Events view open, select **Custom Column Groups** in the **View** drop-down menu.
   The menu label reflects the selected option: Detail View, List View, Log View, or the currently selected column group.



2. Select one of the column groups from the submenu.
   The Legacy Events view is refreshed to reflect the custom column group.

Create a Custom Column Group in the Legacy Events View

1. Go to **Investigate** > **Legacy 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.



- □ sample
- □ RSA Email Analysis
- □ RSA Endpoint Analysis
- □ RSA Malware Analysis
- □ RSA Outbound HTTP
- □ RSA Outbound SSL/TLS
- □ RSA Threat Analysis
- ☑ RSA User & Entity Behavior Analysis
- □ RSA Web Analysis

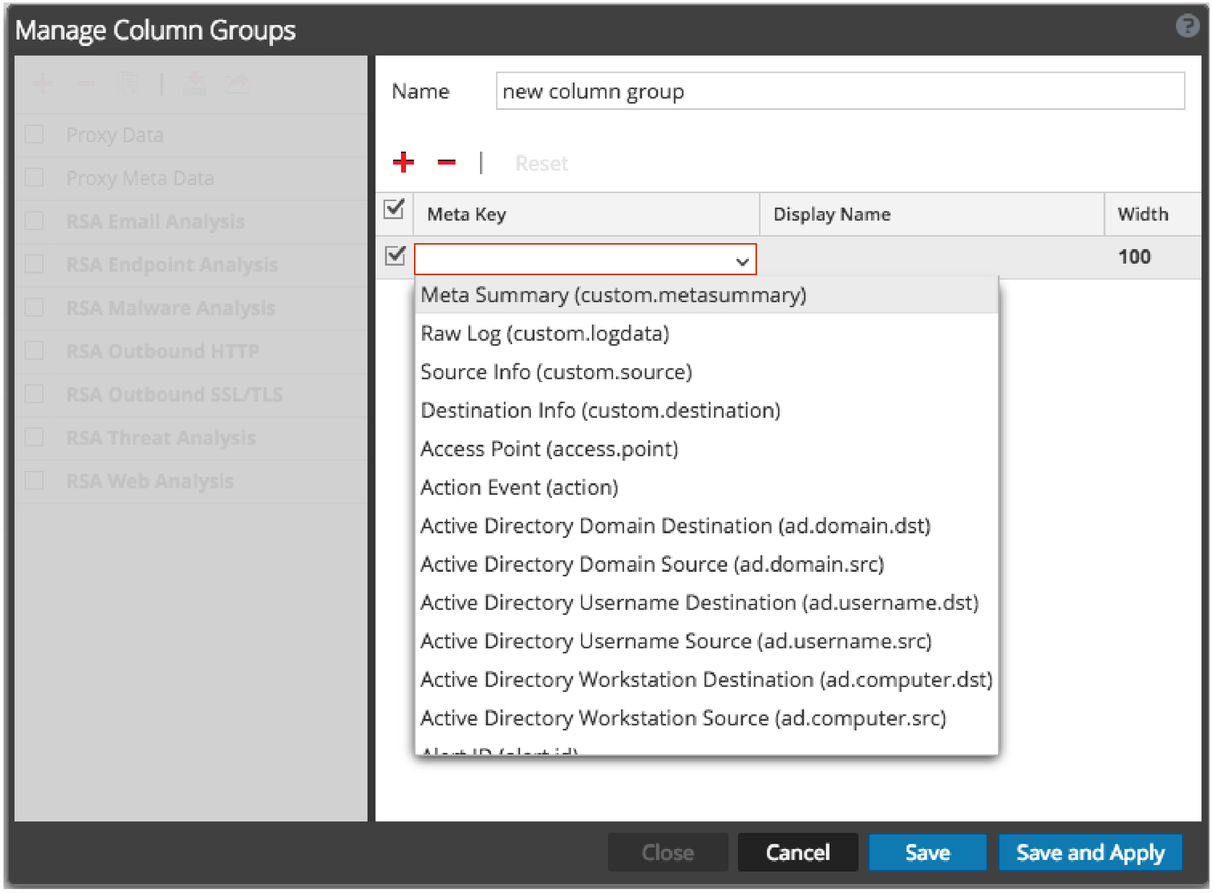
Name: RSA User & Entity Behavior Analysis

□	Meta Key	Display Name	Width
□	user.dst	user.dst	100
□	host.dst	host.dst	100
□	ip.dst	ip.dst	100
□	logon.type	logon.type	100
□	ec.activity	ec.activity	100
□	ec.outcome	ec.outcome	100
□	ec.subject	ec.subject	100
□	user.src	user.src	100
□	host.src	host.src	100
□	ip.src	ip.src	100
□	reference.id	reference.id	100
□	device.ip	device.ip	100
□	device.host	device.host	100
□	alias.host	alias.host	100

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.



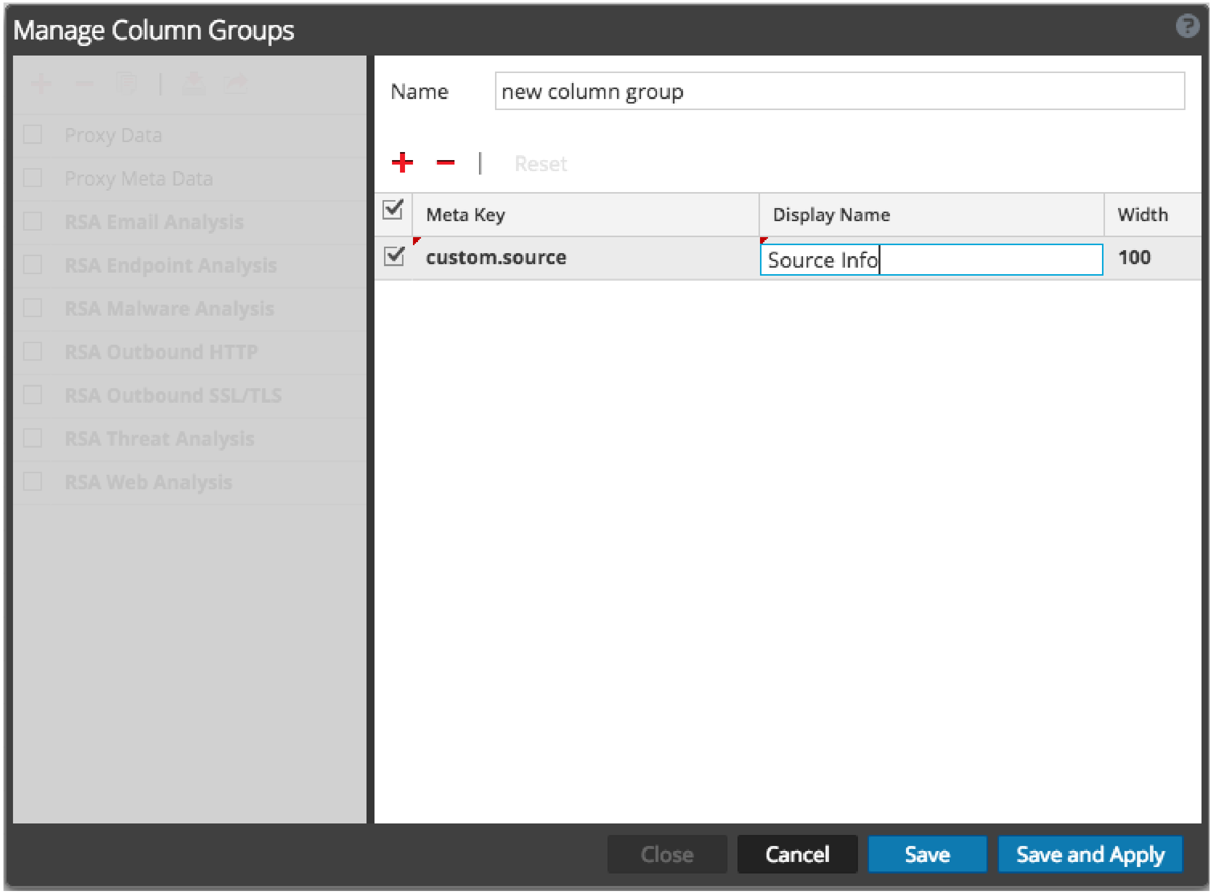
Name: new column group

☑	Meta Key	Display Name	Width
☑			100

Manage Column Groups
Proxy Data
Proxy Meta Data
RSA Email Analysis
RSA Endpoint Analysis
RSA Malware Analysis
RSA Outbound HTTP
RSA Outbound SSL/TLS
RSA Threat Analysis
RSA Web Analysis
Reset
Meta Summary (custom.metasummary)
Raw Log (custom.logdata)
Source Info (custom.source)
Destination Info (custom.destination)
Access Point (access.point)
Action Event (action)
Active Directory Domain Destination (ad.domain.dst)
Active Directory Domain Source (ad.domain.src)
Active Directory Username Destination (ad.username.dst)
Active Directory Username Source (ad.username.src)
Active Directory Workstation Destination (ad.computer.dst)
Active Directory Workstation Source (ad.computer.src)
Close
Cancel
Save
Save and Apply

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.



Name: new column group

☑	Meta Key	Display Name	Width
☑	custom.source	Source Info	100

8. (Optional) To revert to the previous settings for the column group, and undo all of your changes, click **Cancel**.

9. When ready to save, do one of the following:

   a. To save the edited column group and refresh the Legacy Events view with the column group settings, click **Save and Apply**.

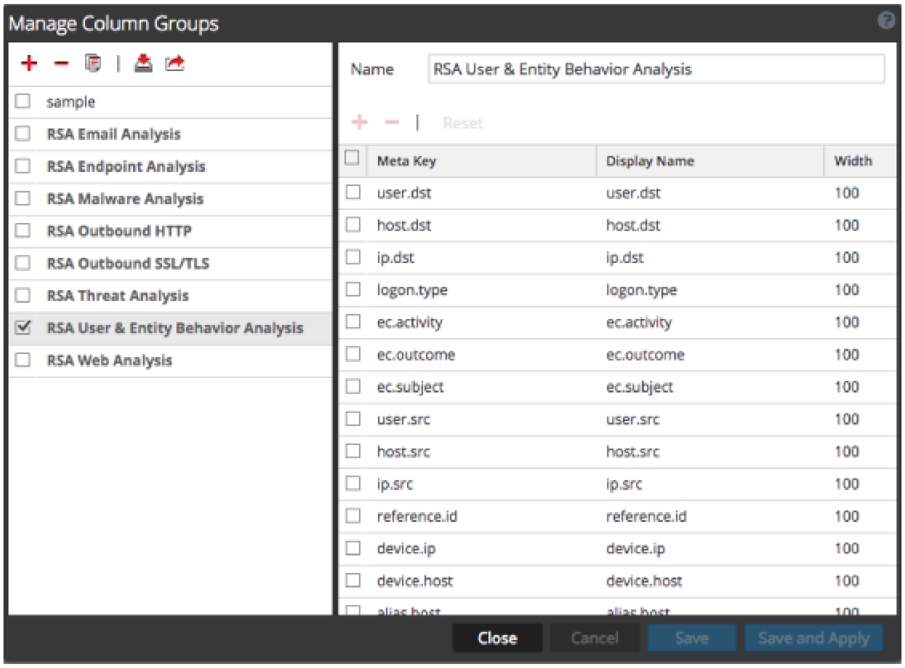
   b. To save the edited column group without refreshing the Legacy Events view, click **Save**.

Delete a Column Group (Legacy Events View)

1. Go to **Investigate** > **Legacy 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.



- □ sample
- □ RSA Email Analysis
- □ RSA Endpoint Analysis
- □ RSA Malware Analysis
- □ RSA Outbound HTTP
- □ RSA Outbound SSL/TLS
- □ RSA Threat Analysis
- ☑ RSA User & Entity Behavior Analysis
- □ RSA Web Analysis

Name: RSA User & Entity Behavior Analysis

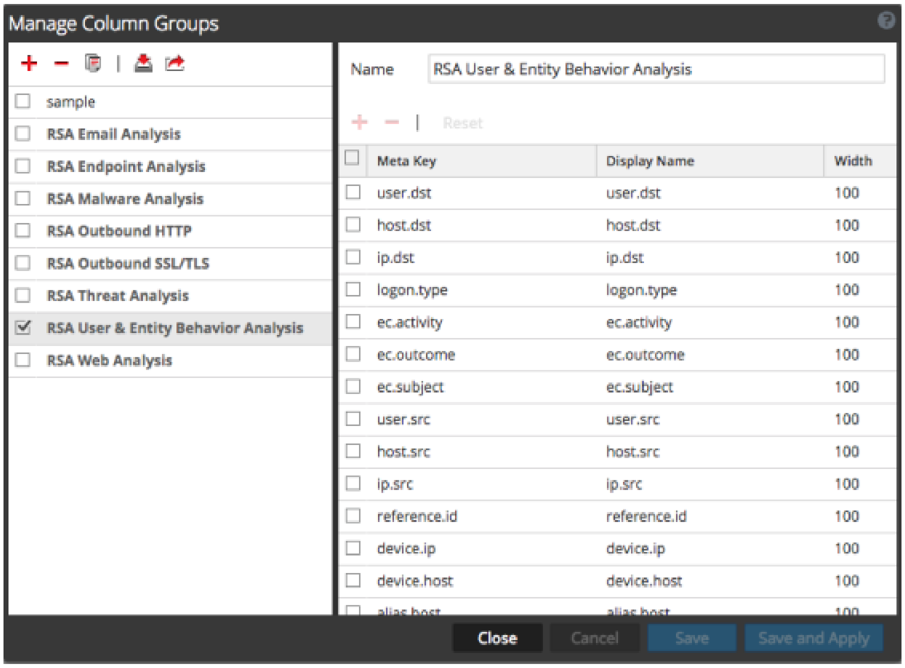
□	Meta Key	Display Name	Width
□	user.dst	user.dst	100
□	host.dst	host.dst	100
□	ip.dst	ip.dst	100
□	logon.type	logon.type	100
□	ec.activity	ec.activity	100
□	ec.outcome	ec.outcome	100
□	ec.subject	ec.subject	100
□	user.src	user.src	100
□	host.src	host.src	100
□	ip.src	ip.src	100
□	reference.id	reference.id	100
□	device.ip	device.ip	100
□	device.host	device.host	100
□	alias.host	alias.host	100

3. To delete a custom column group in the column group panel, select one or more custom column groups and click − in the toolbar.
   A confirmation request is displayed.
4. Do one of the following:
   a. To delete the column group and refresh the Legacy Events view, click **Yes**.
   b. If you decided not to delete the column group , click **No**.
      The selected column groups are deleted and no longer appear anywhere for this service in Investigate.

Edit a Column Group (Events View)

1. Go to **Investigate** > **Legacy 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.



Manage Column Groups

□	sample
□	RSA Email Analysis
□	RSA Endpoint Analysis
□	RSA Malware Analysis
□	RSA Outbound HTTP
□	RSA Outbound SSL/TLS
□	RSA Threat Analysis
☑	RSA User & Entity Behavior Analysis
□	RSA Web Analysis

Name: RSA User & Entity Behavior Analysis

□	Meta Key	Display Name	Width
□	user.dst	user.dst	100
□	host.dst	host.dst	100
□	ip.dst	ip.dst	100
□	logon.type	logon.type	100
□	ec.activity	ec.activity	100
□	ec.outcome	ec.outcome	100
□	ec.subject	ec.subject	100
□	user.src	user.src	100
□	host.src	host.src	100
□	ip.src	ip.src	100
□	reference.id	reference.id	100
□	device.ip	device.ip	100
□	device.host	device.host	100
□	alias.host	alias.host	100

3. Do one of following:

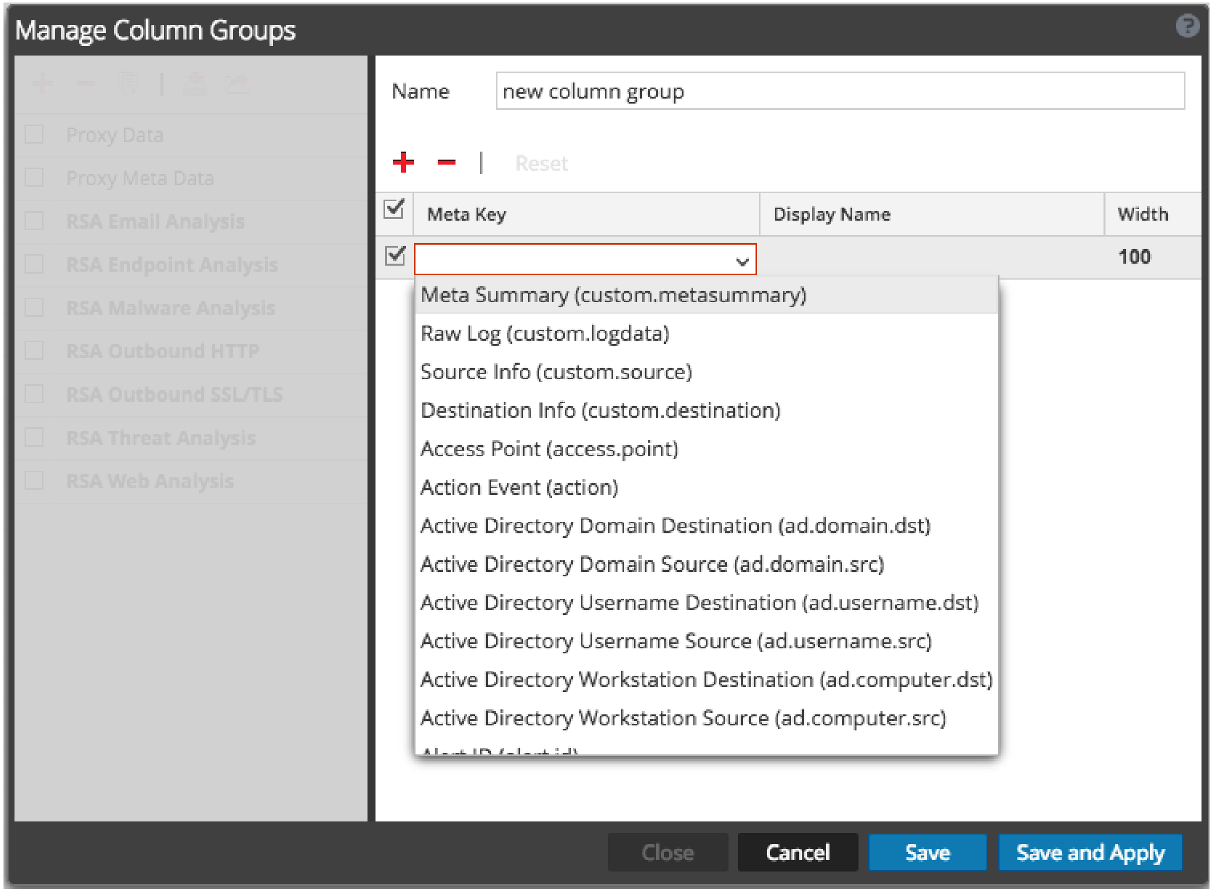
   a. To edit a custom column group in the column group panel, select the checkbox before the name. The column definition panel opens on the right.

   b. To clone and edit a built-in column group or a custom column group, select the checkbox before the name and click the clone icon (📄).
   The column definition panel opens on the right.

4. (Conditional) If you are editing a clone of a group, type the new name of the group.

5. 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.

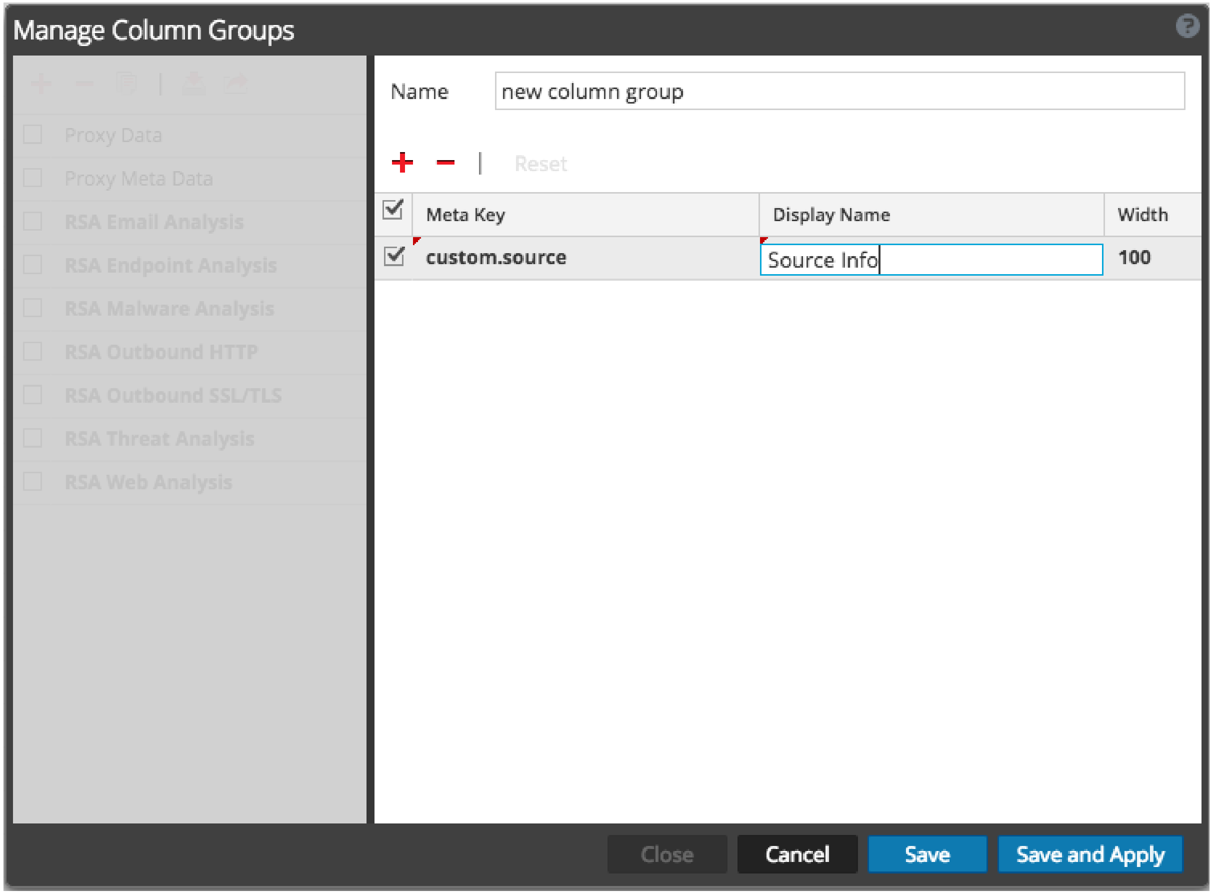

Manage Column Groups
Proxy Data
Proxy Meta Data
RSA Email Analysis
RSA Endpoint Analysis
RSA Malware Analysis
RSA Outbound HTTP
RSA Outbound SSL/TLS
RSA Threat Analysis
RSA Web Analysis
Reset
Meta Key
Display Name
Width
Meta Summary (custom.metasummary)
Raw Log (custom.logdata)
Source Info (custom.source)
Destination Info (custom.destination)
Access Point (access.point)
Action Event (action)
Active Directory Domain Destination (ad.domain.dst)
Active Directory Domain Source (ad.domain.src)
Active Directory Username Destination (ad.username.dst)
Active Directory Username Source (ad.username.src)
Active Directory Workstation Destination (ad.computer.dst)
Active Directory Workstation Source (ad.computer.src)
Alert ID (alert.id)
Close
Cancel
Save
Save and Apply

Name: new column group

☑ | | 100

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

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



Name: new column group

☑	Meta Key	Display Name	Width
☑	custom.source	Source Info	100

9. (Optional) To revert to the previous settings for the column group, and undo all of your changes, click **Cancel**.

10. When ready to save, do one of the following:

    a. To save the edited column group and refresh the Legacy Events view with the column group settings, click **Save and Apply**.

    b. To save the edited column group without refreshing the Legacy Events view, click **Save**.

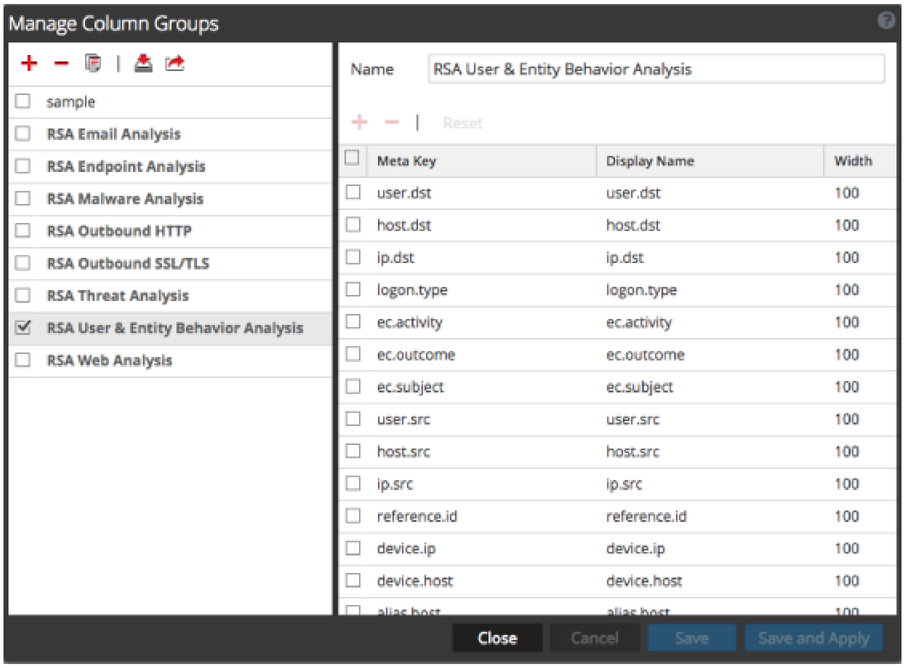
Import and Export a Column Group (Legacy Events View)

You can export custom column groups for use by other members of your team, and other analysts can import column groups if you give them a copy of the exported file.

To export a column group:

1. Go to **Investigate > Legacy 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. Each of these views is a differently formatted events list, and each column represents one

meta key.
The Manage Column Groups dialog is displayed.



Name: RSA User & Entity Behavior Analysis

- □ sample
- □ RSA Email Analysis
- □ RSA Endpoint Analysis
- □ RSA Malware Analysis
- □ RSA Outbound HTTP
- □ RSA Outbound SSL/TLS
- □ RSA Threat Analysis
- ☑ RSA User & Entity Behavior Analysis
- □ RSA Web Analysis

□	Meta Key	Display Name	Width
□	user.dst	user.dst	100
□	host.dst	host.dst	100
□	ip.dst	ip.dst	100
□	logon.type	logon.type	100
□	ec.activity	ec.activity	100
□	ec.outcome	ec.outcome	100
□	ec.subject	ec.subject	100
□	user.src	user.src	100
□	host.src	host.src	100
□	ip.src	ip.src	100
□	reference.id	reference.id	100
□	device.ip	device.ip	100
□	device.host	device.host	100
□	alias.host	alias.host	100

3. To export a column group, select the checkbox before the name and click the Export option ( ). The column group is exported to your local file system as a .jsn file, for example, `CustomColumnGroupsExport.jsn`. If you export another group, the next file is named `CustomColumnGroupsExport-2.jsn` to differentiate.
4. To import a column group that you have available on your local file system, click the Import option ( ).
   The Import Column Groups dialog is displayed.
5. Browse your local drive to find the column group (jsn file), and click **Upload**.
   The column group is added to the list. If it has the same name as an existing column group, a message is displayed and the column group is not imported.

Use Query Profiles to Encapsulate Common Areas for Investigation

Query profiles offer a quick and easy way to define a meta group, column group, and a limiting query (preQuery) that you can apply in the Navigate view, the Events view, and the Legacy Events view.

> **Note:** Version 11.4 has a single Events view, which was known as the Event Analysis view in prior versions. The Legacy Events view from Versions 11.3 and earlier is still available when your administrator enables the view as described in the *System Configuration Guide*. If the Legacy Events view is enabled, both views are available in the Investigate submenu.

NetWitness Platform has these built-in profiles: RSA Email Analysis, RSA Endpoint Analysis, RSA File Analysis, RSA Threat Analysis, RSA User & Entity Behavior Analysis, and RSA Web Analysis. Each built-in profile specifies a built-in meta group, column group, and sometimes includes a pre-Query appropriate for the type of investigation. Built-in query profiles make it easy for you to query a specific area of interest; for example, selecting the built-in RSA Email Analysis query 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 query profiles.

In a query profile:

- The meta group defines the meta keys that are queried (see Use Meta Groups to Focus on Relevant Meta Keys).
- The column group defines which meta keys from the meta group are displayed as columns in the Events list. By default only the first 15 columns in a column group are displayed as a starting point from which you can select additional columns, remove, and rearrange columns (see more about column groups in Use Columns and Column Groups in the Events List.
- The pre-Query adds a limiting filter at the beginning of the query you are creating.

The built-in profile names begin with the RSA prefix and are grouped under Default Profiles. You cannot edit or delete built-in profiles, but you can copy an existing profile and edit the copy in the Navigate view or the Legacy Events view. In the **Navigate** or **Legacy Events** view toolbar, select **Profile > Manage Profiles**.

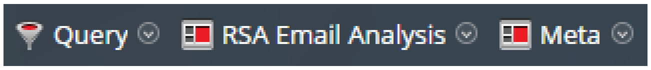
> **Note:** Query profiles are available in the Navigate view, the Legacy Events view, and the Events view and shared globally across users. If one user modifies or deletes a query profile it has an effect on what is available to the other users.

You can create your own custom profiles in the Create Query Profile dialog and the Manage Profiles dialog. The Manage Profiles dialog has some options that are not available in the Create Query Profile dialog.

- From the Manage Profiles dialog (Navigate view and Legacy Events view), you can configure, add, delete, import, and export profiles and profile groups. You can organize your custom query profiles in Profile Groups (Version 11.2 and later). When upgrading to Version 11.4 from an earlier version,only profile groups that contain profiles are imported.

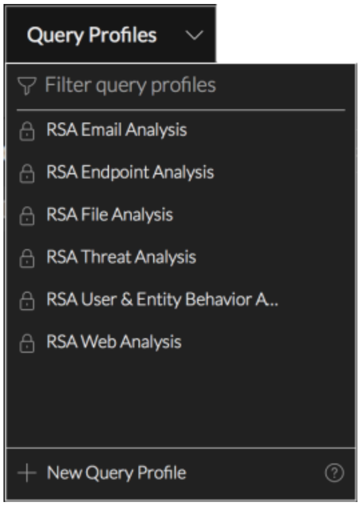
- From the Query Profiles menu (11.4 Events view), you can select and apply a query profile. Options in the menu allow you to create (Create Query Profile dialog), edit, and delete (Query Profile Details dialog) custom query profiles. In Version 11.4, the Events view does not use meta groups or profile groups defined in other views.

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



Version 11.2 and later supports organization of query profiles into groups in the Navigate view and the Legacy Events view. The built-in query profiles are in the Default Profiles group, which cannot be edited. Analysts can create new query profile groups, which anyone can use. After creating profiles, 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.

The following figure illustrates the Query Profiles menu in the Version 11.4 Events view. This menu lists the same profiles that are available in the Navigate view and the Legacy Events view. You can create, edit, delete, and apply profiles.



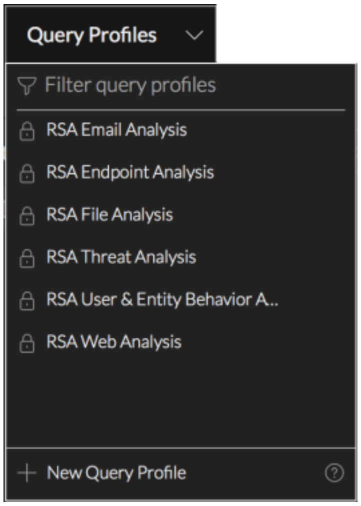
If a query profile created in the Legacy Events view uses the Log View, Detail View, or List View instead of a column group, the same profile in the 11.4 Events view uses the Summary List column group.

View Query Profile Details (Events View)

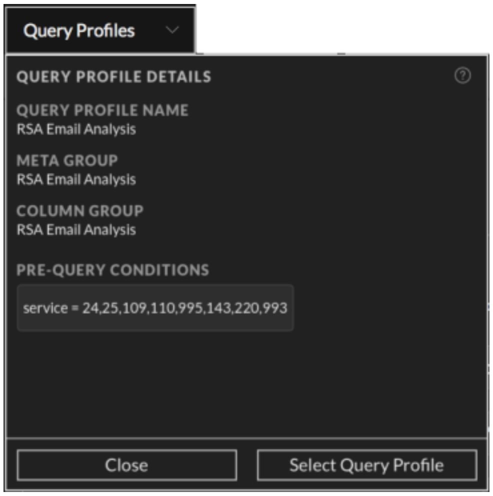
If you want to know which meta groups, column groups, and limiting queries (called preQueries) define a query profile, you can view the details of the profile.

To review the details:

1. Go to **Investigate > Events** and click **Query Profiles** in the query bar.
   The Query Profiles menu opens with a list of available profiles.



2. Hover over a query profile and click the information icon (ⓘ) to see the meta group, column group, and preQuery configured for the profile.
   This figure shows the details for the RSA Email Analysis profile, one of the built-in profiles.



QUERY PROFILE NAME
RSA Email Analysis

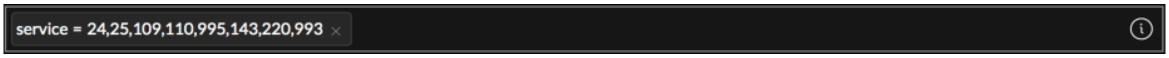
META GROUP
RSA Email Analysis

COLUMN GROUP
RSA Email Analysis

PRE-QUERY CONDITIONS

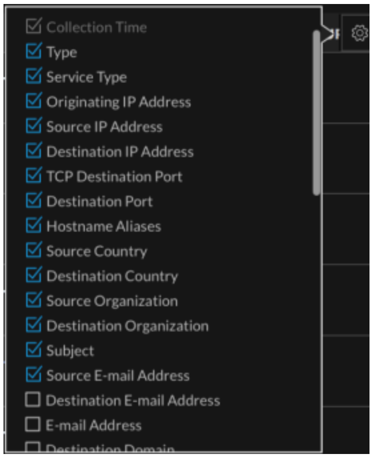
service = 24,25,109,110,995,143,220,993

3. Do one of the following:
   a. To close the dialog, click **Close**.
   b. If you want to apply the profile, click **Select Query Profile**.
      The dialog closes. The Events list is updated to reflect the selected query profile. If the profile uses a different column group, the query is re-executed with the preQuery and column groups for the selected profile. If only the preQuery is different, existing filters in the query bar are removed and the preQuery filter (for example, this query: `service=24,25,109,110,995,143,220,993`) is added in the query bar. The first 15 columns in the associated column group are used in the Events list. You can adjust the columns and create additional filters before executing the query.



service = 24,25,109,110,995,143,220,993

c. If you want to select different columns from the associated column group, click ⚙ above the Events list on the right.
The Column Selection list is displayed and you can choose up to 40 columns to display (see Use Columns and Column Groups in the Events List.



- ☑ Collection Time
- ☑ Type
- ☑ Service Type
- ☑ Originating IP Address
- ☑ Source IP Address
- ☑ Destination IP Address
- ☑ TCP Destination Port
- ☑ Destination Port
- ☑ Hostname Aliases
- ☑ Source Country
- ☑ Destination Country
- ☑ Source Organization
- ☑ Destination Organization
- ☑ Subject
- ☑ Source E-mail Address
- ☐ Destination E-mail Address
- ☐ E-mail Address
- ☐ Destination Domain

Apply a Query Profile (Events View)

If you do not see enough results or the right results in the Events view, an applied profile may be limiting results with a PreQuery. If a PreQuery is applied, the PreQuery filters are visible at the beginning of the query bar.

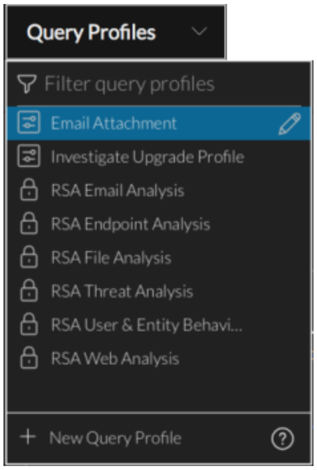
To select a query profile:

1. In the **Events** view toolbar, click **Query Profiles**.
   The Query Profiles menu opens with a list of available profiles.
2. Use the Down and Up arrow keys or the mouse to highlight a profile.
3. Click the highlighted profile.
   The query profile settings are applied immediately. The Events list is updated to reflect the selected profile. If the profile uses a different column group the query is re-executed with the preQuery and column groups for the selected profile. If only the preQuery is different, existing filters in the query bar are removed and the preQuery filters are added in the query bar. The 🔍 button becomes active so that you can resubmit the query with the new preQuery filters. You can add more filters as usual before or after resubmitting the query.

Create or Edit a Custom Query Profile (Events View)

To create or edit a custom query profile:

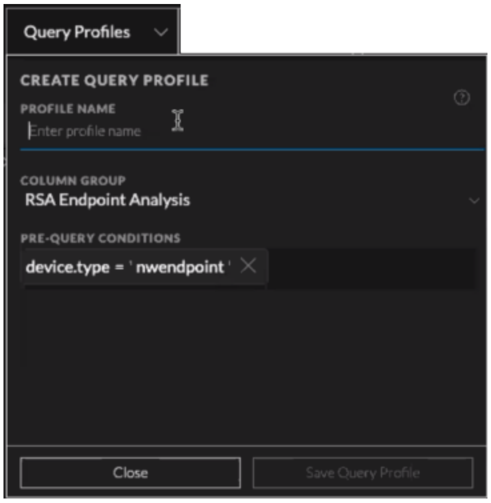
1. In the **Events** view toolbar, click **Query Profiles**.
   The Query Profiles menu opens with a list of available profiles.



2. Do one of the following:

   a. To create a new query profile, click + **New Query Profile**.

   b. To edit an existing query profile, highlight a custom query profile in the menu, and click the edit (✎) icon.
   The Create Query Profile or the Query Profile Details dialog is displayed. This figure shows a new empty profile, which includes the filter from the Query bar as a preQuery.



COLUMN GROUP
RSA Endpoint Analysis

PRE-QUERY CONDITIONS
device.type = 'nwendpoint'

3. In the **Profile Name** field, type a unique profile name that has no more than 80 characters.

4. Select a column group from the **Column Group** drop-down list.

5. In the **PreQuery** field, check the default preQuery from the query bar and add filters if you wish.

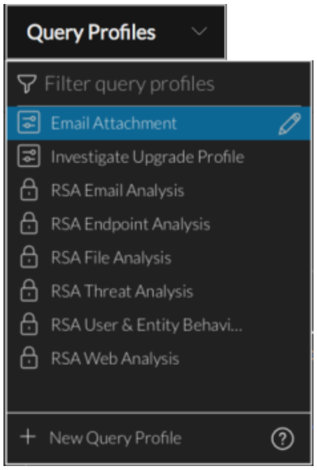
6. Click **Save Query Profile** or **Update Query Profile**.
   The new profile is saved or the edited profile is updated with your changes.

7. To close the dialog, click **Close**.

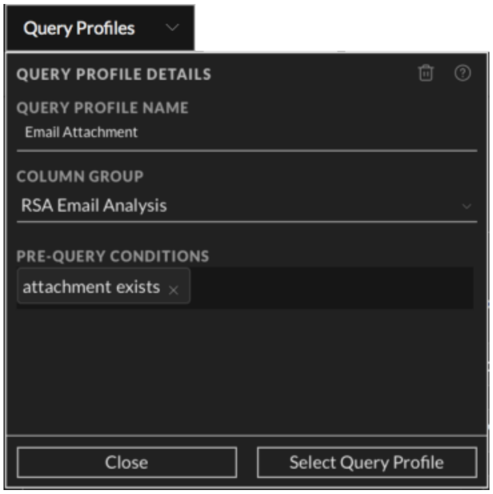
Delete a Custom Query Profile (Events View)

To delete a custom query profile:

1. In the **Events** view toolbar, click **Query Profiles**.
   The Query Profiles menu opens with a list of available profiles.



2. Highlight a custom query profile that you want to delete in the menu, and click the edit (✎)icon.
   The Query Profile Details dialog is displayed.



QUERY PROFILE DETAILS

QUERY PROFILE NAME
Email Attachment

COLUMN GROUP
RSA Email Analysis

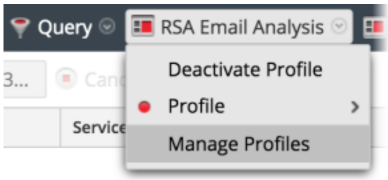
PRE-QUERY CONDITIONS
attachment exists

3. Click the delete icon (🗑).
   The profile is deleted, with no option to reverse your decision. The profile is no longer available to anyone.

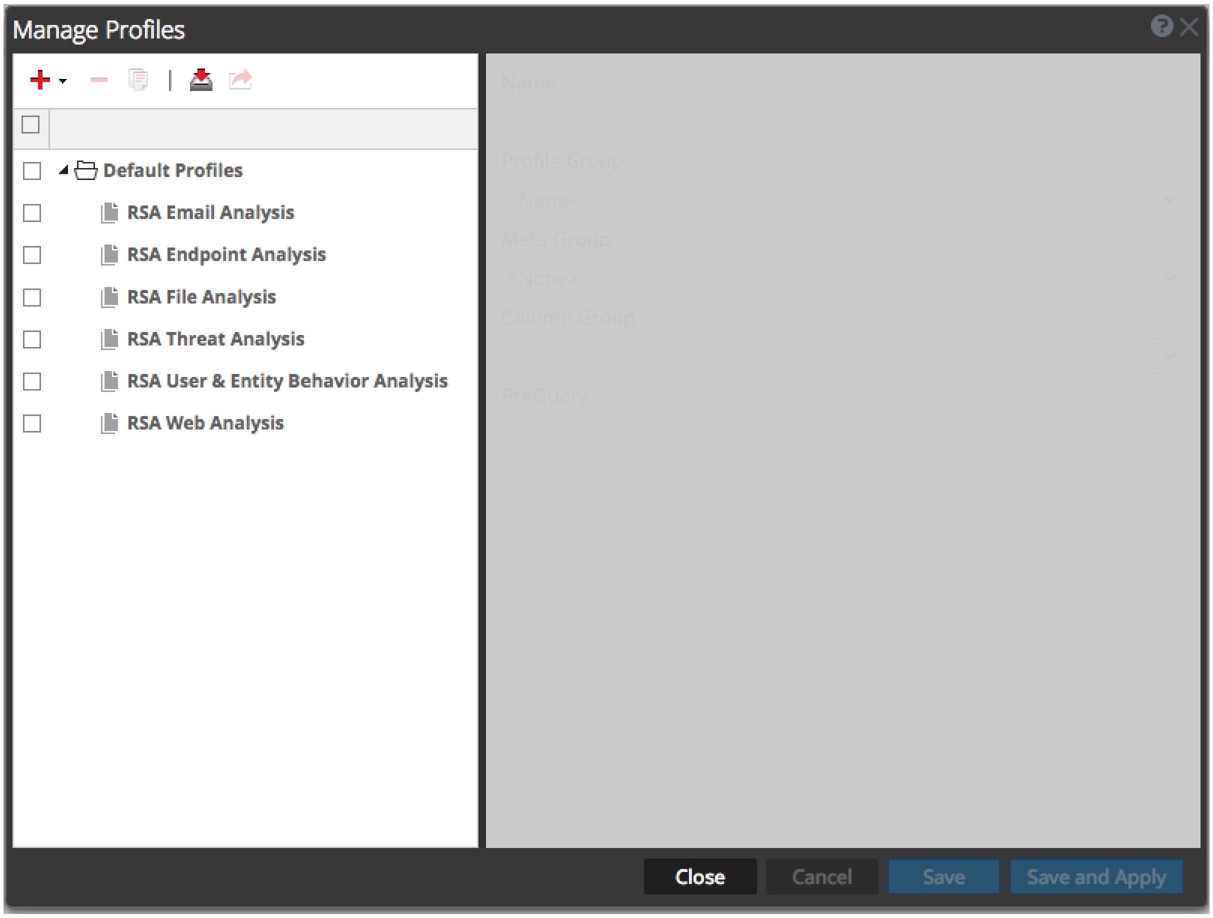
Navigate to the Manage Profiles Dialog (Navigate and Legacy Events Views)

1. Go to **Investigate** > **Navigate** or **Legacy Events**. (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 (Navigate or Legacy Events View)

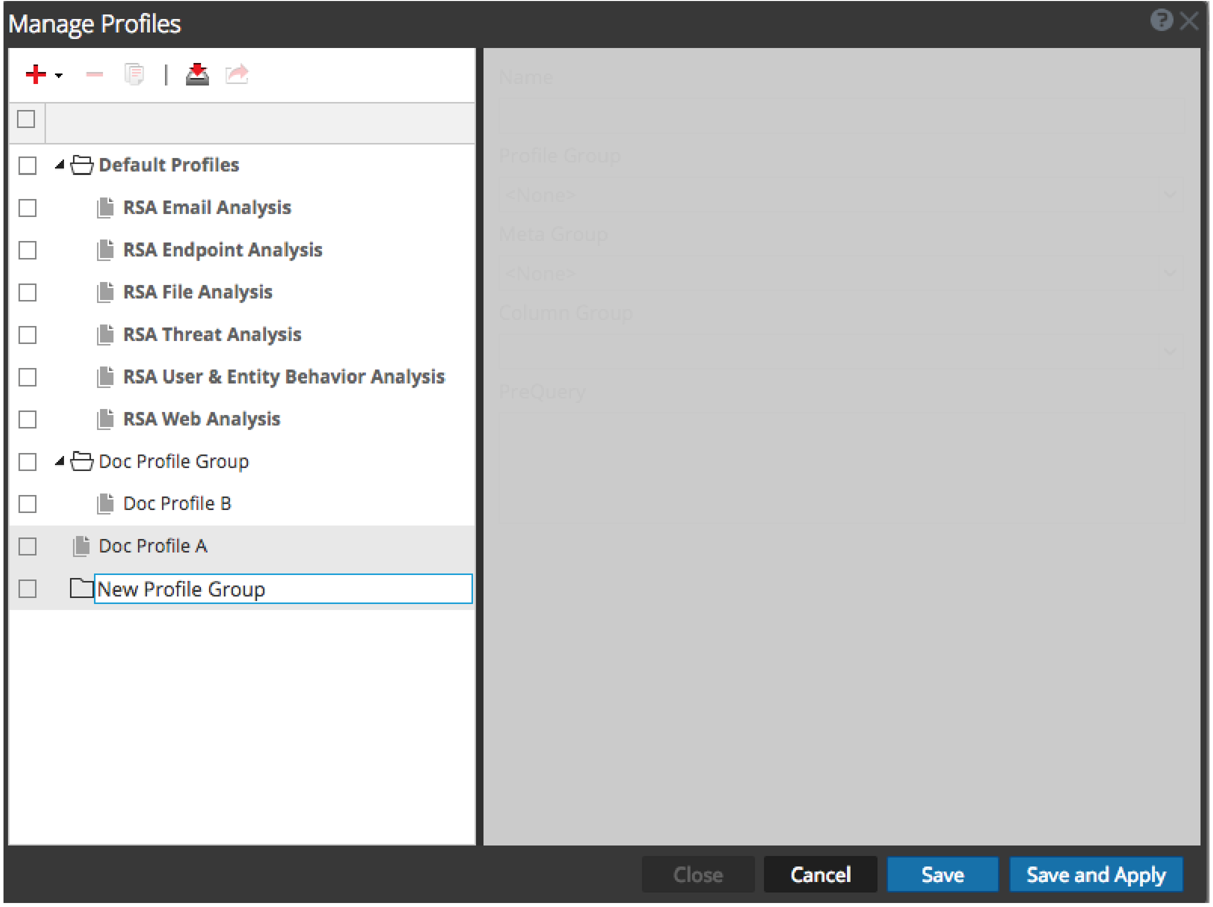
You can create a custom profile group to organize different profiles. Once created, the only edit you can make directly to a profile group is to edit the name of the profile group. To add or remove a profile in a group, edit the profile and assign it to a different profile group as described in Create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

Note: If you migrated profile groups from Version 11.3, empty groups were not migrated.

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

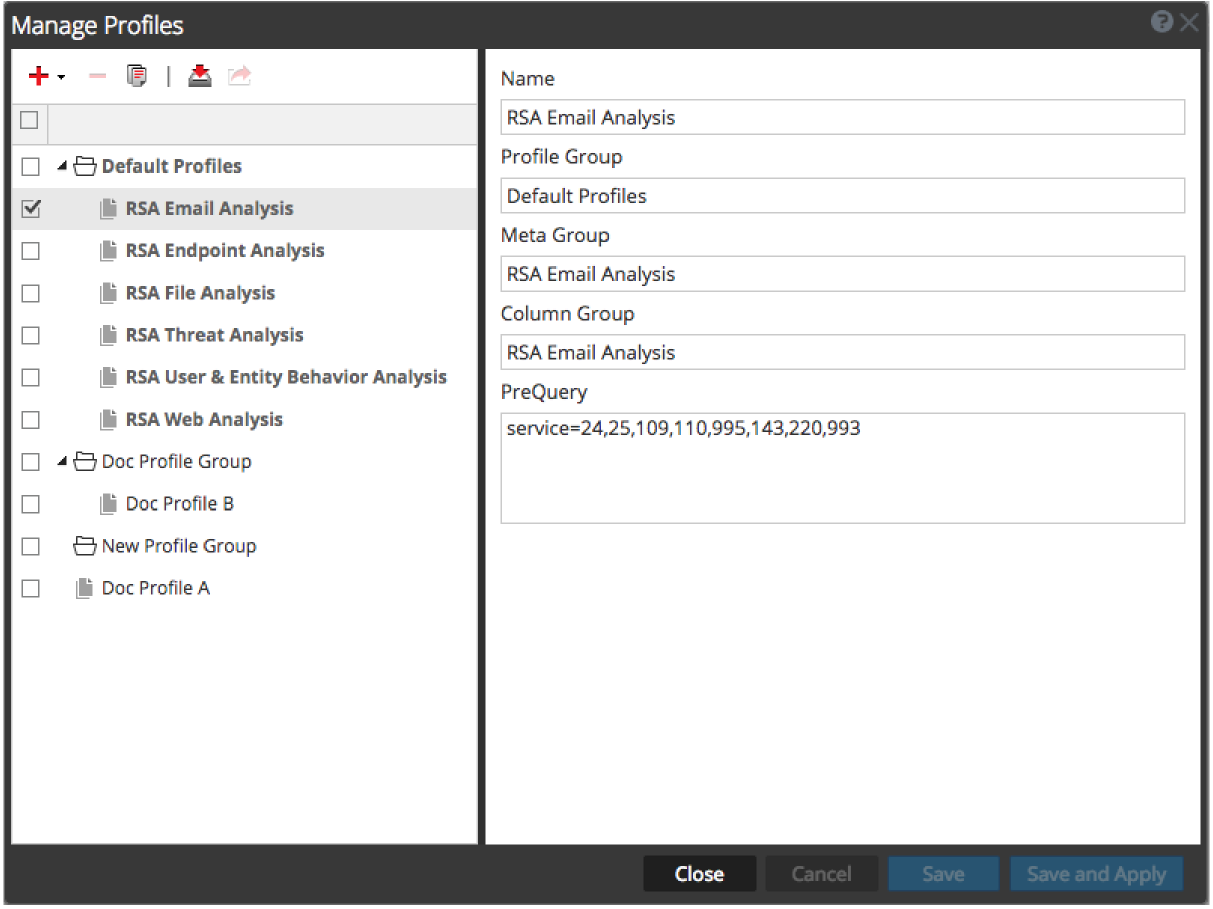
the profiles, only the profile group is deleted and the profiles are moved out of the group and available to add to another profile group.

Create and Edit Profiles (Navigate or Legacy Events View)

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.



Name: RSA Email Analysis

Profile Group: Default Profiles

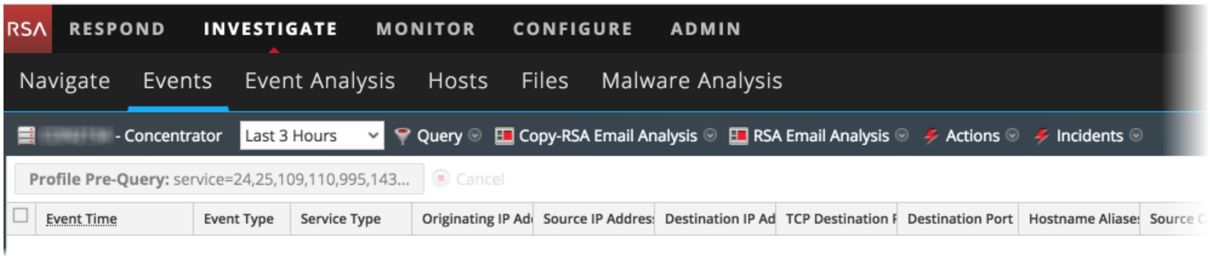
Meta Group: RSA Email Analysis

Column Group: RSA Email Analysis

PreQuery: service=24,25,109,110,995,143,220,993

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 Use Meta Groups to Focus on Relevant Meta Keys.
5. Select a column group for the **Column Group** drop-down list. You can add custom column groups as described in Use Columns and Column Groups in the Events List.
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.



Profile Pre-Query: service=24,25,109,110,995,143...

Delete a Profile (Navigate or Legacy Events View)

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 (Navigate or Legacy Events View)

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 **Legacy 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 **Legacy 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 (Navigate or Legacy Events View)

In the Navigate view and the Legacy Events view, 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 (Navigate or Legacy Events View)

In the Navigate view and the Legacy Events view, 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.

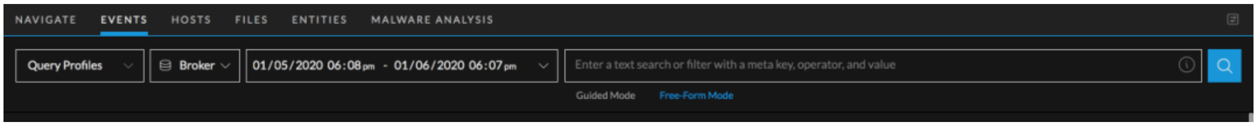
Filter Results in the Events View

Note: This section applies to version 11.1 and later.

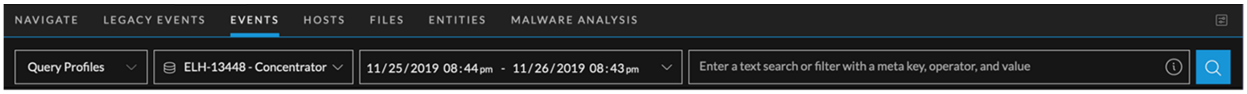
You can filter events in the Events view using the query bar to select a service and time range and then query the service being investigated. Filtering events helps to narrow the focus of an investigation to a smaller, relevant set of events.

In Version 11.4, you can also use column groups to optimize the number or attributes (meta keys, meta groups, meta entities) you look at for a given event (see Use Columns and Column Groups in the Events List).

This figure illustrates the Version 11.4 and earlier Query Bar with tools to filter results in the Events list. Two modes are available Guided Mode and Free-Form Mode.


NAVIGATE
EVENTS
HOSTS
FILES
ENTITIES
MALWARE ANALYSIS
Query Profiles
Broker
01/05/2020 06:08 pm - 01/06/2020 06:07 pm
Enter a text search or filter with a meta key, operator, and value
Guided Mode
Free-Form Mode

This figure illustrates the Version 11.4.1 and later Query Bar in which the Guided and Free-From Modes are no longer necessary. The simplified filter entry form allows you to use advanced auto-suggest options and also to enter a free-form query.

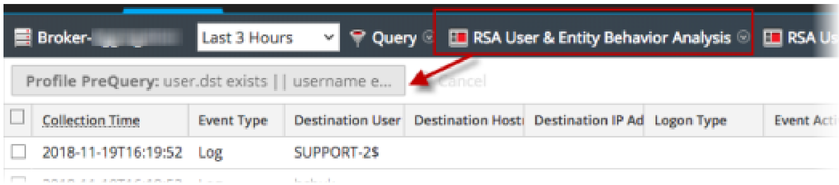

NAVIGATE
LEGACY EVENTS
EVENTS
HOSTS
FILES
ENTITIES
MALWARE ANALYSIS
Query Profiles
ELH-13448 - Concentrator
11/25/2019 08:44 pm - 11/26/2019 08:43 pm
Enter a text search or filter with a meta key, operator, and value

When you go to Investigate > Events, the Query Profiles menu, the service and time range selectors, and the query builder field are displayed in the query bar.

- The Query Profiles menu is available in Version 11.4 and later. You can encapsulate a query and a column group in a profile so that a useful combination of attributes is easily recalled and applied to a set of events in the Events list (see Use Query Profiles to Encapsulate Common Areas for Investigation.)
- By default, the first service is automatically selected (unless you previously selected a service and the selected service is in browser cache). You can select a service as described in Begin an Investigation in the Events View
- 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. This is where you build a query by creating filters. Clicking 🔍 submits the query and sends a request to the selected service to load the data. In Version 11.3 and later, clicking the ⓘ (console icon) opens the query console, where detailed status of the query is provided.

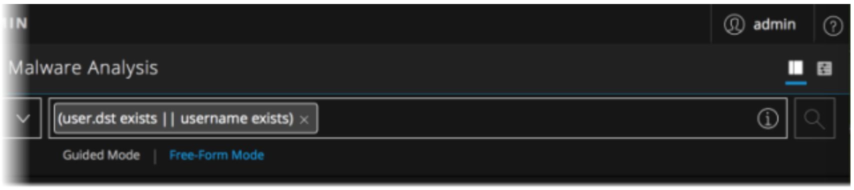
When you go to the Events view from the Legacy Events view or the Navigate view, the service, time range, and any filters that were selected in the Legacy Events view or Navigate view are displayed in the query bar. The service, time range, and individual filters can be modified.

If a profile is selected in the Legacy Events view when you right-click or double-click an event and go to the Events 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 Legacy Events view, and the same query added as the first filter in the Events view.



Profile PreQuery: user.dst exists || username e...

Collection Time	Event Type	Destination User	Destination Host	Destination IP Ad	Logon Type	Event Act
2018-11-19T16:19:52	Log	SUPPORT-2$				



(user.dst exists || username exists)

Query Builder Concepts

In the query builder, you can reduce the number of events to an interesting set by creating three types of filters: simple, free-form, or text.

The basic syntax for each filter is as follows: `<meta key><operator><meta value>`. Here is an example: `direction = 'outbound'`.

In Version 11.4, when you type or paste a query in the query bar, the text is parsed into individual filters separated by the AND operator if the parsing engine determines that AND is needed. Earlier versions use only the AND operator between filters, and the logical operator is not visible.

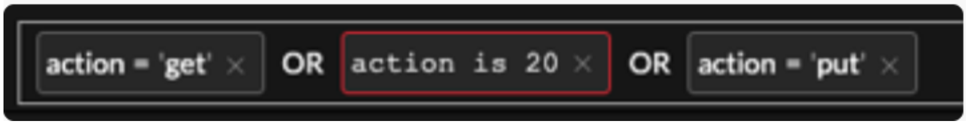
- If you type `action = 'get' action = 'put'`, the result is two filters separated by AND.
- If you type `action = 'get' OR action = 'put'`, the result is two filters separated by OR.

When typing or pasting a filter for `event.time`, use one of the following formats:

- `event.time = '2020-DEC-02 23:00:00'`
- `event.time = '2000-12-20 21:00:00.000'`
- `event.time = '2000-12-20 21:00:00'`

In Version 11.4, the parsing engine converts a longer string of text that you type or paste in the query bar into individual filters. Parts of the filter that are not parsable are converted to a free-form filter. In earlier versions, a long text string is added to the query bar as a single filter. Further enhancement in Version 11.4.1 provides the ability to keep typing text for any query, where you type a meta key and an operator or an operator and a value, as a free-from query. The free-from query is parsed as usual.

- If you type, `action = 'GET' OR action is 20 || action = 'PUT'` in the query bar the Free-Form option is used. Part of this text cannot be parsed so the result is three filters separated by OR.



action = 'get' OR action is 20 OR action = 'put'

- In Version 11.4.1, If you type a meta key-operator-value sequence and you continue typing without pressing Enter, the Free-Form option is automatically used so that you can continue typing the query. For example, you can type `medium = 1 OR medium = 2` without pressing the Enter key before `OR`. The Free-Form option is highlighted while you type and when you press Enter at the end, a free-form filter is created in the query bar.
- Text filters (Version 11.4 and later) are text strings that do not contain spaces. You can search the data set for any exact match of indexed meta keys, not all meta keys. Here are some examples: `failed, login`, or `attempt`.

Note: In some cases, when you are typing a text filter that is close to matching a meta key and operator statement, the auto-suggest feature erroneously suggests a filter using the meta key and operator. The workaround is to begin typing the text and select Text Filter at the point where the auto-suggest feature turns the text into a meta key and operator. For example, there is meta key named `crypto`, and an operator named `contains`, and you want to create a text filter to search for `cryptocurrency`. As you type `c-r-y-p-t-o`, the next `c` in "currency" triggers the `contains` operator instead of continuing to type as a single word. To complete the text filter, right before typing that `c` in `currency`, which would trigger the `contain` operator, highlight the Text Filter option to let the system read the input as text filter.

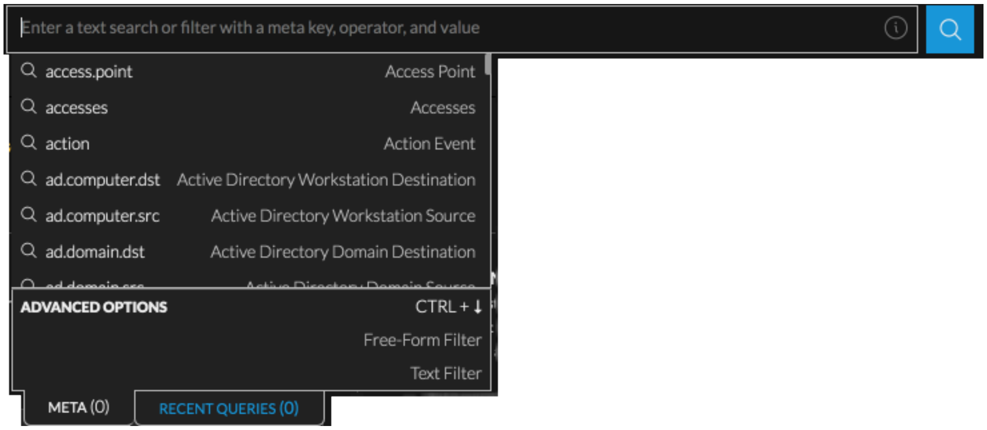
In the query builder, each filter becomes an editable field. Filters line up from left to right, representing the sequence in which the filters were created. As more filters are added and exceed the length of a single line, they wrap to another line and the input area expands vertically so that all filters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

Successive versions of RSA NetWitness® Platform 11 have more capability than the original 11.1 query bar, with Version 11.4 offering extensive help as you create a query.

Guided Mode vs. Free-Form Mode

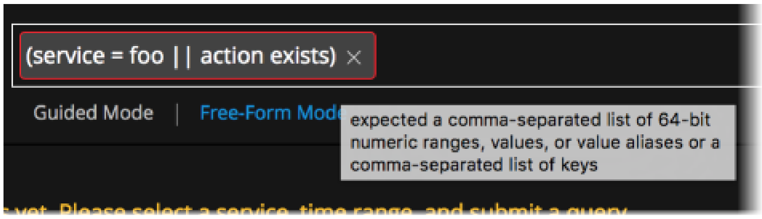
Note: Version 11.4 offered two modes for entering queries in the filter entry form: Guided Mode and Free-Form Mode. Beginning with Version 11.4.1, the powerful auto-completion features and suggested values of Guided Mode and the ability to type or paste a free-form query are fully integrated. References in this document that differentiate between Guided Mode and Free-Form Mode are for analysts using Version 11.4.0.x and earlier.

In Guided Mode, you are guided with suggestions for auto-completion that show valid meta keys and operators, and suggested values in the filter entry form. In version 11.4, you can type, paste, choose a recent query, or select from the drop-down menu. Earlier versions do not support pasting text and recent queries. This is an example of the 11.4 filter entry form.


Enter a text search or filter with a meta key, operator, and value
access.point Access Point
accesses Accesses
action Action Event
ad.computer.dst Active Directory Workstation Destination
ad.computer.src Active Directory Workstation Source
ad.domain.dst Active Directory Domain Destination
ad.domain.src Active Directory Domain Source
ADVANCED OPTIONS CTRL + ↓
Free-Form Filter
Text Filter
META (0)
RECENT QUERIES (0)

As you create 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, free-form 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.


(service = foo || action exists)

expected a comma-separated list of 64-bit numeric ranges, values, or value aliases or a comma-separated list of keys

Guided Mode | Free-Form Mode
yet. Please select a service, time range, and submit a query.

In Free-Form Mode, you can type or paste a long text string. 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.

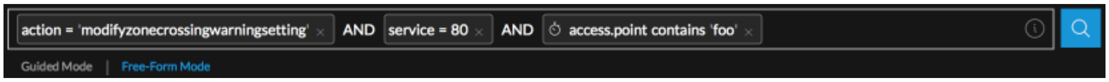
Note: The 🔍 button has a different label in versions earlier than Version 11.3. It was previously named **Query Events**.

Clicking Guided Mode or Free-From Mode toggles between modes. If you selected Free-Form Mode the last time you logged in, this choice is stored in browser cache and is used until the browser cache is cleared.

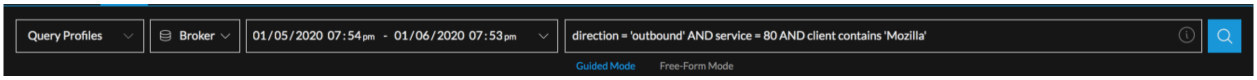
- When you switch from Guided Mode to Free-Form Mode, filters that you created in Guided Mode are transformed to a text query in the Free-Form field.
- When you switch from Free-Form Mode to Guided Mode, the query you were typing is added to the query bar as individual simple filters, but it does not include auto-suggest options.

Note: Before Version 11.3, a Free-Form filter could not be edited in Guided Mode.

The following figure is an example of the query bar with the Guided Mode query builder with several filters.

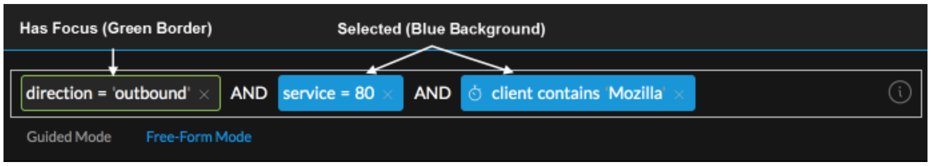

action = 'modifyzonecrossingwarningsetting' AND service = 80 AND access.point contains 'foo'

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

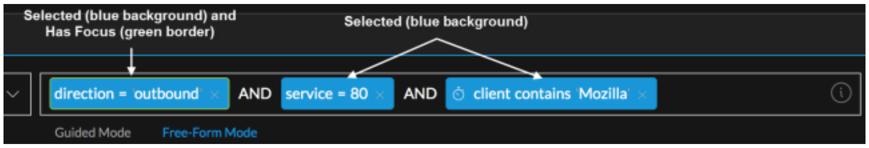

Query Profiles
Broker
01/05/2020 07:54pm - 01/06/2020 07:53pm
direction = 'outbound' AND service = 80 AND client contains 'Mozilla'
Guided Mode
Free-Form Mode

Concepts for Editing Multiple Filters

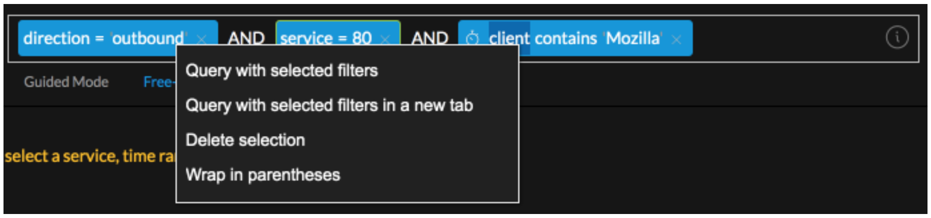
As you work in the query builder, you can see when a filter has focus for editing (a green outline) and which filters are selected (blue background). This is useful because you can have multiple filters selected for right-click actions, but only one can be edited at a time. The figure below shows the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

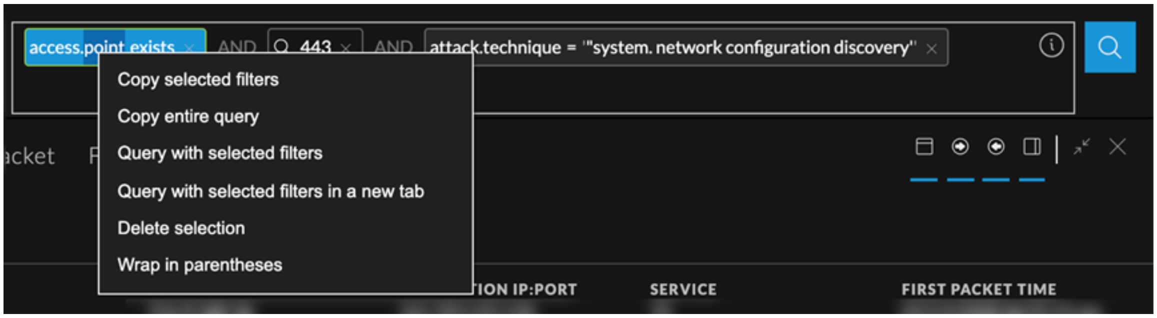


A right-click action from the drop-down menu applies to all selected filters as shown in this figure showing Version 11.4 options.


direction = 'outbound'
AND
service = 80
AND
client contains 'Mozilla'
Guided Mode
Free-
select a service, time ra
Query with selected filters
Query with selected filters in a new tab
Delete selection
Wrap in parentheses

In Version 11.4.1, the menu has two new copy options as shown in the following figure. The options allow you to share the clipboard contents with other analysts or paste the contents to the query bar. You can:

- Select a single filter, right-click it, and then copy the entire query to the local clipboard.
- Select multiple filters, right-click one of them, then copy the selected filters.



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

- 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.

The Version 11.3 and Earlier Query Builder

In Version 11.1, the user interface guides you as you create and edit each simple filter: `<meta key> <operator> <meta value>` filter. The user interface supports only simple filters. If you open an event from the Legacy 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 Events view. Refer to the Investigate User Guide for NetWitness Platform 11.3 for details; it is available here in PDF form: Master Table of Contents for RSA NetWitness Platform Version 11.

In Version 11.2, the user interface has two modes: Guided Mode and Free-Form Mode. Guided Mode guides you as you create and edit each simple `<meta key> <operator> <meta value>` filter. The default mode is Guided Mode, which includes auto-suggest and validation options. You can enter a long text string in Free-Form Mode. In Free-Form Mode validation is performed when you run the query. Refer to the Investigate User Guide for NetWitness Platform 11.2 for details; it is available here in PDF form: Master Table of Contents for RSA NetWitness Platform Version 11.

In Version 11.3, the user interface has these added features:

- When you go to the Events view from the Navigate or Events view, with a preQuery in effect for a profile, the preQuery that was displayed in the breadcrumb is available in the Events view query builder as an editable filter.
- The auto-suggest options in the user interface 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 long text string.
- You can cancel a query while it is executing.
- You can view detailed status information about the query being executed in the query console.

The Version 11.4 Query Builder

You can type; select meta keys, operators, and values from the drop-down menus; or paste a filter in the query bar. Added 11.4 features in the Guided Mode filter entry form are described in detail below.

Meta Keys Cached for Faster Loading

When the Events view opens, meta keys from all connected services are cached for faster data loading. These meta keys are available in user interface elements that have auto-suggest meta keys. (When you are building a column group or profile, if you are expecting to see a meta key and it is not displayed, select the service where the key was added to force a cache update. This usually occurs only when a meta key is not added to all concentrators.)

Text Filter

You can create a text filter to find a text string in the data set. You can use a text filter with no knowledge of meta keys that would contain the values. One text filter per query is supported. A text filter looks through indexed meta keys, not all meta keys.

Pasting Text Instead of Typing

When creating a filter, you can paste a meta key or value in the filter entry form. When you paste text into the filter entry form instead of typing the text, the text is parsed appropriately to create one or more filters. Any portion of the text that cannot be parsed is converted to a free-form filter.

Select All Filters and Copy All Filters (Version 11.4.1)

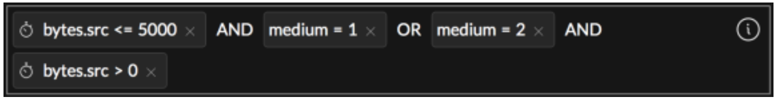
While creating a filter in the Events view query bar, you can use keyboard commands to select all filters (Cmd-A for MacOS, Ctrl-A for Windows) and then copy the selection to the clipboard (Cmd-C for MacOS, Ctrl-C for Windows). The clipboard text is available to share with other analysts or to paste in the query bar using Cmd-V or Ctrl-V).

Use of Recent Queries

The filter entry form offers two methods of entering meta keys, operators, and values: the Meta tab and Recent Queries tab. The Meta tab is the same as the filter entry form for prior versions except that a count of matching results is given in the tab label and icons mark meta keys that are indexed by key, indexed by value, and not indexed. In the Recent Queries tab, up to 100 recent queries are displayed. The list is filtered as you type to show only queries that contain the typed text, and you can select a query from the list.

Use of Advanced Operators

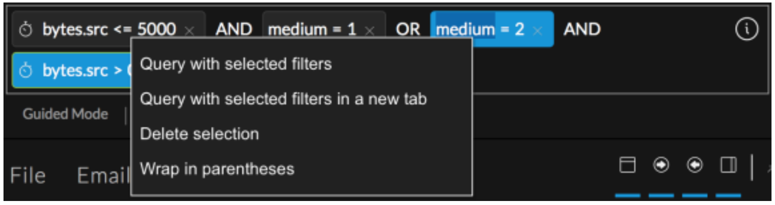
Auto-suggest can parse the following advanced operators that you paste or type into the filter entry form: `<`, `>`, `<=`, `>=`, `OR`, `||`, `AND`, `&&`, `()`, `regex`, and `length`. The text is parsed as multiple filters. For example, if you type or paste `medium > 0 && medium <= 100`, the text is parsed as two simple filters with an explicit AND operator: `medium > 0` AND `medium <= 100`. If you type or paste `bytes.src <= 5000 && medium = 1 || medium = 2 && bytes.src > 0`, four simple filters are created with `AND` and `OR` operators separating them: `bytes.src <= 5000 AND medium = 1 OR medium = 2 AND bytes.src > 0` to make as many valid filters as possible.



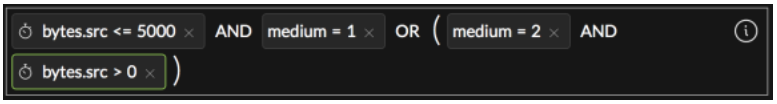
bytes.src <= 5000 × AND medium = 1 × OR medium = 2 × AND

bytes.src > 0 ×

This filter is an example of a filter in which it would be useful to add parentheses. You can select `medium = 2` and `bytes.src > 0`, then right-click and select **Wrap in Parentheses** from the drop-down menu. Text filters are not supported inside parentheses.



The resulting query is `bytes.src <= 5000 AND medium = 1 OR (medium = 2 AND bytes.src > 0)`.



If you encounter errors while creating filters, look for tooltip messages and check the documentation.

Easy Use of AND/OR Operators

When you type `||`and `&&`, they are displayed as `OR` and `AND` in the query bar. You can change `OR` to `AND` and `AND` to `OR` by clicking the word. When you insert the cursor to add a filter, the `AND` operator is added before the cursor. When you delete a filter, orphaned `OR` and `AND` operators are removed. The operator for a text filter must be AND because text filters are always ANDed to a query.

Automatically Balanced Parentheses

When creating and editing filters in the query builder, parentheses pairs are automatically balanced as you type. If you type an open parenthesis in a filter that is open for editing or before a selected filter, the close parenthesis is added at the end of the filter. This works intuitively as you type so that you can add new filters on either side of the parenthesis and between parentheses when there are nested parentheses. Orphaned parentheses are automatically removed. If adding parentheses would create an invalid filter, the parentheses are not added. You can also right-click selected filters, and add parentheses using the Wrap in parentheses option. This option is only available when the result would be a valid filter.

Hints about Available Values

For properly indexed meta keys, the user interface provides hints about available values related to the time range of the query. Up to 100 suggested values are returned and, when you type text, the list of 100 values is filtered to include only relevant values. If no matching values are returned, a message advises "No suggestions found." (The suggested values are based solely on the time range; filters in the query do not filter the list of 100.)

CIDR Notation and Shorthand

When entering a value for an IP address in a filter, you can use CIDR notation to filter for addresses within a range.

The IPv4 CIDR block range is 0 to 32. For example `10.20.30.0/24` specifies `10.20.30.0` with a subnet mask of `255.255.255.0`, which will match an IP in the range `10.20.30.0` through `10.20.30.255`.

The IPv6 CIDR block range is 0 to 128, for example, `1203.0fe1:fe82:b896:89b0:8a7c:99bf:323d/32` specifies `1203:0fe1:0000:0000:0000:0000:0000:0000` through `1203:0fe1:ffff:ffff:ffff:ffff:ffff:ffff:ffff`.

You can also use shorthand to remove groups of zeros or leading zeros in a group in IPv6 addresses, for example,

`1203:fe1::`

There must be no spaces between the IP address and the CIDR mask that you are using.

Ranges or Series of Values

For meta keys that have numerical data, you can use a range of values, a series of values, or both to filter data. For example, this query has a comma-separated list, and two of the values in the series are ranges `src.port = 0-1023, 1024-1050, 65535`. If a comma is a part of a value, the value must be wrapped in quotes. For example, `get,post` is interpreted as two separate values, while `'get,post'` is interpreted as one value. A range of values must be a valid range of positive integers, separated by a dash (with our without a space before and after). The first number in the range must be smaller than the second. For example, `0-1023` and `0 - 1023` are valid ranges, but these are not valid ranges: `-10 - 50`, `50 - 10`, `50.8 - 60.2`, `50 - 70x`.

No Separating Space Required After Meta Key and Operator (Version 11.4.1)

Filters in the query bar need a space between the meta key and the operator, and between the operator and the value. Operators must be typed with a separating space in the filter entry form in order to use the auto-suggest functions for operators and values. To improve the user experience when typing a query, the filter entry form accepts operators typed with no separating space after the meta key. When you type an operator with no separating space, a value is auto-suggested as usual and a space is added between the meta key and the operator. When you type an operator and a value without a separating space, the space between them is automatically added.

Select a Time Range

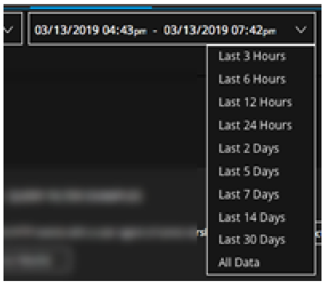
The Time Range selector limits the events returned in the Events view to a specific time range. The time range is displayed in the format `Start Time - End Time`, showing the date, hours, and minutes in your current timezone based on timezone settings configured for your profile. In Version 11.3 and later, you can choose a time range relative to the current collection time or create a custom time range. The time and date format is based on preferences set for the Events 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.

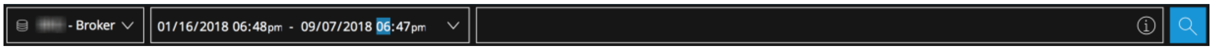
The time format for a query is based on preferences set for the Events view in the Event Preferences dialog (select ☰). The time format can be either database time or wall clock time. When Database Time is selected, the start and end time for a query is based on the time that the event was captured (collection 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. This and other Events view preferences are described in [Configure the Events View](#).

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

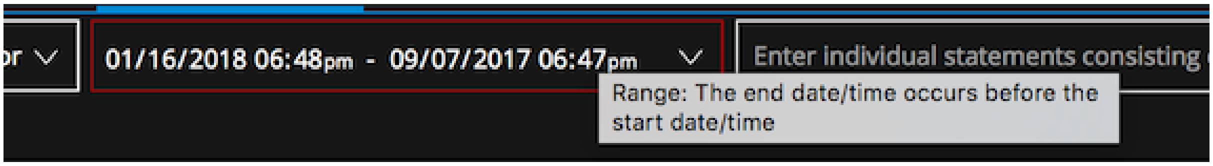
1. Click the drop-down arrow inside the **Time Range** selector and select a time range from the list. Options are in minutes, hours, days, or all data.



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.

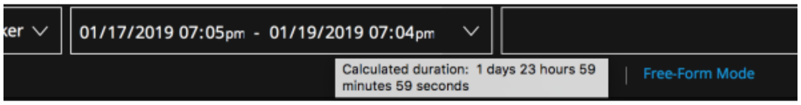


If the time range is invalid (for example, the start time is later than the end time), a red border appears around the Time Range selector. The 🔍 button is disabled because the query is no longer possible, and a tool tip shows an error message explaining what you need to change. The following figure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


01/16/2018 06:48pm - 09/07/2017 06:47pm
Enter individual statements consisting

Range: The end date/time occurs before the start date/time

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.



Calculated duration: 1 days 23 hours 59 minutes 59 seconds

Submit a Query

The 🔍 button on the right side of the query bar is active as needed to submit a query. In version 11.3 and earlier, when you click 🔍, all of the filters are ANDed to generate results and the 🔍 button becomes inactive. In Version 11.4, because the query may contain other operators besides AND, the query is submitted as is. 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 a reconstruction in 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 Events view preferences determines this behavior by enabling or disabling the Update Relative Time Window Automatically option (see Configure the Events View.)

Cancel Execution of a Query

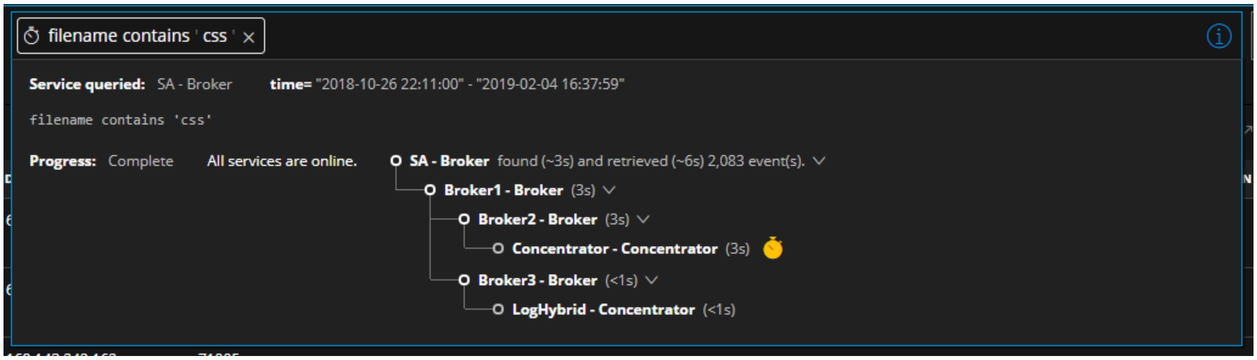
After you click 🔍 to submit a query, the button changes to ⏹ (the stop query option). The stop query option remains until all the events are loaded in the Events panel. To cancel the query, click ⏹.

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 Query Console for Version 11.3 when a query executes successfully and the slowest service is marked by an amber stopwatch.



filename contains ' css ' ×

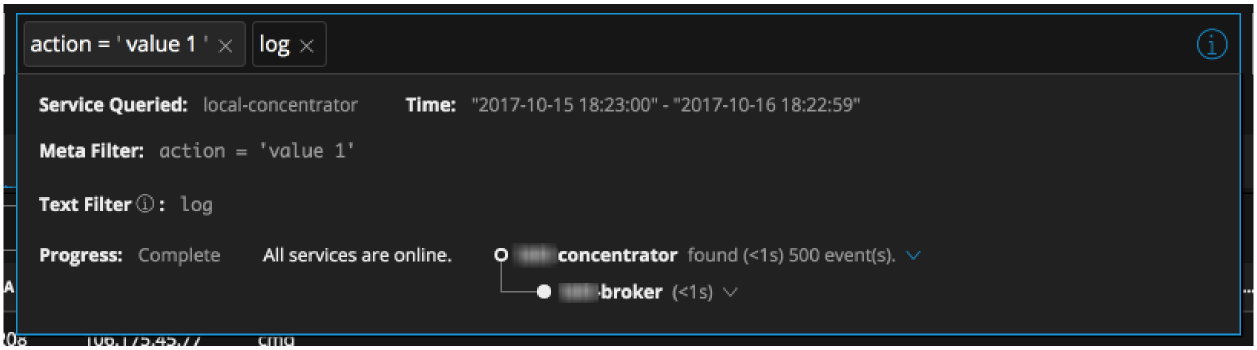
Service queried: SA - Broker **time=** "2018-10-26 22:11:00" - "2019-02-04 16:37:59"

```
filename contains 'css'
```

Progress: Complete All services are online.

```
O SA - Broker found (~3s) and retrieved (~6s) 2,083 event(s).
└─O Broker1 - Broker (3s)
  ├─O Broker2 - Broker (3s)
  │ └─O Concentrator - Concentrator (3s)
  └─O Broker3 - Broker (<1s)
    └─O LogHybrid - Concentrator (<1s)
```

The following figure is an example of the information in the Query Console for Version 11.4 after a query that includes a text filter executes. Notice that the query is shown in two fields, Meta Filter and Text Filter.



action = ' value 1 ' × log ×

Service Queried: local-concentrator **Time:** "2017-10-15 18:23:00" - "2017-10-16 18:22:59"

Meta Filter: action = 'value 1'

Text Filter ⓘ**:** log

Progress: Complete All services are online. ○ [redacted] **concentrator** found (<1s) 500 event(s).
● [redacted]**broker** (<1s)

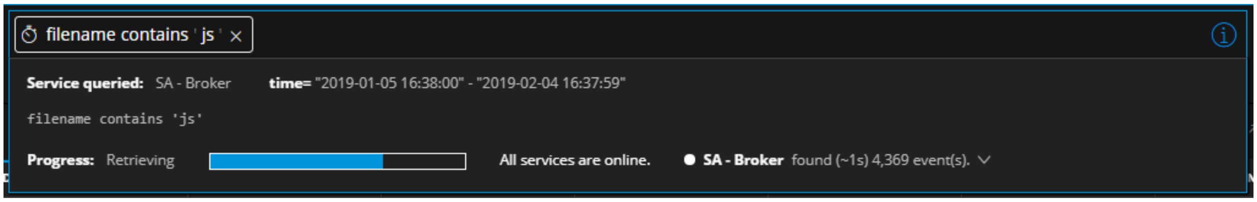
While a query is executing, a progress bar indicates the query's completion percentage at the bottom of the console. The status lets you know details about what is happening; for example, you can tell when the query is executing, queued, reading the index file for the queried service, retrieving events, 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.



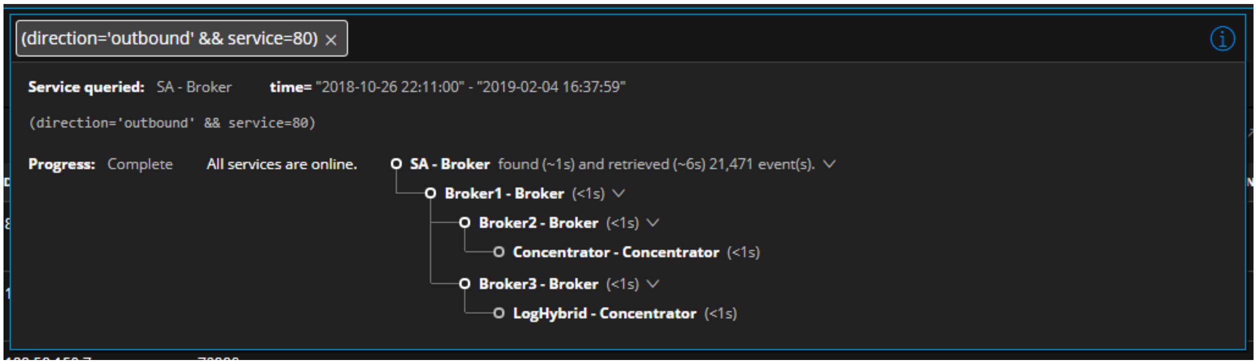
filename contains ' js ' ×

Service queried: SA - Broker **time=** "2019-01-05 16:38:00" - "2019-02-04 16:37:59"

filename contains 'js'

Progress: Retrieving All services are online. ● **SA - Broker** found (~1s) 4,369 event(s).

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.



(direction='outbound' && service=80) ×

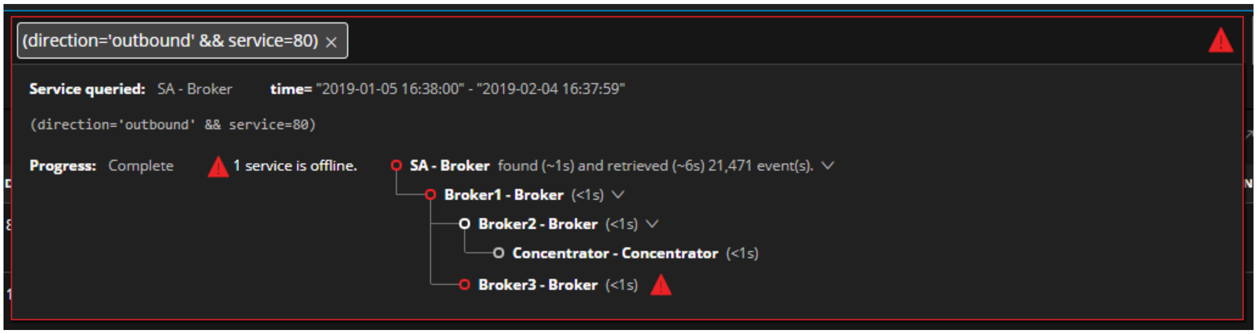
Service queried: SA - Broker **time=** "2018-10-26 22:11:00" - "2019-02-04 16:37:59"

(direction='outbound' && service=80)

Progress: Complete All services are online. ○ **SA - Broker** found (~1s) and retrieved (~6s) 21,471 event(s).
○ **Broker1 - Broker** (<1s)
○ **Broker2 - Broker** (<1s)
○ **Concentrator - Concentrator** (<1s)
○ **Broker3 - Broker** (<1s)
○ **LogHybrid - Concentrator** (<1s)

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.



(direction='outbound' && service=80) ×

Service queried: SA - Broker **time=** "2019-01-05 16:38:00" - "2019-02-04 16:37:59"

```
(direction='outbound' && service=80)
```

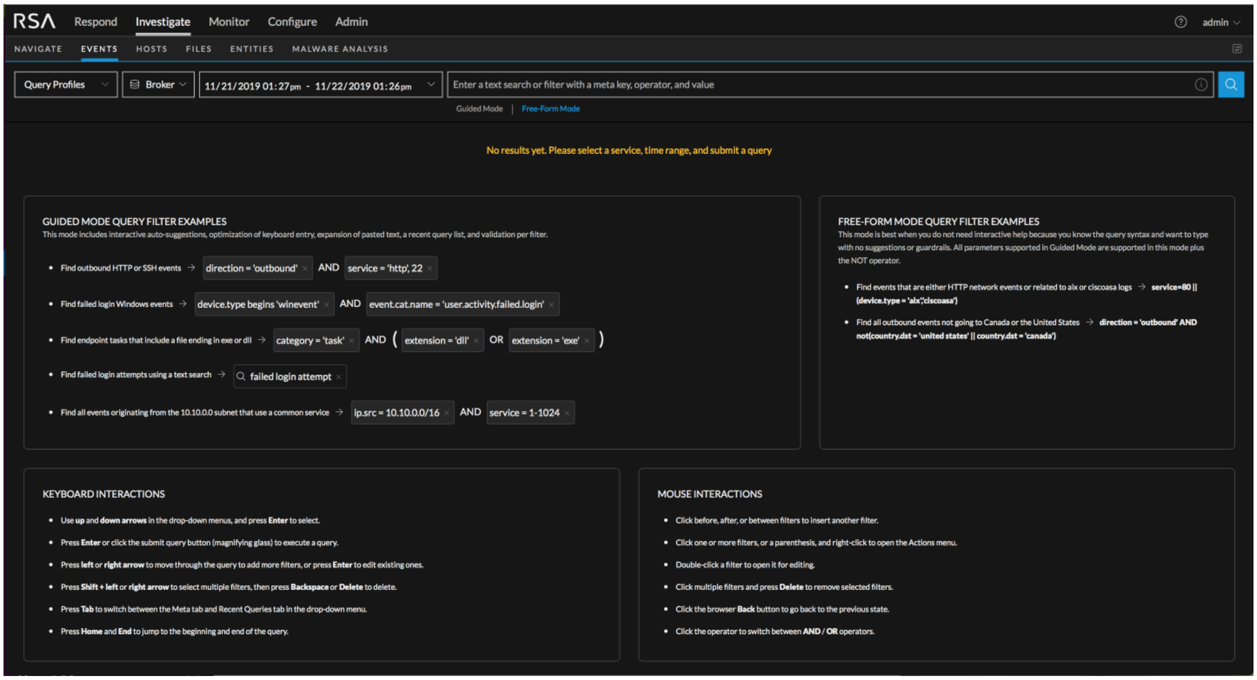
Progress: Complete ⚠ 1 service is offline.

- **SA - Broker** found (~1s) and retrieved (~6s) 21,471 event(s).
  - **Broker1 - Broker** (<1s)
    - **Broker2 - Broker** (<1s)
      - **Concentrator - Concentrator** (<1s)
    - **Broker3 - Broker** (<1s) ⚠

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.

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 Events view with Guided Mode in effect in the query bar (Version 11.3 and earlier).



11/21/2019 01:27pm - 11/22/2019 01:26pm

Enter a text search or filter with a meta key, operator, and value

No results yet. Please select a service, time range, and submit a query

GUIDED MODE QUERY FILTER EXAMPLES

This mode includes interactive auto-suggestions, optimization of keyboard entry, expansion of pasted text, a recent query list, and validation per filter.

- Find outbound HTTP or SSH events → direction = 'outbound' × AND service = 'http', 22 ×
- Find failed login Windows events → device.type begins 'winevent' × AND event.cat.name = 'user.activity.failed.login' ×
- Find endpoint tasks that include a file ending in exe or dll → category = 'task' × AND (extension = 'dll' × OR extension = 'exe' ×)
- Find failed login attempts using a text search → failed login attempt ×
- Find all events originating from the 10.10.0.0 subnet that use a common service → ip.src = 10.10.0.0/16 × AND service = 1-1024 ×

FREE-FORM MODE QUERY FILTER EXAMPLES

This mode is best when you do not need interactive help because you know the query syntax and want to type with no suggestions or guardrails. All parameters supported in Guided Mode are supported in this mode plus the NOT operator.

- Find events that are either HTTP network events or related to aix or ciscoasa logs → **service=80 || (device.type = 'aix','ciscoasa')**
- Find all outbound events not going to Canada or the United States → **direction = 'outbound' AND not(country.dst = 'united states' || country.dst = 'canada')**

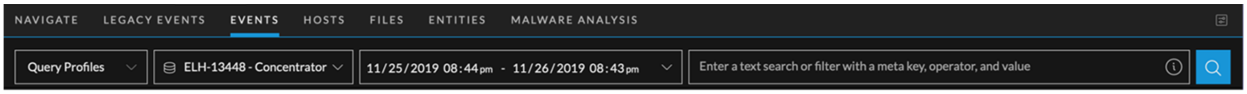
KEYBOARD INTERACTIONS

- Use **up** and **down arrows** in the drop-down menus, and press **Enter** to select.
- Press **Enter** or click the submit query button (magnifying glass) to execute a query.
- Press **left** or **right arrow** to move through the query to add more filters, or press **Enter** to edit existing ones.
- Press **Shift + left** or **right arrow** to select multiple filters, then press **Backspace** or **Delete** to delete.
- Press **Tab** to switch between the Meta tab and Recent Queries tab in the drop-down menu.
- Press **Home** and **End** to jump to the beginning and end of the query.

MOUSE INTERACTIONS

- Click before, after, or between filters to insert another filter.
- Click one or more filters, or a parenthesis, and right-click to open the Actions menu.
- Double-click a filter to open it for editing.
- Click multiple filters and press **Delete** to remove selected filters.
- Click the browser **Back** button to go back to the previous state.
- Click the operator to switch between **AND / OR** operators.

There is no longer a need to select Guided Mode because all Guided Mode features and more improvements are built in to Version 11.4.1. This figure depicts the query bar in Version 11.4.1.


NAVIGATE
LEGACY EVENTS
EVENTS
HOSTS
FILES
ENTITIES
MALWARE ANALYSIS
Query Profiles
ELH-13448 - Concentrator
11/25/2019 08:44pm - 11/26/2019 08:43pm
Enter a text search or filter with a meta key, operator, and value

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.

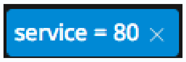
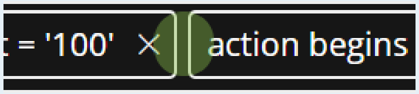
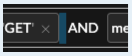
Action	Keyboard Entry
Copy all filters (Version 11.4.1 and later)	With the cursor in the query bar, but not in a filter being edited, and all filters selected, press **Ctrl-C** (Windows OS) or **Cmd-C** (MacOS).
Delete characters in a filter	Selected characters: With characters selected in the query bar, press **Delete** or **Backspace**. Previous character (Version 11.4 and later): With the cursor next to a character in the query bar, press **Backspace** (Windows OS) or **Delete** (MacOS). All characters (Version 11.4 and later): With the cursor in a filter, press **Delete** (Windows OS) or **Fn + Delete** (MacOS).
Delete filters	Selected filters: With one or more filters selected do one of the following: • **Right-click > Delete selected filters** or **Delete selection** (11.4 and later). • Press **Delete**. • Press **Backspace**. Filter that has focus (Version 11.4 and later): With the cursor in a filter that has focus, press **Backspace** (Windows OS) or **Delete** (MacOS). The focused filter is deleted and focus moves to the left. Filter that has focus (Version 11.4 and later): With the cursor in a filter that has focus, press **Delete** (Windows OS) or **Fn + Delete** (MacOS). The focused filter is deleted and the focus moves to the right.
Delete parentheses in a filter, do not delete the contents (Version 11.4 and later)	With a set of parentheses, but not the contents selected, press **Delete** (Windows OS) or **Fn + Delete** (MacOS). The selected parentheses are deleted, but the contents of the parentheses remain.

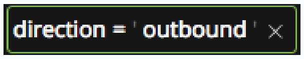
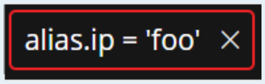
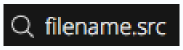
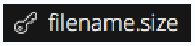
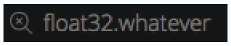
Action	Keyboard Entry
Delete parentheses and their contents in a filter (11.4 and later)	Selected parentheses: With a set of parentheses selected, do one of the following: • **Right-click > Delete selection**. • Press **Backspace** (Windows OS) or **Delete** (MacOS). The selected parentheses and contents are deleted and the focus moves to the left. • Press **Delete** (Windows OS) or **Fn + Delete** (MacOS). The selected parentheses and contents are deleted and the focus moves to the right.
Deselect all filters	With a filter selected, press **Esc**.
Edit a selected filter	With a single filter selected, press **Enter**.
Insert a new filter at the beginning of the query bar, and open for editing (Version 11.4 and later)	With a filter selected, press **Home** (Windows OS) or **Fn + Left Arrow** (MacOS).
Insert a new filter at the end of the query bar, and open for editing (Version 11.4 and later)	With a filter selected, press **End** (Windows OS) or **Fn + Right Arrow** (MacOS).
Insert a new filter to the immediate left of the selected filter, and open for editing	With a filter selected, press **Shift + Left Arrow**.
Insert a new filter to the immediate right of the selected filter, and open for editing.	With a filter selected, press **Shift + Right Arrow**.
Insert a new filter to the immediate left of the selected filter	With a filter selected, press the **Left Arrow**.
Insert a new filter to the immediate right of the selected filter	With a filter selected, press the **Right Arrow**.
Open a new tab with the selected filters	With filters selected, **right-click > Query with selected filters in a new tab**.
Query with the selected filters	With filters selected, **right-click > Query with selected filters**.

Action	Keyboard Entry
Query with content of parentheses (Version 11.4 and later)	With parentheses selected: • To query with the selected parentheses contents, select one side of a parentheses set and **right-click** > **Query with selected filters**. • To query with the selected parentheses contents in a new browser tab, select one side of a parentheses set and **right-click** > **Query with selected filters in new tab**.
Select all filters in the query bar (Version 11.4.1 and later)	With the cursor in the query bar, but not in a filter being edited, press **Ctrl-A** (Windows OS) or **Cmd-A** (MacOS).
Select all filters to the left of the current filter	(Version 11.3.x and earlier) With a filter selected, press **Shift** + **Up Arrow**. (Version 11.4 and later) With a filter selected, press **Shift** + **Right Arrow** twice.
Select all filters to the right of the current filter	(Version 11.3.x and earlier) With a filter selected, press **Shift** + **Down Arrow**. (Version 11.4 and later) With a filter selected, press **Shift** + **Right Arrow** twice.
Select the filter to the immediate left if one exists	With no filter selected, press the **Left Arrow** key.
Select the filter to the immediate right if one exists	With no filter selected, press the **Right Arrow** key.
Submit a query.	With focus on the query bar and no pending filters, press **Enter**.

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	 service = 80 ×	Indicates that a filter is selected.
Green circle between two filters	 = '100' × action begins  GET' × AND me	(Version 11.3 and earlier) A green circle indicates the location of the cursor between two existing filters. Clicking inserts a new filter at this location. (Version 11.4) A bold cursor indicates the insertion point.

Feedback	Icon	Description
Green filter outline	 direction = ' outbound ' ×	Marks the single filter that has focus and ready to edit. This is combined with the blue background, when multiple filters are selected and this filter has focus.
Red filter outline	 alias.ip = 'foo' ×	Indicates that the filter is invalid. A tool tip that explains the error is displayed.
Index indicators in the Meta tab	🔍	(Version 11.4 and later) Indicate the index level of the meta keys in the Meta tab, which determines if you can use it in a filter:  filename.src This meta key is indexed by meta value and can be used in a filter.  filename.size This meta key is indexed by meta key, and can be used in a filter.  float32.whatever This meta key is not indexed, and not selectable for a filter. The `sessionID` meta key is a special case. Unlike other non-indexed meta keys, it is not configurable, but you can use it in a filter so it is marked by the key symbol. Supported operators are `exists`, `!exists`, `=`, and `!=`.

Feedback	Icon	Description
Query Events button	🔍	Used to submit a query, show the status of the query, and cancel a query. The 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	⏱	In the query console, marks the service that took the longest time to load results from the query.
Spinner in the Events list	◔	Indicates that the query is currently being processed. The **Query Events** button is disabled while this occurs.
Stopwatch	⏱	Indicates that the 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 Guided Mode:

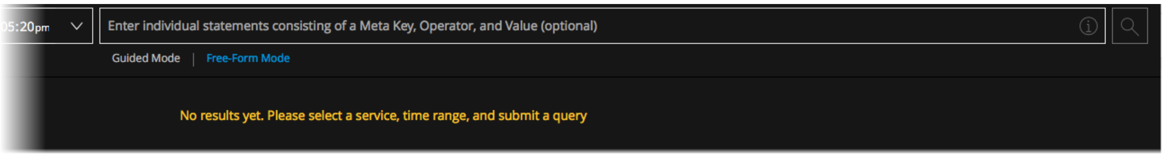
1. Go to the **Events** view (Event Analysis view in Version 11.3 and earlier) and do one of the following:

   a. (Version 11.4.1 and later) Click in the query bar and when the filter entry form is displayed, select the Meta tab if it is not already selected.

   b. (Version 11.4 and later) Select **Guided Mode**, click in the query bar and when the filter entry form is displayed, select the Meta tab if it is not already selected.

   c. (Version 11.2 and later) Select **Guided Mode** and click in the query bar.

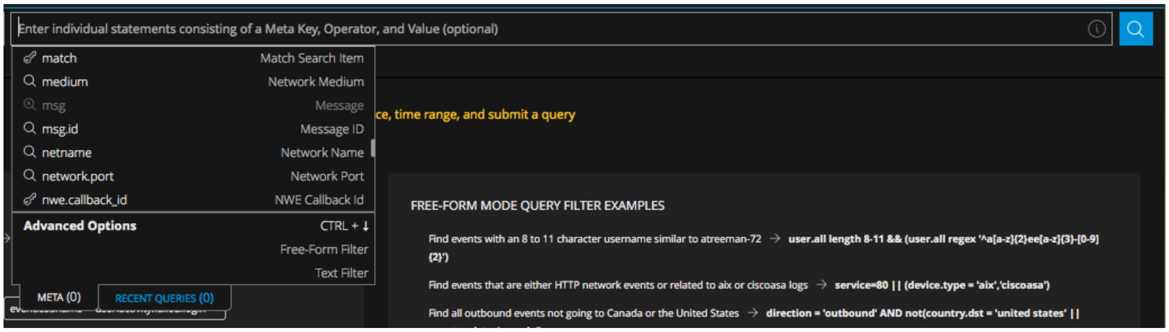
   d. (Version 11.1) Click in the empty query bar, or before or after an existing filter. This is an example of the empty query bar in Guided Mode before you begin entering a filter.



Enter individual statements consisting of a Meta Key, Operator, and Value (optional)

No results yet. Please select a service, time range, and submit a query

If the insertion point is between two filters, a green circle (Version 11.3 and earlier) or a bold cursor (Version 11.4 and later) marks the insertion point. If the insertion point is at the end of the query bar, the filter entry form opens with a blinking cursor at the entry point. A drop-down list displays the available meta keys passed from the service being investigated in alphabetical order. This figure shows the filter entry form from Version 11.4.



Enter individual statements consisting of a Meta Key, Operator, and Value (optional)

ce, time range, and submit a query

FREE-FORM MODE QUERY FILTER EXAMPLES

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}')**

Find events that are either HTTP network events or related to aix or ciscoasa logs → **service=80 || (device.type = 'aix','ciscoasa')**

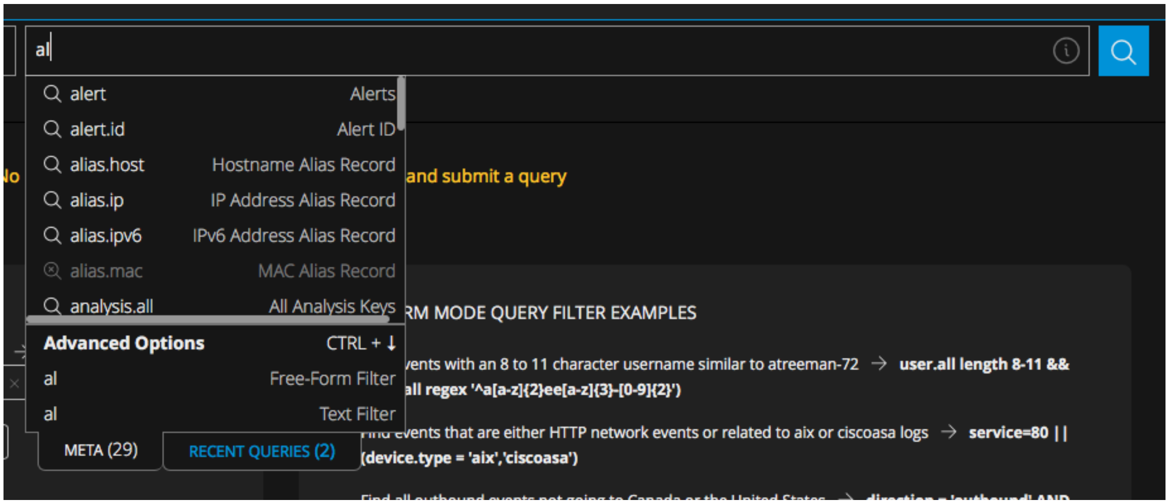
Find all outbound events not going to Canada or the United States → **direction = 'outbound' AND not(country.dst = 'united states' ||**

2. To select a meta key do one of the following:

   a. If there is only one option in the drop-down list, press **Enter**.

   b. If there are two or more options in the drop-down list, click a meta key or select a meta key using the up/down arrows, then press **Enter**.

   c. Start typing the meta key. As you type the meta key, the list is filtered to include only meta keys that contain the text you typed. The count next to the label on the Meta (0) tab increments to enumerate the indexed meta keys that match the typed text. Keys that are not indexed are disabled and not selectable and are not included in the count, for example, `alias.mac` in the figure below is not indexed and is dimmed. Click a meta key or select a meta key using the up/down arrow, then press **Enter**.


al
alert Alerts
alert.id Alert ID
alias.host Hostname Alias Record
alias.ip IP Address Alias Record
alias.ipv6 IPv6 Address Alias Record
alias.mac MAC Alias Record
analysis.all All Analysis Keys
Advanced Options CTRL + ↓
al Free-Form Filter
al Text Filter
META (29)
RECENT QUERIES (2)

No ... and submit a query

RM MODE QUERY FILTER EXAMPLES

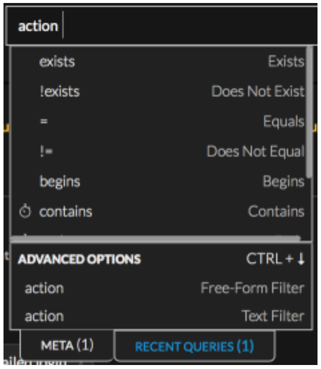
ents with an 8 to 11 character username similar to atreeman-72 → **user.all length 8-11 && all regex '^a[a-z]{2}ee[a-z]{3}-[0-9]{2}')**

events that are either HTTP network events or related to aix or ciscoasa logs → **service=80 || (device.type = 'aix','ciscoasa')**

d. To select a highlighted meta key, press **Enter**.
The count on the Meta label changes to 1.

> **Note:** If no meta key in the drop-down list is selected, and the list has no meta keys to select, either the Free-Form Filter or the Text Filter option is highlighted based on the content already typed in the query bar.
> --If the text typed in the query bar includes some form of query syntax and other operators not yet supported by the user interface, the Free-Form Filter option is highlighted and you can create a free-form filter. In Version 11.3 and earlier, the `**`, `&&`, `||`, `()`, `AND`, `OR`, `comma`, `-`, `length`, and `regex` operators are not supported by the user interface. The Version 11.4 user interface supports these operators. If the Free-Form Filter is not highlighted, and the query bar has no text filter, the Text Filter is highlighted so you can create one.
> --If the first condition is true, and there is already one text filter, the Free-Form Filter option is highlighted so you can create a free-form filter.

e. If you want to edit or delete the meta key, press **Backspace** or **Delete**.
As you backspace and delete characters, the meta key drop-down list is filtered to include meta keys that contain those characters. To select a meta key, press **Enter**.
The meta key is added to the filter entry form, and 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 marking the `contains` operator.



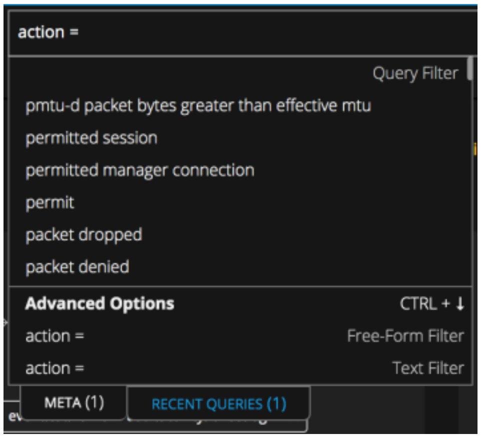
3. To select an operator, do one of the following:

a. If there is only one option in the operators drop-down list, press **Enter** to select it.

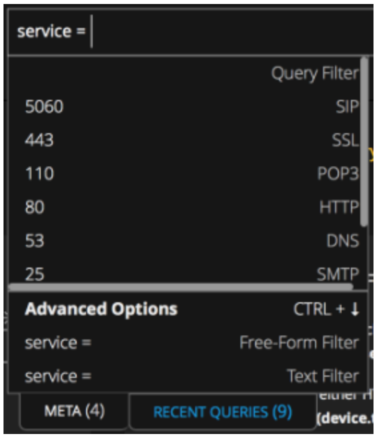
b. If there are two or more options in the operators drop-down list, click an operator or select one using the up/down arrows, then press **Enter**.

c. Type the operator and press **Enter**. As you type, the operators drop-down list is filtered to show only operators that contain the typed text. Click an operator or select one using the up/down arrows, then press **Enter**.
The operator is added to the filter entry form. In Version 11.4 and later, if the operator accepts a value, the suggested values drop-down list is displayed. Earlier versions leave the cursor in the

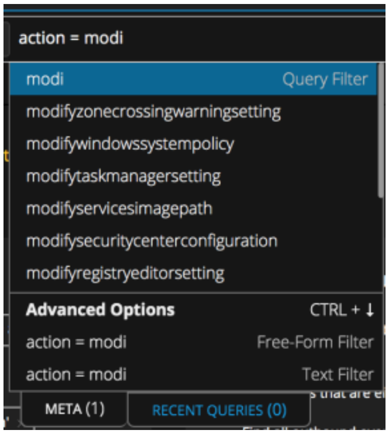
filter entry form so that you can type a value.



4. (Optional) If the selected operator in the filter entry form accepts a value, do one of the following:
   a. In Version 11.3 and earlier, type the value and press **Enter**.
   b. In Version 11.4 and later, paste a value that you have copied from somewhere and press **Enter**.
   c. In Version 11.4 and later, begin typing in the **Query Filter** field.
   As you type, the meta value drop-down list is filtered to return up to 100 properly indexed values that begin with the typed text. The suggested values are based solely on the time range; filters in the query do not filter the list of 100. The auto-suggest function looks for matches in all events in the current data set, not just the (up to 10,000) downloaded events. If nothing in the list matches exactly, the text you typed in the Query Filter field is highlighted and this message tells you that no suggestions were found. Some values, such as the integers for the `service` meta key, also display the definition of the service type.



   If there is an exact match, that value is highlighted. In the following example, there is no exact match for the typed text, modi.



action = modi

modi Query Filter

modifyzonecrossingwarningsetting

modifywindowssystempolicy

modifytaskmanagersetting

modifyservicesimagepath

modifysecuritycenterconfiguration

modifyregistryeditorsetting

Advanced Options CTRL + ↓

action = modi Free-Form Filter

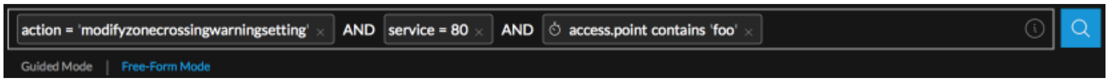
action = modi Text Filter

   i. If the typed text is the value you want to use in the filter, press **Enter**.

   ii. If you see the value that you want to query in the list and it is not highlighted, click the value or use the up/down arrows to highlight the value. Then press **Enter**.

   iii. If you want to edit or delete the value, press **Backspace** or **Delete**.
   As you backspace and delete a character, the meta value drop-down list is filtered to include values that begin with the remaining characters. To select a value, press **Enter**.
   The value is added to the filter entry form.

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 list 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.



action = 'modifyzonecrossingwarningsetting' AND service = 80 AND access.point contains 'foo'

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 10,000 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 ⓘ.

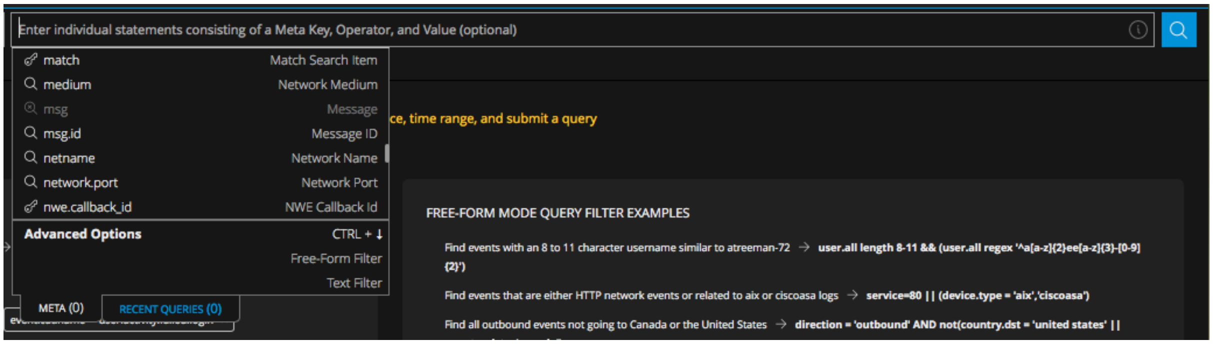
8. (Optional in Version 11.3 and later) If you want to cancel the query before it finishes executing, click ⊡.
   The query stops executing and a notification that the query has been canceled is displayed.

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

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

1. Go to the **Events** view, select **Guided Mode** below the query bar, and click in the query builder field. (For Version 11.4.1, simply click in the query builder field.)
   If the insertion point is between two filters, a green circle or a bold cursor 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.


Enter individual statements consisting of a Meta Key, Operator, and Value (optional)
match Match Search Item
medium Network Medium
msg Message
msg.id Message ID
netname Network Name
network.port Network Port
nwe.callback_id NWE Callback Id
Advanced Options CTRL + ↓
Free-Form Filter
Text Filter
META (0)
RECENT QUERIES (0)

ce, time range, and submit a query

FREE-FORM MODE QUERY FILTER EXAMPLES

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}')

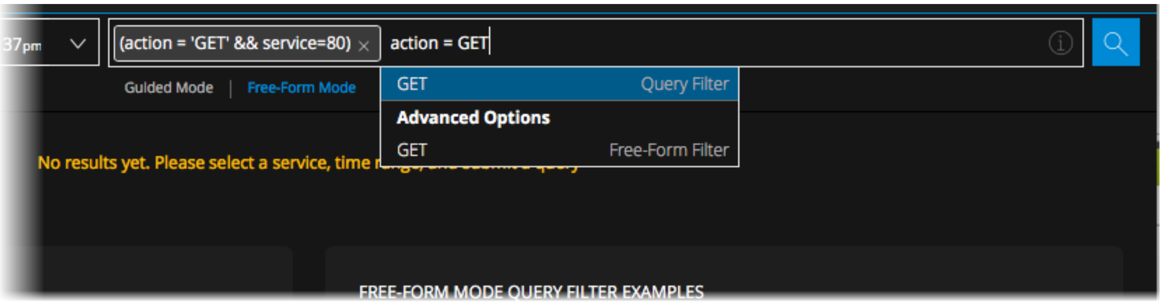
Find events that are either HTTP network events or related to aix or ciscoasa logs → service=80 || (device.type = 'aix','ciscoasa')

Find all outbound events not going to Canada or the United States → direction = 'outbound' AND not(country.dst = 'united states' ||

2. Do one of the following:

    a. Place the cursor in the **Free-Form Filter** field and begin typing the query.

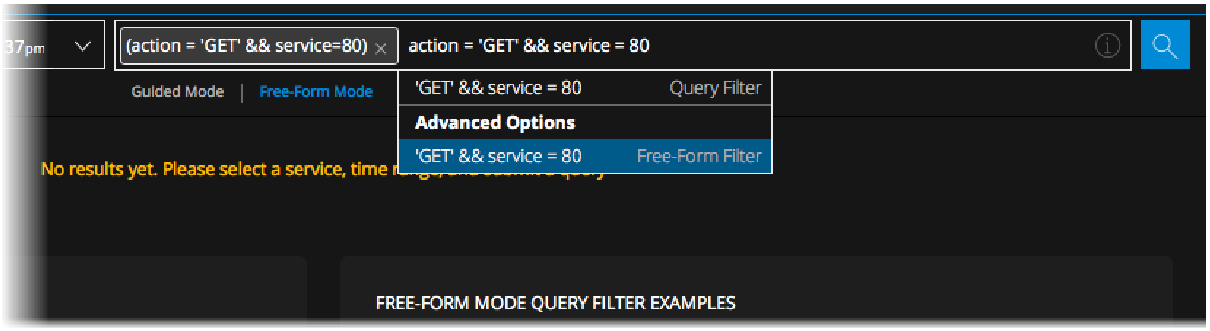
    b. Begin typing the filter beginning with a meta key or with an open parenthesis. When entering and editing filters in the query builder, parentheses pairs are automatically balanced. If you type an open parenthesis, the other part of the pair is added to the filter.
    When no matching meta keys or 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.



No results yet. Please select a service, time r

FREE-FORM MODE QUERY FILTER EXAMPLES

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 free-form expression created by continuing to type after the value GET.

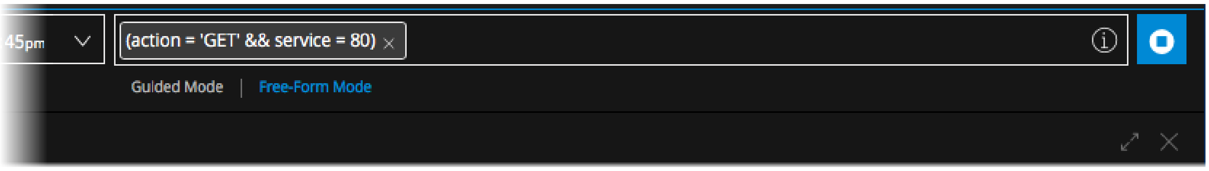

37pm
(action = 'GET' && service=80)
action = 'GET' && service = 80
Guided Mode | Free-Form Mode
'GET' && service = 80 Query Filter
Advanced Options
'GET' && service = 80 Free-Form Filter

No results yet. Please select a service, time r

FREE-FORM MODE QUERY FILTER EXAMPLES

The new filter is inserted, and the blinking cursor is refocused after the last filter, a new filter entry form 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 ⏹.



(action = 'GET' && service = 80) ×

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.

Add a Text Filter to Find a Value Anywhere in the Data Set (Version 11.4 and Later)

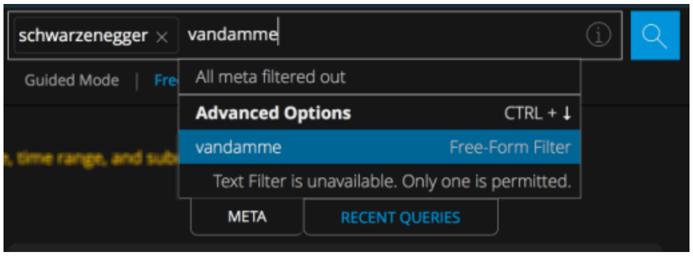
In Version 11.4 and later, the text filter allows you to find a specific value in the current data set (endpoint, logs, and network events). The text filter initiates a case-insensitive search against all the data for meta keys that are indexed by value. The text filter does not search for values that are indexed by meta key or not indexed so you not see all results. A message advises that `Results may be limited by a text filter, which matches only indexed meta keys. If you want to conduct a more exhaustive search against raw events, click here and choose the appropriate options in the Search Events drop-down menu.` Icons in the drop-down list indicate the index level of each meta key:

- filename.size - indexed by meta key
- filename.src - indexed by meta value
- float32.whatever - not indexed

> **Note:** All services in the hierarchy being queried (Broker, Concentrators, and Decoders) must be at Version 11.3 or later. The text filter is not available in the drop-down menu when there are services below Version 11.3 in the hierarchy.

The text filter is useful when you have some idea of what you are looking for, but are not sure where to look (which meta key or service). As an example, if you are interested in looking for a file name, click in the query bar, type the complete text string, and click **Text Filter**. The text filter initiates a search against all the data in the index, within the services and time range being investigated, and returns exact matches to the text string.

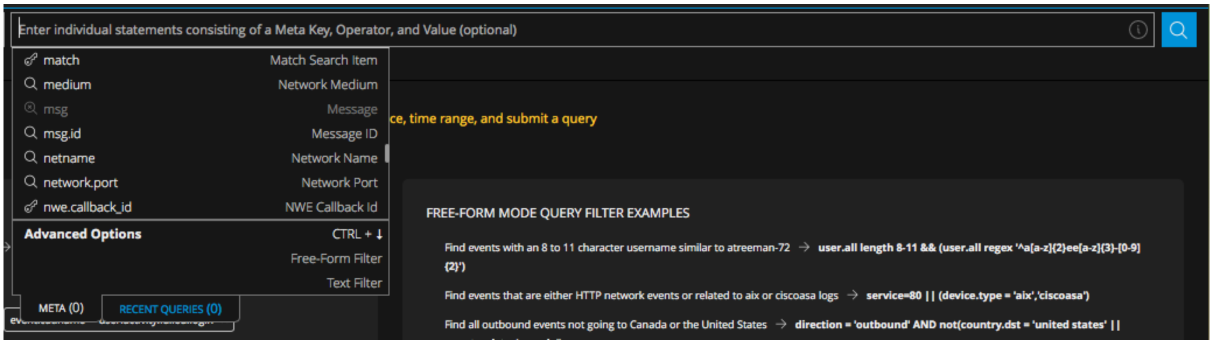
A query can include one text filter and any combination of simple and free-form filters. The operator for a text filter must be AND because it acts as a filter over the results of all the other filters in the entire query. If one text filter already exists in the query bar, the Text Filter option is disabled as shown in the figure below. Text filters are not supported inside parentheses.



Text Filter is unavailable. Only one is permitted.

To create a text filter:

1. Go to the **Events** view and click in the query bar.
   The query entry form is displayed.



Enter individual statements consisting of a Meta Key, Operator, and Value (optional)

ce, time range, and submit a query

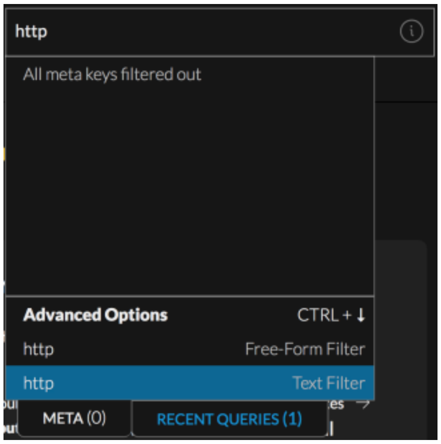
FREE-FORM MODE QUERY FILTER EXAMPLES

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}')

Find events that are either HTTP network events or related to aix or ciscoasa logs → service=80 || (device.type = 'aix','ciscoasa')

Find all outbound events not going to Canada or the United States → direction = 'outbound' AND not(country.dst = 'united states' ||

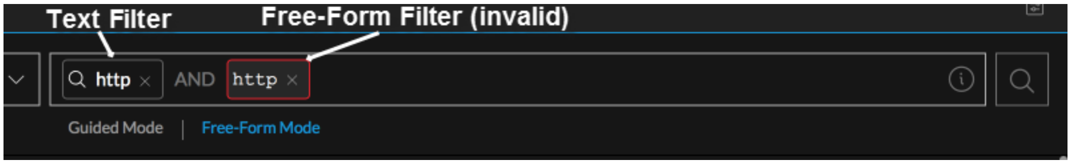
2. Type the text string that you want to find, for example, `http`.
   The text string is displayed in the meta key drop-down list under Advanced Options.



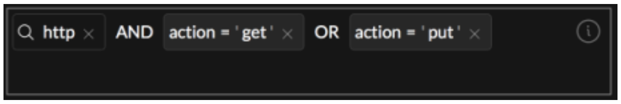
http

All meta keys filtered out

3. Click **Text Filter** under **Advanced Options**.
   The text filter is created in the query bar. The following figure illustrates the different appearance of a text search filter versus a free-form filter. The free-form filter is in a fixed-space font and outlined in red. The red outline indicates a syntax error because a valid expression is expected in a free-form filter. The text filter is marked by the search icon. No syntax requirements are applied to text search filters.

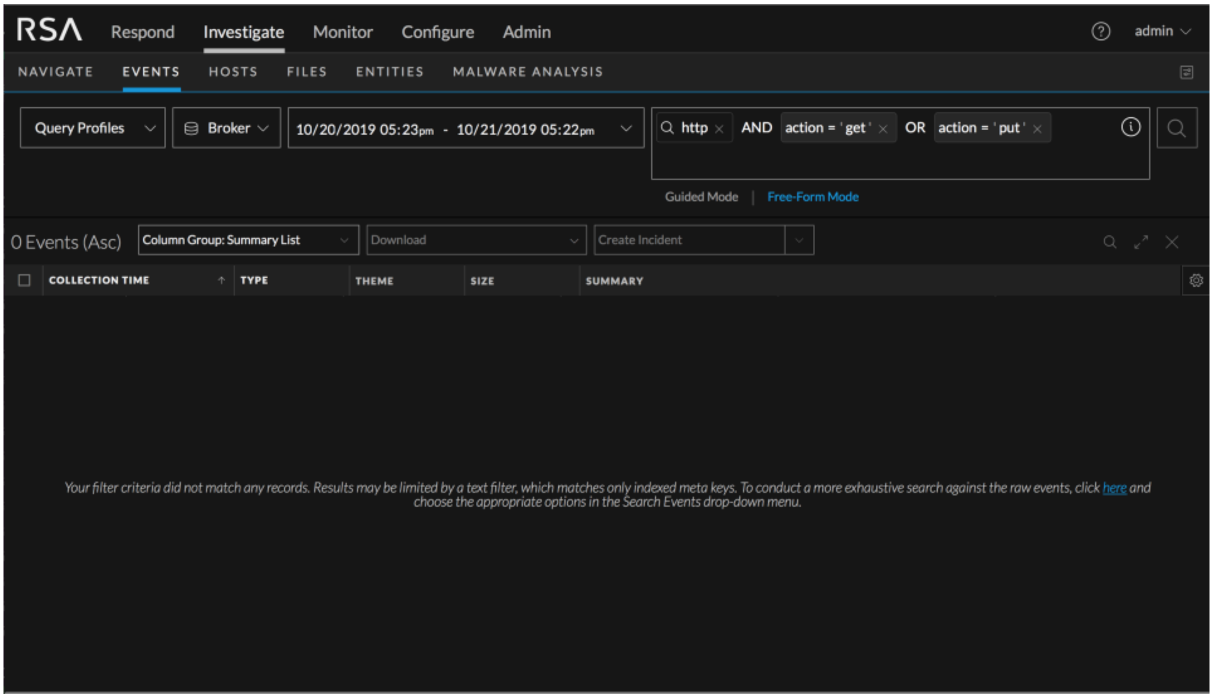


4. (Optional) Create additional simple or free-form filters in the query bar. There can be only one text filter in the query. This example was created by typing `http` as a text filter and then adding two more filters - `action = 'get' OR action = 'put'`



5. To submit the query, click 🔍.
   The results are displayed in the Events panel. This figure illustrates the Events panel with no results

displayed and a message with instructions for improving results. Every time you use a text filter, this message is at the bottom of the results offering a link to expand your search.



10/20/2019 05:23pm - 10/21/2019 05:22pm

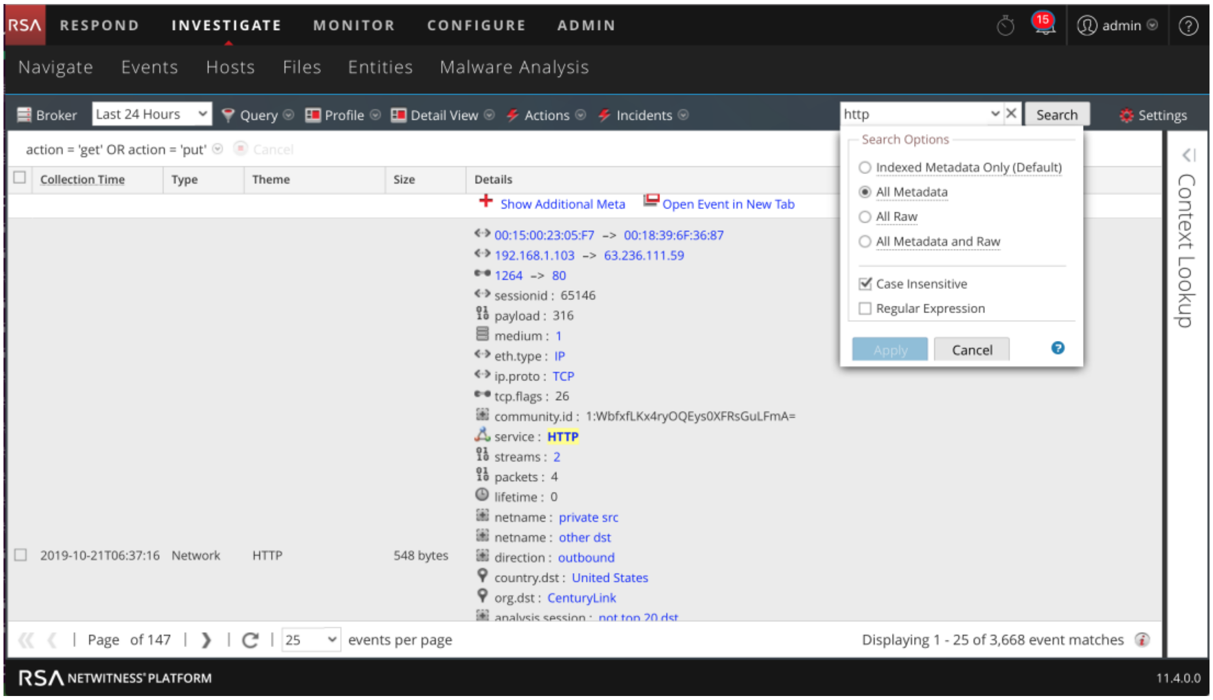
http AND action = 'get' OR action = 'put'

0 Events (Asc)

Your filter criteria did not match any records. Results may be limited by a text filter, which matches only indexed meta keys. To conduct a more exhaustive search against the raw events, click here and choose the appropriate options in the Search Events drop-down menu.

6. Click the **here** link in the message.

 A new browser tab opens with the query results displayed in the Legacy Events view, where you have additional options to improve the search. This figure shows the results for the same query when non-indexed metadata is included.



Last 24 Hours

http

action = 'get' OR action = 'put'

Search Options

○ Indexed Metadata Only (Default)

● All Metadata

○ All Raw

○ All Metadata and Raw

☑ Case Insensitive

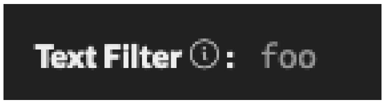
☐ Regular Expression

Collection Time	Type	Theme	Size	Details
2019-10-21T06:37:16	Network	HTTP	548 bytes	00:15:00:23:05:F7 -> 00:18:39:6F:36:87 192.168.1.103 -> 63.236.111.59 1264 -> 80 sessionid : 65146 payload : 316 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 26 community.id : 1:WbfxfLKx4ryOQEys0XFRsGuLFmA= service : HTTP streams : 2 packets : 4 lifetime : 0 netname : private src netname : other dst direction : outbound country.dst : United States org.dst : CenturyLink analysis.session : not top 20 dst

25

Displaying 1 - 25 of 3,668 event matches

7. Click the Information icon ⓘ in the query console to view the status of the query. This figure shows a text filter in the query console.



Text Filter ⓘ: foo

Select All Filters and Copy All Filters in the Query Bar (Version 11.4.1 and Later)

While creating a filter in the Events view query bar, you can use keyboard commands to select all filters (Ctrl-A for Windows OS, Cmd-A for MacOS) and then copy the selection to the local clipboard (Ctrl-C for Windows OS, Cmd-C for MacOS).

To select all filters and copy them to the clipboard:

1. In the **Events** view > **Events** panel, click on a focused pill or in the query entry form, and press **Ctrl-A** for Windows OS or **Cmd-A** for MacOS.
   All filters in the query bar are selected.
2. To copy the selected filters to the clipboard, type **Ctrl-C** for Windows OS or **Cmd-C** for MacOS.
   You can share the clipboard with other analysts or paste the contents in the query bar.

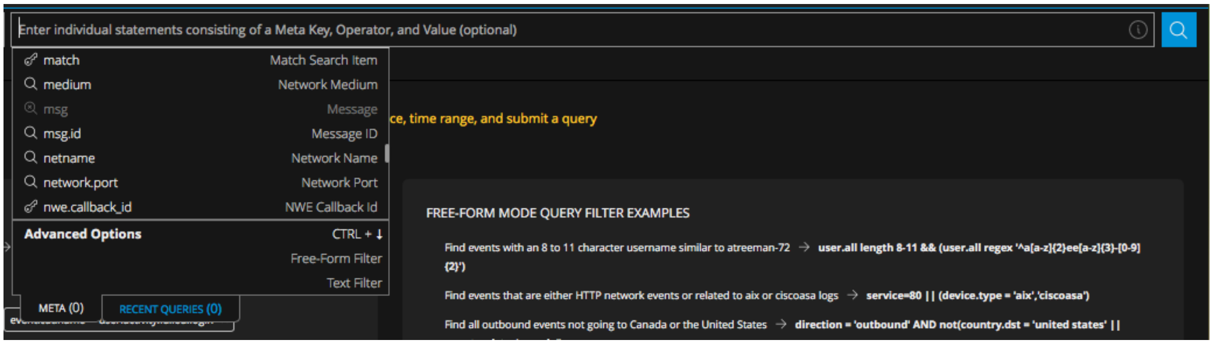
Paste Text in the Query Bar (Version 11.4 and Later)

While creating a filter in the Events view query bar, you can paste instead of typing the complete text of a filter that you have copied from somewhere else. You can paste the text into an empty query bar or next to an existing filter in the query bar. Depending on the text you typed, the query parsing engine parses the information that you pasted and creates a new filter, which can be a simple filter, a free-form filter, or a text filter.

- A text string of this form is added as a new simple filter in the query bar: `<valid meta key> <valid operator> <optional value>`. This is an example: `alias.host contains 's'`.
- A text string of this form is added as two simple filters in the query bar: `<valid meta key> <valid operator> <optional value> && <valid meta key> <valid operator> <optional value>`. This is an example: `alias.host contains 's' && action exists`, which is converted to `alias.host contains 's' AND action exists`.
- A text string that contains unparsable text may be converted to a free-form filter. For example, using `NOT (device.ip = 10.10.10.10)` is unsupported for creation of a filter in Guided Mode, so this would be converted to a free-form filter. Free-form filters are validated by the server when they are submitted.
- Text that does not conform to the filter syntax is added as a free-form filter.

To create a filter by pasting text:

1. Go to the **Events** view > **Events** panel, select **Guided Mode** under the query bar, and click in the query bar. (For Version 11.4.1, simply click in the query bar.)
   The query entry form is displayed.



FREE-FORM MODE QUERY FILTER EXAMPLES

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}')**

Find events that are either HTTP network events or related to aix or ciscoasa logs → **service=80 || (device.type = 'aix','ciscoasa')**

Find all outbound events not going to Canada or the United States → **direction = 'outbound' AND not(country.dst = 'united states' ||**

2. Type **Ctrl-V** (Windows OS), **Cmd-V** (MacOS), or **right-click** and **Paste** to paste text that you have copied into the clipboard from somewhere else. Do one of the following:

   a. If the text you pasted is a statement that can be parsed, one or more simple filters is created.
      If the text you pasted is a statement that cannot be parsed, a new free-form filter is created.
      If the text you pasted is not a statement and not a valid meta key, an invalid syntax error is displayed.
      If you pasted a valid meta key for a new filter you are building, the meta key is highlighted in the drop-down list, and you can continue creating a filter as usual by entering an operator and a value.
      After you select a valid meta key and a valid operator (for example, `city.dst =`) any text that you paste is treated as a text string if the meta key supports a text value, and one filter is created. If the meta key does not support a text value all of the text in the query bar is parsed as described in step a above.

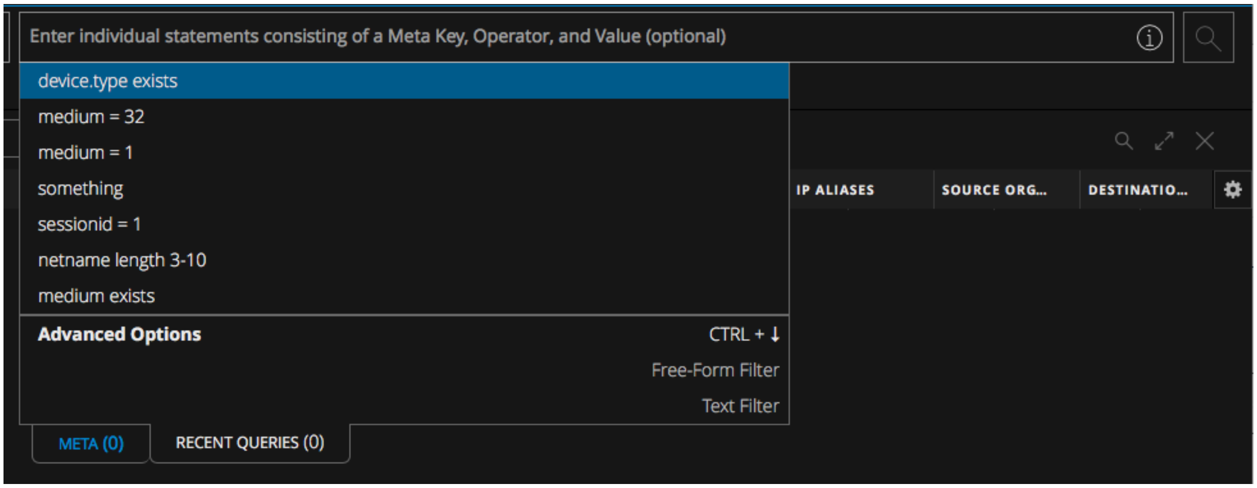
3. Add more filters in the query bar if you wish, and then submit the query.
   The query is executed.

Insert a Filter Based on a Recent Query (Version 11.4 and Later)

In the Guided Mode query bar, you can insert a filter based on a recent query. When the Recent Queries tab is opened and nothing has been typed in the query bar, up to 100 of your most recently executed queries are displayed in a scrollable list. The list is sorted to show the most recent at the top, and the Recent Query count is set to 0. When you begin typing, the list is filtered to display up to 100 queries from the query history database that contain matching text, even if the matches are not in the most recent 100 queries. The Recent Query count changes to reflect the number of matching queries as you type.

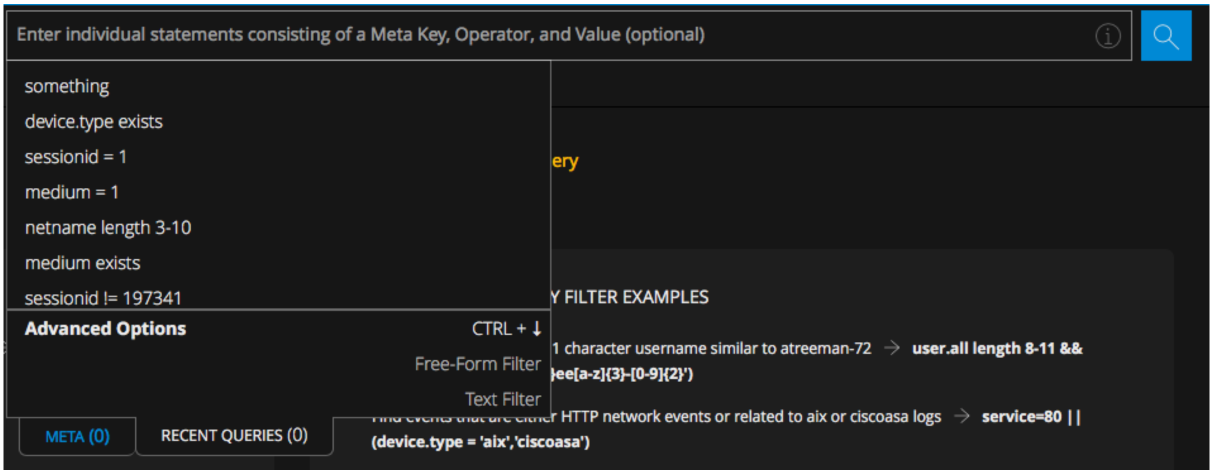
The top entry in the list is highlighted by default. To select a recent query, you can move the highlighting up and down in the list using the up and down arrow or by mouse-over of a recent query. As you type the list is filtered and the highlighting moves back to the top of the list. Clicking a query, or pressing Enter while a query is highlighted, creates a new filter with the text of the selected query.

Whenever you submit a query, the list is sorted to add that query, now the most recent, at the top.



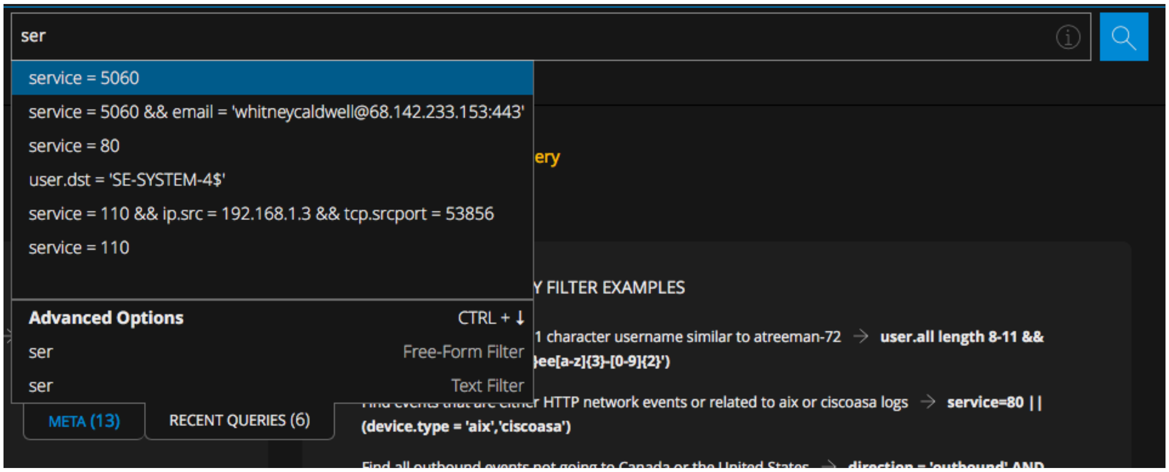
To create a filter based on a recent query:

1. Go to the **Events** view, select **Guided Mode** under the query bar, and click in the query bar. (For Version 11.4.1, simply click in the query bar.)
   The Meta Key drop-down list is displayed in the Meta tab.
2. Select the **Recent Queries** tab.
   The Recent Queries drop-down list is displayed with a count of 0.


Enter individual statements consisting of a Meta Key, Operator, and Value (optional)
something
device.type exists
sessionid = 1
medium = 1
netname length 3-10
medium exists
sessionid != 197341
Advanced Options
CTRL + ↓
Free-Form Filter
Text Filter
META (0)
RECENT QUERIES (0)
ery
Y FILTER EXAMPLES
1 character username similar to atreeman-72 → user.all length 8-11 &&
ee[a-z]{3}-[0-9]{2}')
HTTP network events or related to aix or ciscoasa logs → service=80 ||
(device.type = 'aix','ciscoasa')

3. To search for a recent query, do one of the following:

   a. Begin typing some text.
      As you type more characters or backspace to delete characters, the list is filtered to show recent queries that contain the text you typed. The count in the Recent Queries label increments to show the number of matching queries as you type.



```
ser
service = 5060
service = 5060 && email = 'whitneycaldwell@68.142.233.153:443'
service = 80
user.dst = 'SE-SYSTEM-4$'
service = 110 && ip.src = 192.168.1.3 && tcp.srcport = 53856
service = 110
```

Advanced Options
CTRL + ↓
ser
Free-Form Filter
ser
Text Filter
META (13)
RECENT QUERIES (6)
ery
Y FILTER EXAMPLES
1 character username similar to atreeman-72 → user.all length 8-11 &&
ee[a-z]{3}-[0-9]{2}')
r HTTP network events or related to aix or ciscoasa logs → service=80 ||
(device.type = 'aix','ciscoasa')

b. To select a query and add a new filter, continue to type and use the up and down arrows until the query you want to use as a new filter is highlighted.

c. With a query highlighted, press **Enter** or simply click a query that you see in the list.
The filter is added in the query bar.

4. Add more filters in the query bar if you wish, and then submit the query.
The query is executed and the list is sorted to add that query, now the most recent, at the top.

Edit a Filter in Guided Mode

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

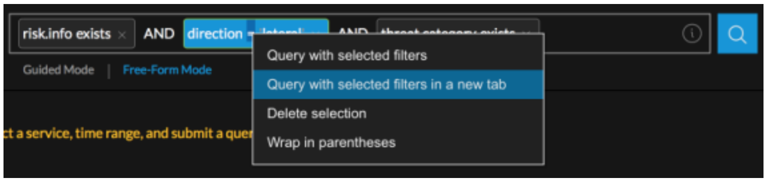
1. Double-click the filter, or click the filter and press **Enter**.
2. Edit the filter. When finished editing, press **Enter** to update the filter.
3. If you want to execute the query again, click 🔍.
The Events panel displays results for the updated filter.

Query Using Selected Filters in Guided Mode

When you have one or more filters in the query bar in Guided Mode, you can refocus the query to include only selected filters, displaying results in the current browser tab or a new browser tab. Some filters include expressions with nested parentheses in Version 11.4, and you can refocus part of a filter that includes nested parentheses. To update the query using only selected filters, do one of the following:

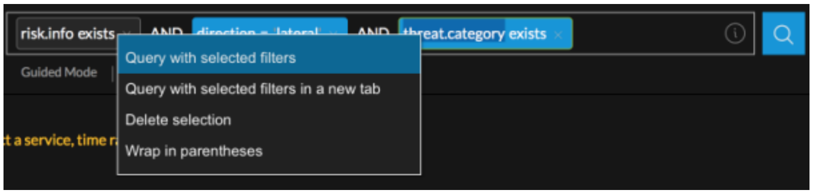
1. Using a query that includes one or more simple filters, for example a query has three filters: `risk.info exists`, `direction ='lateral'`, and `threat.category exists`.

    a. Select `direction = 'lateral'`, right-click the filter and select **Query with selected filters in a new tab** in the drop-down menu.


risk.info exists
AND
direction
Guided Mode
Free-Form Mode
Query with selected filters
Query with selected filters in a new tab
Delete selection
Wrap in parentheses
t a service, time range, and submit a quer

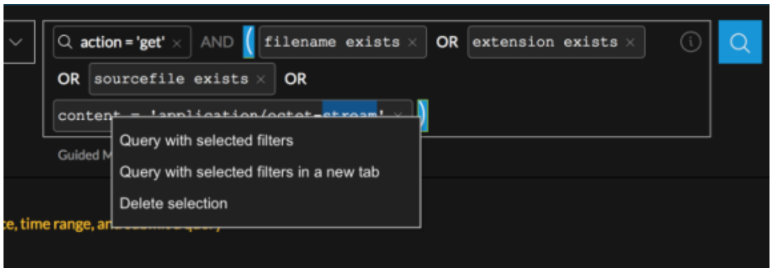
A new tab opens with the results for the selected filter and the original query is left intact on the previous tab.

b. 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.

2. (Version 11.4) For a query that includes a filter containing nested parentheses, for example: `action = 'get' AND (filename exists OR sourcefile exists OR content = 'application/octet-stream')`, do one of the following:



a. Select the close parenthesis after `'application/octet-stream'`, right-click, and select **Query with selected filters in a new tab**.
A new tab opens with results for `(filename exists OR sourcefile exists OR content = 'application/octet-stream')`.

b. Select the same, right-click, and select **Query with selected filters**.
The results for `(filename exists OR sourcefile exists OR content = 'application/octet-stream')` are displayed in the current tab.

Delete a Filter and Delete Text or Parentheses in a Filter in Guided Mode

Some keystroke editing features became available in Version 11.4; these are labeled in the steps.

1. To delete a filter, do any of the following:

a. Click **X** in a filter.

b. Select the filter and press **Delete** (Windows OS) or **Fn** + **Delete** (MacOS).

c. (Version 11.4 and later) Select the filter and press **Backspace** (Windows OS) or **Delete** (MacOS).

d. Right-click one or more filters and select **Delete selected filters** or **Delete selection** (Version 11.4 and later) in the drop-down menu.
The filter and the operator to the right or left of the filter is deleted, ensuring that no extraneous operators remain in the query bar.

2. (Version 11.4 and later) To delete characters in a filter or parentheses and contents in a filter, do any of the following:

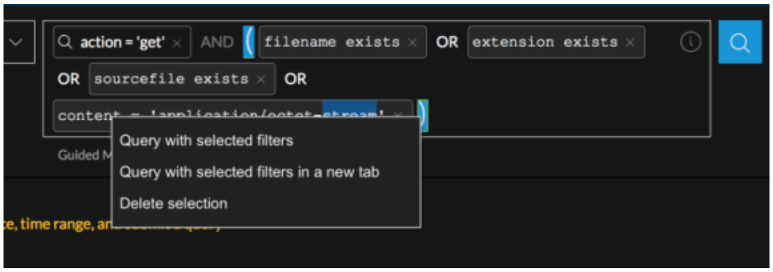
   a. To delete the previous character: With the cursor next to a character in the query bar, press **Backspace** (Windows OS) or **Delete** (MacOS).

   b. To delete all characters: With the cursor in a filter, press **Delete** (Windows OS) or **Fn + Delete** (MacOS).

   c. To delete the selected characters: With characters selected in the query bar, press **Delete** or **Backspace**.

   d. To delete parentheses, but not the characters inside the parentheses, select one of the parentheses and press **Delete** (Windows OS) or **Fn + Delete** (MacOS).

   e. To delete a set of parentheses and the contents, for example, `(filename exists OR sourcefile exists OR content = 'application/octet-stream')`, select the parenthesis after `get`, right-click, and select **Delete selection**.

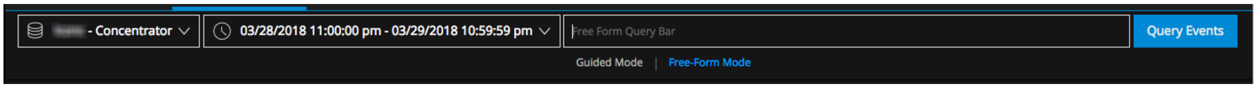


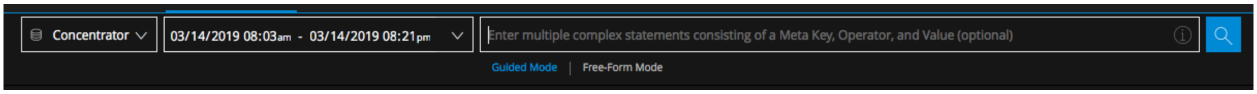
Everything except `action = 'get'` is deleted.

Create a Query in the Free-Form Mode

Free-Form Mode is used in Version 11.2, 11.3, and 11.4, but no longer available in Version 11.4.1.

Free-form queries are most useful when you have a long text string 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 Events view with the empty Free-Form query builder field. The first example is Version 11.2 and the second example is Version 11.3.


[redacted] - Concentrator
03/28/2018 11:00:00 pm - 03/29/2018 10:59:59 pm
Free Form Query Bar
Query Events
Guided Mode
Free-Form Mode


Concentrator
03/14/2019 08:03am - 03/14/2019 08:21pm
Enter multiple complex statements consisting of a Meta Key, Operator, and Value (optional)
Guided Mode
Free-Form Mode

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}')
```

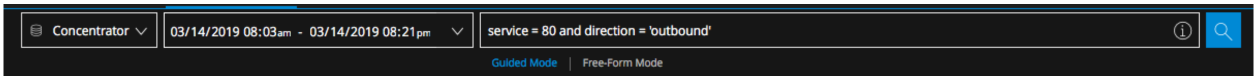
To find events that are either HTTP network events or related to aix or ciscoasa logs:

```
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.



service = 80 and direction = 'outbound'

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 🔍. 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

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

Set the Time Range

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

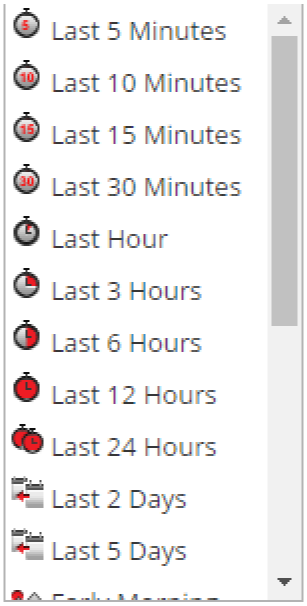
- A time range relative to the collection- ranges relative to the collection are based on the last collection time for data.
- A time range relative to the calendar.
- A custom date range.
- All data.

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.

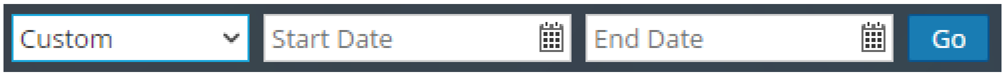


2. Do one of the following:
   - If you want to see all data, select **All Data**.
   - If you want to set a time range in minutes, hours, or days that is relative to the collection, select a value such as **Last 10 minutes**, **Last 3 Hours**, or **Last 5 days**.
   - If you want to set a time range 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.

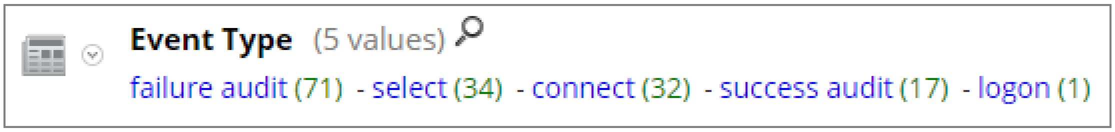
> **Note:** If meta entities (Version 11.1 and later) are used in meta groups, the results will show the top 20 values that matched any of the meta keys contained in the meta entity.

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).

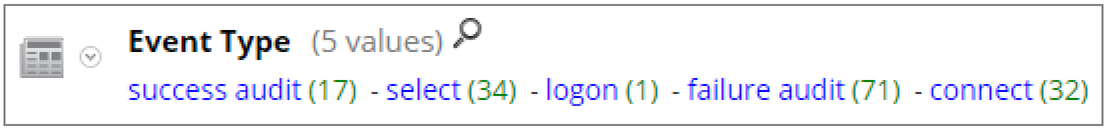
This image shows the `Event Type` meta key presented in order by **Total** in **Descending** order. The value with the greatest count of matches is presented first. The value `failure audit` has 71 matches and is listed first. The value `logon` has only one match and is presented last. The quantification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



Event Type (5 values)

failure audit (71) - select (34) - connect (32) - success audit (17) - logon (1)

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**.



Event Type (5 values)

success audit (17) - select (34) - logon (1) - failure audit (71) - connect (32)

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.

   Event Count

   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: Use Meta Groups to Focus on Relevant Meta Keys.

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.

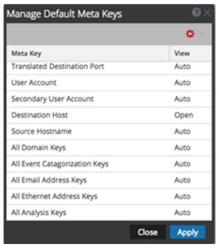
To specify that the initial Navigate view opens using default meta keys:

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:

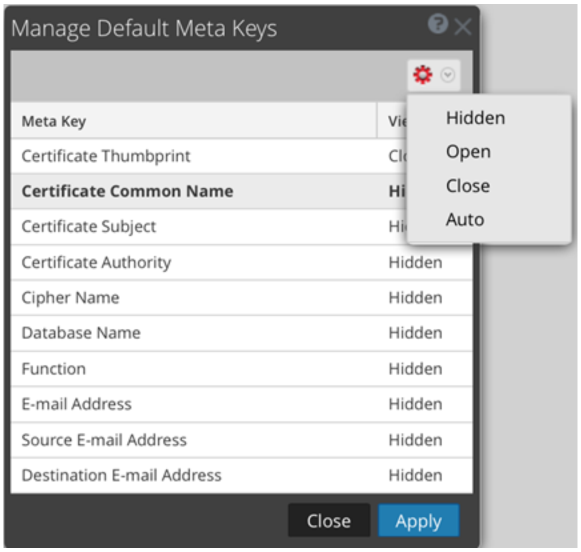
1. In the **Navigate** view toolbar, select **Meta** > **Manage Default Meta Keys**.
   The Manage Default Meta Keys dialog is displayed with the list of available meta keys for the service.



Meta Key	View
Translated Destination Port	Auto
User Account	Auto
Secondary User Account	Auto
Destination Host	Open
Source Hostname	Auto
All Domain Keys	Auto
All Event Catagorization Keys	Auto
All Email Address Keys	Auto
All Ethernet Address Keys	Auto
All Analysis Keys	Auto

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.



Meta Key	Vi
Certificate Thumbprint	Cl
Certificate Common Name	**Hi**
Certificate Subject	Hi
Certificate Authority	Hidden
Cipher Name	Hidden
Database Name	Hidden
Function	Hidden
E-mail Address	Hidden
Source E-mail Address	Hidden
Destination E-mail Address	Hidden

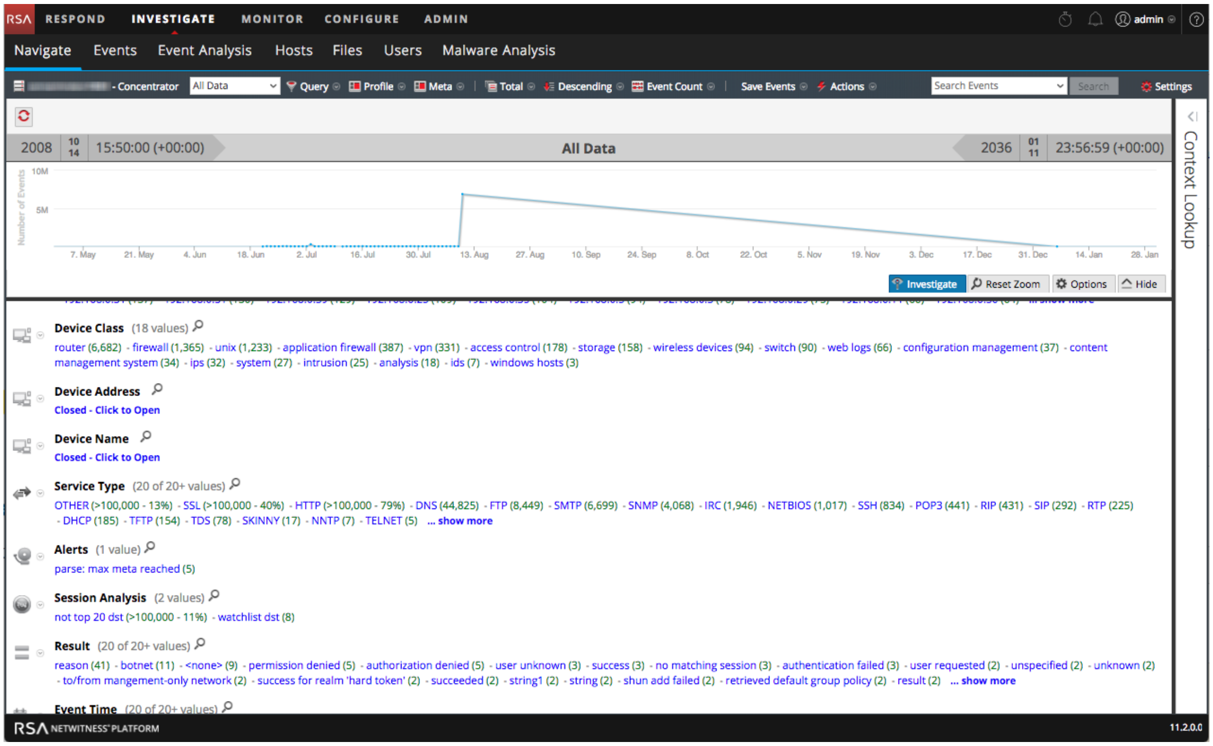
- (Optional) To revert to the default view for meta keys as specified in the service index file, make sure that no keys are selected and in the toolbar, select ⚙ ⌄ > **Auto**.
  When you modify the default view for a non-indexed meta key, you cannot set the key to OPEN. If you change the default view 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.



Device Class (18 values)

router (6,682) - firewall (1,365) - unix (1,233) - application firewall (387) - vpn (331) - access control (178) - storage (158) - wireless devices (94) - switch (90) - web logs (66) - configuration management (37) - content management system (34) - ips (32) - system (27) - intrusion (25) - analysis (18) - ids (7) - windows hosts (3)

Device Address

Closed - Click to Open

Device Name

Closed - Click to Open

Service Type (20 of 20+ values)

OTHER (>100,000 - 13%) - SSL (>100,000 - 40%) - HTTP (>100,000 - 79%) - DNS (44,825) - FTP (8,449) - SMTP (6,699) - SNMP (4,068) - IRC (1,946) - NETBIOS (1,017) - SSH (834) - POP3 (441) - RIP (431) - SIP (292) - RTP (225) - DHCP (185) - TFTP (154) - TDS (78) - SKINNY (17) - NNTP (7) - TELNET (5) ... show more

Alerts (1 value)

parse: max meta reached (5)

Session Analysis (2 values)

not top 20 dst (>100,000 - 11%) - watchlist dst (8)

Result (20 of 20+ values)

reason (41) - botnet (11) - <none> (9) - permission denied (5) - authorization denied (5) - user unknown (3) - success (3) - no matching session (3) - authentication failed (3) - user requested (2) - unspecified (2) - unknown (2) - to/from mangement-only network (2) - success for realm 'hard token' (2) - succeeded (2) - string1 (2) - string (2) - shun add failed (2) - retrieved default group policy (2) - result (2) ... show more

Event Time (20 of 20+ values)

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**.

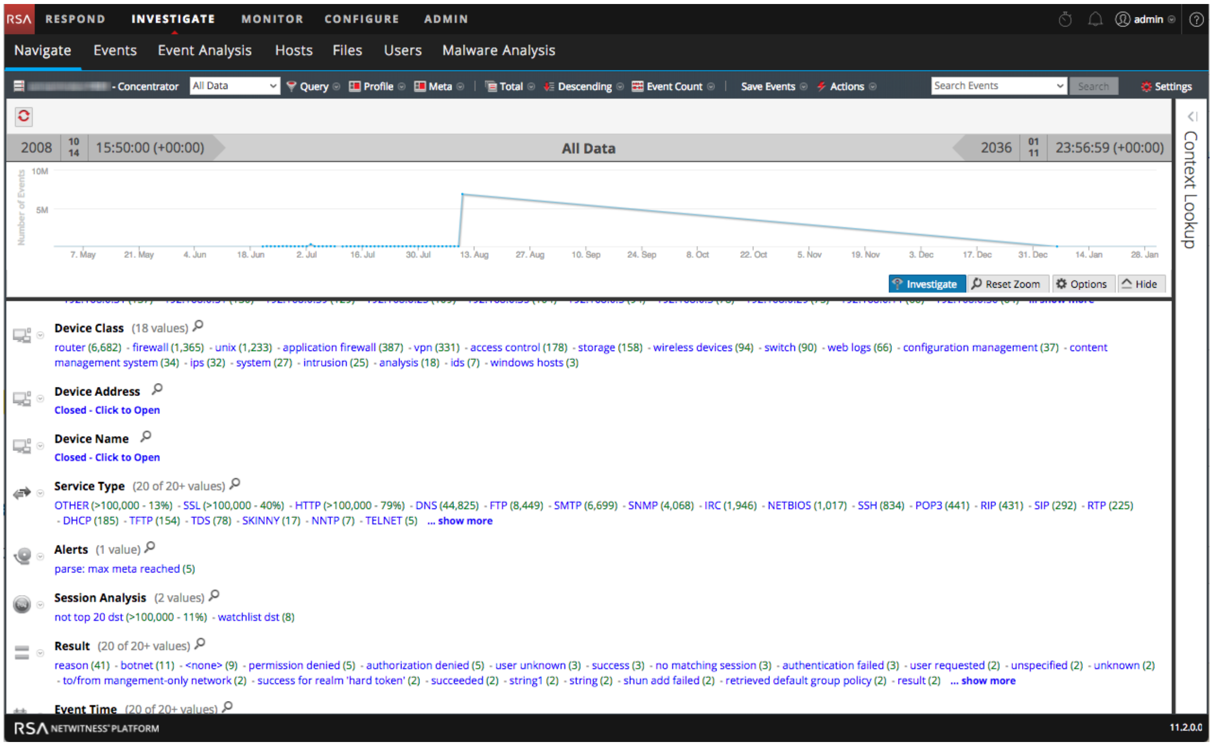
   The URL is updated to reflect the original URL prior to zooming into the data, and the Investigation options panel is updated to reflect the time range selected before zoom. The Time Chart is redrawn for the selected time range and the meta values are loaded for that time range.

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.



Device Class (18 values)
router (6,682) - firewall (1,365) - unix (1,233) - application firewall (387) - vpn (331) - access control (178) - storage (158) - wireless devices (94) - switch (90) - web logs (66) - configuration management (37) - content management system (34) - ips (32) - system (27) - intrusion (25) - analysis (18) - ids (7) - windows hosts (3)

Device Address
Closed - Click to Open

Device Name
Closed - Click to Open

Service Type (20 of 20+ values)
OTHER (>100,000 - 13%) - SSL (>100,000 - 40%) - HTTP (>100,000 - 79%) - DNS (44,825) - FTP (8,449) - SMTP (6,699) - SNMP (4,068) - IRC (1,946) - NETBIOS (1,017) - SSH (834) - POP3 (441) - RIP (431) - SIP (292) - RTP (225) - DHCP (185) - TFTP (154) - TDS (78) - SKINNY (17) - NNTP (7) - TELNET (5) ... show more

Alerts (1 value)
parse: max meta reached (5)

Session Analysis (2 values)
not top 20 dst (>100,000 - 11%) - watchlist dst (8)

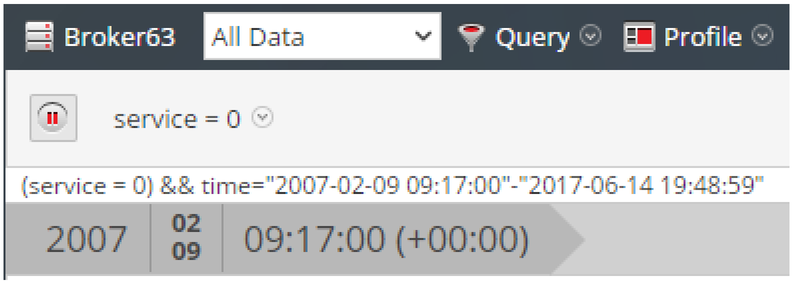
Result (20 of 20+ values)
reason (41) - botnet (11) - <none> (9) - permission denied (5) - authorization denied (5) - user unknown (3) - success (3) - no matching session (3) - authentication failed (3) - user requested (2) - unspecified (2) - unknown (2) - to/from mangement-only network (2) - success for realm 'hard token' (2) - succeeded (2) - string1 (2) - string (2) - shun add failed (2) - retrieved default group policy (2) - result (2) ... show more

Event Time (20 of 20+ values)

2. To drill down into the metadata, do any combination of the following:

   a. Click a **meta key**, for example, **Service Type**.

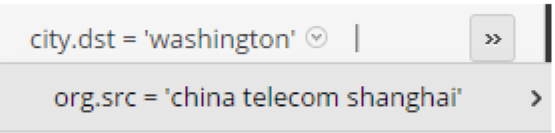
   b. Click a **meta value**, the blue text in the results. For example, **OTHER**.
   Each time you click a meta key or meta value, the investigation query pivots to a narrowed focal point, or drill point, in the data. At each drill point, the Values panel is updated and the new drill point is displayed in the breadcrumb. Below is an example of the first breadcrumb.



service = 0

(service = 0) && time="2007-02-09 09:17:00"-"2017-06-14 19:48:59"

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.



city.dst = 'washington'

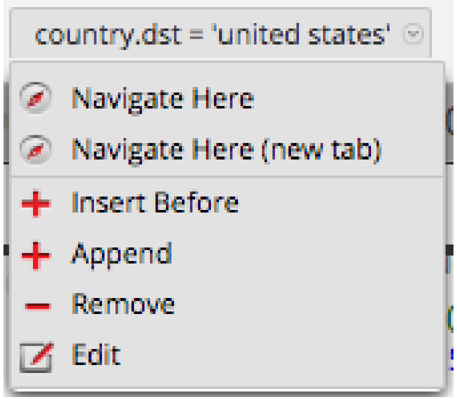
org.src = 'china telecom shanghai'

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.

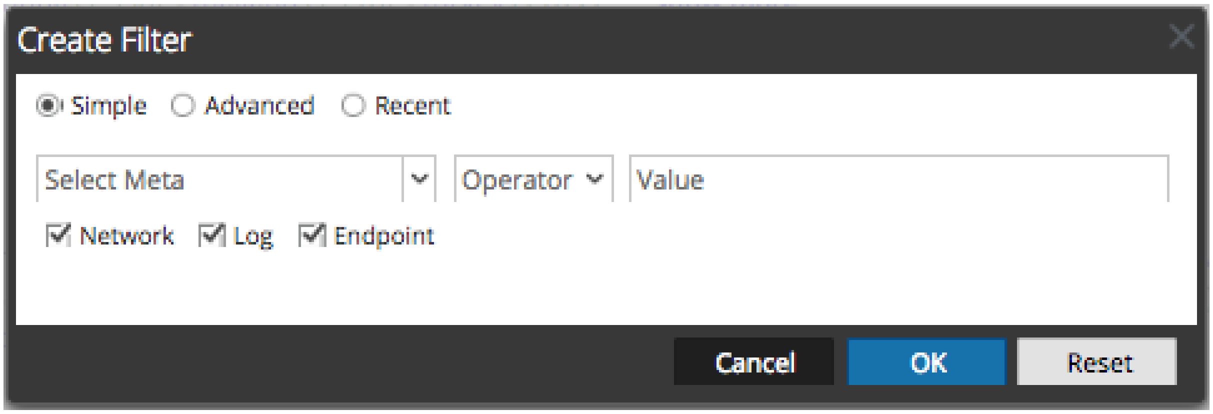
To add a query in the breadcrumb:

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



country.dst = 'united states'

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



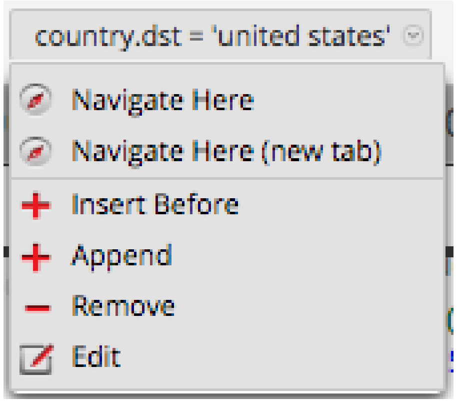
3. Create the Query as described in Create a Query in the Navigate and Legacy Events Views.

To edit a query in the breadcrumb:

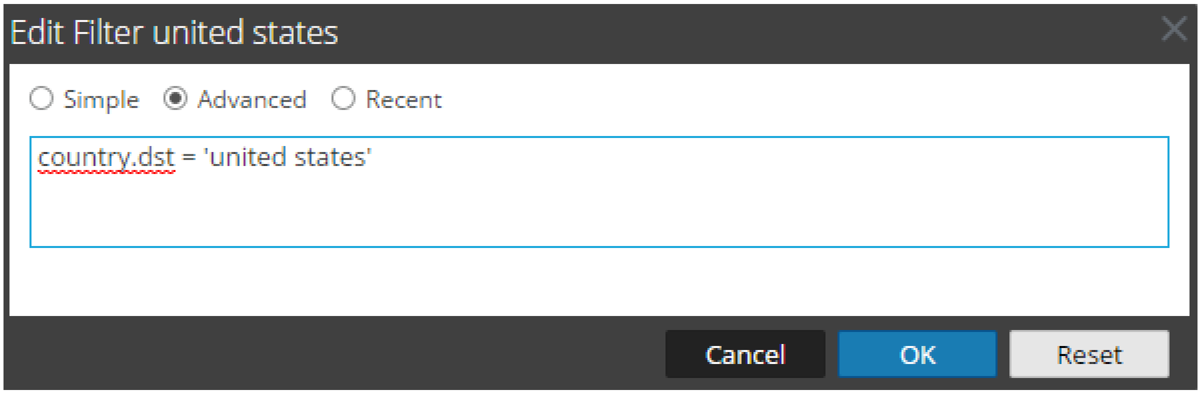
In the breadcrumb, you can click any of the crumbs to display the Query menu. You can delete a crumb and edit a query in a crumb. After each edit in the breadcrumb, NetWitness Platform refreshes the results.

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.

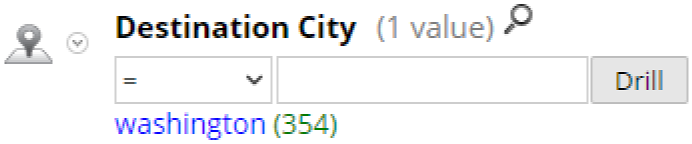


country.dst = 'united states'

3. Edit the fields as described in Create a Query in the Navigate and Legacy Events Views.

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.

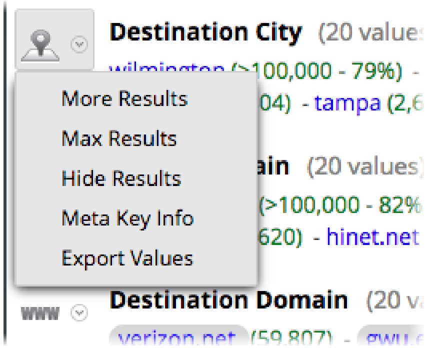


2. (Optional) If you want to close the search form, click the magnifying glass again.
3. Select the operation from the drop-down list on the left and type the text value to search for. Then click **Drill** to perform the execution.
 The metadata for that meta key is used to drill down in the current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

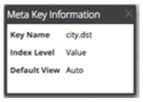
To view meta key information and copy meta values for a meta key:

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.



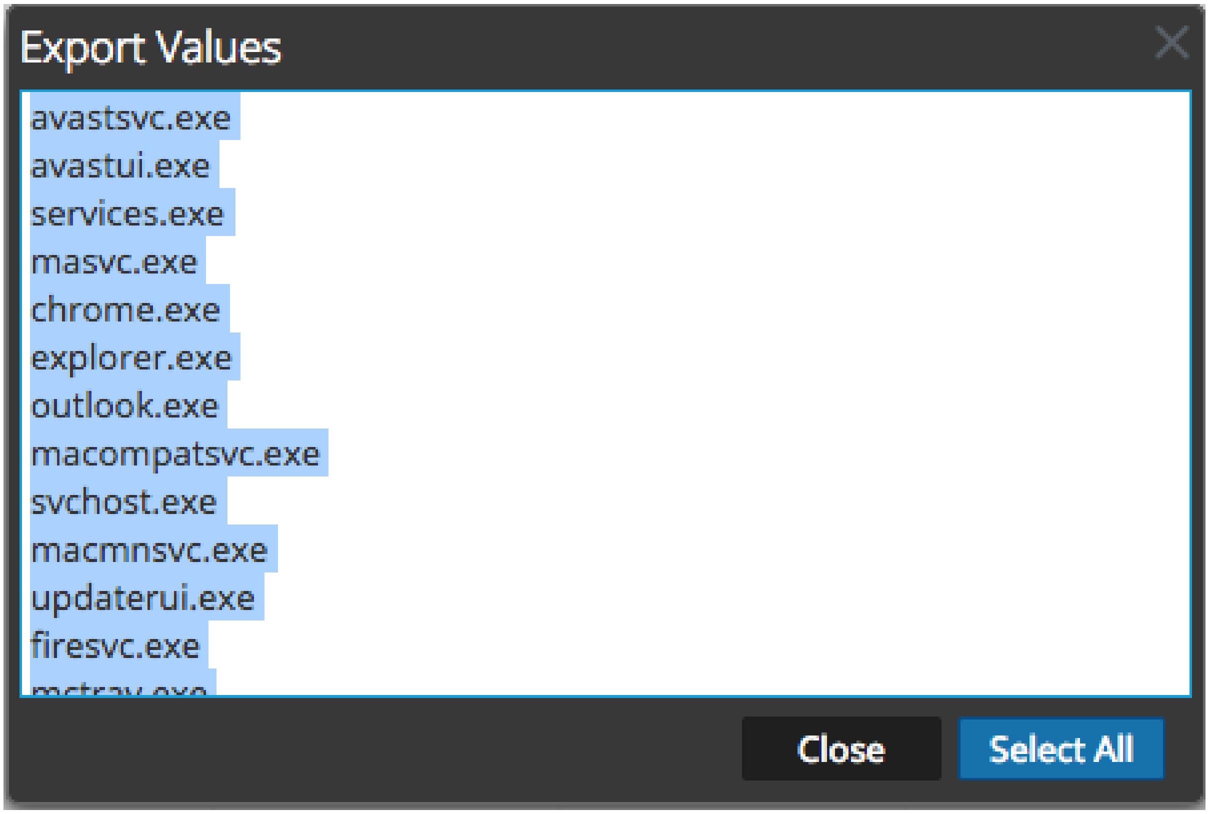
2. Select **Meta Key Info**.
   The Meta Key Info dialog is displayed.



Meta Key Information

Key Name city.dst
Index Level Value
Default View Auto

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.

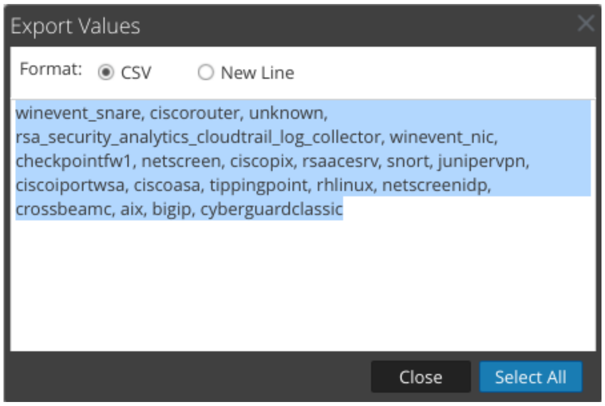


Export Values

```
avastsvc.exe
avastui.exe
services.exe
masvc.exe
chrome.exe
explorer.exe
outlook.exe
macompatsvc.exe
svchost.exe
macmnsvc.exe
updaterui.exe
firesvc.exe
mctray.exe
```

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

CSV.



Format: ● CSV ○ New Line

winevent_snare, ciscorouter, unknown, rsa_security_analytics_cloudtrail_log_collector, winevent_nic, checkpointfw1, netscreen, ciscopix, rsaacesrv, snort, junipervpn, ciscoiportwsa, ciscoasa, tippingpoint, rhlinux, netscreenidp, crossbeamc, aix, bigip, cyberguardclassic

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.

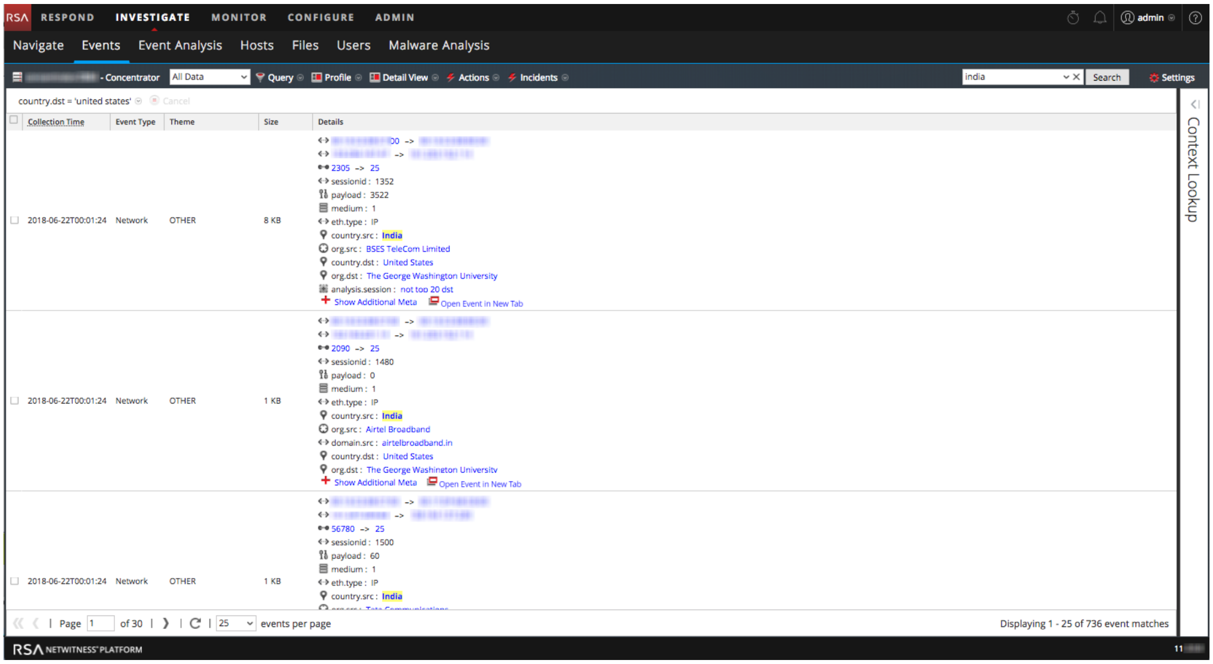
2. Click the count (the number in green) next to a blue meta value.
   The Events view corresponding to the current drill point is displayed.
   The operations that you can perform in the events view are described in Downloading and Acting Upon Results.

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 in the Navigate and Legacy Events Views 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.



country.dst = 'united states'

□	Collection Time	Event Type	Theme	Size	Details
□	2018-06-22T00:01:24	Network	OTHER	8 KB	[redacted] -> [redacted] [redacted] -> [redacted] 2305 -> 25 sessionid : 1352 payload : 3522 medium : 1 eth.type : IP country.src : India org.src : BSES TeleCom Limited country.dst : United States org.dst : The George Washington University analysis.session : not top 20 dst Show Additional Meta Open Event in New Tab
□	2018-06-22T00:01:24	Network	OTHER	1 KB	[redacted] -> [redacted] [redacted] -> [redacted] 2090 -> 25 sessionid : 1480 payload : 0 medium : 1 eth.type : IP country.src : India org.src : Airtel Broadband domain.src : airtelbroadband.in country.dst : United States org.dst : The George Washington University Show Additional Meta Open Event in New Tab
□	2018-06-22T00:01:24	Network	OTHER	1 KB	[redacted] -> [redacted] [redacted] -> [redacted] 56780 -> 25 sessionid : 1500 payload : 60 medium : 1 eth.type : IP country.src : India

Page 1 of 30 | 25 events per page

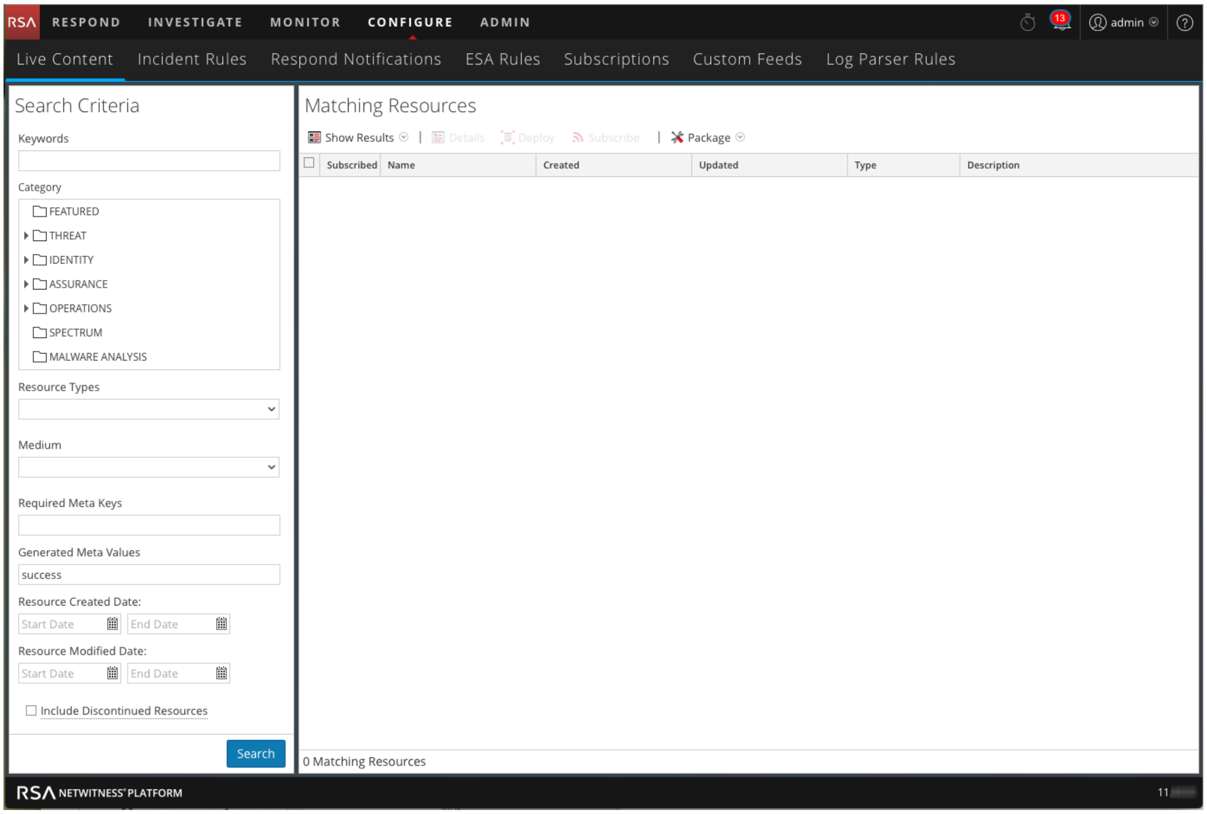
Displaying 1 - 25 of 736 event matches

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**.

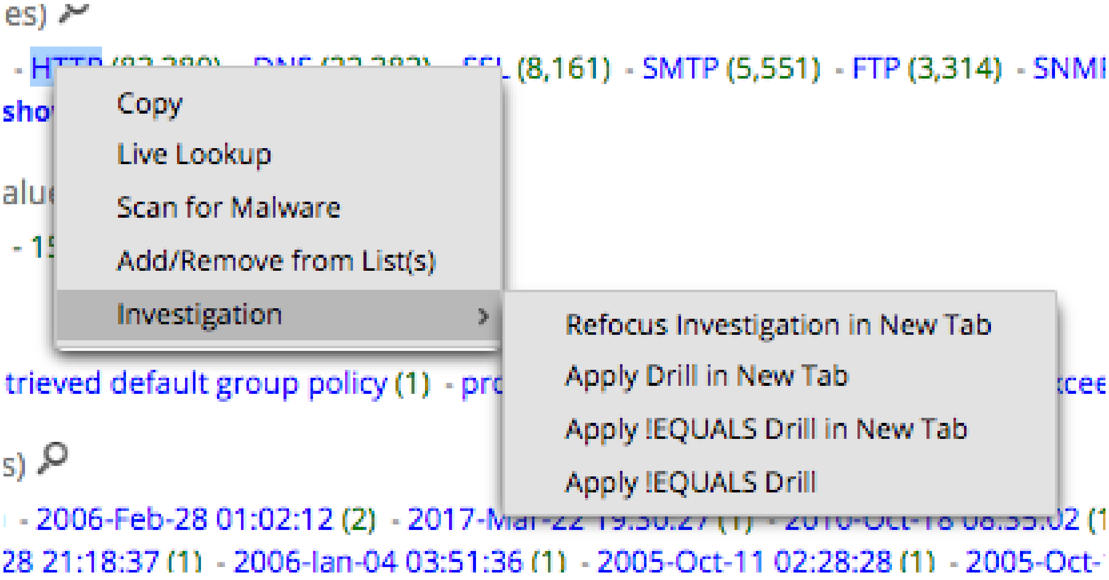
   The Live Search view is displayed with the meta value entered in the Generated Meta Value(s) field, and ready for a search.



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.

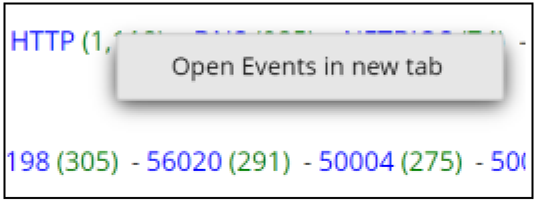

HTTP
SSL (8,161) - SMTP (5,551) - FTP (3,314) - SNMP
Copy
Live Lookup
Scan for Malware
Add/Remove from List(s)
Investigation
Refocus Investigation in New Tab
Apply Drill in New Tab
Apply !EQUALS Drill in New Tab
Apply !EQUALS Drill
trieved default group policy (1) - pro
- 2006-Feb-28 01:02:12 (2) - 2017-Mar-22
28 21:18:37 (1) - 2006-Jan-04 03:51:36 (1) - 2005-Oct-11 02:28:28 (1) - 2005-Oct-

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



Filter Results in the Legacy Events View

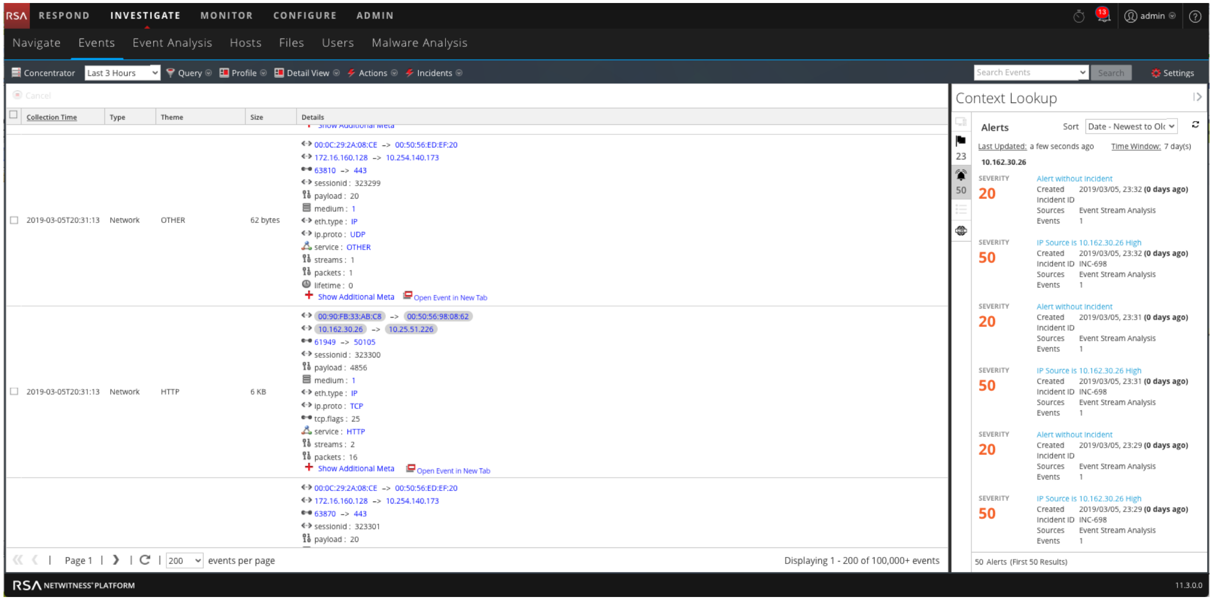
Analysts can filter events in the Legacy Events view by searching for events or selecting the service, setting the time range, and querying the metadata. If you opened the Legacy Events view from a Navigate view drill point, the view opens to the Detail view of events by default. Analysts who do not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

> **Note:** When an Archiver is the currently selected service in the Legacy 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 Legacy Events View

To filter the data displayed in the Legacy Events view:

1. Go to **Investigate** > **Legacy Events**.
   The Legacy Events view is displayed.



	Collection Time	Type	Theme	Size	Details
□	2019-03-05T20:31:13	Network	OTHER	62 bytes	00:0C:29:2A:08:CE -> 00:50:56:ED:EF:20 172.16.160.128 -> 10.254.140.173 63810 -> 443 sessionid : 323299 payload : 20 medium : 1 eth.type : IP ip.proto : UDP service : OTHER streams : 1 packets : 1 lifetime : 0 Show Additional Meta Open Event in New Tab
□	2019-03-05T20:31:13	Network	HTTP	6 KB	00:90:FB:33:AB:C8 -> 00:50:56:98:08:62 10.162.30.26 -> 10.25.51.226 61949 -> 50105 sessionid : 323300 payload : 4856 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 25 service : HTTP streams : 2 packets : 16 Show Additional Meta Open Event in New Tab
					00:0C:29:2A:08:CE -> 00:50:56:ED:EF:20 172.16.160.128 -> 10.254.140.173 63870 -> 443 sessionid : 323301 payload : 20

Page 1 | 200 events per page

Displaying 1 - 200 of 100,000+ events

Alerts Sort Date - Newest to Old

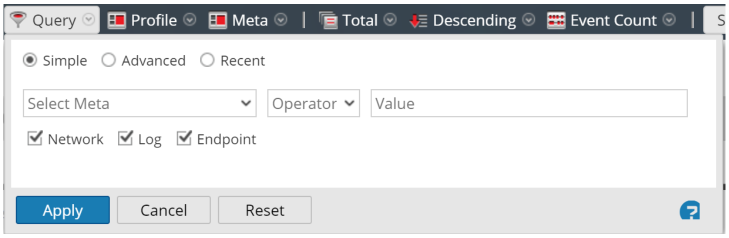
Last Updated: a few seconds ago Time Window: 7 day(s)

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
20	Alert without Incident	
	Created	2019/03/05, 23:31 **(0 days ago)**
	Incident ID	
	Sources	Event Stream Analysis
	Events	1
50	IP Source is 10.162.30.26 High	
	Created	2019/03/05, 23:31 **(0 days ago)**
	Incident ID	INC-698
	Sources	Event Stream Analysis
	Events	1
20	Alert without Incident	
	Created	2019/03/05, 23:29 **(0 days ago)**
	Incident ID	
	Sources	Event Stream Analysis
	Events	1
50	IP Source is 10.162.30.26 High	
	Created	2019/03/05, 23:29 **(0 days ago)**
	Incident ID	INC-698
	Sources	Event Stream Analysis
	Events	1

50 Alerts (First 50 Results)

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 Legacy 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.

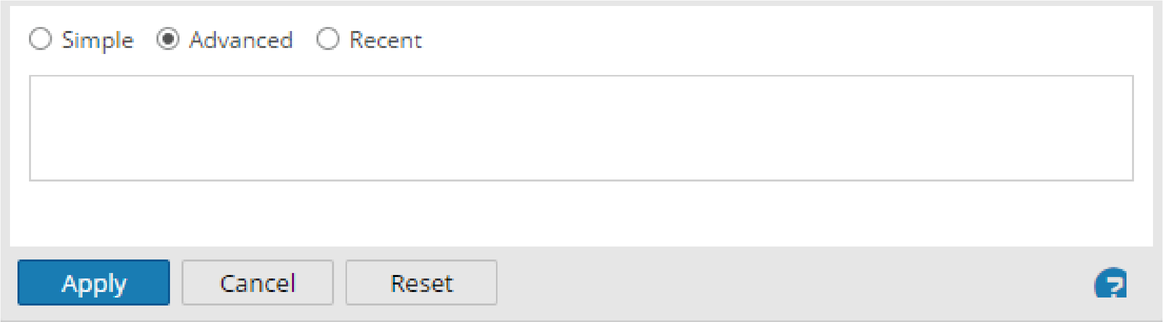
   b. Select an operator from the drop-down list in the **Operator** field.

   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 Legacy Events view.

5. If you want to enter a more complex query based on your knowledge of the meta keys and operators:

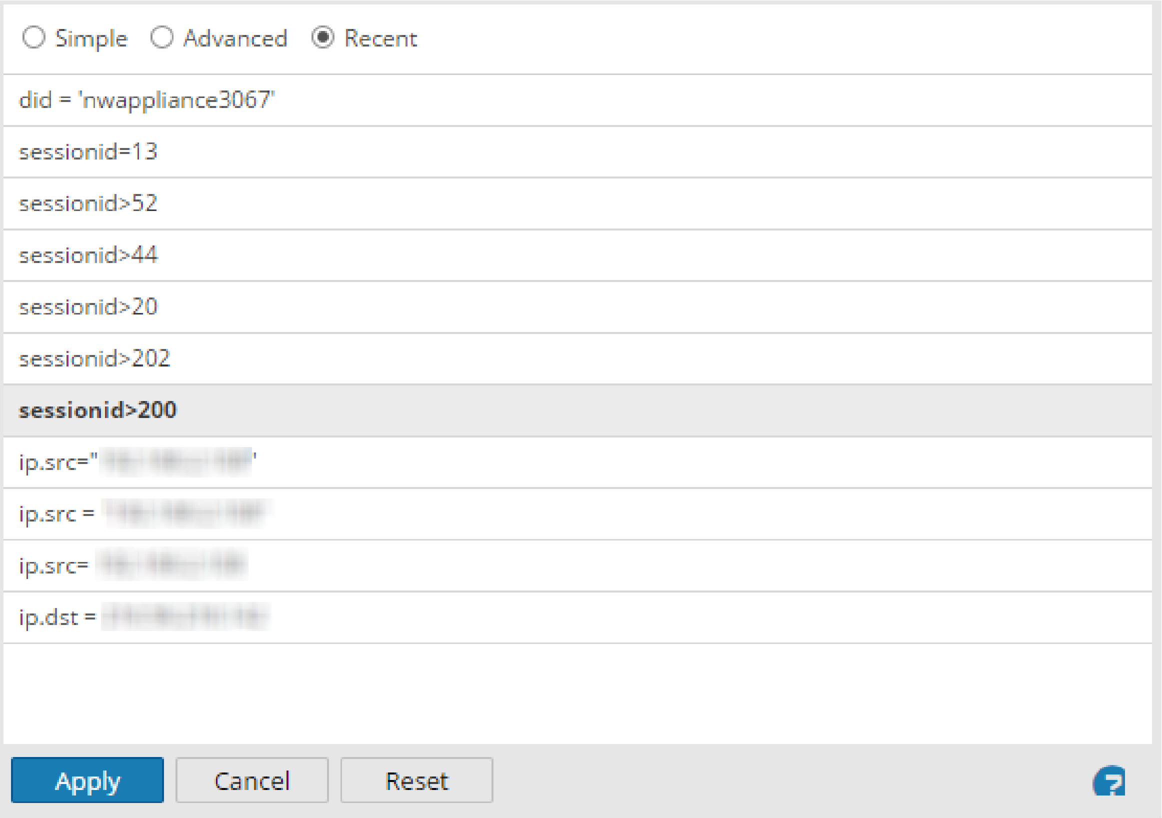
   a. Click **Advanced**.
   The Advanced Query dialog is displayed.



   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.



○ Simple ○ Advanced ● Recent

did = 'nwappliance3067'

sessionid=13

sessionid>52

sessionid>44

sessionid>20

sessionid>202

sessionid>200

ip.src="[redacted]'

ip.src = [redacted]

ip.src= [redacted]

ip.dst = [redacted]

b. Select a query and click **Apply**.
The matching results for the query are displayed in the Detail View in the Legacy 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.

Page Through Events in the Legacy 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 Legacy 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 |.

Create a Query in the Navigate and Legacy Events Views

In the Navigate view or the Legacy 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>]
```

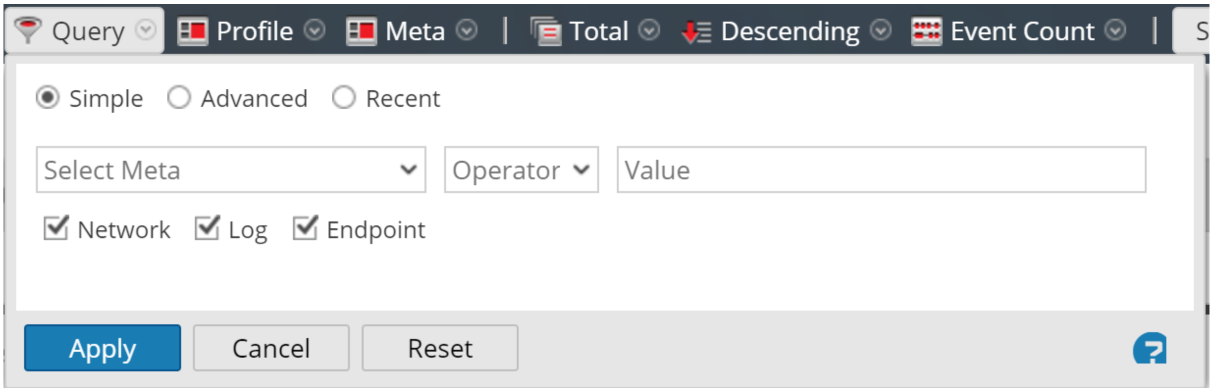
These are a few examples:

```
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 **Legacy Events** view toolbar, select **Query.**
   The Query dialog is displayed, with the Simple option selected.

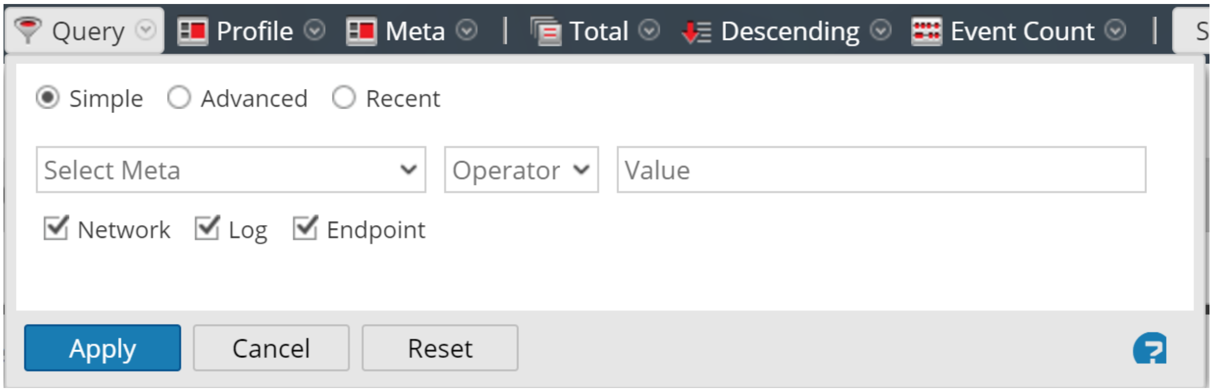


2. In the **Select Meta** field, click to display the drop-down list. The drop-down list has two sections: Meta Groups and All Meta.
3. Select a single meta key under **All Meta** or select a meta group under **Meta Groups**. You can also type in a meta key or meta group in the field.

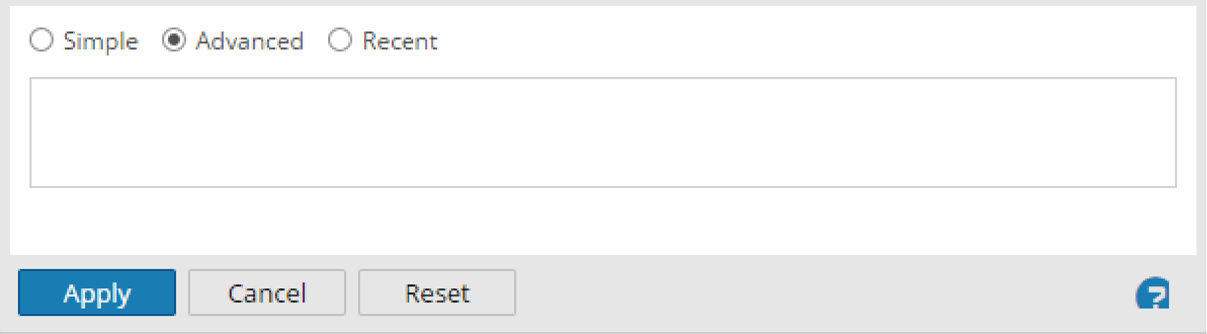
4. In the **Operator** field, type an operator or click on the drop-down list to select a valid operator.
5. (Optional) If you selected an operator that requires a value, for example, =, in the third field type the value for the meta key.
6. In the Network, Log, and Endpoint checkboxes, choose the type 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

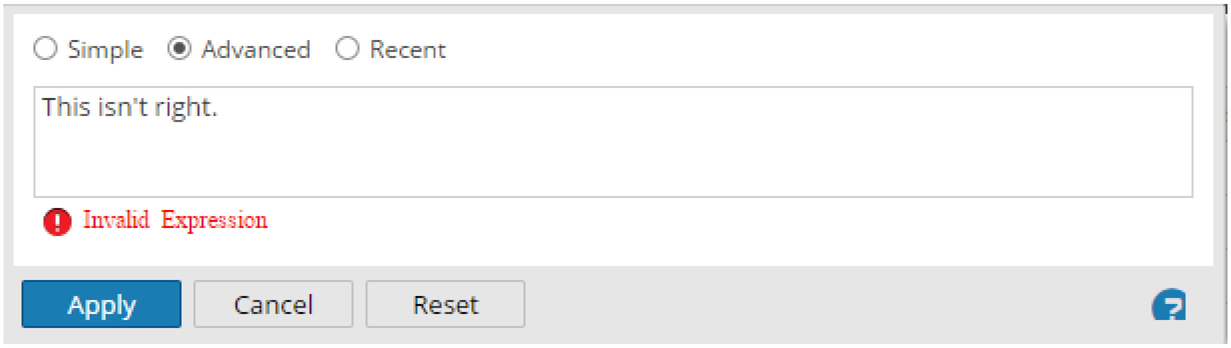
1. In the **Navigate** view or the **Legacy Events** view toolbar, select **Query.**
   The Query dialog is displayed.



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.



This isn't right.

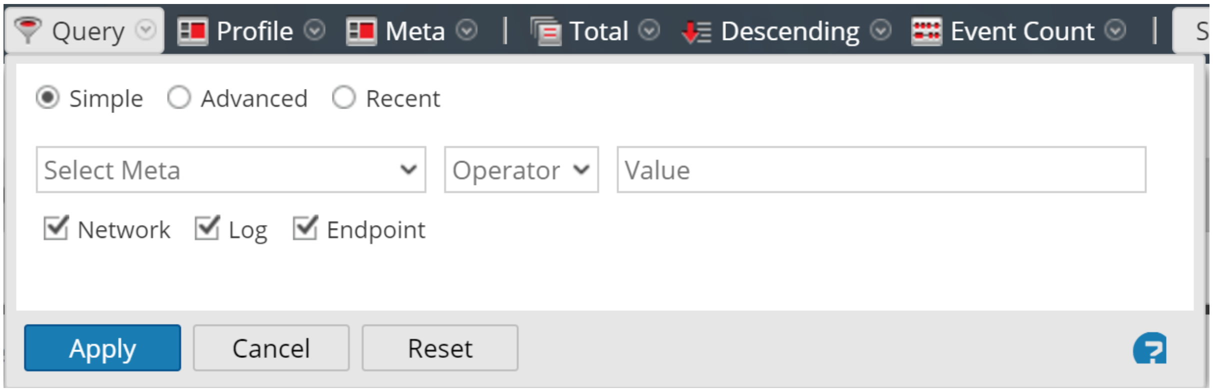
Invalid Expression

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:

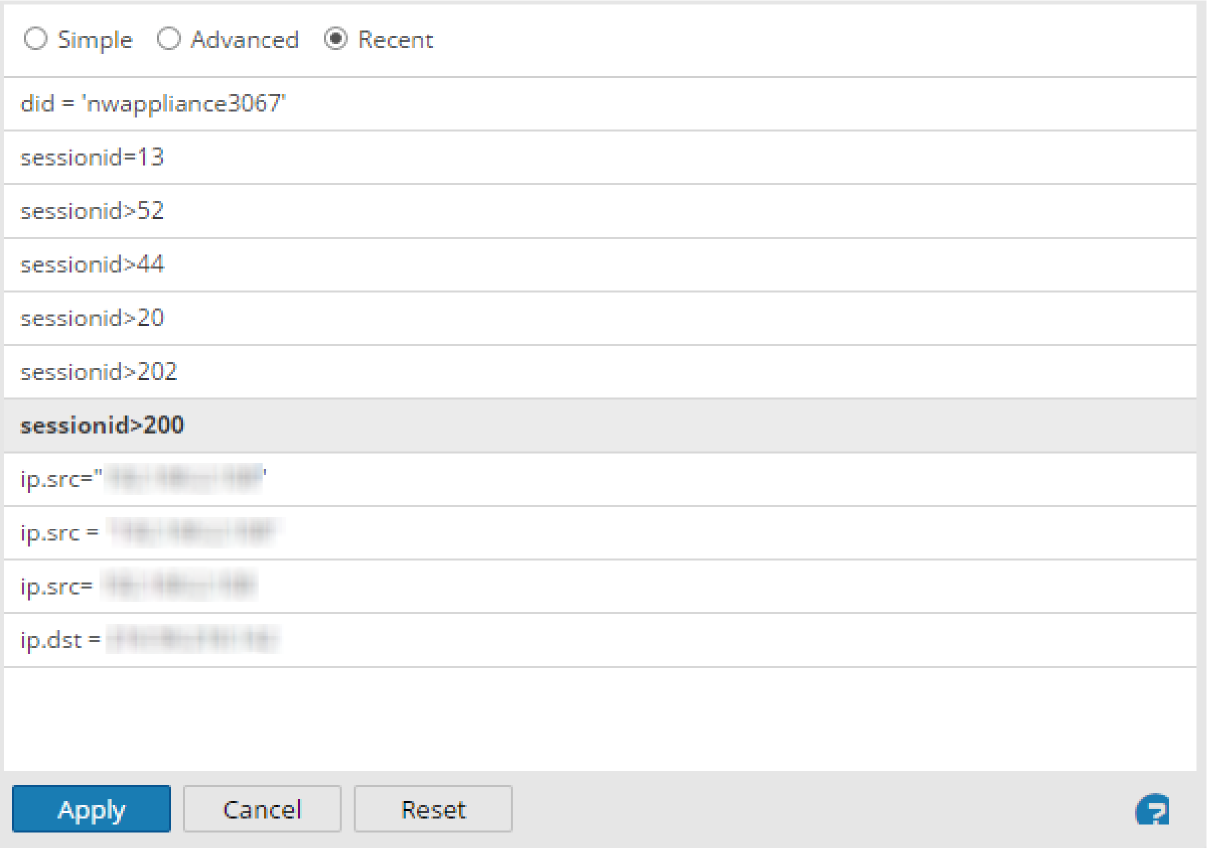
1. In the **Navigate view** or the Events view toolbar, select **Query.**
   The Query dialog is displayed, with the Simple option selected.



● Simple ○ Advanced ○ Recent

☑ Network ☑ Log ☑ Endpoint

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



○ Simple ○ Advanced ● Recent

did = 'nwappliance3067'
sessionid=13
sessionid>52
sessionid>44
sessionid>20
sessionid>202
sessionid>200
ip.src="[redacted]'
ip.src = [redacted]
ip.src= [redacted]
ip.dst = [redacted]

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 in the Navigate and Legacy Events Views

You can search for text patterns within the current set of events in the Navigate view, the Events view, and the Legacy Events view. This section provides information about searching in the Navigate view and the Legacy Events view. For information about searching in the Legacy Events view, see Filter Results in 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 Legacy 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:

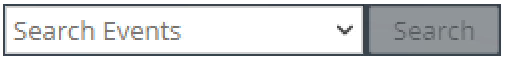
- Each white space delimited word is ANDed, so that every word must be found, but the order or location position in relation to the other words is irrelevant. For example, if you search on `Mark Albert`, both Mark and Albert must be found in the session, but they need not be together or in any specific 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 toast or 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 is 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 metadata, 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

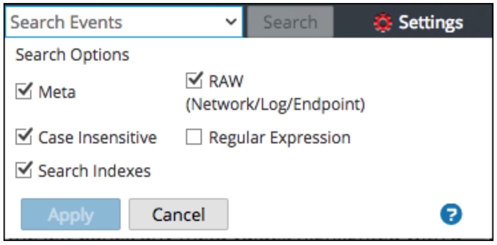
To access the Search box and search options in the Navigate or Legacy Events view:

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 Events** 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.



Search Options

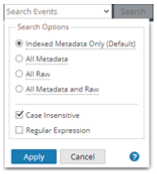
☑ Meta

☑ RAW (Network/Log/Endpoint)

☑ Case Insensitive

□ Regular Expression

☑ Search Indexes



Search Options

● Indexed Metadata Only (Default)

○ All Metadata

○ All Raw

○ All Metadata and Raw

☑ Case Insensitive

□ Regular Expression

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 metadata or raw data.
Apply	Sets the default search options to apply to a search in the Navigate and Legacy 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 Procedures

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 Legacy Events View

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

1. Type a search string in the Search box, and press **Enter** or click **Search**.
   The search results are displayed. 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 Legacy 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 Investigate 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 the 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.

Reconstructing and Analyzing Events

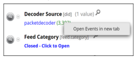
Having refined events in the Navigate view or in the Events list as described in Refining the Results Set, your next step is to learn more about the events by reconstructing them, looking at attachments, and viewing additional context in third-party lookups or internal lookups.

Reconstructions are done in the Events view or the Legacy Events view. If you are starting from the Navigate view, you need to go to the Events view or the Legacy Events view to see a reconstruction.

> **Note:** The Legacy Events view is disabled by default. The administrator can enable to view as described in "Configure Investigation Settings" in the *System Configuration Guide*.

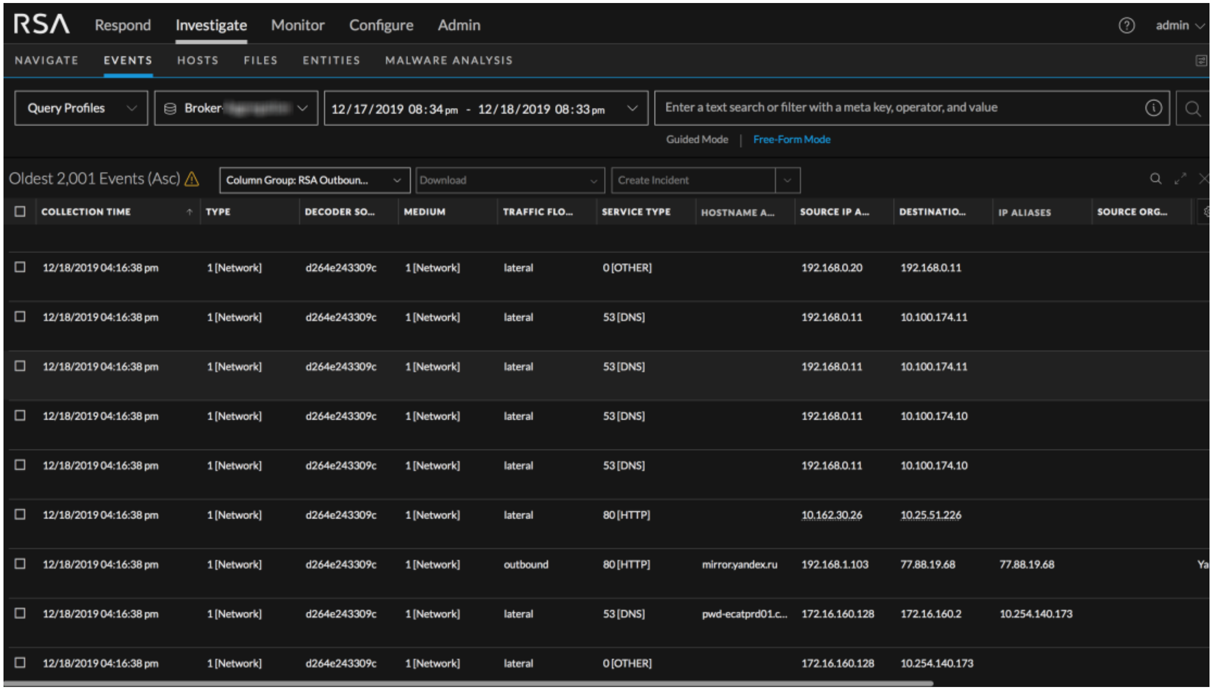
To display events in the Events view, do one of the following:

1. To open the Events view, go to **Investigate** > **Events**.
2. 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 Events in new tab**.

   Decoder Source [did] (1 value)
   packetdecoder (3,3
   Open Events in new tab
   Feed Category [feed.category]
   Closed - Click to Open

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

   Broker [redacted]

   12/17/2019 08:34 pm - 12/18/2019 08:33 pm

   Enter a text search or filter with a meta key, operator, and value

   Oldest 2,001 Events (Asc) ⚠

   Column Group: RSA Outboun...

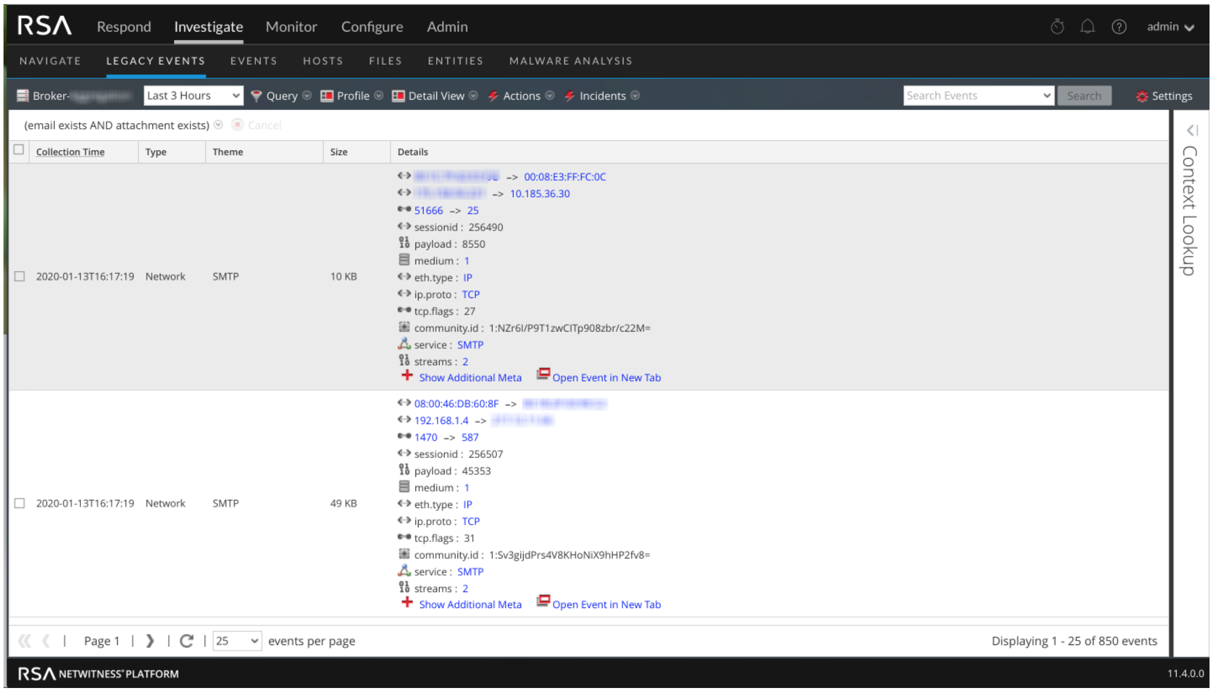
□	COLLECTION TIME ↑	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP A...	DESTINATIO...	IP ALIASES	SOURCE ORG...	
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	0 [OTHER]		192.168.0.20	192.168.0.11			
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.11			
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.11			
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.10			
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]		192.168.0.11	10.100.174.10			
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226			
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	outbound	80 [HTTP]	mirror.yandex.ru	192.168.1.103	77.88.19.68	77.88.19.68		Ya
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	53 [DNS]	pwd-ecatprd01.c...	172.16.160.128	172.16.160.2	10.254.140.173		
□	12/18/2019 04:16:38 pm	1 [Network]	d264e243309c	1 [Network]	lateral	0 [OTHER]		172.16.160.128	10.254.140.173			

For detailed information about the types of analysis that you can use in this view, see Reconstruct an Event in the Events View.

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

1. To open the Legacy Events view using the default query for the default service, go to **Investigate** > **Legacy Events**.

2. To view events for a specific meta value in the Legacy Events view, 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 Legacy Events in new tab**.
   The Legacy Events view displays the events for the selected meta value. The Legacy 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 Legacy Events view. You can extract files, export events, export logs, and open the Event Reconstruction panel by double-clicking an event. See [Downloading and Acting Upon Results](#) for detailed information about these capabilities.
   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.



(email exists AND attachment exists)

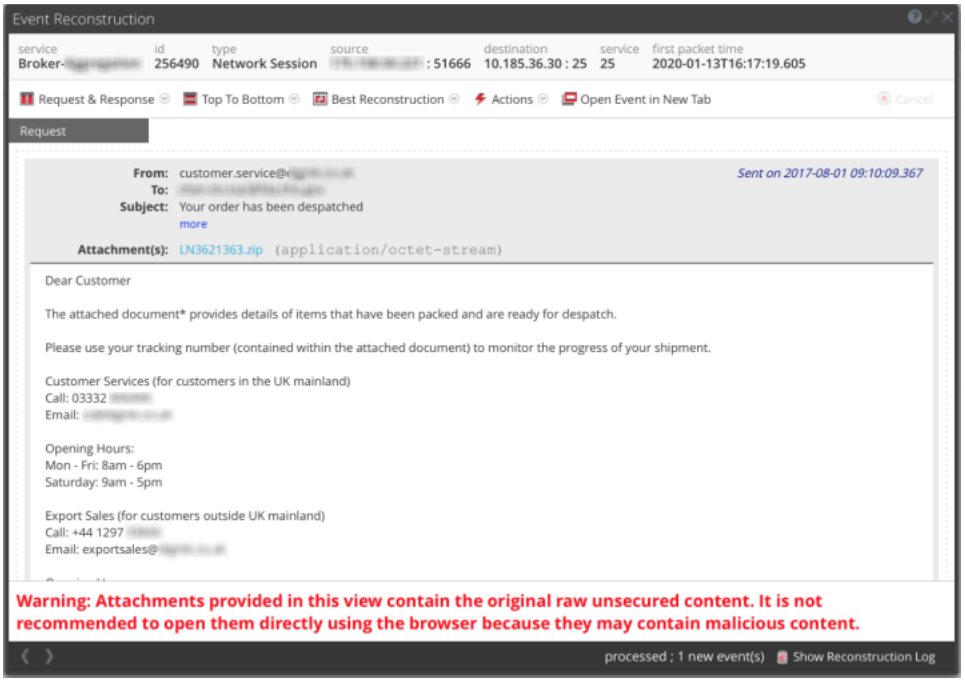
□	Collection Time	Type	Theme	Size	Details
□	2020-01-13T16:17:19	Network	SMTP	10 KB	[redacted] -> 00:08:E3:FF:FC:0C [redacted] -> 10.185.36.30 51666 -> 25 sessionid : 256490 payload : 8550 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 27 community.id : 1:NZr6I/P9T1zwCITp908zbr/c22M= service : SMTP streams : 2 ✚ Show Additional Meta Open Event in New Tab
□	2020-01-13T16:17:19	Network	SMTP	49 KB	08:00:46:DB:60:8F -> [redacted] 192.168.1.4 -> [redacted] 1470 -> 587 sessionid : 256507 payload : 45353 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 31 community.id : 1:Sv3gijdPrs4V8KHoNiX9hHP2fv8= service : SMTP streams : 2 ✚ Show Additional Meta Open Event in New Tab

Page 1 | 25 events per page

Displaying 1 - 25 of 850 events

RSA NETWITNESS® PLATFORM 11.4.0.0

To view a reconstruction of the first event in the list, double-click the event.
The reconstruction opens in a pop-up window in front of the Events list.



service	id	type	source	destination	service	first packet time
Broker-[redacted]	256490	Network Session	[redacted] : 51666	10.185.36.30 : 25	25	2020-01-13T16:17:19.605

From: customer.service@[redacted]

To: [redacted]

Subject: Your order has been despatched

more

Sent on 2017-08-01 09:10:09.367

Attachment(s): LN3621363.zip `(application/octet-stream)`

Dear Customer

The attached document* provides details of items that have been packed and are ready for despatch.

Please use your tracking number (contained within the attached document) to monitor the progress of your shipment.

Customer Services (for customers in the UK mainland)
Call: 03332 [redacted]
Email: [redacted]

Opening Hours:
Mon - Fri: 8am - 6pm
Saturday: 9am - 5pm

Export Sales (for customers outside UK mainland)
Call: +44 1297 [redacted]
Email: exportsales@[redacted]

Warning: Attachments provided in this view contain the original raw unsecured content. It is not recommended to open them directly using the browser because they may contain malicious content.

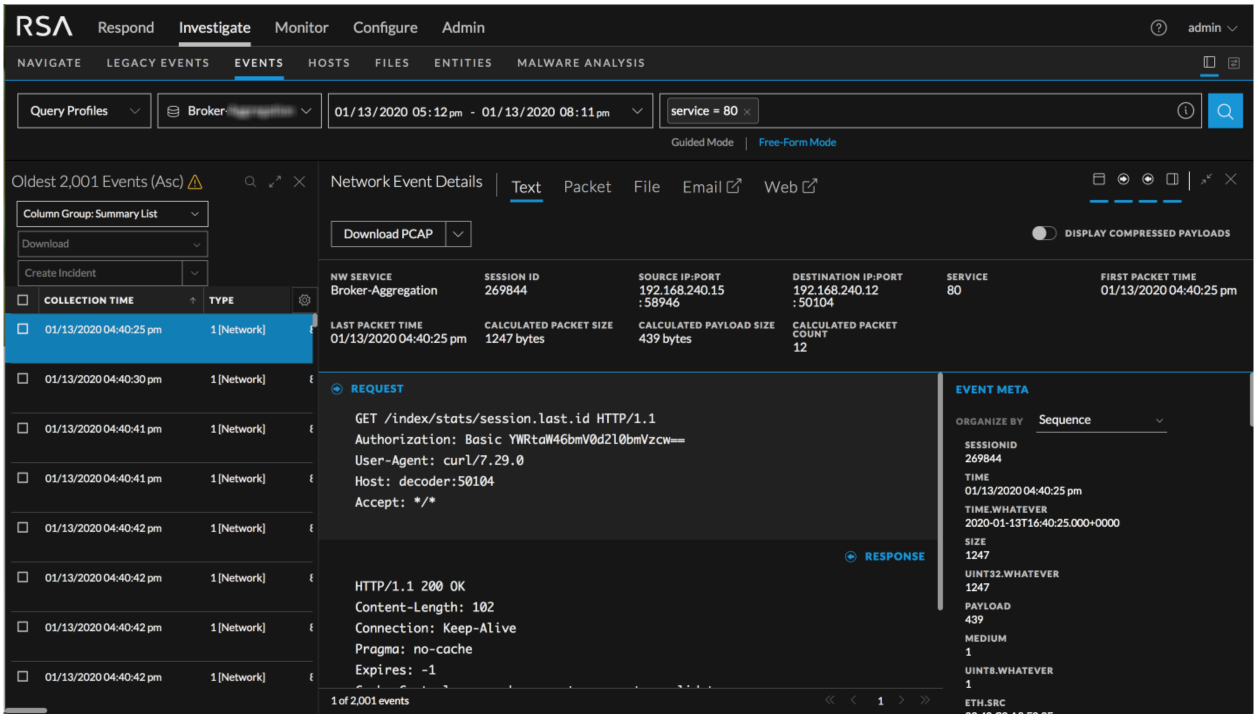
processed ; 1 new event(s)

Reconstruct an Event in the Events View

When hunting for possible threats in captured network, log, and endpoint 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.

In the Events view, you can select the format for the reconstruction: packet, file, text, email, and web. For a log event or endpoint event , only the text reconstruction is available. The default reconstruction for network events is text; 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 Legacy Events view and are described in Reconstruct an Event in the Legacy Events View.

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



Broker-[redacted]

01/13/2020 05:12 pm - 01/13/2020 08:11 pm

service = 80

Oldest 2,001 Events (Asc) ⚠

☐	COLLECTION TIME	TYPE
☐	01/13/2020 04:40:25 pm	1 [Network]
☐	01/13/2020 04:40:30 pm	1 [Network]
☐	01/13/2020 04:40:41 pm	1 [Network]
☐	01/13/2020 04:40:41 pm	1 [Network]
☐	01/13/2020 04:40:42 pm	1 [Network]
☐	01/13/2020 04:40:42 pm	1 [Network]
☐	01/13/2020 04:40:42 pm	1 [Network]
☐	01/13/2020 04:40:42 pm	1 [Network]

Network Event Details

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Broker-Aggregation	269844	192.168.240.15 :58946	192.168.240.12 :50104	80	01/13/2020 04:40:25 pm

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
01/13/2020 04:40:25 pm	1247 bytes	439 bytes	12

REQUEST

```
GET /index/stats/session.last.id HTTP/1.1
Authorization: Basic YWRtaW46bmV0d2l0bmVzcw==
User-Agent: curl/7.29.0
Host: decoder:50104
Accept: */*
```

RESPONSE

```
HTTP/1.1 200 OK
Content-Length: 102
Connection: Keep-Alive
Pragma: no-cache
Expires: -1
```

1 of 2,001 events

EVENT META

ORGANIZE BY Sequence

SESSIONID	269844
TIME	01/13/2020 04:40:25 pm
TIME.WHATEVER	2020-01-13T16:40:25.000+0000
SIZE	1247
UINT32.WHATEVER	1247
PAYLOAD	439
MEDIUM	1
UINT8.WHATEVER	1
ETH.SRC	

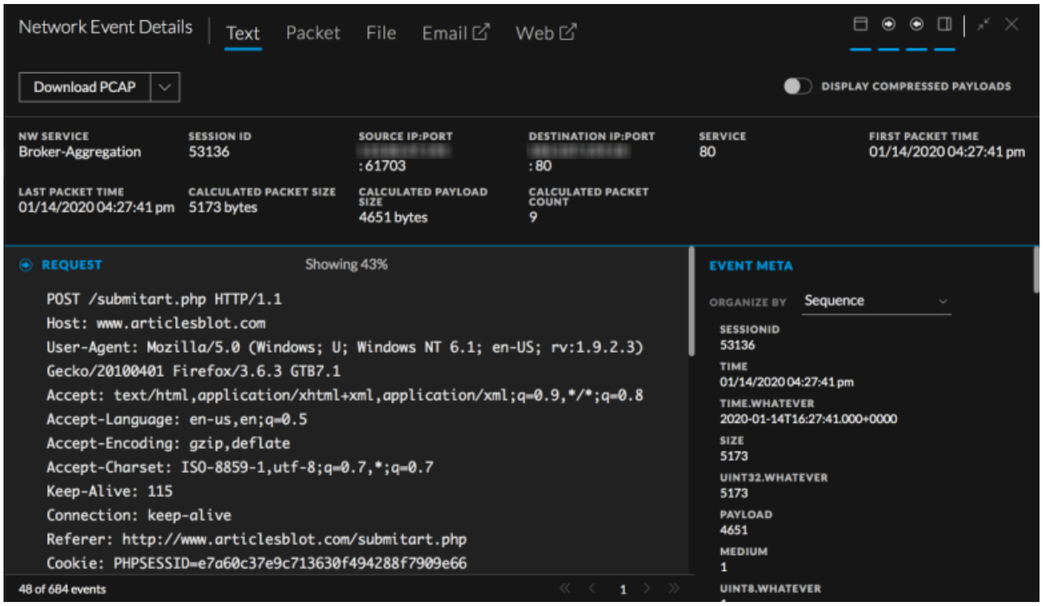
Within each type of analysis, settings are available to enhance your analysis. If you change a setting, the setting is preserved between browser refreshes and logins within the same browser. These are the preserved settings:

- The currently selected reconstruction: Text, Packet, File, or Email.
- 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 without the headers in the Packet panel.
- Whether shaded bytes are displayed in the Packet panel.

- Whether other common file types are highlighted in the Packet panel.
- The number of packets per page in the Packet panel.
- Whether compressed or uncompressed text is displayed in the Text panel.

The Text Panel

You can view all types of events (network events, log events, and endpoint events) in their original text format in the Text panel. The Text 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).



NW SERVICE: Broker-Aggregation
SESSION ID: 53136
SOURCE IP:PORT: [redacted] :61703
DESTINATION IP:PORT: [redacted] :80
SERVICE: 80
FIRST PACKET TIME: 01/14/2020 04:27:41 pm
LAST PACKET TIME: 01/14/2020 04:27:41 pm
CALCULATED PACKET SIZE: 5173 bytes
CALCULATED PAYLOAD SIZE: 4651 bytes
CALCULATED PACKET COUNT: 9

REQUEST — Showing 43%

```
POST /submitart.php HTTP/1.1
Host: www.articlesblot.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3 GTB7.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.articlesblot.com/submitart.php
Cookie: PHPSESSID=e7a60c37e9c713630f494288f7909e66
```

48 of 684 events — 1

EVENT META — ORGANIZE BY: Sequence

SESSIONID: 53136
TIME: 01/14/2020 04:27:41 pm
TIME.WHATEVER: 2020-01-14T16:27:41.000+0000
SIZE: 5173
UINT32.WHATEVER: 5173
PAYLOAD: 4651
MEDIUM: 1
UINT8.WHATEVER

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.

Note: For Version 11.1, 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.

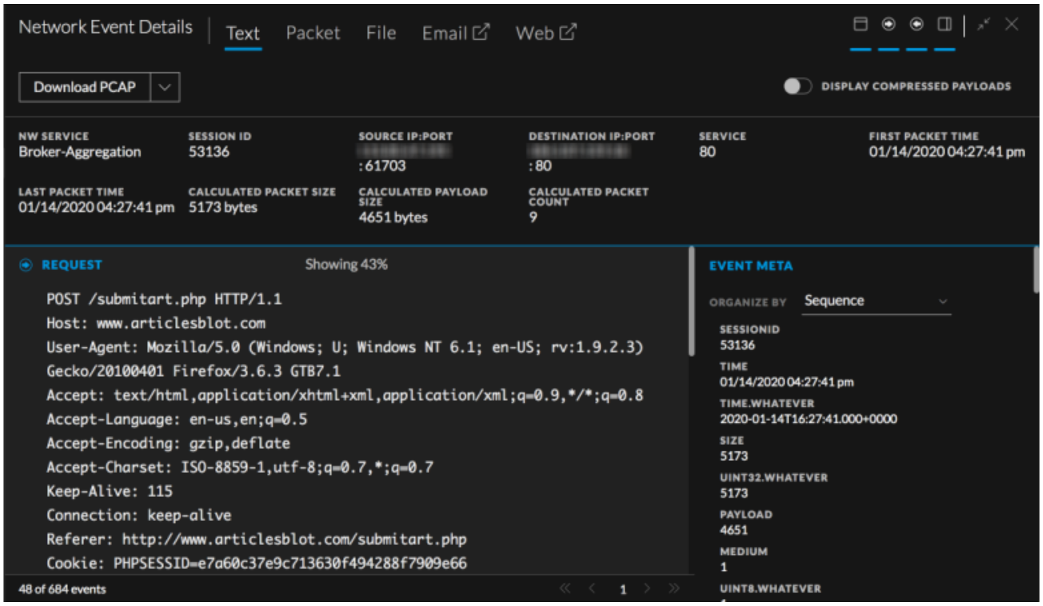
In the Text panel, network events, log events, and endpoint events are presented differently.

- 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 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 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 panel for each type of event, a network event, a log event, and an endpoint event.



NW SERVICE
Broker-Aggregation

SESSION ID
53136

SOURCE IP:PORT
[redacted] :61703

DESTINATION IP:PORT
[redacted] :80

SERVICE
80

FIRST PACKET TIME
01/14/2020 04:27:41 pm

LAST PACKET TIME
01/14/2020 04:27:41 pm

CALCULATED PACKET SIZE
5173 bytes

CALCULATED PAYLOAD SIZE
4651 bytes

CALCULATED PACKET COUNT
9

REQUEST Showing 43%

```
POST /submitart.php HTTP/1.1
Host: www.articlesblot.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3 GTB7.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.articlesblot.com/submitart.php
Cookie: PHPSESSID=e7a60c37e9c713630f494288f7909e66
```

48 of 684 events 1

EVENT META

ORGANIZE BY Sequence

SESSIONID
53136

TIME
01/14/2020 04:27:41 pm

TIME.WHATEVER
2020-01-14T16:27:41.000+0000

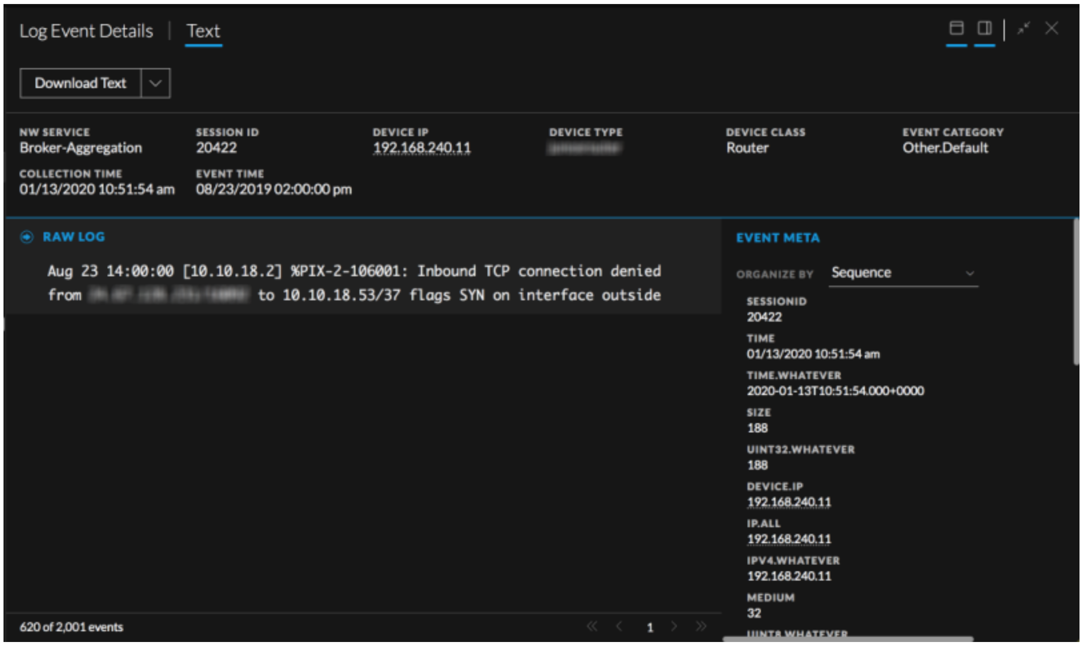
SIZE
5173

UINT32.WHATEVER
5173

PAYLOAD
4651

MEDIUM
1

UINT8.WHATEVER



NW SERVICE
Broker-Aggregation

SESSION ID
20422

DEVICE IP
192.168.240.11

DEVICE TYPE
[redacted]

DEVICE CLASS
Router

EVENT CATEGORY
Other.Default

COLLECTION TIME
01/13/2020 10:51:54 am

EVENT TIME
08/23/2019 02:00:00 pm

RAW LOG

```
Aug 23 14:00:00 [10.10.18.2] %PIX-2-106001: Inbound TCP connection denied
from [redacted] to 10.10.18.53/37 flags SYN on interface outside
```

620 of 2,001 events 1

EVENT META

ORGANIZE BY Sequence

SESSIONID
20422

TIME
01/13/2020 10:51:54 am

TIME.WHATEVER
2020-01-13T10:51:54.000+0000

SIZE
188

UINT32.WHATEVER
188

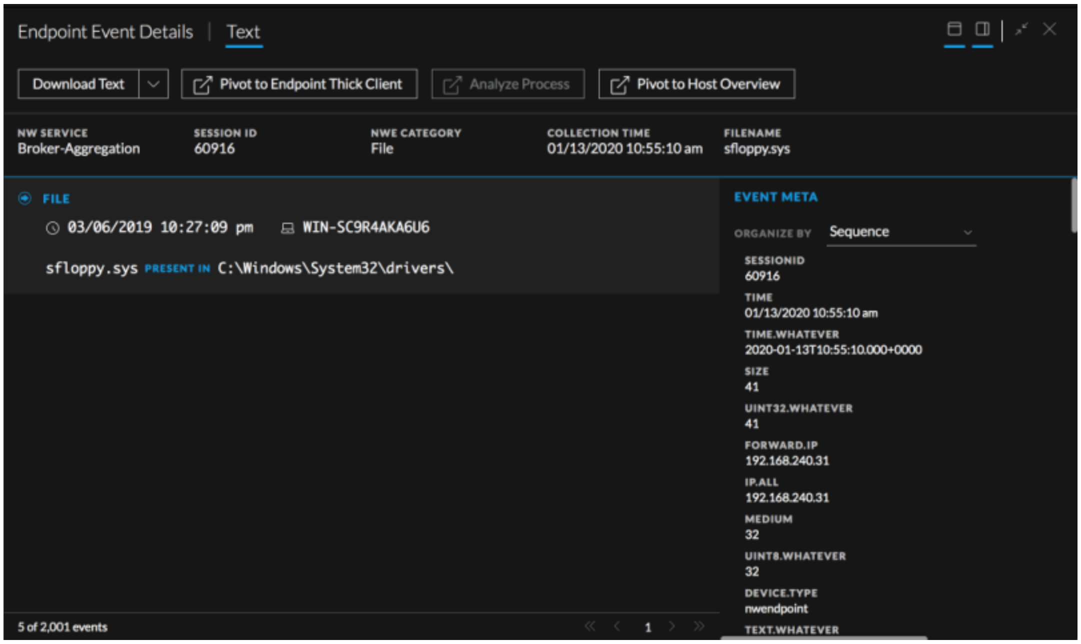
DEVICE.IP
192.168.240.11

IP.ALL
192.168.240.11

IPV4.WHATEVER
192.168.240.11

MEDIUM
32

UINT8.WHATEVER



NW SERVICE Broker-Aggregation
SESSION ID 60916
NWE CATEGORY File
COLLECTION TIME 01/13/2020 10:55:10 am
FILENAME sfloppy.sys

FILE
03/06/2019 10:27:09 pm WIN-SC9R4AKA6U6
sfloppy.sys PRESENT IN C:\Windows\System32\drivers\

EVENT META
ORGANIZE BY Sequence

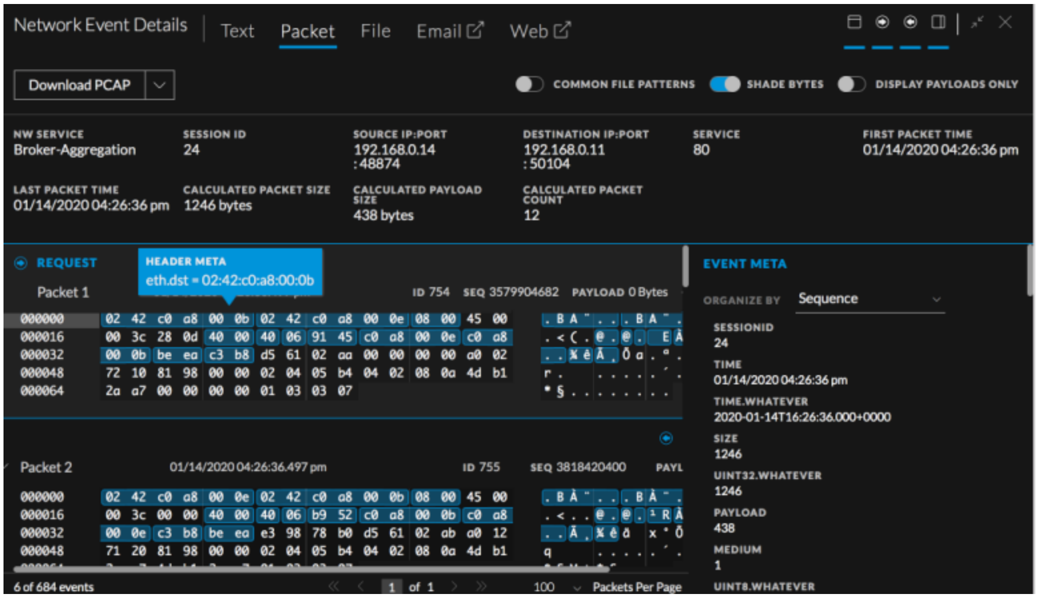
SESSIONID
60916
TIME
01/13/2020 10:55:10 am
TIME.WHATEVER
2020-01-13T10:55:10.000+0000
SIZE
41
UINT32.WHATEVER
41
FORWARD.IP
192.168.240.31
IP.ALL
192.168.240.31
MEDIUM
32
UINT8.WHATEVER
32
DEVICE.TYPE
nwendpoint
TEXT.WHATEVER

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 Panel

The Packet 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 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 PATTERNS ○ SHADE BYTES ● DISPLAY PAYLOADS ONLY ○

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Broker-Aggregation	24	192.168.0.14 :48874	192.168.0.11 :50104	80	01/14/2020 04:26:36 pm

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
01/14/2020 04:26:36 pm	1246 bytes	438 bytes	12

REQUEST

HEADER META
eth.dst = 02:42:c0:a8:00:0b

Packet 1 ID 754 SEQ 3579904682 PAYLOAD 0 Bytes

```
000000  02 42 c0 a8 00 0b 02 42 c0 a8 00 0e 08 00 45 00   . B A ˜ . . . B A ˜ .
000016  00 3c 28 0d 40 00 40 06 91 45 c0 a8 00 0e c0 a8   . < ( . @ . @ .   E Å
000032  00 0b be ea c3 b8 d5 61 02 aa 00 00 00 00 a0 02   . . ¥ ê Ã ¸ Õ a . ª .
000048  72 10 81 98 00 00 02 04 05 b4 04 02 08 0a 4d b1   r .     . . . . . ´ .
000064  2a a7 00 00 00 00 01 03 03 07                     * § . . . . . . . .
```

Packet 2 01/14/2020 04:26:36.497 pm ID 755 SEQ 3818420400 PAYL

```
000000  02 42 c0 a8 00 0e 02 42 c0 a8 00 0b 08 00 45 00   . B À ˜ . . . B À ˜ .
000016  00 3c 00 00 40 00 40 06 b9 52 c0 a8 00 0b c0 a8   . < . . @ . @ . ¹ R À
000032  00 0e c3 b8 be ea e3 98 78 b0 d5 61 02 ab a0 12   . . Ã ¸ ¥ ê ã   x ° Õ
000048  71 20 81 98 00 00 02 04 05 b4 04 02 08 0a 4d b1   q     . . . . . ´ .
```

6 of 684 events « ‹ 1 of 1 › » 100 Packets Per Page

EVENT META

ORGANIZE BY Sequence

SESSIONID
24

TIME
01/14/2020 04:26:36 pm

TIME.WHATEVER
2020-01-14T16:26:36.000+0000

SIZE
1246

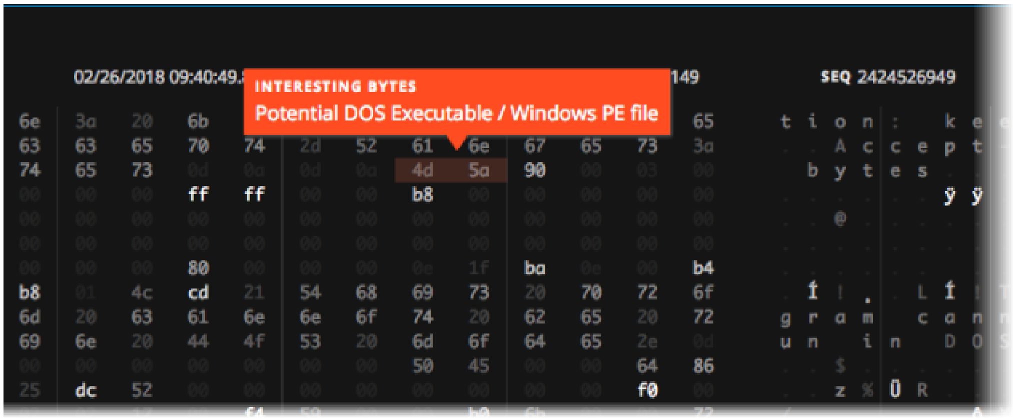
UINT32.WHATEVER
1246

PAYLOAD
438

MEDIUM
1

UINT8.WHATEVER

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.



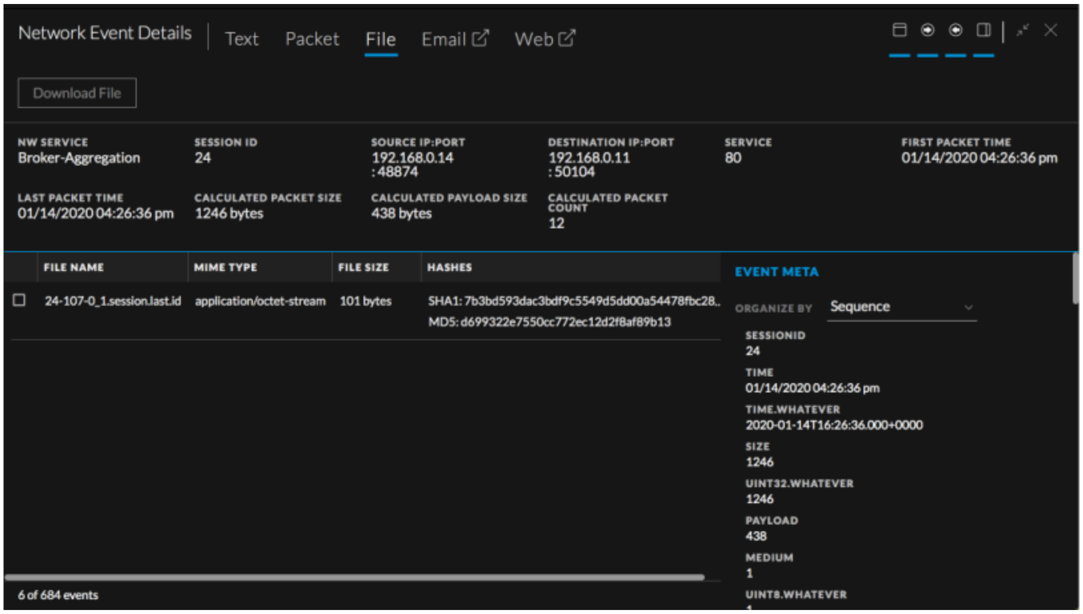
02/26/2018 09:40:49. 149 SEQ 2424526949

INTERESTING BYTES
Potential DOS Executable / Windows PE file

```
6e 3a 20 6b                               65   t i o n :     k e e
63 63 65 70 74 2d 52 61 6e 67 65 73 3a         A c c e p t -
74 65 73 0d 0a 0d 0a 4d 5a 90 00 03 00       b y t e s
00 00 00 ff ff 00 00 b8 00 00 00 00 00                   ÿ ÿ
00 00 00 00 00 00 00 00 00 00 00 00 00           @
00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 80 00 00 00 0e 1f ba 00 00 b4
b8 01 4c cd 21 54 68 69 73 20 70 72 6f       Í !     L Í !
6d 20 63 61 6e 6e 6f 74 20 62 65 20 72     g r a m       c a n
69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d     u n     i n     D O S
00 00 00 00 00 00 00 50 45 00 00 64 86           $
25 dc 52 00 00 00 00 00 00 00 00 f0 00           z % Û R
```

The File Panel

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



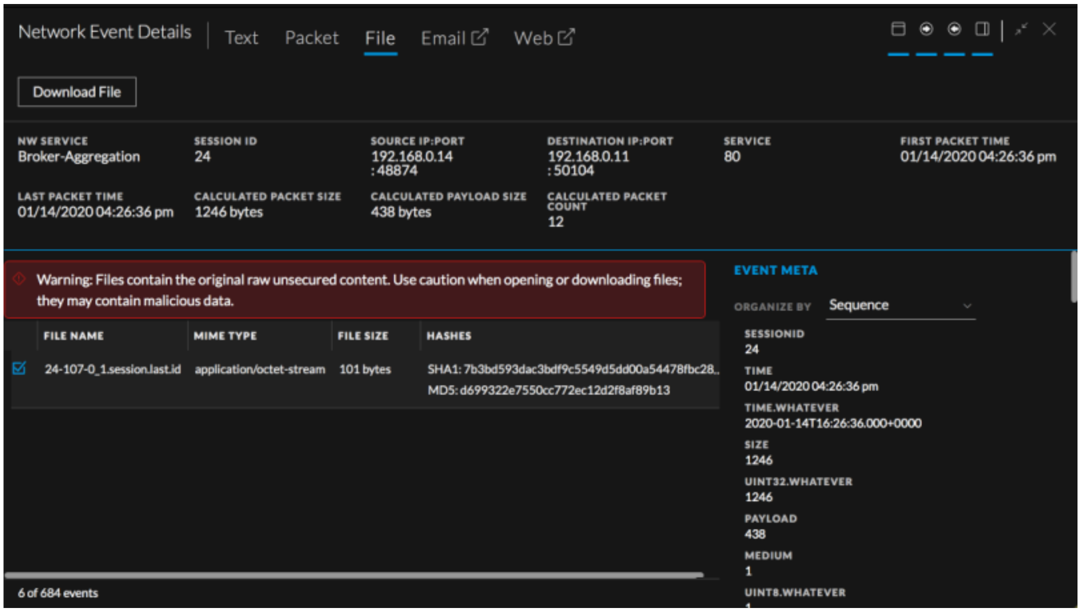
NW SERVICE: Broker-Aggregation
SESSION ID: 24
SOURCE IP:PORT: 192.168.0.14 :48874
DESTINATION IP:PORT: 192.168.0.11 :50104
SERVICE: 80
FIRST PACKET TIME: 01/14/2020 04:26:36 pm
LAST PACKET TIME: 01/14/2020 04:26:36 pm
CALCULATED PACKET SIZE: 1246 bytes
CALCULATED PAYLOAD SIZE: 438 bytes
CALCULATED PACKET COUNT: 12

	FILE NAME	MIME TYPE	FILE SIZE	HASHES
□	24-107-0_1.session.last.id	application/octet-stream	101 bytes	SHA1: 7b3bd593dac3bdf9c5549d5dd00a54478fbc28.. MD5: d699322e7550cc772ec12d2f8af89b13

6 of 684 events

SESSIONID: 24
TIME: 01/14/2020 04:26:36 pm
TIME.WHATEVER: 2020-01-14T16:26:36.000+0000
SIZE: 1246
UINT32.WHATEVER: 1246
PAYLOAD: 438
MEDIUM: 1
UINT8.WHATEVER

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.



NW SERVICE: Broker-Aggregation
SESSION ID: 24
SOURCE IP:PORT: 192.168.0.14 :48874
DESTINATION IP:PORT: 192.168.0.11 :50104
SERVICE: 80
FIRST PACKET TIME: 01/14/2020 04:26:36 pm
LAST PACKET TIME: 01/14/2020 04:26:36 pm
CALCULATED PACKET SIZE: 1246 bytes
CALCULATED PAYLOAD SIZE: 438 bytes
CALCULATED PACKET COUNT: 12

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data.

	FILE NAME	MIME TYPE	FILE SIZE	HASHES
☑	24-107-0_1.session.last.id	application/octet-stream	101 bytes	SHA1: 7b3bd593dac3bdf9c5549d5dd00a54478fbc28.. MD5: d699322e7550cc772ec12d2f8af89b13

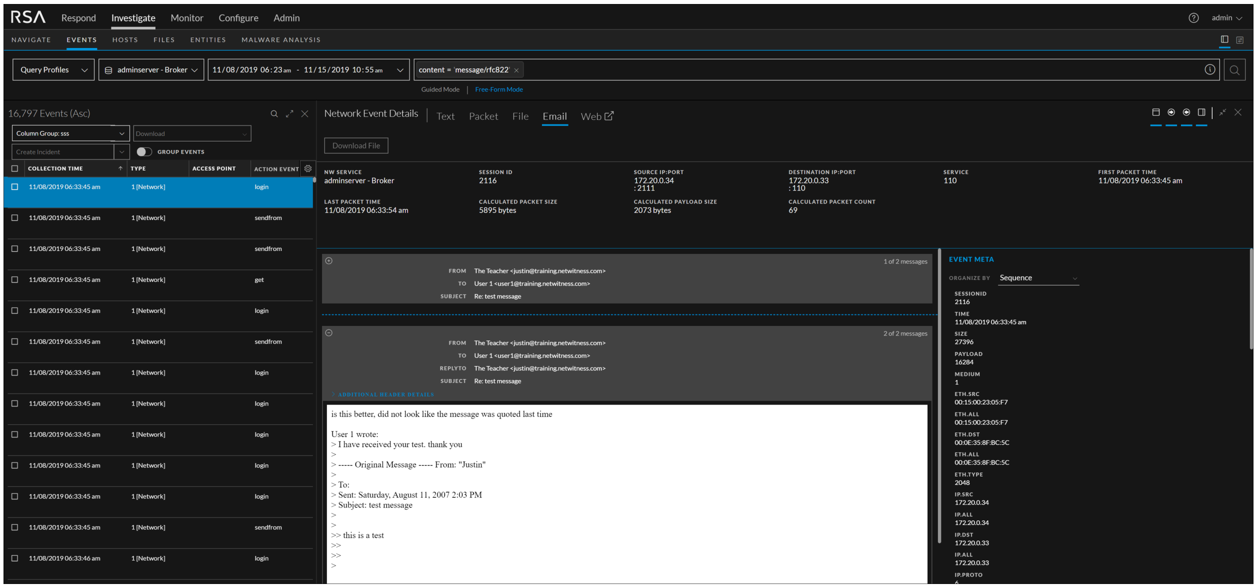
6 of 684 events

SESSIONID: 24
TIME: 01/14/2020 04:26:36 pm
TIME.WHATEVER: 2020-01-14T16:26:36.000+0000
SIZE: 1246
UINT32.WHATEVER: 1246
PAYLOAD: 438
MEDIUM: 1
UINT8.WHATEVER

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.

The Email Panel

The Email panel shows a list of emails associated with the selected network event. This is an example of the Email panel.



Query Profiles | adminserver - Broker | 11/08/2019 06:23 am - 11/15/2019 10:55 am | content = 'message/rfc822'

16,797 Events (Asc)

Column Group: sss

COLLECTION TIME	TYPE	ACCESS POINT	ACTION EVENT
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:45 am	1 [Network]		get
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:46 am	1 [Network]		login

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
adminserver - Broker	2116	172.20.0.34 :2111	172.20.0.33 :110	110	11/08/2019 06:33:45 am

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
11/08/2019 06:33:54 am	5895 bytes	2073 bytes	69

1 of 2 messages

FROM The Teacher <justin@training.netwitness.com>
TO User 1 <user1@training.netwitness.com>
SUBJECT Re: test message

2 of 2 messages

FROM The Teacher <justin@training.netwitness.com>
TO User 1 <user1@training.netwitness.com>
REPLYTO The Teacher <justin@training.netwitness.com>
SUBJECT Re: test message

ADDITIONAL HEADER DETAILS

```
is this better, did not look like the message was quoted last time

User 1 wrote:
> I have received your test. thank you
>
> ----- Original Message ----- From: "Justin"
>
> To:
> Sent: Saturday, August 11, 2007 2:03 PM
> Subject: test message
>
>
>> this is a test
>>
>>
>
```

EVENT META

ORGANIZE BY Sequence

SESSIONID 2116
TIME 11/08/2019 06:33:45 am
SIZE 27396
PAYLOAD 16284
MEDIUM 1
ETH.SRC 00:15:00:23:05:F7
ETH.ALL 00:15:00:23:05:F7
ETH.DST 00:0E:35:8F:BC:5C
ETH.ALL 00:0E:35:8F:BC:5C
ETH.TYPE 2048
IP.SRC 172.20.0.34
IP.ALL 172.20.0.34
IP.DST 172.20.0.33
IP.ALL 172.20.0.33
IP.PROTO

- By default, a single email is expanded and multiple emails are collapsed.
- Emails that contain attachments can be downloaded using one of the following methods:
  - To download single or multiple attachments, select the attachments and click **Download File**.
  - To download all attachments, select **All Attachments** and click **Download Files**.

> **Caution:** When you download and open attachments from an email, they may contain malicious data.

- An external link in an email cannot be accessed. Clicking an external link displays a **Link Address** popup window that provides the actual link.
- When an email body is too long, **Showing %** is displayed in the beginning of the email. To view the remaining content, click **Show Remaining %** at the bottom of the email.
- If an event contains a web email supported by the `alias.host` metadata of `mail.google.com`, `mail.live.com`, or `mail.yahoo.com`, a message is displayed with a link to view the reconstruction for the associated session in the Events Reconstruction page. If not, a "*No Email reconstruction is available for this event*" message is displayed.

Analytical Tools for Each Event Type

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

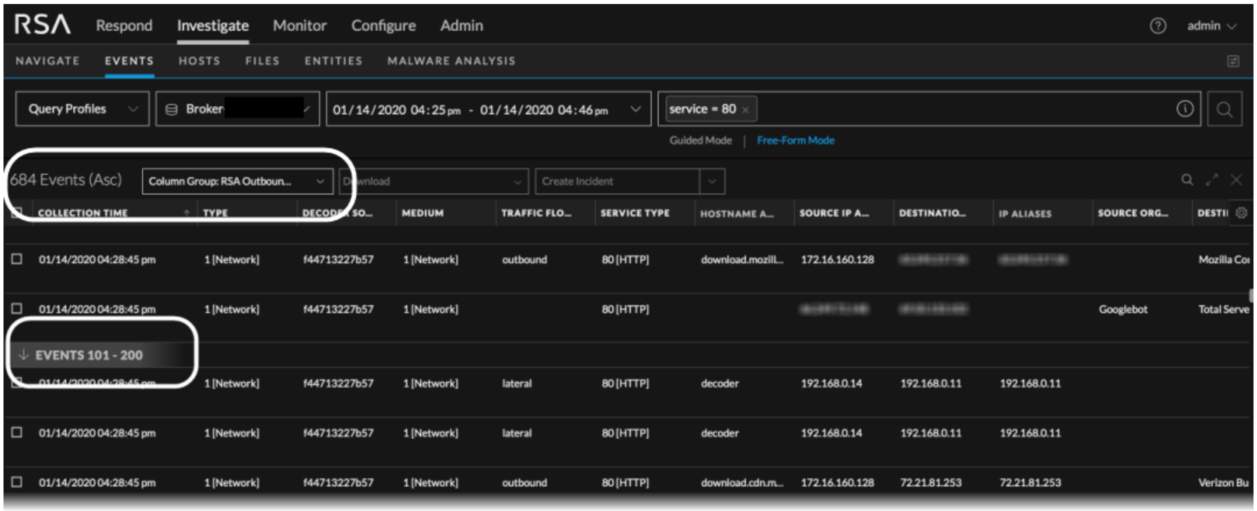
Analyze Events in the Events View

Note: In Version 11.4, the Event Analysis view was renamed as the Events view, replacing the Legacy Events view as the default view for the Events list. Any information regarding features prior to 11.4 also applies to the 11.3 and earlier Event Analysis view. The Legacy Events view is disabled by default, but the administrator can enable it as described in "Configure Investigation Settings" in the *System Configuration Guide*. You can view the details about prior versions as PDF documents here: https://community.rsa.com/docs/DOC-81328.

After a query is submitted in the Events 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 configurable limit on the number of events that can be loaded; the default value is 5,000. Administrators set the limit as described in the *System Configuration Guide*. 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.



01/14/2020 04:25 pm - 01/14/2020 04:46 pm

service = 80

684 Events (Asc)

Column Group: RSA Outboun...

□	COLLECTION TIME	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP A...	DESTINATIO...	IP ALIASES	SOURCE ORG...	DESTI
□	01/14/2020 04:28:45 pm	1 [Network]	f44713227b57	1 [Network]	outbound	80 [HTTP]	download.mozill...	172.16.160.128	[redacted]	[redacted]		Mozilla Co
□	01/14/2020 04:28:45 pm	1 [Network]	f44713227b57	1 [Network]		80 [HTTP]		[redacted]	[redacted]		Googlebot	Total Serve
	↓ EVENTS 101 - 200											
□	01/14/2020 04:28:45 pm	1 [Network]	f44713227b57	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.14	192.168.0.11	192.168.0.11		
□	01/14/2020 04:28:45 pm	1 [Network]	f44713227b57	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.14	192.168.0.11	192.168.0.11		
□	01/14/2020 04:28:45 pm	1 [Network]	f44713227b57	1 [Network]	outbound	80 [HTTP]	download.cdn.m...	172.16.160.128	72.21.81.253	72.21.81.253		Verizon Bu

A spinner is displayed while the events are loaded. If that count is greater than or equal to the threshold, a message under the spinner advises that fact and directs you to the Query Console for more details. As data begins loading, the message is removed and the spinner remains until all events are loaded. When all events have loaded, one of these messages is added to the bottom of the list:

- "All events loaded."
- "Reached the 5,000 event limit. Consider refining your query."
- "Retrieved 4,000 of 5,000 events prior to query cancellation."

In version 11.3 and later, you can set the sort sequence for the events listed in the Events panel in the Event Preferences dialog, either earliest collection time or latest collections time first. The default setting is earliest collection time first, which is well suited to most investigations. When investigating logs, you may want to change the sort sequence to latest collection time first. This user setting from the Events Preferences dialog is saved in the database and persists after logging out and logging back in.

In Version 11.4.1 and later, there is a new unsorted option, which is the default preference and lists events as processed by the Core services. Unsorted is faster because it streams back the events as soon as a match is found versus waiting for all Core services to respond and then displaying them in order.

If the number of events that match the query exceeds the limit of 5,000 events, the newest or oldest 5,000 events in the time window are loaded in ascending order. The portion of events loaded is based on the sort order. For example, if 300,000 events match your query and the sort sequence is set to Ascending, the oldest 5,000 events are loaded by default. You can change this by changing the sort order to Descending and the newest 5,000 events are loaded.

Ascending sort, which loads the oldest events first is usually the best setting for investigating network events. If you want to view the newest 5,000 events in the time window, you can change the user preference sort order to Descending in the Event Preferences panel. Any change in the setting goes into effect the next time you submit a query.

A message at the top of the list indicates the total number of events loaded and if the 5,000 event limit has been reached:

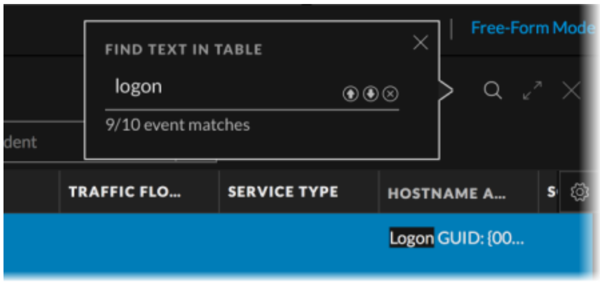
- The message when less than 5,000 events are listed is: "xx,xxx Events (Asc)"
- The message when more than 5,000 events are listed is: "Oldest 10,000 Events (Asc)"

From this view, you can select a column for sorting events in the Events panel and select a set of meta keys that help with a specific type of investigation (column group). You can download events and create an incident in Respond. Clicking an event opens a reconstruction of the event in different formats (Packet, Text, File, Web, and Email). The Events panel and the reconstruction panel can be open at the same time. Within the Packet panel and the Text panel, you can use additional features to adjust the way the reconstruction is displayed and bring interesting data into focus.

Find a Text String in the Events Panel (Version 11.4 and Later)

With the Events panel open, you can search for a text string in the list of events. This search is similar to the CTRL-F search in a browser window. The search scans all text in every row of the table, visible columns only, to find matching text and highlights the matches. Columns that are not displayed are not searched. The search function is disabled if the Summary column is part of the table.

1. With events loaded in the Events panel, click 🔍 on the right side of the toolbar.



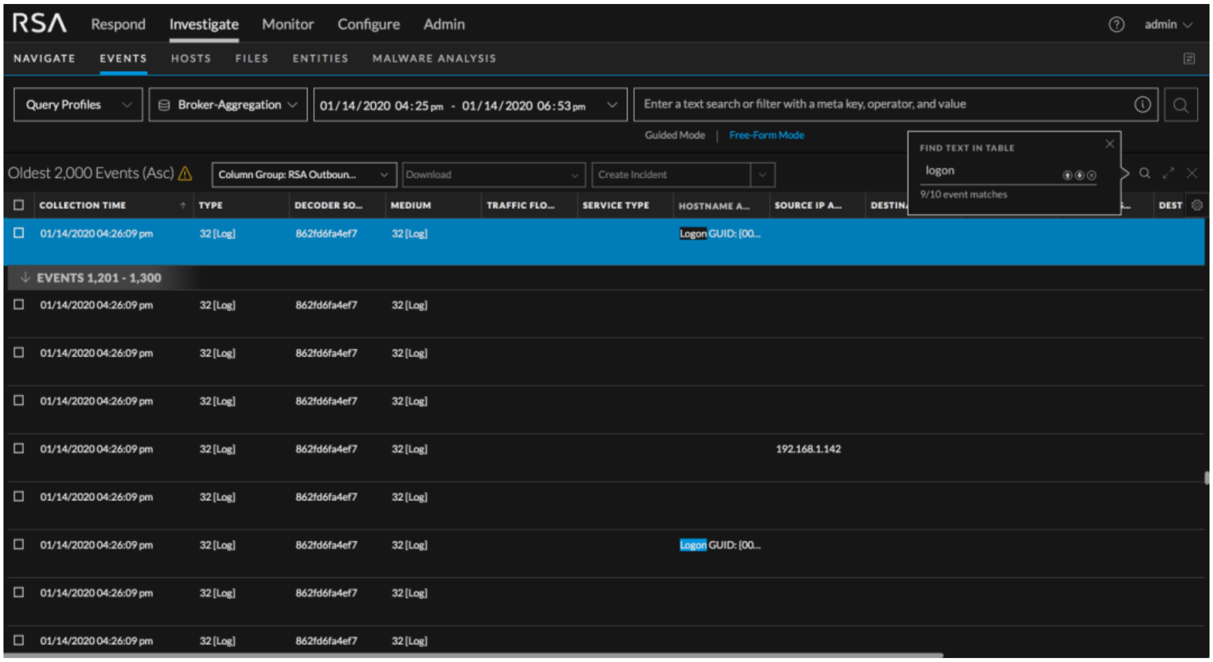
FIND TEXT IN TABLE

logon

9/10 event matches

2. In the **Find Text in Table** dialog, start typing a text string.
   After you type two characters, exact matches of the text string without regard to case are highlighted

in the Events panel. As you type more text, highlighted events are further refined. The following figure is an example of the results found after entering "logon" in the Find Text in Table dialog. The text string was found in 10 events. The first event is highlighted in blue with the text string within the event also highlighted. Icons are available for navigating the search results and closing the dialog.



01/14/2020 04:25 pm - 01/14/2020 06:53 pm

Enter a text search or filter with a meta key, operator, and value

Oldest 2,000 Events (Asc) ⚠

Column Group: RSA Outboun...

FIND TEXT IN TABLE

logon

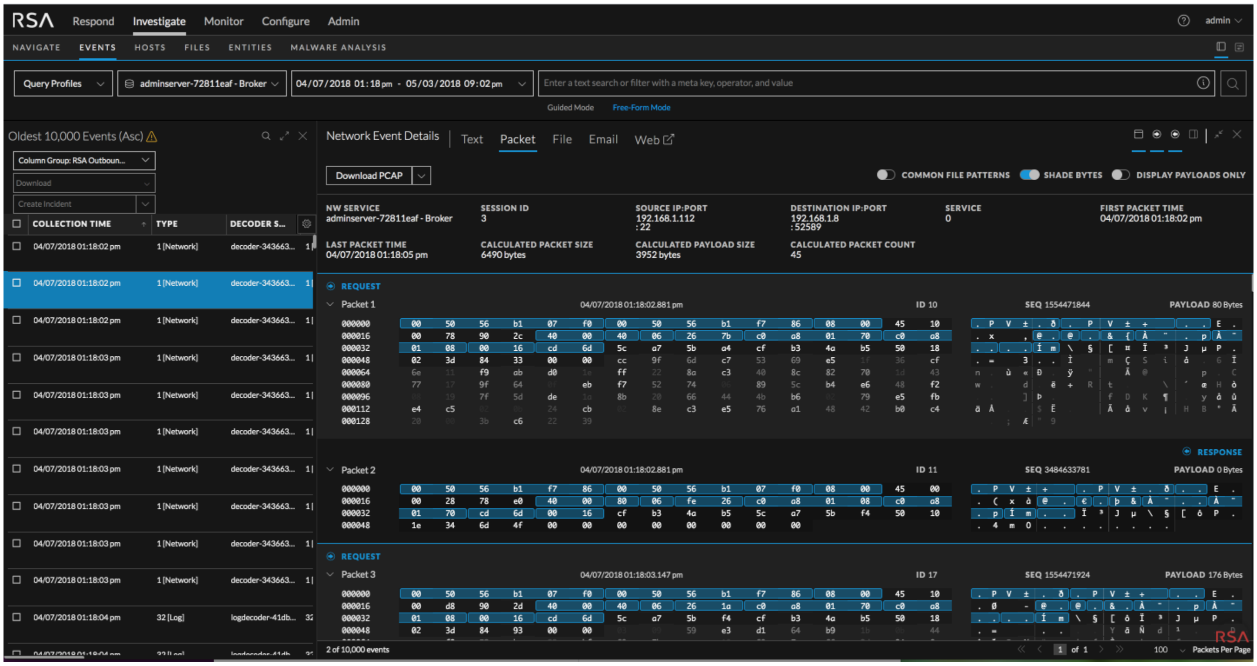
9/10 event matches

□	COLLECTION TIME	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP A...	DESTIN...	DEST
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]			Logon GUID: {00...			
↓ EVENTS 1,201 - 1,300										
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]						
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]						
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]						
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]				192.168.1.142		
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]						
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]			Logon GUID: {00...			
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]						
□	01/14/2020 04:26:09 pm	32 [Log]	862fd6fa4ef7	32 [Log]						

3. To navigate through the search results, click the up and down arrows.
   - To view the next event that contains the text string and navigate downward through the search results, click the down arrow. If you click the down arrow when viewing the last result, the first result is highlighted.
   - To view the immediately prior event that contains the text string and navigate upward through the search results, click the up arrow. If you click the up arrow while viewing the first result, the last result is highlighted.
4. To close the search dialog, click X or press the ESCAPE key. The dialog also closes if you open a reconstruction, select a new column group, or execute a new query.

Open, Close, and Adjust the Size of the Panels in the Events View

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



□	COLLECTION TIME	TYPE	DECODER S...	
□	04/07/2018 01:18:02 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:02 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:02 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:03 pm	1 [Network]	decoder-343663...	1
□	04/07/2018 01:18:04 pm	32 [Log]	logdecoder-41db...	32
□	04/07/2018 01:18:04 pm	32 [Log]	logdecoder-41db...	32

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
adminserver-72811eaf - Broker	3	192.168.1.112 :22	192.168.1.8 :52589	0	04/07/2018 01:18:02 pm

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
04/07/2018 01:18:05 pm	6490 bytes	3952 bytes	45

```
REQUEST
Packet 1        04/07/2018 01:18:02.881 pm        ID 10        SEQ 1554471844        PAYLOAD 80 Bytes
000000  00 50 56 b1 07 f0 00 50 56 b1 f7 86 08 00 45 10
000016  00 78 90 2c 40 00 40 06 26 7b c0 a8 01 70 c0 a8
000032  01 08 00 16 cd 6d 5c a7 5b a4 cf b3 4a b5 50 18
000048  02 3d 84 33 00 00 cc 9f 6d c7 53 69 e5 1f 36 cf
000064  6e 11 f9 ab d0 1e ff 22 8a c3 40 8c 82 70 1d 43
000080  77 17 9f 64 0f eb f7 52 74 06 89 5c b4 e6 48 f2
000096  08 19 7f 5d de 1a 8b 20 66 44 4b b6 02 79 e5 fb
000112  e4 c5 02 0b 24 cb 02 8e c3 e5 76 a1 48 42 b0 c4
000128  20 00 3b c6 22 39

RESPONSE
Packet 2        04/07/2018 01:18:02.881 pm        ID 11        SEQ 3484633781        PAYLOAD 0 Bytes
000000  00 50 56 b1 f7 86 00 50 56 b1 07 f0 08 00 45 00
000016  00 28 78 e0 40 00 80 06 fe 26 c0 a8 01 08 c0 a8
000032  01 70 cd 6d 00 16 cf b3 4a b5 5c a7 5b f4 50 10
000048  1e 34 6d 4f 00 00 00 00 00 00 00 00

REQUEST
Packet 3        04/07/2018 01:18:03.147 pm        ID 17        SEQ 1554471924        PAYLOAD 176 Bytes
000000  00 50 56 b1 07 f0 00 50 56 b1 f7 86 08 00 45 10
000016  00 d8 90 2d 40 00 40 06 26 1a c0 a8 01 70 c0 a8
000032  01 08 00 16 cd 6d 5c a7 5b f4 cf b3 4a b5 50 18
000048  02 3d 84 93 00 00 03 09 59 e3 d1 64 b9 1b 0b 44
```

2 of 10,000 events

1 of 1 100 Packets Per Page

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.

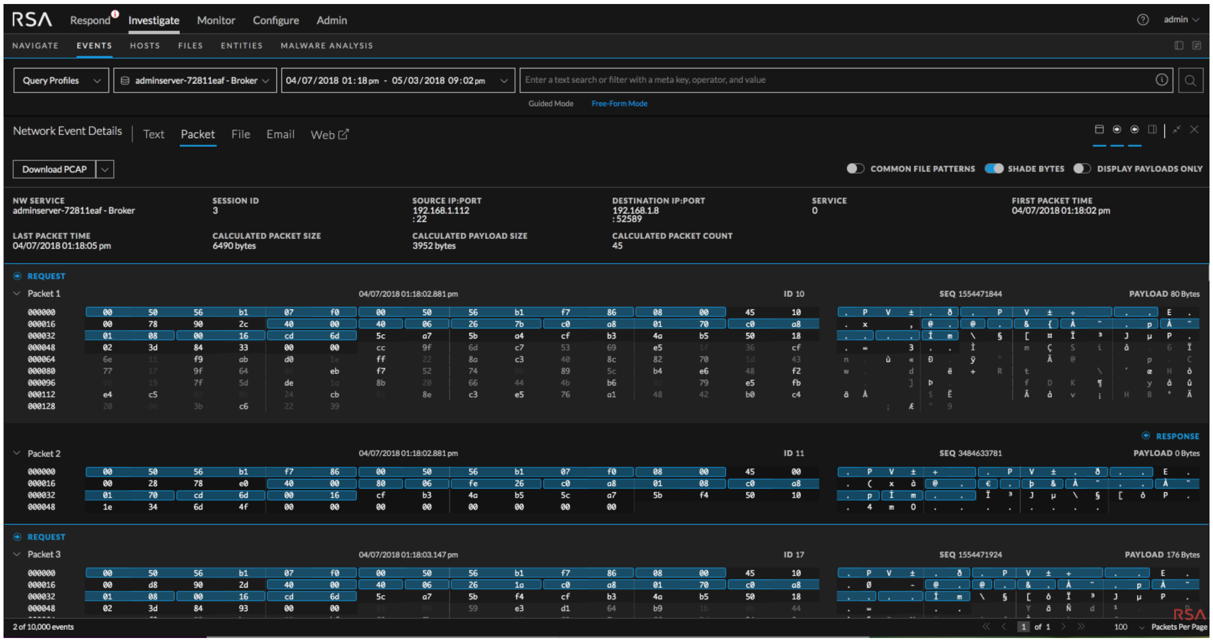
To optimize your view:

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.



NW SERVICE
adminserver-72811eaf - Broker

SESSION ID
3

SOURCE IP:PORT
192.168.1.112
: 22

DESTINATION IP:PORT
192.168.1.8
: 52589

SERVICE
0

FIRST PACKET TIME
04/07/2018 01:18:02 pm

LAST PACKET TIME
04/07/2018 01:18:05 pm

CALCULATED PACKET SIZE
6490 bytes

CALCULATED PAYLOAD SIZE
3952 bytes

CALCULATED PACKET COUNT
45

REQUEST

```
Packet 1          04/07/2018 01:18:02.881 pm          ID 10          SEQ 1554471844          PAYLOAD 80 Bytes
000000  00 50 56 b1 07 f0 00 50 56 b1 f7 86 08 00 45 10    . P V ± . ð . P V ± ÷   . . E .
000016  00 78 90 2c 40 00 40 06 26 7b c0 a8 01 70 c0 a8    . x   , @ . @ . & { À ¨ . p À ¨
000032  01 08 00 16 cd 6d 5c a7 5b a4 cf b3 4a b5 50 18    . . . . Í m \ § [ ¤ Ï ³ J µ P .
000048  02 3d 84 33 00 00 cc 9f 6d c7 53 69 e5 1f 36 cf    . =   3 . . Ì   m Ç S i å . 6 Ï
000064  6e 11 f9 ab d0 1e ff 22 8a c3 40 8c 82 70 1d 43    n . ù « Ð . ÿ "   Ã @     p . C
000080  77 17 9f 64 0f eb f7 52 74 06 89 5c b4 e6 48 f2    w .   d . ë ÷ R t .   \ ´ æ H ò
000096  08 19 7f 5d de 1a 8b 20 66 44 4b b6 02 79 e5 fb    . .   ] Þ .     f D K ¶ . y å û
000112  e4 c5 02 0b 24 cb 02 8e c3 e5 76 a1 48 42 b0 c4    ä Å . . $ Ë .   Ã å v ¡ H B ° Ä
000128  20 00 3b c6 22 39                                    . ; Æ " 9
```

RESPONSE

```
Packet 2          04/07/2018 01:18:02.881 pm          ID 11          SEQ 3484633781          PAYLOAD 0 Bytes
000000  00 50 56 b1 f7 86 00 50 56 b1 07 f0 08 00 45 00    . P V ± ÷   . P V ± . ð . . E .
000016  00 28 78 e0 40 00 80 06 fe 26 c0 a8 01 08 c0 a8    . ( x à @ . € . þ & À ¨ . . À ¨
000032  01 70 cd 6d 00 16 cf b3 4a b5 5c a7 5b f4 50 10    . p Í m . . Ï ³ J µ \ § [ ô P .
000048  1e 34 6d 4f 00 00 00 00 00 00 00 00                . 4 m O . . . . . . . .
```

REQUEST

```
Packet 3          04/07/2018 01:18:03.147 pm          ID 17          SEQ 1554471924          PAYLOAD 176 Bytes
000000  00 50 56 b1 07 f0 00 50 56 b1 f7 86 08 00 45 10    . P V ± . ð . P V ± ÷   . . E .
000016  00 d8 90 2d 40 00 40 06 26 1a c0 a8 01 70 c0 a8    . Ø   - @ . @ . & . À ¨ . p À ¨
000032  01 08 00 16 cd 6d 5c a7 5b f4 cf b3 4a b5 50 18    . . . . Í m \ § [ ô Ï ³ J µ P .
000048  02 3d 84 93 00 00 83 09 59 e3 d1 64 b9 1b 0b 44    . =   . . .   . Y ã Ñ d ¹ . . D
```

2 of 10,000 events

1 of 1 · 100 Packets Per Page

3. To reopen the Events panel after closing, click □ in the top right corner of the Events 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 the Analysis Type for an Event

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

1. In the Events view toolbar, click the analysis type in the toolbar.

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

Note: The packet reconstruction is only available for network events.

Adjust the Display of Requests and Responses

For analysis 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 panel is an example of a reconstruction type without requests and responses. A reconstructed log event in the Text panel is another example.

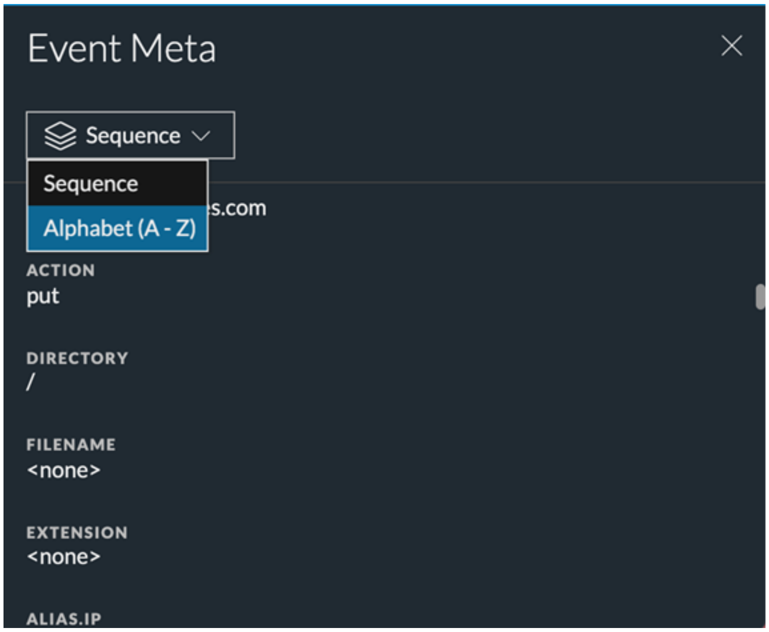
To select which side of the conversation to show, Request (➡, Response ⬅, or both, click one or both of the direction icons. The reconstruction is refreshed with the selected information.

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 Associated Metadata for an Event

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

Analysts reviewing the metadata associated with results in the Events view can change the order of the metadata listed to better track down what they are looking for. The layout of the list of metadata has been changed to be more intuitive, and metadata can optionally be organized by the sequence in which they were generated or alphabetically by meta key. This figure illustrates metadata organized as meta keys sorted alphabetically.



Event Meta

s.com

ACTION
put

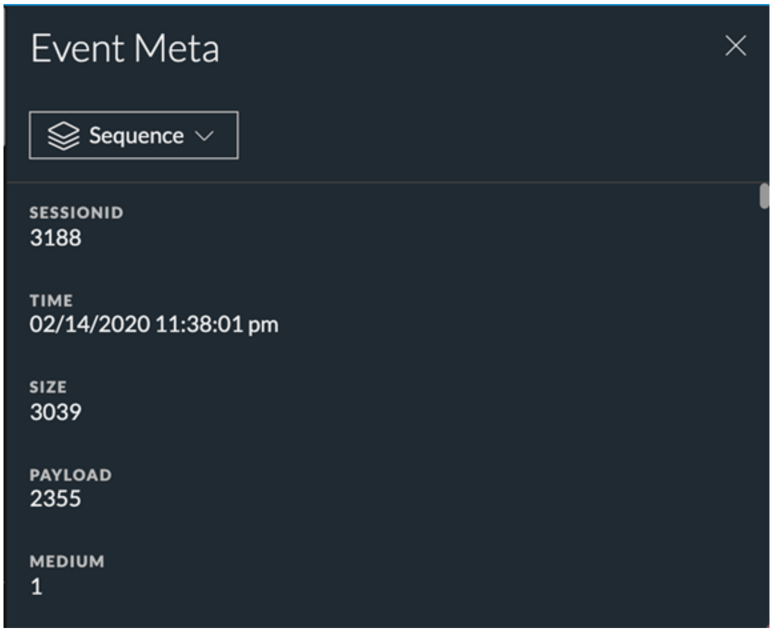
DIRECTORY
/

FILENAME
<none>

EXTENSION
<none>

ALIAS.IP

This figure illustrates the same metadata presented in the sequence that the meta keys were generated.



SESSIONID
3188

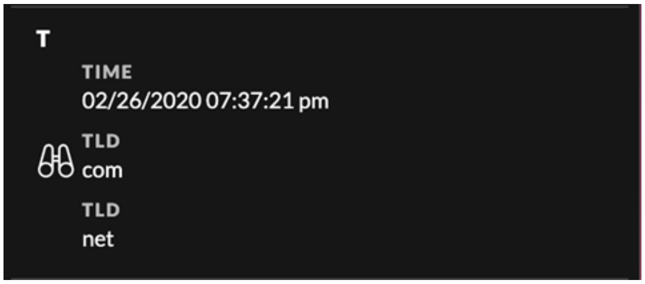
TIME
02/14/2020 11:38:01 pm

SIZE
3039

PAYLOAD
2355

MEDIUM
1

When viewing a 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 figure is an example of white binoculars on a black background marking a searchable meta key.

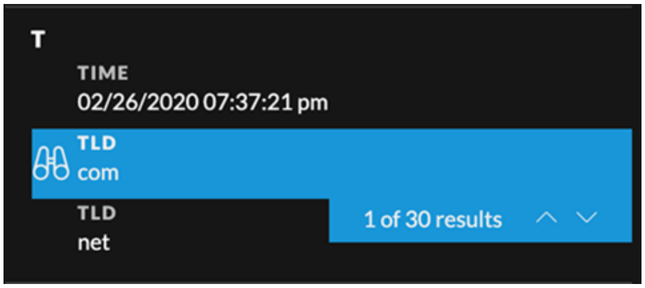


TIME
02/26/2020 07:37:21 pm

TLD
com

TLD
net

Clicking the icon triggers a search for the meta key/meta value pair (case-insensitive) in the Text panel and each instance is highlighted. This is an example of white binoculars on a blue background after clicking a searchable meta key/ meta value combination.



TIME
02/26/2020 07:37:21 pm

TLD
com

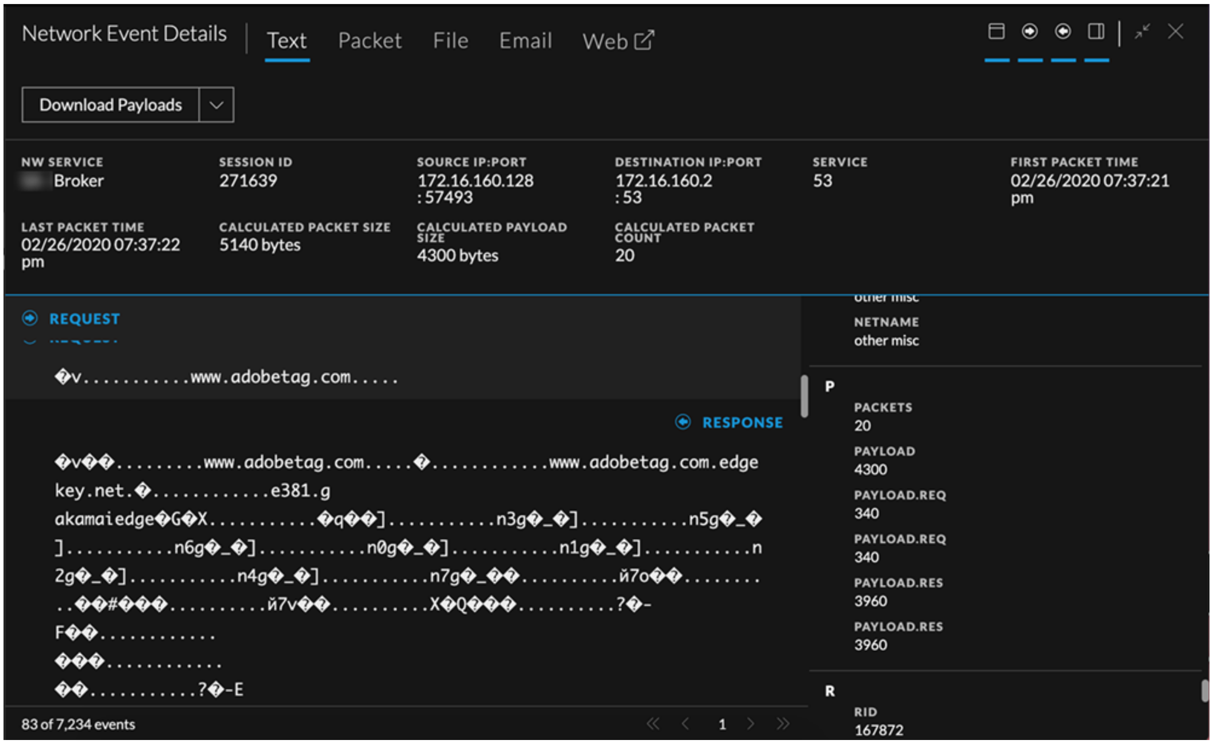
TLD
net

In the Event Meta panel, the highlighted row has a count of the results and up and down arrows that you can use to quickly find each result in the Text 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 panel and click ◫ to open the Event Meta panel.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Broker	271639	172.16.160.128 :57493	172.16.160.2 :53	53	02/26/2020 07:37:21 pm

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
02/26/2020 07:37:22 pm	5140 bytes	4300 bytes	20

```
�v..........www.adobetag.com.....
```

```
�v��.........www.adobetag.com.....�...........www.adobetag.com.edge
key.net.�...........e381.g
akamaiedge�G�X..........�q��]..........n3g�_�]..........n5g�_�
]..........n6g�_�]..........n0g�_�]..........n1g�_�]..........n
2g�_�]..........n4g�_�]..........n7g�_��..........й7o��........
..��#���..........й7v��..........X�Q���..........?�-
F��...........
���...........
��..........?�-E
```

other misc

NETNAME
other misc

P

PACKETS
20

PAYLOAD
4300

PAYLOAD.REQ
340

PAYLOAD.REQ
340

PAYLOAD.RES
3960

PAYLOAD.RES
3960

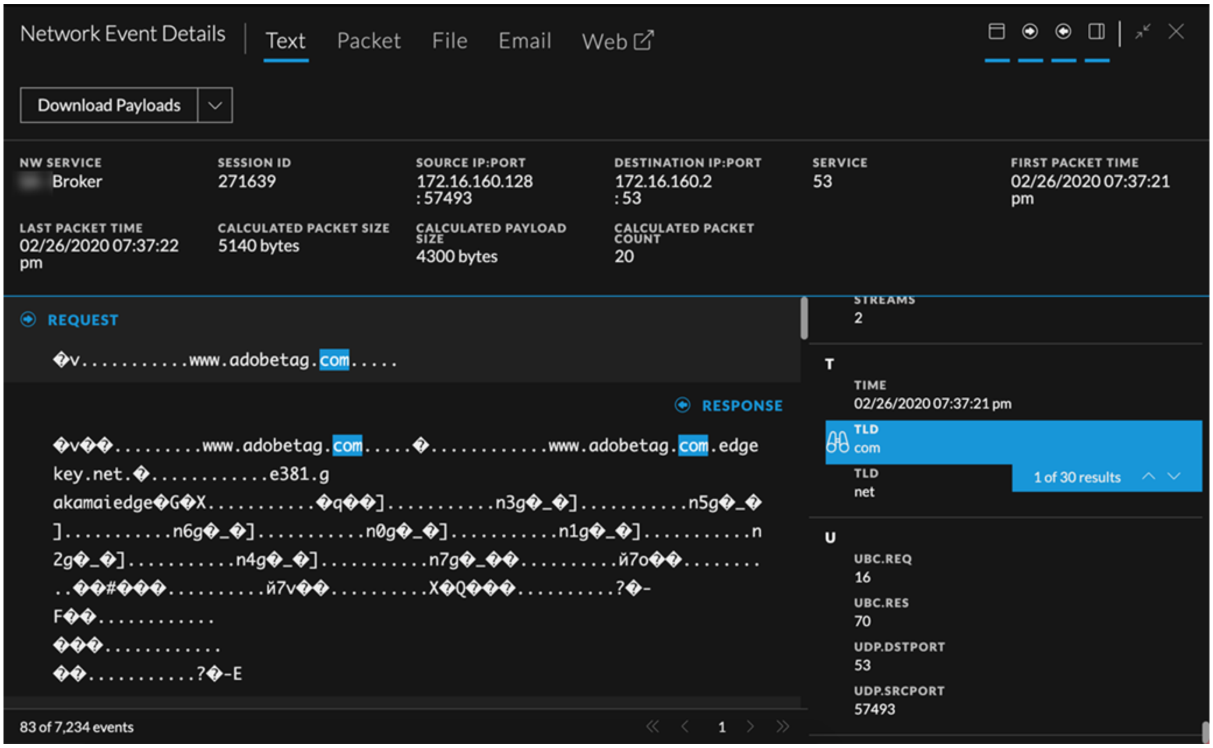
R

RID
167872

2. Hover the mouse over the meta key/meta value pairs in the list until you see a binoculars icon next to a meta key.

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 panel.
   If one or more relevant instances of the value is found in the Text panel, each occurrence is highlighted. The value that you are searching for is highlighted in the Event Meta panel and the

up/down arrows for scrolling are visible.



NW SERVICE [redacted] Broker | SESSION ID 271639 | SOURCE IP:PORT 172.16.160.128 :57493 | DESTINATION IP:PORT 172.16.160.2 :53 | SERVICE 53 | FIRST PACKET TIME 02/26/2020 07:37:21 pm

LAST PACKET TIME 02/26/2020 07:37:22 pm | CALCULATED PACKET SIZE 5140 bytes | CALCULATED PAYLOAD SIZE 4300 bytes | CALCULATED PACKET COUNT 20

REQUEST

```
�v..........www.adobetag.com.....
```

RESPONSE

```
�v��........www.adobetag.com.....�...........www.adobetag.com.edge
key.net.�...........e381.g
akamaiedge�G�X...........�q��]..........n3g�_�]..........n5g�_�
]..........n6g�_�]..........n0g�_�]..........n1g�_�]..........n
2g�_�]..........n4g�_�]..........n7g�_��.........й7o��.......
..��#���.........й7v��.........X�Q���.........?�-
F��...........
���...........
��..........?�-E
```

83 of 7,234 events « ‹ 1 › »

STREAMS 2

T

TIME 02/26/2020 07:37:21 pm

TLD com

TLD net

1 of 30 results

U

UBC.REQ 16

UBC.RES 70

UDP.DSTPORT 53

UDP.SRCPORT 57493

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

Note: When a meta 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 panel, Text panel, or File panel, providing more vertical space for the data, click ▭. Clicking the icon again shows the Event Header.

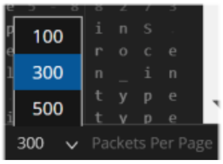
Page Through Events in the Packet and Text Panels

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

Note: Pagination controls are available in Version 11.2 and later of the Text panel.

To use pagination controls:

1. With an event open in the Events view, click the current number of packets per page (**50, 100**, **300**, or **500**), and select the new number of packets per page from the drop-down menu.

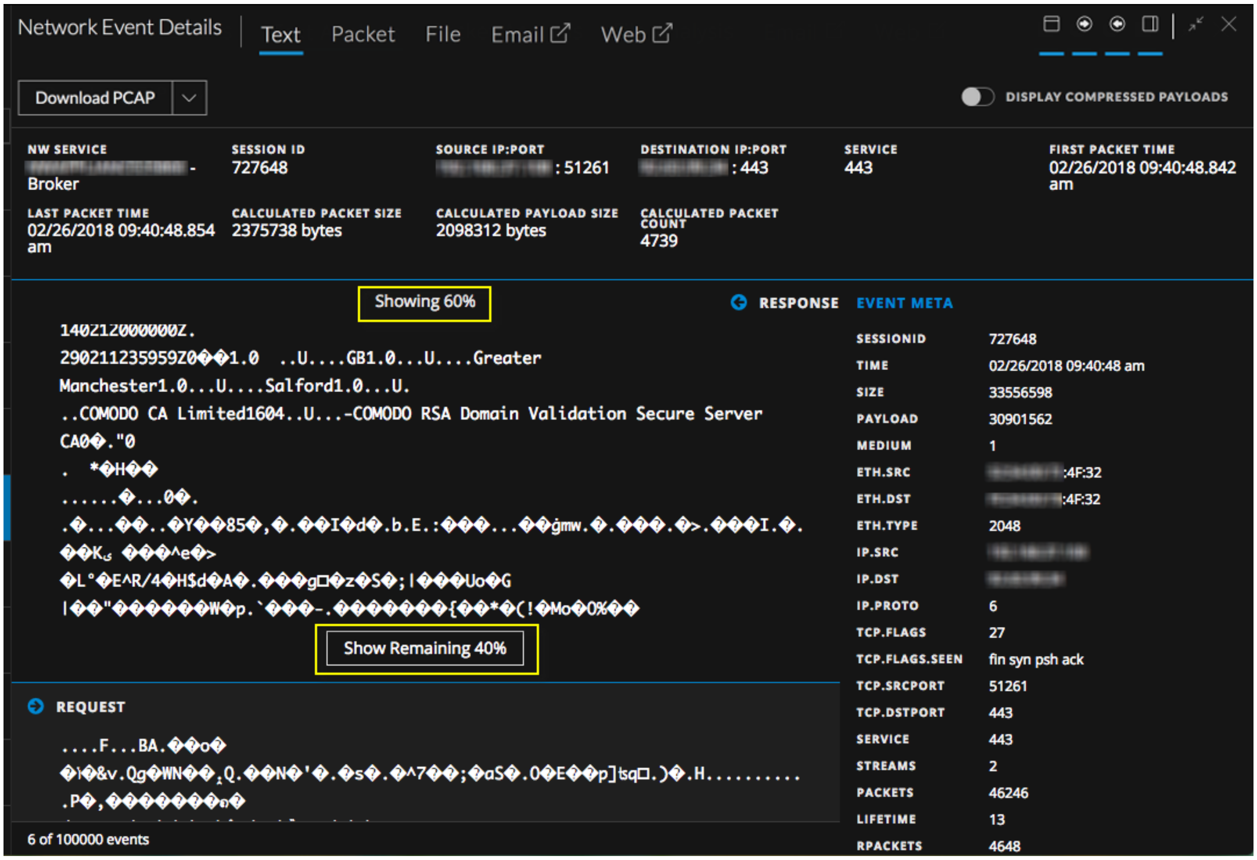
2. To page forward or back, use the page control icons:
   Click › to go to the next page.
   Click » to go to the last page.
   Click ‹ to go the previous page.
   Click « to go to the first page.

3. To go to a specific page, type a page number in the page number field 1 of 206.

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

Expand Truncated Text Entries in the Text Panel

A reconstruction of a network event in the Text 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.



NW SERVICE: [redacted] - Broker
SESSION ID: 727648
SOURCE IP:PORT: [redacted] : 51261
DESTINATION IP:PORT: [redacted] : 443
SERVICE: 443
FIRST PACKET TIME: 02/26/2018 09:40:48.842 am
LAST PACKET TIME: 02/26/2018 09:40:48.854 am
CALCULATED PACKET SIZE: 2375738 bytes
CALCULATED PAYLOAD SIZE: 2098312 bytes
CALCULATED PACKET COUNT: 4739

```
140212000000Z.
290211235959Z0��1.0  ..U....GB1.0...U....Greater
Manchester1.0...U....Salford1.0...U.
..COMODO CA Limited1604..U...-COMODO RSA Domain Validation Secure Server
CA0�."0
.  *�H��
......�...0�.
.�...��..�Y��85�,�.��I�d�.b.E.:���...��ġmw.�.���.�>.���I.�.
��K؊ ���^e�>
�L°�E^R/4�H$d�A�.���g□�z�S�;|���Uo�G
|��"�������W�p.`���-.��������{��*�(!�Mo�0%��
```

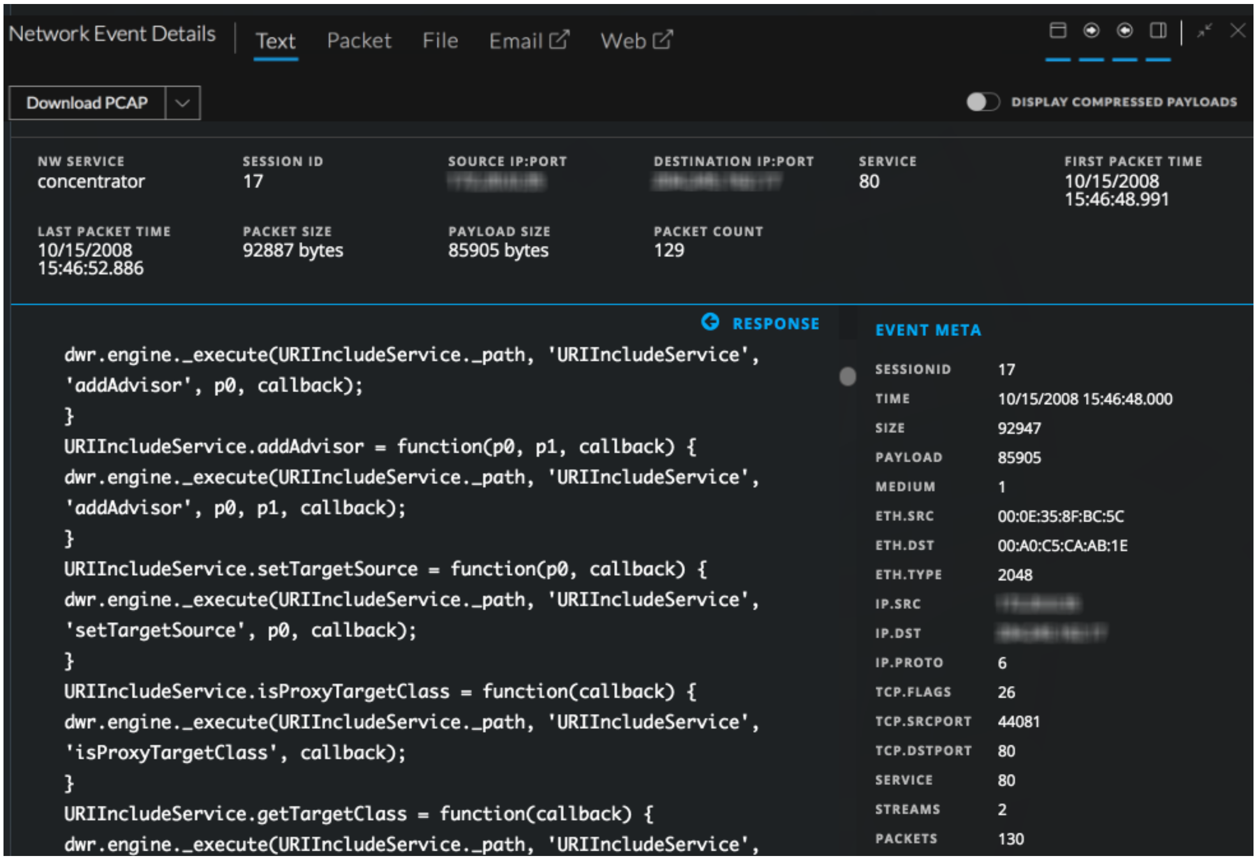
```
....F...BA.��o�
�ǃ�&v.Qg�WN��ꜰQ.��N�'�.�s�.�^7��;�aS�.0�E��p]ʦq□.)�.H.........
.P�,��������ɒ�
```

6 of 100000 events

EVENT META

SESSIONID	727648
TIME	02/26/2018 09:40:48 am
SIZE	33556598
PAYLOAD	30901562
MEDIUM	1
ETH.SRC	[redacted]:4F:32
ETH.DST	[redacted]:4F:32
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	27
TCP.FLAGS.SEEN	fin syn psh ack
TCP.SRCPORT	51261
TCP.DSTPORT	443
SERVICE	443
STREAMS	2
PACKETS	46246
LIFETIME	13
RPACKETS	4648

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.



NW SERVICE concentrator
SESSION ID 17
SOURCE IP:PORT [redacted]
DESTINATION IP:PORT [redacted]
SERVICE 80
FIRST PACKET TIME 10/15/2008 15:46:48.991
LAST PACKET TIME 10/15/2008 15:46:52.886
PACKET SIZE 92887 bytes
PAYLOAD SIZE 85905 bytes
PACKET COUNT 129

```
dwr.engine._execute(URIIncludeService._path, 'URIIncludeService',
'addAdvisor', p0, callback);
}
URIIncludeService.addAdvisor = function(p0, p1, callback) {
dwr.engine._execute(URIIncludeService._path, 'URIIncludeService',
'addAdvisor', p0, p1, callback);
}
URIIncludeService.setTargetSource = function(p0, callback) {
dwr.engine._execute(URIIncludeService._path, 'URIIncludeService',
'setTargetSource', p0, callback);
}
URIIncludeService.isProxyTargetClass = function(callback) {
dwr.engine._execute(URIIncludeService._path, 'URIIncludeService',
'isProxyTargetClass', callback);
}
URIIncludeService.getTargetClass = function(callback) {
dwr.engine._execute(URIIncludeService._path, 'URIIncludeService',
```

SESSIONID	17
TIME	10/15/2008 15:46:48.000
SIZE	92947
PAYLOAD	85905
MEDIUM	1
ETH.SRC	00:0E:35:8F:BC:5C
ETH.DST	00:A0:C5:CA:AB:1E
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	26
TCP.SRCPORT	44081
TCP.DSTPORT	80
SERVICE	80
STREAMS	2
PACKETS	130

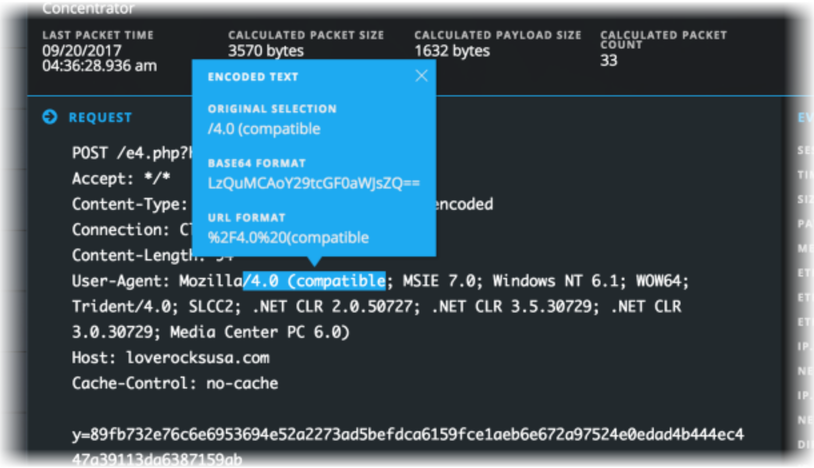
If you search for metadata seen in the Event Meta panel while text is truncated in the Text panel, the truncated text is searched. If the metadata exists inside hidden text, the text entry expands to reveal the text with the found metadata.

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

If a network session being reconstructed in the Text 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 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.



Concentrator

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
09/20/2017 04:36:28.936 am	3570 bytes	1632 bytes	33

ENCODED TEXT

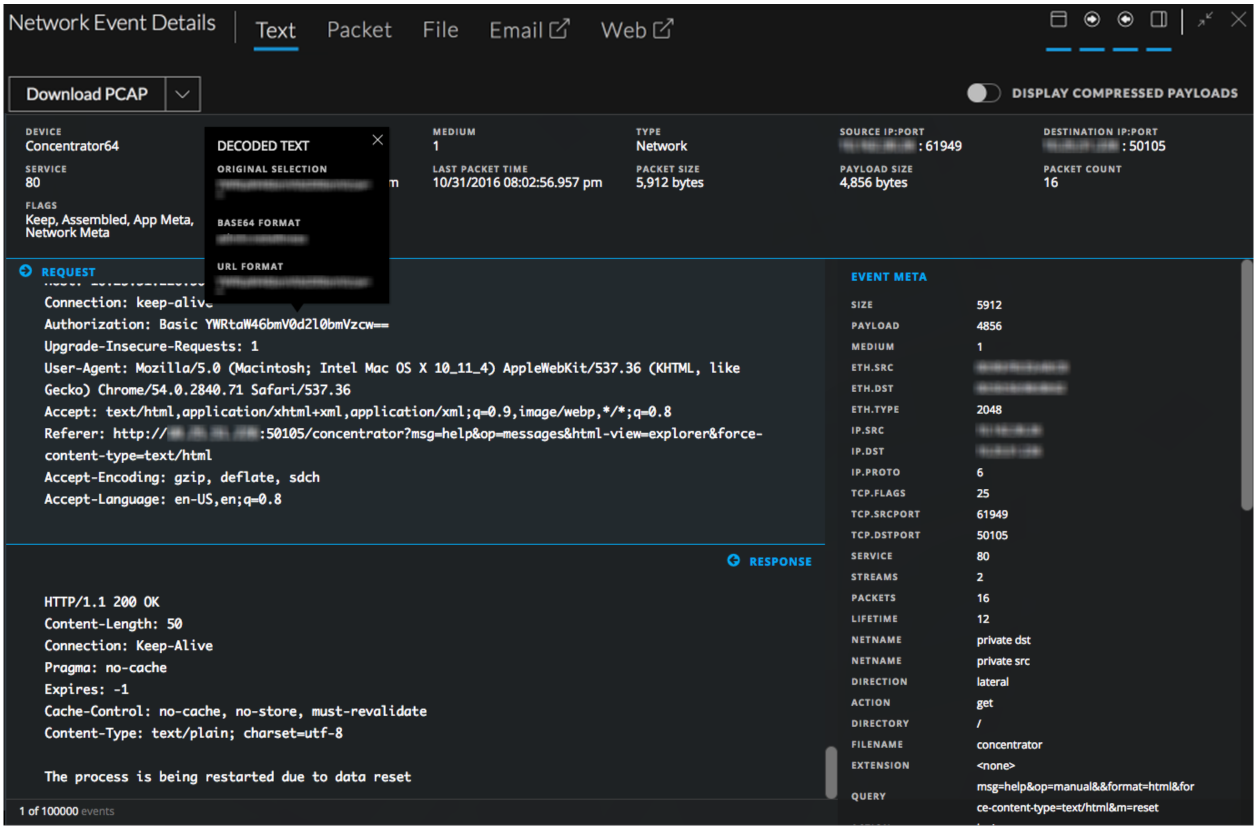
ORIGINAL SELECTION
/4.0 (compatible

BASE64 FORMAT
LzQuMCAoY29tcGF0aWJsZQ==

URL FORMAT
%2F4.0%20(compatible

REQUEST

```
POST /e4.php?
Accept: */*
Content-Type:                          encoded
Connection: C
Content-Length: 
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Host: loverocksusa.com
Cache-Control: no-cache

y=89fb732e76c6e6953694e52a2273ad5befdca6159fce1aeb6e672a97524e0edad4b444ec4
47a39113da6387159ab
```



DEVICE	MEDIUM	TYPE	SOURCE IP:PORT	DESTINATION IP:PORT
Concentrator64	1	Network	[redacted] : 61949	[redacted] : 50105

SERVICE	LAST PACKET TIME	PACKET SIZE	PAYLOAD SIZE	PACKET COUNT
80	10/31/2016 08:02:56.957 pm	5,912 bytes	4,856 bytes	16

FLAGS
Keep, Assembled, App Meta, Network Meta

DECODED TEXT

ORIGINAL SELECTION
[redacted]

BASE64 FORMAT
[redacted]

URL FORMAT
[redacted]

REQUEST

```
Connection: keep-alive
Authorization: Basic YWRtaW46bmV0d2l0bmVzcw==
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/54.0.2840.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://[redacted]:50105/concentrator?msg=help&op=messages&html-view=explorer&force-
content-type=text/html
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
```

RESPONSE

```
HTTP/1.1 200 OK
Content-Length: 50
Connection: Keep-Alive
Pragma: no-cache
Expires: -1
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: text/plain; charset=utf-8

The process is being restarted due to data reset
```

1 of 100000 events

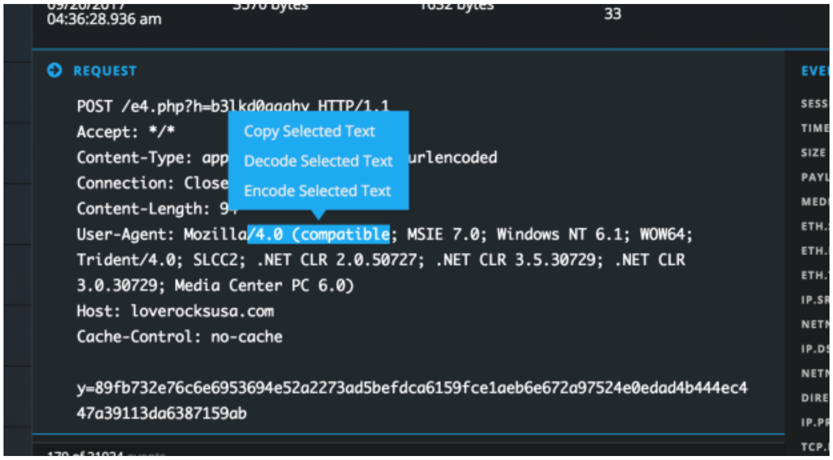
EVENT META

SIZE	5912
PAYLOAD	4856
MEDIUM	1
ETH.SRC	[redacted]
ETH.DST	[redacted]
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	25
TCP.SRCPORT	61949
TCP.DSTPORT	50105
SERVICE	80
STREAMS	2
PACKETS	16
LIFETIME	12
NETNAME	private dst
NETNAME	private src
DIRECTION	lateral
ACTION	get
DIRECTORY	/
FILENAME	concentrator
EXTENSION	<none>
QUERY	msg=help&op=manual&&format=html&force-content-type=text/html&m=reset

To perform encoding and decoding in the Text panel:

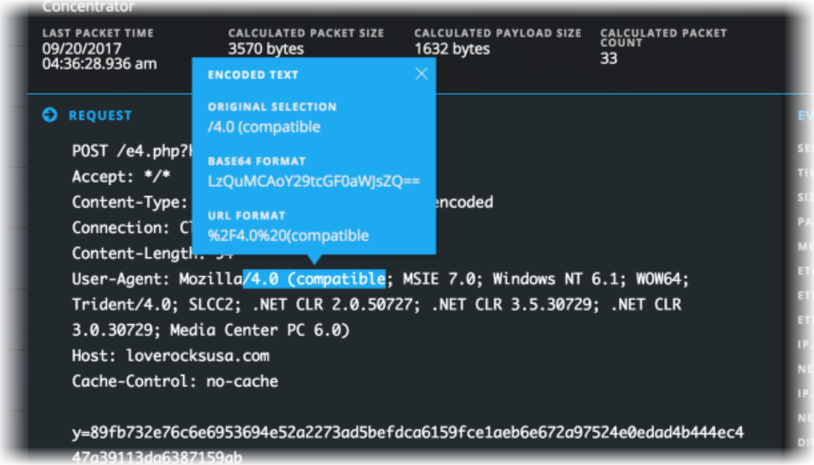
1. In the **Events view**, go to the Text panel of a session that contains encoded or decoded content.
2. To view some decoded text in encoded form, drag to select the text within a single Request or Response.

A menu offers options to encode and decode.



```
04:36:28.936 am                                              33

POST /e4.php?h=b3lkd0aaahy HTTP/1.1
Accept: */*
Content-Type: app                    urlencoded
Connection: Close
Content-Length: 9
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Host: loverocksusa.com
Cache-Control: no-cache

y=89fb732e76c6e6953694e52a2273ad5befdca6159fce1aeb6e672a97524e0edad4b444ec4
47a39113da6387159ab
```

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 panel, close the Events panel, select another event for reconstruction, or switch to a different reconstruction view.



LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
09/20/2017 04:36:28.936 am	3570 bytes	1632 bytes	33

ENCODED TEXT

ORIGINAL SELECTION
/4.0 (compatible

BASE64 FORMAT
LzQuMCAoY29tcGF0aWJsZQ==

URL FORMAT
%2F4.0%20(compatible

```
POST /e4.php?
Accept: */*
Content-Type:                        encoded
Connection: C
Content-Length
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Host: loverocksusa.com
Cache-Control: no-cache

y=89fb732e76c6e6953694e52a2273ad5befdca6159fce1aeb6e672a97524e0edad4b444ec4
47a39113da6387159ab
```

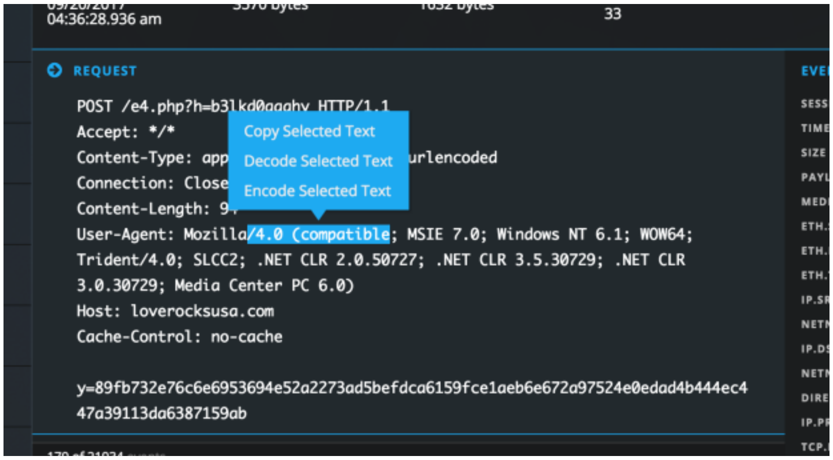
   When a longer text is selected, the hover box is scrollable and large enough to fit the entire selected text and the decoded text.

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 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.



```
POST /e4.php?h=b3lkd0aaahv HTTP/1.1
Accept: */*
Content-Type: app                        urlencoded
Connection: Close
Content-Length: 9
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Host: loverocksusa.com
Cache-Control: no-cache

y=89fb732e76c6e6953694e52a2273ad5befdca6159fce1aeb6e672a97524e0edad4b444ec4
47a39113da6387159ab
```

   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 Panel

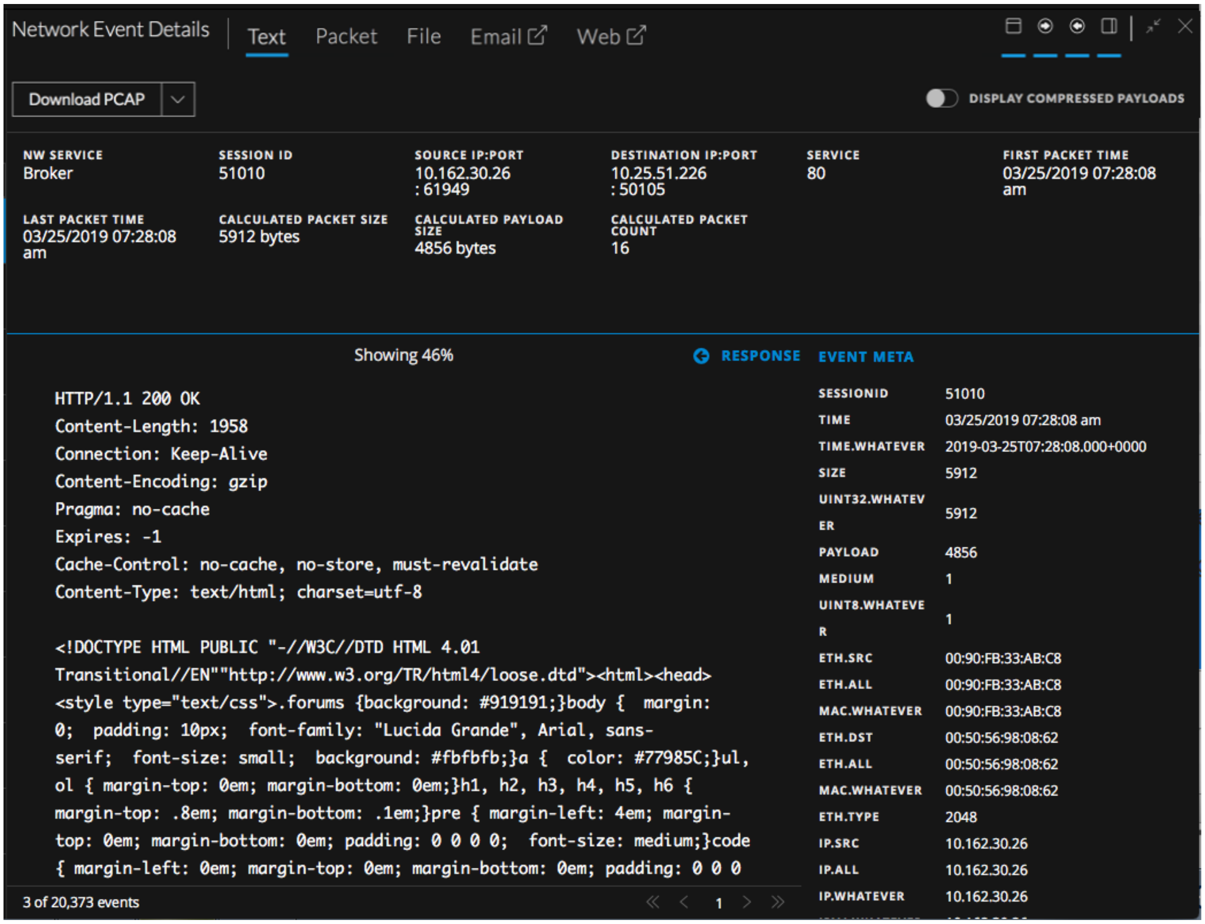
When the content of an HTTP network session is compressed and you are viewing the Text panel, NetWitness Platform displays decompressed content by default. This helps you to determine if there are any patterns and view the readable characters. You can switch between a compressed and decompressed view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

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

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

1. Open the Text 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.



NW SERVICE Broker

SESSION ID 51010

SOURCE IP:PORT 10.162.30.26 : 61949

DESTINATION IP:PORT 10.25.51.226 : 50105

SERVICE 80

FIRST PACKET TIME 03/25/2019 07:28:08 am

LAST PACKET TIME 03/25/2019 07:28:08 am

CALCULATED PACKET SIZE 5912 bytes

CALCULATED PAYLOAD SIZE 4856 bytes

CALCULATED PACKET COUNT 16

Showing 46%

RESPONSE

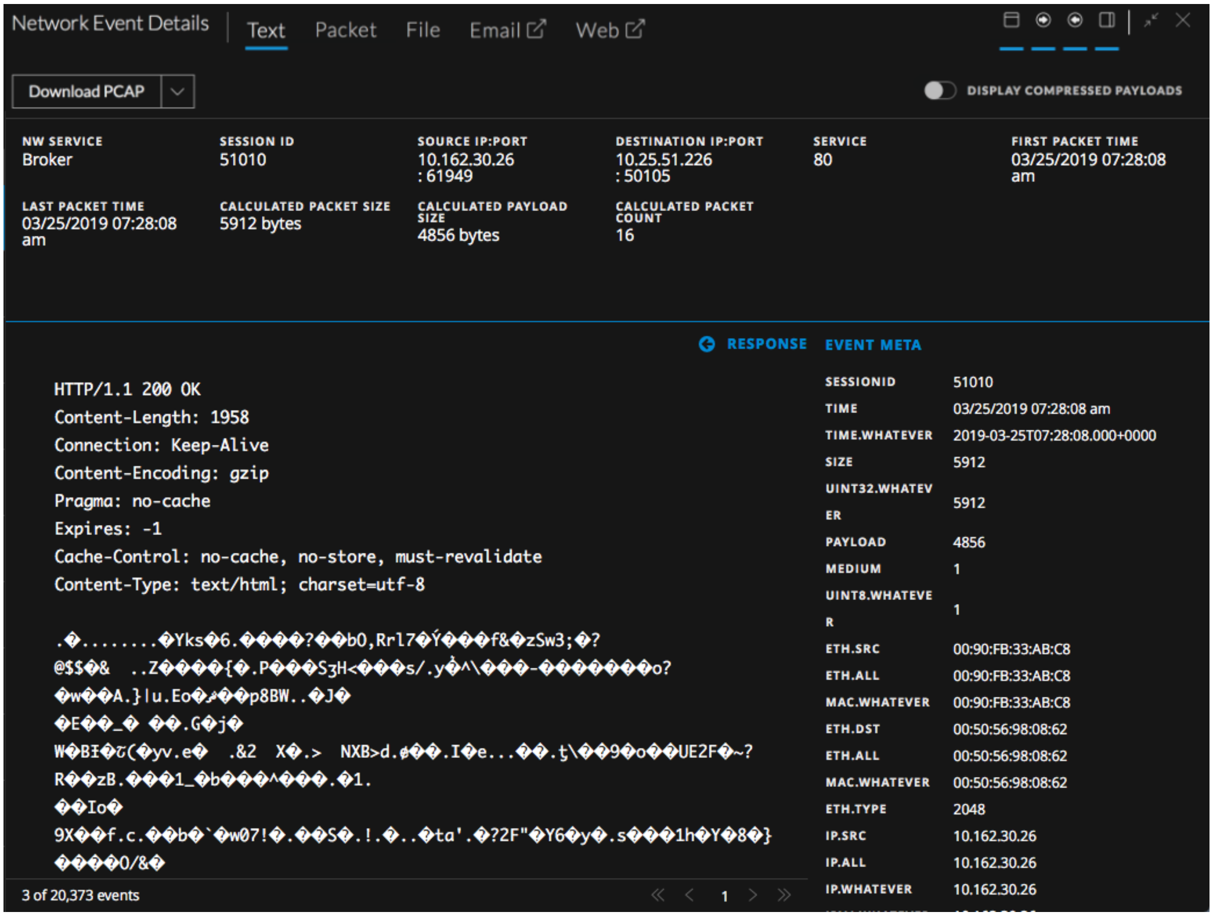
```
HTTP/1.1 200 OK
Content-Length: 1958
Connection: Keep-Alive
Content-Encoding: gzip
Pragma: no-cache
Expires: -1
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN""http://www.w3.org/TR/html4/loose.dtd"><html><head>
<style type="text/css">.forums {background: #919191;}body {  margin:
0;  padding: 10px;  font-family: "Lucida Grande", Arial, sans-
serif;  font-size: small;  background: #fbfbfb;}a {  color: #77985C;}ul,
ol { margin-top: 0em; margin-bottom: 0em;}h1, h2, h3, h4, h5, h6 {
margin-top: .8em; margin-bottom: .1em;}pre { margin-left: 4em; margin-
top: 0em; margin-bottom: 0em; padding: 0 0 0 0;  font-size: medium;}code
{ margin-left: 0em; margin-top: 0em; margin-bottom: 0em; padding: 0 0 0
```

3 of 20,373 events

EVENT META

SESSIONID	51010
TIME	03/25/2019 07:28:08 am
TIME.WHATEVER	2019-03-25T07:28:08.000+0000
SIZE	5912
UINT32.WHATEVER	5912
PAYLOAD	4856
MEDIUM	1
UINT8.WHATEVER	1
ETH.SRC	00:90:FB:33:AB:C8
ETH.ALL	00:90:FB:33:AB:C8
MAC.WHATEVER	00:90:FB:33:AB:C8
ETH.DST	00:50:56:98:08:62
ETH.ALL	00:50:56:98:08:62
MAC.WHATEVER	00:50:56:98:08:62
ETH.TYPE	2048
IP.SRC	10.162.30.26
IP.ALL	10.162.30.26
IP.WHATEVER	10.162.30.26

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.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Broker	51010	10.162.30.26 : 61949	10.25.51.226 : 50105	80	03/25/2019 07:28:08 am

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
03/25/2019 07:28:08 am	5912 bytes	4856 bytes	16

```
HTTP/1.1 200 OK
Content-Length: 1958
Connection: Keep-Alive
Content-Encoding: gzip
Pragma: no-cache
Expires: -1
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: text/html; charset=utf-8

.�........�Yks�6.����?��b0,Rrl7�Ý���f&�zSw3;�?
@$$�&  ..Z�����{�.P���S3H<���s/.y�^\���-��������o?
�w��A.}|u.Eo�⸙��p8BW..�J�
�E��_� ��.G�j�
W�BI�ϛ(�yv.e�  .&2  X�.>  NXB>d.ø��.I�e...��.ţ\���9�o��UE2F�~?
R��zB.���1_�b���^���.�1.
��Io�
9X��f.c.��b�`�w07!�.��S�.!.�..�ta'.�?2F"�Y6�y�.s���1h�Y�8�}
����0/&�
```

EVENT META	
SESSIONID	51010
TIME	03/25/2019 07:28:08 am
TIME.WHATEVER	2019-03-25T07:28:08.000+0000
SIZE	5912
UINT32.WHATEVER	5912
PAYLOAD	4856
MEDIUM	1
UINT8.WHATEVER	1
ETH.SRC	00:90:FB:33:AB:C8
ETH.ALL	00:90:FB:33:AB:C8
MAC.WHATEVER	00:90:FB:33:AB:C8
ETH.DST	00:50:56:98:08:62
ETH.ALL	00:50:56:98:08:62
MAC.WHATEVER	00:50:56:98:08:62
ETH.TYPE	2048
IP.SRC	10.162.30.26
IP.ALL	10.162.30.26
IP.WHATEVER	10.162.30.26

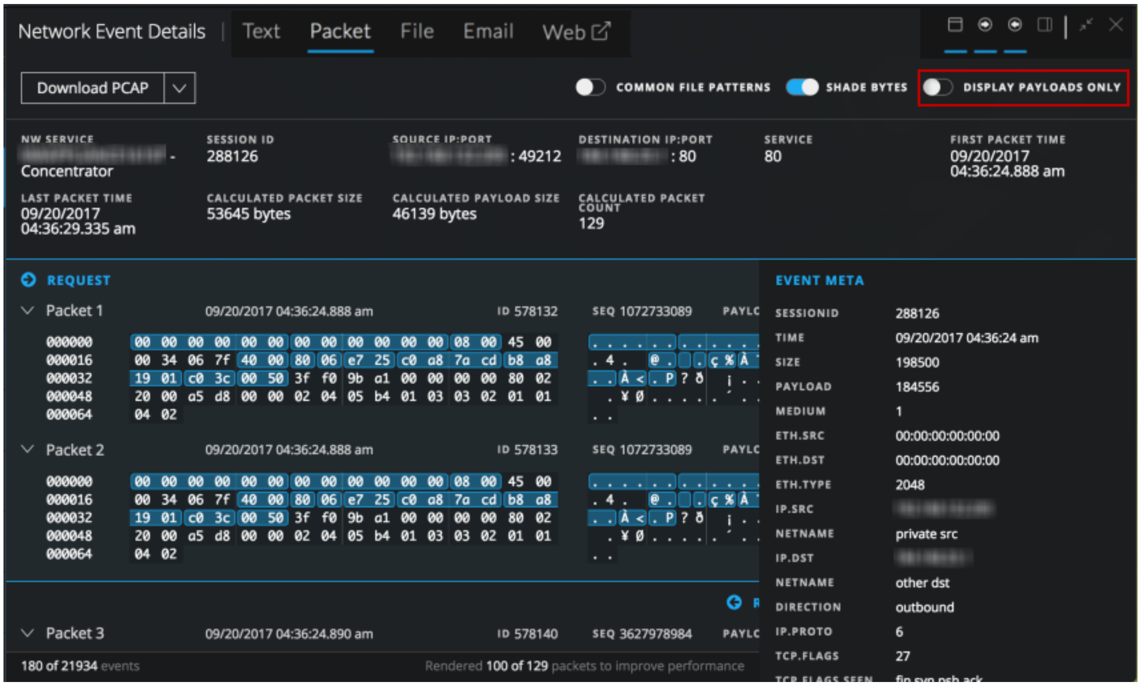
3. To return to the view of decompressed text, click the switch again.

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

When viewing a reconstruction of a network session in the Packet 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 off. 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 **Events** view, go to the Packet panel of a network session.
   By default the session is reconstructed with the packet header, footer, and payload displayed.



NW SERVICE: [redacted] - Concentrator
SESSION ID: 288126
SOURCE IP:PORT: [redacted] : 49212
DESTINATION IP:PORT: [redacted] : 80
SERVICE: 80
FIRST PACKET TIME: 09/20/2017 04:36:24.888 am
LAST PACKET TIME: 09/20/2017 04:36:29.335 am
CALCULATED PACKET SIZE: 53645 bytes
CALCULATED PAYLOAD SIZE: 46139 bytes
CALCULATED PACKET COUNT: 129

REQUEST

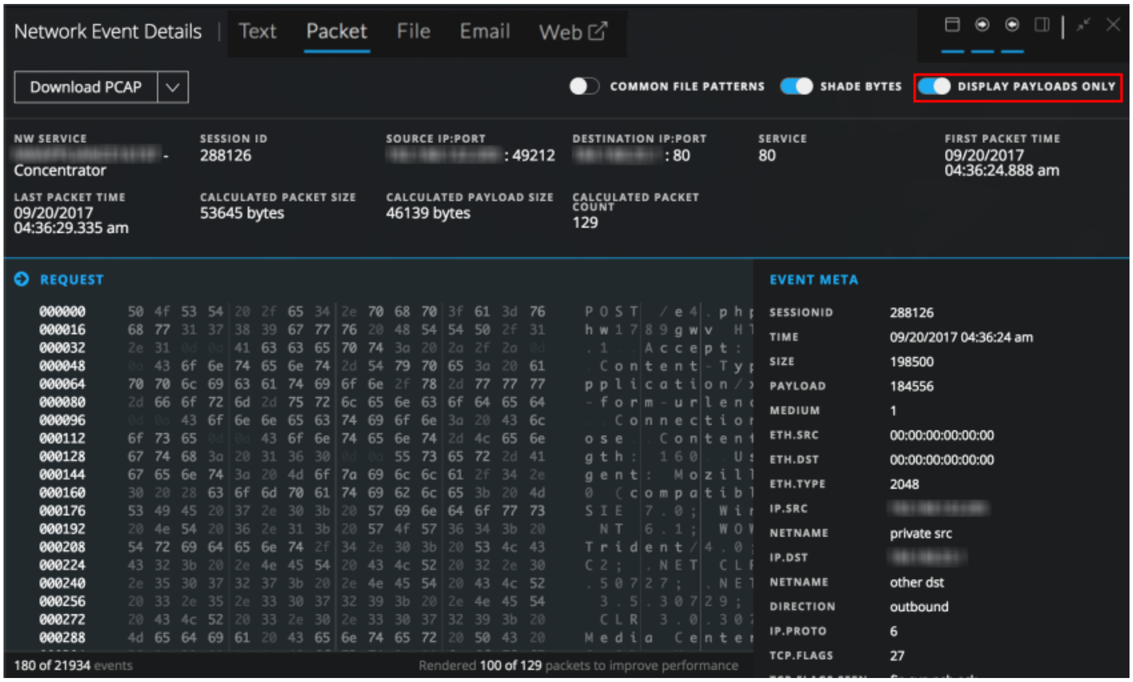
```
Packet 1        09/20/2017 04:36:24.888 am        ID 578132    SEQ 1072733089    PAYLC

000000   00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00   . . . . . . . . . . . . . . .
000016   00 34 06 7f 40 00 80 06 e7 25 c0 a8 7a cd b8 a8   . 4 .   @ .   . ç % À
000032   19 01 c0 3c 00 50 3f f0 9b a1 00 00 00 00 80 02   . . À < . P ? ð   ¡ . .
000048   20 00 a5 d8 00 00 02 04 05 b4 01 03 03 02 01 01     . ¥ Ø . . . . . ´ . .
000064   04 02                                             . .

Packet 2        09/20/2017 04:36:24.888 am        ID 578133    SEQ 1072733089    PAYLC

000000   00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00   . . . . . . . . . . . . . . .
000016   00 34 06 7f 40 00 80 06 e7 25 c0 a8 7a cd b8 a8   . 4 .   @ .   . ç % À
000032   19 01 c0 3c 00 50 3f f0 9b a1 00 00 00 00 80 02   . . À < . P ? ð   ¡ . .
000048   20 00 a5 d8 00 00 02 04 05 b4 01 03 03 02 01 01     . ¥ Ø . . . . . ´ . .
000064   04 02                                             . .

Packet 3        09/20/2017 04:36:24.890 am        ID 578140    SEQ 3627978984    PAYLC
```

180 of 21934 events
Rendered 100 of 129 packets to improve performance

EVENT META

SESSIONID	288126
TIME	09/20/2017 04:36:24 am
SIZE	198500
PAYLOAD	184556
MEDIUM	1
ETH.SRC	00:00:00:00:00:00
ETH.DST	00:00:00:00:00:00
ETH.TYPE	2048
IP.SRC	[redacted]
NETNAME	private src
IP.DST	[redacted]
NETNAME	other dst
DIRECTION	outbound
IP.PROTO	6
TCP.FLAGS	27
TCP.FLAGS SEEN	fin syn psh ack

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



NW SERVICE: [redacted] - Concentrator
SESSION ID: 288126
SOURCE IP:PORT: [redacted] : 49212
DESTINATION IP:PORT: [redacted] : 80
SERVICE: 80
FIRST PACKET TIME: 09/20/2017 04:36:24.888 am
LAST PACKET TIME: 09/20/2017 04:36:29.335 am
CALCULATED PACKET SIZE: 53645 bytes
CALCULATED PAYLOAD SIZE: 46139 bytes
CALCULATED PACKET COUNT: 129

REQUEST

```
000000   50 4f 53 54 20 2f 65 34 2e 70 68 70 3f 61 3d 76   P O S T   / e 4 . p h p
000016   68 77 31 37 38 39 67 77 76 20 48 54 54 50 2f 31   h w 1 7 8 9 g w v   H T
000032   2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d   . 1 . . A c c e p t :
000048   0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61   . C o n t e n t - T y p
000064   70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77   p p l i c a t i o n / x
000080   2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64   - f o r m - u r l e n c
000096   0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c   . . C o n n e c t i o n
000112   6f 73 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e   o s e . . C o n t e n t
000128   67 74 68 3a 20 31 36 30 0d 0a 55 73 65 72 2d 41   g t h :   1 6 0 . . U s
000144   67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e   g e n t :   M o z i l l
000160   30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d   0   ( c o m p a t i b l
000176   53 49 45 20 37 2e 30 3b 20 57 69 6e 64 6f 77 73   S I E   7 . 0 ;   W i n
000192   20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20     N T   6 . 1 ;   W O W
000208   54 72 69 64 65 6e 74 2f 34 2e 30 3b 20 53 4c 43   T r i d e n t / 4 . 0 ;
000224   43 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 30   C 2 ;   . N E T   C L R
000240   2e 35 30 37 32 37 3b 20 2e 4e 45 54 20 43 4c 52   . 5 0 7 2 7 ;   . N E T
000256   20 33 2e 35 2e 33 30 37 32 39 3b 20 2e 4e 45 54     3 . 5 . 3 0 7 2 9 ;
000272   20 43 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20     C L R   3 . 0 . 3 0 7
000288   4d 65 64 69 61 20 43 65 6e 74 65 72 20 50 43 20   M e d i a   C e n t e r
```

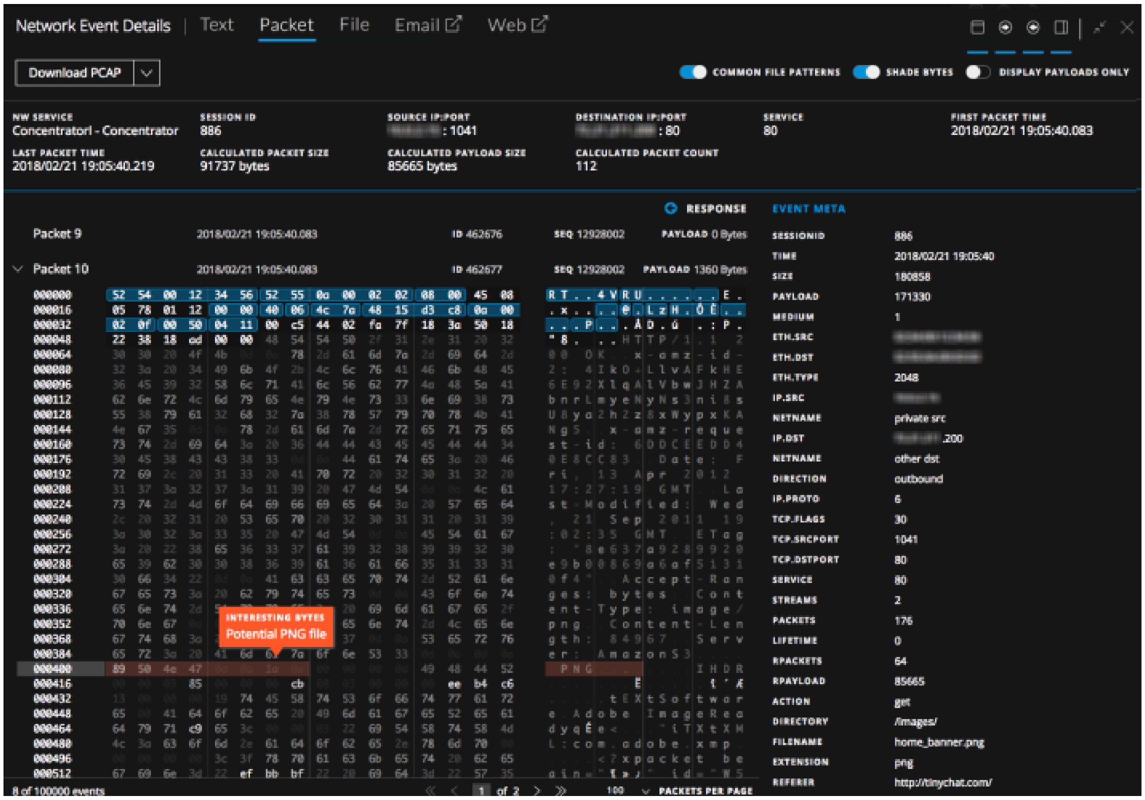
180 of 21934 events
Rendered 100 of 129 packets to improve performance

EVENT META

SESSIONID	288126
TIME	09/20/2017 04:36:24 am
SIZE	198500
PAYLOAD	184556
MEDIUM	1
ETH.SRC	00:00:00:00:00:00
ETH.DST	00:00:00:00:00:00
ETH.TYPE	2048
IP.SRC	[redacted]
NETNAME	private src
IP.DST	[redacted]
NETNAME	other dst
DIRECTION	outbound
IP.PROTO	6
TCP.FLAGS	27

View Highlighted Bytes in the Packet Panel

When you first open a reconstruction in the Packet 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 with highlighting and byte shading.



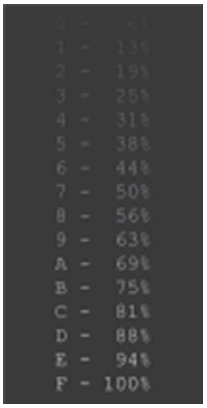
NW SERVICE: Concentratorl - Concentrator
SESSION ID: 886
SOURCE IP:PORT: [redacted] : 1041
DESTINATION IP:PORT: [redacted] : 80
SERVICE: 80
FIRST PACKET TIME: 2018/02/21 19:05:40.083
LAST PACKET TIME: 2018/02/21 19:05:40.219
CALCULATED PACKET SIZE: 91737 bytes
CALCULATED PAYLOAD SIZE: 85665 bytes
CALCULATED PACKET COUNT: 112

```
Packet 9    2018/02/21 19:05:40.083   ID 462676   SEQ 12928002   PAYLOAD 0 Bytes
Packet 10   2018/02/21 19:05:40.083   ID 462677   SEQ 12928002   PAYLOAD 1360 Bytes

000000  52 54 00 12 34 56 52 55 0a 00 02 02 08 00 45 08   R T . . 4 V R U . . . . . . E .
000016  05 78 01 12 00 00 40 06 4c 7a 48 15 d3 c8 0a 00   . x . . . . @ . L z H . Ó È . .
000032  02 0f 00 50 04 11 00 c5 44 02 fa 7f 18 3a 50 18   . . . P . . . Å D . ú . . : P .
000048  22 38 18 ad 00 00 48 54 54 50 2f 31 2e 31 20 32   " 8 . . . . H T T P / 1 . 1   2
000064  30 30 20 4f 4b 0d 0a 78 2d 61 6d 7a 2d 69 64 2d   0 0   O K . . x - a m z - i d -
000080  32 3a 20 34 49 6b 4f 2b 4c 6c 76 41 46 6b 48 45   2 :   4 I k O + L l v A F k H E
000096  36 45 39 32 58 6c 71 41 6c 56 62 77 4a 48 5a 41   6 E 9 2 X l q A l V b w J H Z A
000112  62 6e 72 4c 6d 79 65 4e 79 4e 73 33 6e 69 38 73   b n r L m y e N y N s 3 n i 8 s
000128  55 38 79 61 32 68 32 7a 38 78 57 79 70 78 4b 41   U 8 y a 2 h 2 z 8 x W y p x K A
000144  4e 67 35 0d 0a 78 2d 61 6d 7a 2d 72 65 71 75 65   N g 5 . . x - a m z - r e q u e
000160  73 74 2d 69 64 3a 20 36 44 44 43 45 45 44 44 34   s t - i d :   6 D D C E E D D 4
000176  30 45 38 43 43 38 33 0d 0a 44 61 74 65 3a 20 46   0 E 8 C C 8 3 . . D a t e :   F
000192  72 69 2c 20 31 33 20 41 70 72 20 32 30 31 32 20   r i ,   1 3   A p r   2 0 1 2
000208  31 37 3a 32 37 3a 31 39 20 47 4d 54 0d 0a 4c 61   1 7 : 2 7 : 1 9   G M T . . L a
000224  73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 57 65 64   s t - M o d i f i e d :   W e d
000240  2c 20 32 31 20 53 65 70 20 32 30 31 31 20 31 39   ,   2 1   S e p   2 0 1 1   1 9
000256  3a 30 32 3a 33 35 20 47 4d 54 0d 0a 45 54 61 67   : 0 2 : 3 5   G M T . . E T a g
000272  3a 20 22 38 65 36 33 37 61 39 32 38 39 39 32 30   :   " 8 e 6 3 7 a 9 2 8 9 9 2 0
000288  65 39 62 30 30 38 36 39 61 36 61 66 35 31 33 31   e 9 b 0 0 8 6 9 a 6 a f 5 1 3 1
000304  30 66 34 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e   0 f 4 " . . A c c e p t - R a n
000320  67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74   g e s :   b y t e s . . C o n t
000336  65 6e 74 2d                20 69 6d 61 67 65 2f   e n t - T y p e :   i m a g e /
000352  70 6e 67 0d                65 6e 74 2d 4c 65 6e   p n g . . C o n t e n t - L e n
000368  67 74 68 3a                37 0d 0a 53 65 72 76   g t h :   8 4 9 6 7 . . S e r v
000384  65 72 3a 20 41 6d 6a 7a 6f 6e 53 33 0d 0a 0d 0a   e r :   A m a z o n S 3 . . . .
000400  89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52   . P N G . . . . . . . . I H D R
000416  00 00 03 85 00 00 00 cb 08 03 00 00 00 ee b4 c6   . . . . . . . Ë . . . . . î ´ Æ
000432  13 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72   . . . . . t E X t S o f t w a r
000448  65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61   e . A d o b e   I m a g e R e a
000464  64 79 71 c9 65 3c 00 00 03 22 69 54 58 74 58 4d   d y q É e < . . . " i T X t X M
000480  4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00   L : c o m . a d o b e . x m p .
000496  00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65   . . . . < ? x p a c k e t   b e
000512  67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35   g i n = " ï » ¿ "   i d = " W 5

8 of 100000 events
```

EVENT META

SESSIONID	886
TIME	2018/02/21 19:05:40
SIZE	180858
PAYLOAD	171330
MEDIUM	1
ETH.SRC	[redacted]
ETH.DST	[redacted]
ETH.TYPE	2048
IP.SRC	[redacted]
NETNAME	private src
IP.DST	[redacted].200
NETNAME	other dst
DIRECTION	outbound
IP.PROTO	6
TCP.FLAGS	30
TCP.SRCPORT	1041
TCP.DSTPORT	80
SERVICE	80
STREAMS	2
PACKETS	176
LIFETIME	0
RPACKETS	64
RPAYLOAD	85665
ACTION	get
DIRECTORY	/images/
FILENAME	home_banner.png
EXTENSION	png
REFERER	http://tinychat.com/

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.

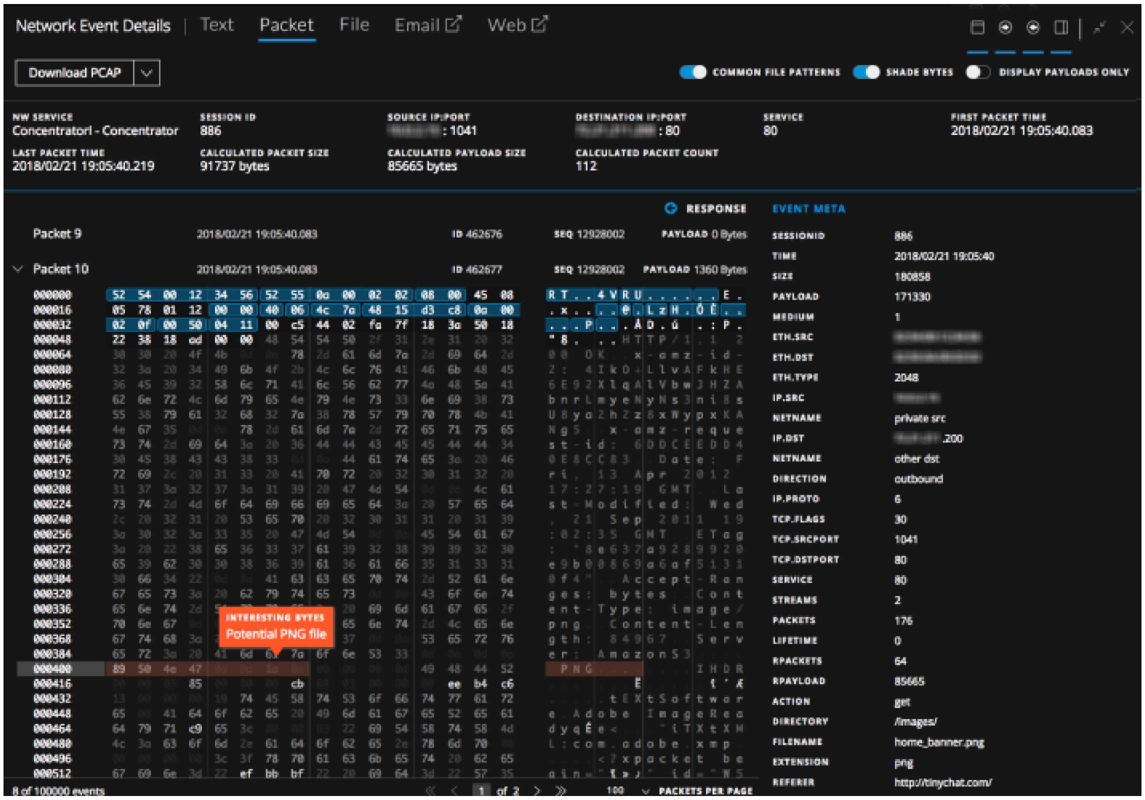


```
0 -   6%
1 -  13%
2 -  19%
3 -  25%
4 -  31%
5 -  38%
6 -  44%
7 -  50%
8 -  56%
9 -  63%
A -  69%
B -  75%
C -  81%
D -  88%
E -  94%
F - 100%
```

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 Panel

In the Packet 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.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
ConcentratorI - Concentrator	886	[redacted] : 1041	[redacted] : 80	80	2018/02/21 19:05:40.083

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
2018/02/21 19:05:40.219	91737 bytes	85665 bytes	112

```
  Packet 9     2018/02/21 19:05:40.083    ID 462676    SEQ 12928002    PAYLOAD 0 Bytes

∨ Packet 10    2018/02/21 19:05:40.083    ID 462677    SEQ 12928002    PAYLOAD 1360 Bytes

000000  52 54 00 12 34 56 52 55 0a 00 02 02 08 00 45 00   R T . . 4 V R U . . . . . . E .
000016  05 78 01 12 00 00 40 06 4c 7a 48 15 d3 c8 0a 00   . x . . . . @ . L z H . Ó È . .
000032  02 0f 00 50 04 11 00 c5 44 02 fa 7f 18 3a 50 18   . . . P . . . Å D . ú . . : P .
000048  22 38 18 ad 00 00 48 54 54 50 2f 31 2e 31 20 32   " 8 . . . . H T T P / 1 . 1   2
000064  30 30 20 4f 4b 0d 0a 78 2d 61 6d 7a 2d 69 64 2d   0 0   O K . . x - a m z - i d -
000080  32 3a 20 34 49 6b 4f 2b 4c 6c 76 41 46 6b 48 45   2 :   4 I k O + L l v A F k H E
000096  36 45 39 32 58 6c 71 41 6c 56 62 77 4a 48 5a 41   6 E 9 2 X l q A l V b w J H Z A
000112  62 6e 72 4c 6d 79 65 4e 79 4e 73 33 6e 69 38 73   b n r L m y e N y N s 3 n i 8 s
000128  55 38 79 61 32 68 32 7a 38 78 57 79 70 78 4b 41   U 8 y a 2 h 2 z 8 x W y p x K A
000144  4e 67 35 0d 0a 78 2d 61 6d 7a 2d 72 65 71 75 65   N g 5 . . x - a m z - r e q u e
000160  73 74 2d 69 64 3a 20 36 44 44 43 45 45 44 44 34   s t - i d :   6 D D C E E D D 4
000176  30 45 38 43 43 38 33 0d 0a 44 61 74 65 3a 20 46   0 E 8 C C 8 3 . . D a t e :   F
000192  72 69 2c 20 31 33 20 41 70 72 20 32 30 31 32 20   r i ,   1 3   A p r   2 0 1 2
000208  31 37 3a 32 37 3a 31 39 20 47 4d 54 0d 0a 4c 61   1 7 : 2 7 : 1 9   G M T . . L a
000224  73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 57 65 64   s t - M o d i f i e d :   W e d
000240  2c 20 32 31 20 53 65 70 20 32 30 31 31 20 31 39   ,   2 1   S e p   2 0 1 1   1 9
000256  3a 30 32 3a 33 35 20 47 4d 54 0d 0a 45 54 61 67   : 0 2 : 3 5   G M T . . E T a g
000272  3a 20 22 38 65 36 33 37 61 39 32 38 39 39 32 30   :   " 8 e 6 3 7 a 9 2 8 9 9 2 0
000288  65 39 62 30 30 38 36 39 61 36 61 66 35 31 33 31   e 9 b 0 0 8 6 9 a 6 a f 5 1 3 1
000304  30 66 34 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e   0 f 4 " . . A c c e p t - R a n
000320  67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74   g e s :   b y t e s . . C o n t
000336  65 6e 74 2d                20 69 6d 61 67 65 2f   e n t - T y p e :   i m a g e /
000352  70 6e 67 0d                65 6e 74 2d 4c 65 6e   p n g . . C o n t e n t - L e n
000368  67 74 68 3a                37 0d 0a 53 65 72 76   g t h :   8 4 9 6 7 . . S e r v
000384  65 72 3a 20 41 6d 61 7a 6f 6e 53 33 0d 0a 0d 0a   e r :   A m a z o n S 3 . . . .
000400  89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52   . P N G . . . . . . . . I H D R
000416  00 00 03 85 00 00 00 cb 08 03 00 00 00 ee b4 c6   . . . . . . . Ë . . . . . î ´ Æ
000432  13 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72   . . . . . t E X t S o f t w a r
000448  65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61   e . A d o b e   I m a g e R e a
000464  64 79 71 c9 65 3c 00 00 03 22 69 54 58 74 58 4d   d y q É e < . . . " i T X t X M
000480  4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00   L : c o m . a d o b e . x m p .
000496  00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65   . . . . < ? x p a c k e t   b e
000512  67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35   g i n = " ï » ¿ "   i d = " W 5

8 of 100000 events                  «  ‹  1 of 2  ›  »        100 ∨ PACKETS PER PAGE
```

EVENT META	
SESSIONID	886
TIME	2018/02/21 19:05:40
SIZE	180858
PAYLOAD	171330
MEDIUM	1
ETH.SRC	[redacted]
ETH.DST	[redacted]
ETH.TYPE	2048
IP.SRC	[redacted]
NETNAME	private src
IP.DST	[redacted].200
NETNAME	other dst
DIRECTION	outbound
IP.PROTO	6
TCP.FLAGS	30
TCP.SRCPORT	1041
TCP.DSTPORT	80
SERVICE	80
STREAMS	2
PACKETS	176
LIFETIME	0
RPACKETS	64
RPAYLOAD	85665
ACTION	get
DIRECTORY	/images/
FILENAME	home_banner.png
EXTENSION	png
REFERER	http://tinychat.com/

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
GIF	47 49 46 38 37 61	GIF87a

File Type	Hexadecimal Signature	ASCII Encoding
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	ĐÏ.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.

Reconstruct an Event in the Legacy Events View

When viewing a list of events in Legacy 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.

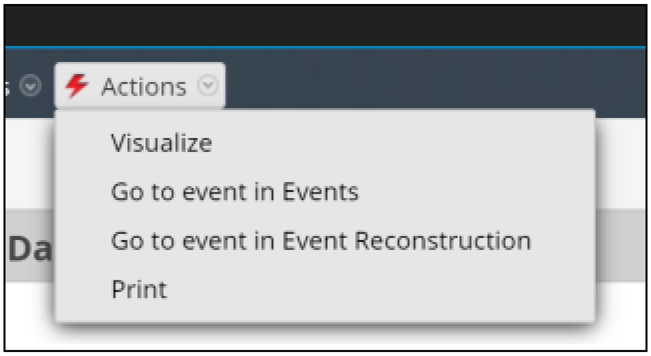
> **Note:** Reconstruction Settings and Reconstruction Cache Settings allow an administrator to manage application performance for Investigation. As analysts reconstruct sessions that they are investigating, two situations can affect performance and results.
> -Some events can be very large and contain 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 Using an Event ID

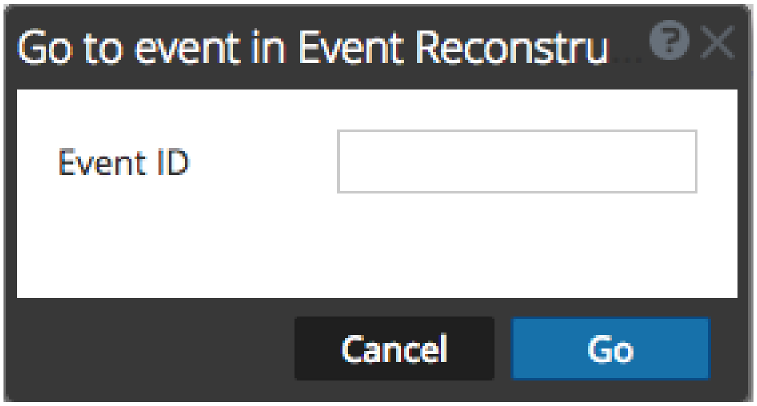
You can reconstruct an event directly from the Navigate view given a known Event ID. You can use this option without executing a query as you usually do when beginning an investigation. A service and time range must be selected to be able to jump directly to an event using just its `eventid`.

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

1. Go to **Investigate > Navigate** and select **Actions > Go to event in Events** or **Go to event in Event Reconstruction**.

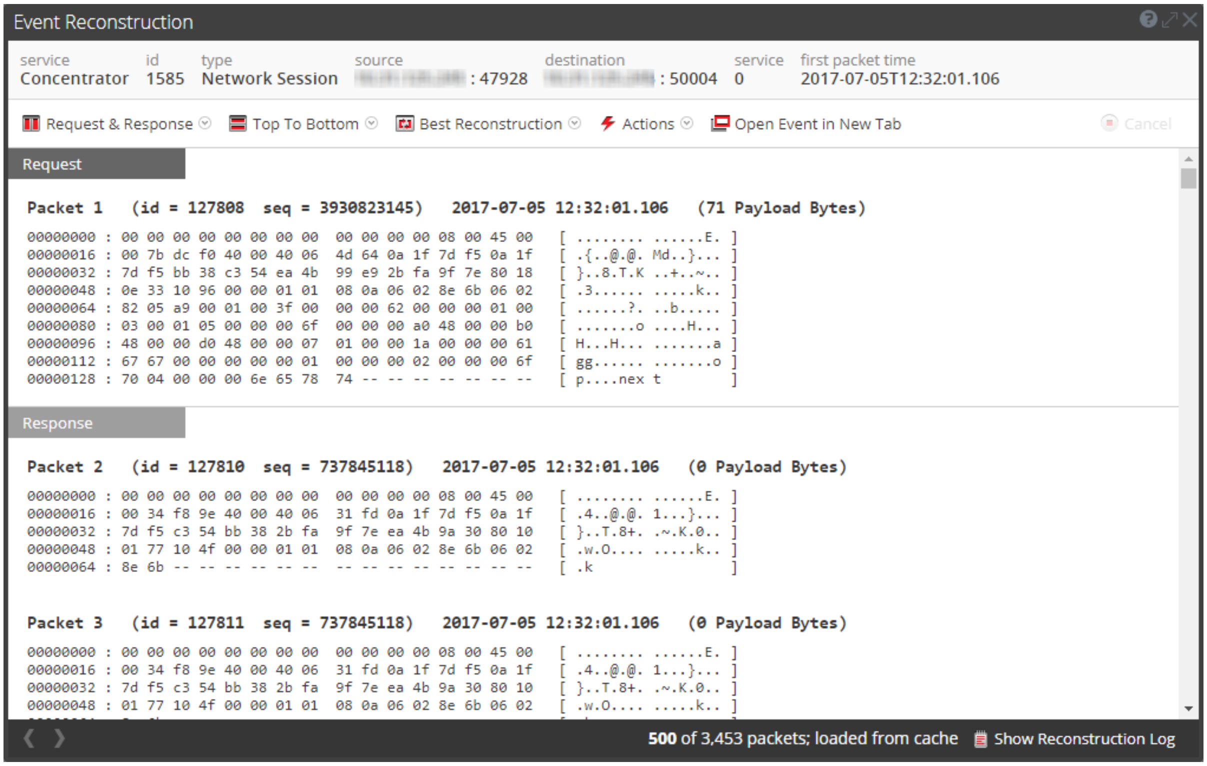
   The Go to event dialog is displayed. There are two dialogs, one for Events and one for Legacy Event reconstruction. Both ask for the Event ID.

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

Reconstruct an Event from a Drill Point in the Navigate View

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 Legacy 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.



Event Reconstruction

service Concentrator | id 1585 | type Network Session | source [redacted] : 47928 | destination [redacted] : 50004 | service 0 | first packet time 2017-07-05T12:32:01.106

Request

```
Packet 1   (id = 127808  seq = 3930823145)   2017-07-05 12:32:01.106   (71 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 7b dc f0 40 00 40 06  4d 64 0a 1f 7d f5 0a 1f   [ .{..@.@. Md..}... ]
00000032 : 7d f5 bb 38 c3 54 ea 4b  99 e9 2b fa 9f 7e 80 18   [ }..8.T.K ..+..~.. ]
00000048 : 0e 33 10 96 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .3...... .....k.. ]
00000064 : 82 05 a9 00 01 00 3f 00  00 00 62 00 00 00 01 00   [ ......?. ..b..... ]
00000080 : 03 00 01 05 00 00 00 6f  00 00 00 a0 48 00 00 b0   [ .......o ....H... ]
00000096 : 48 00 00 d0 48 00 00 07  01 00 00 1a 00 00 00 61   [ H...H... .......a ]
00000112 : 67 67 00 00 00 00 00 01  00 00 00 02 00 00 00 6f   [ gg...... .......o ]
00000128 : 70 04 00 00 00 6e 65 78  74 -- -- -- -- -- -- --   [ p....nex t        ]
```

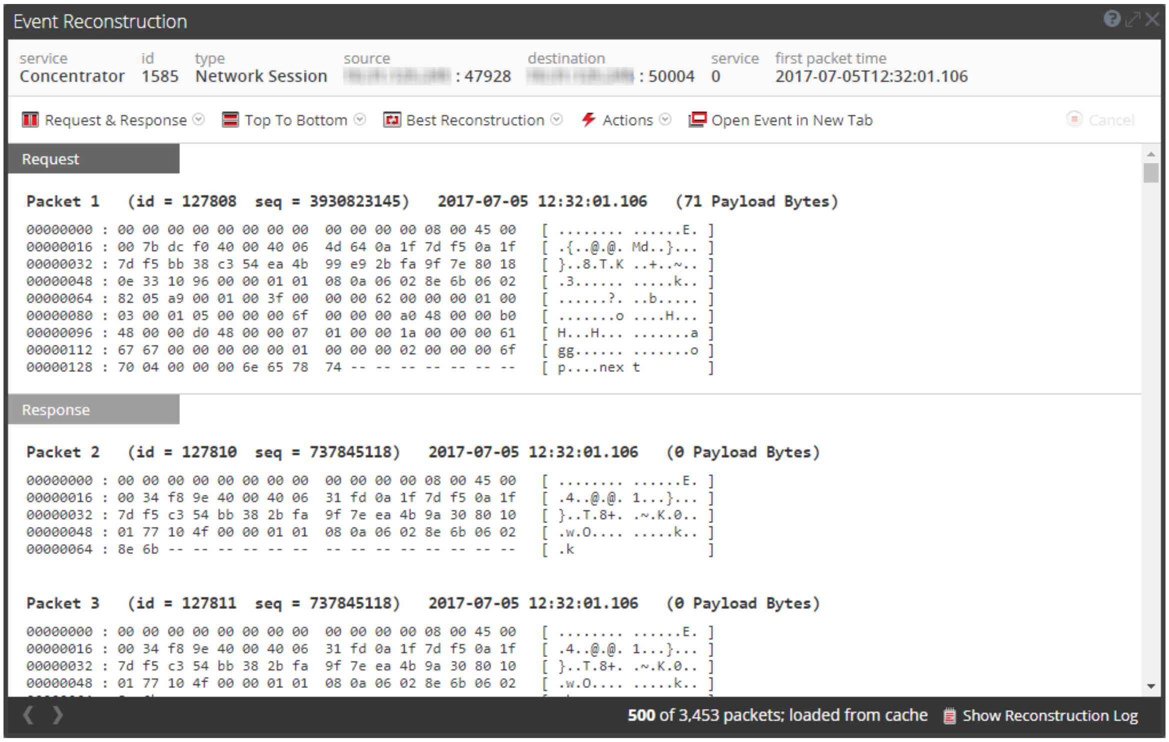
Response

```
Packet 2   (id = 127810  seq = 737845118)   2017-07-05 12:32:01.106   (0 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 34 f8 9e 40 00 40 06  31 fd 0a 1f 7d f5 0a 1f   [ .4..@.@. 1...}... ]
00000032 : 7d f5 c3 54 bb 38 2b fa  9f 7e ea 4b 9a 30 80 10   [ }..T.8+. .~.K.0.. ]
00000048 : 01 77 10 4f 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .w.O.... .....k.. ]
00000064 : 8e 6b -- -- -- -- -- --  -- -- -- -- -- -- -- --   [ .k                ]


Packet 3   (id = 127811  seq = 737845118)   2017-07-05 12:32:01.106   (0 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 34 f8 9e 40 00 40 06  31 fd 0a 1f 7d f5 0a 1f   [ .4..@.@. 1...}... ]
00000032 : 7d f5 c3 54 bb 38 2b fa  9f 7e ea 4b 9a 30 80 10   [ }..T.8+. .~.K.0.. ]
00000048 : 01 77 10 4f 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .w.O.... .....k.. ]
```

500 of 3,453 packets; loaded from cache

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 **Legacy 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.



service	id	type	source	destination	service	first packet time
Concentrator	1585	Network Session	[redacted] : 47928	[redacted] : 50004	0	2017-07-05T12:32:01.106

```
Packet 1   (id = 127808   seq = 3930823145)   2017-07-05 12:32:01.106   (71 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 7b dc f0 40 00 40 06  4d 64 0a 1f 7d f5 0a 1f   [ .{..@.@. Md..}... ]
00000032 : 7d f5 bb 38 c3 54 ea 4b  99 e9 2b fa 9f 7e 80 18   [ }..8.T.K ..+..~.. ]
00000048 : 0e 33 10 96 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .3...... .....k.. ]
00000064 : 82 05 a9 00 01 00 3f 00  00 00 62 00 00 00 01 00   [ ......?. ..b..... ]
00000080 : 03 00 01 05 00 00 00 6f  00 00 00 a0 48 00 00 b0   [ .......o ....H... ]
00000096 : 48 00 00 d0 48 00 00 07  01 00 00 1a 00 00 00 61   [ H...H... .......a ]
00000112 : 67 67 00 00 00 00 00 01  00 00 00 02 00 00 00 6f   [ gg...... .......o ]
00000128 : 70 04 00 00 00 6e 65 78  74 -- -- -- -- -- -- --   [ p....nex t        ]
```

```
Packet 2   (id = 127810   seq = 737845118)   2017-07-05 12:32:01.106   (0 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 34 f8 9e 40 00 40 06  31 fd 0a 1f 7d f5 0a 1f   [ .4..@.@. 1...}... ]
00000032 : 7d f5 c3 54 bb 38 2b fa  9f 7e ea 4b 9a 30 80 10   [ }..T.8+. .~.K.0.. ]
00000048 : 01 77 10 4f 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .w.O.... .....k.. ]
00000064 : 8e 6b -- -- -- -- -- --  -- -- -- -- -- -- -- --   [ .k                ]


Packet 3   (id = 127811   seq = 737845118)   2017-07-05 12:32:01.106   (0 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 34 f8 9e 40 00 40 06  31 fd 0a 1f 7d f5 0a 1f   [ .4..@.@. 1...}... ]
00000032 : 7d f5 c3 54 bb 38 2b fa  9f 7e ea 4b 9a 30 80 10   [ }..T.8+. .~.K.0.. ]
00000048 : 01 77 10 4f 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .w.O.... .....k.. ]
```

500 of 3,453 packets; loaded from cache

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.

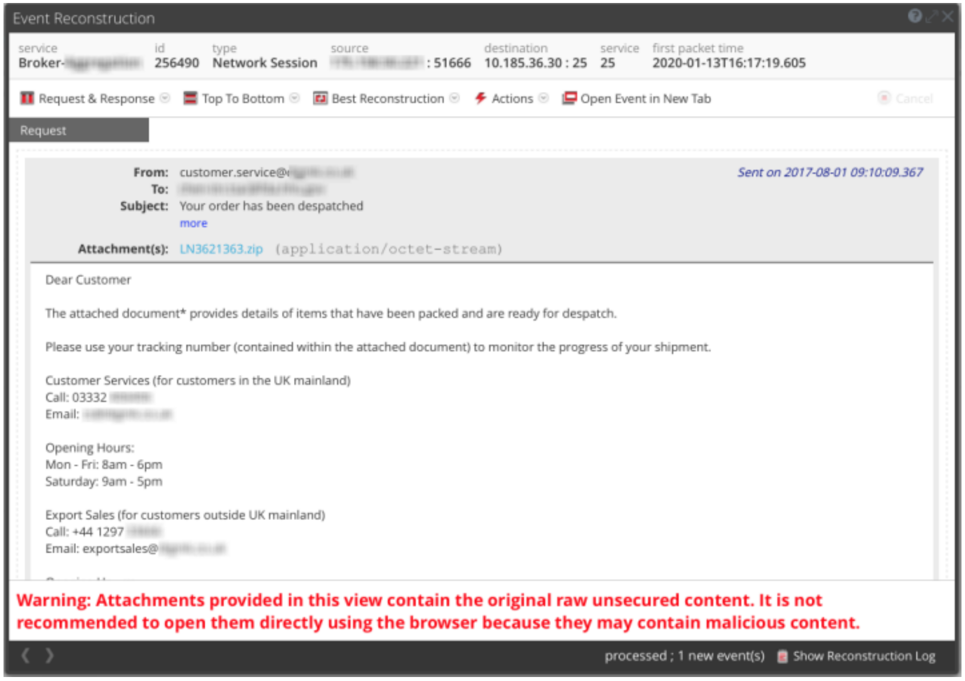
Open or Download an Email Attachment

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.



service	id	type	source	destination	service	first packet time
Broker-[redacted]	256490	Network Session	[redacted] : 51666	10.185.36.30 : 25	25	2020-01-13T16:17:19.605

From: customer.service@[redacted]
To: [redacted]
Subject: Your order has been despatched

Sent on 2017-08-01 09:10:09.367

Attachment(s): LN3621363.zip (application/octet-stream)

Dear Customer

The attached document* provides details of items that have been packed and are ready for despatch.

Please use your tracking number (contained within the attached document) to monitor the progress of your shipment.

Customer Services (for customers in the UK mainland)
Call: 03332 [redacted]
Email: [redacted]

Opening Hours:
Mon - Fri: 8am - 6pm
Saturday: 9am - 5pm

Export Sales (for customers outside UK mainland)
Call: +44 1297 [redacted]
Email: exportsales@[redacted]

Warning: Attachments provided in this view contain the original raw unsecured content. It is not recommended to open them directly using the browser because they may contain malicious content.

processed ; 1 new event(s)

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.

Look Up Additional Context for Results

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.

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*.

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, Events view, and Legacy 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. 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 a file hash. The data from configured sources, such as RSA NetWitness Endpoint, can help you understand what is happening.

In addition, you can add lists and list values for Context Hub enrichment; 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.

Note: In Version 11.2 and earlier, you can look up additional context in the Navigate view or the Legacy Events view, but not the Event Analysis view.

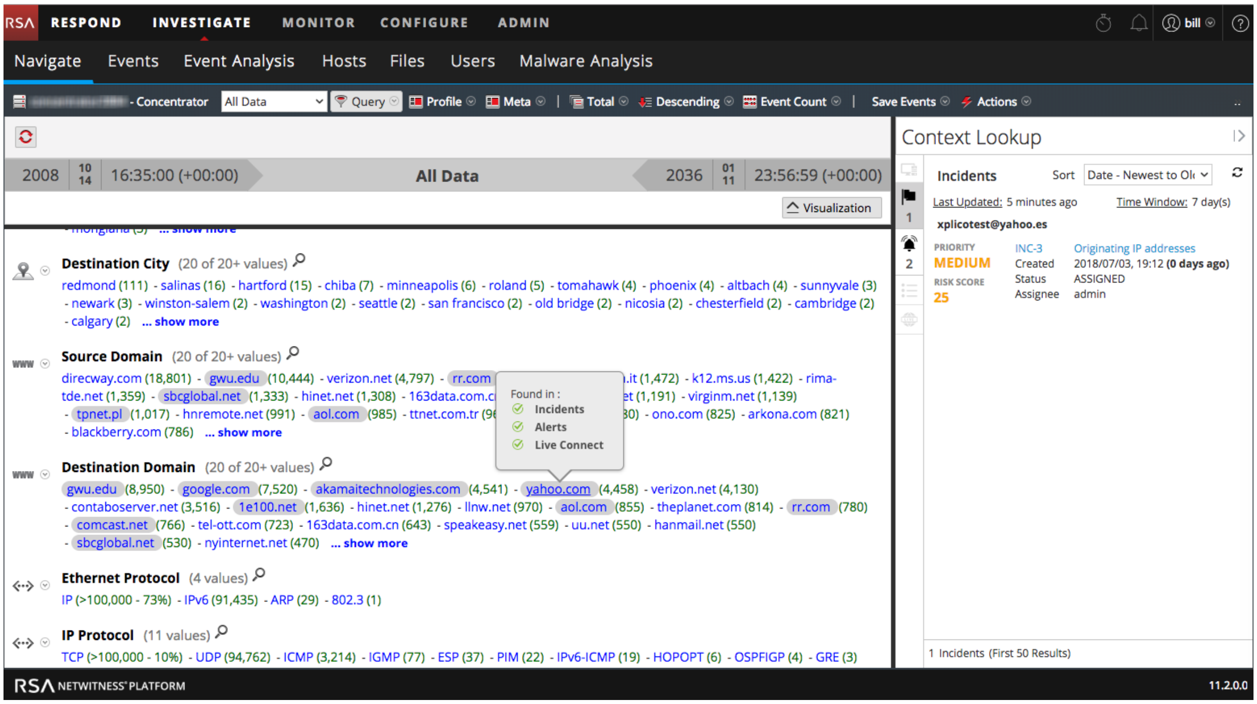
For an analyst to manage lists in Investigate, the administrator must:

- 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*.

Open the Context Lookup Panel

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.

In the Navigate view and Legacy 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.



2008 10 14 16:35:00 (+00:00) All Data 2036 01 11 23:56:59 (+00:00)

Destination City (20 of 20+ values)
redmond (111) - salinas (16) - hartford (15) - chiba (7) - minneapolis (6) - roland (5) - tomahawk (4) - phoenix (4) - altbach (4) - sunnyvale (3) - newark (3) - winston-salem (2) - washington (2) - seattle (2) - san francisco (2) - old bridge (2) - nicosia (2) - chesterfield (2) - cambridge (2) - calgary (2) ... show more

Source Domain (20 of 20+ values)
direcway.com (18,801) - gwu.edu (10,444) - verizon.net (4,797) - rr.com .it (1,472) - k12.ms.us (1,422) - rima-tde.net (1,359) - sbcglobal.net (1,333) - hinet.net (1,308) - 163data.com.c et (1,191) - virginm.net (1,139) - tpnet.pl (1,017) - hnremote.net (991) - aol.com (985) - ttnet.com.tr (9 30) - ono.com (825) - arkona.com (821) - blackberry.com (786) ... show more

Found in :
✓ Incidents
✓ Alerts
✓ Live Connect

Destination Domain (20 of 20+ values)
gwu.edu (8,950) - google.com (7,520) - akamaitechnologies.com (4,541) - yahoo.com (4,458) - verizon.net (4,130) - contaboserver.net (3,516) - 1e100.net (1,636) - hinet.net (1,276) - llnw.net (970) - aol.com (855) - theplanet.com (814) - rr.com (780) - comcast.net (766) - tel-ott.com (723) - 163data.com.cn (643) - speakeasy.net (559) - uu.net (550) - hanmail.net (550) - sbcglobal.net (530) - nyinternet.net (470) ... show more

Ethernet Protocol (4 values)
IP (>100,000 - 73%) - IPv6 (91,435) - ARP (29) - 802.3 (1)

IP Protocol (11 values)
TCP (>100,000 - 10%) - UDP (94,762) - ICMP (3,214) - IGMP (77) - ESP (37) - PIM (22) - IPv6-ICMP (19) - HOPOPT (6) - OSPFIGP (4) - GRE (3)

Context Lookup

Incidents Sort Date - Newest to Ol

Last Updated: 5 minutes ago Time Window: 7 day(s)

xplicotest@yahoo.es

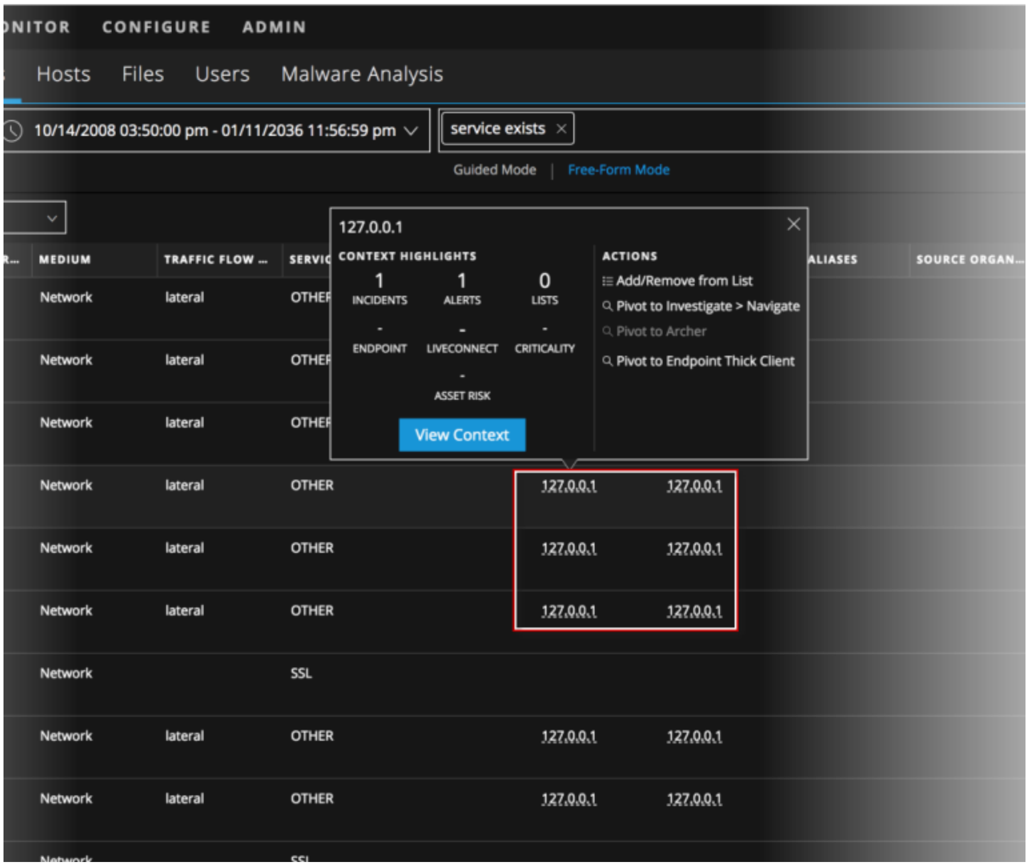
PRIORITY MEDIUM INC-3 Originating IP addresses
Created 2018/07/03, 19:12 **(0 days ago)**
RISK SCORE 25 Status ASSIGNED
Assignee admin

1 Incidents (First 50 Results)

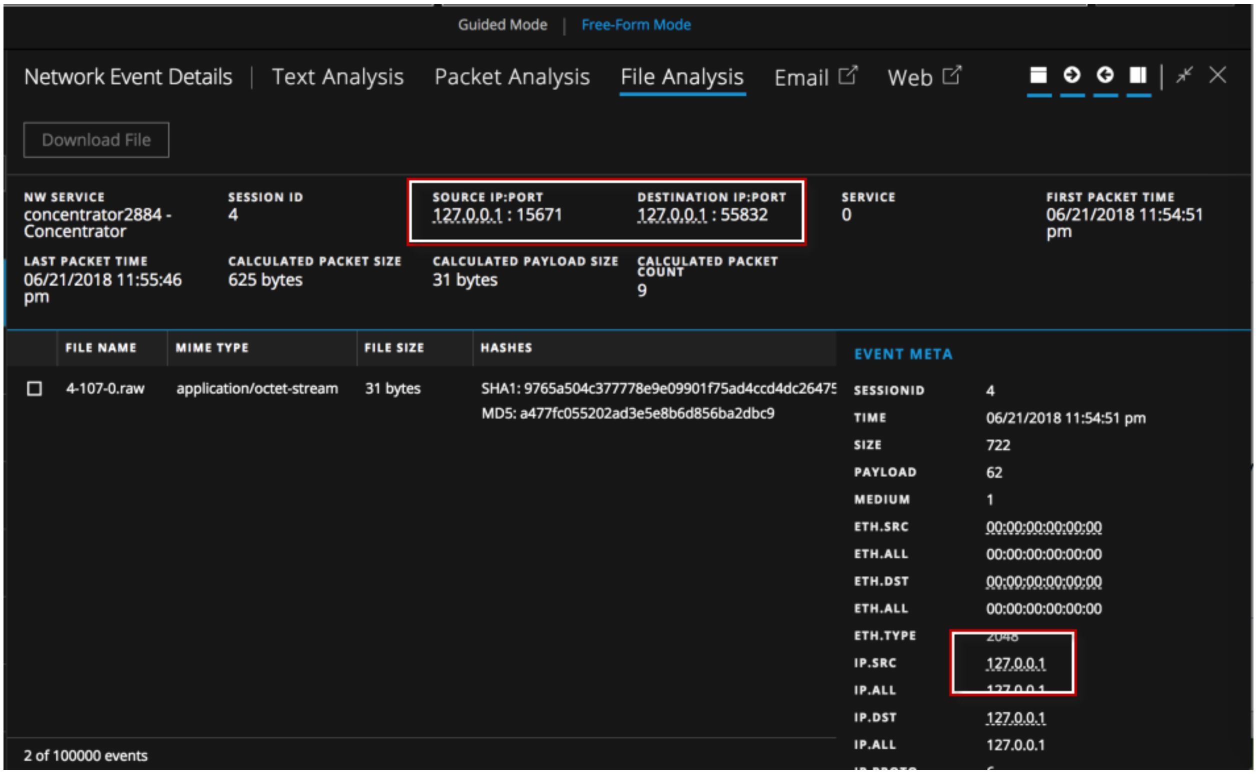
In the Events view, you can see underlined entities in the Events panel, the Event Header, or the Event Meta panel. If an entity is underlined, NetWitness Platform is populating information about that entity type in the Context Hub. There may be additional information available about that entity in the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


Guided Mode | Free-Form Mode
Network Event Details | Text Analysis Packet Analysis File Analysis Email Web
Download File
FILE NAME
MIME TYPE
FILE SIZE
HASHES
EVENT META
2 of 100000 events

NW SERVICE: concentrator2884 - Concentrator
SESSION ID: 4
SOURCE IP:PORT: 127.0.0.1 : 15671
DESTINATION IP:PORT: 127.0.0.1 : 55832
SERVICE: 0
FIRST PACKET TIME: 06/21/2018 11:54:51 pm
LAST PACKET TIME: 06/21/2018 11:55:46 pm
CALCULATED PACKET SIZE: 625 bytes
CALCULATED PAYLOAD SIZE: 31 bytes
CALCULATED PACKET COUNT: 9

FILE NAME	MIME TYPE	FILE SIZE	HASHES
□ 4-107-0.raw	application/octet-stream	31 bytes	SHA1: 9765a504c377778e9e09901f75ad4ccd4dc2647! MD5: a477fc055202ad3e5e8b6d856ba2dbc9

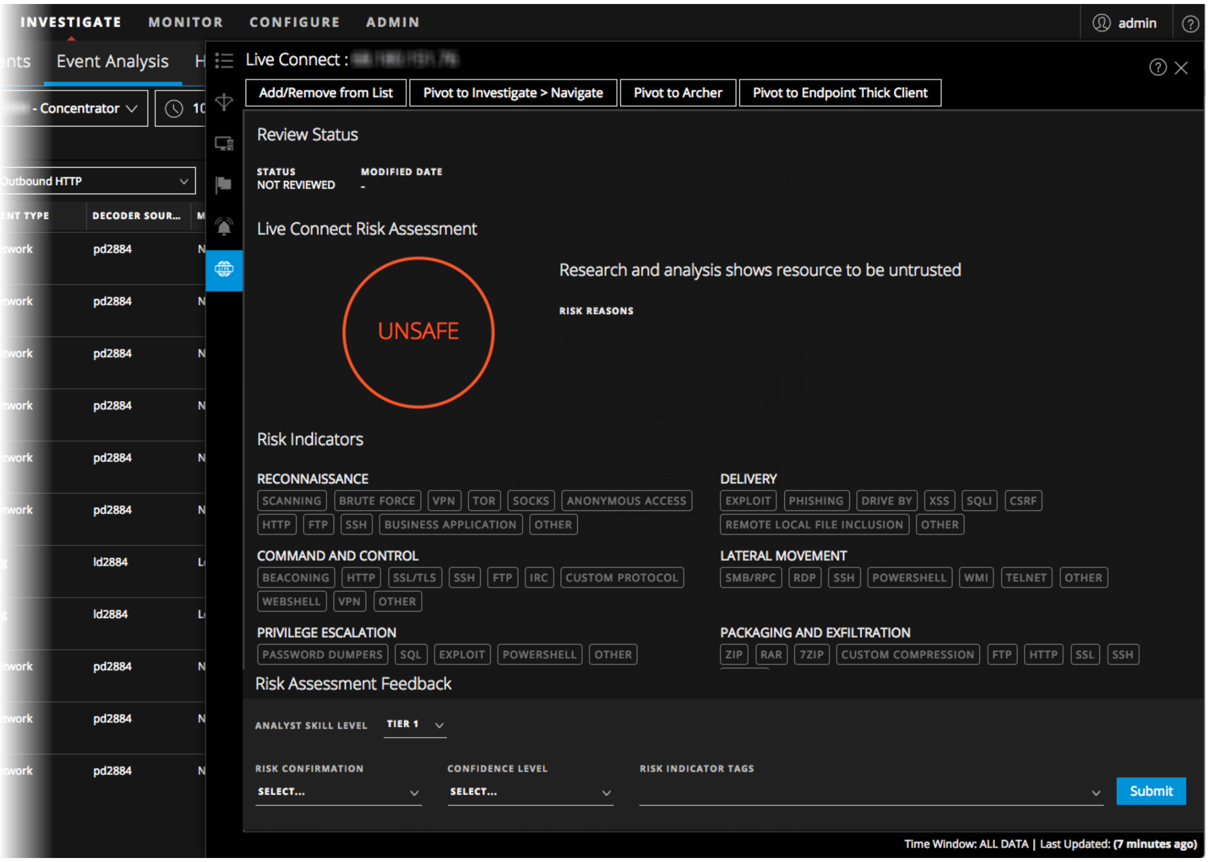
EVENT META	
SESSIONID	4
TIME	06/21/2018 11:54:51 pm
SIZE	722
PAYLOAD	62
MEDIUM	1
ETH.SRC	00:00:00:00:00:00
ETH.ALL	00:00:00:00:00:00
ETH.DST	00:00:00:00:00:00
ETH.ALL	00:00:00:00:00:00
ETH.TYPE	2048
IP.SRC	127.0.0.1
IP.ALL	127.0.0.1
IP.DST	127.0.0.1
IP.ALL	127.0.0.1

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.

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

To view information in the Context Lookup panel in the Events 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.



Live Connect : [redacted]

STATUS: NOT REVIEWED

MODIFIED DATE: -

Research and analysis shows resource to be untrusted

ANALYST SKILL LEVEL: TIER 1

RISK CONFIRMATION: SELECT...

CONFIDENCE LEVEL: SELECT...

RISK INDICATOR TAGS

Time Window: ALL DATA | Last Updated: **(7 minutes ago)**

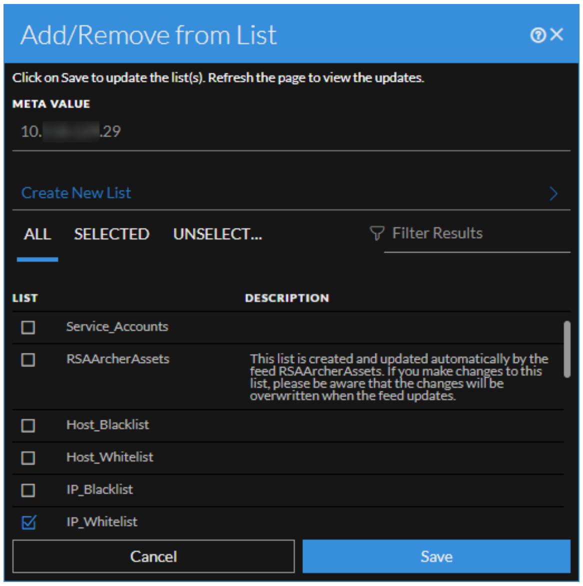
3. To perform actions on an entity, select one of the available actions in the context tooltip: Add /Remove from List, Pivot to Investigate > Navigate, Pivot to Archer, Pivot to Endpoint Thick Client. For more information, see Pivot to Investigate > Navigate (Events View), Pivot to Archer (Events View),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



Add/Remove from List

Click on Save to update the list(s). Refresh the page to view the updates.

META VALUE

10.[redacted].29

Create New List

ALL SELECTED UNSELECT... Filter Results

LIST		DESCRIPTION
□	Service_Accounts	
□	RSAArcherAssets	This list is created and updated automatically by the feed RSAArcherAssets. If you make changes to this list, please be aware that the changes will be overwritten when the feed updates.
□	Host_Blacklist	
□	Host_Whitelist	
□	IP_Blacklist	
☑	IP_Whitelist	

3. Select one or more lists and click **Save**.
   The entity is added to the selected lists.

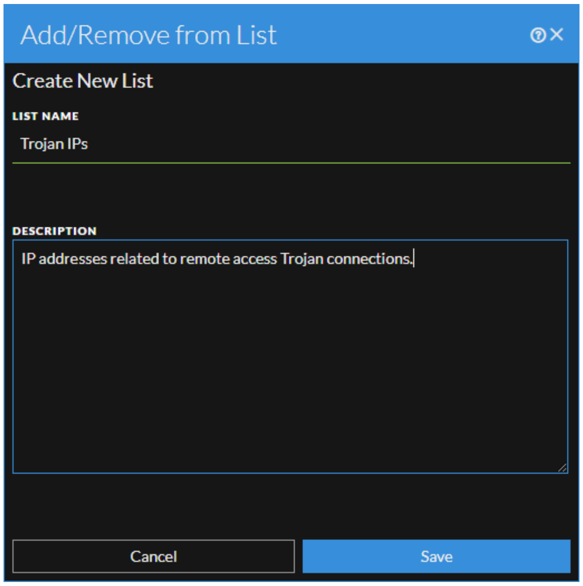
Create a List (Events View)

You can create lists in Context Hub from the Events 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 the 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**.



LIST NAME: Trojan IPs

DESCRIPTION: IP addresses related to remote access Trojan connections.

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 (Events View)

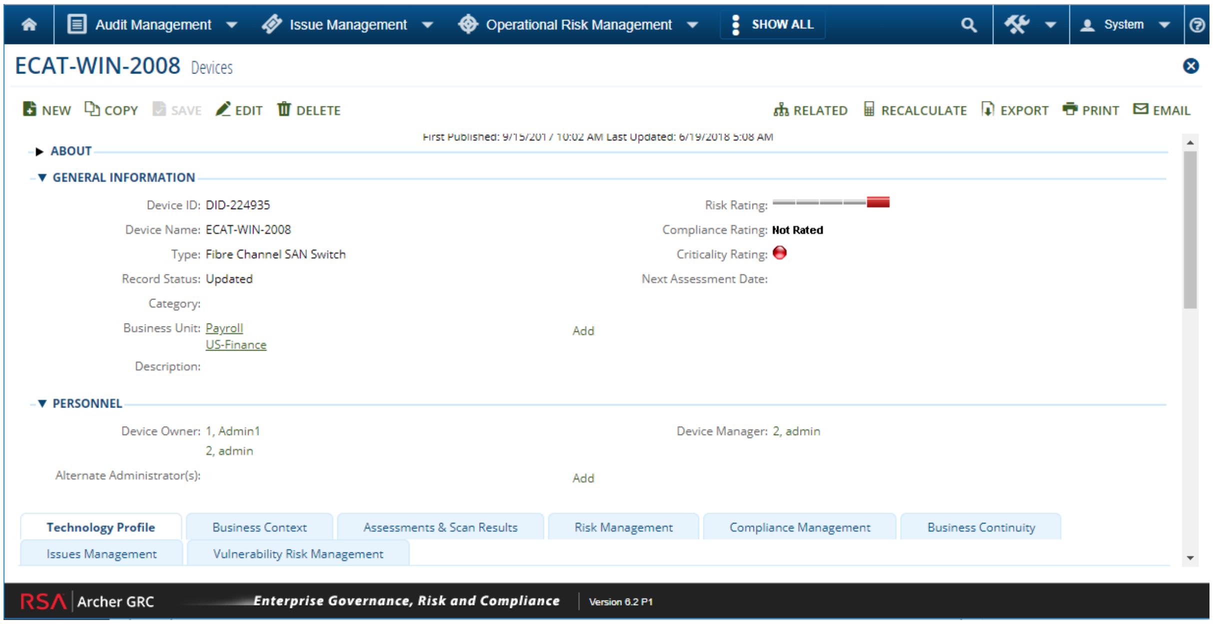
For a more thorough investigation of an entity, you can open the the Navigate view.

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 Refining the Results Set.

Pivot to Archer (Events View)

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.



ECAT-WIN-2008 Devices

First Published: 9/15/2017 10:02 AM Last Updated: 6/19/2018 5:08 AM

GENERAL INFORMATION

Device ID: DID-224935

Device Name: ECAT-WIN-2008

Type: Fibre Channel SAN Switch

Record Status: Updated

Category:

Business Unit: Payroll
US-Finance

Description:

Risk Rating:

Compliance Rating: **Not Rated**

Criticality Rating: ●

Next Assessment Date:

PERSONNEL

Device Owner: 1, Admin1
2, admin

Alternate Administrator(s):

Device Manager: 2, admin

> **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 (Events View)

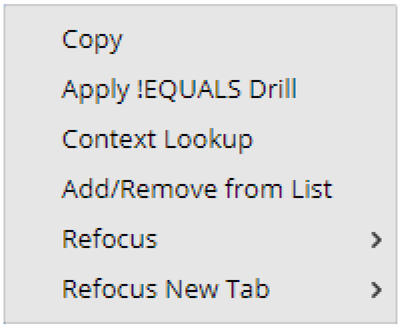
If you have the NetWitness Endpoint thick client application installed, you can launch it through the context tooltip. From there, you can further investigate a suspicious IP address, Host, or MAC address.

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*.

View the Context Lookup Panel in the Navigate View or Legacy 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.

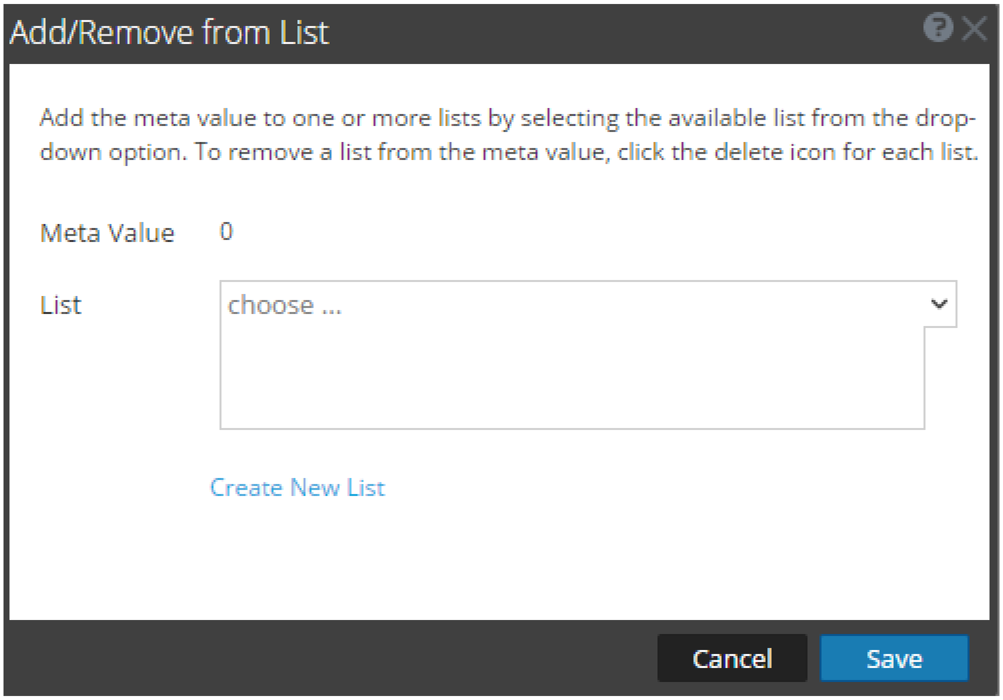
3. To perform actions from the Context Lookup panel, right-click an entity such as IP address. The following options are available: Open Link in New Tab, Query in Investigate, Copy Link, Paste, Google Lookup, Virus Total Lookup, and Query in Endpoint.

4. To close the Context Lookup panel, click ☒ in the panel.

Add Meta Values to an Existing List (Navigate and Legacy Events Views)

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

1. While investigating a service in the **Navigate** view or the **Legacy 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.



Add/Remove from List

Add the meta value to one or more lists by selecting the available list from the drop-down option. To remove a list from the meta value, click the delete icon for each list.

Meta Value 0

List choose ...

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 (Navigate and Legacy Events Views)

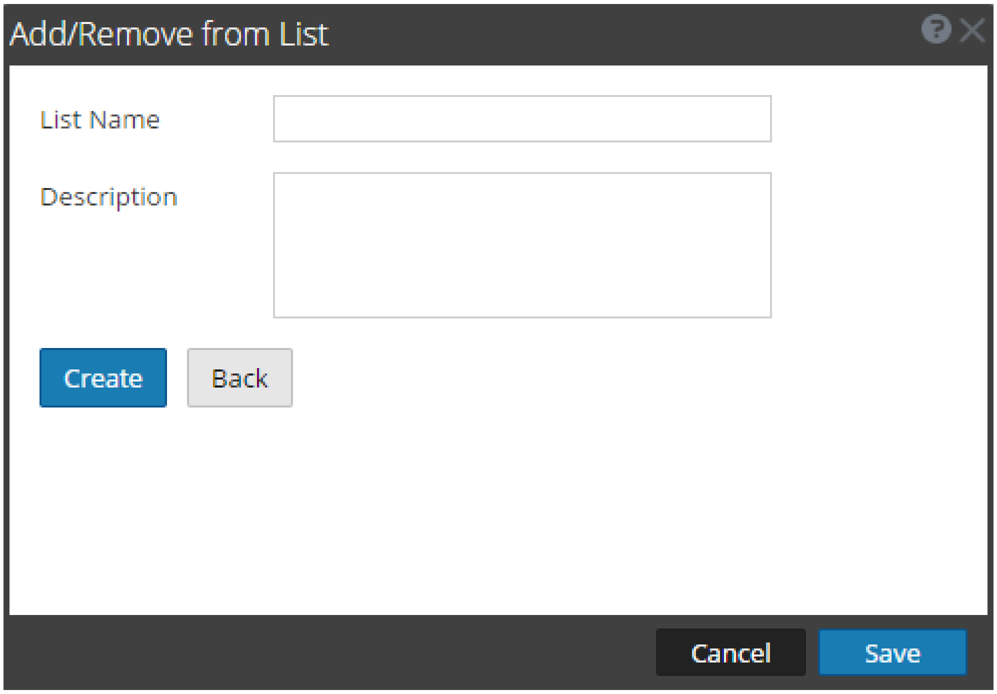
To remove a meta value from list:

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 (Navigate and Legacy Events Views)

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.

Launch a Lookup of a Meta Key

When you have found data of interest in the Navigate view, the Events view, or the Legacy Events 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.

Analysts can use the external lookups to save time during investigations. The external 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
- IPVoidSearch: 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*.

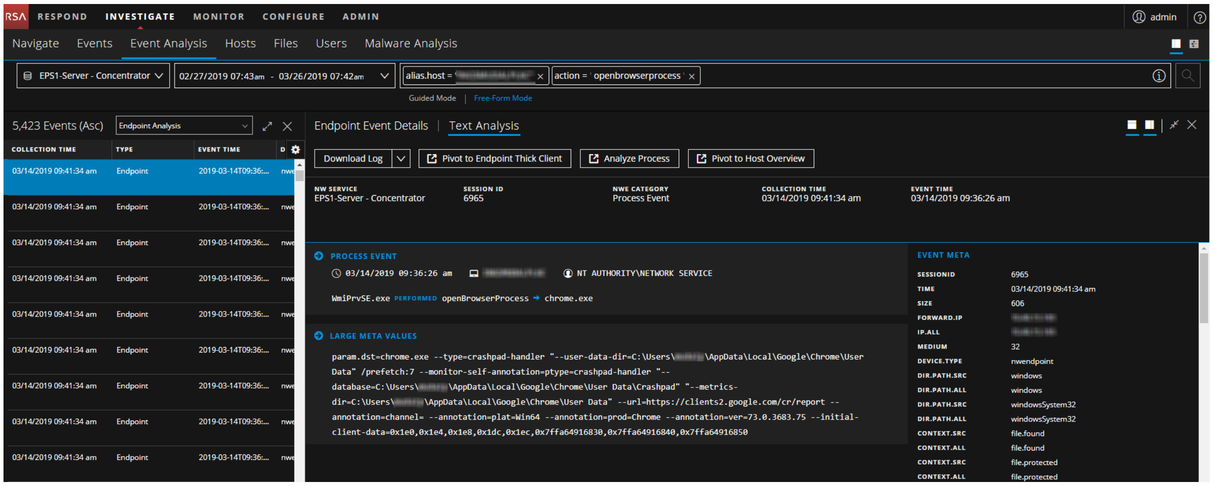
Launch an Endpoint Thick Client Lookup in the Events View

When viewing an endpoint event in the Text 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 **Events** in the menu.
2. (Version 11.1 and later) Go to **INVESTIGATE > Events**. 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 Events view opens with the selected event displayed in the Text view.



EPS1-Server - Concentrator

02/27/2019 07:43am - 03/26/2019 07:42am

alias.host = [redacted] action = ' openbrowserprocess '

5,423 Events (Asc) Endpoint Analysis

COLLECTION TIME	TYPE	EVENT TIME	D
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36:...	nwe

NW SERVICE	SESSION ID	NWE CATEGORY	COLLECTION TIME	EVENT TIME
EPS1-Server - Concentrator	6965	Process Event	03/14/2019 09:41:34 am	03/14/2019 09:36:26 am

```
03/14/2019 09:36:26 am   [redacted]   NT AUTHORITY\NETWORK SERVICE

WmiPrvSE.exe PERFORMED openBrowserProcess → chrome.exe
```

```
param.dst=chrome.exe --type=crashpad-handler "--user-data-dir=C:\Users\[redacted]\AppData\Local\Google\Chrome\User
Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--
database=C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-
dir=C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --
annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=73.0.3683.75 --initial-
client-data=0x1e0,0x1e4,0x1e8,0x1dc,0x1ec,0x7ffa64916830,0x7ffa64916840,0x7ffa64916850
```

SESSIONID	6965
TIME	03/14/2019 09:41:34 am
SIZE	606
FORWARD.IP	[redacted]
IP.ALL	[redacted]
MEDIUM	32
DEVICE.TYPE	nwendpoint
DIR.PATH.SRC	windows
DIR.PATH.ALL	windows
DIR.PATH.SRC	windowsSystem32
DIR.PATH.ALL	windowsSystem32
CONTEXT.SRC	file.found
CONTEXT.ALL	file.found
CONTEXT.SRC	file.protected
CONTEXT.ALL	file.protected

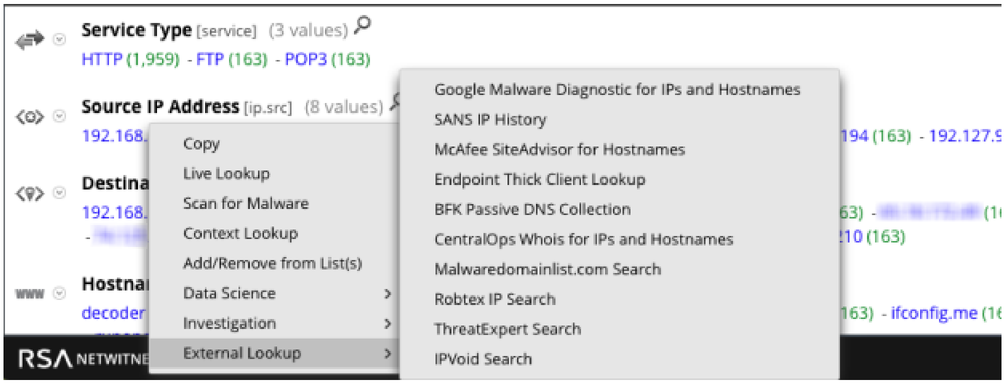
4. In the Event Header click **Pivot to Endpoint.**
   A new browser tab with the url `ecatui://<id>` opens and the NWE Thick Client is launched. If the NetWitness Endpoint Thick Client is not installed, no data is displayed and the following message is displayed: `Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

Launch an Endpoint Thick Client Lookup in the Navigate View

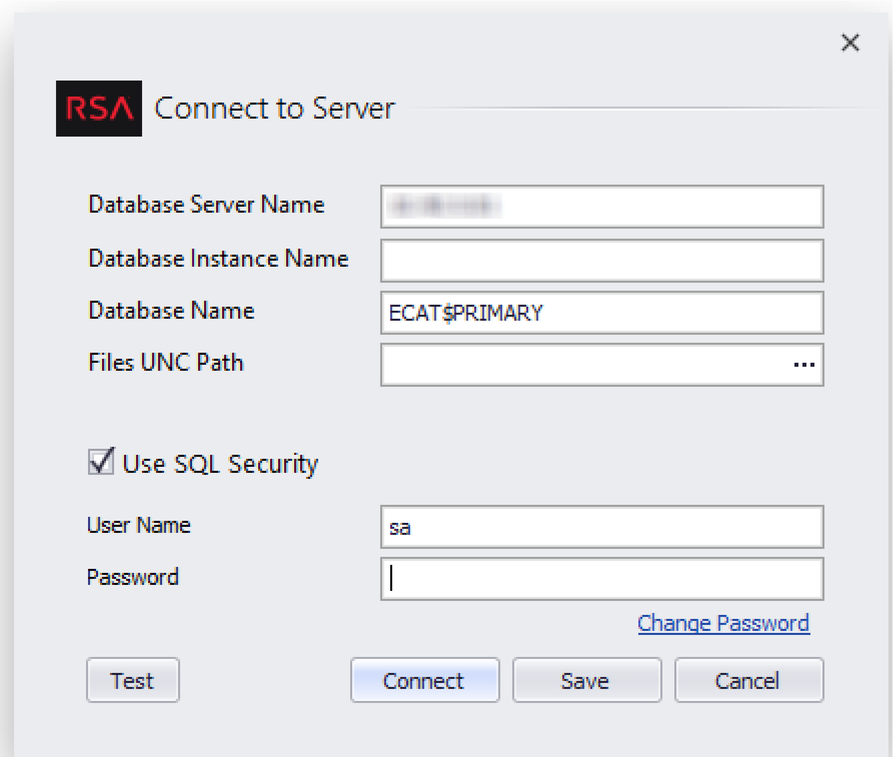
To launch an Endpoint Thick Client lookup of data from the Navigate view:

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.


Service Type [service] (3 values)
HTTP (1,959) - FTP (163) - POP3 (163)
Source IP Address [ip.src] (8 values)
192.168.
194 (163) - 192.127.9
Destina
192.168.
63) -
(1
10 (163)
Hostna
decoder
163) - ifconfig.me (16
RSA NETWITNE
Copy
Live Lookup
Scan for Malware
Context Lookup
Add/Remove from List(s)
Data Science
Investigation
External Lookup
Google Malware Diagnostic for IPs and Hostnames
SANS IP History
McAfee SiteAdvisor for Hostnames
Endpoint Thick Client Lookup
BFK Passive DNS Collection
CentralOps Whois for IPs and Hostnames
Malwaredomainlist.com Search
Robtex IP Search
ThreatExpert Search
IPVoid Search

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



Database Server Name

Database Instance Name

Database Name ECAT$PRIMARY

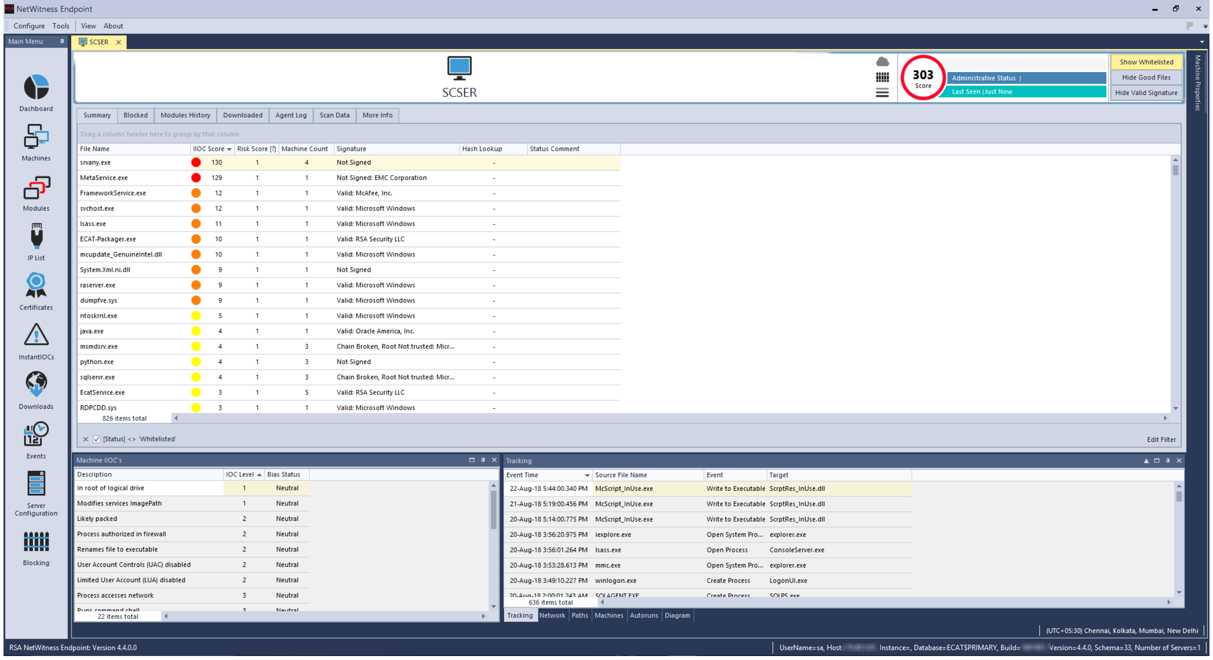
Files UNC Path ...

☑ Use SQL Security

User Name sa

Password

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.



File Name	IIOC Score	Risk Score [?]	Machine Count	Signature	Hash Lookup	Status Comment
srvany.exe	● 130	1	4	Not Signed	-	
MetaService.exe	● 129	1	1	Not Signed: EMC Corporation	-	
FrameworkService.exe	● 12	1	1	Valid: McAfee, Inc.	-	
svchost.exe	● 12	1	1	Valid: Microsoft Windows	-	
lsass.exe	● 11	1	1	Valid: Microsoft Windows	-	
ECAT-Packager.exe	● 10	1	1	Valid: RSA Security LLC	-	
mcupdate_GenuineIntel.dll	● 10	1	1	Valid: Microsoft Windows	-	
System.Xml.ni.dll	● 9	1	1	Not Signed	-	
raserver.exe	● 9	1	1	Valid: Microsoft Windows	-	
dumpfve.sys	● 9	1	1	Valid: Microsoft Windows	-	
ntoskrnl.exe	● 5	1	1	Valid: Microsoft Windows	-	
java.exe	● 4	1	1	Valid: Oracle America, Inc.	-	
msmdsrv.exe	● 4	1	3	Chain Broken, Root Not trusted: Micr...	-	
python.exe	● 4	1	3	Not Signed	-	
sqlservr.exe	● 4	1	3	Chain Broken, Root Not trusted: Micr...	-	
EcatService.exe	● 3	1	5	Valid: RSA Security LLC	-	
RDPCDD.sys	● 3	1	1	Valid: Microsoft Windows	-	

826 items total

× ☑ [Status] <> 'Whitelisted'

Description	IOC Level	Bias Status
In root of logical drive	1	Neutral
Modifies services ImagePath	1	Neutral
Likely packed	2	Neutral
Process authorized in firewall	2	Neutral
Renames file to executable	2	Neutral
User Account Controls (UAC) disabled	2	Neutral
Limited User Account (LUA) disabled	2	Neutral
Process accesses network	3	Neutral
Runs command shell	3	Neutral

22 items total

Event Time	Source File Name	Event	Target
22-Aug-18 5:44:00.340 PM	McScript_InUse.exe	Write to Executable	ScrptRes_InUse.dll
21-Aug-18 5:19:00.456 PM	McScript_InUse.exe	Write to Executable	ScrptRes_InUse.dll
20-Aug-18 5:14:00.775 PM	McScript_InUse.exe	Write to Executable	ScrptRes_InUse.dll
20-Aug-18 3:56:20.975 PM	iexplore.exe	Open System Pro...	explorer.exe
20-Aug-18 3:56:01.264 PM	lsass.exe	Open Process	ConsoleServer.exe
20-Aug-18 3:53:28.613 PM	mmc.exe	Open System Pro...	explorer.exe
20-Aug-18 3:49:10.227 PM	winlogon.exe	Create Process	LogonUI.exe
20-Aug-18 2:00:01.243 AM	SQLAGENT.EXE	Create Process	SQLPS.exe

636 items total

(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

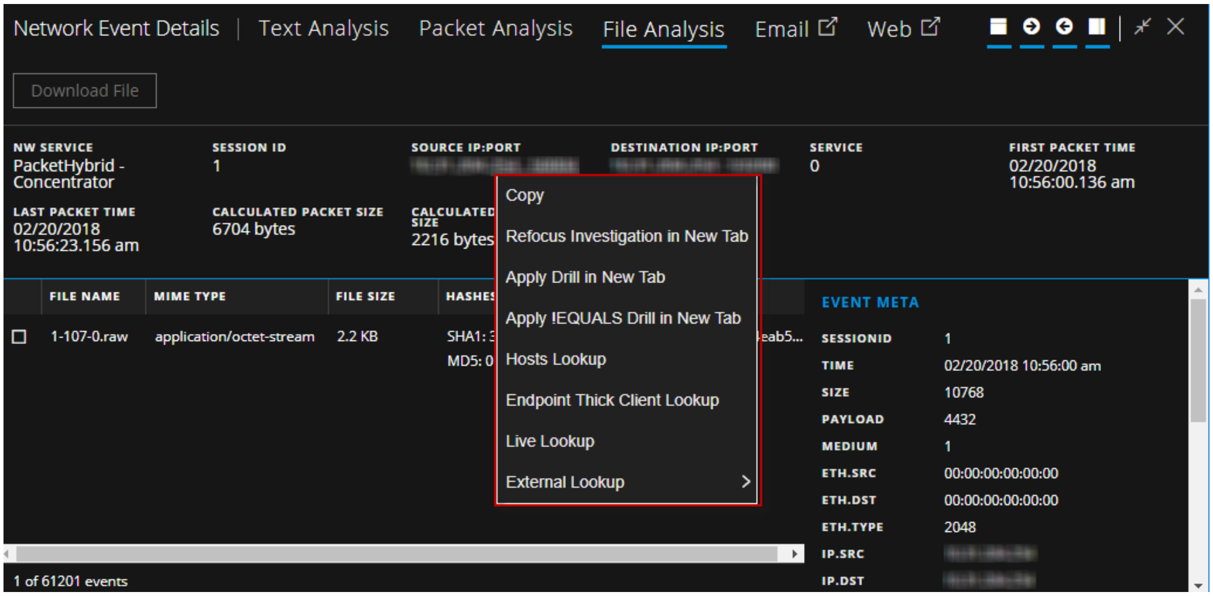
RSA NetWitness Endpoint: Version 4.4.0.0

UserName=sa, Host [redacted] Instance=, Database=ECAT$PRIMARY, Build= [redacted] Version=4.4.0, Schema=33, Number of Servers=1

Perform Lookups of Meta Values in Events

In the Events 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 Events 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.



NW SERVICE: PacketHybrid - Concentrator

SESSION ID: 1

SOURCE IP:PORT: [redacted]

DESTINATION IP:PORT: [redacted]

SERVICE: 0

FIRST PACKET TIME: 02/20/2018 10:56:00.136 am

LAST PACKET TIME: 02/20/2018 10:56:23.156 am

CALCULATED PACKET SIZE: 6704 bytes

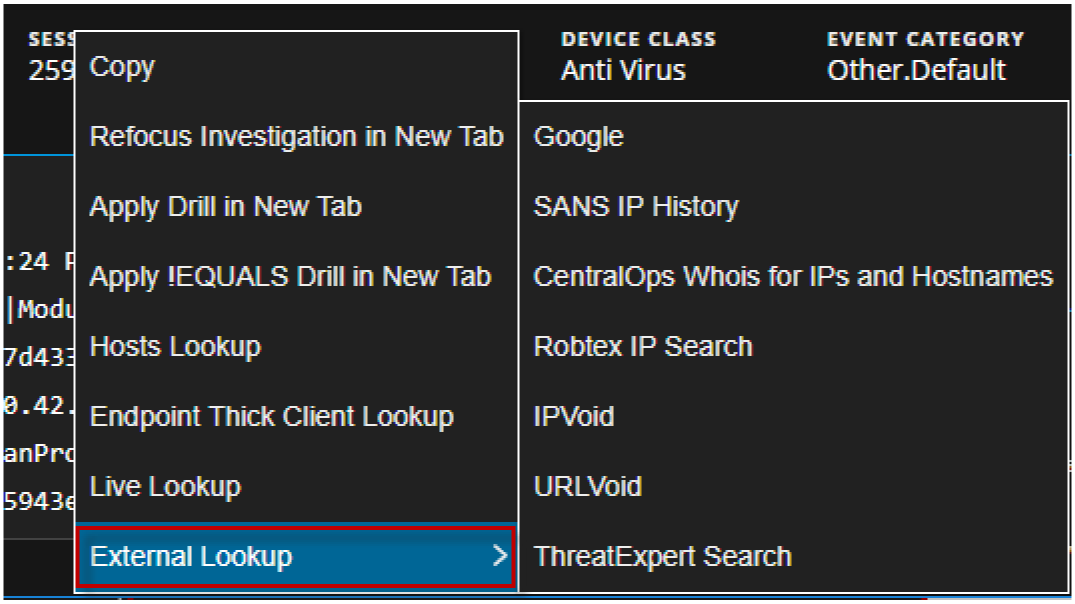
CALCULATED SIZE: 2216 bytes

	FILE NAME	MIME TYPE	FILE SIZE	HASHES
□	1-107-0.raw	application/octet-stream	2.2 KB	SHA1: 3 ...eab5... MD5: 0

SESSIONID	1
TIME	02/20/2018 10:56:00 am
SIZE	10768
PAYLOAD	4432
MEDIUM	1
ETH.SRC	00:00:00:00:00:00
ETH.DST	00:00:00:00:00:00
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]

1 of 61201 events

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**.



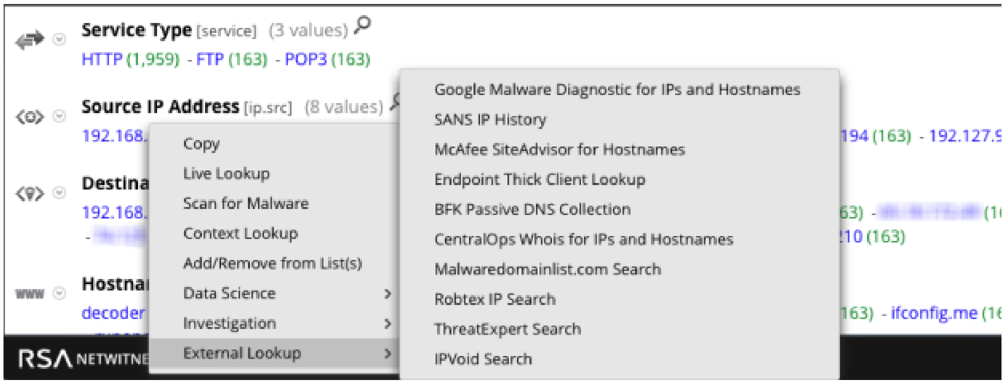
4. In the submenu select one of the available external lookups:
   - **Google**: Looks up a meta value on Google.com
   - **SANS IP History**: Looks up a meta value on SANS IP History, domain = http://isc.sans.org/ipinfo.html?ip=ipaddress
   - **CentralOps Whois for IPs and Hostnames**: Looks up a meta value on CentralOps Whois for IPs and Hostnames, domain = http://centralops.net/co/DomainDossier.aspx?addr=domain&amp;dom_whois=true&amp;dom_dns=true&amp;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

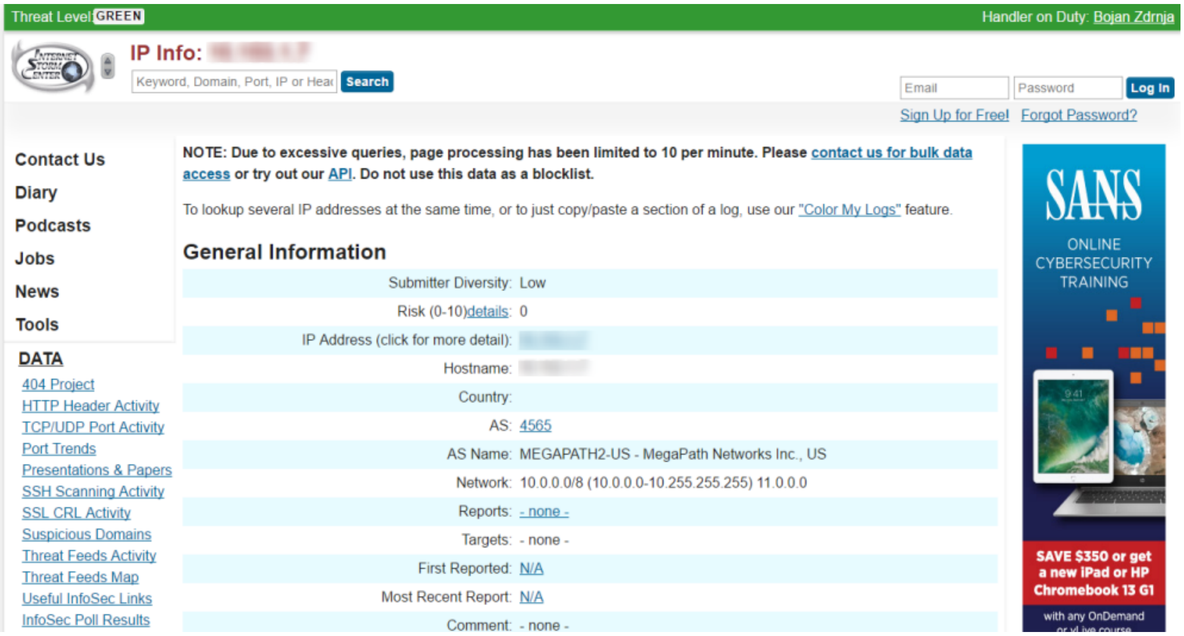
Launch Other External Lookups from the Navigate View

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.


Service Type [service] (3 values)
HTTP (1,959) - FTP (163) - POP3 (163)
Source IP Address [ip.src] (8 values)
192.168.
194 (163) - 192.127.9
Destina
192.168.
63) - [redacted] (1
[redacted]
10 (163)
Hostna
decoder
163) - ifconfig.me (16
RSA NETWITNE
Copy
Live Lookup
Scan for Malware
Context Lookup
Add/Remove from List(s)
Data Science
Investigation
External Lookup
Google Malware Diagnostic for IPs and Hostnames
SANS IP History
McAfee SiteAdvisor for Hostnames
Endpoint Thick Client Lookup
BFK Passive DNS Collection
CentralOps Whois for IPs and Hostnames
Malwaredomainlist.com Search
Robtex IP Search
ThreatExpert Search
IPVoid Search

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.



Threat Level GREEN

Handler on Duty: Bojan Zdrnja

IP Info: [redacted]

Keyword, Domain, Port, IP or Head | Search

Email | Password | Log In

Sign Up for Free! Forgot Password?

Contact Us
Diary
Podcasts
Jobs
News
Tools

DATA
404 Project
HTTP Header Activity
TCP/UDP Port Activity
Port Trends
Presentations & Papers
SSH Scanning Activity
SSL CRL Activity
Suspicious Domains
Threat Feeds Activity
Threat Feeds Map
Useful InfoSec Links
InfoSec Poll Results

NOTE: Due to excessive queries, page processing has been limited to 10 per minute. Please contact us for bulk data access or try out our API. Do not use this data as a blocklist.

To lookup several IP addresses at the same time, or to just copy/paste a section of a log, use our "Color My Logs" feature.

General Information

Submitter Diversity:	Low
Risk (0-10)details:	0
IP Address (click for more detail):	[redacted]
Hostname:	[redacted]
Country:	
AS:	4565
AS Name:	MEGAPATH2-US - MegaPath Networks Inc., US
Network:	10.0.0.0/8 (10.0.0.0-10.255.255.255) 11.0.0.0
Reports:	- none -
Targets:	- none -
First Reported:	N/A
Most Recent Report:	N/A
Comment:	- none -

SANS
ONLINE CYBERSECURITY TRAINING
SAVE $350 or get a new iPad or HP Chromebook 13 G1
with any OnDemand or vLive course

Launch a Malware Analysis Scan from the Navigate View

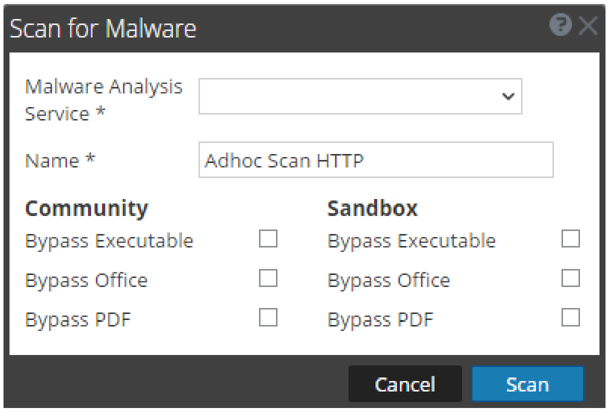
From within Investigate, analysts can launch an on-demand Malware Analysis scan by selecting a service and meta value, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis.

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.



Malware Analysis Service *

Name * Adhoc Scan HTTP

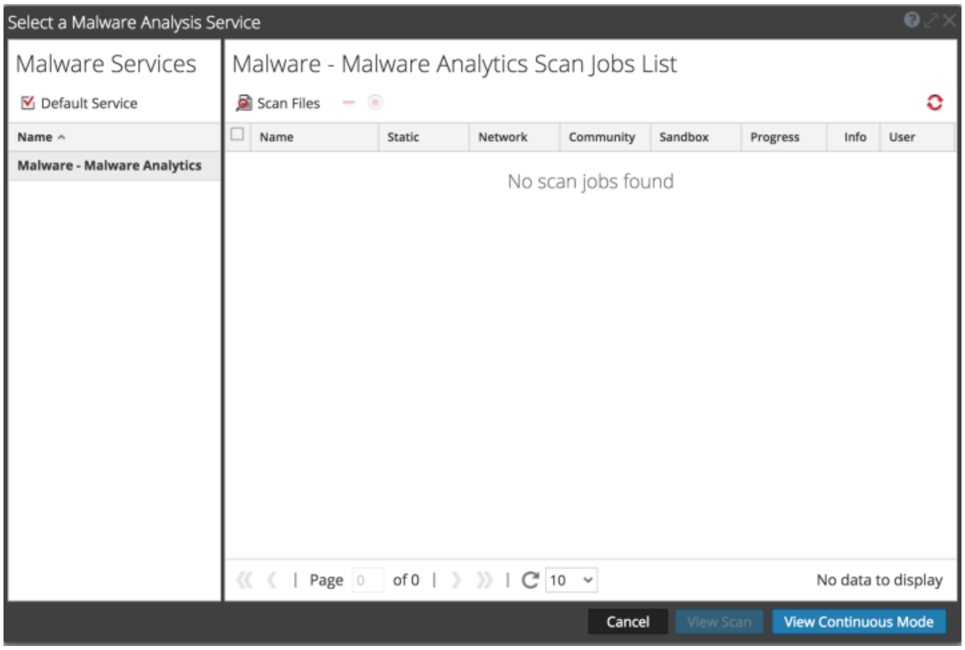
Community		**Sandbox**	
Bypass Executable	□	Bypass Executable	□
Bypass Office	□	Bypass Office	□
Bypass PDF	□	Bypass PDF	□

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.



Malware Services

☑ Default Service

Name
Malware - Malware Analytics

Malware - Malware Analytics Scan Jobs List

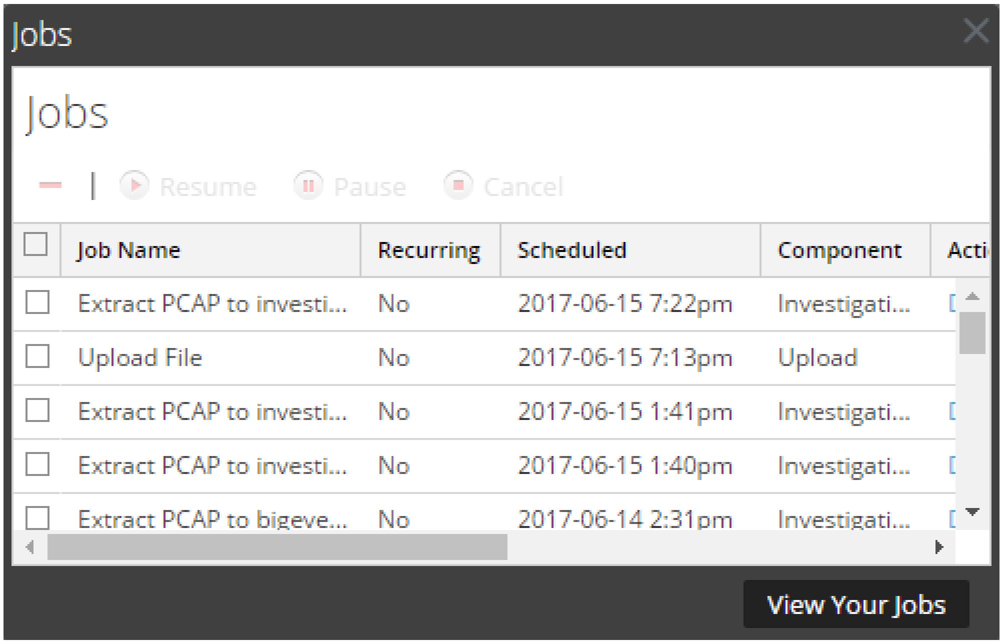
Scan Files

□	Name	Static	Network	Community	Sandbox	Progress	Info	User

No scan jobs found

Page 0 of 0 | 10 — No data to display

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**.



Jobs

□	Job Name	Recurring	Scheduled	Component	Acti
□	Extract PCAP to investi...	No	2017-06-15 7:22pm	Investigati...	[
□	Upload File	No	2017-06-15 7:13pm	Upload	
□	Extract PCAP to investi...	No	2017-06-15 1:41pm	Investigati...	[
□	Extract PCAP to investi...	No	2017-06-15 1:40pm	Investigati...	[
□	Extract PCAP to bigeve...	No	2017-06-14 2:31pm	Investigati...	[

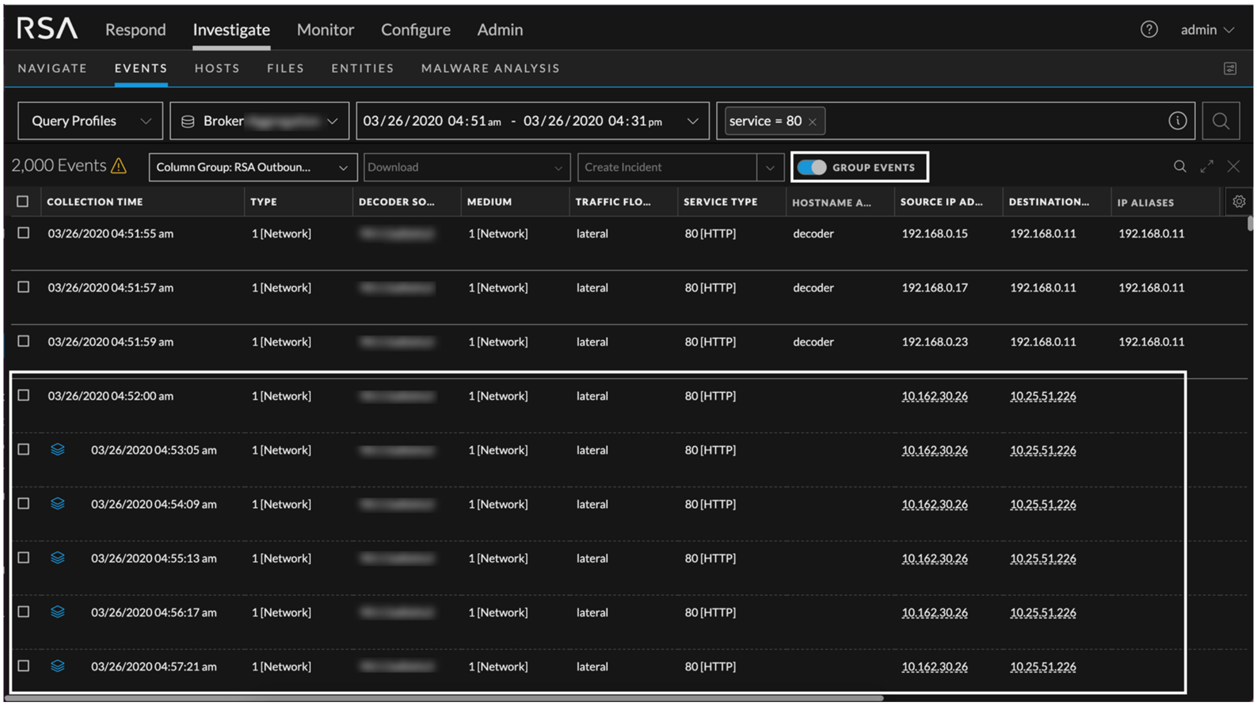
The Malware Summary of Events for the selected scan is displayed. The scan is also added to the list of available scans in the dialog for selecting scans in the Investigation > Malware tab.

Group Events from Split and Related Sessions in the Events and Legacy Events Views

In the Events view listing of events, events from split and related sessions are listed in the order they were parsed; for this reason, they are not always listed together in the Events list. In Version 11.4.1 and later, the Group Events option allows you to change the order in which the events are listed so that you can more easily detect relationships in the captured data. When events are grouped, we refer to the first event as the leading event.

The user interface is designed to help you identify grouped events. Solid row lines delineate different groups of related events while dotted lines depict the events that are part of the same related group. In a group of events, the leading event is first and subsequent events are nested under the leading event with indentation and relationship icons for subsequent events. The numbers next to the relationship icon distinguish the session split count.

If the leading event is not included in the current data set, the subsequent events are still grouped together under the first subsequent event. Only the leading event or the first subsequent event, in the case of no leading event, is sorted; indented events are not sorted. Hovering over the subsequent event marker (◈) displays a tool tip explaining the relationship. The following figure is an example of related events as they are displayed in the Events list.



Broker [redacted]

03/26/2020 04:51 am - 03/26/2020 04:31 pm

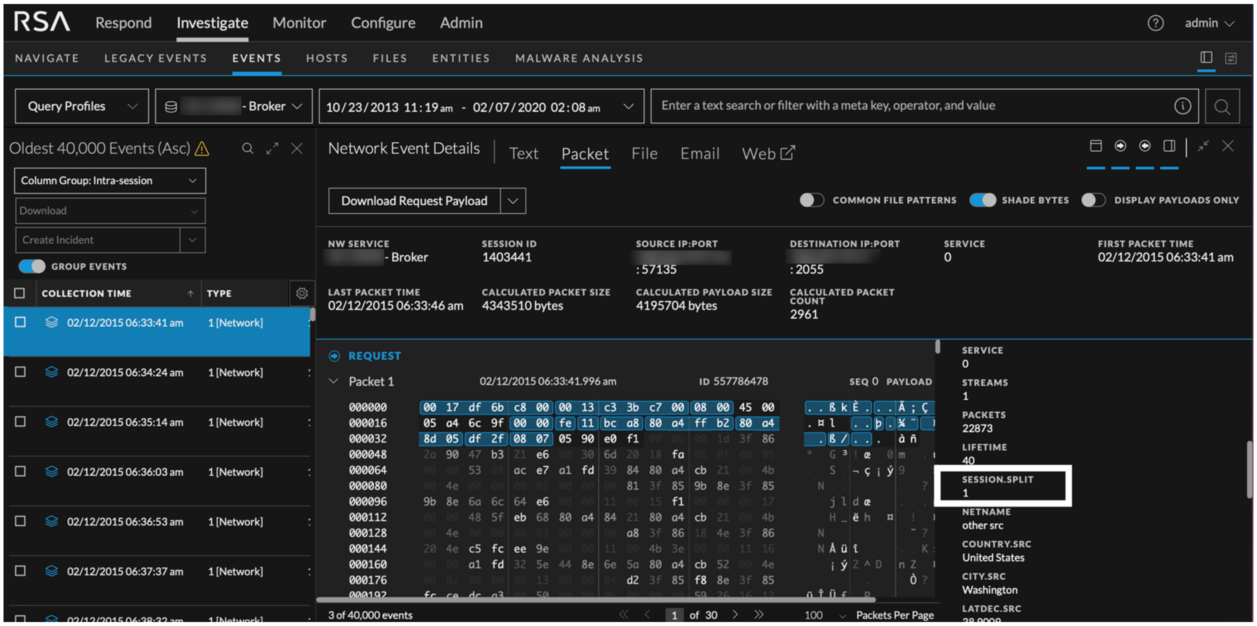
service = 80

2,000 Events ⚠

Column Group: RSA Outboun...

□	COLLECTION TIME	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP AD...	DESTINATION...	IP ALIASES
□	03/26/2020 04:51:55 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.15	192.168.0.11	192.168.0.11
□	03/26/2020 04:51:57 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.17	192.168.0.11	192.168.0.11
□	03/26/2020 04:51:59 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.23	192.168.0.11	192.168.0.11
□	03/26/2020 04:52:00 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	◈ 03/26/2020 04:53:05 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	◈ 03/26/2020 04:54:09 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	◈ 03/26/2020 04:55:13 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	◈ 03/26/2020 04:56:17 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	◈ 03/26/2020 04:57:21 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	

If events are related based on session fragments, when you select a subsequent event and open the reconstruction, you can see the `session.split` meta key in the Event Meta panel.



[redacted] - Broker

10/23/2013 11:19 am - 02/07/2020 02:08 am

Oldest 40,000 Events (Asc) ⚠

□	COLLECTION TIME	TYPE
□	02/12/2015 06:33:41 am	1 [Network]
□	02/12/2015 06:34:24 am	1 [Network]
□	02/12/2015 06:35:14 am	1 [Network]
□	02/12/2015 06:36:03 am	1 [Network]
□	02/12/2015 06:36:53 am	1 [Network]
□	02/12/2015 06:37:37 am	1 [Network]
□	02/12/2015 06:38:32 am	1 [Network]

NW SERVICE: [redacted] - Broker
SESSION ID: 1403441
SOURCE IP:PORT: [redacted] :57135
DESTINATION IP:PORT: [redacted] :2055
SERVICE: 0
FIRST PACKET TIME: 02/12/2015 06:33:41 am
LAST PACKET TIME: 02/12/2015 06:33:46 am
CALCULATED PACKET SIZE: 4343510 bytes
CALCULATED PAYLOAD SIZE: 4195704 bytes
CALCULATED PACKET COUNT: 2961

Packet 1 02/12/2015 06:33:41.996 am ID 557786478 SEQ 0 PAYLOAD

```
000000  00 17 df 6b c8 00 00 13 c3 3b c7 00 08 00 45 00
000016  05 a4 6c 9f 00 00 fe 11 bc a8 80 a4 ff b2 80 a4
000032  8d 05 df 2f 08 07 05 90 e0 f1 00 05 00 1d 3f 86
000048  2a 90 47 b3 21 e6 00 30 6d 20 18 fa 05 0f 00 05
000064  00 00 53 08 ac e7 a1 fd 39 84 80 a4 cb 21 00 4b
000080  00 4e 00 00 00 01 00 00 00 81 3f 85 9b 8e 3f 85
000096  9b 8e 6a 6c 64 e6 00 00 11 00 15 f1 00 00 0b 17
000112  00 00 48 5f eb 68 80 a4 84 21 80 a4 cb 21 00 4b
000128  00 4e 00 00 00 03 00 00 00 a8 3f 86 18 4e 3f 86
000144  20 4e c5 fc ee 9e 00 00 11 00 4b 3e 00 00 11 16
000160  00 00 a1 fd 32 5e 44 8e 6e 5a 80 a4 cb 52 00 4e
000176  00 02 00 00 00 13 00 00 04 d2 3f 85 f8 8e 3f 85
```

3 of 40,000 events   1 of 30   100 Packets Per Page

SERVICE: 0
STREAMS: 1
PACKETS: 22873
LIFETIME: 40
SESSION.SPLIT: 1
NETNAME: other src
COUNTRY.SRC: United States
CITY.SRC: Washington
LATDEC.SRC: 38.9008

Split Network Session

If you see a tool tip like this, the listed events are part of a split network session:
`The event is part of a split session (session.split: #) matching these parameters: ip.src=127.0.0.1 AND ip.dst=127.0.0.1 AND tcp.srcport=25 AND tcp.dstport=1234.`

The reason for the split is one of the following:

- The original event was split into sub-parts by creating additional events for each transaction inside the original event.
- The original session was split as it was ingested into the Network Decoder because the size was larger than the Assembler Maximum Size (default=32 MB).
- The original session was split as it was ingested into the Network Decoder because the time was longer than the Assembler Timeout Session (default=60 sec).

Session Size and Time Split

Network Decoders are configured with a default session size (`assembler.size.max`) and a session timeout (`assembler.timeout.session`). The configuration is described in "Configure Session Split Timeouts" in the *Decoder Configuration Guide*. When a session exceeds either limit, the Network Decoder splits the session, and all subsequent packets become part of a new session, fragmenting the actual network session across multiple Network Decoder sessions. To process session fragments with the context that they are fragments of the larger network session and to improve association of source and destination addresses, ports, and application protocols, Network Decoders parse contextual fragments and highlight session fragments.

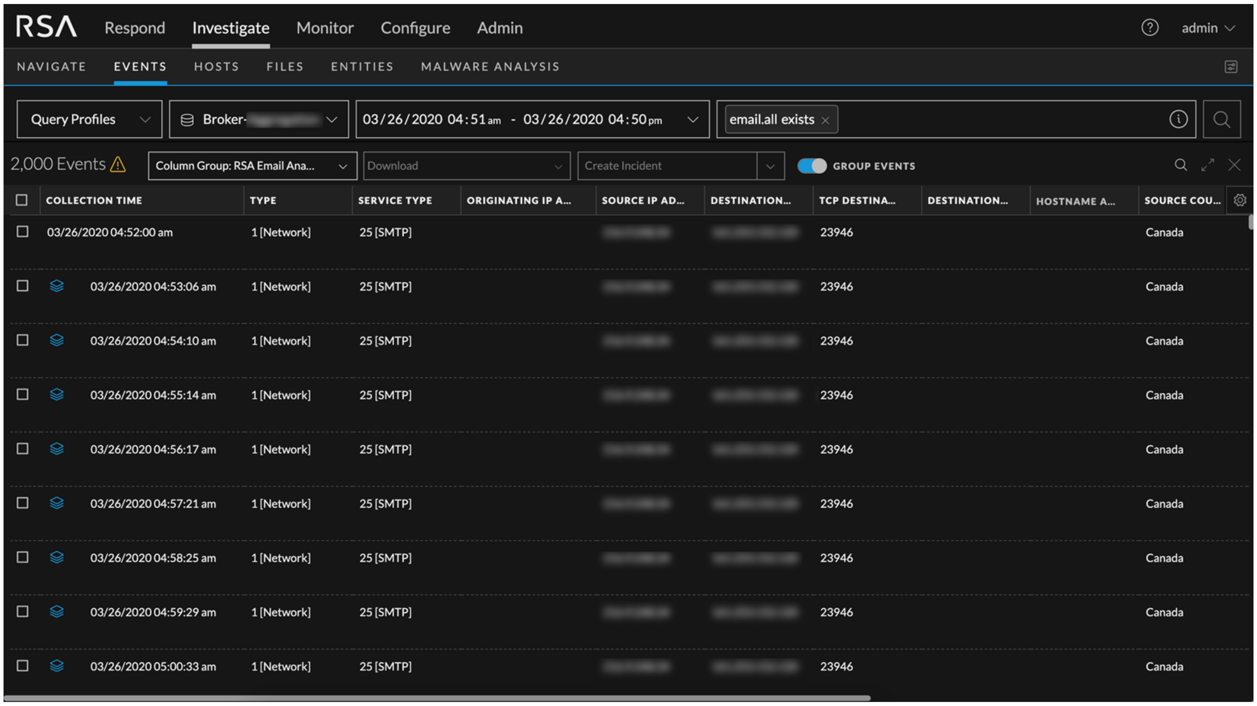
Note: In the Legacy Events view, you can find session fragments and export all packets viewed in the Events list to a single PCAP as described in Find and Combine Fragments in the Legacy Events View.

The Network Decoder completes session parsing before splitting the session based on the configured maximum session size (default = 32 MB) or the configured timeout (default = 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.

Transaction Handling Split

Administrators can configure a Network Decoder to subdivide incoming sessions into smaller transaction sessions when using Lua parsers that are designed to create transactions. The configuration is described in "Configure Transaction Handling on a Decoder" in the *Decoder Configuration Guide*. The Decoder service configuration node has a parameter that controls the behavior of the Network Decoder when a parser defines a transaction within a network session: `/decoder/parsers/config/parser.transaction.mode`. If the mode is set to `split`, a large session with multiple application-level transactions is split when a parser generates an application-level transaction such as an email. An example of this is a large session containing multiple emails. For each email (transaction), a new session item (split session) is created, network meta items are copied into the new session, and meta items marked in the transaction are copied from the original session to the new session.

Transactions require a parser update to function, and initially they only support SMTP and HTTP pipelining use cases. This is an example of the reconstruction of an email that is separated based on the individual emails inside the original event. Each transaction highlights a single email and the metadata associated with the transaction is only related to that email. To provide this functionality, the original packets are stored on the Network Decoder as usual for a network event, but the new related transaction events are created on the Concentrator. As a result, analysts see visual queues in the user interface, and they also have the ability to query to find only specific emails or attributes of emails that were previously all bundled together. To eliminate the original event from the query results, the `session.split` meta key has been indexed. When there are transaction splits, the original event does not have that meta key associated with it while all the related transactional events do.



Broker-[redacted]

03/26/2020 04:51 am - 03/26/2020 04:50 pm

email.all exists

2,000 Events ⚠

Column Group: RSA Email Ana...

☐	COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATING IP A...	SOURCE IP AD...	DESTINATION...	TCP DESTINA...	DESTINATION...	HOSTNAME A...	SOURCE COU...
☐	03/26/2020 04:52:00 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:53:06 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:54:10 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:55:14 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:56:17 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:57:21 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:58:25 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 04:59:29 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada
☐	03/26/2020 05:00:33 am	1 [Network]	25 [SMTP]		[redacted]	[redacted]	23946			Canada

Session Fragments Highlighting

Both types of session fragments have an additional meta key: `session.split`. 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 key 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` metadata if the session is parsed before exceeding the maximum session size.

Transaction splits start with a `session.split` value of 1. When viewing sessions, the `session.split` meta key clearly identifies sessions that are fragments in the Events view and the Legacy Events view (Events List view and the Events Detail view).

If this was a session size and timeout split, you can view the session fragments and 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 separately from the 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.

Related Network Session

If you see a tool tip like this, separate events processed by the Network Decoder share a set of four values that identify the IP source, IP destination, source port, and destination port:

```
 The event is related to a previous session matching these parameters:
ip.src=127.0.0.1 AND ip.dst=127.0.0.1 AND tcp.srcport=25 AND
tcp.dstport=1234"Second category: Related Network Session
```

In this case, the Network Decoder has not inserted a split, and there is no `session.split` metadata associated to any of the events. The reason these events grouped together is to highlight the events that are worthy of scrutiny based on a pattern. Each event has the same source IP address, the same destination IP address, the same source port, and the same destination port. The grouping of related events does not occur if any of the four meta keys is obfuscated for data privacy reasons.

These are the combinations of meta keys that must match to categorize an event as a Related Network Session:

- `ip.dst`, `ip.src`, `tcp.dstport`, `tcp.srcport`
- `ip.dst`, `ip.src`, `upd.dstport`, `udp.srcport`
- `ipv6.dst`, `ipv6.src`, `tcp.dstport`, `tcp.srcport`
- `ipv6.dst`, `ipv6.src`, `upd.dstport`, `udp.srcport`

Use Cases for Viewing Events from Split and Related Network Sessions

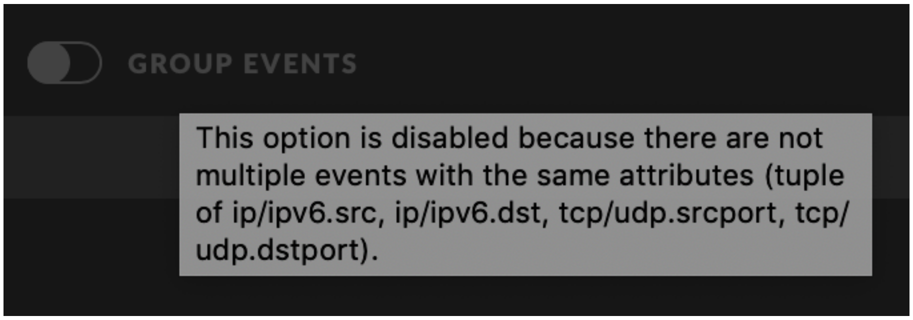
These are examples of practical use cases for viewing events from split sessions:

- A Network Decoder that is inline with a proxy server receives a lot of email connections that get bundled into a single session based on event time as NetWitness sees them. The single session has multiple meta values for `subject`, `email.src`, `email.dst`, and other meta keys relevant to email, which are difficult to map together correctly. Seeing the session organized as leading and subsequent events, gives the analyst a clear idea of the details of each email.

- An analyst is attempting to understand what IP address out of all the metadata associated with a session resulted in the generated metadata or an alert, but the IP address is not in the output. For example, a feed that is parsing for an indicator of compromise may have many triggers in a session that has many IP addresses. By viewing the complete event organized as leading and subsequent events, the analyst can understand which IP triggered the alert.
- An analyst wants to know which file was deleted from which directory versus which file was read out in which directory, but the session encompasses multiple files and directories. For example, an HTTP connection with commands: `directory /keep/`, `directory /temp/`, `filename foo.txt`, `filename me.doc`, `action delete`, and `action read`. Viewing the leading and subsequent events tells the analyst that `/temp/me.doc` was deleted and `/keep/foo.txt` was read. Now the analyst or analytics can form an opinion about how bad these actions really were.
- An analyst is attempting to retrieve a large file related to an event that triggered a suspicous alert. However, the file that was transferred was so large that the network decoder split it into 100 separate sessions. When viewing this group related split sessions, the analyst can download a PCAP of the sessions, then extract the original file by either running it through a Decoder with larger assembler settings or a third-party tool.

Show and Hide Relationships in the Events List

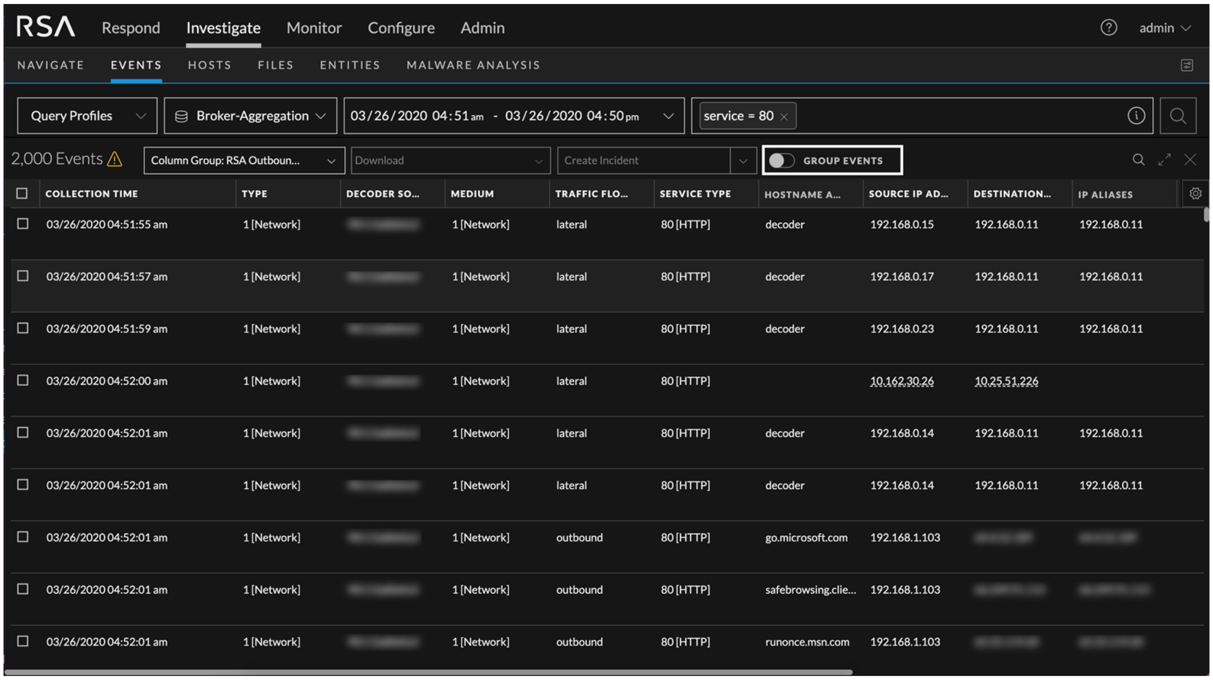
For both types of related events, you can see the relationship of events in the Events view Events list. When the Events list is first displayed, you can tell if set of results includes related events by looking at the Group Events switch at the top of the Events list. If the results do not include related events, the switch is dimmed as shown in the following figure.



This option is disabled because there are not multiple events with the same attributes (tuple of ip/ipv6.src, ip/ipv6.dst, tcp/udp.srcport, tcp/udp.dstport).

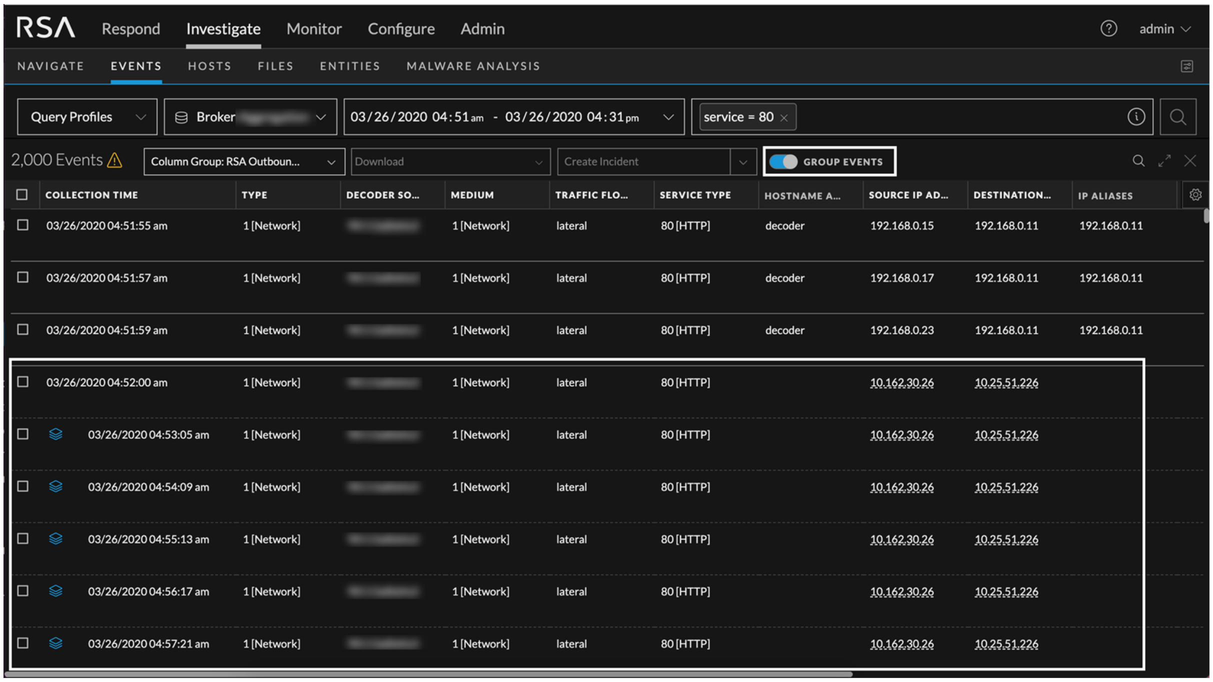
To look for related events in the Events list:

1. Go to **Investigate > Events** and submit a query.
   If the results include related events, the Group Events switch is active, but not enabled. The figure below illustrates a set of results that include split sessions, and the Group Events switch is disabled. The related events are not nested.



□	COLLECTION TIME	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP AD...	DESTINATION...	IP ALIASES
□	03/26/2020 04:51:55 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.15	192.168.0.11	192.168.0.11
□	03/26/2020 04:51:57 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.17	192.168.0.11	192.168.0.11
□	03/26/2020 04:51:59 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.23	192.168.0.11	192.168.0.11
□	03/26/2020 04:52:00 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	03/26/2020 04:52:01 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.14	192.168.0.11	192.168.0.11
□	03/26/2020 04:52:01 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.14	192.168.0.11	192.168.0.11
□	03/26/2020 04:52:01 am	1 [Network]	[redacted]	1 [Network]	outbound	80 [HTTP]	go.microsoft.com	192.168.1.103	[redacted]	[redacted]
□	03/26/2020 04:52:01 am	1 [Network]	[redacted]	1 [Network]	outbound	80 [HTTP]	safebrowsing.clie...	192.168.1.103	[redacted]	[redacted]
□	03/26/2020 04:52:01 am	1 [Network]	[redacted]	1 [Network]	outbound	80 [HTTP]	runonce.msn.com	192.168.1.103	[redacted]	[redacted]

2. Click the **Group Events** switch.
   Related subsequent events are nested below the leading event. The subsequent events are indented and marked by an icon. Clicking on the icon explains why the event is grouped.

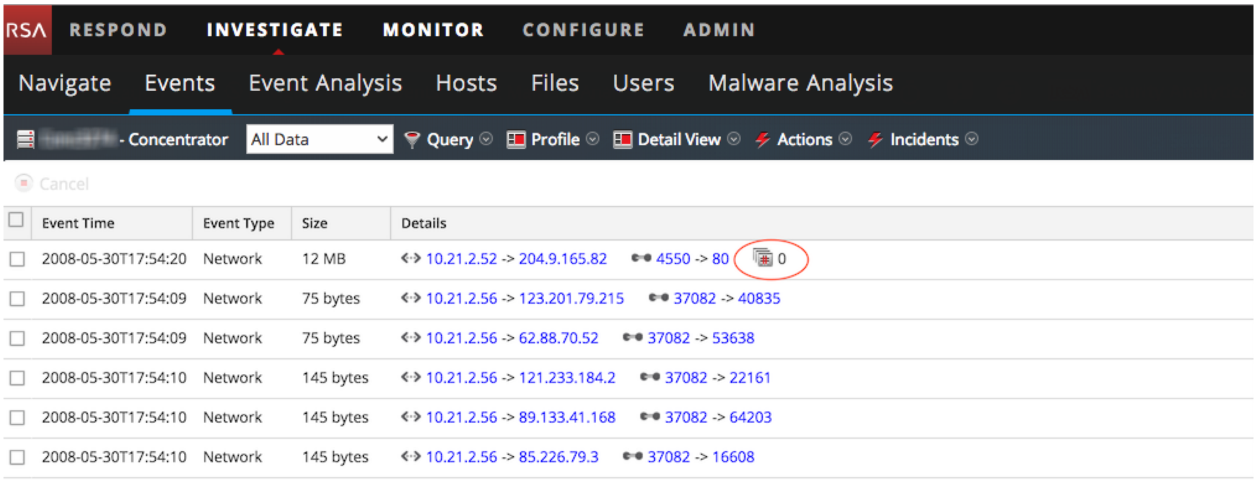


□	COLLECTION TIME	TYPE	DECODER SO...	MEDIUM	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP AD...	DESTINATION...	IP ALIASES
□	03/26/2020 04:51:55 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.15	192.168.0.11	192.168.0.11
□	03/26/2020 04:51:57 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.17	192.168.0.11	192.168.0.11
□	03/26/2020 04:51:59 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]	decoder	192.168.0.23	192.168.0.11	192.168.0.11
□	03/26/2020 04:52:00 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	≋ 03/26/2020 04:53:05 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	≋ 03/26/2020 04:54:09 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	≋ 03/26/2020 04:55:13 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	≋ 03/26/2020 04:56:17 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	
□	≋ 03/26/2020 04:57:21 am	1 [Network]	[redacted]	1 [Network]	lateral	80 [HTTP]		10.162.30.26	10.25.51.226	

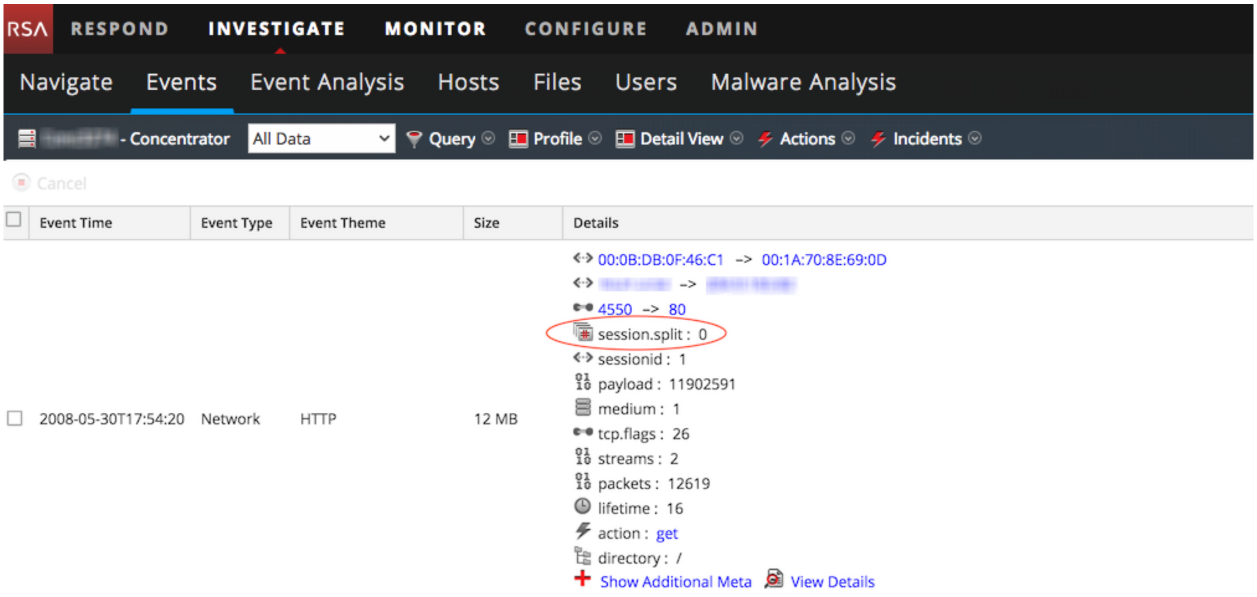
Session Fragments Highlighting (11.3 Events View)

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.



☐	Event Time	Event Type	Size	Details
☐	2008-05-30T17:54:20	Network	12 MB	<-> 10.21.2.52 -> 204.9.165.82 4550 -> 80 0
☐	2008-05-30T17:54:09	Network	75 bytes	<-> 10.21.2.56 -> 123.201.79.215 37082 -> 40835
☐	2008-05-30T17:54:09	Network	75 bytes	<-> 10.21.2.56 -> 62.88.70.52 37082 -> 53638
☐	2008-05-30T17:54:10	Network	145 bytes	<-> 10.21.2.56 -> 121.233.184.2 37082 -> 22161
☐	2008-05-30T17:54:10	Network	145 bytes	<-> 10.21.2.56 -> 89.133.41.168 37082 -> 64203
☐	2008-05-30T17:54:10	Network	145 bytes	<-> 10.21.2.56 -> 85.226.79.3 37082 -> 16608



☐	Event Time	Event Type	Event Theme	Size	Details
☐	2008-05-30T17:54:20	Network	HTTP	12 MB	<-> 00:0B:DB:0F:46:C1 -> 00:1A:70:8E:69:0D <-> [redacted] -> [redacted] 4550 -> 80 session.split : 0 sessionid : 1 payload : 11902591 medium : 1 tcp.flags : 26 streams : 2 packets : 12619 lifetime : 16 action : get directory : / + Show Additional Meta View Details

> **Note:** The `session.split` meta key must be indexed to help you find the split sessions in the results.

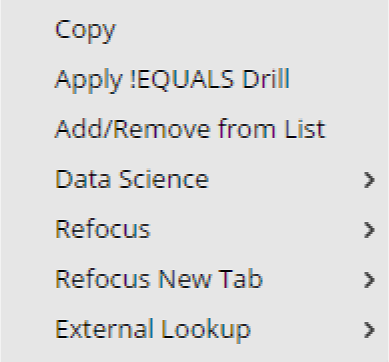
The `session.split` metadata is displayed immediately following the address and port metadata in the details view (Legacy Events view). These enhancements make it possible to quickly:

- 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.

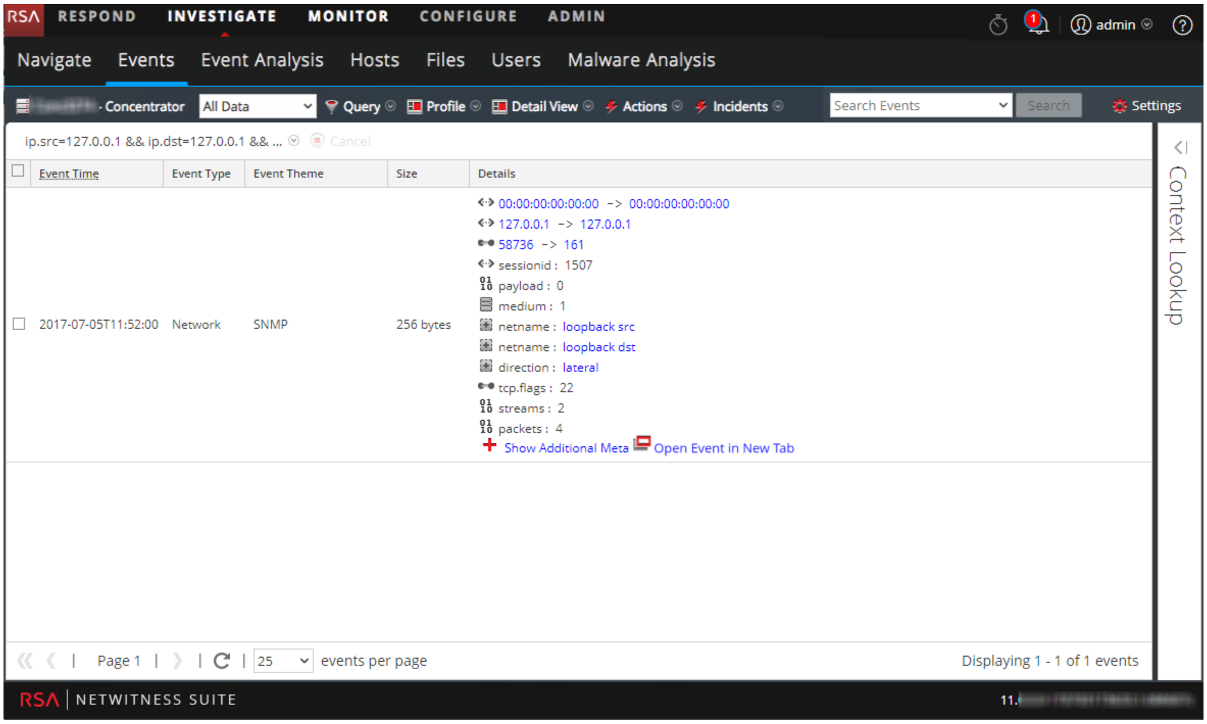
Find and Combine Fragments in the Legacy Events View

From within the Legacy 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 **Legacy 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).



ip.src=127.0.0.1 && ip.dst=127.0.0.1 && ...

□	Event Time	Event Type	Event Theme	Size	Details
□	2017-07-05T11:52:00	Network	SNMP	256 bytes	00:00:00:00:00:00 -> 00:00:00:00:00:00 127.0.0.1 -> 127.0.0.1 58736 -> 161 sessionid : 1507 payload : 0 medium : 1 netname : loopback src netname : loopback dst direction : lateral tcp.flags : 22 streams : 2 packets : 4 + Show Additional Meta Open Event in New Tab

Page 1 | 25 events per page

Displaying 1 - 1 of 1 events

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.

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 Use Meta Groups to Focus on Relevant Meta Keys) 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 built-in 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

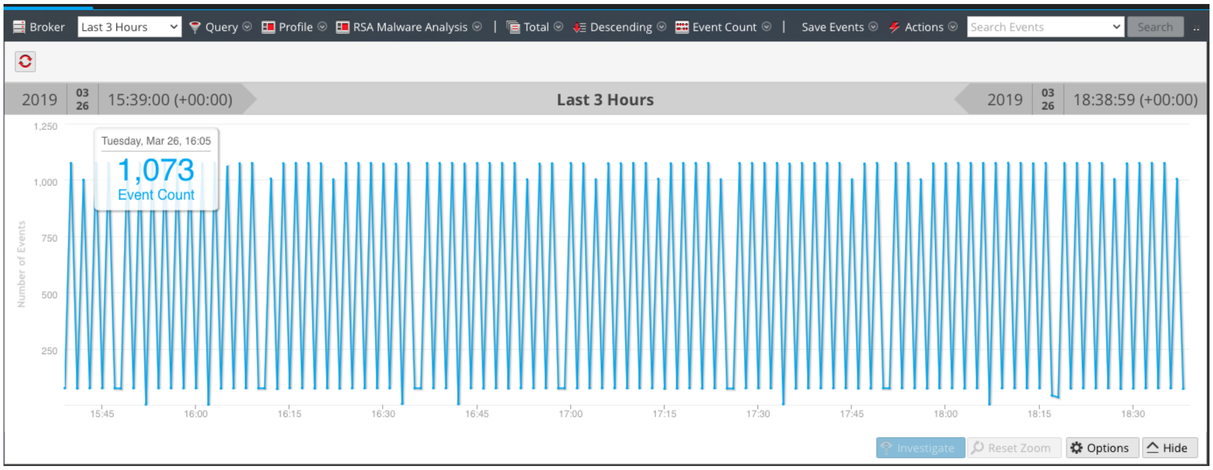
A set of predefined meta groups is included with NetWitness Platform. If you want to get the latest version, you can import the meta groups file, `MetaGroups_ootb_w_query.jsn`, in the Manage Meta Groups dialog. Some of the targeted activities that lend themselves well to Parallel Coordinates visualizations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

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

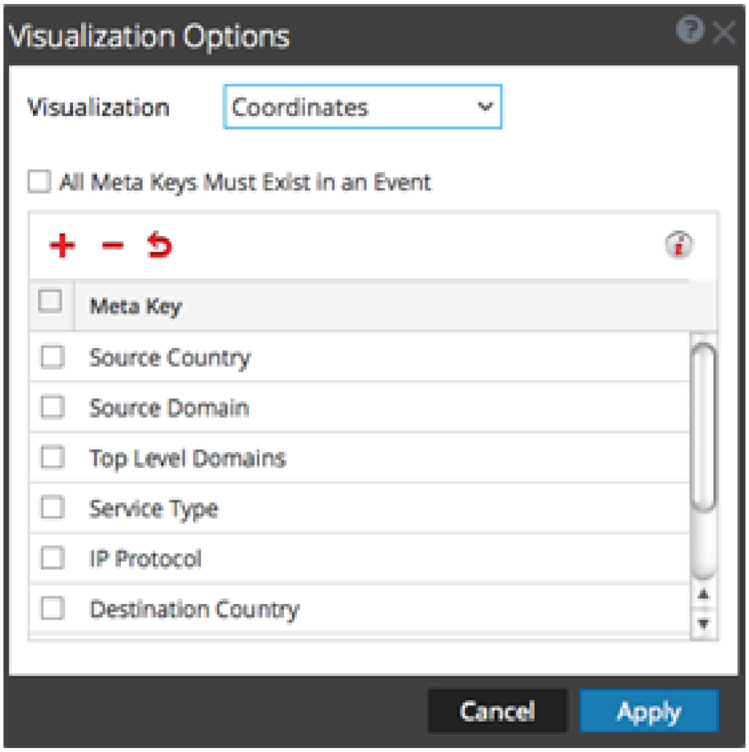
View a Parallel Coordinates Visualization

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**.



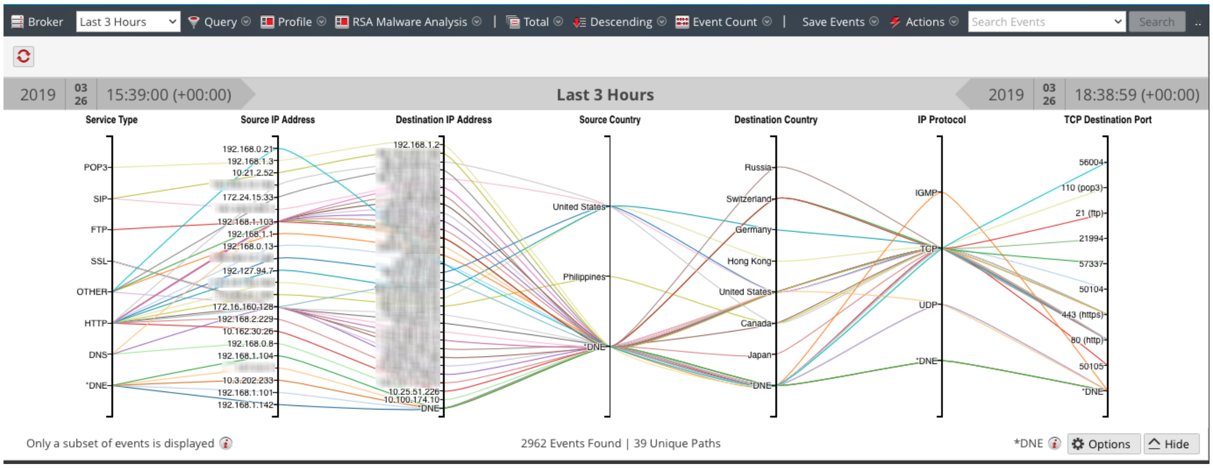
Visualization Options

Visualization: Coordinates

□ All Meta Keys Must Exist in an Event

□	Meta Key
□	Source Country
□	Source Domain
□	Top Level Domains
□	Service Type
□	IP Protocol
□	Destination Country

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



Only a subset of events is displayed

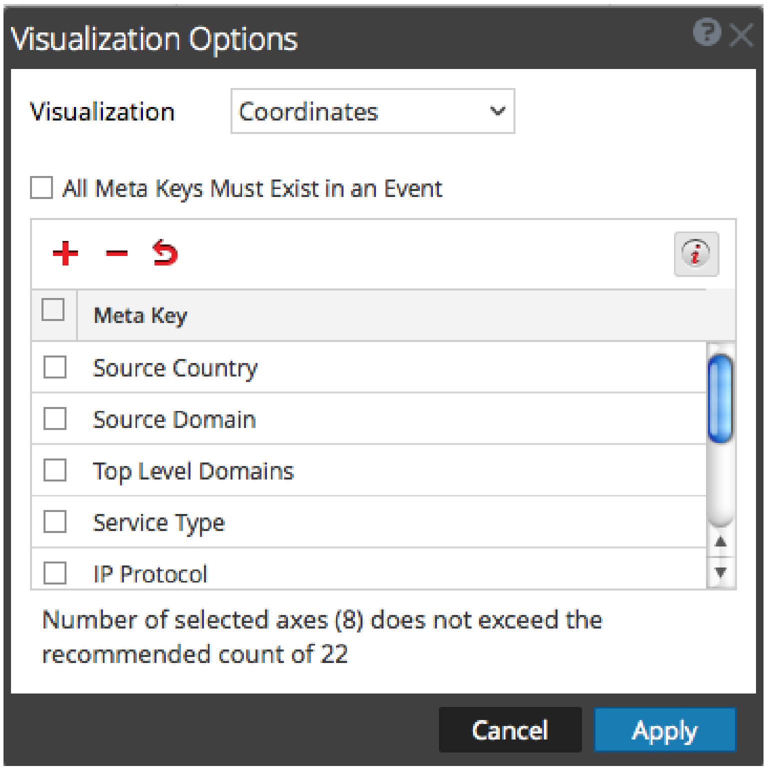
2962 Events Found | 39 Unique Paths

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.



Visualization Options

Visualization: Coordinates

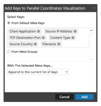
☐ All Meta Keys Must Exist in an Event

☐	Meta Key
☐	Source Country
☐	Source Domain
☐	Top Level Domains
☐	Service Type
☐	IP Protocol

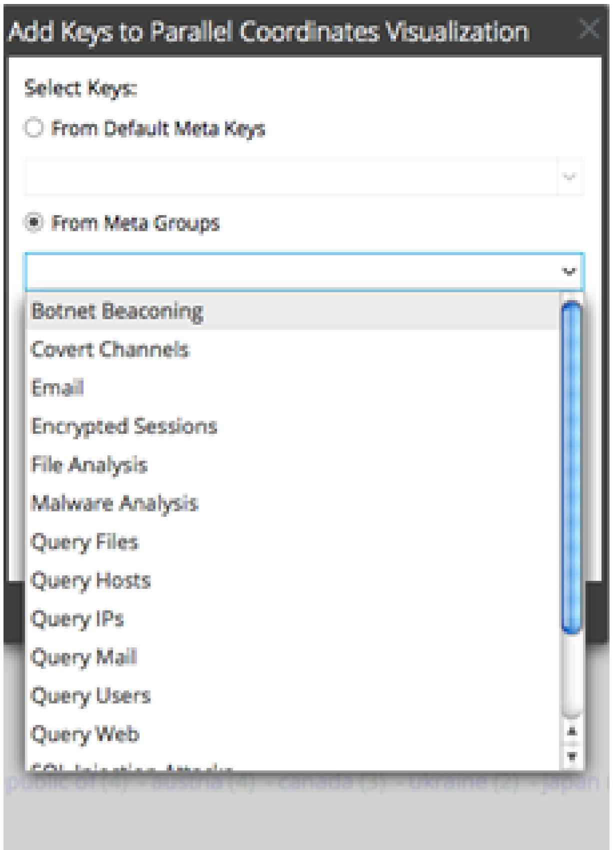
Number of selected axes (8) does not exceed the recommended count of 22

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.

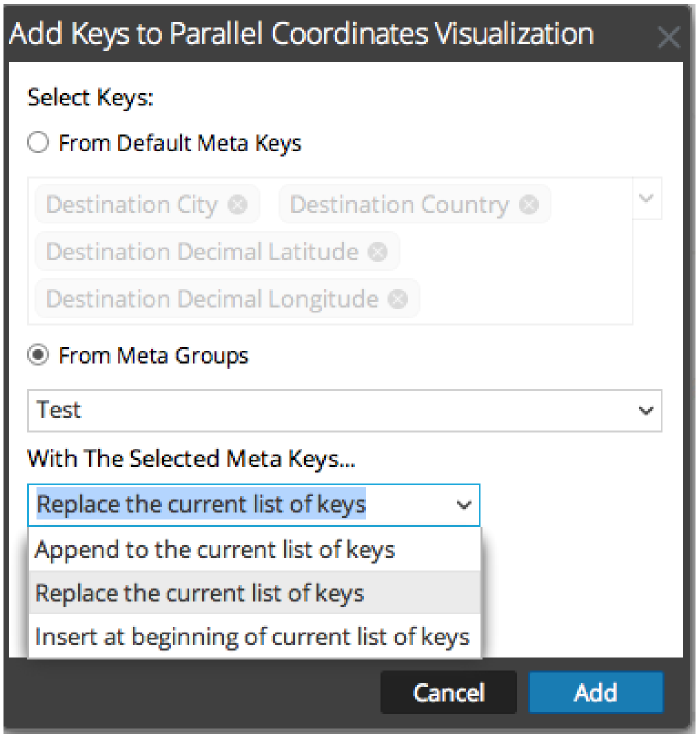
   

6. If you want to add all the keys in a meta group, you cannot add individual meta keys. Select **From Meta Groups**, and select a group from the drop-down list.



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.**



Add Keys to Parallel Coordinates Visualization

Select Keys:

○ From Default Meta Keys

Destination City ⊗ Destination Country ⊗ Destination Decimal Latitude ⊗ Destination Decimal Longitude ⊗

● From Meta Groups

Test

With The Selected Meta Keys...

Replace the current list of keys

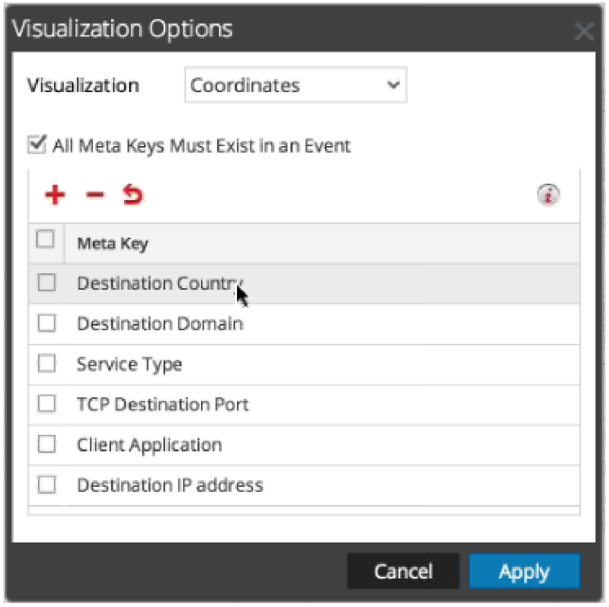
Append to the current list of keys
Replace the current list of keys
Insert at beginning of current list of keys
Cancel
Add

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.**



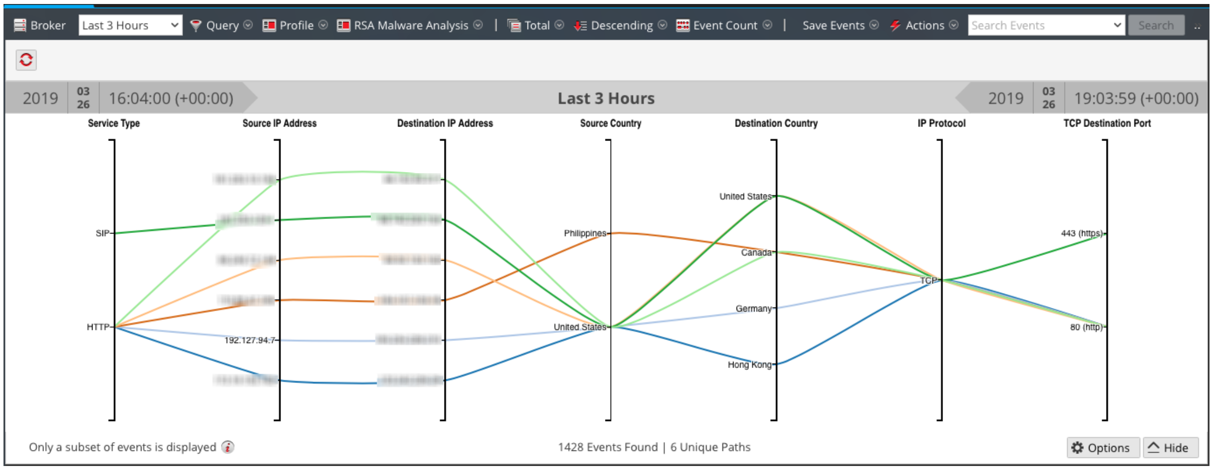
Visualization Options

Visualization: Coordinates

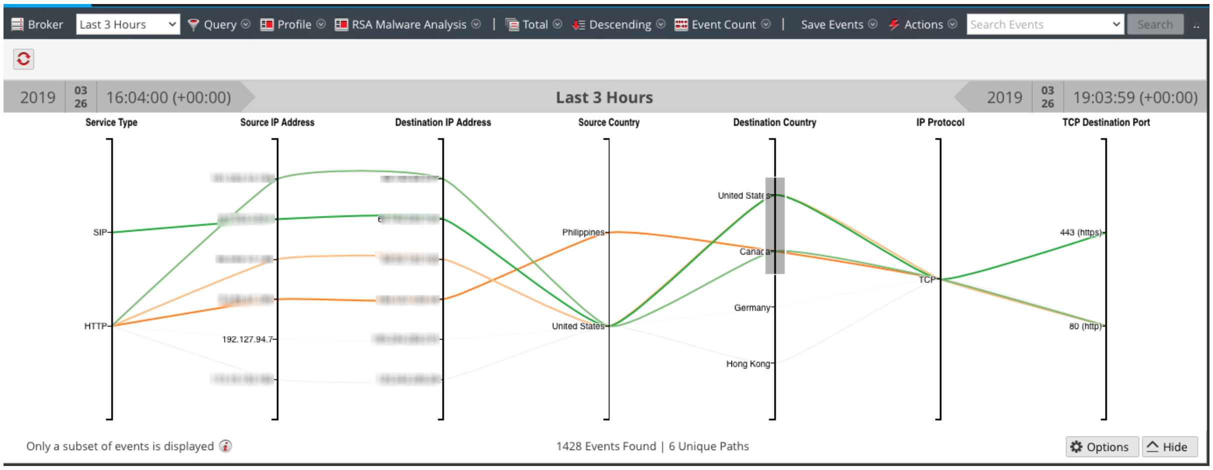
☑ All Meta Keys Must Exist in an Event

□	Meta Key
□	Destination Country
□	Destination Domain
□	Service Type
□	TCP Destination Port
□	Client Application
□	Destination IP address

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.



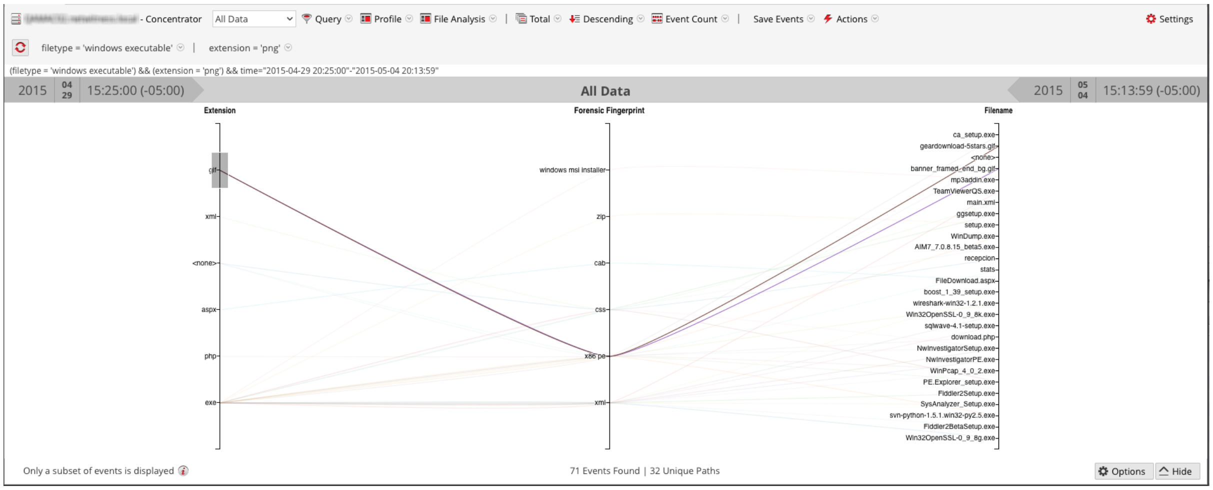
4. If you want to enlarge the visualization, drag the bottom edge of the panel down and drag the right edge of the browser window wider.

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`.



[redacted] - Concentrator

filetype = 'windows executable' | extension = 'png'

(filetype = 'windows executable') && (extension = 'png') && time="2015-04-29 20:25:00"-"2015-05-04 20:13:59"

2015 04 29 15:25:00 (-05:00) All Data 2015 05 04 15:13:59 (-05:00)

Only a subset of events is displayed

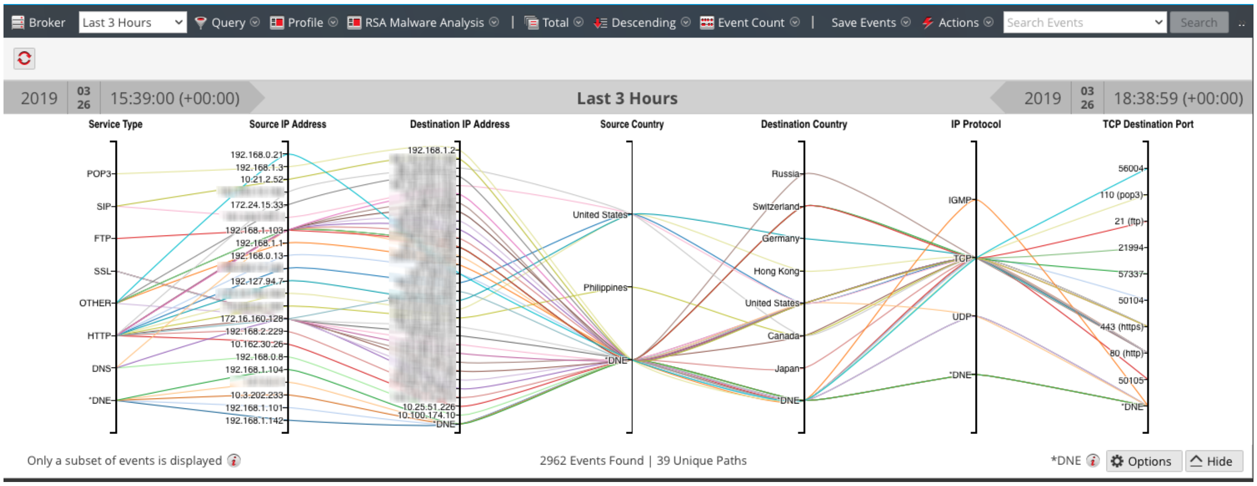
71 Events Found | 32 Unique Paths

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.**



Only a subset of events is displayed

2962 Events Found | 39 Unique Paths

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.

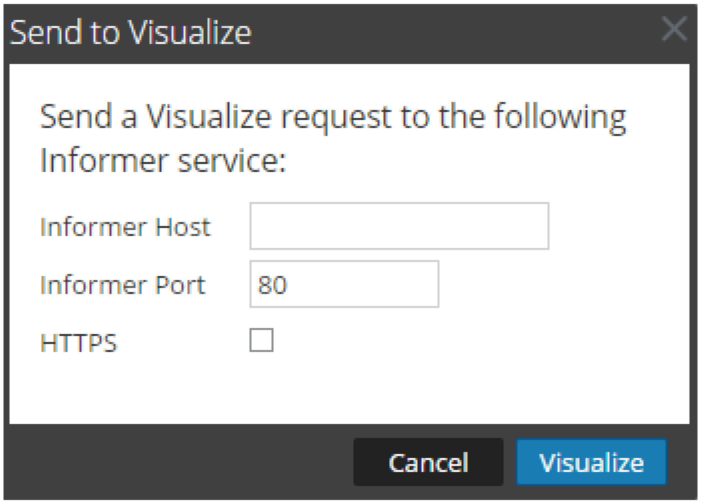
Visualize the Current Drill Point in Informer

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.



Send to Visualize

Send a Visualize request to the following Informer service:

Informer Host

Informer Port 80

HTTPS □

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.

Downloading and Acting Upon Results

When working in Investigate, you may want to extract and shared data with other analysts, incident responders, SOC managers, and others. The topics in this section provide instructions for downloading results and creating incidents that appear in the Respond view:

- Download Data in the Events View
- Export or Print a Drill Point in the Navigate View
- Export Events in the Legacy Events View
- Add Events to an Incident in the Events View
- Add Events to an Incident in the Legacy Events View

Download Data in the Events View

In the Events view, you can download data from the Events panel and from a reconstruction. The Events panel download available in Version 11.4 is a bulk download of log and network events for all the event types. Version 11.4.1 has the added capability to downloadvisible metadata for all the event types. From within a reconstruction, you can download events, logs, and files.

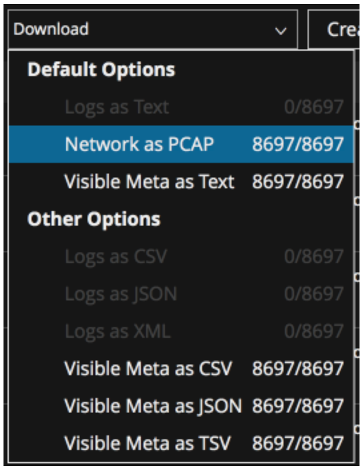
Note: The information that you can view and download is managed by Role-Based Access Controls (RBAC) that your administrator has implemented. When RBAC is configured to prevent downloads of certain data, events for which you do not have download permission may appear to download successfully, but they are 0 byte in size. When RBAC is configured to prevent reconstruction of certain events, the reconstruction is disabled from the Events panel, but the bulk download button is still enabled.

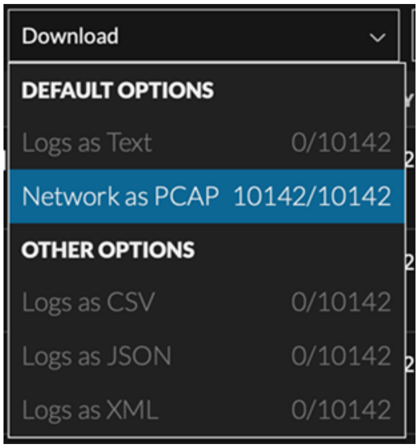
Download Log, Visible Metadata, or Network Events in the Events Panel (Version 11.4 and Later)

After submitting a query you can download logs, network events, or visible metadata for events in your preferred format, directly from the Events panel. The preferences are set in the Event Preferences dialog and any changes made there are reflected inside the **Download** menu. See Configure the Events View for more information about preferences.

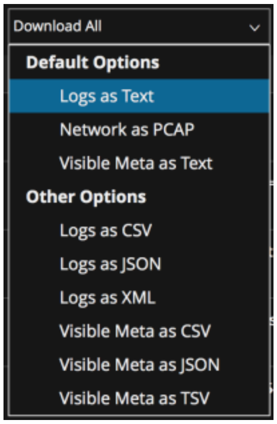
Note: When you download visible metadata; it is sorted in order of collection time rather than the current sort order in the Events panel.

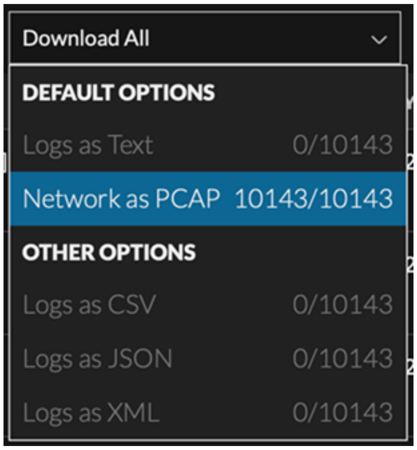
In the Events panel, you can select events individually or select all events returned by your search. The selection checkboxes appear only if you have permission to download the events. All checkboxes are deselected when a new query is submitted. When you select events and click Download, the Download menu is displayed. The number of events selected for each event type is displayed next to each option in the format `Events of this type selected/ Total number of events selected`. If an event type has no events selected, the corresponding download option is disabled and the number of events selected is displayed as `0 / Total number of events selected` as shown in the following figures. Notice that the Version 11.4.1 menu has options to download visible metadata and the Version 11.4 menu does not have those options.


Download
Cre
Default Options
Logs as Text 0/8697
Network as PCAP 8697/8697
Visible Meta as Text 8697/8697
Other Options
Logs as CSV 0/8697
Logs as JSON 0/8697
Logs as XML 0/8697
Visible Meta as CSV 8697/8697
Visible Meta as JSON 8697/8697
Visible Meta as TSV 8697/8697



If the select all checkbox is selected in the Events list, the event count is no longer displayed in the menu as shown in the following figures. Notice that the Version 11.4.1 menu has options to download visible metadata and the Version 11.4 menu does not have those options.



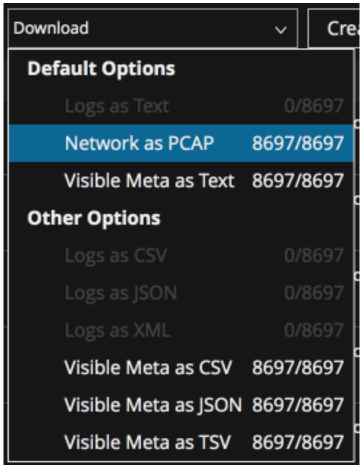


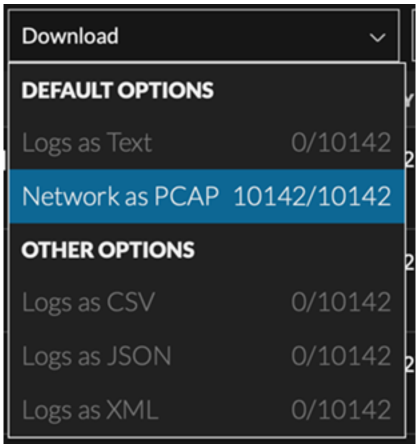
Note: When you select all events for download, only the events in the current result set are downloaded. If you canceled the query before all results were returned, only the events that were loaded are downloaded.

To download event data for one event, multiple events, or all events in the Events panel:

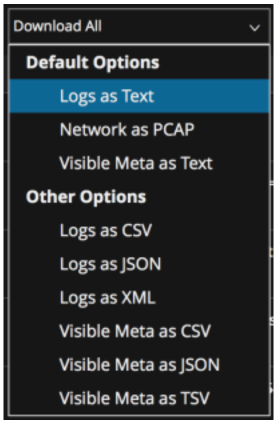
1. Do one of the following:

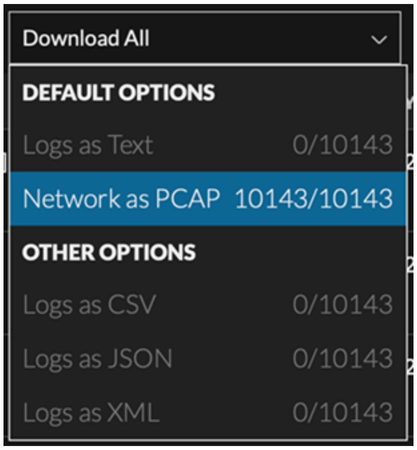
   a. To select events individually, select the checkbox next to each event you want to download, and click the **Download** menu label to see the options. Notice that the Version 11.4.1 menu has options to download visible metadata and the Version 11.4 menu does not have those options.


Download
Cre
Default Options
Logs as Text 0/8697
Network as PCAP 8697/8697
Visible Meta as Text 8697/8697
Other Options
Logs as CSV 0/8697
Logs as JSON 0/8697
Logs as XML 0/8697
Visible Meta as CSV 8697/8697
Visible Meta as JSON 8697/8697
Visible Meta as TSV 8697/8697



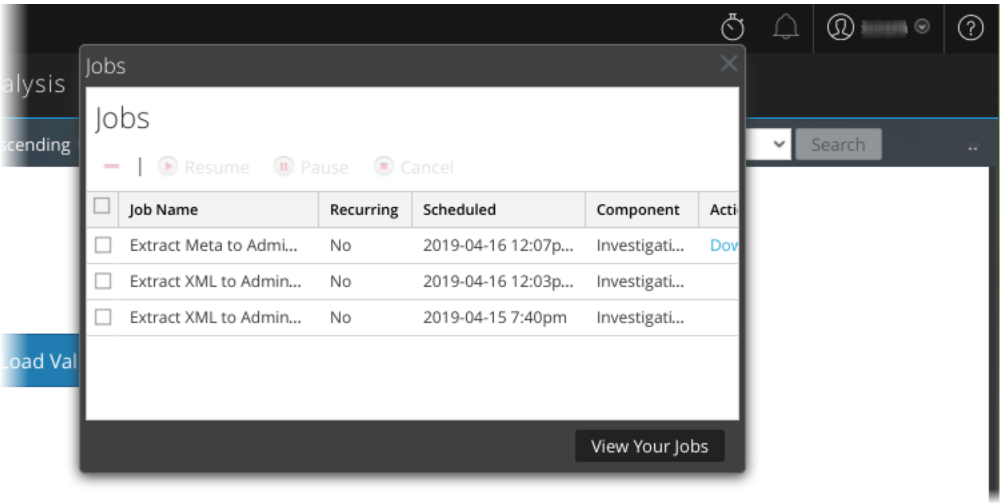
b. To select all events displayed in the Events panel, select the checkbox at the top of the Events panel and click the **Download All** menu label.





2. Review the **Default Options** in effect in the top section of the menu. If you do not want to use the default format, you can choose a different format from the **Other Options** section of the menu.
   - Logs are downloaded in the preferred format that you selected in the Events Preference menu (**Logs asText**, **Logs as CSV**, **Logs as JSON**, or **Logs as XML**). If you want to choose a different format for this download, select one of the formats from lower part of the menu.
   - Network events are downloaded as a PCAP. When downloading multiple network events in the Events panel, the format is always PCAP. The preferred format that you specified in the Events Preference menu (**Network as PCAP**, **Network as Payloads**, **Network as Request Payload**, or **Network as Response Payload**) is ignored in this menu. Your preferred format applies only to downloading a single network event in the network reconstruction panel.
   - Visible metadata is downloaded in the format that you selected in the Events Preference menu (**Visible Meta as Text**, **Visible Meta as CSV**, **Visible Meta as JSON**, or **Visible Meta as TSV**). If you want to choose a different format for this download, select one of the formats from lower part of the menu. The downloaded metadata for each event corresponds to the columns visible when the metadata is downloaded. If the Summary column group is selected in the Events panel, all metadata for the events is downloaded.
3. Click the menu label: **Download** or **Download All**.
   The download begins immediately within the browser window if the **Download extracted files automatically** preference is set (**Events** view > ☰). If the preference is not set, the download job for the selected events is added to the Jobs tray, where you can download the events.
   If the download fails, a message provides feedback regarding why the download failed. The download button is re-enabled and any selected events remain selected. These are examples of reasons for a failed download: timeout after X minutes, connection failed, event limit reached, and permission denied.
4. To display the Jobs tray, go to **Investigate > Navigate** or **Investigate > Events**, and click the ⏱ Jobs icon, which looks like a stop watch.

The jobs are displayed in the Jobs tray.



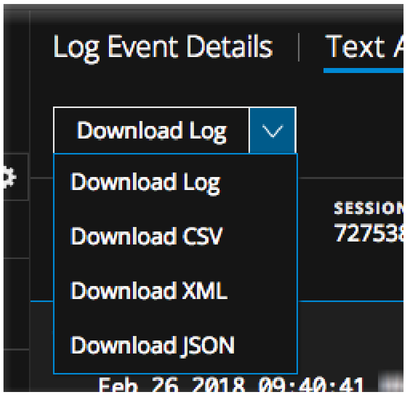
□	Job Name	Recurring	Scheduled	Component	Acti
□	Extract Meta to Admi...	No	2019-04-16 12:07p...	Investigati...	Dov
□	Extract XML to Admin...	No	2019-04-16 12:03p...	Investigati...	
□	Extract XML to Admin...	No	2019-04-15 7:40pm	Investigati...	

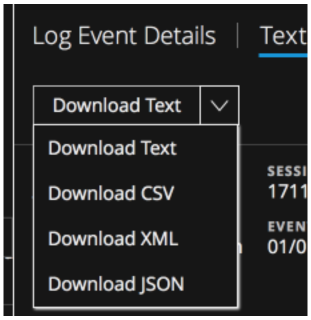
Download a Log in the Text Panel

When viewing a log reconstruction in the Text 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** (11.3) or **Download Text** (11.4 and later) 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** (11.3) or **Download Text** (11.4 and later) menu options displayed.





Note: The**Download Log** (11.3) or **Download Text** (11.4 and later) 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:

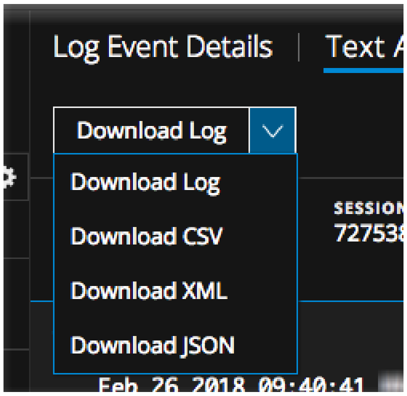
- `<service-ID or host name>` is the name of the service (for example a Concentrator or Broker) where the session was saved.
- `SID<n>` is the session ID number.
- `<filetype>` identifies the format of the downloaded log. These are the possible log types: raw log, CSV, XML, and JSON. By default, the format is a raw log.

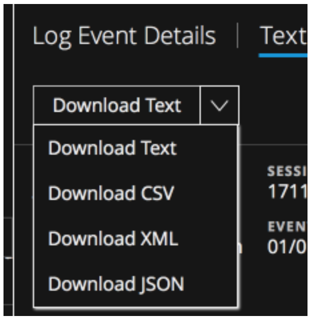
Note: Some formats do not have time stamps or the device IP where the event was generated, so a log downloaded in CSV, XML, or JSON format has an extra value called `timestamp` along with the raw log content. The additional information inside the log is in this form: `Log timestamp="1490824512" source="10.12.35.65"`.

To download the log for a session:

In the Text 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** or **(Download Text in 11.4)**.
- To download the log in one of the other formats, click the downward arrow on the **Download Log** (11.3) or **Download Text (11.4 and later)** 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 Panel or the Packet Panel

When viewing a reconstructed network event in the Packet panel or the Text 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** (11.3) or **Download Payloads** (11.4) 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.

The label on the download menu button is one of these formats, based on the setting selected in the Event Preferences dialog. If the event does not have that type of date, the menu button is dimmed. You can click on the menu button to see which options are available. For example, if an event has a request payload, but no response payload, the Download Response Payload button is dimmed. You can click on the button and select **Download Request Payload** for this download. After selecting a valid format, clicking the button executes the download.

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.

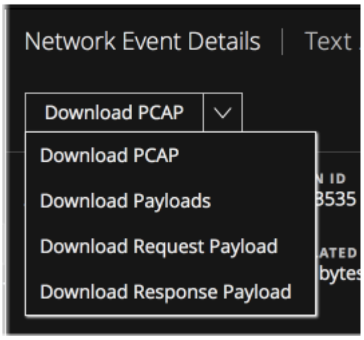
The network data is downloaded directly into your browser if the download is quick. If the download takes longer due to network factors or file size, the file is downloaded in the background and the task is tracked in the Jobs queue. In this case, you can check your jobs in the queue and get the file 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 panel of a network event click the Download menu button. The label is the same as the download option set in the Events Preferences dialog. Click the **Download** menu label to see other formats that you can select.

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



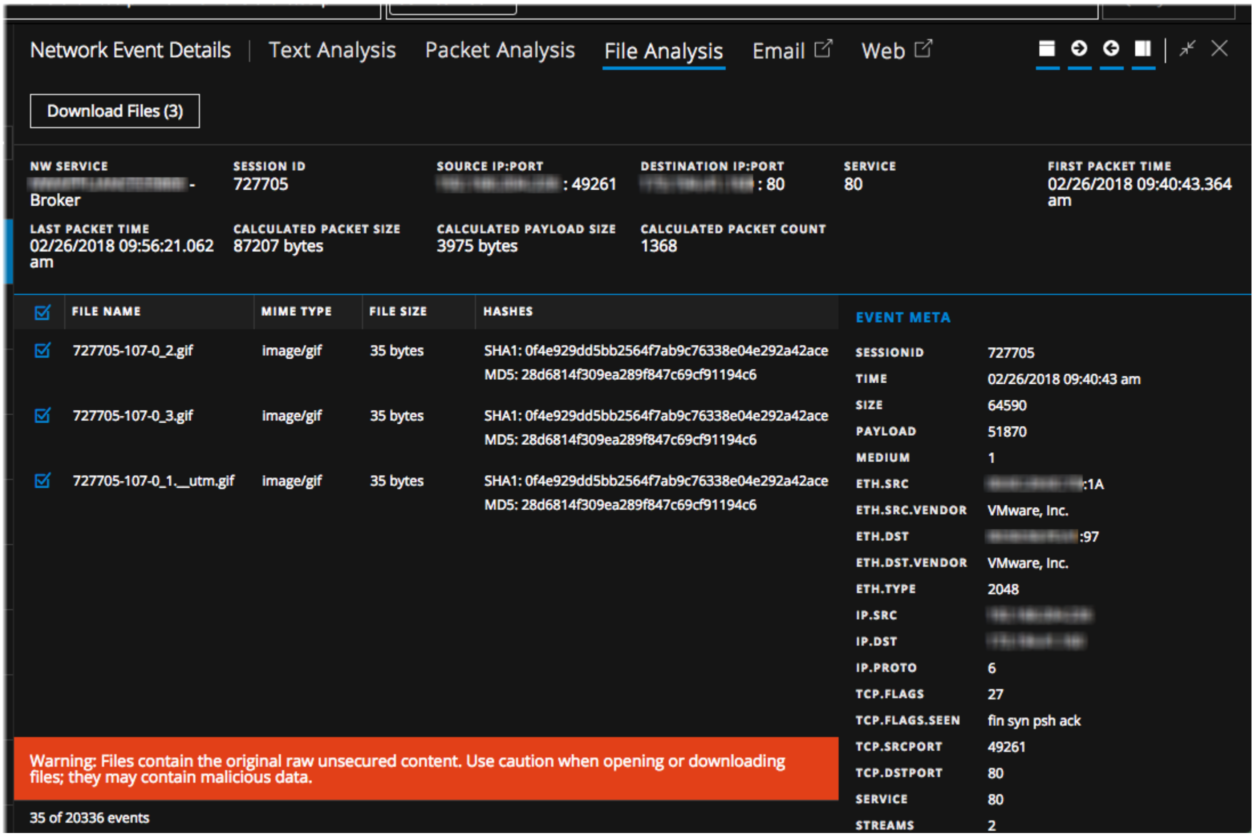
The network data file is downloaded to your local file system in the format specified.

Download Files from a Network Event in the File Panel

When viewing reconstructed network events that contain files in the File 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.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
[redacted] - Broker	727705	[redacted] : 49261	[redacted] : 80	80	02/26/2018 09:40:43.364 am

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
02/26/2018 09:56:21.062 am	87207 bytes	3975 bytes	1368

☑	FILE NAME	MIME TYPE	FILE SIZE	HASHES
☑	727705-107-0_2.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6
☑	727705-107-0_3.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6
☑	727705-107-0_1._utm.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data.

35 of 20336 events

EVENT META

SESSIONID	727705
TIME	02/26/2018 09:40:43 am
SIZE	64590
PAYLOAD	51870
MEDIUM	1
ETH.SRC	[redacted]:1A
ETH.SRC.VENDOR	VMware, Inc.
ETH.DST	[redacted]:97
ETH.DST.VENDOR	VMware, Inc.
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	27
TCP.FLAGS.SEEN	fin syn psh ack
TCP.SRCPORT	49261
TCP.DSTPORT	80
SERVICE	80
STREAMS	2

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
```

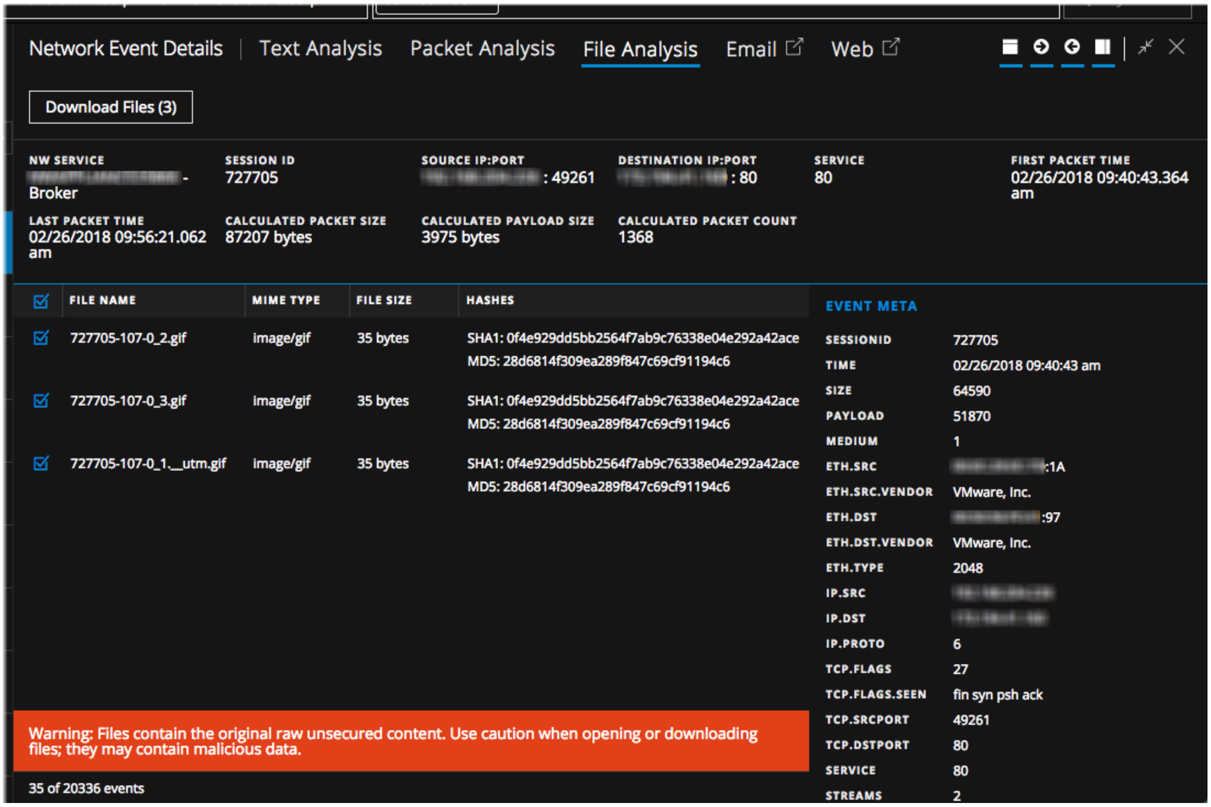
where:

- `<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 **Events** view, go to the File panel of an event that contains files.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
[redacted] - Broker	727705	[redacted] : 49261	[redacted] : 80	80	02/26/2018 09:40:43.364 am

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
02/26/2018 09:56:21.062 am	87207 bytes	3975 bytes	1368

☑	FILE NAME	MIME TYPE	FILE SIZE	HASHES
☑	727705-107-0_2.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6
☑	727705-107-0_3.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6
☑	727705-107-0_1.__utm.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data.

35 of 20336 events

EVENT META

SESSIONID	727705
TIME	02/26/2018 09:40:43 am
SIZE	64590
PAYLOAD	51870
MEDIUM	1
ETH.SRC	[redacted]:1A
ETH.SRC.VENDOR	VMware, Inc.
ETH.DST	[redacted]:97
ETH.DST.VENDOR	VMware, Inc.
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	27
TCP.FLAGS.SEEN	fin syn psh ack
TCP.SRCPORT	49261
TCP.DSTPORT	80
SERVICE	80
STREAMS	2

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`.

Export or Print a Drill Point in the Navigate View

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

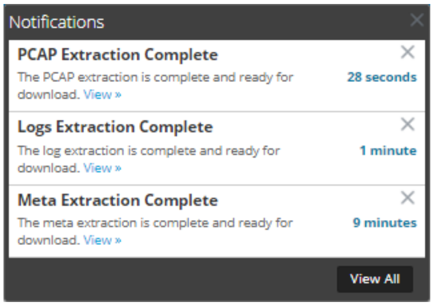
- Extract files from a session and choose the type of files to extract: archives, audio BitTorrent, documents, executable, images, other, video, and web.
- Export the drill point as a packet capture (PCAP) file, a log file, or a metadata file.
- Print the drill point.

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.



PCAP Extraction Complete
The PCAP extraction is complete and ready for download. View »
28 seconds

Logs Extraction Complete
The log extraction is complete and ready for download. View »
1 minute

Meta Extraction Complete
The meta extraction is complete and ready for download. View »
9 minutes

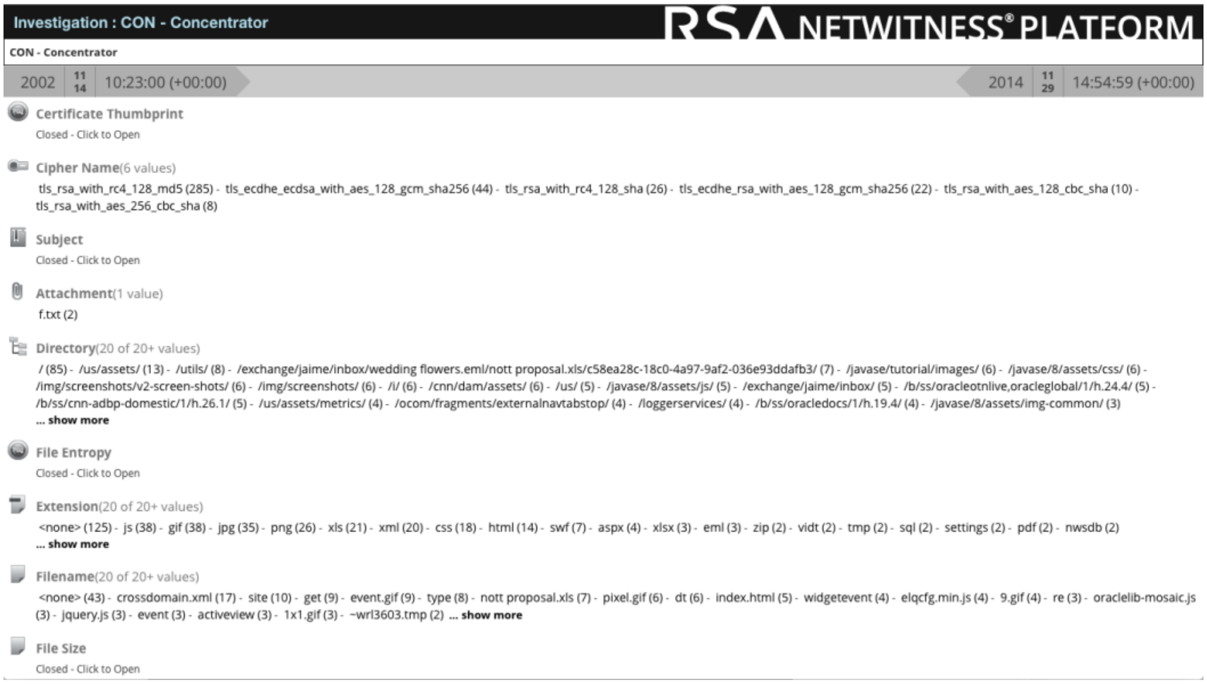
6. Click the **View** link in the Jobs tray and download the specific extraction file requested.

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.



Certificate Thumbprint
Closed - Click to Open

Cipher Name(6 values)
tls_rsa_with_rc4_128_md5 (285) - tls_ecdhe_ecdsa_with_aes_128_gcm_sha256 (44) - tls_rsa_with_rc4_128_sha (26) - tls_ecdhe_rsa_with_aes_128_gcm_sha256 (22) - tls_rsa_with_aes_128_cbc_sha (10) - tls_rsa_with_aes_256_cbc_sha (8)

Subject
Closed - Click to Open

Attachment(1 value)
f.txt (2)

Directory(20 of 20+ values)
/ (85) - /us/assets/ (13) - /utils/ (8) - /exchange/jaime/inbox/wedding flowers.eml/nott proposal.xls/c58ea28c-18c0-4a97-9af2-036e93ddafb3/ (7) - /javase/tutorial/images/ (6) - /javase/8/assets/css/ (6) - /img/screenshots/v2-screen-shots/ (6) - /img/screenshots/ (6) - /i/ (6) - /cnn/dam/assets/ (6) - /us/ (5) - /javase/8/assets/js/ (5) - /exchange/jaime/inbox/ (5) - /b/ss/oracleotnlive,oracleglobal/1/h.24.4/ (5) - /b/ss/cnn-adbp-domestic/1/h.26.1/ (5) - /us/assets/metrics/ (4) - /ocom/fragments/externalnavtabstop/ (4) - /loggerservices/ (4) - /b/ss/oracledocs/1/h.19.4/ (4) - /javase/8/assets/img-common/ (3)
... show more

File Entropy
Closed - Click to Open

Extension(20 of 20+ values)
<none> (125) - js (38) - gif (38) - jpg (35) - png (26) - xls (21) - xml (20) - css (18) - html (14) - swf (7) - aspx (4) - xlsx (3) - eml (3) - zip (2) - vidt (2) - tmp (2) - sql (2) - settings (2) - pdf (2) - nwsdb (2)
... show more

Filename(20 of 20+ values)
<none> (43) - crossdomain.xml (17) - site (10) - get (9) - event.gif (9) - type (8) - nott proposal.xls (7) - pixel.gif (6) - dt (6) - index.html (5) - widgetevent (4) - elqcfg.min.js (4) - 9.gif (4) - re (3) - oraclelib-mosaic.js (3) - jquery.js (3) - event (3) - activeview (3) - 1x1.gif (3) - ~wrl3603.tmp (2) **... show more**

File Size
Closed - Click to Open

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

Export Events in the Legacy Events View

In the Legacy 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.

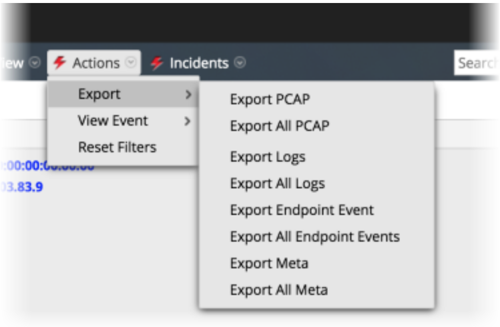
The export function queries the service for all sessions inside the selected time range and drill point to extract the content of each session. The details being exported are affected by both the time range and drill point at the time of exporting. In the File Extraction dialog, you can choose to export:

- 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.**.



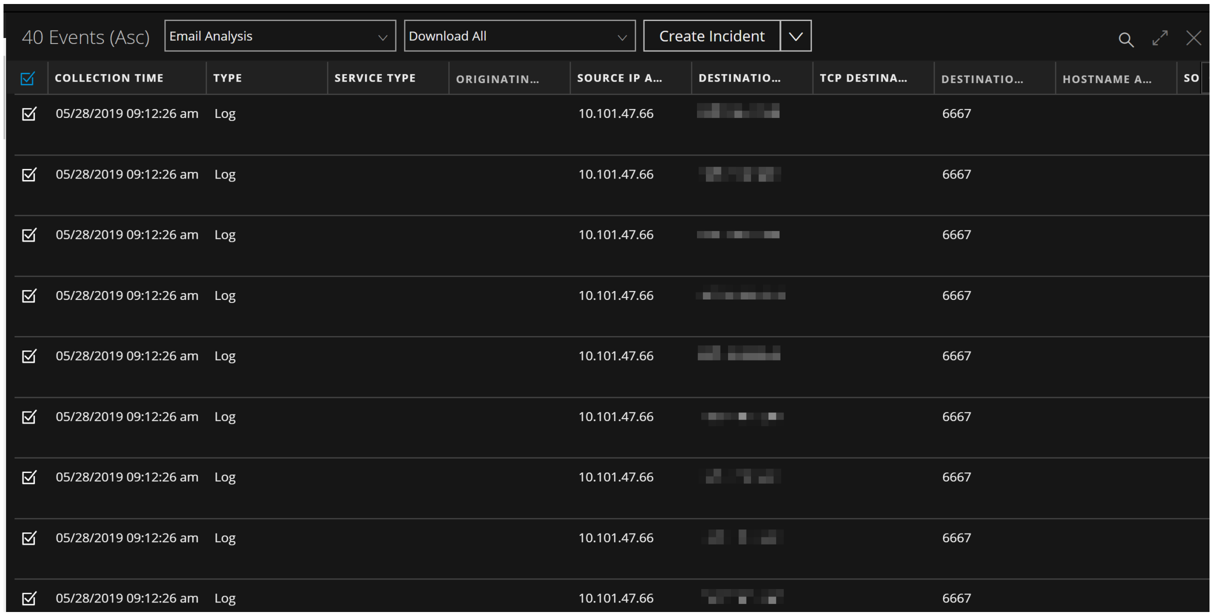
3. Select the export option.
   A message informs you that the PCAP is being downloaded.

Add Events to an Incident in the Events View

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. When you create an incident, if access restrictions are in effect, you can view only incidents to which you have access. For example, when creating incidents from the Investigate view, analysts must assign the incidents to themselves to view them in the Respond view. You can also add events to an existing incident in Respond to which you have access.

Note: An administrator must configure the `respond-server.incident.manage` and `investigate-server.incident.manage` roles and permissions. For more information, see "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

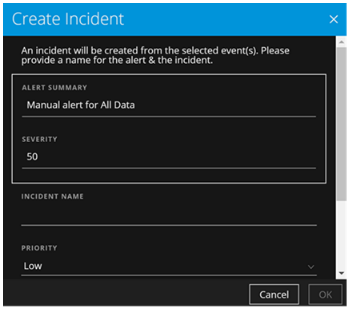
1. Go to **Investigate** > **Events**.
2. In the Events view, select one or more events.



40 Events (Asc) | Email Analysis | Download All | Create Incident

☑	COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATIN...	SOURCE IP A...	DESTINATIO...	TCP DESTINA...	DESTINATIO...	HOSTNAME A...	SO
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		
☑	05/28/2019 09:12:26 am	Log			10.101.47.66	[redacted]		6667		

3. Click **Create Incident.**
   The Create Incident dialog is displayed. Complete the information in the Create Incident dialog.



Create Incident

An incident will be created from the selected event(s). Please provide a name for the alert & the incident.

ALERT SUMMARY
Manual alert for All Data

SEVERITY
50

INCIDENT NAME

PRIORITY
Low

a. Select the severity. The alert summary field is a pre-defined value which is auto-populated but can be edited if required.

b. Type a name for the incident in the **Incident Name** field.

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

d. Select an assignee for the incident from the drop-down list. This list includes the built-in users that have access to Investigate as well as any custom users that have been added to your system. For example, this list might include users for admin, analyst, dpo, operator, and users for incident responders.

e. From the Categories drop-down list, select one or more categories of events that apply to this incident.

f. Click **OK**.
An incident is created with the selected event in Investigate.

4. To add one or more events to an existing incident, select one or more events, and then click **Add to Incident**.

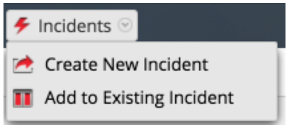
5. In the Add to Incident dialog, select the alert summary and severity, and select one or more open and existing incidents to which the incidents will be added. You can Search for an existing incident by Incident-ID or Incident Name. When ready, click **OK**. The event is added to the selected incidents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

Add Events to an Incident in the Legacy Events View

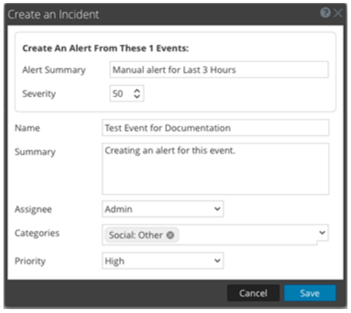
When conducting an investigation in the Legacy Events, you can select one or more events and create an incident that is available for incident responders in Respond. When you create an incident, if access restrictions are in effect, you can view only incidents to which you have access. For example, when creating incidents from the Investigate view, analysts must assign the incidents to themselves to view them in the Respond view. 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** > **Legacy Events**.
2. In the Legacy Events view, select one or more events, and then **Incidents** > **Create New Incident**.



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



Create An Alert From These 1 Events:
Alert Summary: Manual alert for Last 3 Hours
Severity: 50
Name: Test Event for Documentation
Summary: Creating an alert for this event.
Assignee: Admin
Categories: Social: Other
Priority: High

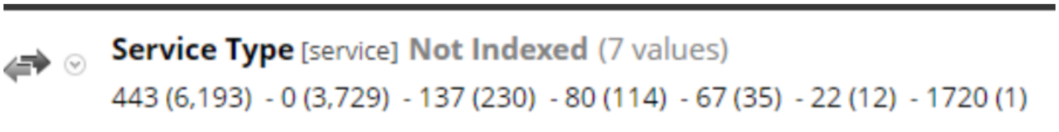
   a. Select the severity, an integer between 1 and 100, with 100 being the most severe.
   b. Type a name for the incident and describe the incident in the **Summary** field.
   c. Select an assignee for the incident from the drop-down list. This list includes the built-in roles that have access to Respond 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.

Troubleshooting NetWitness Investigate

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

Navigate View and Legacy Events View Issues

Behavior	A meta key that normally returns values in the Navigate view returns values, but has a `Not Indexed` message following the meta key name. For example, the in this figure the Service Type meta key is followed by the message: `Service Type[service] Not Indexed`.  **Service Type** [service] **Not Indexed** (7 values) 443 (6,193) - 0 (3,729) - 137 (230) - 80 (114) - 67 (35) - 22 (12) - 1720 (1)
Issue	When you first set up the environment or very rarely after performing a data reset on the broker due to other issues, you see meta keys as Not Indexed when they are indexed at meta key or meta values level.
Explanation	To fix the issue on a Broker, log out of NetWitness Platform and then log in again. Valid sessions will be displayed.

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 Legacy Events view.

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

Events View Issues

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 Events 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.

Behavior	Download jobs are in a Waiting state or Failed state in the Jobs tray during and after upgrading the software to Version 11.4.
Issue	If you had download jobs running while your administrator was upgrading the software, you may see a job in a Waiting state while the upgrade is in progress and then in a Failed state after the upgrade is complete. You cannot resume or cancel the failed job.
Explanation	To delete the failed jobs, select the failed jobs in the Jobs tray and click — .

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 Events. 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 Events view, the view opens with the message.
Explanation	Your administrator has prevented access to the Events view using role and permissions.

Behavior	If you can download an event in the Events view, but get a 0-byte file, the administrator may have restricted access to the content.
Issue	Role-Based Access Controls applied by your administrator allowed you to download an event for which you did not have permission; therefore, the file download was empty.
Explanation	If you believe you should have access to the event, contact your administrator.

Message	`Insufficient permissions for the requested data.`
Issue	While attempting to access an event in the Events view, 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.

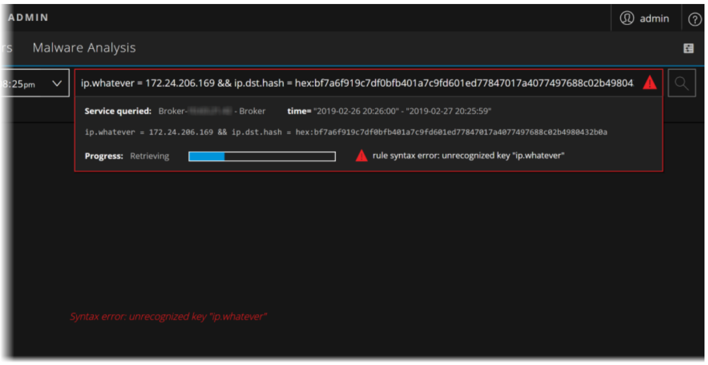
Behavior	Investigation Profiles and built-in column groups are not present in 11.1 Event Analysis.
Issue	Post upgrade to RSA NetWitness v11.1, the default column groups - Endpoint Analysis, Outbound SSL and Outbound HTTP are not added under column groups. Also, a few of the Investigation Profiles are missing post upgrade.
Explanation	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 built-in 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	`Memory limit of <XXXXXX> GB reached, controlled by setting max.query.memory`
Issue	The query that you submitted failed because the result set was too large, and the memory limit set by `max.query.memory` was reached.
Explanation	To avoid this error, try to further limit results by narrowing the time range, adding filters, and decreasing the number of columns in the column group. You can also ask an administrator to limit the number of events returned.

Behavior	No text data was generated during content reconstruction. This could mean that the event data was corrupt or 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 Events view, no data is displayed and the message is displayed.
Explanation	If you do not see the raw text in other Events views or Legacy 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 Events view.  ip.whatever = 172.24.206.169 && ip.dst.hash = hex:bf7a6f919c7df0bfb401a7c9fd601ed77847017a4077497688c02b49804 **Service queried:** Broker-[redacted] - Broker **time=** "2019-02-26 20:26:00" - "2019-02-27 20:25:59" `ip.whatever = 172.24.206.169 && ip.dst.hash = hex:bf7a6f919c7df0bfb401a7c9fd601ed77847017a4077497688c02b4980432b0a` **Progress:** Retrieving ▭ rule syntax error: unrecognized key "ip.whatever" *Syntax error: unrecognized key "ip.whatever"*
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*.

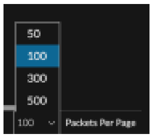
Message	`Selected Column Group is no longer available. The default summary column group has been selected instead.`
Issue	If you had set a preferred column group before the 11.4 upgrade, on your first visit to the Events view, the flash message is displayed even when the column group is available or is the default group (summary). This issue was resolved in Version 11.4.1.
Explanation	This is a one-time occurrence. If you reload the Events view, the message is not displayed.

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 query on channel <channel-number> was auto-canceled by the system for exceeding time usage limits. Check timeout values. Query running time was 00:05:00 (HH:MM:SS)`
Issue	If you continually get this timeout message, first check the query console to determine if there are issues around time it takes for a service to respond, index error messages, or other warnings that may need to be addressed to increase query response time.
Explanation	If there are no messages indicating any specific warnings, ask your administrator to increase the Core Query Timeout from 5 minutes to 10 minutes as described in the *System Security and User Management Guide*.

Message	`The session id is too large to be handled:<<eventId>`
Issue	The session id that you typed in, or got from the Legacy Events view or Navigate view is too large.
Explanation	If you manually typed the sessionId or edited a sessionId in the Events view, you may have created an integer that is too large for Events to process.

Behavior	When reconstructing network events with a large number of packets (>250) in the Events view > Packets panel, with the option to display only payloads enabled and the packets per page setting higher than the default (100), the current browser tab may become unresponsive for up to 45 seconds as it is working to render the payloads.
Issue	Depending on the amount of resources (memory and CPU) on the client machine and the

Explanation	number of packets in the event there may be a performance lag when displaying only payloads in packet reconstruction.
	To limit the amount of data processed in a reconstruction of a single event, change the Packets per Page setting in the footer to a lower value. 

Behavior	When working in the Version 11.4 Events view, the Query Profile drop-down menu and Column Group drop-down menu do not function.
Issue	You do not have permission to read columns groups and profiles. The default column group , Summary List, is applied to the Events list, and you cannot change the column group, create a column group, or delete a column group.
Explanation	This occurs only when the administrator has created a custom role for you instead of assigning the default Analyst role. Ask your administrator to enable column group read and profile read permission for your role.

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.

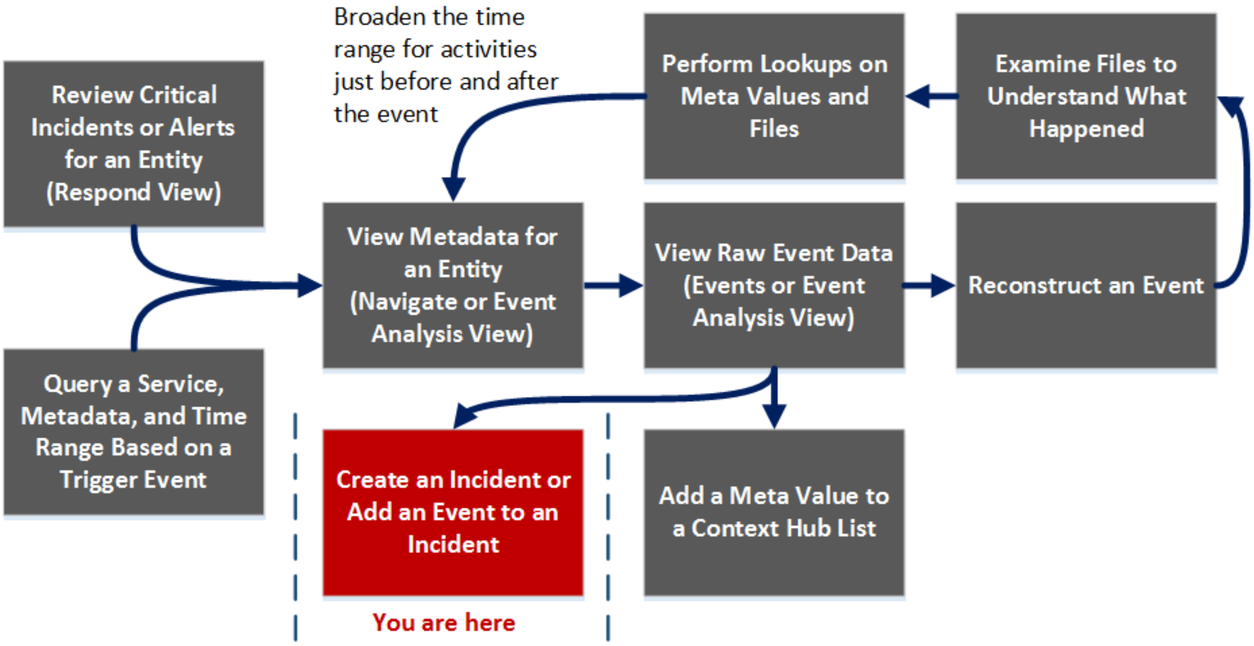
- Investigate View
- Navigate View
- Legacy Events View
- Events View
- Add/Remove from List Dialog
- Add Events to an Incident Dialog
- Column Groups Dialogs
- Context Lookup Panel
- Create an Incident Dialog
- Events View - Email Panel
- Events View - Text Panel
- Events View - Packet Panel
- Events View - File Panel
- Investigate Dialog
- Investigation Tab - User Preferences Panel
- Legacy Event Reconstruction View
- Manage Default Meta Keys Dialog
- Manage Meta Groups Dialog
- Navigate View
- Query Dialog
- Query Profiles Dialogs
- 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 and the Legacy Events view, see Add Events to an Incident in the Events View and Add Events to an Incident in the Legacy Events View..

Workflow

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Create an Incident or Add an Event to an Incident
You are here
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View

User Role	I want to ...	Show me how
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

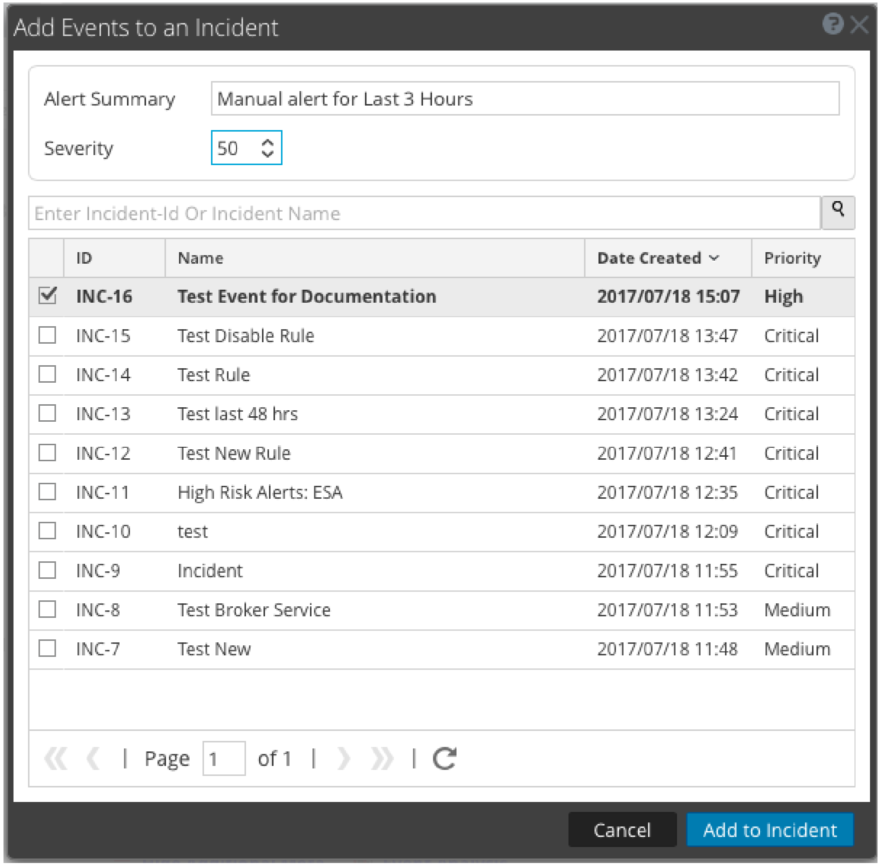
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View
- Legacy Events View

Quick Look

The following figure is an example of the Add Events to an Incident dialog in the Legacy Events. The table describes the information and options in the Add Events to an Incident dialog .



Add Events to an Incident

Alert Summary: Manual alert for Last 3 Hours

Severity: 50

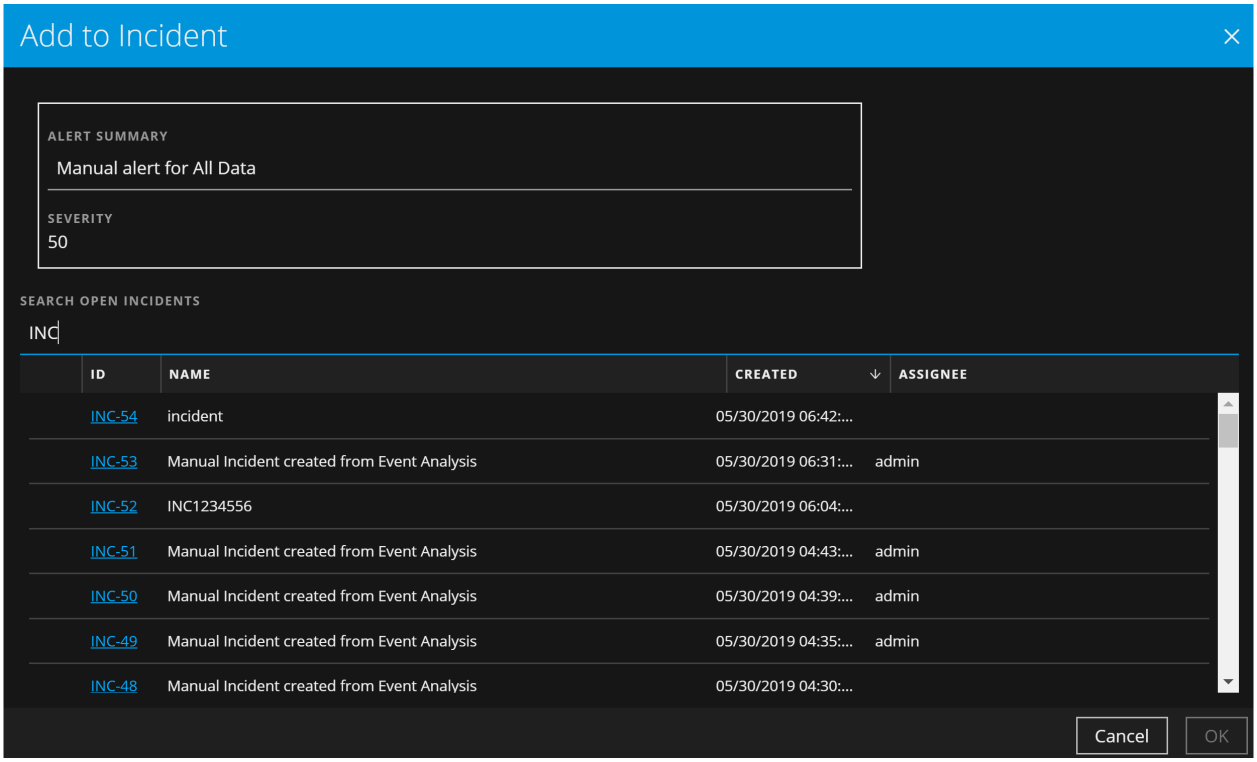
Enter Incident-Id Or Incident Name

	ID	Name	Date Created	Priority
☑	**INC-16**	**Test Event for Documentation**	**2017/07/18 15:07**	**High**
□	INC-15	Test Disable Rule	2017/07/18 13:47	Critical
□	INC-14	Test Rule	2017/07/18 13:42	Critical
□	INC-13	Test last 48 hrs	2017/07/18 13:24	Critical
□	INC-12	Test New Rule	2017/07/18 12:41	Critical
□	INC-11	High Risk Alerts: ESA	2017/07/18 12:35	Critical
□	INC-10	test	2017/07/18 12:09	Critical
□	INC-9	Incident	2017/07/18 11:55	Critical
□	INC-8	Test Broker Service	2017/07/18 11:53	Medium
□	INC-7	Test New	2017/07/18 11:48	Medium

Page 1 of 1

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

The following figure is an example of the Add to Incident dialog in the Events view. The table describes the information and options in the Add to Incident dialog.



ALERT SUMMARY
Manual alert for All Data

SEVERITY
50

SEARCH OPEN INCIDENTS
INC

ID	NAME	CREATED ↓	ASSIGNEE
INC-54	incident	05/30/2019 06:42:...	
INC-53	Manual Incident created from Event Analysis	05/30/2019 06:31:...	admin
INC-52	INC1234556	05/30/2019 06:04:...	
INC-51	Manual Incident created from Event Analysis	05/30/2019 04:43:...	admin
INC-50	Manual Incident created from Event Analysis	05/30/2019 04:39:...	admin
INC-49	Manual Incident created from Event Analysis	05/30/2019 04:35:...	admin
INC-48	Manual Incident created from Event Analysis	05/30/2019 04:30:...	

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.
Severity	The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.
Search Open Incidents	Allows you to search for an existing incidents.
ID	The ID of the incident.
Name	The incident name.
Created	Displays the date and time the incident was created.
Assignee	Displays the team member currently assigned to the incident
Cancel	Closes the dialog without saving changes.
OK	Adds the alerts to the incident. A confirmation message is displayed after the incident is 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.

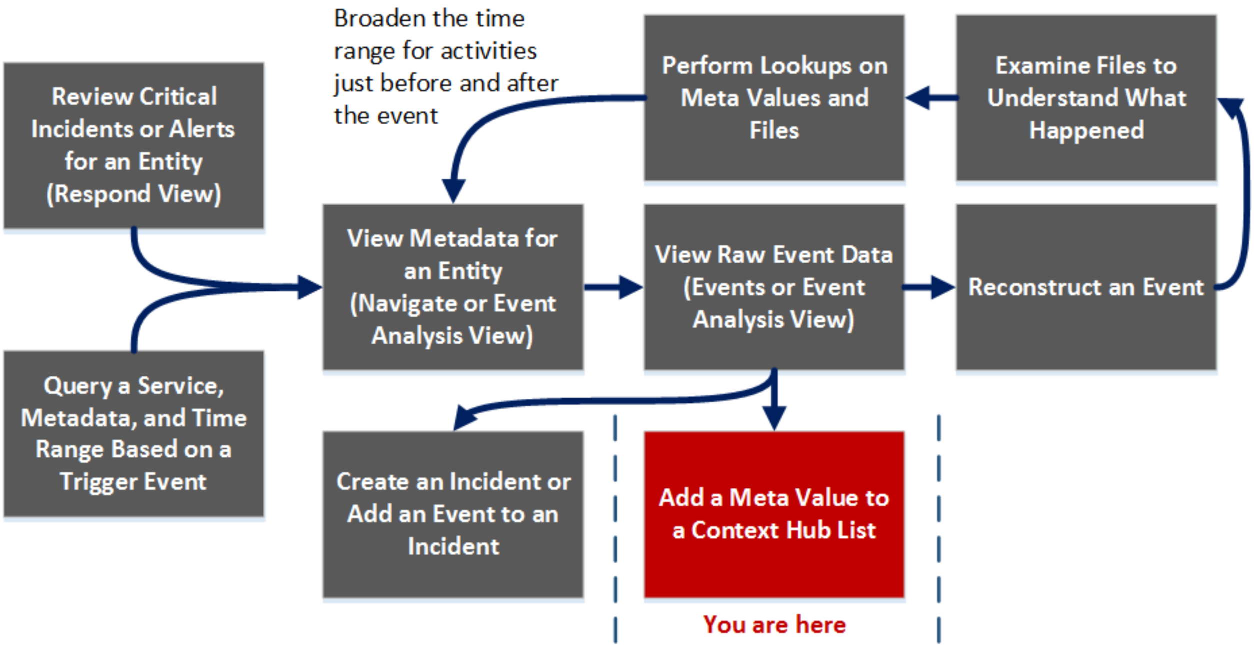
You can add entities or meta values to more than one list. For example, you can add them to one list for suspected domains related to command and control connections and to another list for Trojan connection IP addresses related to remote access. If a list is not available, you can create a list.

The dialog is available in NetWitness Investigate and in NetWitness Respond. When working in Investigate, in the Navigate view, Legacy Events view, or Events view, 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 Legacy 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 Events 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. This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
Broaden the time range for activities just before and after the event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List
You are here

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View

User Role	I want to ...	Show me how
Threat Hunter	examine files	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context for Results

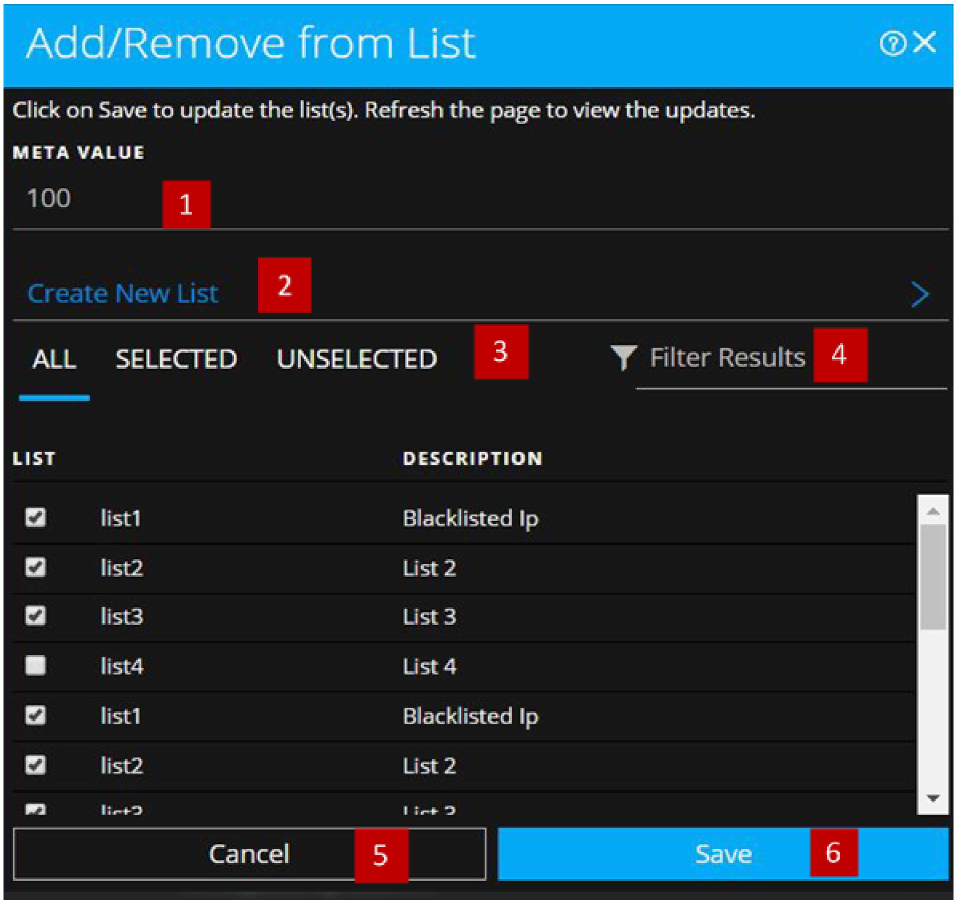
*You can perform this task in the current view.

Related Topics

- Look Up Additional Context for Results
- Navigate View
- Legacy Events View
- Events View

Quick Look in the Events View

The following is an example of the **Add/Remove from List** dialog in the Events view.



Click on Save to update the list(s). Refresh the page to view the updates.

META VALUE

100

	LIST	DESCRIPTION
☑	list1	Blacklisted Ip
☑	list2	List 2
☑	list3	List 3
□	list4	List 4
☑	list1	Blacklisted Ip
☑	list2	List 2
☑	list3	List 3

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.

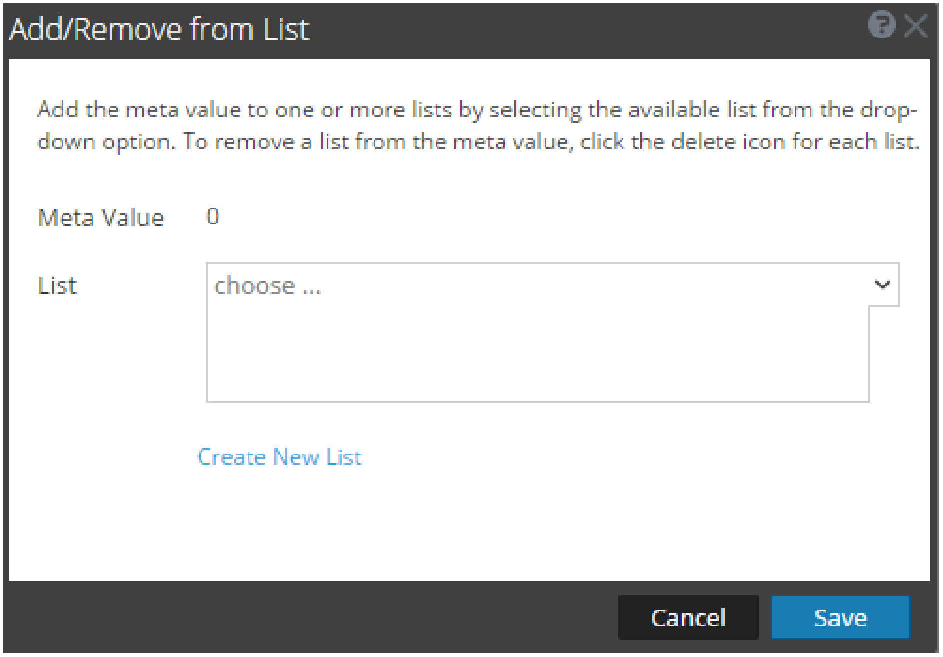
The following table shows the options in the Add/Remove from List dialog.

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.

Quick Look in the Navigate and Legacy Events Views

The following figure is an example of the Add/Remove from List dialog when initially opened.



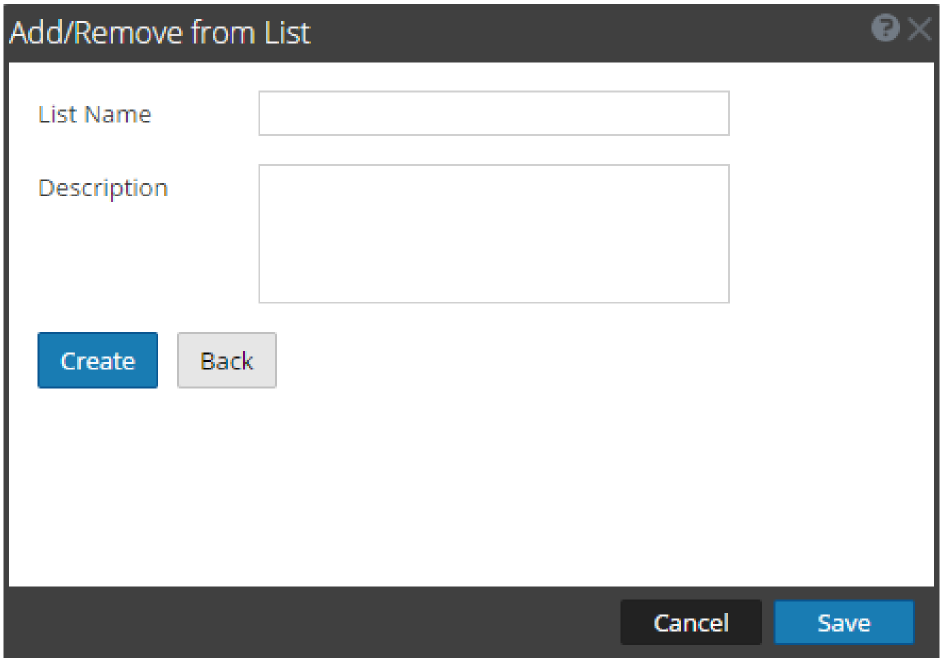
Add/Remove from List

Add the meta value to one or more lists by selecting the available list from the drop-down option. To remove a list from the meta value, click the delete icon for each list.

Meta Value 0

List choose ...

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.

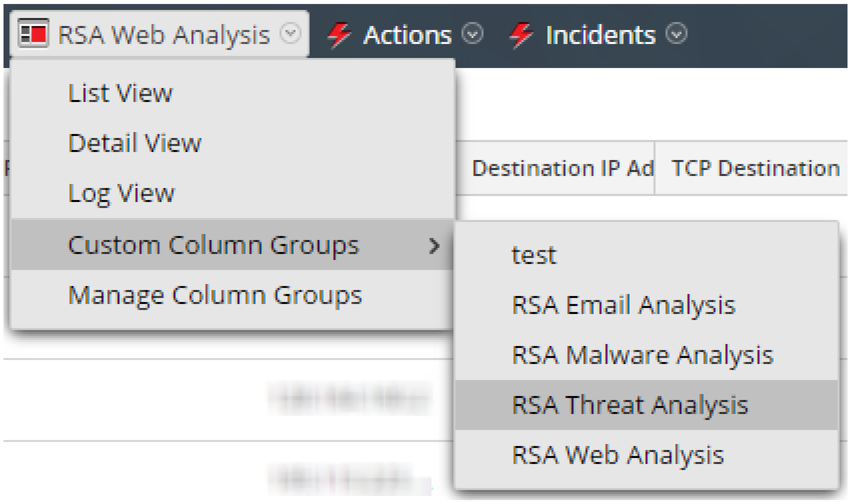
Feature	Description
Meta Value	The selected meta value to be added to the existing or new list.
List	The list to which the selected meta value must be added. A drop-down menu provides a list of available lists to which you can add the meta value.
Create New List	Opens a new dialog in which you can create 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.

Column Groups Dialogs

Column groups allow you to format the events list to include only the relevant meta keys in the Events view and Legacy Events view (see Use Columns and Column Groups in the Events List). When the events list in Investigate is populated with events, each column lists the values returned for a meta key. Changing the meta keys displayed in the events list is a useful method of narrowing the focus of your investigation. For example, the default column group includes columns for **Collection Time**, **Type**, **Theme**, **Size**, and **Summary**. These are just the basic information, not specialized in any way. The RSA Email Analysis list has only that contain information useful when investigating email.

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, built-in column groups are available. The built-in column groups are prefixed with RSA and can be duplicated but cannot be edited or deleted. You can also create custom column groups.

- The Create Column Group dialog is for the 11.4 Events view. To access this dialog, select **Column Group > New Column Group** in the **Events** view toolbar.
- The Column Group Details dialog is for the 11.4 Events view. To access this dialog, select **Column Group** in the **Events** view toolbar, then click the edit icon (🖉) next to a custom column group name.
- The Manage Column Groups dialog is for the Legacy Events view (Version 11.4) , and the Events view (Version 11.4 and earlier). The Manage Column Groups dialog has one feature that is not yet available in the Create Column Group dialog: set column width, import, and export. To access this dialog, go to **Investigate > Legacy 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.



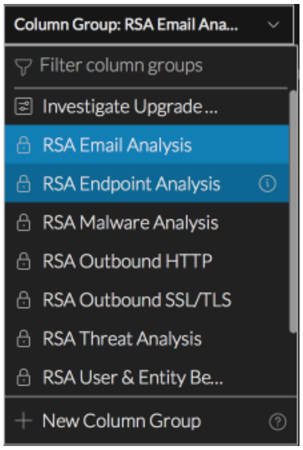
After column groups are defined, you can use them in other Investigate views. In the Navigate view, Profiles allow you to select a column group to use when the profile is applied. In the Events view amd the Legacy Events view, you can select a column group to apply to the Events panel.

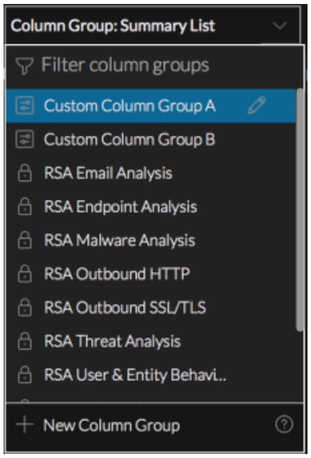
Related Topics

- How NetWitness Investigate Works
- Events View
- Legacy Events View

Quick Look - Column Group Menu, Create Column Group Dialog, and Column Group Details Dialog

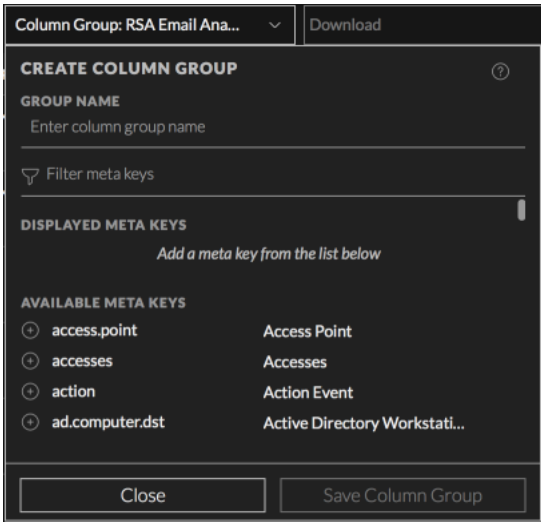
This section introduces the Column Group Menu, Create Column dialog, and the Column Group Details dialog. The following figures are examples of the Column Group menu. The example on the left has a built-in column group highlighted so that the information icon is visible. Notice the color difference between the highlighted column group (RSA Endpoint Analysis) versus the selected column group (RSA Email Analysis). The example on the right has a custom column group highlighted so that the edit icon is visible. The table describes the options.





Feature	Description
Filter Column Groups	Filters the list of column groups as you type text so that only group names that contain that text are displayed.
Column Group List	The list of column groups consists of custom and built-in groups, which are distinguished by the icons that precede the name. In the second example, Custom Column Group A and Custom Column Group B are custom column groups. The RSA column groups are built-in column groups.
New Column Group	Displays the Create Column Group dialog, where you can create a custom column group.

The Create Column Group dialog, shown in the figure on the left, allows you to define a custom column group. The figure on the right illustrates the Column Group Details dialog, in which you can edit a custom column group. The table describes the fields and options in the dialogs.



Column Group: RSA Email Ana... | Download

CREATE COLUMN GROUP

GROUP NAME

Enter column group name

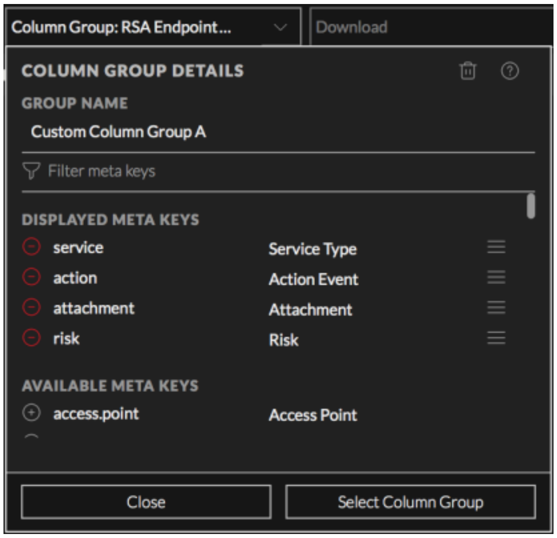
Filter meta keys

DISPLAYED META KEYS

Add a meta key from the list below

AVAILABLE META KEYS

⊕ access.point	Access Point
⊕ accesses	Accesses
⊕ action	Action Event
⊕ ad.computer.dst	Active Directory Workstati...



Column Group: RSA Endpoint... | Download

COLUMN GROUP DETAILS

GROUP NAME

Custom Column Group A

Filter meta keys

DISPLAYED META KEYS

⊖ service	Service Type
⊖ action	Action Event
⊖ attachment	Attachment
⊖ risk	Risk

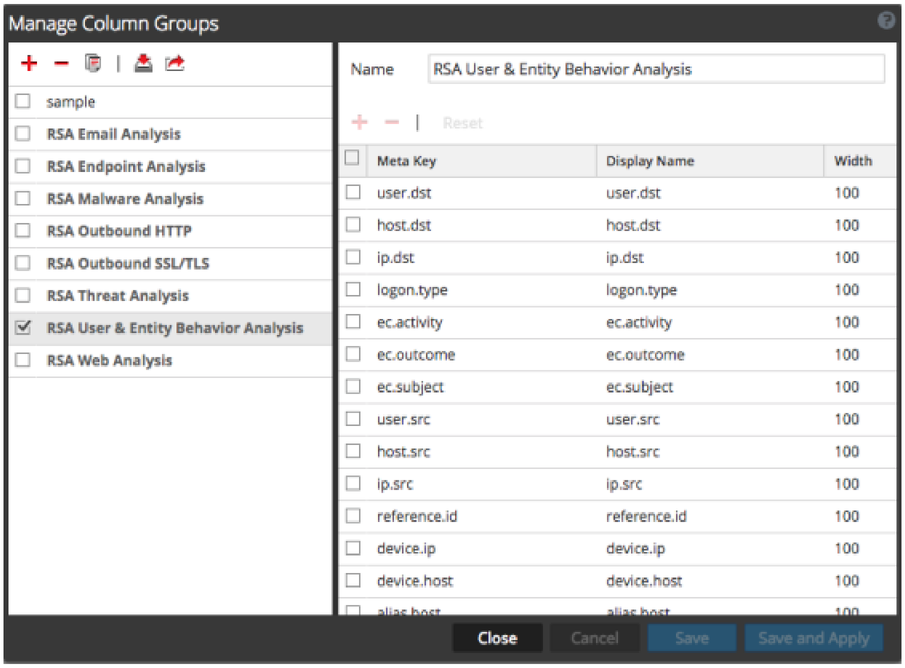
AVAILABLE META KEYS

⊕ access.point	Access Point

Feature	Description
🗑	Deletes the custom column group in the Column Group Details dialog. This action is irreversible and applies globally; the column group is no longer available to anyone who is using it on this service.
Group Name	Displays the name of the column group. The name must be unique and contain fewer than 64 characters. You can type in this field to edit the name in a custom column group.
Filter Meta Keys	Filters the Displayed Meta Keys and Available Meta Keys based on the text that you type. Only meta keys that contain the typed text are displayed.
Displayed Meta Keys	Displays a scrollable list of meta keys that are selected for use in the custom column group. You can add meta keys in the Available Meta Keys list to this list, remove meta keys from this list ⊖, and drag meta keys up or down to change the order in this list (≡).
Available Meta Keys	Displays a scrollable list of meta keys that are available (on the service) for use in the custom column group. You can add them to the Available Meta Keys list. Clicking ⊕ next to the meta key name adds it to the Displayed Meta Keys list.
Close button	Closes the dialog.
Save Column Group	For the Create Column Group dialog only, saves the new column group.
Reset	For the Column Group Details dialog only, reverts the edited column group to the last saved state.
Update Column Group	For the Column Group Details dialog only, applies changes to an edited column group.

Feature	Description
Select Column Group	Applies the column group.

Quick Look - Manage Column Groups Dialog



☐ sample
☐ RSA Email Analysis
☐ RSA Endpoint Analysis
☐ RSA Malware Analysis
☐ RSA Outbound HTTP
☐ RSA Outbound SSL/TLS
☐ RSA Threat Analysis
☑ RSA User & Entity Behavior Analysis
☐ RSA Web Analysis

Name: RSA User & Entity Behavior Analysis

☐	Meta Key	Display Name	Width
☐	user.dst	user.dst	100
☐	host.dst	host.dst	100
☐	ip.dst	ip.dst	100
☐	logon.type	logon.type	100
☐	ec.activity	ec.activity	100
☐	ec.outcome	ec.outcome	100
☐	ec.subject	ec.subject	100
☐	user.src	user.src	100
☐	host.src	host.src	100
☐	ip.src	ip.src	100
☐	reference.id	reference.id	100
☐	device.ip	device.ip	100
☐	device.host	device.host	100
☐	alias.host	alias.host	100

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.

Action	Description
➦	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.

Context Lookup Panel

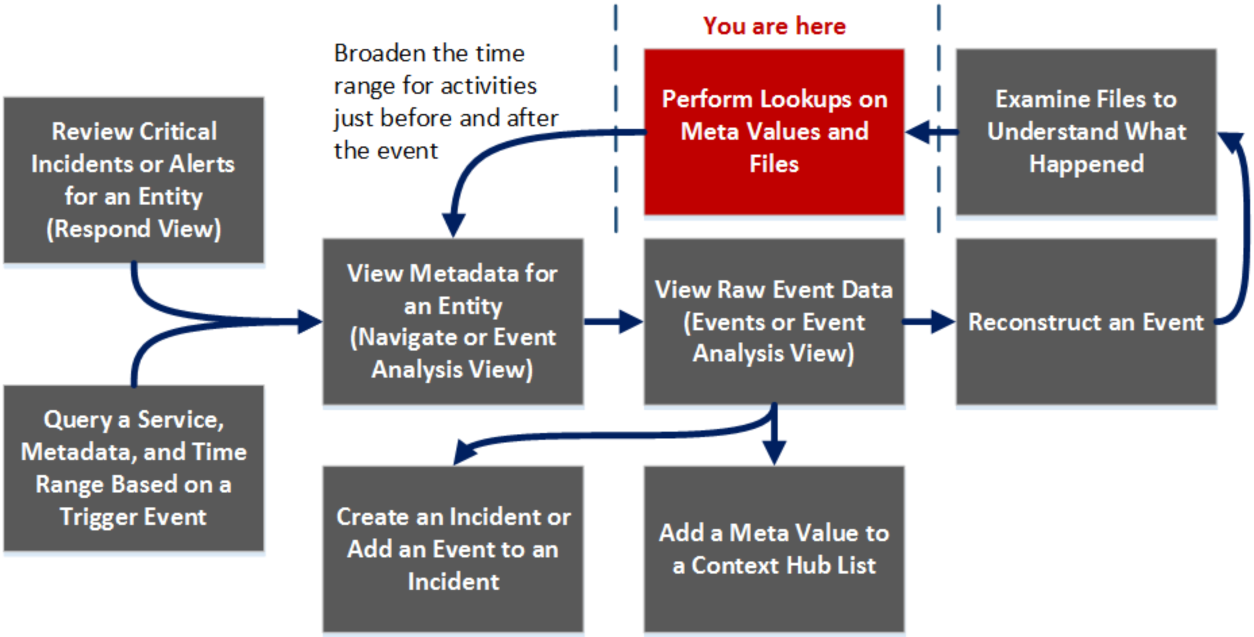
After an administrator configures the Context Hub service, you can view the contextual information for the meta values in the Navigate view, Legacy Events view, and Events view (Version 11.2 and later). The Context Hub service is pre-configured with a default meta type and meta key mapping. For information 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, Legacy Events view, or Events view. Meta values that have been added to a Context Hub list are highlighted in gray in the Navigate view or Legacy Events view results. In the Events 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 Events view.

Workflow

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


You are here
Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
View Raw Event Data (Events or Event Analysis View)
Examine Files to Understand What Happened
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups*	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Legacy Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

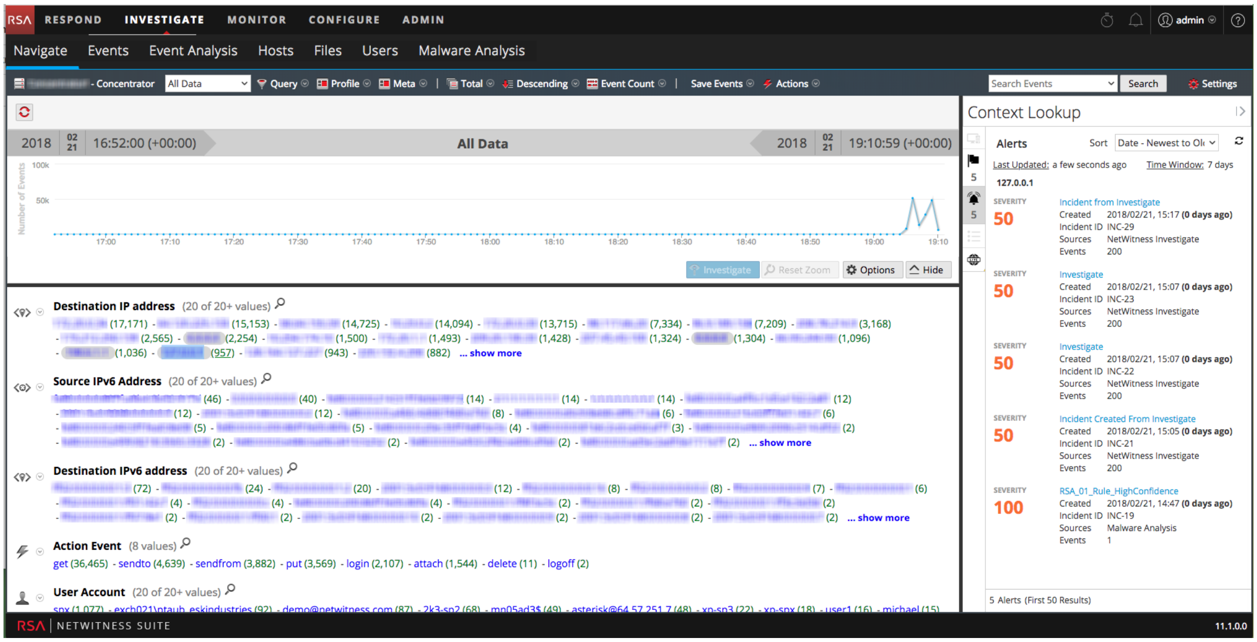
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Legacy Events View
- Navigate View
- Events View
- "NetWitness Feedback and Data Sharing" in the *Live Services Management Guide*

Quick Look (in the Navigate and Legacy Events Views)

The following figure is an example of the Context Lookup panel as it appears in the Navigate view and Legacy Events view. Controls and features are described in the table.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Navigate
Events
Event Analysis
Hosts
Files
Users
Malware Analysis
- Concentrator
All Data
Query
Profile
Meta
Total
Descending
Event Count
Save Events
Actions
Search Events
Search
Settings
2018
02 21
16:52:00 (+00:00)
All Data
2018
02 21
19:10:59 (+00:00)
Number of Events
100k
50k
17:00
17:10
17:20
17:30
17:40
17:50
18:00
18:10
18:20
18:30
18:40
18:50
19:00
19:10
Investigate
Reset Zoom
Options
Hide
Destination IP address (20 of 20+ values)
(17,171) - (15,153) - (14,725) - (14,094) - (13,715) - (7,334) - (7,209) - (3,168) - (2,565) - (2,254) - (1,500) - (1,493) - (1,428) - (1,324) - (1,304) - (1,096) - (1,036) - (957) - (943) - (882) ... show more
Source IPv6 Address (20 of 20+ values)
(46) - (40) - (14) - (14) - (14) - (12) - (12) - (12) - (8) - (6) - (6) - (5) - (5) - (4) - (3) - (2) - (2) - (2) - (2) - (2) ... show more
Destination IPv6 address (20 of 20+ values)
(72) - (24) - (20) - (12) - (8) - (8) - (7) - (6) - (4) - (4) - (4) - (2) - (2) - (2) - (2) - (2) - (2) - (2) - (2) - (2) ... show more
Action Event (8 values)
get (36,465) - sendto (4,639) - sendfrom (3,882) - put (3,569) - login (2,107) - attach (1,544) - delete (11) - logoff (2)
User Account (20 of 20+ values)
spx (1,077) - exch021\ptaub_eskindustries (92) - demo@netwitness.com (87) - 2k3-sp2 (68) - mp05ad3$ (49) - asterisk@64.57.251.7 (48) - xp-sp3 (22) - xp-spx (18) - user1 (16) - michael (15)
Context Lookup
5
5
RSA | NETWITNESS SUITE
11.1.0.0

Alerts Sort Date - Newest to Ol

Last Updated: a few seconds ago Time Window: 7 days

127.0.0.1

SEVERITY	
50	Incident from Investigate Created 2018/02/21, 15:17 **(0 days ago)** Incident ID INC-29 Sources NetWitness Investigate Events 200
50	Investigate Created 2018/02/21, 15:07 **(0 days ago)** Incident ID INC-23 Sources NetWitness Investigate Events 200
50	Investigate Created 2018/02/21, 15:07 **(0 days ago)** Incident ID INC-22 Sources NetWitness Investigate Events 200
50	Incident Created From Investigate Created 2018/02/21, 15:05 **(0 days ago)** Incident ID INC-21 Sources NetWitness Investigate Events 200
100	RSA_01_Rule_HighConfidence Created 2018/02/21, 14:47 **(0 days ago)** Incident ID INC-19 Sources Malware Analysis Events 1

5 Alerts (First 50 Results)

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

Feature	Description
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.
<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

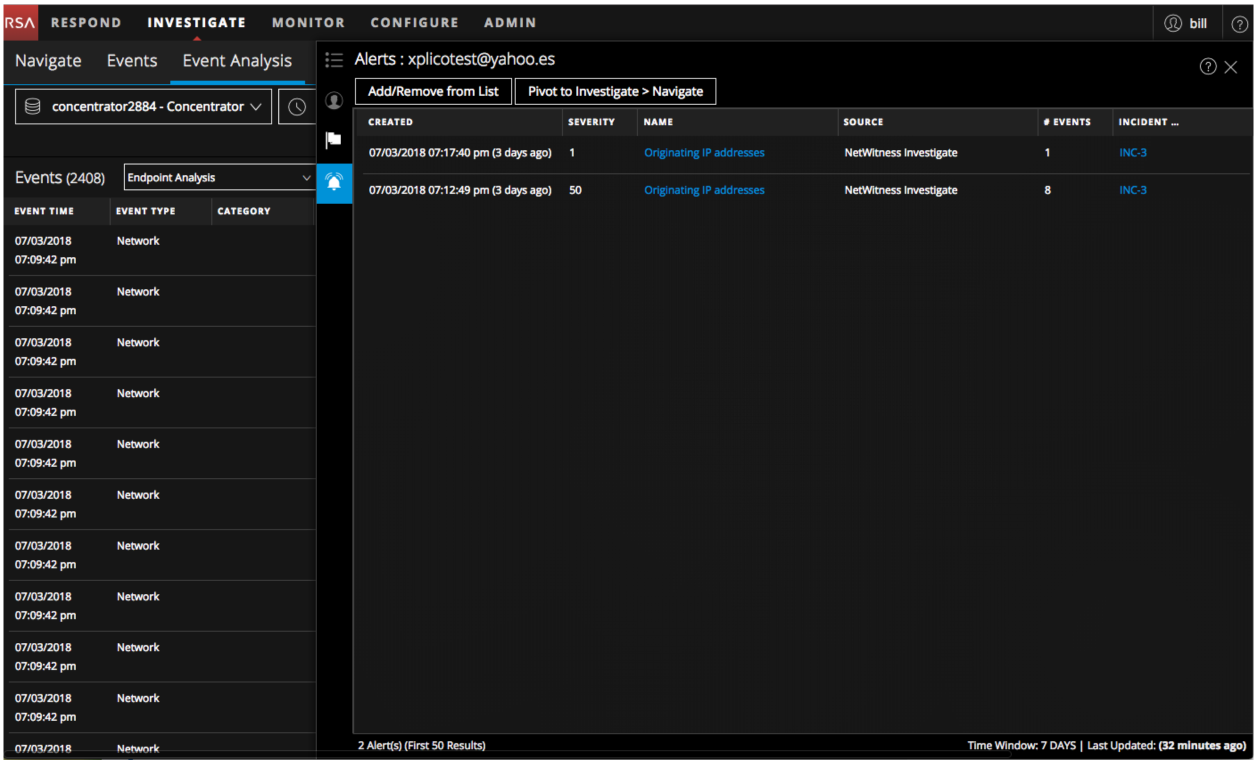
Endpoint

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 Events View (Version 11.2 and Later)

The following figure is an example of the Context Lookup panel as it appears in the Events view.



EVENT TIME	EVENT TYPE	CATEGORY
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018 07:09:42 pm	Network	
07/03/2018	Network	

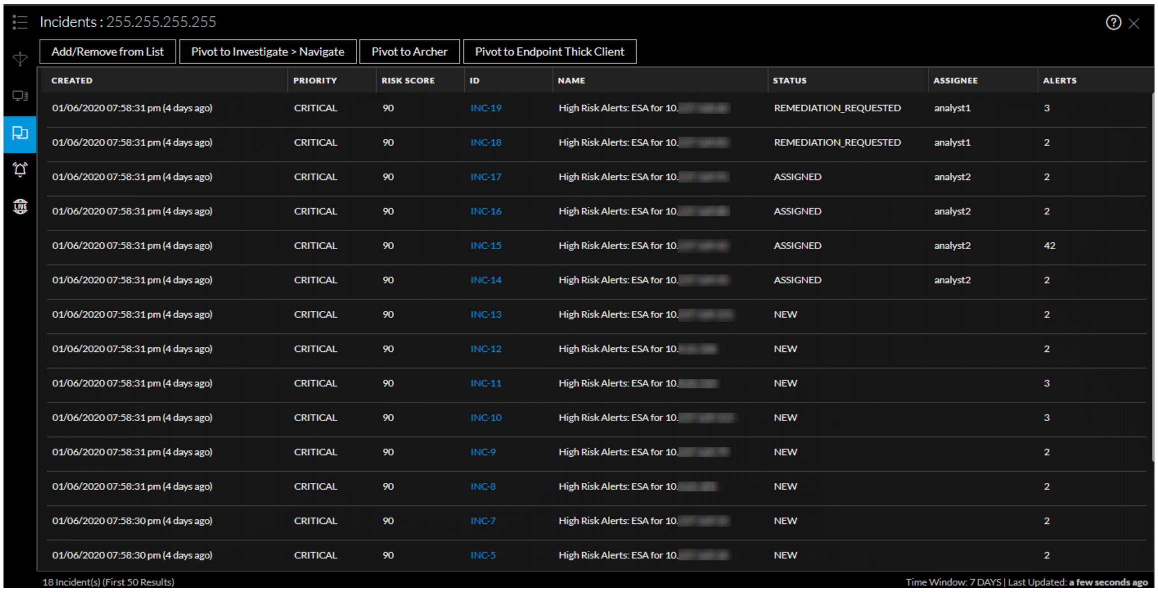
Alerts : xplicotest@yahoo.es

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	INCIDENT ...
07/03/2018 07:17:40 pm (3 days ago)	1	Originating IP addresses	NetWitness Investigate	1	INC-3
07/03/2018 07:12:49 pm (3 days ago)	50	Originating IP addresses	NetWitness Investigate	8	INC-3

2 Alert(s) (First 50 Results)

Time Window: 7 DAYS | Last Updated: **(32 minutes ago)**

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.


Incidents : 255.255.255.255
Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-19	High Risk Alerts: ESA for 10.[redacted]	REMEDIATION_REQUESTED	analyst1	3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-18	High Risk Alerts: ESA for 10.[redacted]	REMEDIATION_REQUESTED	analyst1	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-17	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-16	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-15	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	42
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-14	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-13	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-12	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-11	High Risk Alerts: ESA for 10.[redacted]	NEW		3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-10	High Risk Alerts: ESA for 10.[redacted]	NEW		3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-9	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-8	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:30 pm (4 days ago)	CRITICAL	90	INC-7	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:30 pm (4 days ago)	CRITICAL	90	INC-5	High Risk Alerts: ESA for 10.[redacted]	NEW		2

18 Incident(s) (First 50 Results)

Time Window: 7 DAYS | Last Updated: **a few seconds ago**

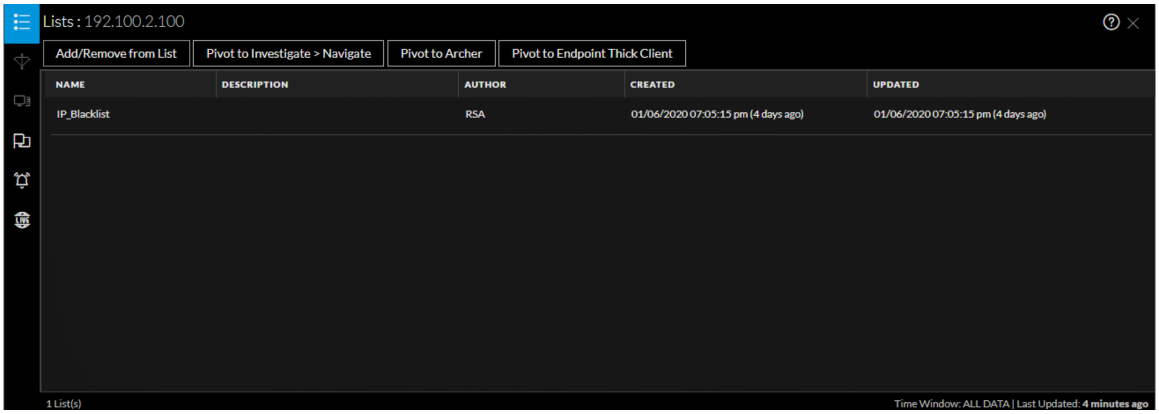
The following table describes the data available on each tab and the supported entities.

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
(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

Tab	Description	Supported Entities
(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 (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.



Lists : 192.100.2.100

Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client

NAME	DESCRIPTION	AUTHOR	CREATED	UPDATED
IP_Blacklist		RSA	01/06/2020 07:05:15 pm (4 days ago)	01/06/2020 07:05:15 pm (4 days ago)

1 List(s)

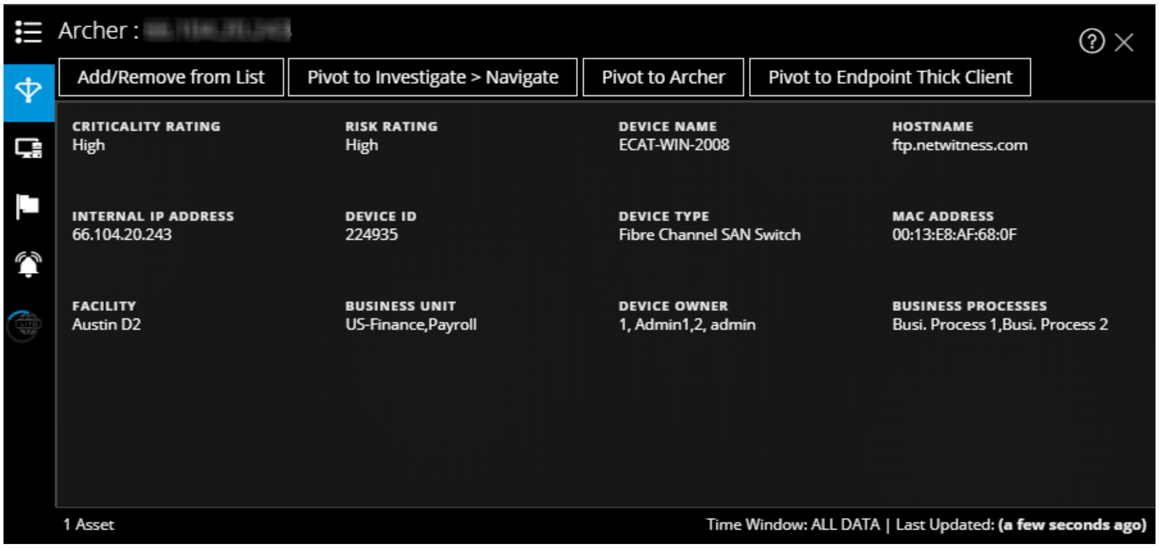
Time Window: ALL DATA | Last Updated: **4 minutes ago**

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.

Field	Description
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.


Archer : [redacted]
Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client

CRITICALITY RATING
High

RISK RATING
High

DEVICE NAME
ECAT-WIN-2008

HOSTNAME
ftp.netwitness.com

INTERNAL IP ADDRESS
66.104.20.243

DEVICE ID
224935

DEVICE TYPE
Fibre Channel SAN Switch

MAC ADDRESS
00:13:E8:AF:68:0F

FACILITY
Austin D2

BUSINESS UNIT
US-Finance,Payroll

DEVICE OWNER
1, Admin1,2, admin

BUSINESS PROCESSES
Busi. Process 1,Busi. Process 2

1 Asset

Time Window: ALL DATA | Last Updated: **(a few seconds ago)**

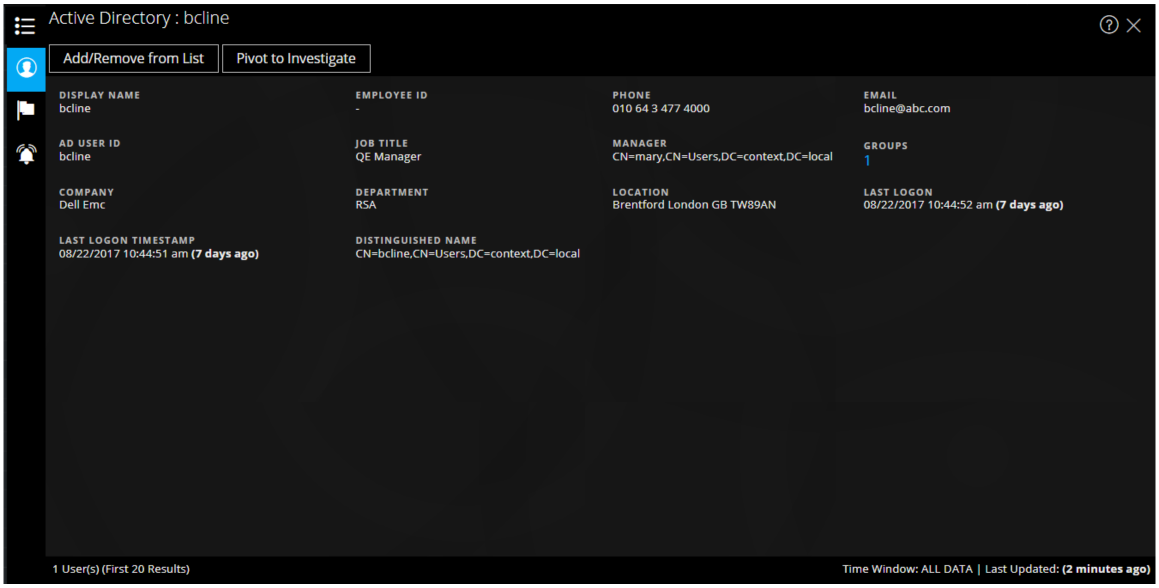
Field	Description
Criticality Rating	The device operational criticality based on the applications it supports. The criticality ratings can be set as Not Rated, Low, Medium-Low, Medium, Medium-High, or High.
Risk Rating	The calculated risk rating for the device based on the most recent assessment and 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.

Field	Description
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.
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.



DISPLAY NAME
bcline

EMPLOYEE ID
-

PHONE
010 64 3 477 4000

EMAIL
bcline@abc.com

AD USER ID
bcline

JOB TITLE
QE Manager

MANAGER
CN=mary,CN=Users,DC=context,DC=local

GROUPS
1

COMPANY
Dell Emc

DEPARTMENT
RSA

LOCATION
Brentford London GB TW89AN

LAST LOGON
08/22/2017 10:44:52 am **(7 days ago)**

LAST LOGON TIMESTAMP
08/22/2017 10:44:51 am **(7 days ago)**

DISTINGUISHED NAME
CN=bcline,CN=Users,DC=context,DC=local

1 User(s) (First 20 Results)

Time Window: ALL DATA | Last Updated: **(2 minutes ago)**

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

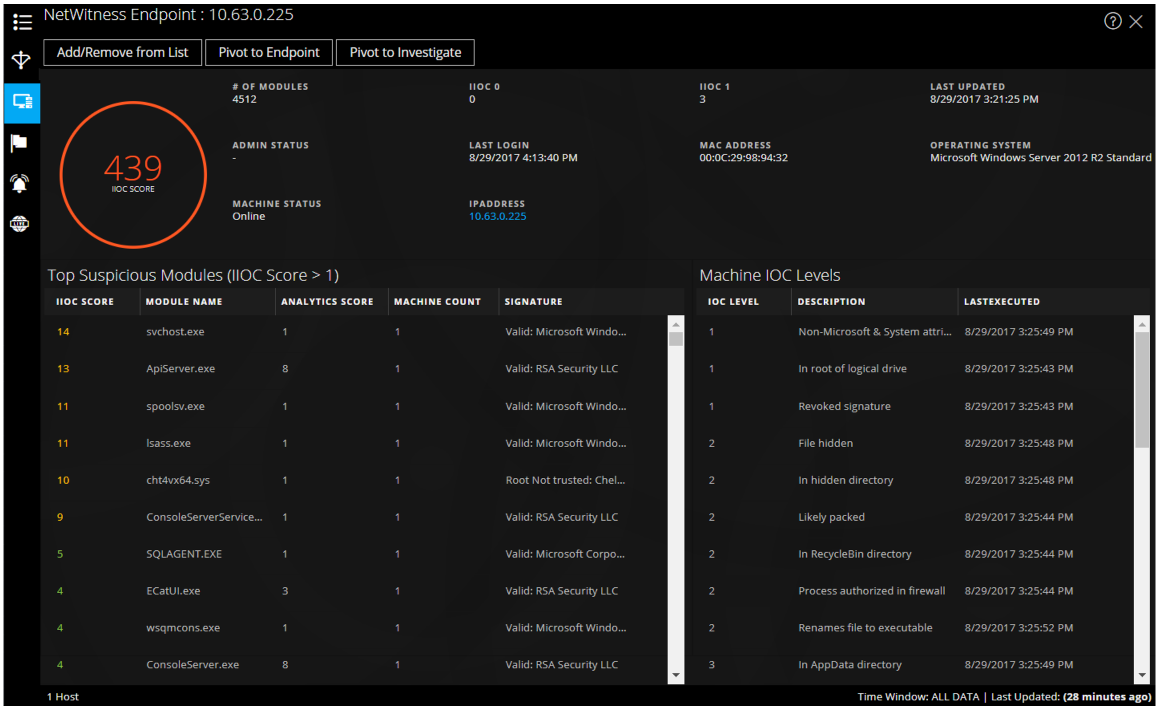
- sAMAccountName

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.
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.



OF MODULES: 4512

IIOC 0: 0

IIOC 1: 3

LAST UPDATED: 8/29/2017 3:21:25 PM

ADMIN STATUS: -

LAST LOGIN: 8/29/2017 4:13:40 PM

MAC ADDRESS: 00:0C:29:98:94:32

OPERATING SYSTEM: Microsoft Windows Server 2012 R2 Standard

MACHINE STATUS: Online

IPADDRESS: 10.63.0.225

Top Suspicious Modules (IIOC Score > 1)

IIOC SCORE	MODULE NAME	ANALYTICS SCORE	MACHINE COUNT	SIGNATURE
14	svchost.exe	1	1	Valid: Microsoft Windo...
13	ApiServer.exe	8	1	Valid: RSA Security LLC
11	spoolsv.exe	1	1	Valid: Microsoft Windo...
11	lsass.exe	1	1	Valid: Microsoft Windo...
10	cht4vx64.sys	1	1	Root Not trusted: Chel...
9	ConsoleServerService...	1	1	Valid: RSA Security LLC
5	SQLAGENT.EXE	1	1	Valid: Microsoft Corpo...
4	ECatUI.exe	3	1	Valid: RSA Security LLC
4	wsqmcons.exe	1	1	Valid: Microsoft Windo...
4	ConsoleServer.exe	8	1	Valid: RSA Security LLC

Machine IOC Levels

IOC LEVEL	DESCRIPTION	LASTEXECUTED
1	Non-Microsoft & System attri...	8/29/2017 3:25:49 PM
1	In root of logical drive	8/29/2017 3:25:43 PM
1	Revoked signature	8/29/2017 3:25:43 PM
2	File hidden	8/29/2017 3:25:48 PM
2	In hidden directory	8/29/2017 3:25:48 PM
2	Likely packed	8/29/2017 3:25:44 PM
2	In RecycleBin directory	8/29/2017 3:25:44 PM
2	Process authorized in firewall	8/29/2017 3:25:44 PM
2	Renames file to executable	8/29/2017 3:25:52 PM
3	In AppData directory	8/29/2017 3:25:49 PM

1 Host

Time Window: ALL DATA | Last Updated: **(28 minutes ago)**

The following information displayed for IIOCs.

Field	Description
# Of Modules	The number modules that are looked up.
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*.

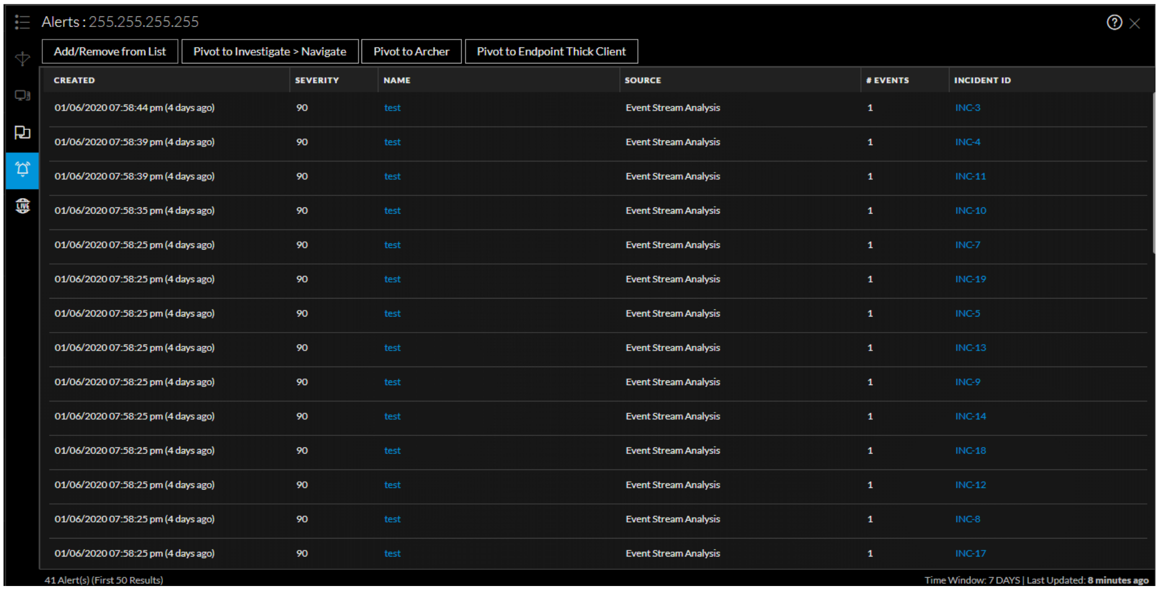
Field	Description
Module Name	The name of the module that is being looked up.
Analystic Score	The number of active files for the selected machine.
Machine Count	The number of machines on which that particular IOC got triggered.
Signature	Indicator of whether the file is signed or unsigned, valid or invalid, 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.


Alerts : 255.255.255.255
Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	INCIDENT ID
01/06/2020 07:58:44 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-3
01/06/2020 07:58:39 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-4
01/06/2020 07:58:39 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-11
01/06/2020 07:58:35 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-10
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-7
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-19
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-5
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-13
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-9
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-14
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-18
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-12
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-8
01/06/2020 07:58:25 pm (4 days ago)	90	test	Event Stream Analysis	1	INC-17

41 Alert(s) (First 50 Results)

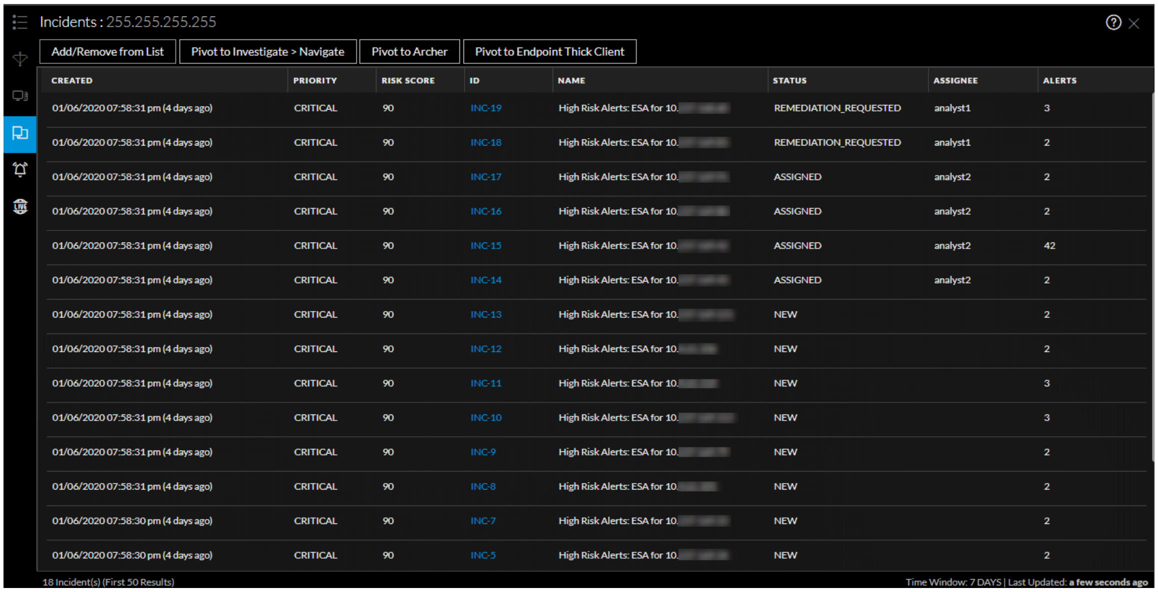
Time Window: 7 DAYS | Last Updated: **8 minutes ago**

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.


Incidents : 255.255.255.255
Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-19	High Risk Alerts: ESA for 10.[redacted]	REMEDIATION_REQUESTED	analyst1	3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-18	High Risk Alerts: ESA for 10.[redacted]	REMEDIATION_REQUESTED	analyst1	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-17	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-16	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-15	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	42
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-14	High Risk Alerts: ESA for 10.[redacted]	ASSIGNED	analyst2	2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-13	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-12	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-11	High Risk Alerts: ESA for 10.[redacted]	NEW		3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-10	High Risk Alerts: ESA for 10.[redacted]	NEW		3
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-9	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:31 pm (4 days ago)	CRITICAL	90	INC-8	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:30 pm (4 days ago)	CRITICAL	90	INC-7	High Risk Alerts: ESA for 10.[redacted]	NEW		2
01/06/2020 07:58:30 pm (4 days ago)	CRITICAL	90	INC-5	High Risk Alerts: ESA for 10.[redacted]	NEW		2

18 Incident(s) (First 50 Results)

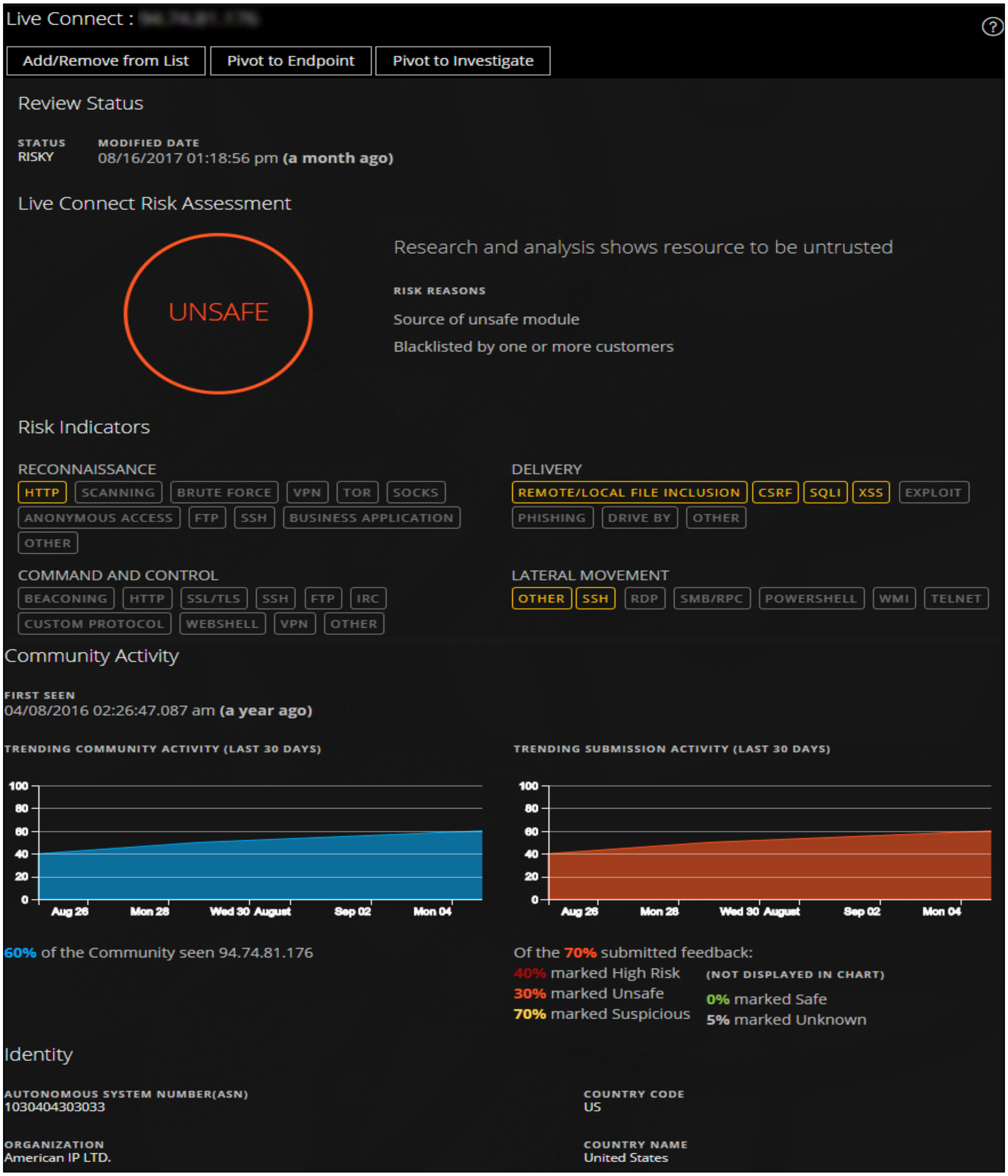
Time Window: 7 DAYS | Last Updated: **a few seconds ago**

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.



Live Connect : [redacted]

Review Status

STATUS
RISKY

MODIFIED DATE
08/16/2017 01:18:56 pm **(a month ago)**

Live Connect Risk Assessment

UNSAFE

Research and analysis shows resource to be untrusted

RISK REASONS

Source of unsafe module

Blacklisted by one or more customers

Risk Indicators

RECONNAISSANCE
HTTP SCANNING BRUTE FORCE VPN TOR SOCKS ANONYMOUS ACCESS FTP SSH BUSINESS APPLICATION OTHER

DELIVERY
REMOTE/LOCAL FILE INCLUSION CSRF SQLI XSS EXPLOIT PHISHING DRIVE BY OTHER

COMMAND AND CONTROL
BEACONING HTTP SSL/TLS SSH FTP IRC CUSTOM PROTOCOL WEBSHELL VPN OTHER

LATERAL MOVEMENT
OTHER SSH RDP SMB/RPC POWERSHELL WMI TELNET

Community Activity

FIRST SEEN
04/08/2016 02:26:47.087 am **(a year ago)**

TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)

TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)

60% of the Community seen 94.74.81.176

Of the **70%** submitted feedback:
40% marked High Risk
30% marked Unsafe
70% marked Suspicious

(NOT DISPLAYED IN CHART)
0% marked Safe
5% marked Unknown

Identity

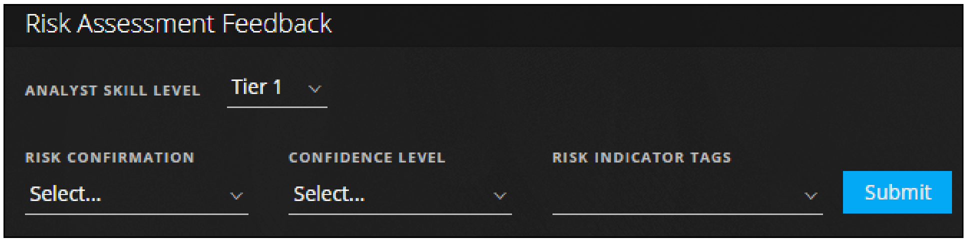
AUTONOMOUS SYSTEM NUMBER(ASN)
1030404303033

COUNTRY CODE
US

ORGANIZATION
American IP LTD.

COUNTRY NAME
United States

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.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Risk Assessment Feedback</td><td>

Risk Assessment Feedback

ANALYST SKILL LEVEL: Tier 1

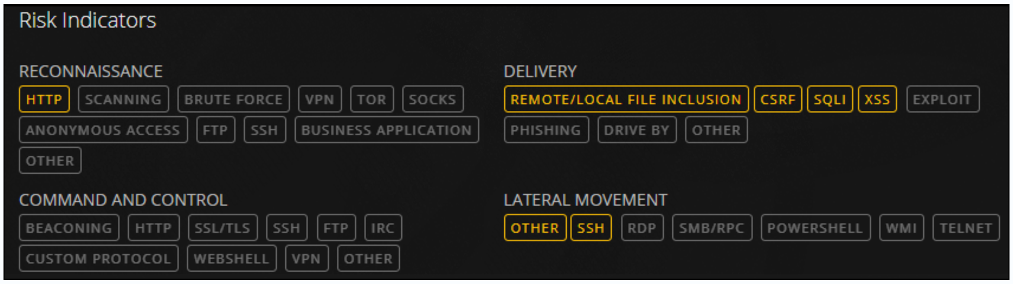
RISK CONFIRMATION: Select...

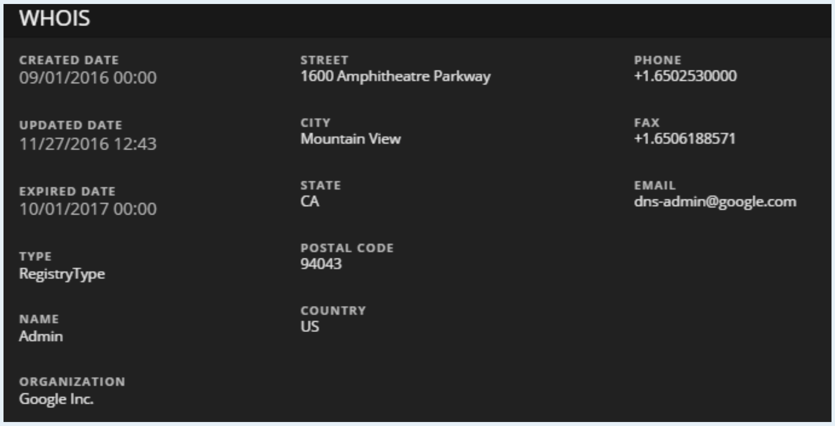
CONFIDENCE LEVEL: Select...

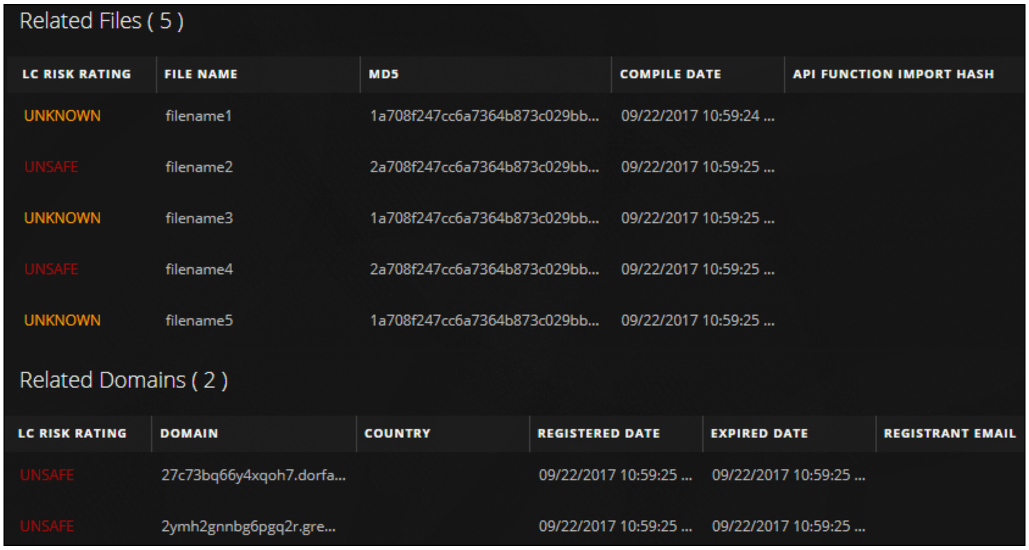
RISK INDICATOR TAGS:

Risk Assessment Feedback allows the analyst to submit threat intelligence feedback about an entity to the Live Connect server.

<ul>
<li><b>Analyst Skill Level</b>
Below are the Analyst skill level options:
<ul>
<li><b>Tier 1 -</b> 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.</li>
<li><b>Tier 2 -</b> Analysts who investigate incidents and capture intelligence from an investigation to feed back into the various workflows in a SOC.</li>
<li><b>Tier 3 -</b> 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.</li>
</ul>
<b>Note:</b> 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.
</li>
<li><b>Risk Confirmation</b> - The risk confirmation for the selected Live Connect entity (IP, file, or domain). The Risk confirmation categories are:
<ul>
<li><b>Safe</b>: The Live Connect entity is considered to be safe.</li>
<li><b>Unknown</b>: The analyst does not have enough information to provide a risk confirmation</li>
<li><b>High Risk</b>: Marked as high risk based on the analysis and risk reasons provided by the community. Entities marked as high risk require immediate attention.</li>
<li><b>Suspicious</b>: Marked as suspicious based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action.</li>
<li><b>Unsafe</b>: Marked as unsafe based on the analysis and risk reasons provided by the community.</li>
</ul>
</li>
<li><b>Confidence Level</b> - The confidence level of an analyst in providing feedback for the Live Connect entity. The confidence level categories are: High, Medium, and Low.</li>
<li><b>Risk Indicator Tags</b> - Allows you to select a tag category based on the analysis.</li>
</ul>
</td></tr>
</table>

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 RECONNAISSANCE HTTP SCANNING BRUTE FORCE VPN TOR SOCKS ANONYMOUS ACCESS FTP SSH BUSINESS APPLICATION OTHER DELIVERY REMOTE/LOCAL FILE INCLUSION CSRF SQLI XSS EXPLOIT PHISHING DRIVE BY OTHER COMMAND AND CONTROL BEACONING HTTP SSL/TLS SSH FTP IRC CUSTOM PROTOCOL WEBSHELL VPN OTHER LATERAL MOVEMENT OTHER SSH RDP SMB/RPC POWERSHELL WMI TELNET 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	 WHOIS CREATED DATE 09/01/2016 00:00 UPDATED DATE 11/27/2016 12:43 EXPIRED DATE 10/01/2017 00:00 TYPE RegistryType NAME Admin ORGANIZATION Google Inc. STREET 1600 Amphitheatre Parkway CITY Mountain View STATE CA POSTAL CODE 94043 COUNTRY US PHONE +1.6502530000 FAX +1.6506188571 EMAIL dns-admin@google.com 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.

Related Files (5)

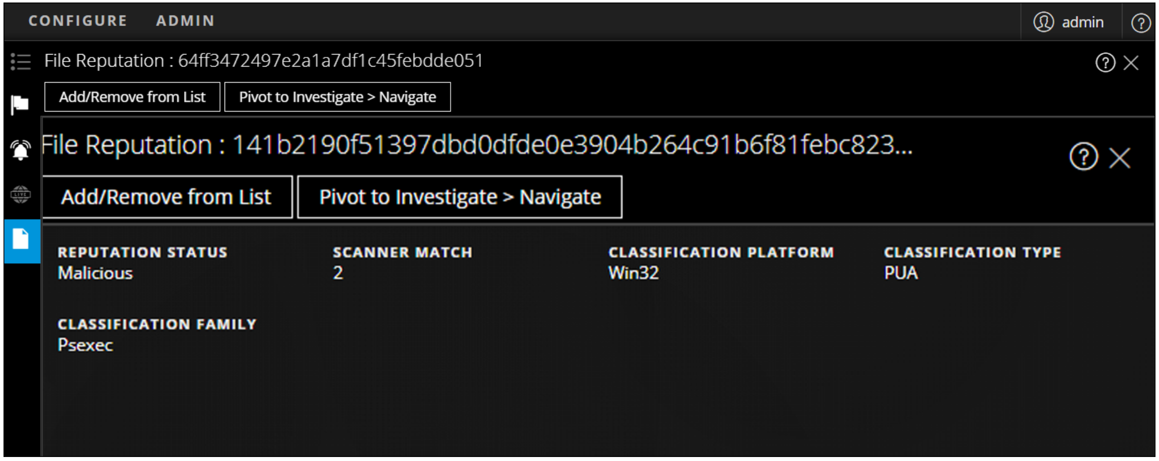
LC RISK RATING	FILE NAME	MD5	COMPILE DATE	API FUNCTION IMPORT HASH
UNKNOWN	filename1	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:24 ...	
UNSAFE	filename2	2a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...	
UNKNOWN	filename3	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...	
UNSAFE	filename4	2a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...	
UNKNOWN	filename5	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...	

Related Domains (2)

LC RISK RATING	DOMAIN	COUNTRY	REGISTERED DATE	EXPIRED DATE	REGISTRANT EMAIL
UNSAFE	27c73bq66y4xqoh7.dorfa...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	
UNSAFE	2ymh2gnnbg6pgq2r.gre...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	

File Reputation Tab

The Context Lookup panel for File Reputation displays the file reputation status of a file.


CONFIGURE
ADMIN
admin
Add/Remove from List
Pivot to Investigate > Navigate
Add/Remove from List
Pivot to Investigate > Navigate

File Reputation : 64ff3472497e2a1a7df1c45febdde051

File Reputation : 141b2190f51397dbd0dfde0e3904b264c91b6f81febc823...

REPUTATION STATUS
Malicious

SCANNER MATCH
2

CLASSIFICATION PLATFORM
Win32

CLASSIFICATION TYPE
PUA

CLASSIFICATION FAMILY
Psexec

Field	Description
Reputation Status	Reputation Status of filehash. For more information about reputation status, see "View Reputation of files" in the *UEBA User Guide*.
Scanner Match	Number of scanners that detected malware or suspicious activity in the last scan.

Field	Description
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.

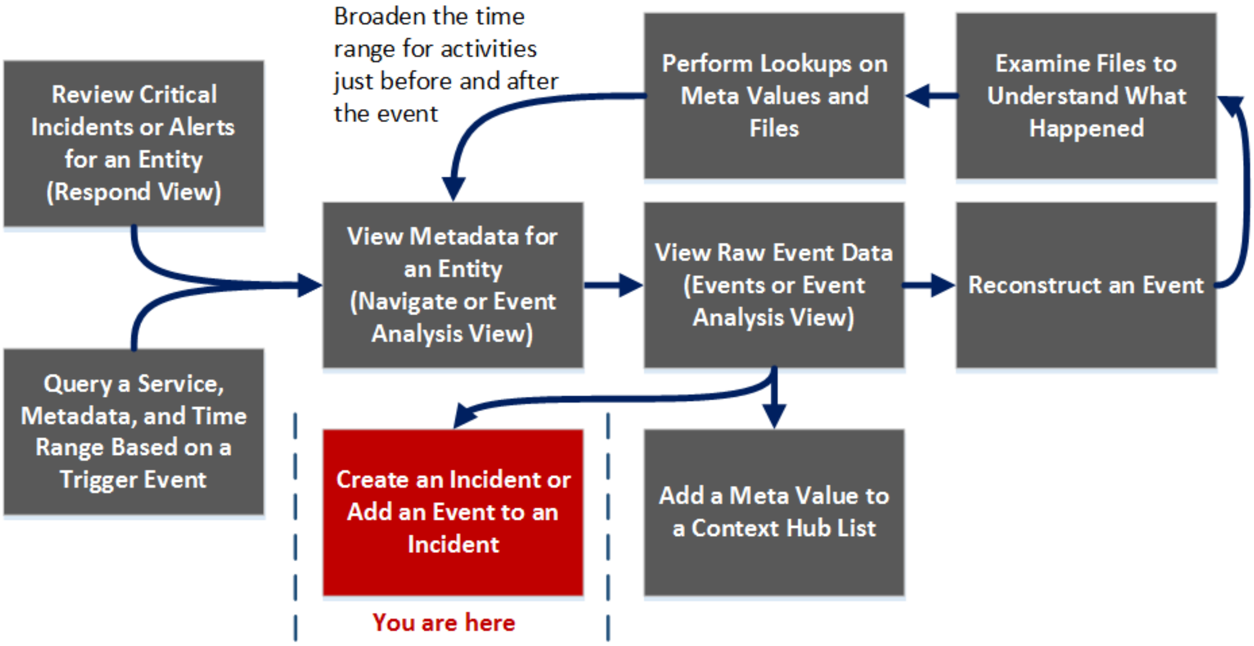
Create an Incident Dialog

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

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Review Critical Incidents or Alerts for an Entity (Respond View)
Broaden the time range for activities just before and after the event
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Metadata for an Entity (Navigate or Event Analysis View)
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Query a Service, Metadata, and Time Range Based on a Trigger Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List
You are here

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View

User Role	I want to ...	Show me how
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

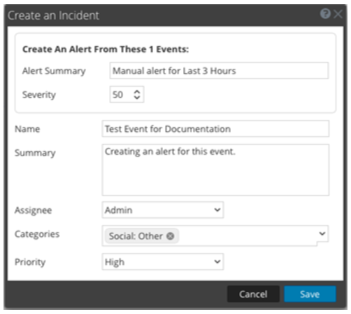
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Legacy Events View

Quick Look

The following figure is an example of the Create an Incident Dialog, and the features are described in the table.



Create an Incident

Create An Alert From These 1 Events:

Alert Summary: Manual alert for Last 3 Hours

Severity: 50

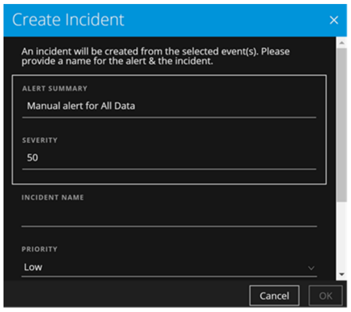
Name: Test Event for Documentation

Summary: Creating an alert for this event.

Assignee: Admin

Categories: Social: Other

Priority: High



Create Incident

An incident will be created from the selected event(s). Please provide a name for the alert & the incident.

ALERT SUMMARY: Manual alert for All Data

SEVERITY: 50

INCIDENT NAME

PRIORITY: Low

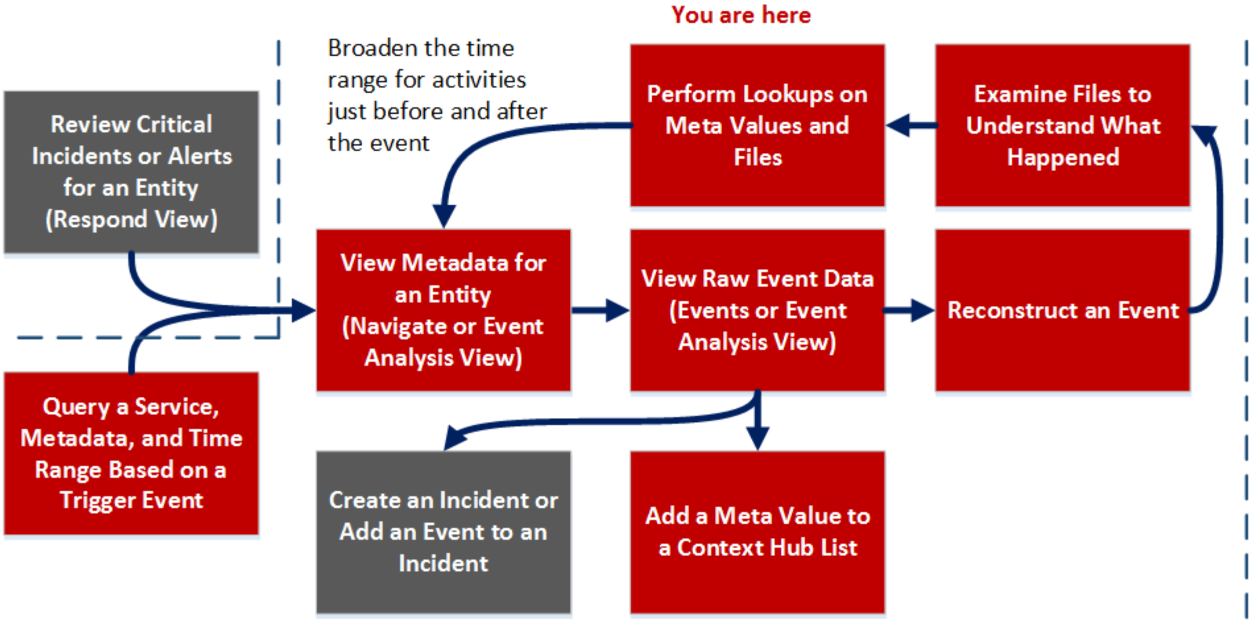
Feature	Description
Create Summary from These Events	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.
Name	(Required) Specifies a name 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.

Events View

In the Events 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 the preferred alternative to the static Legacy Events view and Event Reconstruction view. You can view network, log, and endpoint events in the Events view. The Events view offers packet, text, log, and email reconstruction. When you open a web reconstruction of an event, the same web reconstruction used in the Legacy Events view is displayed.

Workflow

The following figure is a high-level workflow illustrating the tasks you can do in NetWitness Investigate, with the Events view tasks highlighted in red. This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


You are here
Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata*	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data*	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event*	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups*	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context for Results

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View - Packet Panel
- Events View - Text Panel
- Events View - File Panel
- Events View - Email Panel

Quick Look

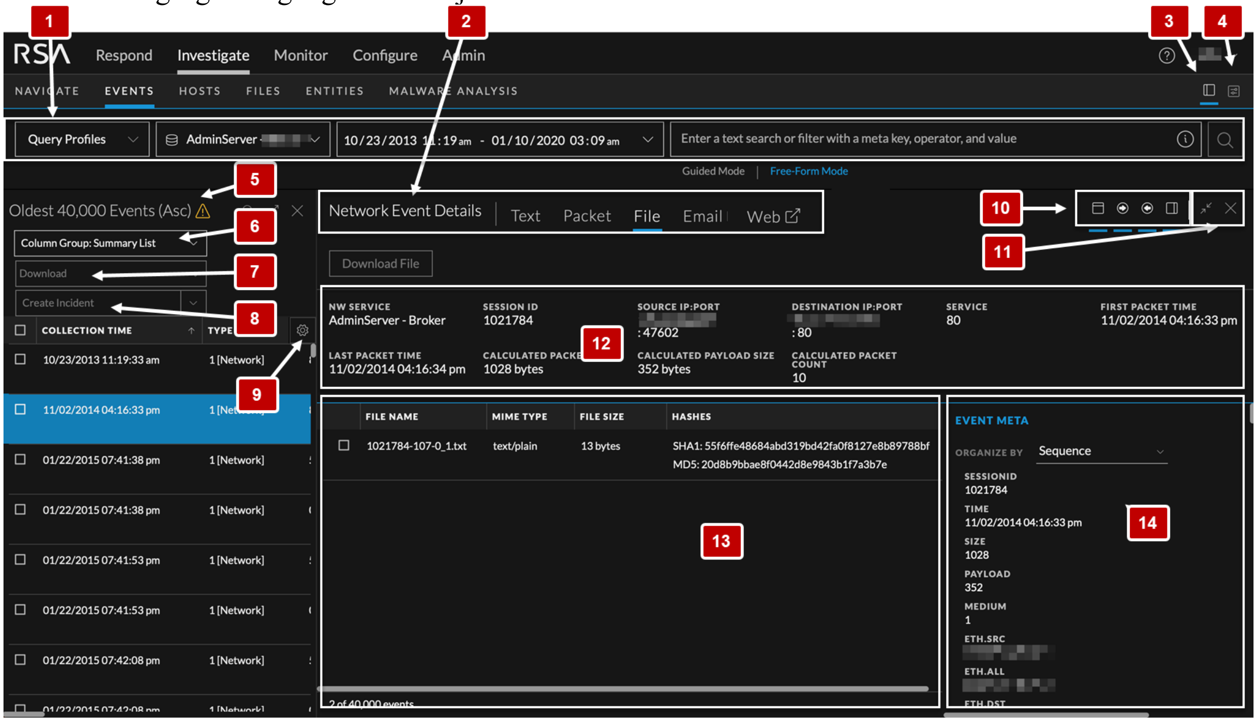
There are multiple access points to this view, which are described in Begin an Investigation in the Events View. If you access the Events view from the Respond view, you can see the analysis for a selected event in an incident. The options are a subset of the options available when you open an event from within the Investigate view. To get complete functionality and examine other events, you can go to the Event view directly (INVESTIGATE > Event).

The Events 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 Legacy Events view, or results for a query entered in the Events view query bar.

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 10,000 events, and 10,000 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, Text , or File).

> **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 Events view for Versions 11.4.1 and later.



10/23/2013 11:19:33 am - 01/10/2020 03:09 am

	COLLECTION TIME	TYPE
□	10/23/2013 11:19:33 am	1 [Network]
□	11/02/2014 04:16:33 pm	1 [Network]
□	01/22/2015 07:41:38 pm	1 [Network]
□	01/22/2015 07:41:38 pm	1 [Network]
□	01/22/2015 07:41:53 pm	1 [Network]
□	01/22/2015 07:41:53 pm	1 [Network]
□	01/22/2015 07:42:08 pm	1 [Network]
□	01/22/2015 07:42:08 pm	1 [Network]

NW SERVICE: AdminServer - Broker
SESSION ID: 1021784
SOURCE IP:PORT: [redacted] :47602
DESTINATION IP:PORT: [redacted] :80
SERVICE: 80
FIRST PACKET TIME: 11/02/2014 04:16:33 pm
LAST PACKET TIME: 11/02/2014 04:16:34 pm
CALCULATED PACKE[T SIZE]: 1028 bytes
CALCULATED PAYLOAD SIZE: 352 bytes
CALCULATED PACKET COUNT: 10

	FILE NAME	MIME TYPE	FILE SIZE	HASHES
□	1021784-107-0_1.txt	text/plain	13 bytes	SHA1: 55f6ffe48684abd319bd42fa0f8127e8b89788bf MD5: 20d8b9bbae8f0442d8e9843b1f7a3b7e

2 of 40,000 events

SESSIONID: 1021784
TIME: 11/02/2014 04:16:33 pm
SIZE: 1028
PAYLOAD: 352
MEDIUM: 1
ETH.SRC: [redacted]
ETH.ALL: [redacted]
ETH.DST

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 Events View and refine the query as described in Filter Results in the Events View. Clicking 🔍 submits the query and sends a request to the selected

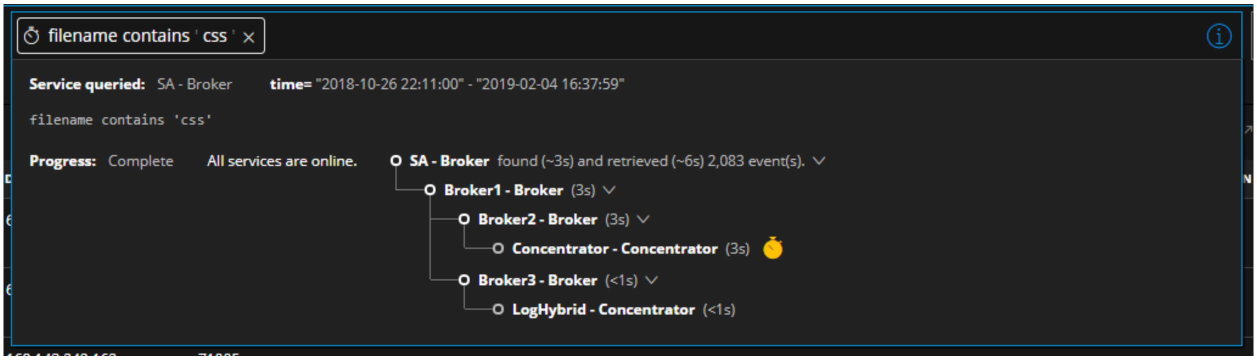
]

	service to load the data. In Version 11.3 and later, 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 and the type of reconstruction are reflected in the heading. - These are the event types: **Network Event Details**, **Log Event Details**, or **Endpoint Event Details**. - The types of analysis available for the event type are Text, Packet, File, Email, and Web. Network events can use all types of analysis: text, packet, file, and email (Version 11.4.1 and later). Log and endpoint events use only text analysis. The email (Version 11.4.0.x and earlier) type and web type open the current event as an email or web reconstruction in the Events view. For details, see Reconstruct an Event in the Events View.
3	Reopens the Events panel if you have closed it. For details, see Analyze Events in the Events View.
4	Sets preferences for the Event view (see Configure the Events View).
5	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 10,000 events are found, only the oldest 10,000 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 Events View. - Versions prior to 11.3 simply list the number of events found, and you can load 100 of them at a time. In Version 11.4 and later, clicking 🔍 opens the Find Text in Table dialog.
6	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, Endpoint Analysis, Malware Analysis, Outbound HTTP, Outbound SSL/TLS, and Summary List. Summary List is the default column group. For details, see Use Columns and Column Groups in the Events List.
7	The Download drop-down menu lists the available options for downloading event data. The options are Log, Visible Meta, and Network (see Downloading and Acting Upon Results. You can change the preferred format of the event type data in the Event Preferences dialog (see Configure the Events View).
8	The Create Incident button enables you to create incidents from events. The Add to Incident button enables you to add selected events to an open and existing incident (see Add Events to an Incident in the Events View and Add Events to an Incident in the Legacy Events View).
9	Displays the column selection settings to select the individual columns displayed in the Events panel. For details, see Use Columns and Column Groups in the Events List.
10	Controls to show or hide the Event Header, show or hide requests and responses, and open the Event Meta panel. For details, see Analyze Events in the Events View.

11	Controls to change the size of the panel and close the panel. For details, see Analyze Events in the Events View.
12	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).
13	The event data for the event you are currently analyzing.
14	The Event Meta panel lists the meta keys and values found in the data. This data can be sorted in two ways - Alphabets or Sequence. Some metadata are searchable; they have a binoculars icon, which you can click to see the associated data highlighted in the event data (see Analyze Events in the Events View). • 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 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.)

Query Console

Clicking ⓘ (the console icon) opens the query console, where detailed status of the query is provided.



filename contains ' css '

Service queried: SA - Broker **time=** "2018-10-26 22:11:00" - "2019-02-04 16:37:59"

```
filename contains 'css'
```

Progress: Complete All services are online.

```
SA - Broker found (~3s) and retrieved (~6s) 2,083 event(s).
  Broker1 - Broker (3s)
    Broker2 - Broker (3s)
      Concentrator - Concentrator (3s)
    Broker3 - Broker (<1s)
      LogHybrid - Concentrator (<1s)
```

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.

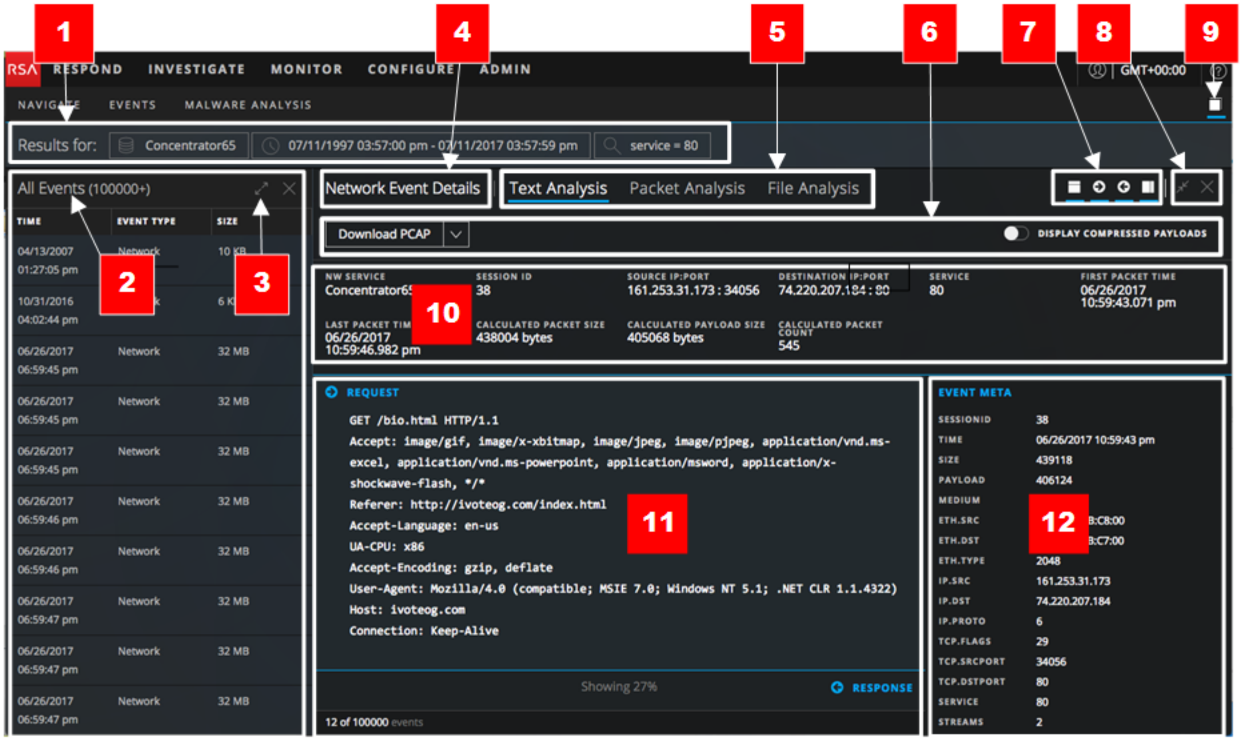
The server has a per-operation limit on execution time, and the requested operation exceeded the limit. To avoid this error, split the operation into smaller pieces, such as smaller time ranges.

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.



Results for: Concentrator65 | 07/11/1997 03:57:00 pm - 07/11/2017 03:57:59 pm | service = 80

All Events (100000+)

TIME	EVENT TYPE	SIZE
04/13/2007 01:27:05 pm	Network	10 KB
10/31/2016 04:02:44 pm	k	6 K
06/26/2017 06:59:45 pm	Network	32 MB
06/26/2017 06:59:45 pm	Network	32 MB
06/26/2017 06:59:45 pm	Network	32 MB
06/26/2017 06:59:46 pm	Network	32 MB
06/26/2017 06:59:46 pm	Network	32 MB
06/26/2017 06:59:47 pm	Network	32 MB
06/26/2017 06:59:47 pm	Network	32 MB
06/26/2017 06:59:47 pm	Network	32 MB

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
Concentrator65	38	161.253.31.173 : 34056	74.220.207.184 : 80	80	06/26/2017 10:59:43.071 pm

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
06/26/2017 10:59:46.982 pm	438004 bytes	405068 bytes	545

REQUEST

```
GET /bio.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, application/x-
shockwave-flash, */*
Referer: http://ivoteog.com/index.html
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: ivoteog.com
Connection: Keep-Alive
```

12 of 100000 events

EVENT META

SESSIONID	38
TIME	06/26/2017 10:59:43 pm
SIZE	439118
PAYLOAD	406124
MEDIUM	
ETH.SRC	B:C8:00
ETH.DST	B:C7:00
ETH.TYPE	2048
IP.SRC	161.253.31.173
IP.DST	74.220.207.184
IP.PROTO	6
TCP.FLAGS	29
TCP.SRCPORT	34056
TCP.DSTPORT	80
SERVICE	80
STREAMS	2

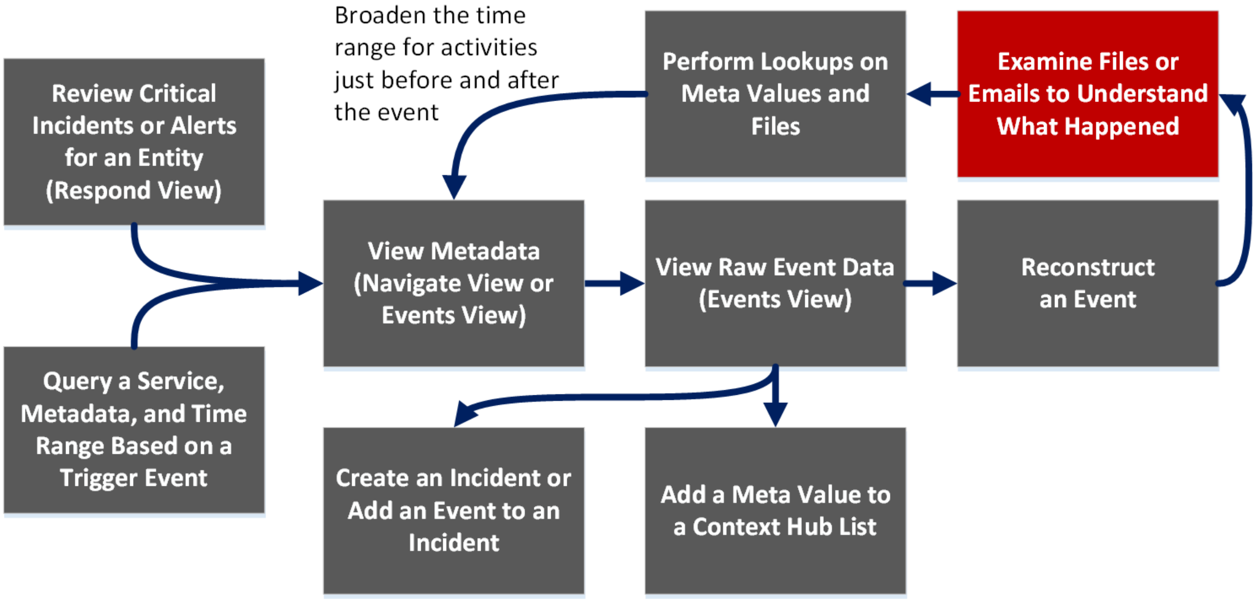
1	The read-only breadcrumb displays the selected service, time range, and query entered in the Navigate view or Events view.

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 Analyze Events in the Events 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 Analyze Events in the Events 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 Analyze Events in the Events 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 Analyze Events in the Events 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 Analyze Events in the Events View.

Events View - Email Panel

In the Email panel (**Events** > **Email)**, you can view a list of email received and associated attachments for an event.

Workflow


Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata (Navigate View or Events View)
View Raw Event Data (Events View)
Reconstruct an Event
Examine Files or Emails to Understand What Happened
Perform Lookups on Meta Values and Files
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

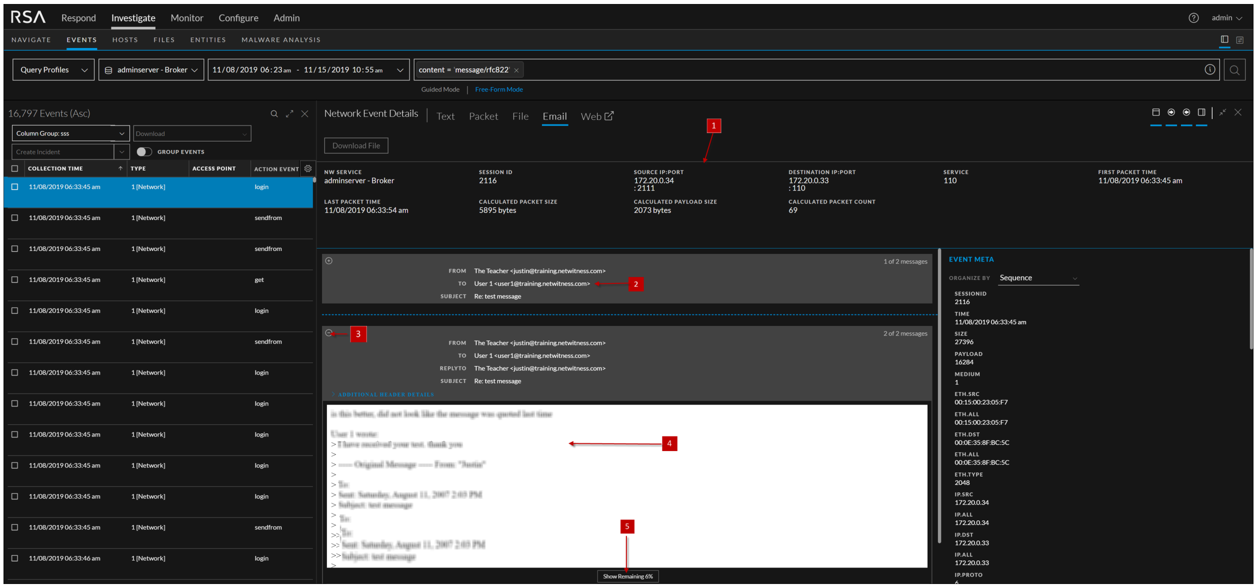
Related Topics

- How NetWitness Investigate Works
- Events View
- Events View - Text Panel
- Events View - Packet Panel
- Events View - File Panel

Quick Look

The Email panel displays a list of emails associated with a network event. When an analyst opens the email, the email reconstruction is displayed along with the associated attachments and additional header details, if any.

The following figure highlights the features of the email reconstruction.



adminserver - Broker

11/08/2019 06:23 am - 11/15/2019 10:55 am

content = 'message/rfc822'

16,797 Events (Asc)

COLLECTION TIME	TYPE	ACCESS POINT	ACTION EVENT
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:45 am	1 [Network]		get
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		login
11/08/2019 06:33:45 am	1 [Network]		sendfrom
11/08/2019 06:33:46 am	1 [Network]		login

NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
adminserver - Broker	2116	172.20.0.34 : 2111	172.20.0.33 : 110	110	11/08/2019 06:33:45 am

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
11/08/2019 06:33:54 am	5895 bytes	2073 bytes	69

1 of 2 messages

FROM The Teacher <justin@training.netwitness.com>
TO User 1 <user1@training.netwitness.com>
SUBJECT Re: test message

2 of 2 messages

FROM The Teacher <justin@training.netwitness.com>
TO User 1 <user1@training.netwitness.com>
REPLYTO The Teacher <justin@training.netwitness.com>
SUBJECT Re: test message

is this better, did not look like the message was quoted last time

User 1 wrote:
> I have received your test. thank you
>
> ----- Original Message ----- From: "Justin"
>
> To:
> Sent: Saturday, August 11, 2007 2:03 PM
> Subject: test message
>
> To:
>> To:
>> Sent: Saturday, August 11, 2007 2:03 PM
>> Subject: test message

SESSIONID 2116
TIME 11/08/2019 06:33:45 am
SIZE 27396
PAYLOAD 16284
MEDIUM 1
ETH.SRC 00:15:00:23:05:F7
ETH.ALL 00:15:00:23:05:F7
ETH.DST 00:0E:35:8F:BC:5C
ETH.ALL 00:0E:35:8F:BC:5C
ETH.TYPE 2048
IP.SRC 172.20.0.34
IP.ALL 172.20.0.34
IP.DST 172.20.0.33
IP.ALL 172.20.0.33
IP.PROTO

1 Displays the details of the selected event.

2 Displays the details of the email header.

3 Clicking this expands and collapses the email.

4 Displays the content of the email.

5 Clicking**Show Remaining %** displays the complete email.

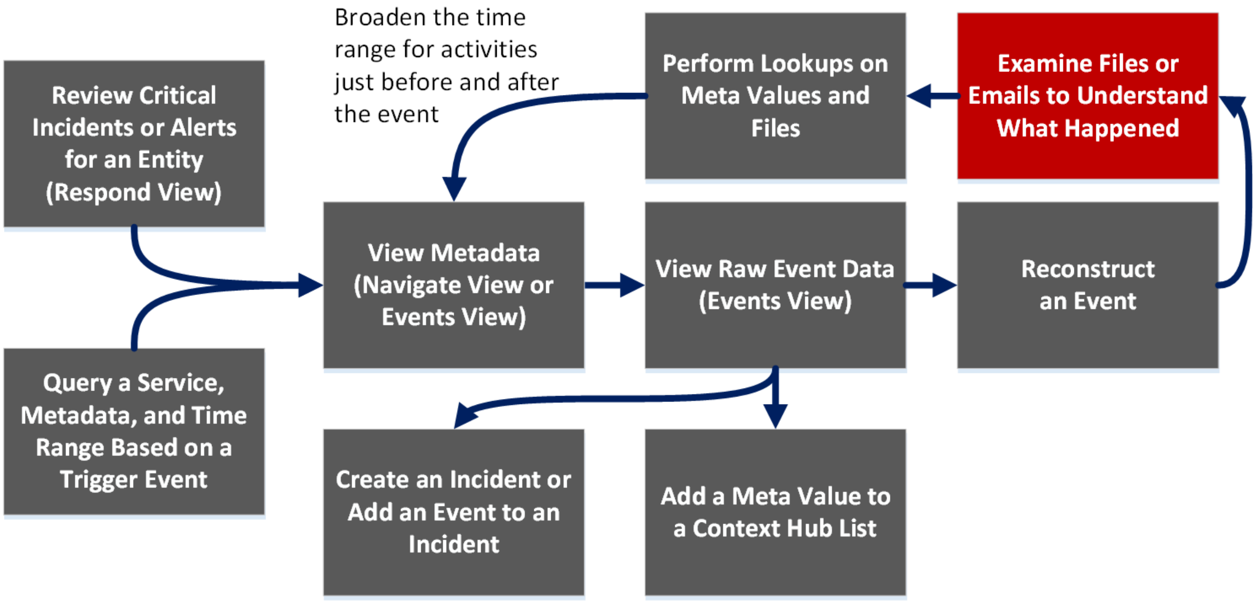
The following table describes all the fields within an email.

Field	Description
From	Displays the email address of the sender of the email.
To	Displays the email addresses of the recipients of the email.
CC (Carbon Copy)	Displays email addresses of additional recipients of the email. The field is displayed only if the sent email has any value and the email addresses are visible to the recipient.
BCC	Displays email addresses of additional recipients privately. This field is displayed only if the sent email has any value and the email addresses are not visible to the recipient.
Subject	Displays the subject of the email.
Attachments	Displays any files shared by the sender that can be downloaded by the recipient. This field is displayed only if email contains attachments.
Additional Header Details	Provides additional details of the email event such as Received, Sender, Message-ID and others.

Events View - File Panel

In the File panel (**Events** > **File),** you can safely view a list of files and download one or more files in an event.

Workflow


Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
Broaden the time range for activities just before and after the event
View Metadata (Navigate View or Events View)
Perform Lookups on Meta Values and Files
View Raw Event Data (Events View)
Examine Files or Emails to Understand What Happened
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set

User Role	I want to ...	Show me how
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

*You can perform this task in the current view.

Related Topics

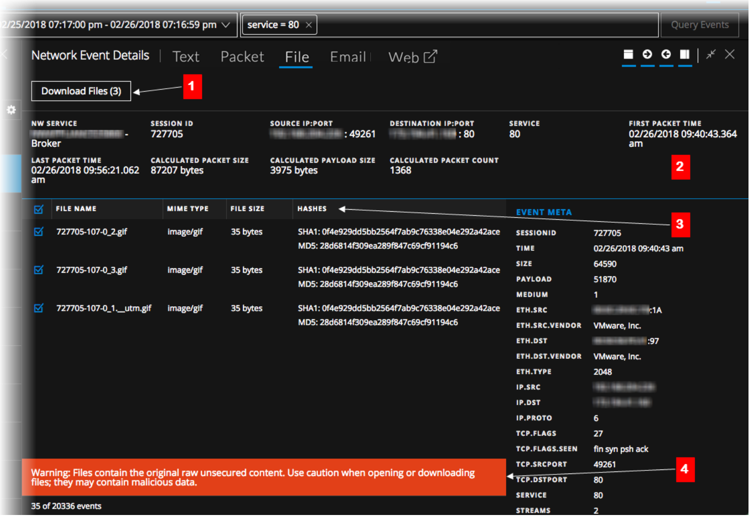
- How NetWitness Investigate Works
- Events View
- Events View - Text Panel
- Events View - Packet Panel

Quick Look

The File 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 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.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
[redacted] - Broker	727705	[redacted] : 49261	[redacted] : 80	80	02/26/2018 09:40:43.364 am

LAST PACKET TIME	CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT
02/26/2018 09:56:21.062 am	87207 bytes	3975 bytes	1368

☑	FILE NAME	MIME TYPE	FILE SIZE	HASHES
☑	727705-107-0_2.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6
☑	727705-107-0_3.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6
☑	727705-107-0_1.__utm.gif	image/gif	35 bytes	SHA1: 0f4e929dd5bb2564f7ab9c76338e04e292a42ace MD5: 28d6814f309ea289f847c69cf91194c6

Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data.

35 of 20336 events

EVENT META

SESSIONID	727705
TIME	02/26/2018 09:40:43 am
SIZE	64590
PAYLOAD	51870
MEDIUM	1
ETH.SRC	[redacted]:1A
ETH.SRC.VENDOR	VMware, Inc.
ETH.DST	[redacted]:97
ETH.DST.VENDOR	VMware, Inc.
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	27
TCP.FLAGS.SEEN	fin syn psh ack
TCP.SRCPORT	49261
TCP.DSTPORT	80
SERVICE	80
STREAMS	2

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.

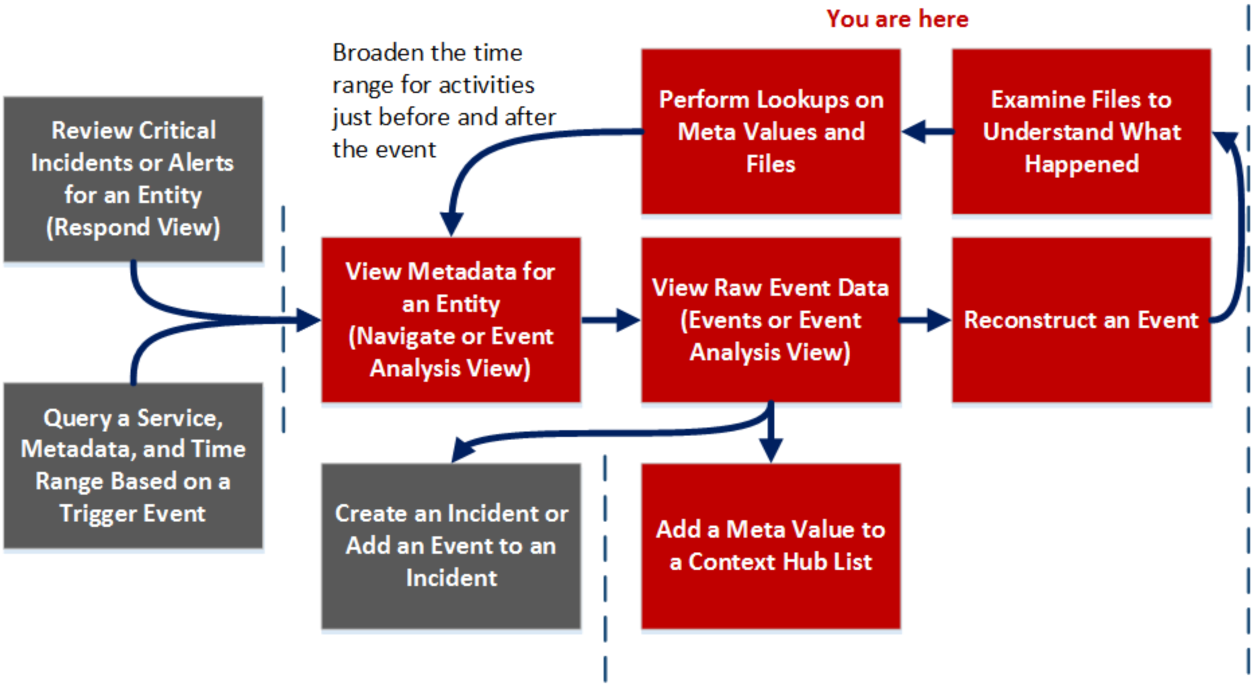
4 Reminder that caution is necessary when downloading potentially malicious files.

Events View - Packet Panel

In the Packet panel (**Events > Packet),** you can safely view and interactively analyze the packets and payload of an event.

Workflow

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


You are here
Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata for an Entity (Navigate or Event Analysis View)
Create an Incident or Add an Event to an Incident
Perform Lookups on Meta Values and Files
View Raw Event Data (Events or Event Analysis View)
Add a Meta Value to a Context Hub List
Examine Files to Understand What Happened
Reconstruct an Event

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata*	Analyze Events in the Events View Refining the Results Set

User Role	I want to ...	Show me how
Threat Hunter	view raw event data*	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event*	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups*	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context for Results

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View
- Events View - Text Panel
- Events View - File Panel
- Events View - Email Panel

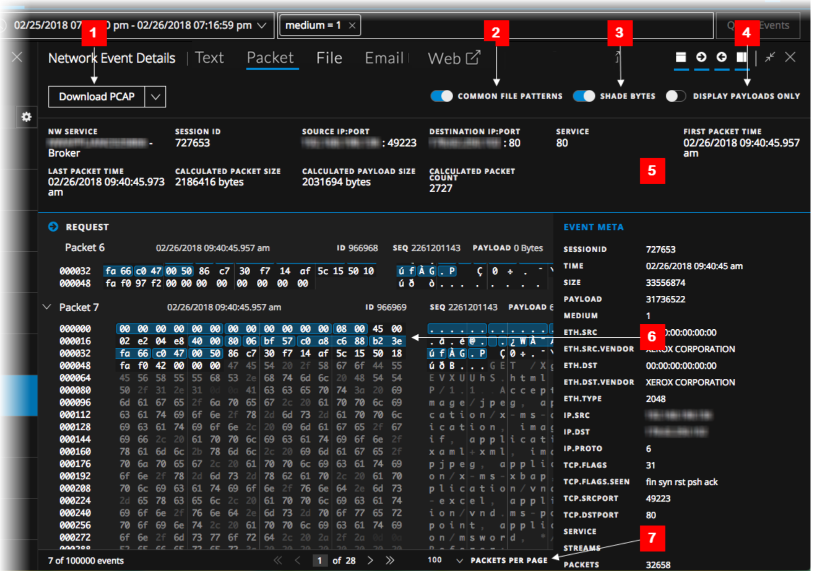
Quick Look

Only network events can be analyzed in the Packet panel. The Packet 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 (50, 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 panel with labels to identify features. For details and examples of each feature, see Analyze Events in the Events View.



NW SERVICE [redacted] - Broker
SESSION ID 727653
SOURCE IP:PORT [redacted] : 49223
DESTINATION IP:PORT [redacted] : 80
SERVICE 80
FIRST PACKET TIME 02/26/2018 09:40:45.957 am
LAST PACKET TIME 02/26/2018 09:40:45.973 am
CALCULATED PACKET SIZE 2186416 bytes
CALCULATED PAYLOAD SIZE 2031694 bytes
CALCULATED PACKET COUNT 2727

REQUEST

```
Packet 6       02/26/2018 09:40:45.957 am        ID 966968   SEQ 2261201143   PAYLOAD 0 Bytes

000032   fa 66 c0 47 00 50 86 c7 30 f7 14 af 5c 15 50 10    ú f À G . P   Ç 0 ÷ .   ¯
000048   fa f0 97 f2 00 00 00 00 00 00 00 00                ú ð   ò . . . . . . . .

Packet 7       02/26/2018 09:40:45.957 am        ID 966969   SEQ 2261201143   PAYLOAD 6

000000   00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00    . . . . . . . . . . . . .
000016   02 e2 04 e8 40 00 80 06 bf 57 c0 a8 c6 88 b2 3e    . â . è @ .     . ¿ W À ¨
000032   fa 66 c0 47 00 50 86 c7 30 f7 14 af 5c 15 50 18    ú f À G . P   Ç 0 ÷ .   ¯
000048   fa f0 42 00 00 00 47 45 54 20 2f 58 67 6f 44 55    ú ð B . . . G E T   / X
000064   45 56 58 55 55 68 53 2e 68 74 6d 6c 20 48 54 54    E V X U U h S . h t m l
000080   50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69    P / 1 . 1 . . A c c e p
000096   6d 61 67 65 2f 6a 70 65 67 2c 20 61 70 70 6c 69    m a g e / j p e g ,   a
000112   63 61 74 69 6f 6e 2f 78 2d 6d 73 2d 61 70 70 6c    c a t i o n / x - m s -
000128   69 63 61 74 69 6f 6e 2c 20 69 6d 61 67 65 2f 67    i c a t i o n ,   i m a
000144   69 66 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f    i f ,   a p p l i c a t
000160   78 61 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 65 2f    x a m l + x m l ,   i m
000176   70 6a 70 65 67 2c 20 61 70 70 6c 69 63 61 74 69    p j p e g ,   a p p l i
000192   6f 6e 2f 78 2d 6d 73 2d 78 62 61 70 2c 20 61 70    o n / x - m s - x b a p
000208   70 6c 69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d 73    p l i c a t i o n / v n
000224   2d 65 78 63 65 6c 2c 20 61 70 70 6c 69 63 61 74    - e x c e l ,   a p p l
000240   69 6f 6e 2f 76 6e 64 2e 6d 73 2d 70 6f 77 65 72    i o n / v n d . m s - p
000256   70 6f 69 6e 74 2c 20 61 70 70 6c 69 63 61 74 69    p o i n t ,   a p p l i
000272   6f 6e 2f 6d 73 77 6f 72 64 2c 20 2a 2f 2a 0d 0a    o n / m s w o r d ,   *

7 of 100000 events        « ‹ 1 of 28 › »        100 ⌄ PACKETS PER PAGE
```

EVENT META

SESSIONID	727653
TIME	02/26/2018 09:40:45 am
SIZE	33556874
PAYLOAD	31736522
MEDIUM	1
ETH.SRC	:00:00:00:00:00
ETH.SRC.VENDOR	X OX CORPORATION
ETH.DST	00:00:00:00:00:00
ETH.DST.VENDOR	XEROX CORPORATION
ETH.TYPE	2048
IP.SRC	[redacted]
IP.DST	[redacted]
IP.PROTO	6
TCP.FLAGS	31
TCP.FLAGS.SEEN	fin syn rst psh ack
TCP.SRCPORT	49223
TCP.DSTPORT	80
SERVICE	
STREAMS	
PACKETS	32658

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.

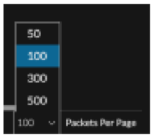
« - Go to the first page

‹ - Go to the previous page

1 of 206 - Go to a specific page

› - Go to the next page

» - Go to the last page



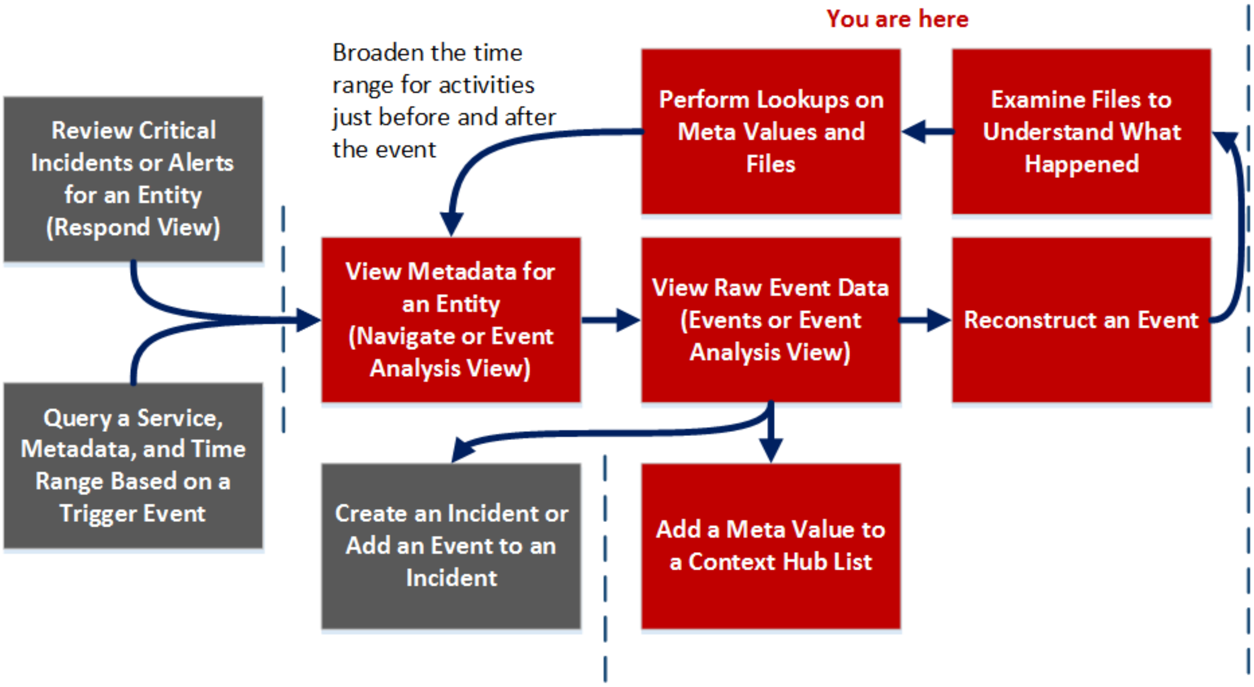
- Select the number of packets per page. If you are reconstructing large packets, lowering this limit can improve performance.

Events View - Text Panel

In the Text panel (**Events > Text),** you can safely view and analyze the raw text payload of an event. The Text reconstruction 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 reconstruction is available for all types of events: network, log, and endpoint.

Workflow

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


You are here
Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata for an Entity (Navigate or Event Analysis View)
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata*	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data*	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event*	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups*	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context for Results

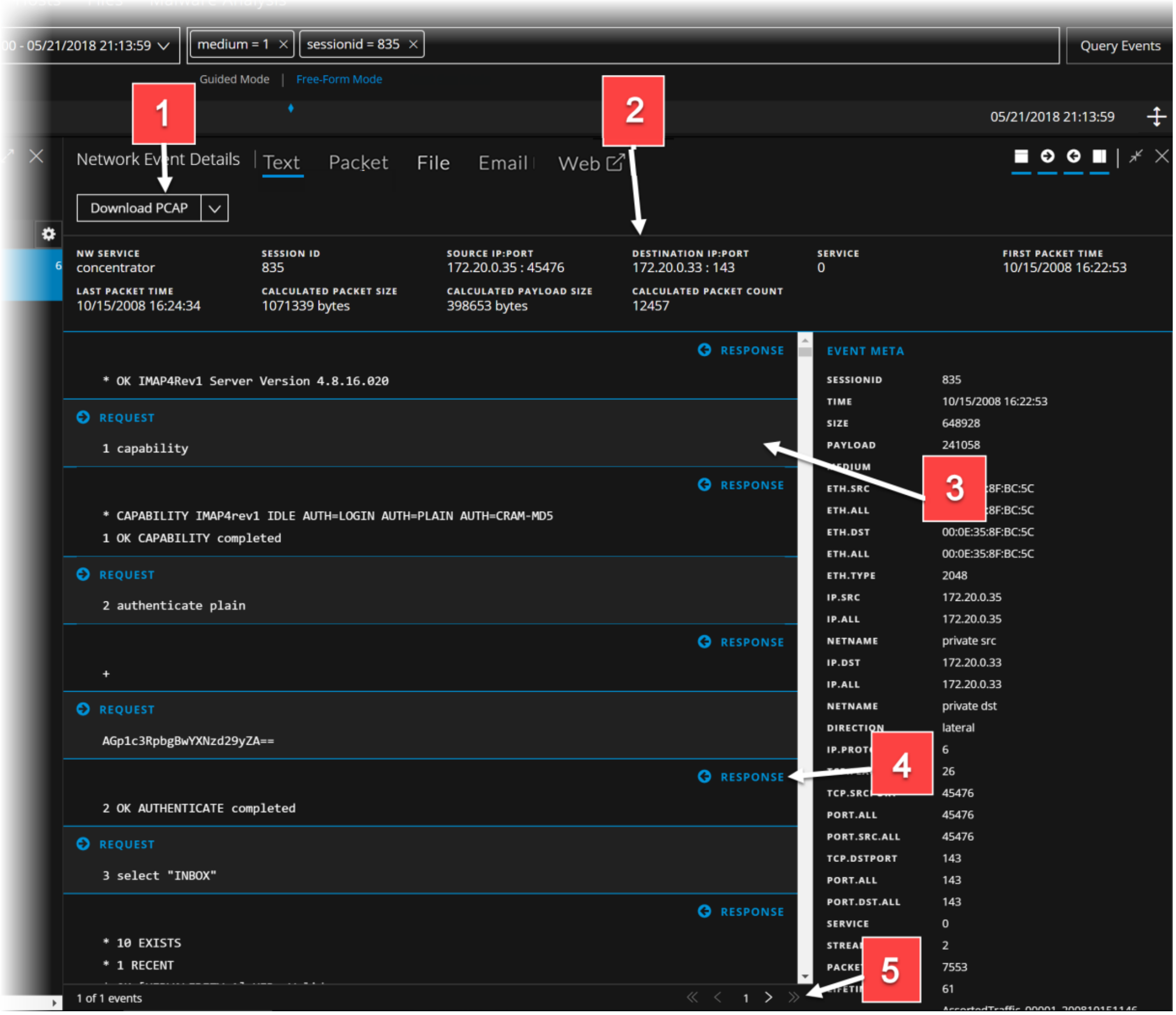
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View
- Events View - Packet Panel
- Events View - File Panel
- Events View - Email Panel

Quick Look

The Events view displays the text of a single event in the Text panel. When you click an event in the Event list panel, the adjacent panel shows the text reconstruction. Only the raw log for log events and endpoint events is shown in the Text 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, see Reconstructing and Analyzing Events. For detailed procedures, see Analyze Events in the Events View.



NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME
concentrator	835	172.20.0.35 : 45476	172.20.0.33 : 143	0	10/15/2008 16:22:53
LAST PACKET TIME	**CALCULATED PACKET SIZE**	**CALCULATED PAYLOAD SIZE**	**CALCULATED PACKET COUNT**		
10/15/2008 16:24:34	1071339 bytes	398653 bytes	12457		

```
                                                   RESPONSE
  * OK IMAP4Rev1 Server Version 4.8.16.020

REQUEST
  1 capability

                                                   RESPONSE
  * CAPABILITY IMAP4rev1 IDLE AUTH=LOGIN AUTH=PLAIN AUTH=CRAM-MD5
  1 OK CAPABILITY completed

REQUEST
  2 authenticate plain

                                                   RESPONSE
  +

REQUEST
  AGp1c3RpbgBwYXNzd29yZA==

                                                   RESPONSE
  2 OK AUTHENTICATE completed

REQUEST
  3 select "INBOX"

                                                   RESPONSE
  * 10 EXISTS
  * 1 RECENT
```

EVENT META

SESSIONID	835
TIME	10/15/2008 16:22:53
SIZE	648928
PAYLOAD	241058
MEDIUM	
ETH.SRC	8F:BC:5C
ETH.ALL	8F:BC:5C
ETH.DST	00:0E:35:8F:BC:5C
ETH.ALL	00:0E:35:8F:BC:5C
ETH.TYPE	2048
IP.SRC	172.20.0.35
IP.ALL	172.20.0.35
NETNAME	private src
IP.DST	172.20.0.33
IP.ALL	172.20.0.33
NETNAME	private dst
DIRECTION	lateral
IP.PROT	6
	26
TCP.SRC	45476
PORT.ALL	45476
PORT.SRC.ALL	45476
TCP.DSTPORT	143
PORT.ALL	143
PORT.DST.ALL	143
SERVICE	0
STREA	2
PACKE	7553
	61
	AssortedTraffic_00001_20081015114

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

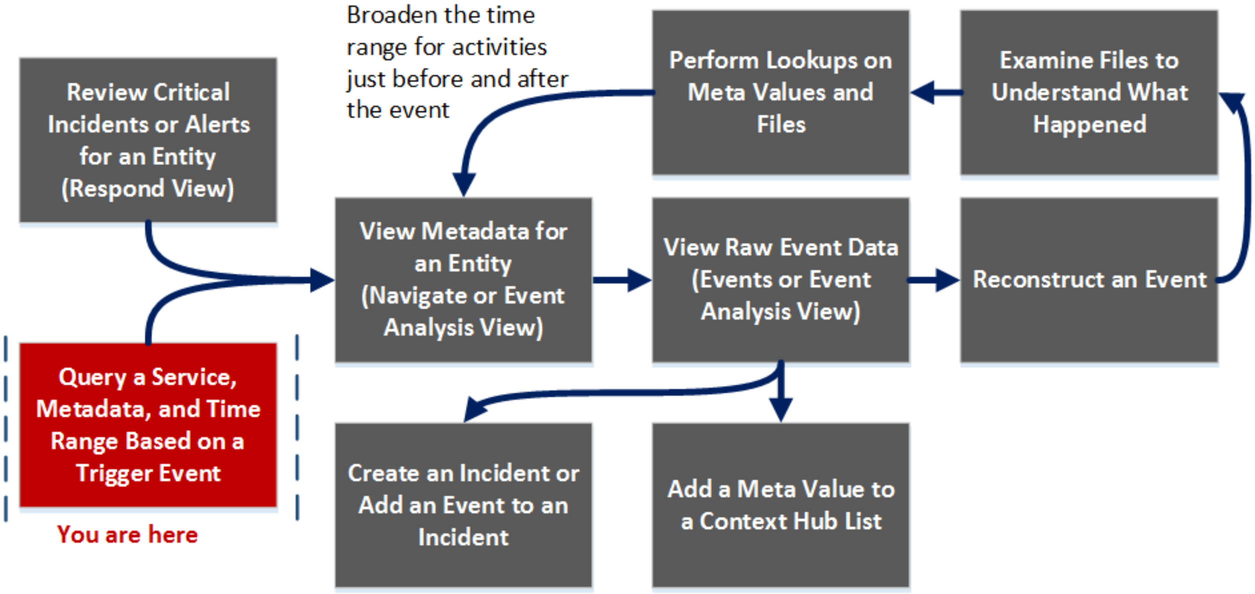
» - Go to last page (Only available after last page has already been navigated to)

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 Legacy 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

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
You are here
Broaden the time range for activities just before and after the event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set

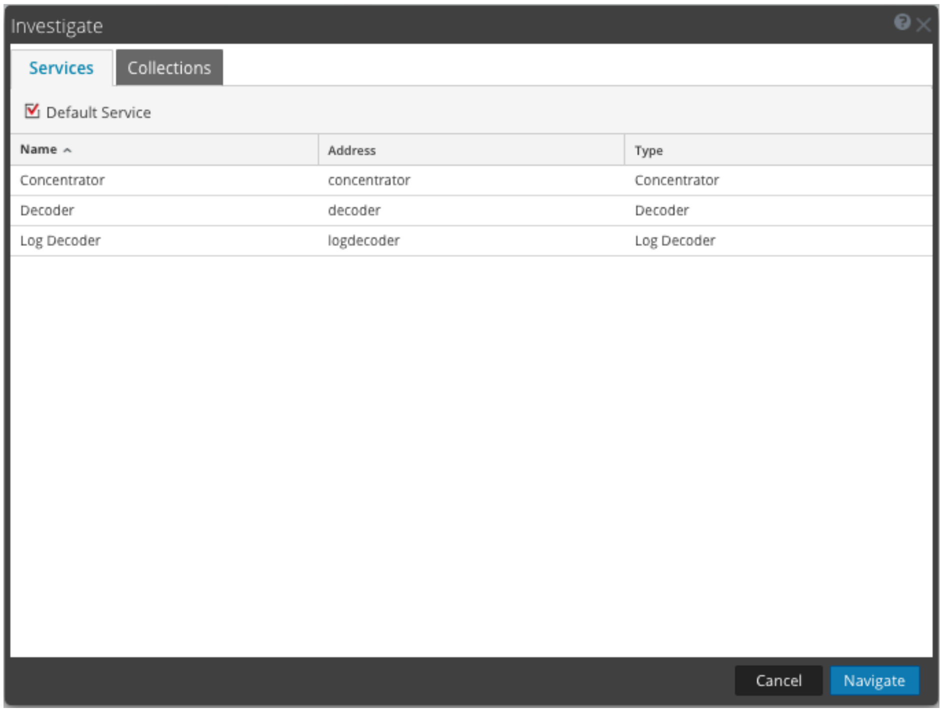
User Role	I want to ...	Show me how
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Legacy Events View

Quick Look



☑ Default Service

Name	Address	Type
Concentrator	concentrator	Concentrator
Decoder	decoder	Decoder
Log Decoder	logdecoder	Log Decoder

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 Legacy 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

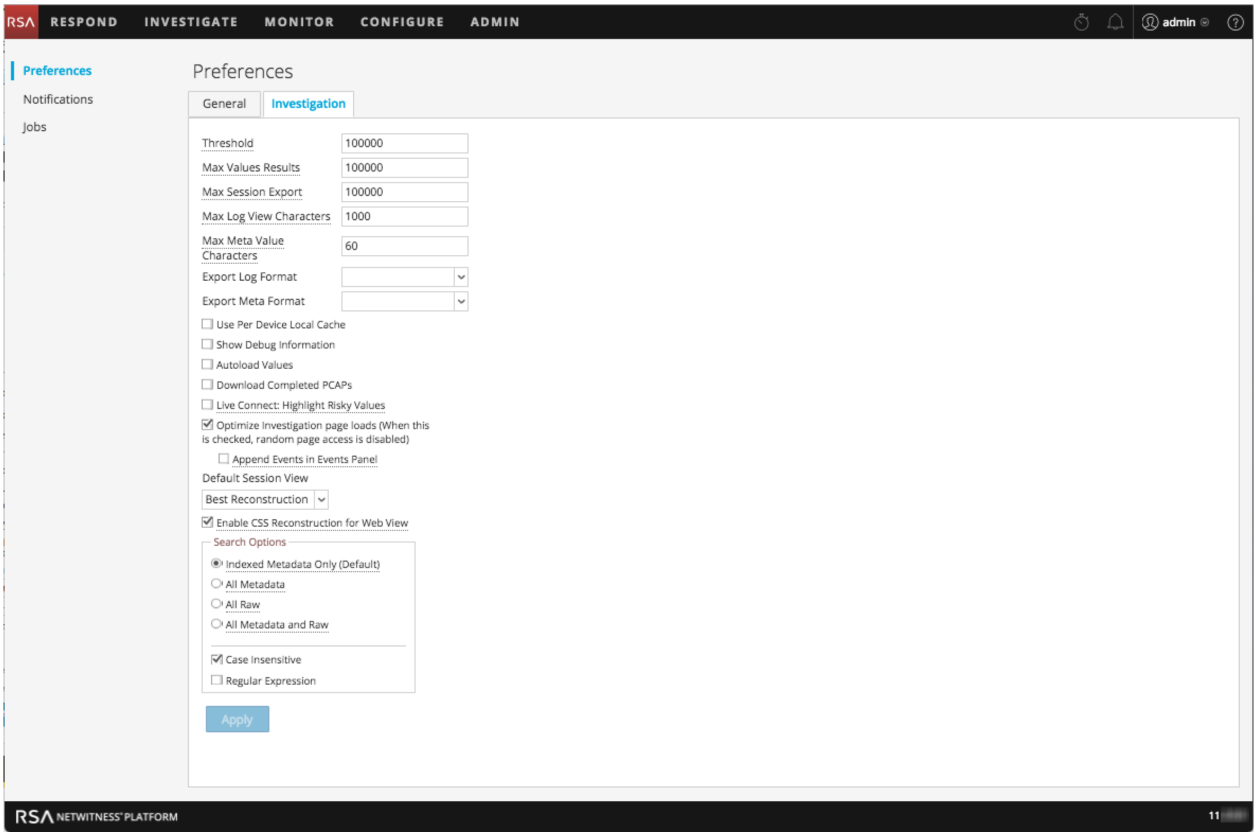
In the Profile view > Preferences panel > Investigation tab, users can set several preferences that affect the performance and behavior of NetWitness Platform when analyzing data, viewing events, and reconstructing events in NetWitness Investigate. To access this tab, select 👤 > > 👤 Profile from the Navigate view or the Legacy 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]
- [Legacy 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 in the Navigate and Legacy Events Views].



Preferences

Threshold	100000
Max Values Results	100000
Max Session Export	100000
Max Log View Characters	1000
Max Meta Value Characters	60
Export Log Format	
Export Meta Format	

□ Use Per Device Local Cache

□ Show Debug Information

□ Autoload Values

□ Download Completed PCAPs

□ Live Connect: Highlight Risky Values

☑ Optimize Investigation page loads (When this is checked, random page access is disabled)

□ Append Events in Events Panel

Default Session View: Best Reconstruction

☑ Enable CSS Reconstruction for Web View

Search Options

● Indexed Metadata Only (Default)

○ All Metadata

○ All Raw

○ All Metadata and Raw

☑ Case Insensitive

□ Regular Expression

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 **Investigate > Legacy Events > Log Text**. The default value is **1000**.
Export Log Format	This setting specifies the default format for exporting logs from Investigate. 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 Investigate. 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 Legacy 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 Legacy Events views. Search for Text Patterns in the Navigate and Legacy Events Views provides detailed information.

Feature	Description
Apply	Saves your preferences and puts them into effect immediately.

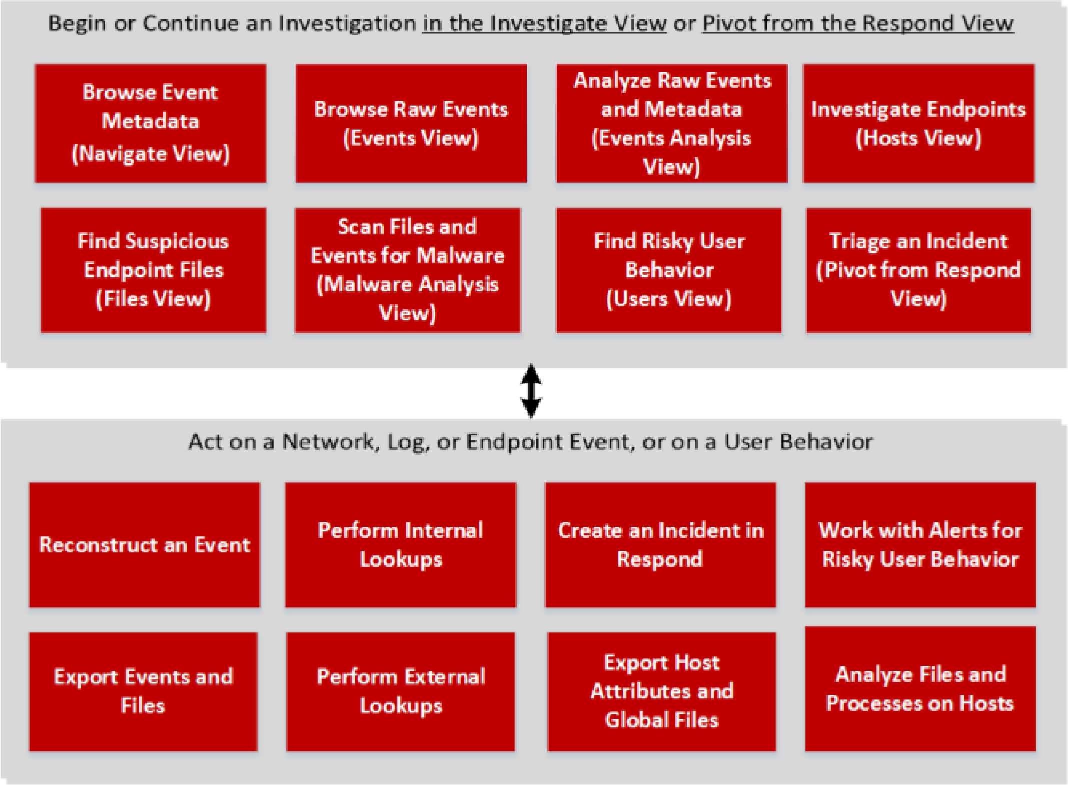
Investigate View

The Investigate view 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, Legacy Events, Events (formerly Event Analysis), Hosts, Files, Entities (formerly Users), and Malware Analysis.

> **Note:** The Legacy Events view was the original Events view (11.0 to 11.3.x.x). In Version 11.4 and later, the Legacy Events is no longer needed and it is hidden unless the administrator enables it. By default only the Events view appears in the menu, but when the Legacy Events view is enabled, both the Events view and the Legacy Events view are visible in the menu bar.

Workflow

The figure below depicts the high-level tasks that you can perform in the Investigate view. This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Begin or Continue an Investigation in the Investigate View or Pivot from the Respond View
Browse Event Metadata (Navigate View)
Browse Raw Events (Events View)
Analyze Raw Events and Metadata (Events Analysis View)
Investigate Endpoints (Hosts View)
Find Suspicious Endpoint Files (Files View)
Scan Files and Events for Malware (Malware Analysis View)
Find Risky User Behavior (Users View)
Triage an Incident (Pivot from Respond View)
Act on a Network, Log, or Endpoint Event, or on a User Behavior
Reconstruct an Event
Perform Internal Lookups
Create an Incident in Respond
Work with Alerts for Risky User Behavior
Export Events and Files
Perform External Lookups
Export Host Attributes and Global Files
Analyze Files and Processes on Hosts

You can use the submenu options to move between the different views.

- The Navigate view, Events view, and Legacy Events 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 Entities view (formerly known as 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 Legacy Events View
Threat Hunter	browse raw events	Begin an Investigation in the Events View Begin an Investigation in the Navigate or Legacy Events View
Threat Hunter	analyze raw events and metadata	Begin an Investigation in the Events 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

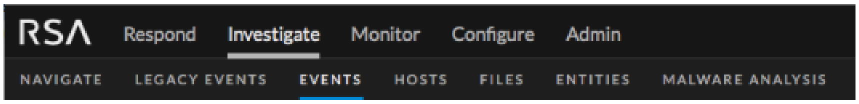
- How NetWitness Investigate Works
- Beginning an Investigation
- Configuring NetWitness Investigate Views and Preferences
- Navigate View

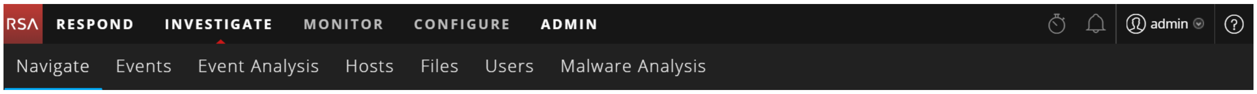
- Legacy Events View
- Events View
- *NetWitness Investigate Quick Start Guide*
- *NetWitness Endpoint Quick Start Guide*
- *NetWitness UEBA Quick Start Guide*
- *Malware Analysis User Guide*

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 first figure below illustrates the submenus under Investigate in Version 11.4. The second figure illustrates the menu in prior versions.

> **Note:** The Hosts, and Files submenus are available in Version 11.1 and later. The Entities (formerly Users) menu is available in Version 11.2 and later. Configured permissions per user role and user determine which submenus are displayed.





Legacy Event Reconstruction View

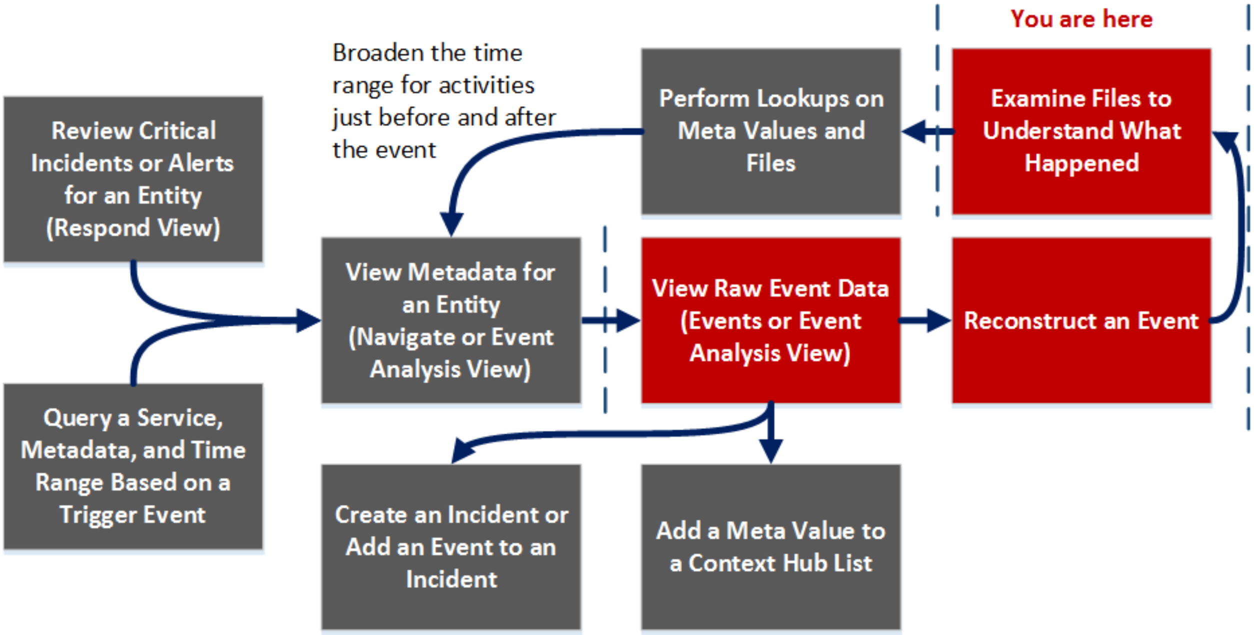
The Event Reconstruction view provides a reconstruction of a selected event from the Legacy Events view. By default, NetWitness Platform displays the best reconstruction for the event determined by the event content, or the default reconstruction that you have selected in the Default Session View setting 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 Legacy Events view, double-click an event.
- In the Legacy Events view with Detail View selected, right-click **Events** 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

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


You are here
Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
View Raw Event Data (Events or Event Analysis View)
Examine Files to Understand What Happened
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data*	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event*	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

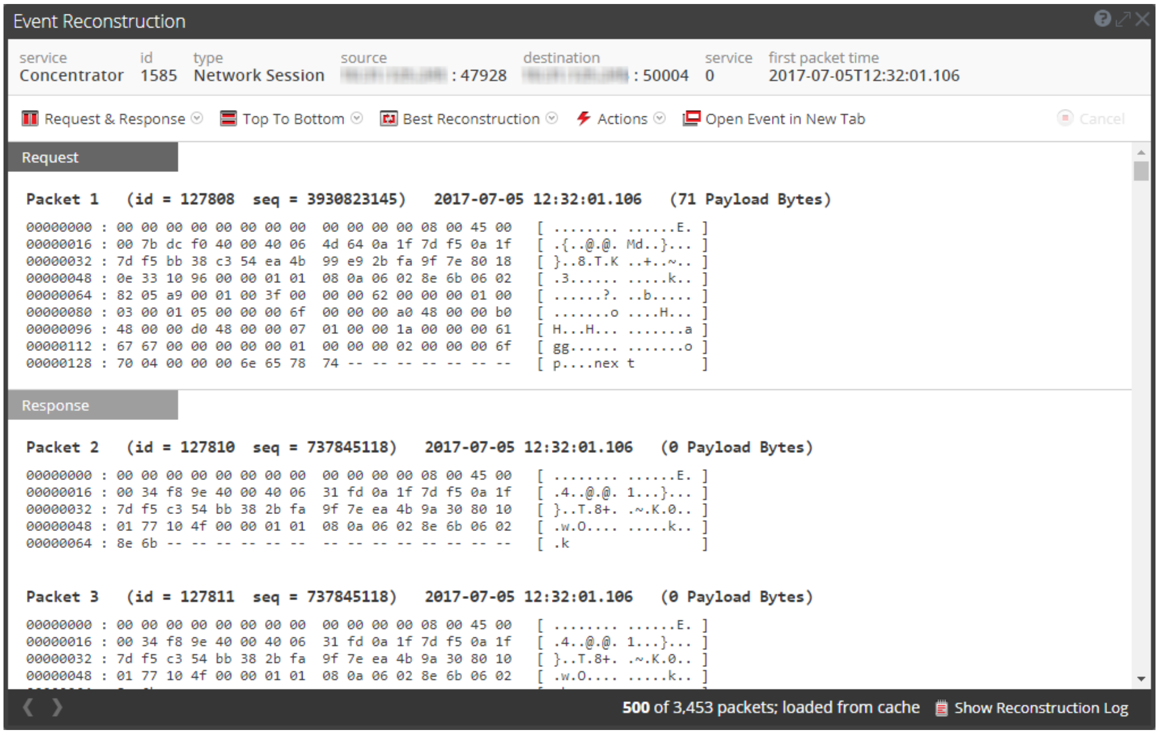
*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Events View

Quick Look

This figure is an example of the Event Reconstruction view. The following table describes the toolbar options.



Event Reconstruction

service	id	type	source	destination	service	first packet time
Concentrator	1585	Network Session	[redacted] : 47928	[redacted] : 50004	0	2017-07-05T12:32:01.106

Request

```
Packet 1   (id = 127808   seq = 3930823145)   2017-07-05 12:32:01.106   (71 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 7b dc f0 40 00 40 06  4d 64 0a 1f 7d f5 0a 1f   [ .{..@.@. Md..}... ]
00000032 : 7d f5 bb 38 c3 54 ea 4b  99 e9 2b fa 9f 7e 80 18   [ }..8.T.K ..+..~.. ]
00000048 : 0e 33 10 96 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .3...... .....k.. ]
00000064 : 82 05 a9 00 01 00 3f 00  00 00 62 00 00 00 01 00   [ ......?. ..b..... ]
00000080 : 03 00 01 05 00 00 00 6f  00 00 00 a0 48 00 00 b0   [ .......o ....H... ]
00000096 : 48 00 00 d0 48 00 00 07  01 00 00 1a 00 00 00 61   [ H...H... .......a ]
00000112 : 67 67 00 00 00 00 00 01  00 00 00 02 00 00 00 6f   [ gg...... .......o ]
00000128 : 70 04 00 00 00 6e 65 78  74 -- -- -- -- -- -- --   [ p....nex t        ]
```

Response

```
Packet 2   (id = 127810   seq = 737845118)   2017-07-05 12:32:01.106   (0 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 34 f8 9e 40 00 40 06  31 fd 0a 1f 7d f5 0a 1f   [ .4..@.@. 1...}... ]
00000032 : 7d f5 c3 54 bb 38 2b fa  9f 7e ea 4b 9a 30 80 10   [ }..T.8+. .~.K.0.. ]
00000048 : 01 77 10 4f 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .w.O.... .....k.. ]
00000064 : 8e 6b -- -- -- -- -- --  -- -- -- -- -- -- -- --   [ .k                ]


Packet 3   (id = 127811   seq = 737845118)   2017-07-05 12:32:01.106   (0 Payload Bytes)

00000000 : 00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   [ ........ ......E. ]
00000016 : 00 34 f8 9e 40 00 40 06  31 fd 0a 1f 7d f5 0a 1f   [ .4..@.@. 1...}... ]
00000032 : 7d f5 c3 54 bb 38 2b fa  9f 7e ea 4b 9a 30 80 10   [ }..T.8+. .~.K.0.. ]
00000048 : 01 77 10 4f 00 00 01 01  08 0a 06 02 8e 6b 06 02   [ .w.O.... .....k.. ]
```

500 of 3,453 packets; loaded from cache

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.

Feature	Description
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).
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.

Legacy Events View

In the Legacy 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.

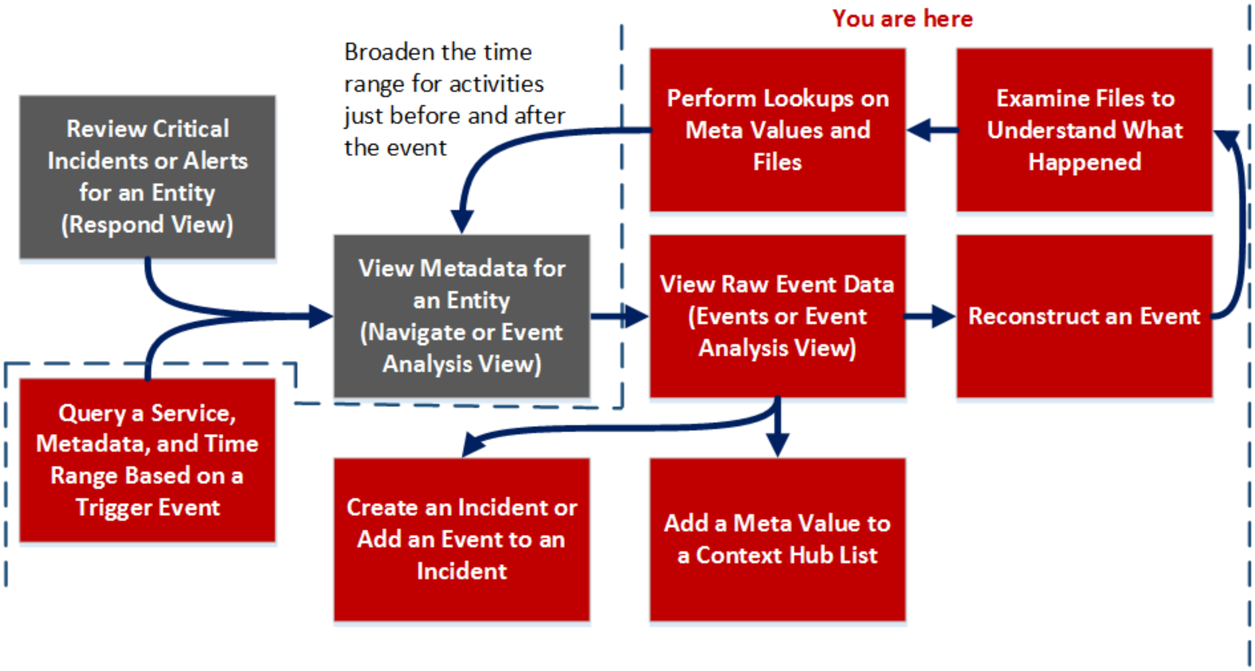
There are two ways to display the Legacy Events view:

- Go to **Investigate > Legacy 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 Legacy Events view displays events on the selected service, with the oldest events first.
- From within the **Navigate** view, double-click an event. The Legacy Events view displays the events on the selected service based on the drill point in the Navigate view.

> **Note:** The Legacy Events view was the original Events view (11.0 to 11.3.x.x). The Legacy Events is no longer needed and it is hidden unless the administrator enables it. By default only the Events view appears in the menu, but when the Legacy Events view is enabled, both the Events view and the Legacy Events view are visible in the menu bar.

Workflow

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


You are here
Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Query a Service, Metadata, and Time Range Based on a Trigger Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data*	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event*	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups*	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident*	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context for Results

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Filter Results in the Legacy Events View

- Downloading and Acting Upon Results

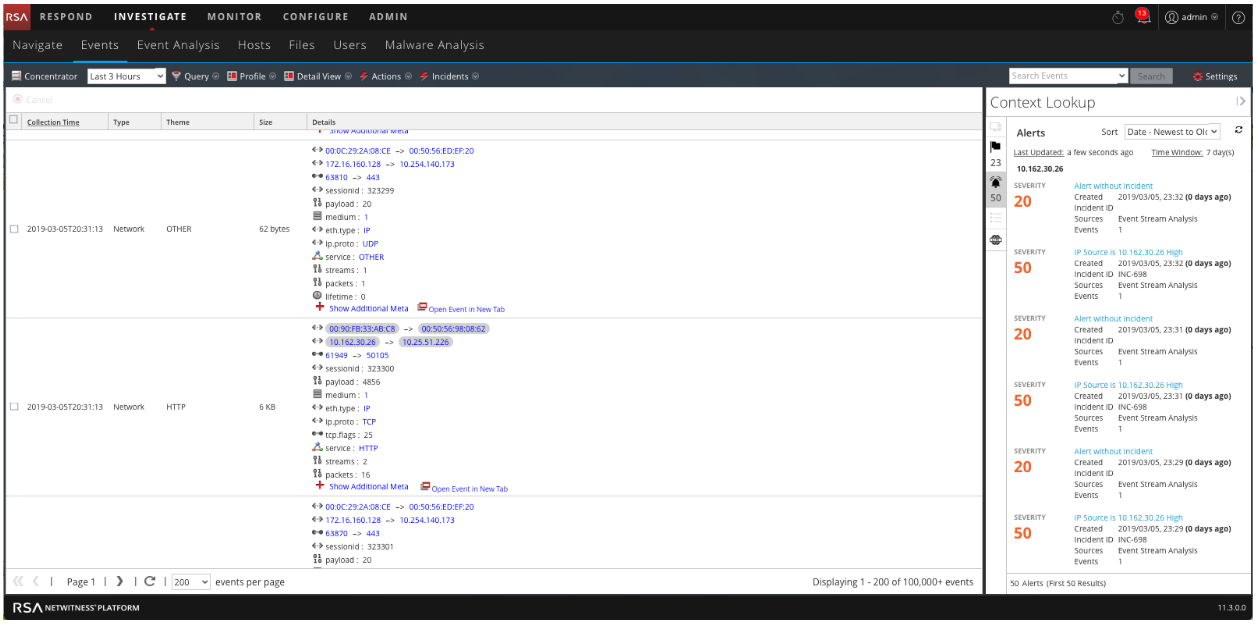
Quick Look

The Legacy 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 Legacy Events view. From any view type in Legacy 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 the Events view.

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.



□	Collection Time	Type	Theme	Size	Details
□	2019-03-05T20:31:13	Network	OTHER	62 bytes	00:0C:29:2A:08:CE -> 00:50:56:ED:EF:20 172.16.160.128 -> 10.254.140.173 63810 -> 443 sessionid : 323299 payload : 20 medium : 1 eth.type : IP ip.proto : UDP service : OTHER streams : 1 packets : 1 lifetime : 0
□	2019-03-05T20:31:13	Network	HTTP	6 KB	00:90:FB:33:AB:C8 -> 00:50:56:98:08:62 10.162.30.26 -> 10.25.51.226 61949 -> 50105 sessionid : 323300 payload : 4856 medium : 1 eth.type : IP ip.proto : TCP tcp.flags : 25 service : HTTP streams : 2 packets : 16
					00:0C:29:2A:08:CE -> 00:50:56:ED:EF:20 172.16.160.128 -> 10.254.140.173 63870 -> 443 sessionid : 323301 payload : 20

200 events per page

Displaying 1 - 200 of 100,000+ events

Context Lookup

Alerts Sort Date - Newest to Olc

Last Updated: a few seconds ago Time Window: 7 day(s)

23

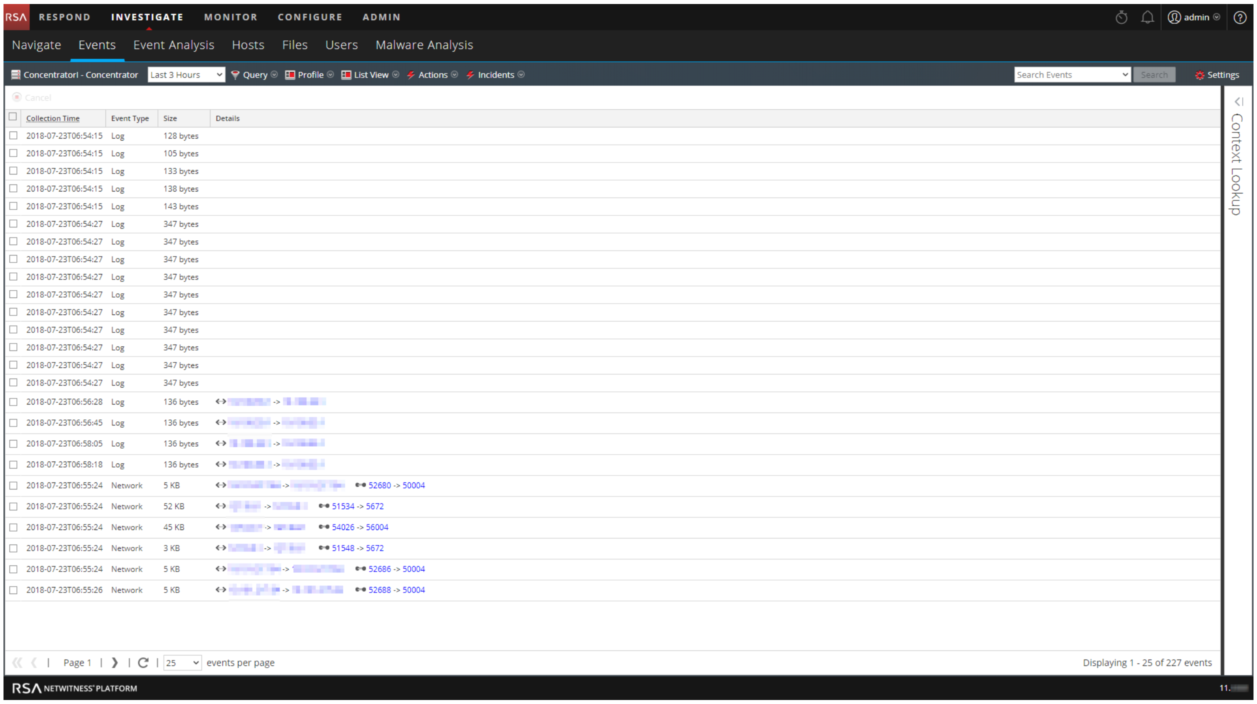
50

10.162.30.26

Severity	Alert	Created	Incident ID	Sources	Events
20	Alert without Incident	2019/03/05, 23:32 **(0 days ago)**		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:32 **(0 days ago)**	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:31 **(0 days ago)**		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:31 **(0 days ago)**	INC-698	Event Stream Analysis	1
20	Alert without Incident	2019/03/05, 23:29 **(0 days ago)**		Event Stream Analysis	1
50	IP Source is 10.162.30.26 High	2019/03/05, 23:29 **(0 days ago)**	INC-698	Event Stream Analysis	1

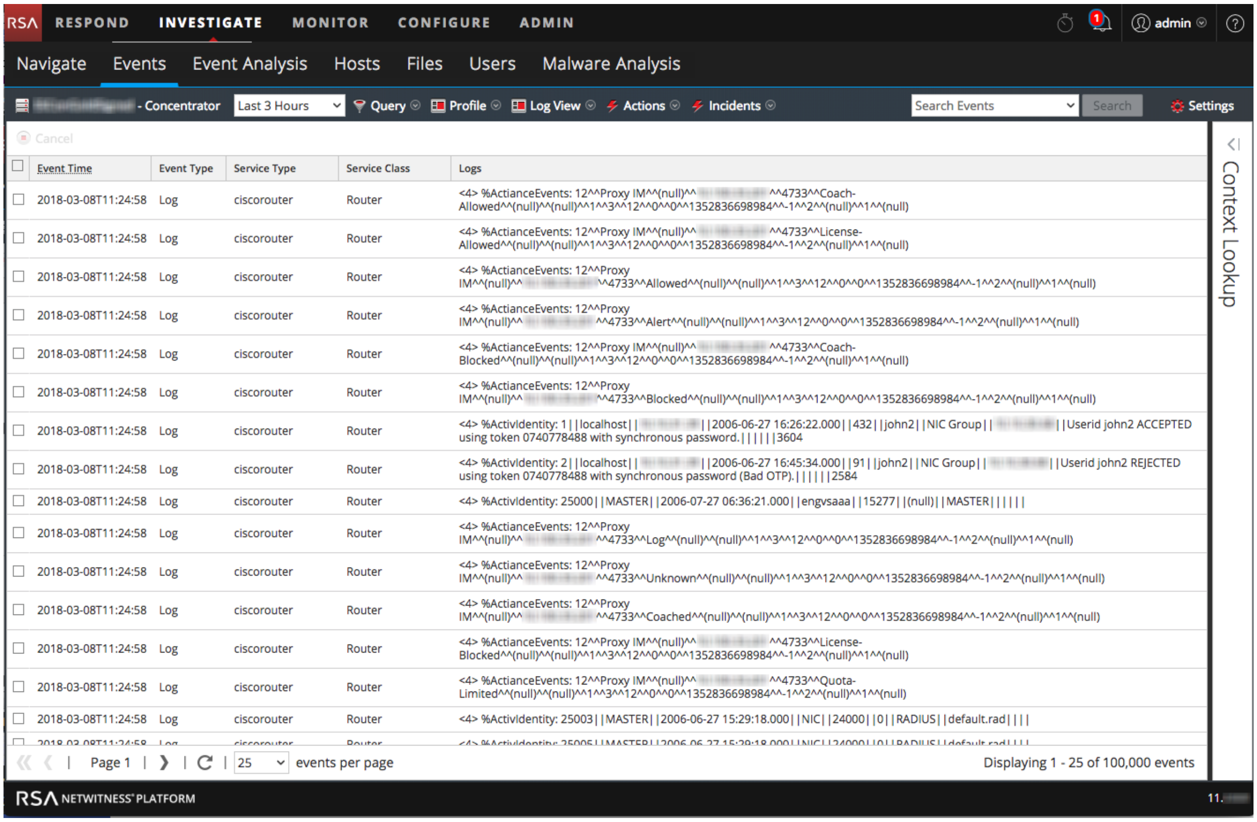
50 Alerts (First 50 Results)

The following figure is an example of events in the List View.



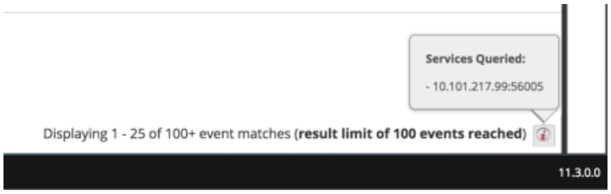
□	Collection Time	Event Type	Size	Details
□	2018-07-23T06:54:15	Log	128 bytes	
□	2018-07-23T06:54:15	Log	105 bytes	
□	2018-07-23T06:54:15	Log	133 bytes	
□	2018-07-23T06:54:15	Log	138 bytes	
□	2018-07-23T06:54:15	Log	143 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:54:27	Log	347 bytes	
□	2018-07-23T06:56:28	Log	136 bytes	<-> [redacted] -> [redacted]
□	2018-07-23T06:56:45	Log	136 bytes	<-> [redacted] -> [redacted]
□	2018-07-23T06:58:05	Log	136 bytes	<-> [redacted] -> [redacted]
□	2018-07-23T06:58:18	Log	136 bytes	<-> [redacted] -> [redacted]
□	2018-07-23T06:55:24	Network	5 KB	<-> [redacted] -> [redacted] 52680 -> 50004
□	2018-07-23T06:55:24	Network	52 KB	<-> [redacted] -> [redacted] 51534 -> 5672
□	2018-07-23T06:55:24	Network	45 KB	<-> [redacted] -> [redacted] 54026 -> 56004
□	2018-07-23T06:55:24	Network	3 KB	<-> [redacted] -> [redacted] 51548 -> 5672
□	2018-07-23T06:55:24	Network	5 KB	<-> [redacted] -> [redacted] 52686 -> 50004
□	2018-07-23T06:55:26	Network	5 KB	<-> [redacted] -> [redacted] 52688 -> 50004

The following figure is an example of the Log View.



<table>
<tr><th>□</th><th>Event Time</th><th>Event Type</th><th>Service Type</th><th>Service Class</th><th>Logs</th></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Coach-Allowed^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^License-Allowed^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Allowed^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Alert^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Coach-Blocked^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Blocked^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActivIdentity: 1||localhost|| [redacted] ||2006-06-27 16:26:22.000||432||john2||NIC Group|| [redacted] ||Userid john2 ACCEPTED using token 0740778488 with synchronous password.||||||3604</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActivIdentity: 2||localhost|| [redacted] ||2006-06-27 16:45:34.000||91||john2||NIC Group|| [redacted] ||Userid john2 REJECTED using token 0740778488 with synchronous password (Bad OTP).||||||2584</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActivIdentity: 25000||MASTER||2006-07-27 06:36:21.000||engvsaaa||15277||(null)||MASTER|||||</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Log^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Unknown^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Coached^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^License-Blocked^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActianceEvents: 12^^Proxy IM^^(null)^^ [redacted] ^^4733^^Quota-Limited^^(null)^^(null)^^1^^3^^12^^0^^0^^1352836698984^^-1^^2^^(null)^^1^^(null)</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActivIdentity: 25003||MASTER||2006-06-27 15:29:18.000||NIC||24000||0||RADIUS||default.rad|||</td></tr>
<tr><td>□</td><td>2018-03-08T11:24:58</td><td>Log</td><td>ciscorouter</td><td>Router</td><td><4> %ActivIdentity: 25005||MASTER||2006-06-27 15:29:18.000||NIC||24000||0||RADIUS||default.rad|||</td></tr>
</table>

The following figure shows the information added to the footer for Version 11.3 and later.



Services Queried:
- 10.101.217.99:56005

Displaying 1 - 25 of 100+ event matches **(result limit of 100 events reached)**

11.3.0.0

Detailed Description

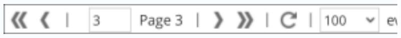
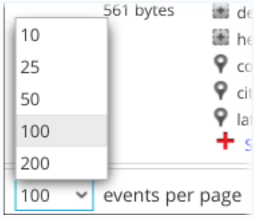
The Legacy Events view has a toolbar at the top with the following options.

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 Query in the Navigate and Legacy Events Views).
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 Legacy Events view (column groups and queries) as you investigate events. (see Use Query 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 Legacy 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 Legacy 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 in the Navigate and Legacy Events Views.
Settings	Displays the Investigation settings for the Legacy Events view (which are also available in the Profile view) so that you can change Investigation settings without navigating away from the Legacy Events view. When you change a setting In the Legacy Events view, the setting is also changed in the Profile view (see Configure the Navigate View and Legacy Events View).

Other features of the Legacy 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 Events 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  561 bytes 10 25 50 100 200 100 events per 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.

Manage Default Meta Keys Dialog

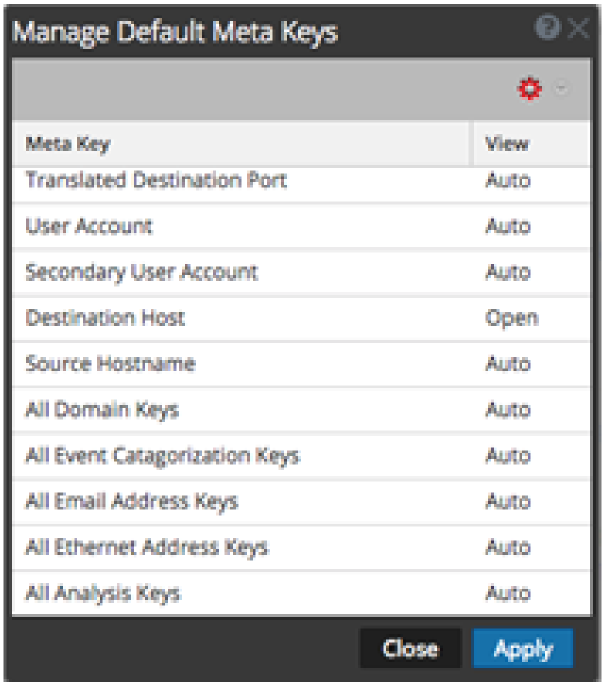
In the Manage Default Meta Keys dialog, analysts can specify the meta keys to be displayed in the Navigate view > Values panel (see Manage and Apply Default Meta Keys in an Investigation. This can help you find the desired data more quickly and prevents the loading of meta keys that are not of interest. To access this dialog, in the **Navigate View** toolbar, select **Meta > Manage Default Meta Keys**.

Related Topics

- How NetWitness Investigate Works
- Use Meta Groups to Focus on Relevant Meta Keys

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.



Meta Key	View
Translated Destination Port	Auto
User Account	Auto
Secondary User Account	Auto
Destination Host	Open
Source Hostname	Auto
All Domain Keys	Auto
All Event Catagorization Keys	Auto
All Email Address Keys	Auto
All Ethernet Address Keys	Auto
All Analysis Keys	Auto

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).

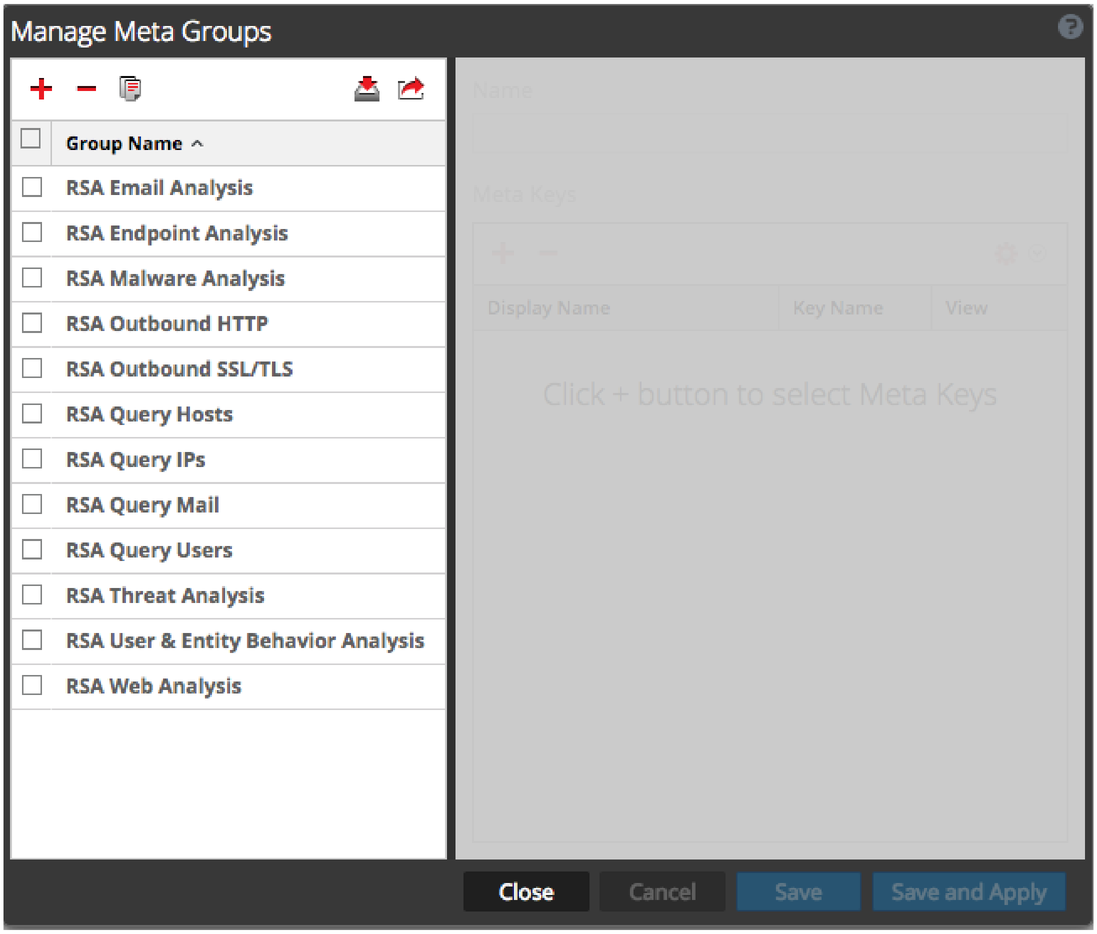
To access this dialog in the **INVESTIGATE > Navigate view** toolbar, select **Meta > Manage Meta Groups**

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.



Manage Meta Groups

□	Group Name ^
□	RSA Email Analysis
□	RSA Endpoint Analysis
□	RSA Malware Analysis
□	RSA Outbound HTTP
□	RSA Outbound SSL/TLS
□	RSA Query Hosts
□	RSA Query IPs
□	RSA Query Mail
□	RSA Query Users
□	RSA Threat Analysis
□	RSA User & Entity Behavior Analysis
□	RSA Web Analysis

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.
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.

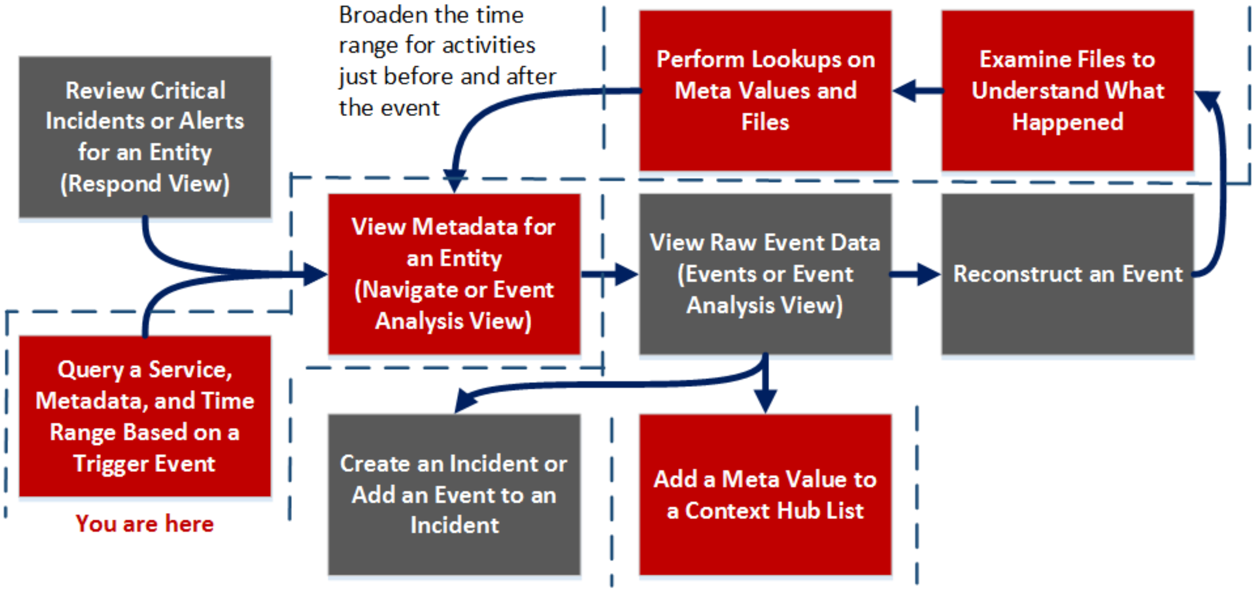
Feature	Description
Close	Closes the dialog.
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and immediately applies all changes.

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. This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Broaden the time range for activities just before and after the event
Review Critical Incidents or Alerts for an Entity (Respond View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Metadata for an Entity (Navigate or Event Analysis View)
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Query a Service, Metadata, and Time Range Based on a Trigger Event
You are here
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Legacy Events or the Events 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*
Threat Hunter	query a service, metadata, and time range*	Filter Results in the Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata*	Analyze Events in the Events View Refining the Results Set
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files*	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups*	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list*	Look Up Additional Context for Results

*You can perform this task in the current view.

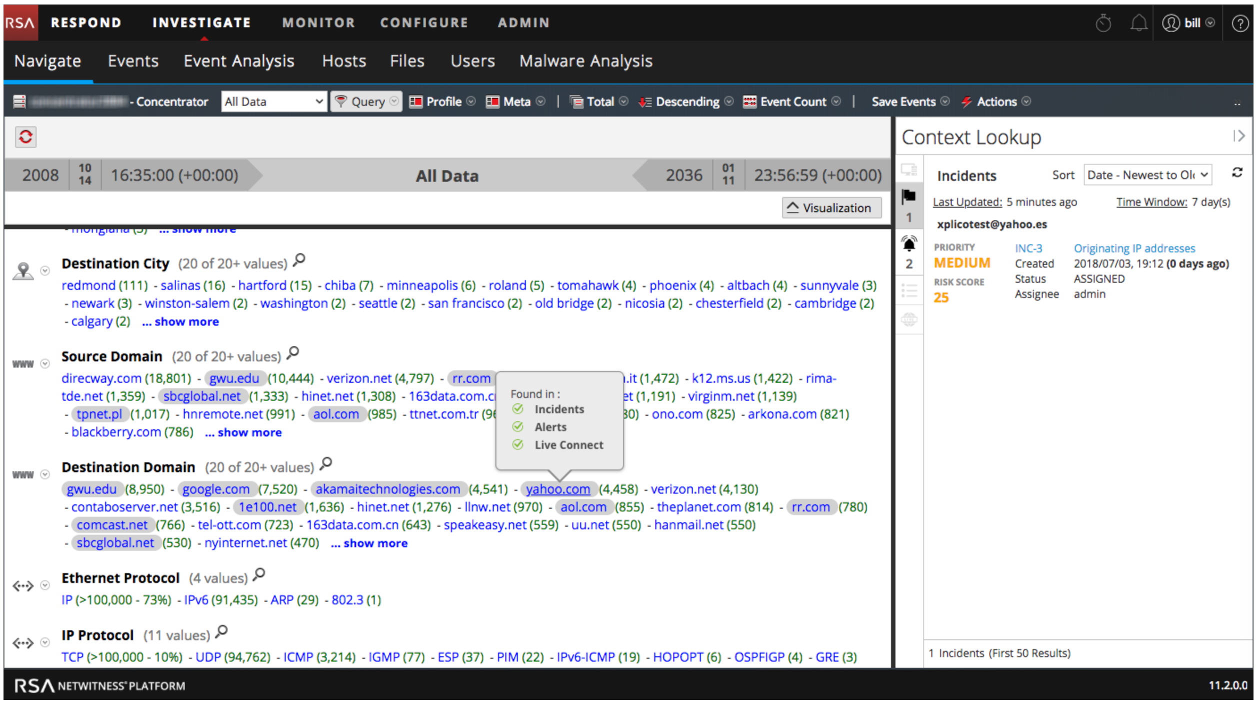
Related Topics

- How NetWitness Investigate Works
- Legacy Events View

- Events View

Quick Look

This figure illustrates the 11.2 Navigate view.



- mongiana (3) ... show more

Destination City (20 of 20+ values)
redmond (111) - salinas (16) - hartford (15) - chiba (7) - minneapolis (6) - roland (5) - tomahawk (4) - phoenix (4) - altbach (4) - sunnyvale (3) - newark (3) - winston-salem (2) - washington (2) - seattle (2) - san francisco (2) - old bridge (2) - nicosia (2) - chesterfield (2) - cambridge (2) - calgary (2) ... show more

Source Domain (20 of 20+ values)
direcway.com (18,801) - gwu.edu (10,444) - verizon.net (4,797) - rr.com .it (1,472) - k12.ms.us (1,422) - rima-tde.net (1,359) - sbcglobal.net (1,333) - hinet.net (1,308) - 163data.com.c et (1,191) - virginm.net (1,139) - tpnet.pl (1,017) - hnremote.net (991) - aol.com (985) - ttnet.com.tr (9 30) - ono.com (825) - arkona.com (821) - blackberry.com (786) ... show more

Destination Domain (20 of 20+ values)
gwu.edu (8,950) - google.com (7,520) - akamaitechnologies.com (4,541) - yahoo.com (4,458) - verizon.net (4,130) - contaboserver.net (3,516) - 1e100.net (1,636) - hinet.net (1,276) - llnw.net (970) - aol.com (855) - theplanet.com (814) - rr.com (780) - comcast.net (766) - tel-ott.com (723) - 163data.com.cn (643) - speakeasy.net (559) - uu.net (550) - hanmail.net (550) - sbcglobal.net (530) - nyinternet.net (470) ... show more

Ethernet Protocol (4 values)
IP (>100,000 - 73%) - IPv6 (91,435) - ARP (29) - 802.3 (1)

IP Protocol (11 values)
TCP (>100,000 - 10%) - UDP (94,762) - ICMP (3,214) - IGMP (77) - ESP (37) - PIM (22) - IPv6-ICMP (19) - HOPOPT (6) - OSPFIGP (4) - GRE (3)

Context Lookup

Incidents Sort Date - Newest to Ol

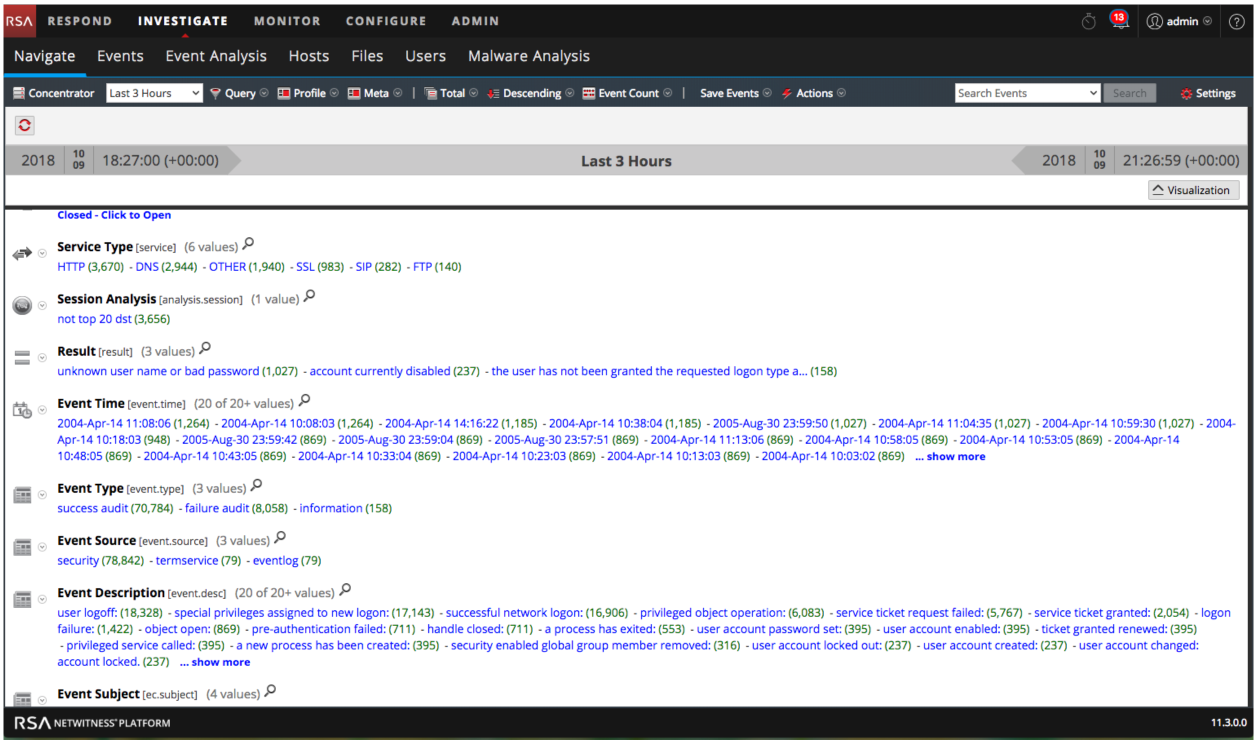
Last Updated: 5 minutes ago Time Window: 7 day(s)

xplicotest@yahoo.es

PRIORITY MEDIUM
RISK SCORE 25
INC-3 Originating IP addresses
Created 2018/07/03, 19:12 **(0 days ago)**
Status ASSIGNED
Assignee admin

1 Incidents (First 50 Results)

This figure illustrates the 11.3 Navigate view.



Closed - Click to Open

Service Type [service] (6 values)
HTTP (3,670) - DNS (2,944) - OTHER (1,940) - SSL (983) - SIP (282) - FTP (140)

Session Analysis [analysis.session] (1 value)
not top 20 dst (3,656)

Result [result] (3 values)
unknown user name or bad password (1,027) - account currently disabled (237) - the user has not been granted the requested logon type a... (158)

Event Time [event.time] (20 of 20+ values)
2004-Apr-14 11:08:06 (1,264) - 2004-Apr-14 10:08:03 (1,264) - 2004-Apr-14 14:16:22 (1,185) - 2004-Apr-14 10:38:04 (1,185) - 2005-Aug-30 23:59:50 (1,027) - 2004-Apr-14 11:04:35 (1,027) - 2004-Apr-14 10:59:30 (1,027) - 2004-Apr-14 10:18:03 (948) - 2005-Aug-30 23:59:42 (869) - 2005-Aug-30 23:59:04 (869) - 2005-Aug-30 23:57:51 (869) - 2004-Apr-14 11:13:06 (869) - 2004-Apr-14 10:58:05 (869) - 2004-Apr-14 10:53:05 (869) - 2004-Apr-14 10:48:05 (869) - 2004-Apr-14 10:43:05 (869) - 2004-Apr-14 10:33:04 (869) - 2004-Apr-14 10:23:03 (869) - 2004-Apr-14 10:13:03 (869) - 2004-Apr-14 10:03:02 (869) ... show more

Event Type [event.type] (3 values)
success audit (70,784) - failure audit (8,058) - information (158)

Event Source [event.source] (3 values)
security (78,842) - termservice (79) - eventlog (79)

Event Description [event.desc] (20 of 20+ values)
user logoff: (18,328) - special privileges assigned to new logon: (17,143) - successful network logon: (16,906) - privileged object operation: (6,083) - service ticket request failed: (5,767) - service ticket granted: (2,054) - logon failure: (1,422) - object open: (869) - pre-authentication failed: (711) - handle closed: (711) - a process has exited: (553) - user account password set: (395) - user account enabled: (395) - ticket granted renewed: (395) - privileged service called: (395) - a new process has been created: (395) - security enabled global group member removed: (316) - user account locked out: (237) - user account created: (237) - user account changed: account locked. (237) ... show more

Event Subject [ec.subject] (4 values)

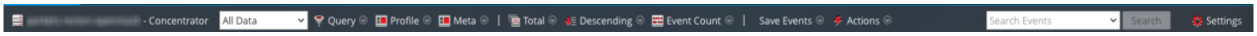
The Navigate view consists of these features:

- 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 Legacy Events view or Events 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.

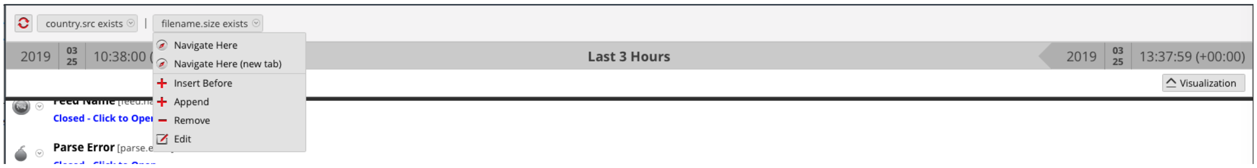
Option	Description
	Displays the selected service name next to the icon. Clicking the icon opens the Investigate a Service dialog, in which you can select a service to investigate and set the default service to investigate (see Begin an Investigation in the Navigate or Legacy Events View). Changing the 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), the Legacy Events view, and the Events view (column groups and queries). See Use Query 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 Use Meta Groups to Focus on Relevant Meta Keys).
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 Refining the Results Set). In Version 11.1 and later, the options are Visualize, Go to event in Event Reconstruction, Go to event in Events view, 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 Legacy Events view and the Investigations profile (see Search for Text Patterns in the Navigate and Legacy Events Views).
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 Legacy 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 Query in the Navigate and Legacy Events Views).
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 Query in the Navigate and Legacy Events Views).
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.

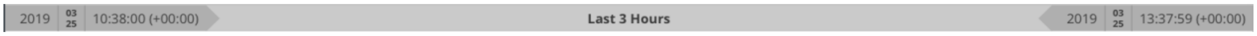
For example:

```
(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.

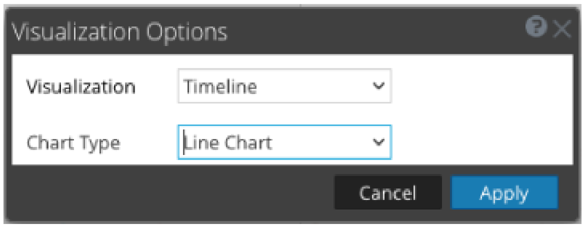


Visualizations

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

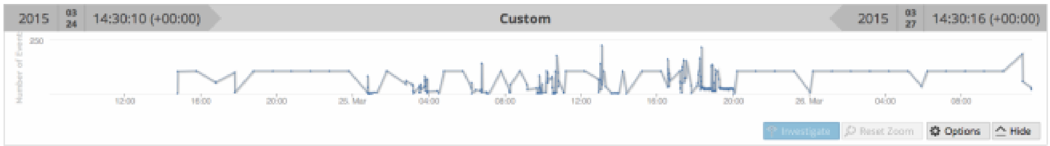
The timeline is the count of the number of events that occur at a specific instance. The timeline provides event counts so that you can see if the number of events increases drastically at a given point in time. The timeline displays activity for the specified service and time range as a line chart or 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.

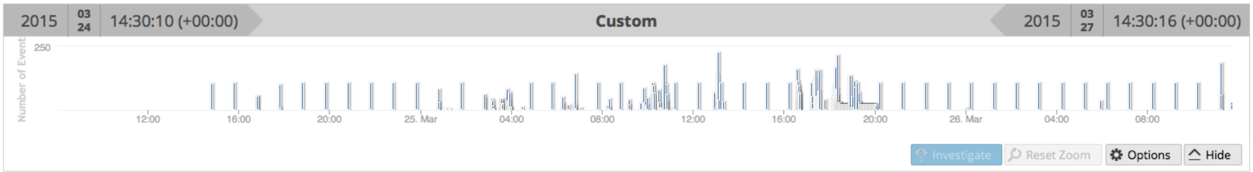


Visualization Options

Visualization: Timeline

Chart Type: Line Chart



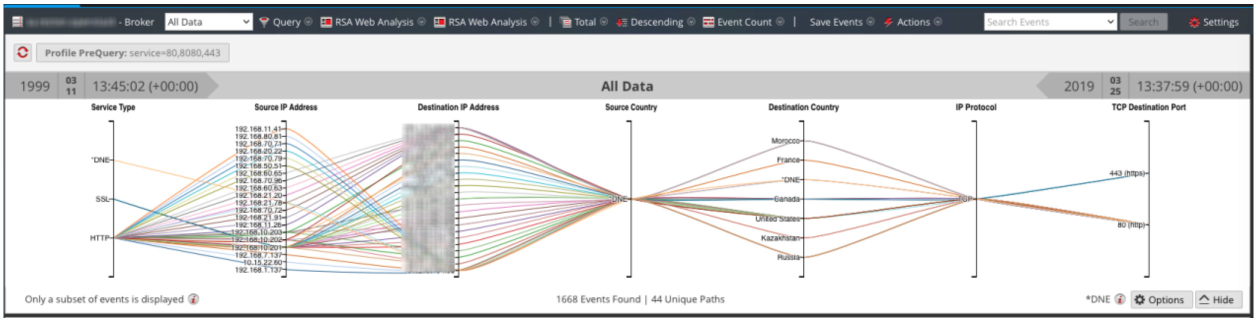


The timeline displays activity for the specified service and time range, as a line chart or a bar chart based on your choice in the Options menu.

Feature	Description
Number of Events (Timeline)	The Y axis of the chart based on thousands of events.
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.



Profile PreQuery: service=80,8080,443

Only a subset of events is displayed

1668 Events Found | 44 Unique Paths

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.

Feature	Description
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.
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.

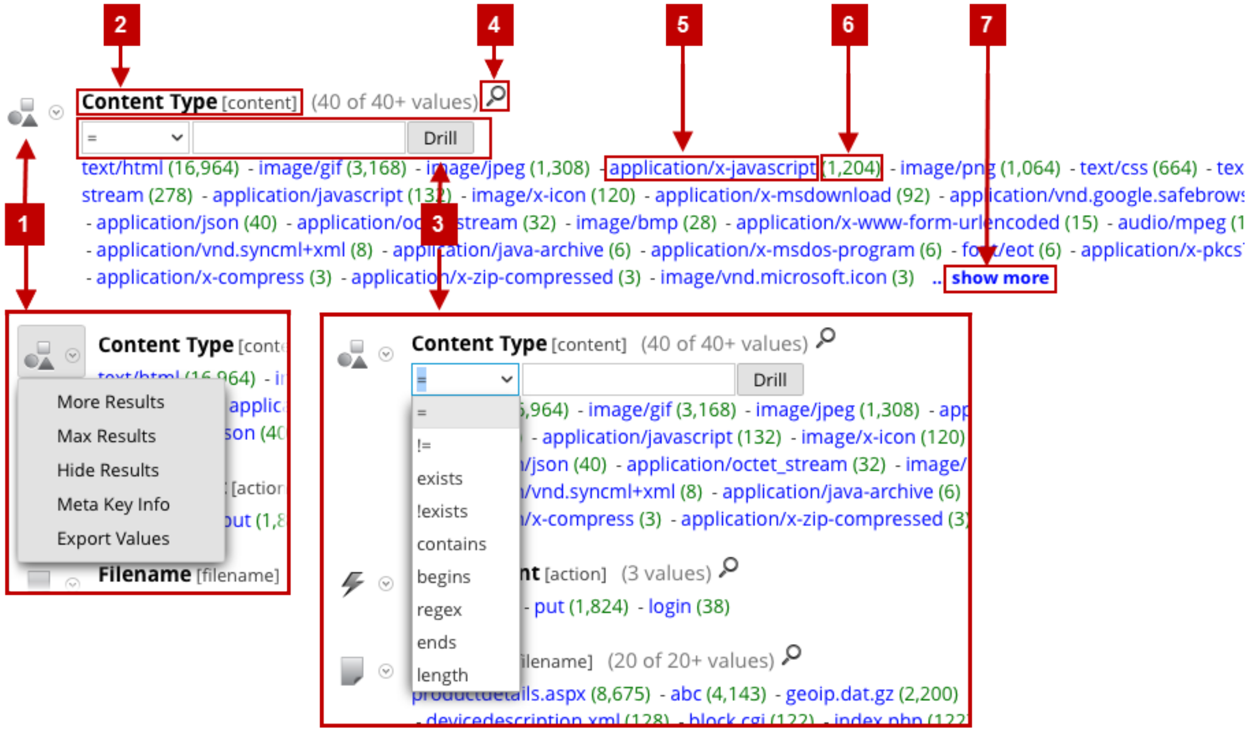
Feature	Description
Visualization selection	Displays a drop-down list of visualization types: Timeline and Coordinates
All Meta Keys Must Exist in an Event	Limits the data represented in the visualization to only those events that include all selected meta keys. This can result in a cleaner, more targeted 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.
ℹ	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.
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.



1
2
3
4
5
6
7
Content Type [content] (40 of 40+ values)
=
Drill
text/html (16,964) - image/gif (3,168) - image/jpeg (1,308) - application/x-javascript (1,204) - image/png (1,064) - text/css (664)
stream (278) - application/javascript (132) - image/x-icon (120) - application/x-msdownload (92)
- application/json (40) - application/octet_stream (32) - image/bmp (28) - application/x-www-form-urlencoded (15) - audio/mpeg
- application/vnd.syncml+xml (8) - application/java-archive (6) - application/x-msdos-program (6) - font/eot (6)
- application/x-compress (3) - application/x-zip-compressed (3) - image/vnd.microsoft.icon (3)
show more
More Results
Max Results
Hide Results
Meta Key Info
Export Values
Filename [filename]
=
!=
exists
!exists
contains
begins
regex
ends
length
[action] (3 values)
put (1,824) - login (38)
(20 of 20+ values)
productdetails.aspx (8,675) - abc (4,143) - geoip.dat.gz (2,200)

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

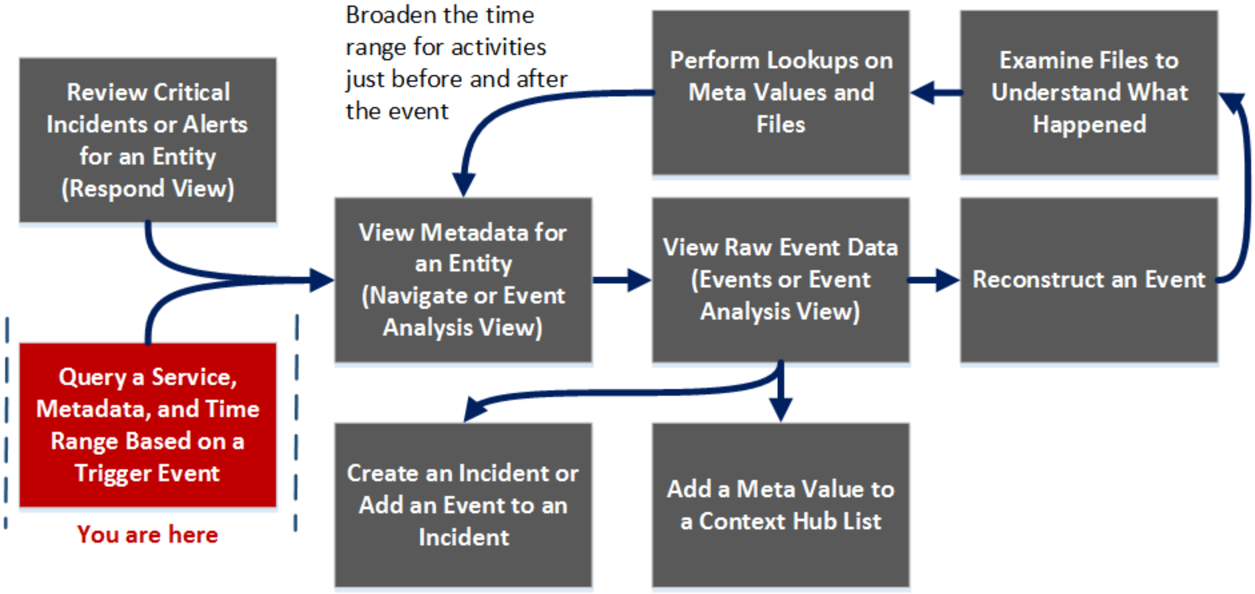
For each meta key, there is a list of values (blue text) and counts (green text) found in the current drill point. When you click a value to drill down into a subset of the currently selected data, the display is updated and the new drill point is recorded in the breadcrumb. You can specify the sorting and quantification methods for the values list using the option in the toolbar.

Query Dialog

In the Navigate view or Legacy 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 **Legacy Events** view toolbar, select **Query**.

Workflow

This workflow has references to several views that were renamed in Version 11.4: the Event Analysis view became Events view, the Events view became Legacy Events view.


Review Critical Incidents or Alerts for an Entity (Respond View)
Query a Service, Metadata, and Time Range Based on a Trigger Event
You are here
Broaden the time range for activities just before and after the event
View Metadata for an Entity (Navigate or Event Analysis View)
Perform Lookups on Meta Values and Files
Examine Files to Understand What Happened
View Raw Event Data (Events or Event Analysis View)
Reconstruct an Event
Create an Incident or Add an Event to an Incident
Add a Meta Value to a Context Hub List

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 Events View Filter Results in the Navigate View Create a Query in the Navigate and Legacy Events Views Filter Results in the Legacy Events View
Threat Hunter	view metadata	Analyze Events in the Events View Refining the Results Set

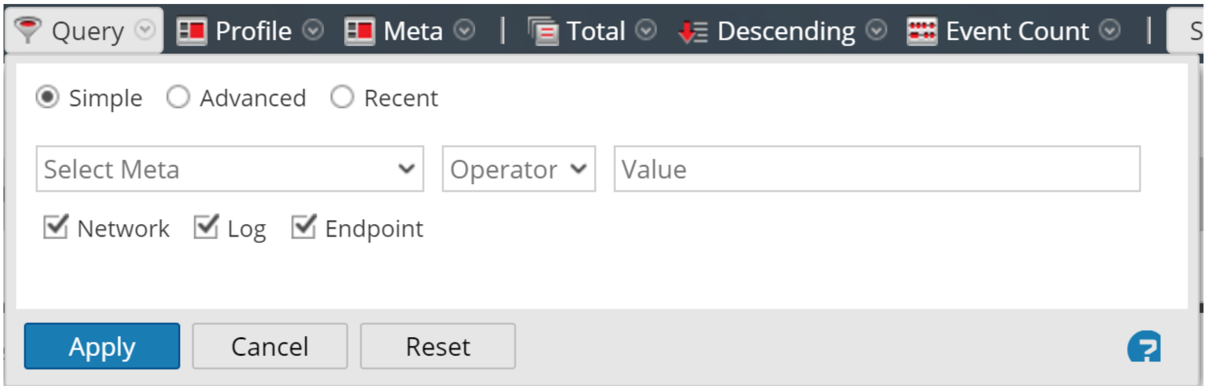
User Role	I want to ...	Show me how
Threat Hunter	view raw event data	Filter Results in the Events View Analyze Events in the Events View Filter Results in the Legacy Events View
Threat Hunter	reconstruct the event	Analyze Events in the Events View Reconstruct an Event in the Events View Reconstruct an Event in the Legacy Events View
Threat Hunter	examine files	Download Data in the Events View Export or Print a Drill Point in the Navigate View Export Events in the Legacy Events View
Threat Hunter	perform lookups	Look Up Additional Context for Results Launch a Lookup of a Meta Key
Threat Hunter	create an incident or add to an incident	Add Events to an Incident in the Legacy Events View Add Events to an Incident in the Events View
Threat Hunter	add a meta value to a Context Hub list	Look Up Additional Context for Results

*You can perform this task in the current view.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Legacy Events View

Quick Look

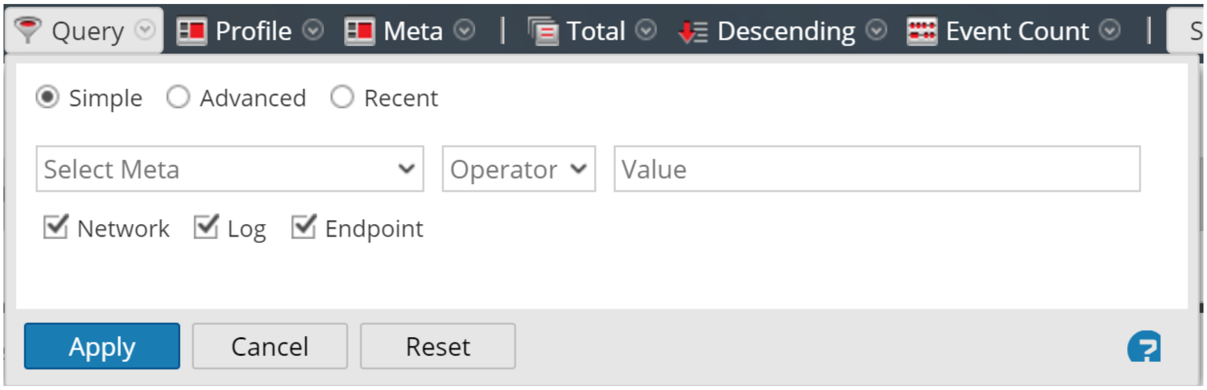


The Query dialog has three views:

- 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

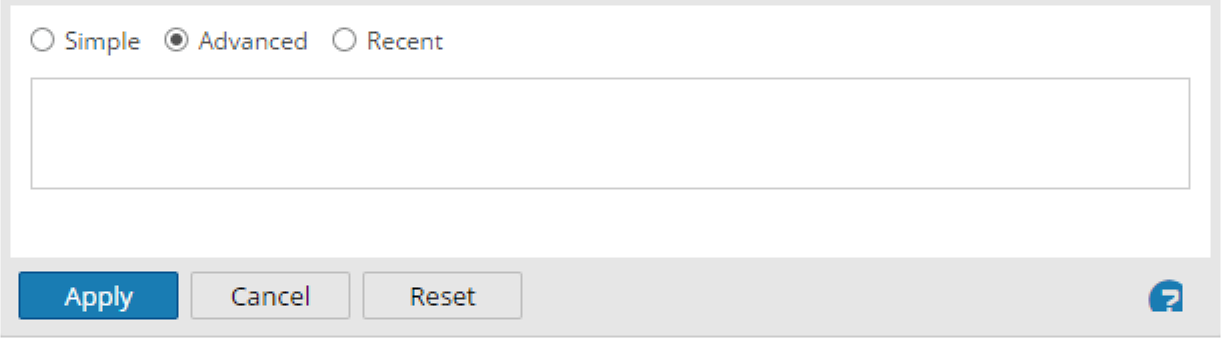


● Simple ○ Advanced ○ Recent

Select Meta | Operator | Value

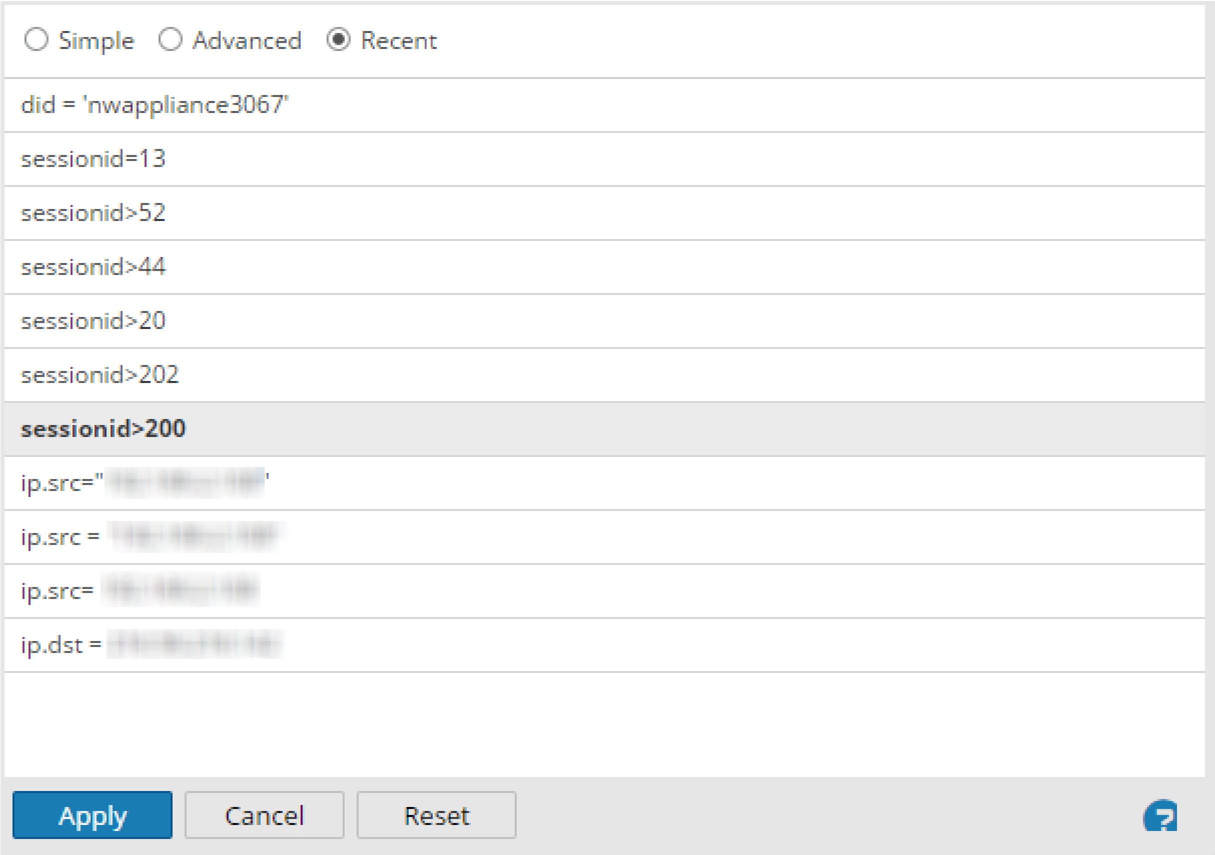
☑ Network ☑ Log ☑ Endpoint

Advanced View



○ Simple ● Advanced ○ Recent

Recent View



○ Simple ○ Advanced ● Recent

did = 'nwappliance3067'

sessionid=13

sessionid>52

sessionid>44

sessionid>20

sessionid>202

sessionid>200

ip.src="[redacted]'

ip.src = [redacted]

ip.src= [redacted]

ip.dst = [redacted]

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.

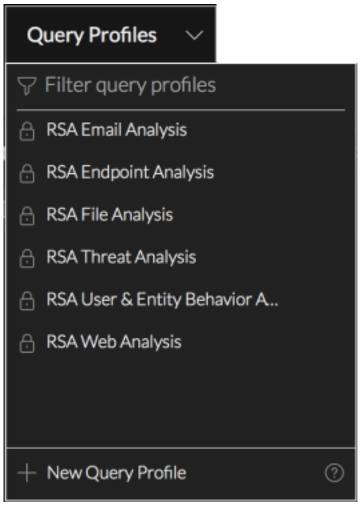
Feature	Description
Query list	Allows you to select a query from a list of recent queries in the Recent view. Double-clicking a query automatically applies it.
Apply	Applies the new query to the current Investigation view.
Cancel	Closes the dialog without applying changes.
Reset	Resets all fields.

Query Profiles Dialogs

Query profiles allow you to set up custom views in the Navigate view, Events view, and Legacy Events view based on a meta group, column group, and limiting query (see Use Query Profiles to Encapsulate Common Areas for Investigation). Built-in profiles are available when you first log in; the names begin with the RSA prefix and are grouped under Default Profiles. You cannot edit or delete built-in profiles.

You can manage built-in profiles and custom profiles in the Manage Profiles dialog, the Create Query Profile dialog and the Query Profile Details dialog.

- The Manage Profiles dialog is for the Navigate view, the Legacy Events view (Version 11.4) , and the Events view (Version 11.3 and earlier). The Manage Profiles dialog has features that are not yet available in the Query Profile dialog: select a meta group for the profile, import and export profiles, copy and edit profiles, and organize profiles into profile groups. To access this dialog, select **Profile > Manage Profiles** in the **Navigate** or **Legacy Events** view toolbar.
- The Create Query Profile dialog is for the 11.4 Events view. To access this dialog, select **Query Profiles > New Query Profile** in the **Events** view toolbar.



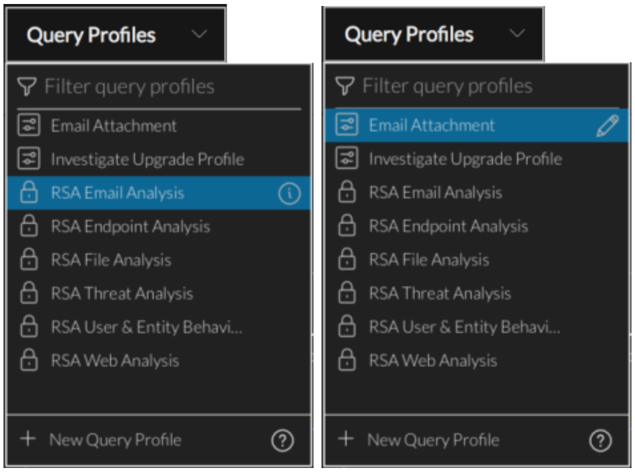
- The Query Profile Details dialog is for the 11.4 Events view. To access this dialog, select **Query Profiles** in the **Events** view toolbar, then click the edit icon (✎) next to a custom profile name.

Related Topics

- How NetWitness Investigate Works
- Navigate View
- Events View
- Legacy Events View

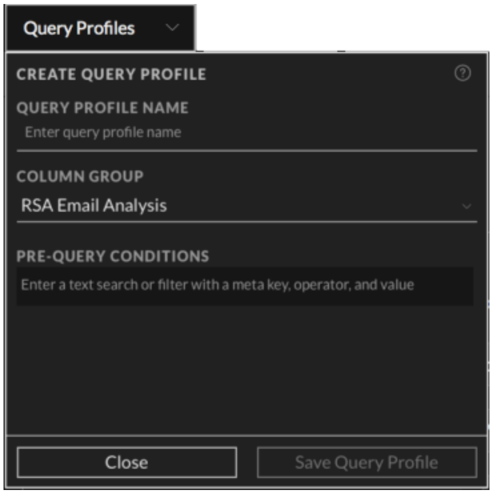
Quick Look - Query Profile Menu, Create Query Profile Dialog, and Query Profile Details Dialog

This section introduces the Query Profile Menu, Query Profile dialog, and the Query Profile Details dialog. The following figure is an example of the Query Profiles menu and the table describes the options. The example on the left has built-in profile highlighted so that the information icon is visible. The example on the right has a custom profile highlighted so that the edit icon is visible.



Feature	Description
Filter Query Profiles	Filters the list of profiles as you type text so that only profile names that contain that text are displayed.
Query Profile List	The list of profiles consists of custom and built-in profiles, which are distinguished by the icons that precede the name. In the example, Email Attachment and Investigate Upgrade Profile are custom profiles. The RSA profiles are built-in profiles.
New Query Profile	Displays the Create Query Profile dialog, where you can create a custom profile.

The Create Query Profile dialog, shown in the figure on the left, allows you to define a custom profile. The figure on the right illustrates the Query Profile Details dialog, in which you can edit a custom profile. The table describes the fields and options in the dialogs.

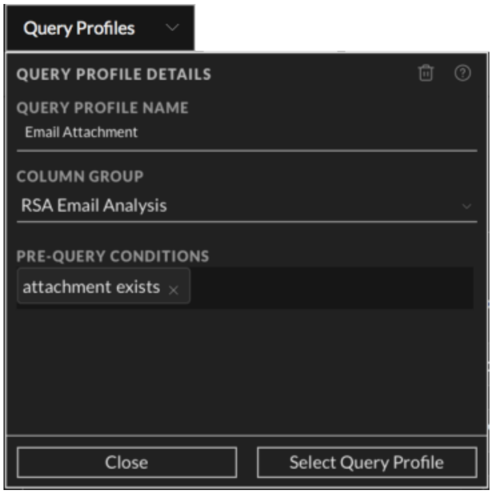


CREATE QUERY PROFILE

QUERY PROFILE NAME: Enter query profile name

COLUMN GROUP: RSA Email Analysis

PRE-QUERY CONDITIONS: Enter a text search or filter with a meta key, operator, and value



QUERY PROFILE DETAILS

QUERY PROFILE NAME: Email Attachment

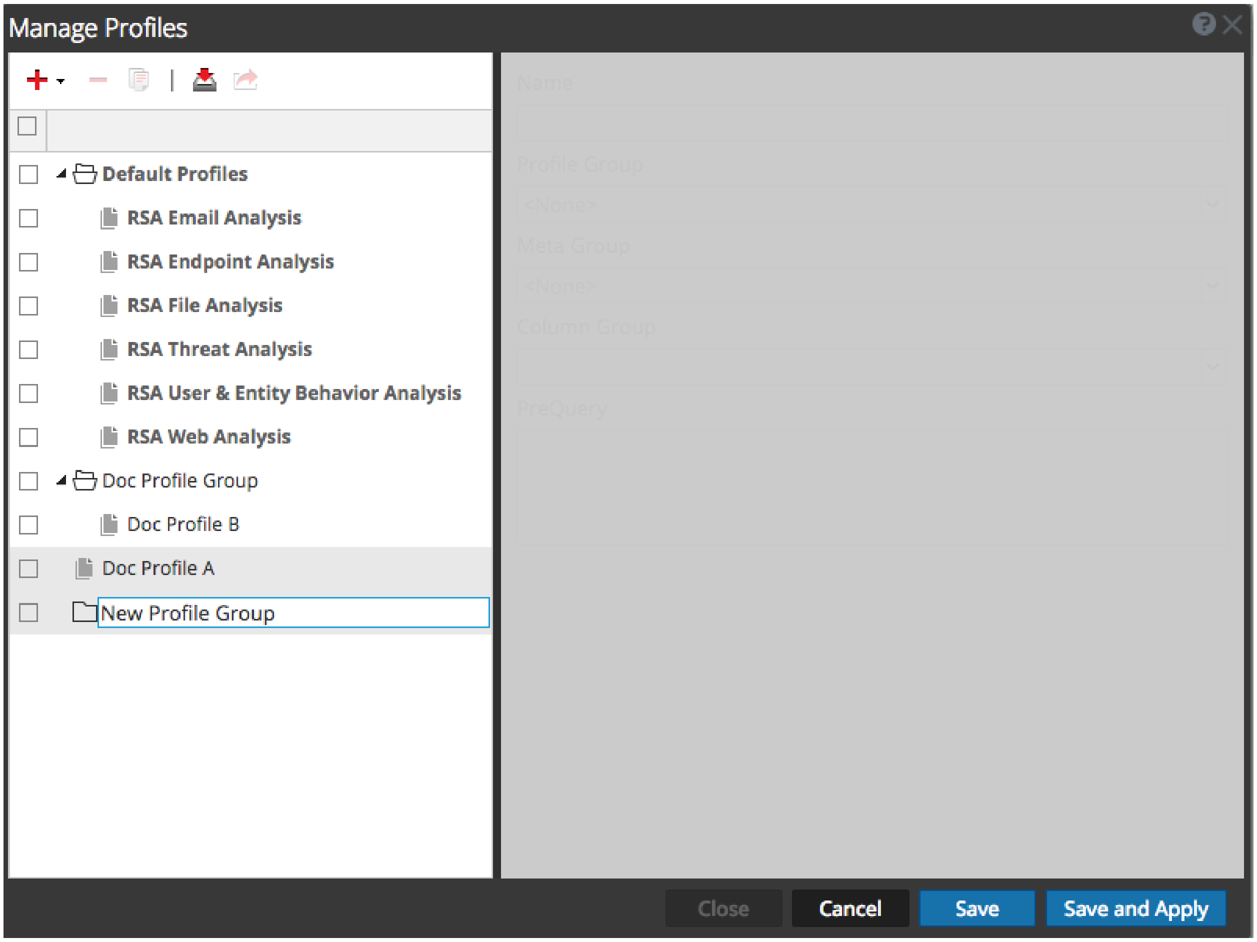
COLUMN GROUP: RSA Email Analysis

PRE-QUERY CONDITIONS: attachment exists

Feature	Description
🗑	Deletes the custom profile in the Query Profile Details dialog. This action is irreversible and applies globally; the profile is no longer available to anyone who is using the profiles on this service.
Query Profile Name	Displays the name of the profile. The name must be unique and contain fewer than 64 characters. You can edit the name in a custom profile.
Column Group	Displays a drop-down menu listing available column groups, with the currently selected column group from the Events list already selected. You can change the column group in a custom profile.
PreQuery Conditions	Defines a limiting query for filtering Investigate results. If you had a query active in the query bar when you began to create the new profile, the active query is added to the preQuery field. In a custom profile, you can delete the prepopulated preQuery and type additional text for a text search or additional filters in the preQuery field. This query is used when the associated profile is applied and the preQuery applies to any queries used in the Navigate and Events views. This is an example of a preQuery: `'service=80,25,110'`.
Close button	Closes the dialog.
Save Query Profile	For the Create Query Profile dialog only, saves the new profile.
Reset	For the Query Profile Details dialog only, reverts the edited profile to the last saved state.
Update Query Profile	For the Query Profile Details dialog only, applies changes to an edited profile.
Select Query Profile	Applies the query profile.

Quick Look - Manage Profiles Dialog

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.

Field	Description
➦	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 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.

Settings Dialogs for Investigate Views

NetWitness PlatformVersion 11.0 has two settings dialogs, one for the Navigate view and one for the Legacy Events view. With the addition of the settings dialog for the Events view in Version 11.1, Investigate has three settings dialogs.

The settings in these dialogs are a subset of the Investigation settings made in the Profiles > Preferences panel > Investigation. 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 **Legacy Events** view, and select the **Settings** option in the toolbar.

The settings in the Events view have no corresponding settings in the Profiles > Preferences panel.

Related Topics

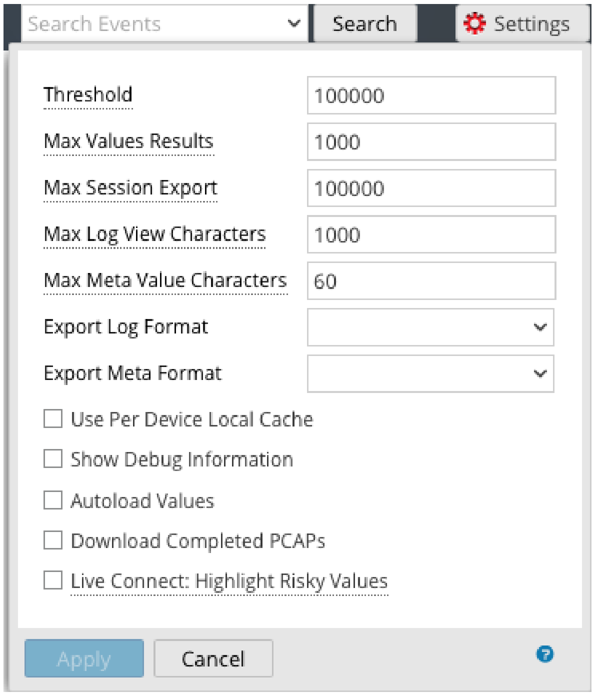
- How NetWitness Investigate Works

Quick Look

This is a quick look at the settings dialog for the Navigate view, Legacy Events view, and Events 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.



Threshold 100000

Max Values Results 1000

Max Session Export 100000

Max Log View Characters 1000

Max Meta Value Characters 60

Export Log Format

Export Meta Format

□ Use Per Device Local Cache

□ Show Debug Information

□ Autoload Values

□ Download Completed PCAPs

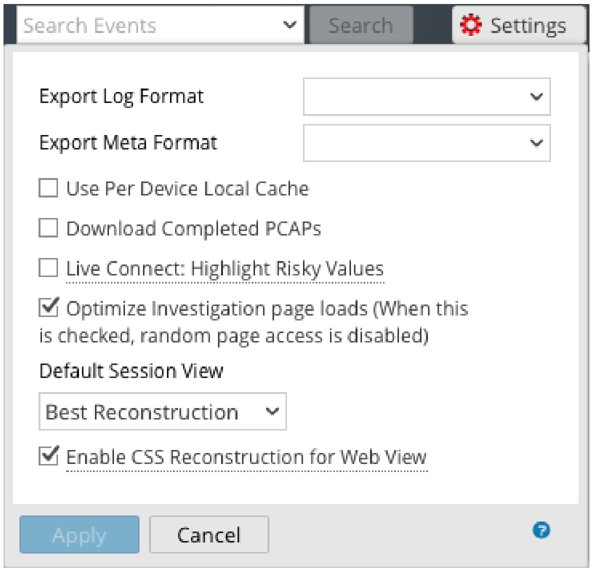
□ Live Connect: Highlight Risky Values

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.

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.
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).
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.

Legacy Events View Settings Dialog

The following figure is an example of the Settings dialog for the Legacy Events view, and the table describes the features.



Export Log Format

Export Meta Format

☐ Use Per Device Local Cache

☐ Download Completed PCAPs

☐ Live Connect: Highlight Risky Values

☑ Optimize Investigation page loads (When this is checked, random page access is disabled)

Default Session View: Best Reconstruction

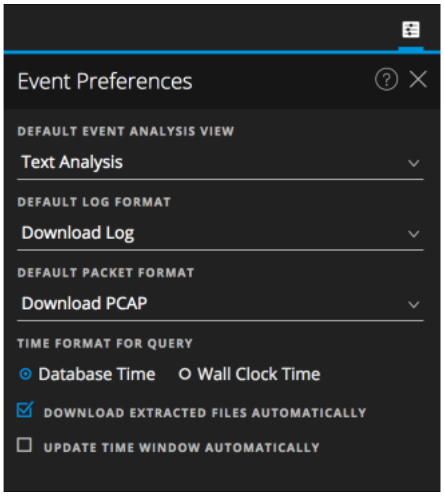
☑ Enable CSS Reconstruction for Web View

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.
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).

Feature	Description
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 Legacy 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.

Events View Preferences Dialog

Beginning with Version 11.1, the Events view has user preferences that you can configure in the Events view > Event Preferences dialog. These settings persist so that they are applied each time you log in and go to the Events view. The following figures are examples of the dialog for Version 11.3 and Version 11.4.1. The table below describes the options.



Event Preferences

DEFAULT EVENT ANALYSIS VIEW

Text Analysis

DEFAULT LOG FORMAT

Download Log

DEFAULT PACKET FORMAT

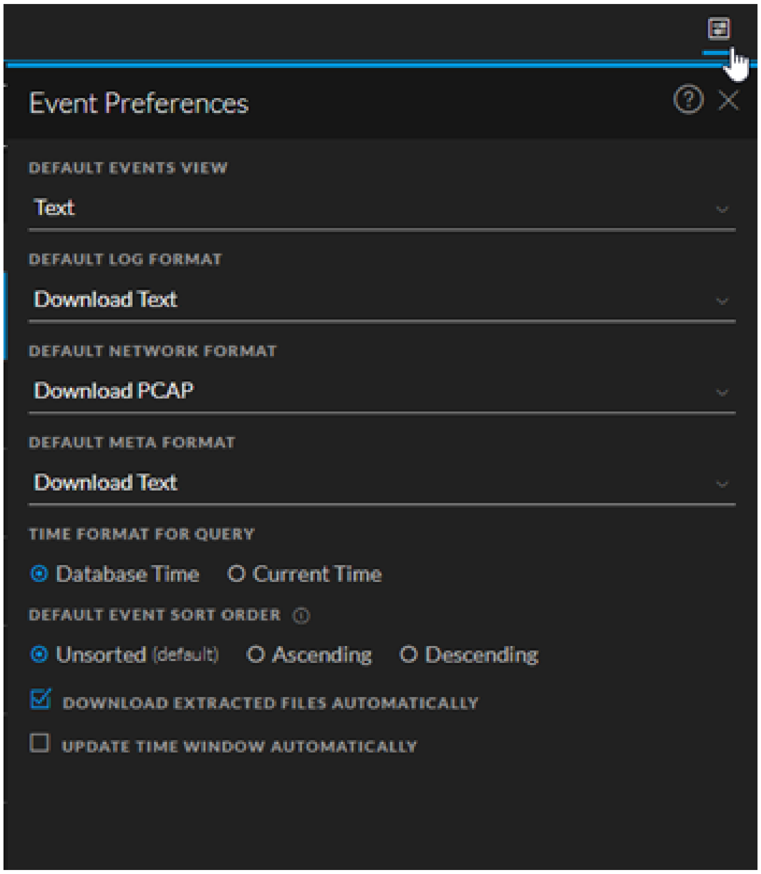
Download PCAP

TIME FORMAT FOR QUERY

● Database Time ○ Wall Clock Time

☑ DOWNLOAD EXTRACTED FILES AUTOMATICALLY

□ UPDATE TIME WINDOW AUTOMATICALLY



Event Preferences

DEFAULT EVENTS VIEW

Text

DEFAULT LOG FORMAT

Download Text

DEFAULT NETWORK FORMAT

Download PCAP

DEFAULT META FORMAT

Download Text

TIME FORMAT FOR QUERY

● Database Time ○ Current Time

DEFAULT EVENT SORT ORDER

● Unsorted (default) ○ Ascending ○ Descending

☑ DOWNLOAD EXTRACTED FILES AUTOMATICALLY

□ UPDATE TIME WINDOW AUTOMATICALLY

Feature	Description
Default Events View	Selects the default event analysis view that is displayed every time you open the Events view. For example, if you select File, the File Analysis panel is highlighted and displayed every time you investigate an event in the Events view. These are following options: • **Text** : View and analyze the raw text payload of an event. • **Packet** : View and interactively analyze the packets and payload of an event. • **File** : 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** or **Download Text**: 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 or Default Network Format	Selects the default format for downloading packets. • **Download PCAP**: To download the entire event as a packet capture (*.pcap) file. • **Download All Payloads** or **Download 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.
Default Meta Format	Selects the default format for downloading metadata: • **Download CSV**: Comma-separated values (CSV) format. • **Download JSON**: The JavaScript Object Notation (JSON) format. • **Download Text**: Plain text format. • **Download TSV**: Tab-separated values (TSV) format.
Time Format for Query	The Events 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 **Current Time** (labeled **Wall Clock Time** in Version 11.3 and earlier) 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.
Event Sort Order (Version 11.4 and Later)	Sets the sort sequence by collection time for the events listed in the Events panel. If results exceed the events limit, not all events can be loaded. The portion of returned events loaded in the Events panel matches the sort order preference: the oldest portion of events is loaded when Ascending order is selected, and newest portion of events is loaded when Descending order is selected. A change to this setting becomes effective the next time you submit a query. **Unsorted**: Default sorting method for Version 11.4.1. To list events as processed by the Core services. Unsorted is faster because it streams back the events as soon as a match is found versus waiting for all Core services to respond and then displaying them in the chosen order. **Ascending**: Default sorting method for Version 11.4. To put the events with the earliest collection time first in the list. **Descending**: To put the events with the latest collection time first in the list. When investigating logs, you may want to change the sort sequence to latest collection time first.

Feature	Description
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 query bar 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.