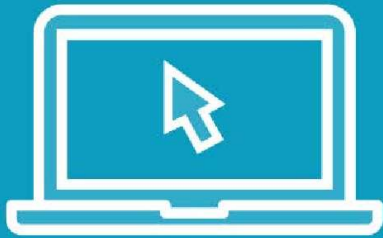


# Basic Splunking Techniques

---



## Overview



Search Terms  
Commands  
Functions  
Arguments  
Clauses

# Splunk Search Language Example

Search

Pipes

```
sourcetype=acc* status=200 | stats list(product_name) as "Games Sold" | top "Games
```

Search Terms

Command  
Function  
Argument  
Clause

Closed Captions

## Preferences



Global



SPL Editor

The advanced editor can provide auto-formatting, line numbers, and highlight search syntax for increased readability. You can also turn off the advanced editor to use the basic search format.

Advanced editor



General

Themes

Search assistant

Full

Compact

None

Full search assistant is useful when first learning to create searches. Compact provides more succinct assistance.

Cancel

Apply

# Search Limitations

Search Command

command/function

command/function

# Search Commands

---

# SPL

Splunk Processing Language

```
source="WinEventLog:*" host="Henson-Lap"
```

## Search Commands



# Chaining Commands

```
source="WinEventLog:*" host="Henson-Lap" | command 1 |  
command 2 ...
```

```
source="WinEventLog:*" host="Henson-Lap" | search EventCode=100
```

## Filtering Results

Allows for users to filter results in query. For example show results where event code = 100

```
source="WinEventLog:*" host="Henson-Lap" | dedup EventCode
```

## Remove Duplicates

Only shows unique events. For example show only EventCodes once

```
[query] | head 10
```

◀ Show first 10 results

```
[query] | reverse
```

◀ Reverse result order

```
[query] | sort user
```

◀ Order by user ascending or user descending

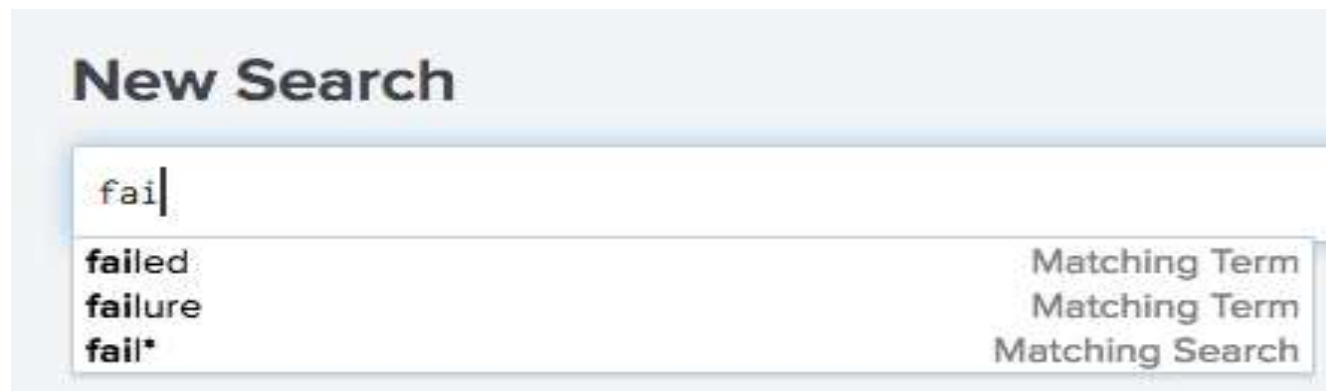
```
[query] | sort -user
```

```
[query] | tail 10
```

◀ Show last 10 results

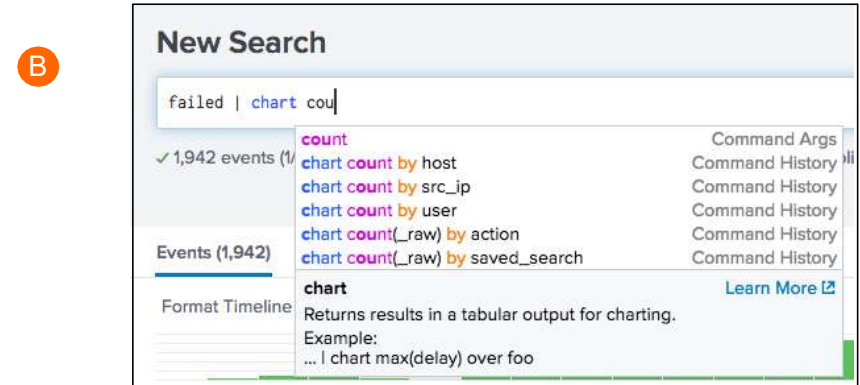
# Search Assistant

- Search Assistant provides selections for how to complete the search string
- Before the first pipe (|), it looks for matching terms
- You can continue typing OR select a term from the list
  - If you select a term from the list, it is added to the search



# Search Assistant (cont.)

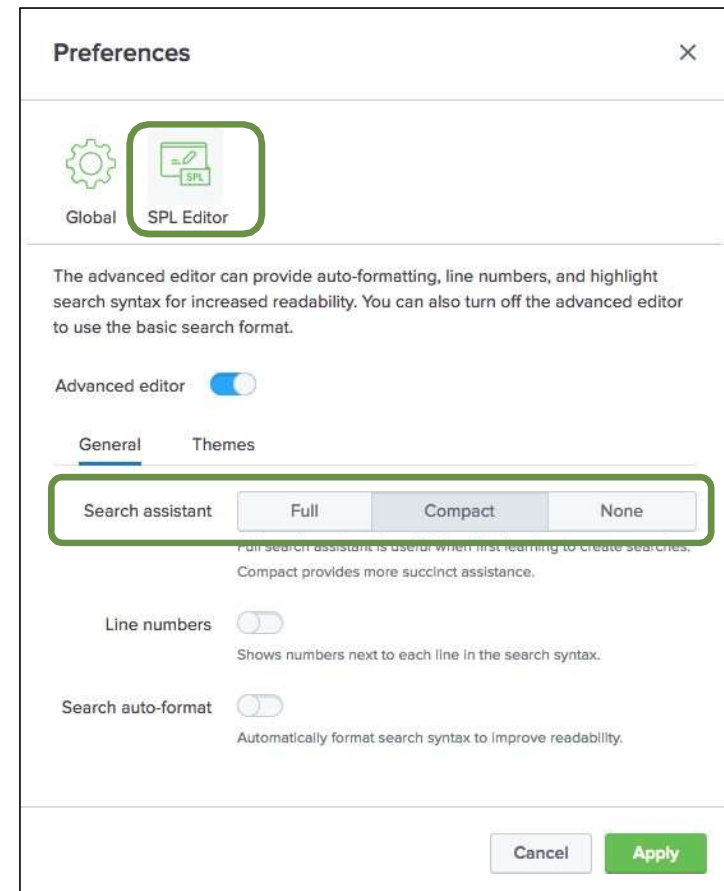
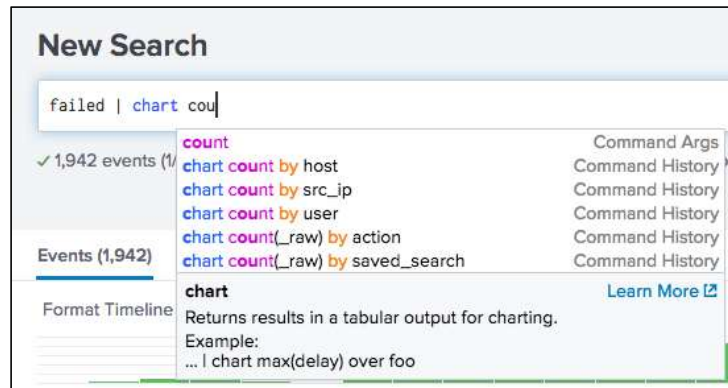
- After the first pipe, the Search Assistant shows a list of commands that can be entered into the search string
- A • You can continue typing OR scroll through and select a command to add
- If you mouse over a command, more information about the command is shown B As you continue to type, Search Assistant makes more suggestions



# Search Assistant (cont.)

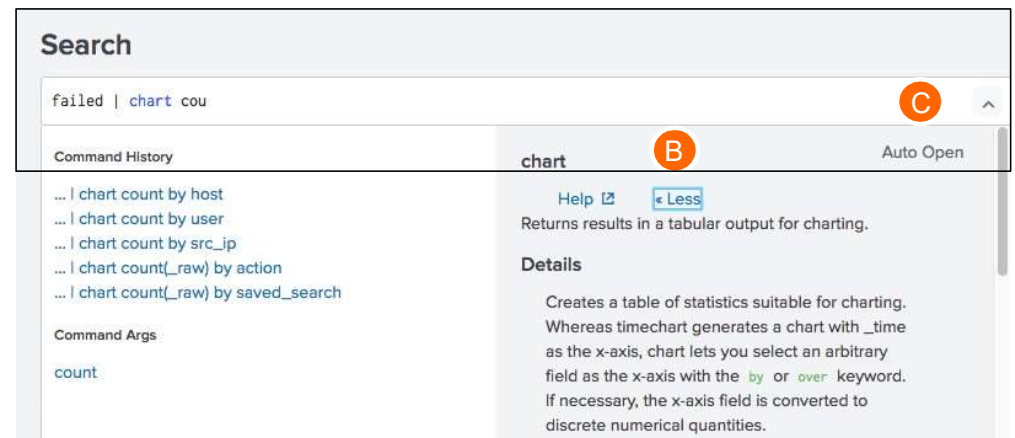
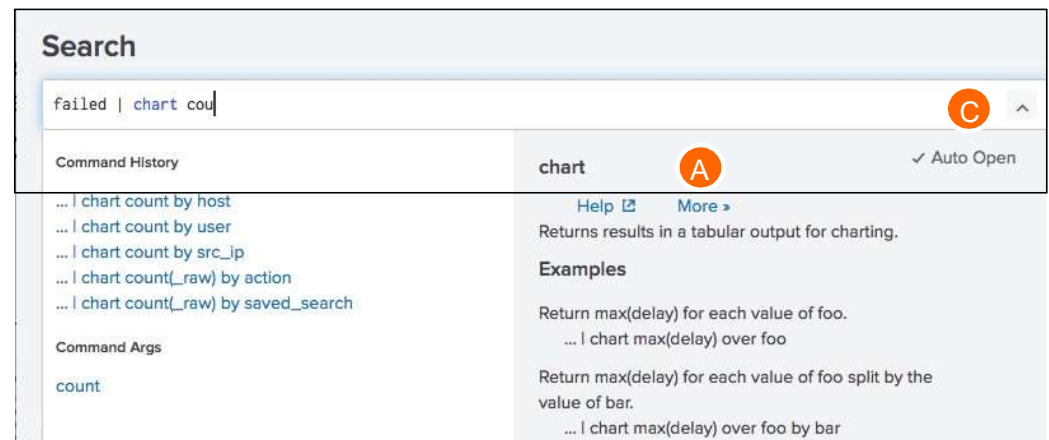
- Search Assistant is enabled by default in the **SPL Editor** user preferences
- By default, **Compact** is selected
- To show more information, choose **Full**

## Compact Mode



# Search Assistant – Full Mode

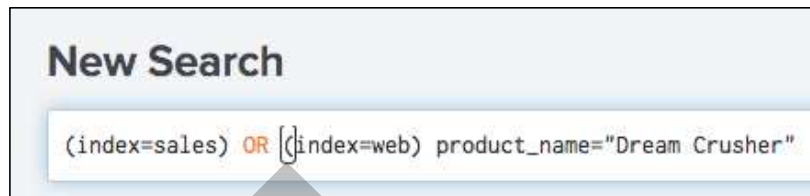
- A** To show more information, click **More »**
- B** To show less information, click **« Less**
- C** To toggle Full mode off, de-select **Auto Open**





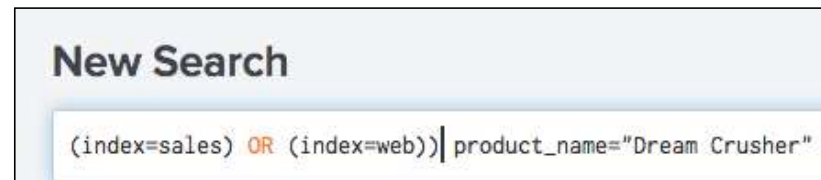
# Search Assistant – Parentheses

- The Search Assistant provides help to match parentheses as you type
- When an end parenthesis is typed, the corresponding beginning parenthesis is automatically highlighted
  - If a beginning parenthesis cannot be found, *nothing* is highlighted



(index

Beginning parenthesis  
found!



Beginning parenthesis  
NOT found!

# Search Assistant – Parentheses

1. You can use parentheses to introduce an abbreviation. SPL is the abbreviation for Search Processing Language.
2. You can use parentheses when explaining that a task is optional in a procedure.
3. You can also use parentheses when writing about one or more fields in statistical commands and charting functions for SPL

`(index="main") OR (index="_internal") error`  
`(index="main") AND (index="_internal") error`

`index="main" OR index="_internal" error`  
`index="main" AND index="_internal" error`

# Viewing Search Results

- Matching results are returned immediately
- Displayed in reverse chronological order (newest first)
- Matching search terms are highlighted

The screenshot displays the Splunk Search interface. At the top, the search bar contains the query "failed password". Below the search bar, a timeline visualization shows the distribution of events over time. The main results table lists individual events in reverse chronological order. The first event shows a failed password attempt for the user 'munin' from IP 200.6.134.23. The second event shows a failed password attempt for the user 'ftp' from IP 10.2.10.163. The third event shows a failed password attempt for the user 'news' from IP 10.2.10.163. The interface includes various controls for filtering, zooming, and saving the search.

**New Search** Save As Close

"failed password" Yesterday Q

✓ 1,942 events (1/4/18 12:00:00.000 AM to 1/5/18 12:00:00.000 AM) No Event Sampling Job || → ⌵ ⌴ Smart Mode

**Events (1,942)** Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 9 Next

<span>&lt; Hide Fields</span> <span>All Fields</span>	i	Time	Event
<b>SELECTED FIELDS</b> <span>a host 4</span> <span>a source 4</span> <span>a sourcetype 1</span>	>	1/4/18 11:45:09.000 PM	Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2 host = mailsv1 source = /opt/log/maillsv1/secure.log sourcetype = linux_secure
<b>INTERESTING FIELDS</b> <span>a action 1</span> <span>a app 1</span> <span># date_hour 20</span>	>	1/4/18 9:57:02.000 PM	Thu Jan 04 2018 21:57:02 mailsv1 sshd[4690]: Failed password for ftp from 10.2.10.163 port 4283 ssh2 host = mailsv1 source = /opt/log/maillsv1/secure.log sourcetype = linux_secure
	>	1/4/18 8:09:05.000 PM	Thu Jan 04 2018 20:09:05 mailsv1 sshd[3867]: Failed password for news from 10.2.10.163 port 4017 ssh2

# Viewing Search Results (cont.)

- Splunk parses data into individual events, extracts time, and assigns metadata
- Each event has:
  - timestamp
  - host
  - source
  - sourcetype
  - index

The screenshot displays the Splunk Search interface. At the top, the search bar contains the query "failed password". Below the search bar, a summary bar indicates "1,942 events (1/4/18 12:00:00.000 AM to 1/5/18 12:00:00.000 AM)". The interface includes tabs for "Events (1,942)", "Patterns", "Statistics", and "Visualization". A timeline visualization is shown with green bars representing event density. Below the timeline, a table of search results is displayed. The table has columns for "Time" and "Event". The first event is highlighted with a green box and shows the following details:

Time	Event
1/4/18 11:45:09.000 PM	Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2 host = mailsv1 source = /opt/log/maillsv1/secure.log sourcetype = linux_secure
1/4/18 9:57:02.000 PM	Thu Jan 04 2018 21:57:02 mailsv1 sshd[4690]: Failed password for ftp from 10.2.10.163 port 4283 ssh2 host = mailsv1 source = /opt/log/maillsv1/secure.log sourcetype = linux_secure
1/4/18 8:09:05.000 PM	Thu Jan 04 2018 20:09:05 mailsv1 sshd[3867]: Failed password for news from 10.2.10.163 port 4017 ssh2

# Viewing Search Results (cont.)

The screenshot shows the Splunk search results interface. At the top, the "New Search" header is visible. Below it, the search query "failed password" is entered. The time range picker shows "Yesterday". The search results are displayed in the "Events" tab, showing 1,942 events. The timeline view is selected, showing a bar chart of events over time. The paginator shows 20 results per page, with the first page selected. The fields sidebar on the left shows selected fields: host, source, and sourcetype. The main table displays search results with columns for Time and Event. The first row shows a failed password event for user munin from 200.6.134.23. The second row shows a failed password event for user ftp from 10.2.10.163. The third row shows a failed password event for user news from 10.2.10.163.

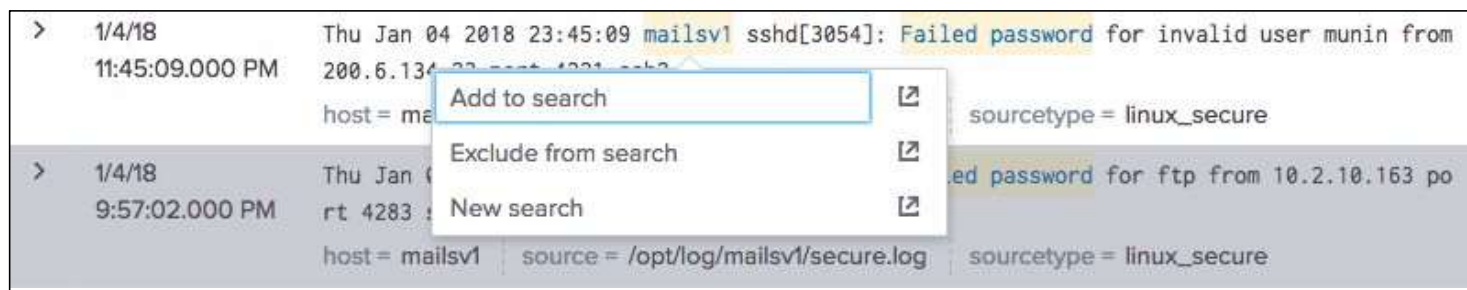
Annotations in the image include:

- time range picker
- search results appear in the Events tab
- search mode
- timeline
- paginator
- Fields sidebar
- timestamp
- selected fields
- events

Time	Event
1/4/18 11:45:09.000 PM	Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2
1/4/18 9:57:02.000 PM	Thu Jan 04 2018 21:57:02 mailsv1 sshd[4690]: Failed password for ftp from 10.2.10.163 port 4283 ssh2
1/4/18 8:09:05.000 PM	Thu Jan 04 2018 20:09:05 mailsv1 sshd[3867]: Failed password for news from 10.2.10.163 port 4017 ssh2

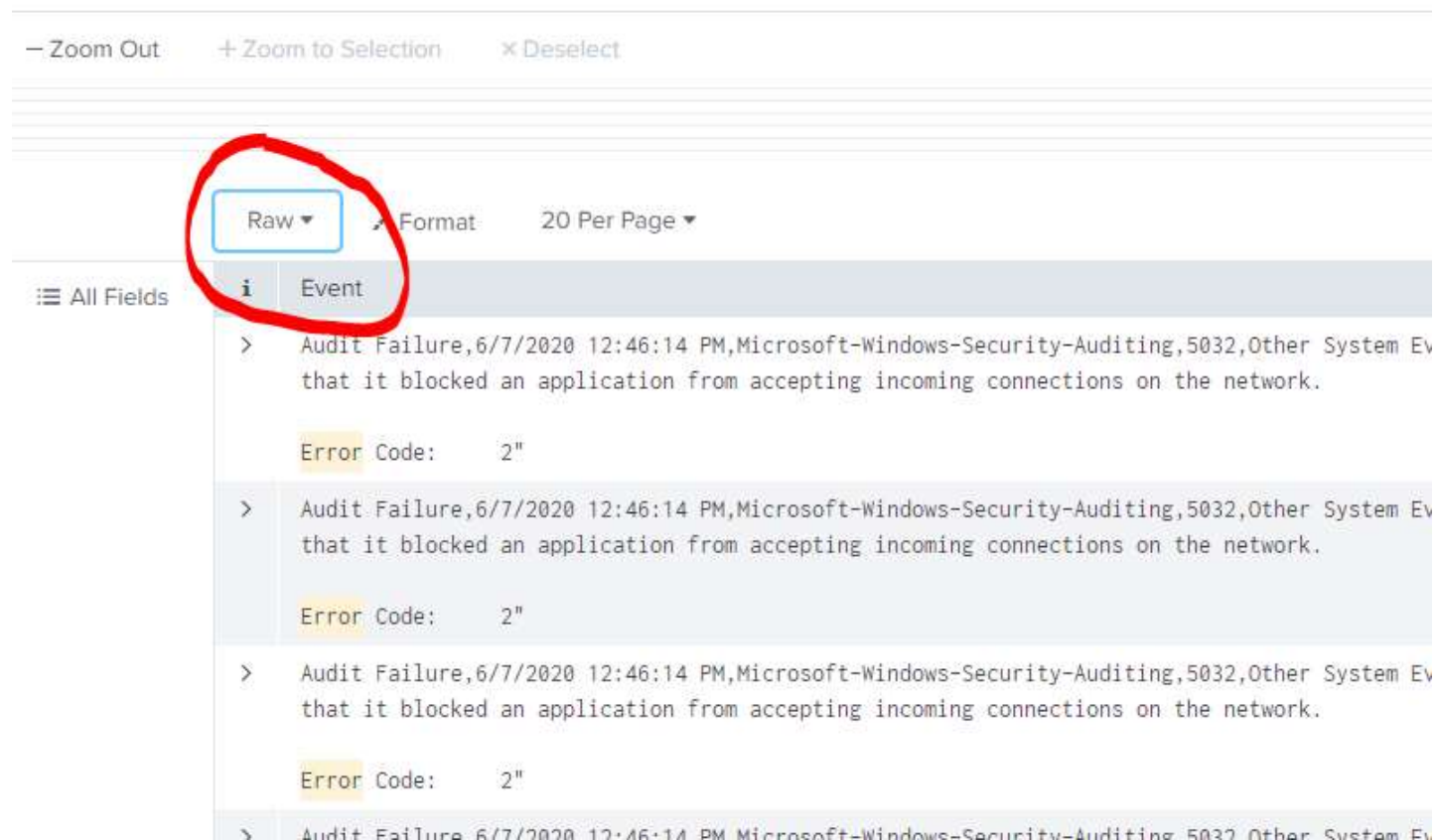
# Using Search Results to Modify a Search

- When you mouse over search results, keywords are highlighted
- Click any item in your search results; a window appears allowing you to:
  - Add the item to the search
  - Exclude the item from the search
  - Open a new search including only that item



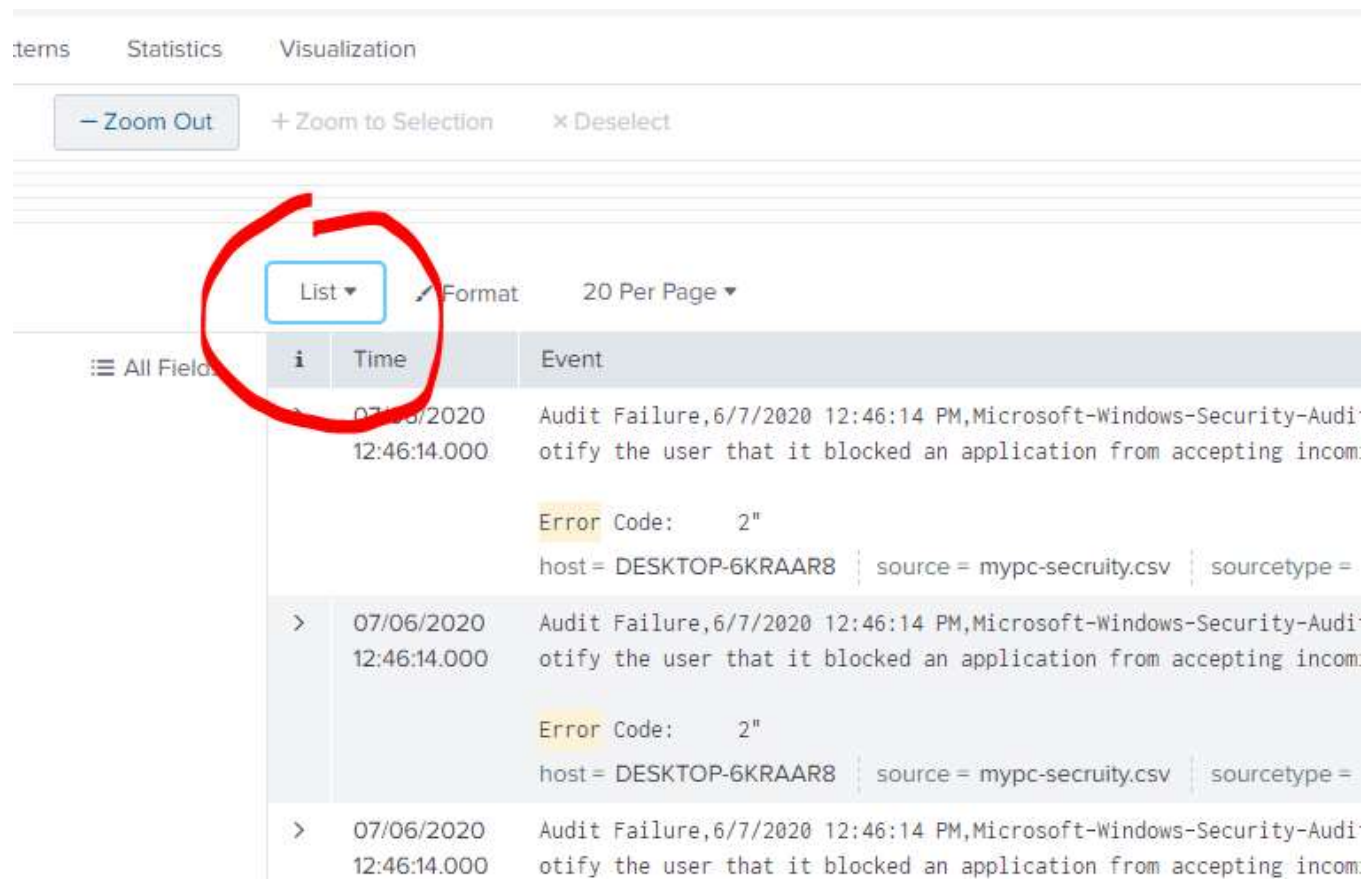
# Changing Search Results View Options

You have several layout options for displaying your search results



# Changing Search Results View Options

You have several layout options for displaying your search results



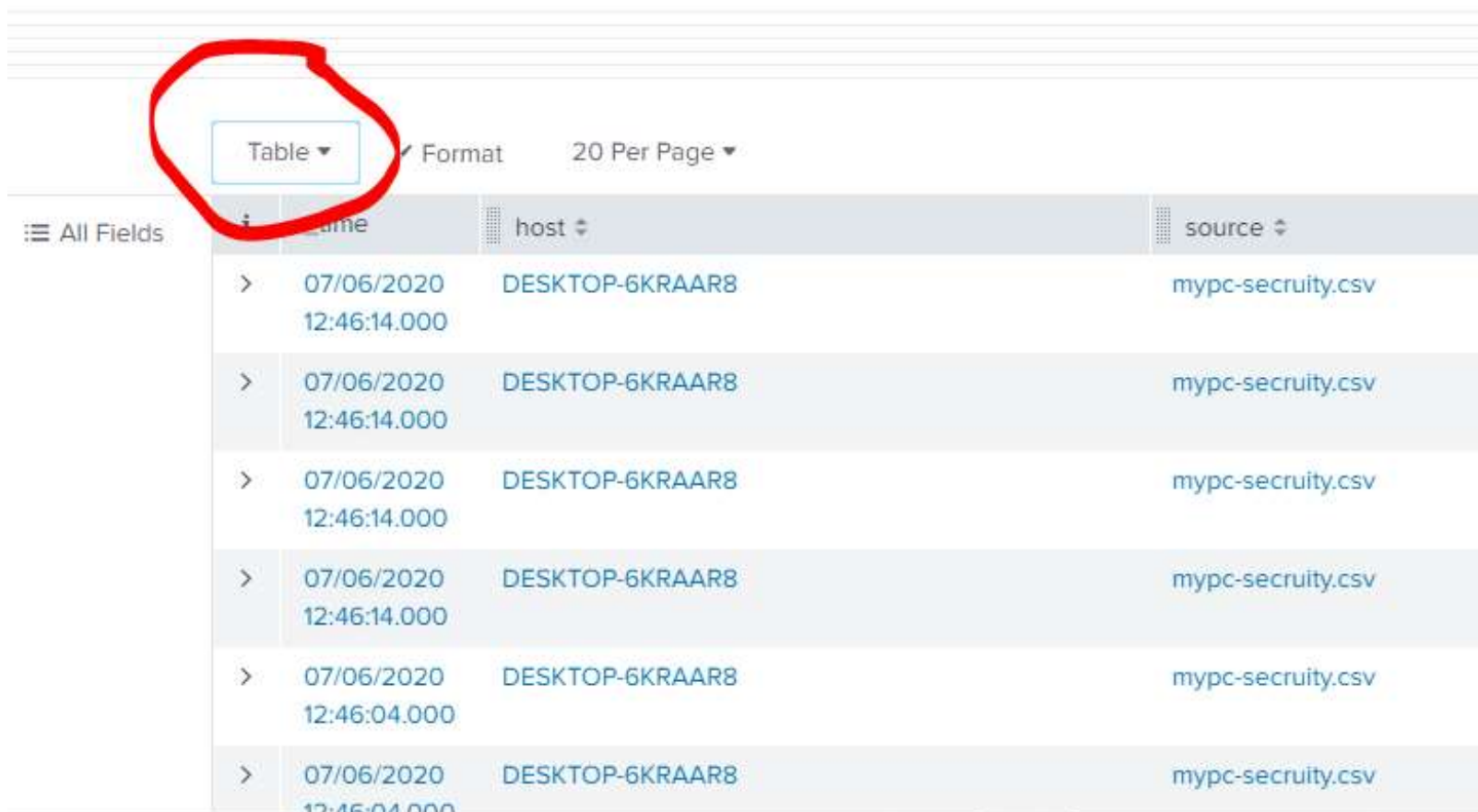
The screenshot shows a search results interface with a top navigation bar containing 'Items', 'Statistics', and 'Visualization'. Below this is a toolbar with buttons for 'Zoom Out', 'Zoom to Selection', and 'Deselect'. A red circle highlights the 'List' button in the view options section, which also includes a 'Format' icon and a '20 Per Page' dropdown. Below the view options is a table with columns 'All Fields', 'Time', and 'Event'. The table contains three rows of search results, each showing a timestamp, an event description, and an error code.

All Fields	Time	Event
	07/06/2020 12:46:14.000	Audit Failure,6/7/2020 12:46:14 PM,Microsoft-Windows-Security-Auditing otify the user that it blocked an application from accepting incoming connections. Error Code: 2 host = DESKTOP-6KRAAR8   source = mypc-security.csv   sourcetype =
>	07/06/2020 12:46:14.000	Audit Failure,6/7/2020 12:46:14 PM,Microsoft-Windows-Security-Auditing otify the user that it blocked an application from accepting incoming connections. Error Code: 2 host = DESKTOP-6KRAAR8   source = mypc-security.csv   sourcetype =
>	07/06/2020 12:46:14.000	Audit Failure,6/7/2020 12:46:14 PM,Microsoft-Windows-Security-Auditing otify the user that it blocked an application from accepting incoming connections. Error Code: 2 host = DESKTOP-6KRAAR8   source = mypc-security.csv   sourcetype =



# Changing Search Results View Options

You have several layout options for displaying your search results



The screenshot shows a search results interface. At the top, there is a navigation bar with a 'Table' dropdown menu, a 'Format' button, and a '20 Per Page' dropdown. The 'Table' dropdown is highlighted with a red circle. Below the navigation bar, there is a table with columns: 'All Fields', 'time', 'host', and 'source'. The table contains six rows of search results, each with a expandable icon (greater-than sign) in the first column, followed by the time, host, and source information.

	time	host	source
>	07/06/2020 12:46:14.000	DESKTOP-6KRAAR8	mypc-secruity.csv
>	07/06/2020 12:46:14.000	DESKTOP-6KRAAR8	mypc-secruity.csv
>	07/06/2020 12:46:14.000	DESKTOP-6KRAAR8	mypc-secruity.csv
>	07/06/2020 12:46:14.000	DESKTOP-6KRAAR8	mypc-secruity.csv
>	07/06/2020 12:46:04.000	DESKTOP-6KRAAR8	mypc-secruity.csv
>	07/06/2020 12:46:04.000	DESKTOP-6KRAAR8	mypc-secruity.csv

# Selecting a Specific

▼ Relative

Earliest: 7 Days Ago ▾ Latest: ☒ Now ☐ Beginning of today 1/5/18 11:26:07.000 AM

☐ No Snap-to ☒ Beginning of day 12/29/17 12:00:00.000 AM

▼ Real-time

Earliest: 7 Days Ago ▾ Latest: now

12/29/17 11:26:07.000 AM

▼ Date Range

Between ▾ 12/29/2017 00:00:00 and 01/05/2018 24:00:00

▼ Date & Time Range

Between ▾ 12/29/2017 11:00:00.000 and 01/05/2018 11:26:07.000

HH:MM:SS.SSS HH:MM:SS.SSS

▼ Advanced

Earliest: -24h@h 1/4/18 10:00:00.000 AM Latest: now 1/5/18 10:56:30.000 AM  [Documentation](#)

Last 7 days ▾

▼ Presets

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

preset time ranges

> Relative  
> Real-time  
> Date Range  
> Date & Time Range  
> Advanced

custom time ranges

# Time Range Abbreviations

- Time ranges are specified in the **Advanced** tab of the time range picker
- Time unit abbreviations include:

s = seconds   m = minutes   h = hours   d = days   w = week   mon = months   y = year

- @symbol "snaps" to the time unit you specify
  - Snapping rounds *down* to the nearest specified unit
  - Example: Current time when the search starts is 09:37:12

**-30m@h**

looks back to 09:00:00

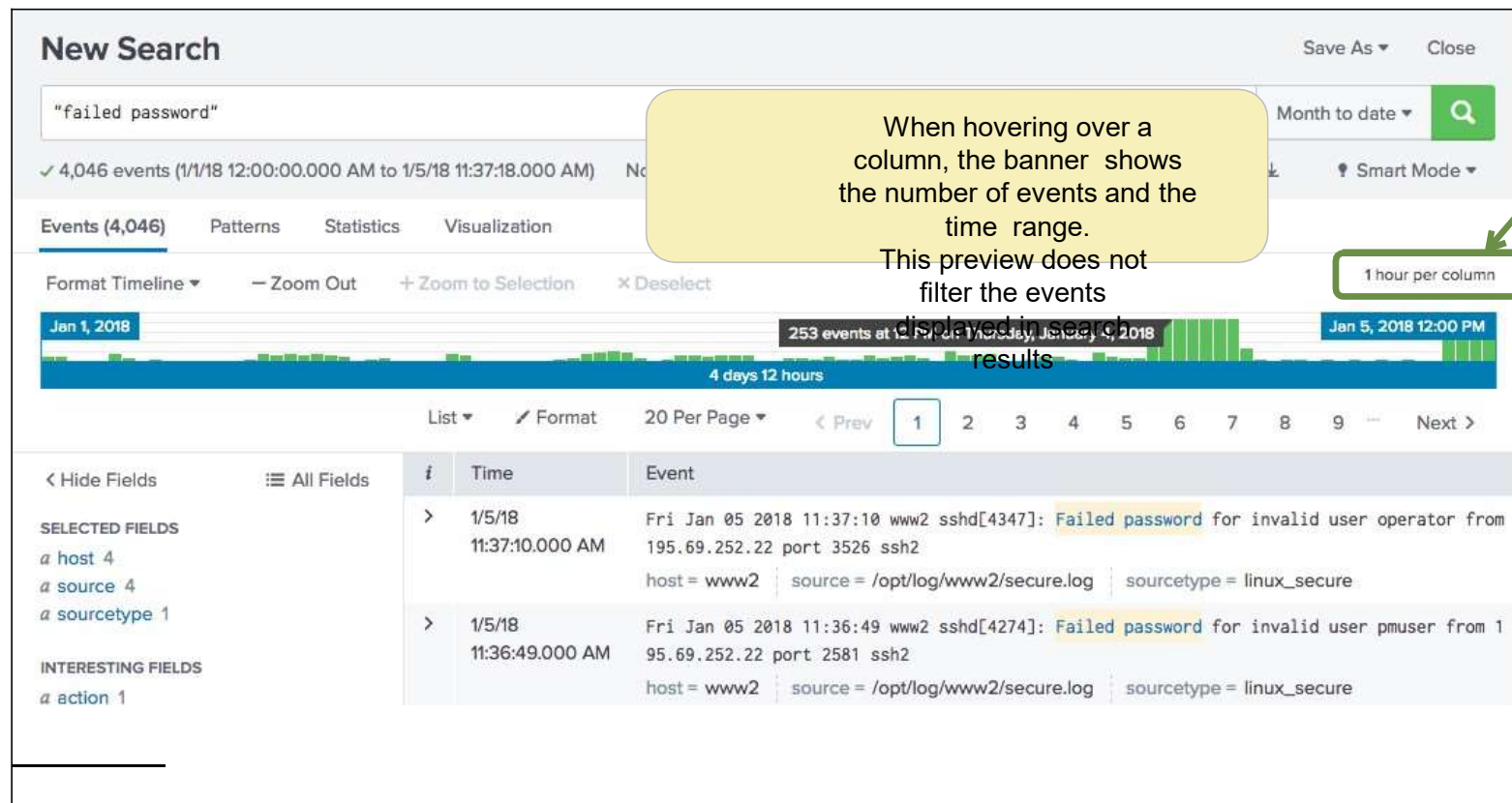
# Time Range: earliest and latest

- You can also specify a time range in the search bar
- To specify a beginning and an ending for a time range, use `earliest and latest`
- Examples:

<https://www.devopsschool.com/blog/how-to-specify-time-modifiers-in-splunk-search/>

# Viewing the Timeline

- Timeline shows distribution of events specified in the time range
  - Mouse over for details, or single-click to filter results for that time period



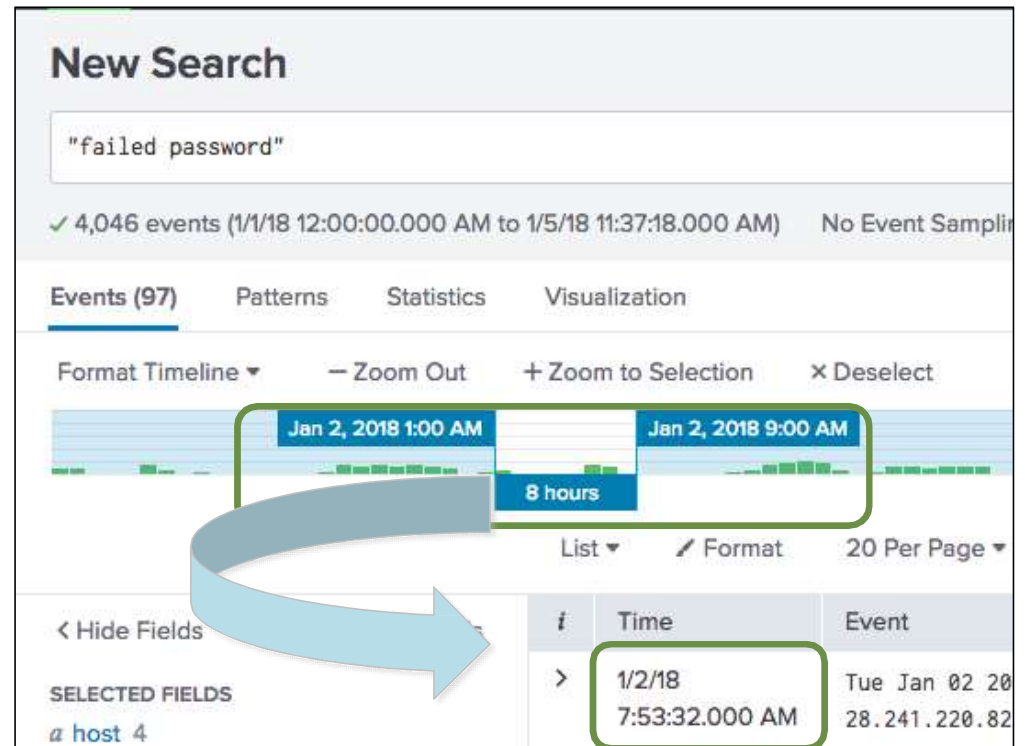
When hovering over a column, the banner shows the number of events and the time range.

This preview does not filter the events displayed in search results

Timeline legend shows the scale of the timeline

# Viewing a Subset of the Results with Timeline

- To select a narrower time range, click and drag across a series of bars
  - This action filters the current search results
    - ☐ Does not re-execute the search
  - This filters the events and displays them in reverse chronological order (most recent first)



# Using Other Timeline Controls

- **Format Timeline**

- Hides or shows the timeline in different views

- **Zoom Out**

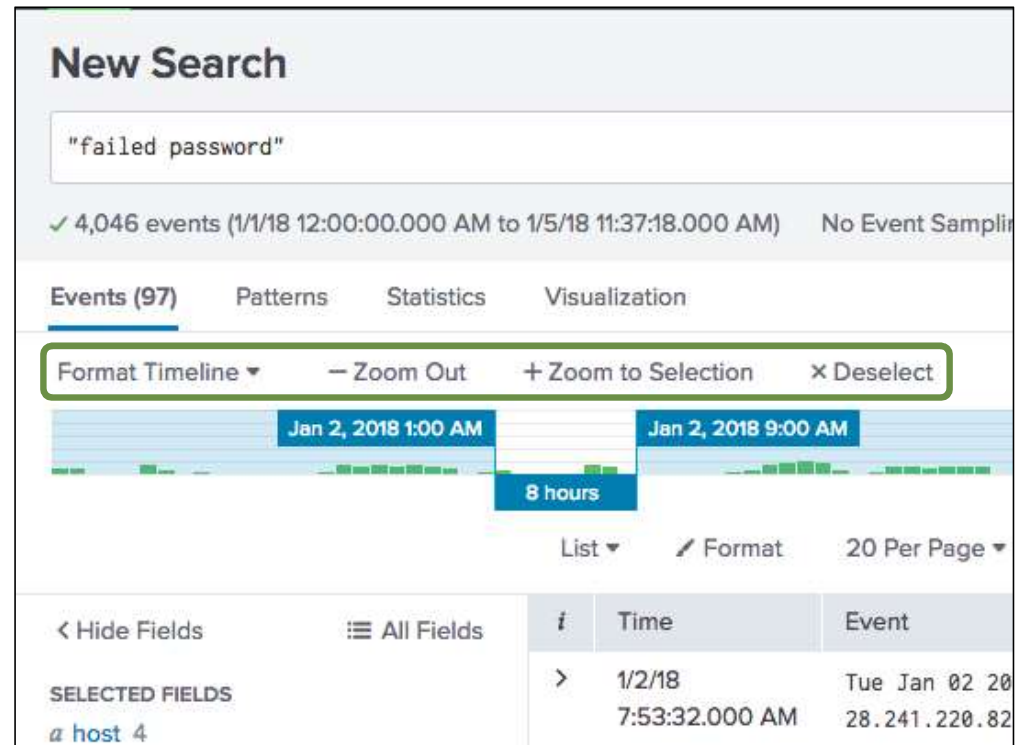
- Expands the time focus and re-executes the search

- **Zoom to Selection**

- Narrows the time range and re-executes the search

- **Deselect**

- If in a drilldown, returns to the original results set
- Otherwise, grayed out / unavailable



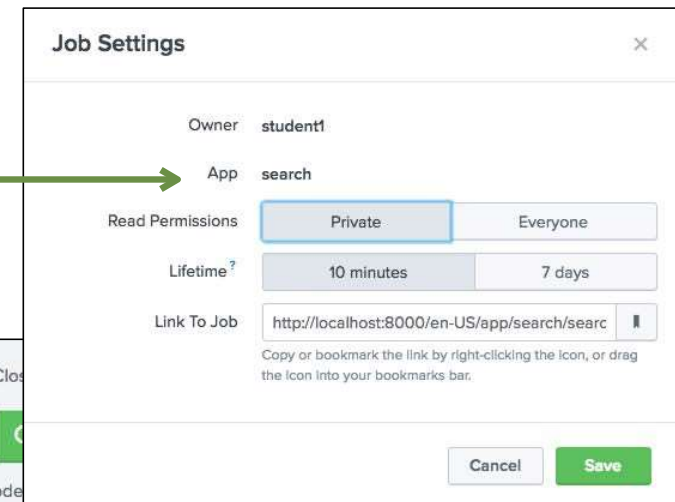
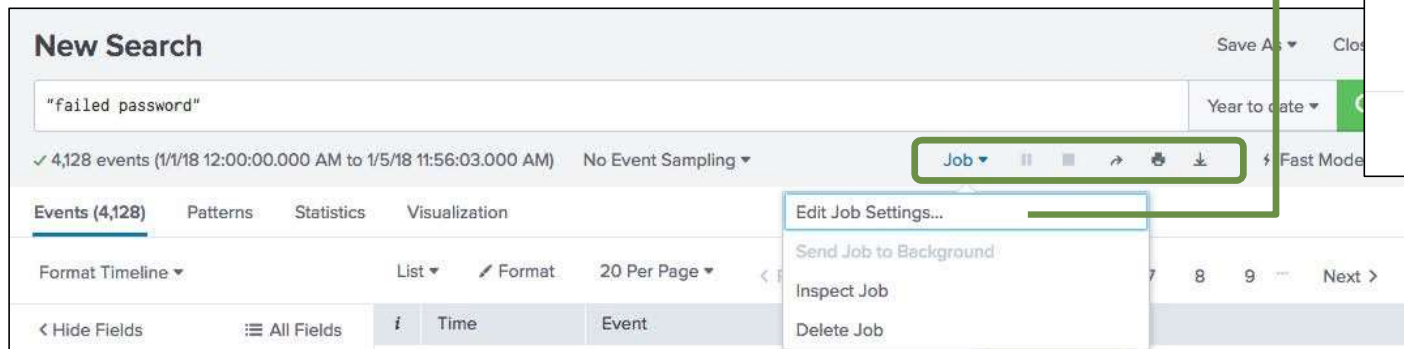
# Controlling and Saving Search Jobs

- Every search is also a **job**
- Use the Job bar to control search execution

 **Pause** – toggles to resume the search

 **Stop** – finalizes the search in progress

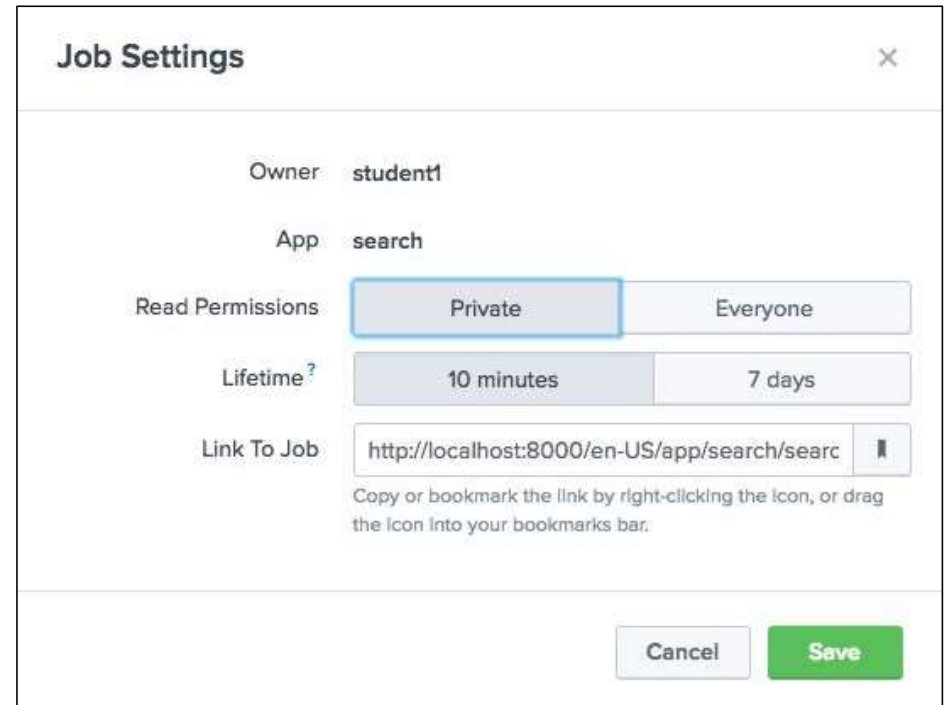
- Jobs are available for 10 minutes (default)
- Get a link to results from the **Job** menu





# Job Setting Permissions

- **Private** [default]
  - Only the creator can access
- **Everyone**
  - All app users can access search results
- **Lifetime**
  - Default is 10 minutes
  - Can be extended to 7 days
  - To keep your search results longer, schedule a report



The image shows a 'Job Settings' dialog box with a close button (X) in the top right corner. The settings are as follows:

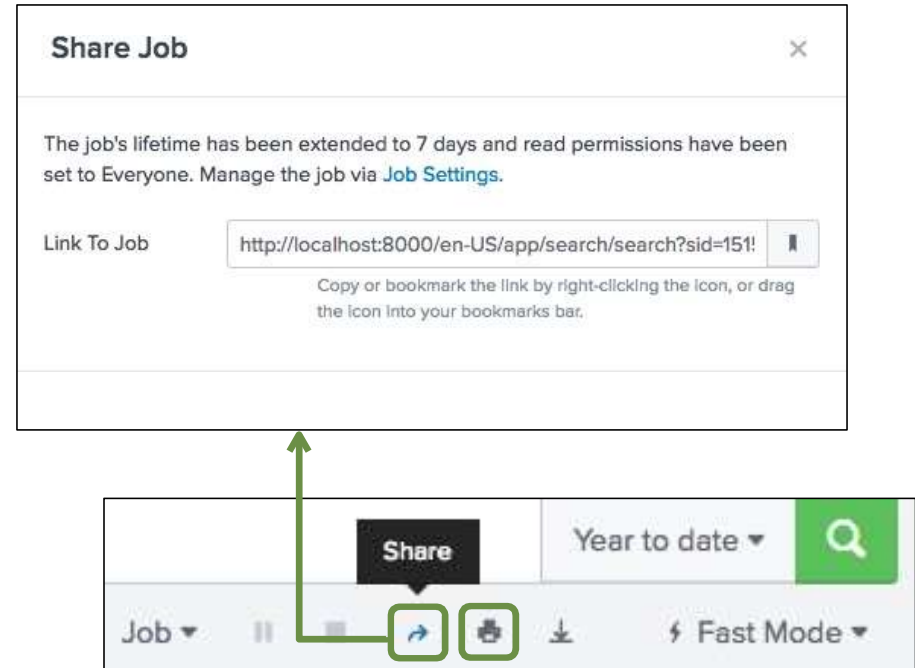
Setting	Value
Owner	student1
App	search
Read Permissions	Private (selected), Everyone
Lifetime?	10 minutes (selected), 7 days
Link To Job	<a href="http://localhost:8000/en-US/app/search/search">http://localhost:8000/en-US/app/search/search</a> [Copy Icon]

Below the 'Link To Job' field, there is a note: 'Copy or bookmark the link by right-clicking the icon, or drag the icon into your bookmarks bar.'

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

# Sharing Search Jobs

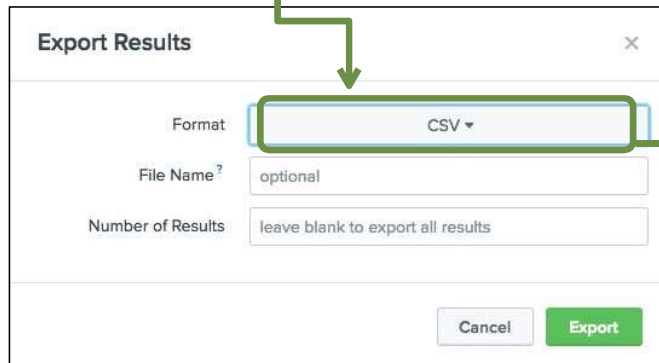
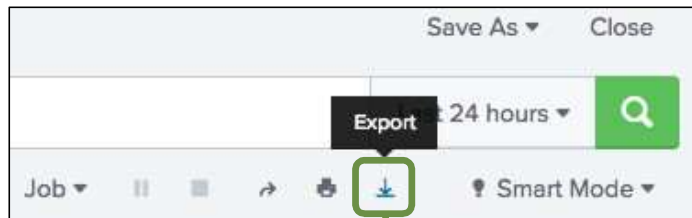
- Use the Share button next to the Job bar to quickly:
  - Give everyone read permissions
  - Extend results retention to 7 days
  - Get a sharable link to the results
- Sharing search allows multiple users working on same issue to see same data
  - More efficient than each running search separately
  - Less load on server and disk space used



- Can also click printer icon to print results or save as PDF

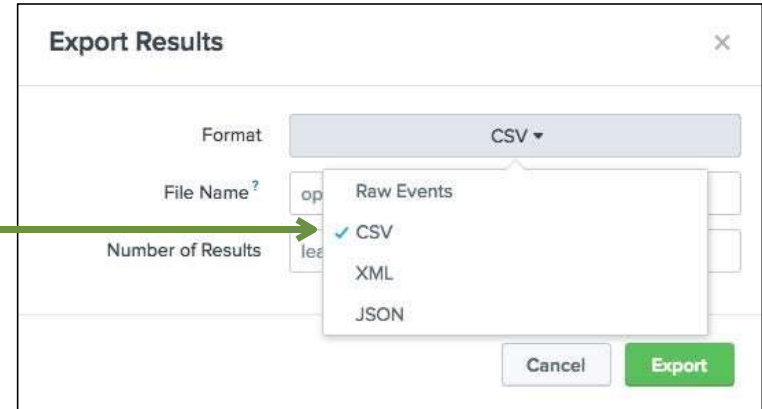
# Exporting Search Results

For an external copy of the results, **export** search results to Raw Events (text file), CSV, XML, or JSON format



## Note

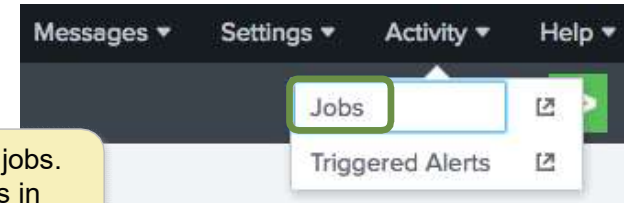
Note that exporting the results of a large search is very memory-intensive!



# Viewing Your Saved Jobs

- Access saved search jobs from the **Activity** menu
- The Search Jobs view displays jobs that:
  - You have run in the last 10 minutes
  - You have extended for 7 days
- Click on a job link to view the results in the designated app view

Click **Activity** > **Jobs** to view your saved jobs. Click the job's name to examine results in Search view. (The job name is the search string.)



3 Jobs    App: Search & Reporting (search) ▾    Filter by owner ▾    Status: All ▾     🔍    10 Per Page ▾

Edit Selected ▾

	<input type="checkbox"/>	Owner ▾	Application ▾	Events ▾	Size ▾	Created at ▾	Expires ▾	Runtime ▾	Status	Actions
>	<input type="checkbox"/>	student1	search	2,449	616 KB	Jan 5, 2018 12:45:47 PM	Jan 5, 2018 1:02:50 PM	00:00:01	Done	Job ▾          ■    ↻    ⬇
"failed password" [1/4/18 12:00:00.000 PM to 1/5/18 12:45:47.000 PM]										

# Viewing Your Search History

1. Search History displays your most recent ad-hoc searches – 5 per page
2. You can set a time filter to further narrow your results
3. Click the > icon in the leftmost column to expand long queries to display the full text

The screenshot shows the Splunk Search & Reporting interface. The top navigation bar includes links for Search, Datasets, Reports, Alerts, and Dashboards. The Search & Reporting section is active, showing a search bar with the placeholder "enter search here..." and a "Last 24 hours" filter. Below the search bar, there are sections for "How to Search" and "What to Search". The "What to Search" section displays "537,902 Events INDEXED" and "3 months ago EARLIEST EVENT" and "a few seconds ago LATEST EVENT".

On the left side, there is a "Search History" panel. A green box with a red circle "1" highlights the "> Search History" link. A dropdown menu is open, showing options for "No Time Filter", "Today", "Last 7 Days", and "Last 30 Days". A red circle "2" highlights the "No Time Filter" option. Below the dropdown, the "Search History" panel shows a list of searches. A red circle "3" highlights the first search entry, which is expanded to show the full query: "(sourcetype=cisco\_wsa\_squid OR sourcetype=access\_combined) status>399 | timechart count by sourcetype | eval cisco\_wsa\_squid=cisco\_wsa\_squid\*3 | where access\_combined>cisco\_wsa\_squid". The table also includes columns for "Actions" (Add to Search) and "Last Run" (a few seconds ago).

Search	Actions	Last Run
(sourcetype=cisco_wsa_squid OR sourcetype=access_combined) status>399   timechart count by sourcetype   eval cisco_wsa_squid=cisco_wsa_squid*3   where access_combined>cisco_wsa_squid	<a href="#">Add to Search</a>	a few seconds ago
"failed password"	<a href="#">Add to Search</a>	25 minutes ago
(index=sales) OR (index=web) product_name="Dream Crusher"	<a href="#">Add to Search</a>	2 hours ago
index=* "failed password"	<a href="#">Add to Search</a>	3 hours ago

# Demo



Adding more data

Dive into Splunksearch

# What Are Fields?

- Fields are searchable key/value pairs in your event data
  - Examples: `host=www1 status=503`
- Fields can be searched with their names, like separating an http status code of 404 from Atlanta's area code (`area_code=404`)
- Between search terms, **AND** is implied unless otherwise specified

area\_code=404 Yesterday ▾ 🔍

action=purchase status=503 Yesterday ▾ 🔍

source=/var/log/messages\* NOT host=mail2 Yesterday ▾ 🔍

sourcetype=access\_combined Yesterday ▾ 🔍

# Field Discovery

- Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data
- Prior to search time, some fields are already stored with the event in the index:
  - Meta fields, such as **host**, **source**, **sourcetype**, and **index**
  - Internal fields such as **\_time** and **\_raw**
- At search time, *field discovery* discovers fields directly related to the search's results
- Some fields in the overall data may not appear within the results of a particular search

## Note

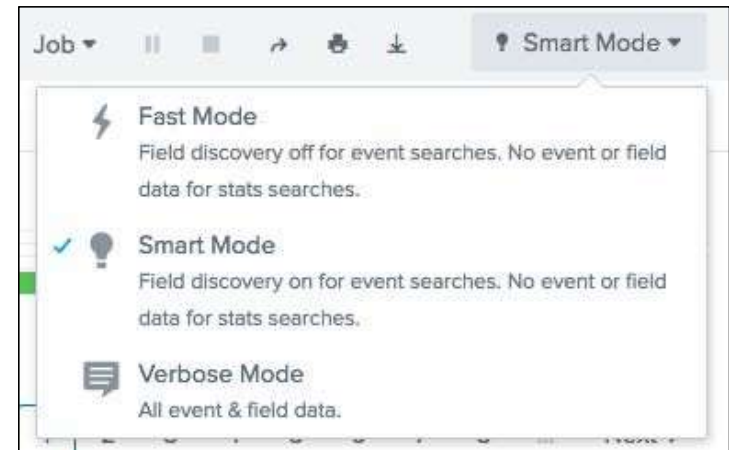


While Splunk auto-extracts many fields, you can learn how to create your own in the *Splunk Fundamentals 2* course.



# Search Modes: Fast, Smart, Verbose

- Fast: emphasizes speed over completeness
- Smart: balances speed and completeness (default)
- Verbose:
  - Emphasizes completeness over speed
  - Allows access to underlying events when using reporting or statistical commands (in addition to totals and stats)



## Note

You'll discuss statistical commands later in this course.

# Identify Data-Specific Fields

- Data-specific fields come from the specific characteristics of your data
  - Sometimes, this is indicated by obvious key = value pairs (**action = purchase**)
  - Sometimes, this comes from data within the event, defined by the sourcetype (**status = 200**)

i	Time	Event
>	1/5/18 1:21:10.000 PM	192.162.19.179 - - [05/Jan/2018:13:21:10] "POST /cart/success.do?JSESSIONID=SD1SL6FF4ADFF4964 HT TP 1.1" <b>200</b> 966 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5 .0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version /5.0.2 Mobile/8L1 Safari/6533.18.5" 552

## Note



For more information, please see:

<http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes>

# Fields Sidebar

For the current search:

- **Selected Fields** – a set of configurable fields displayed for each event
- **Interesting Fields** – occur in at least 20% of resulting events
- **All Fields** link to view all fields (including non-interesting fields)

indicates the field's values are alpha-numeric

indicates that the majority of the field values are numeric

The screenshot shows the 'New Search' interface in Splunk. The search query is '"failed password"'. It shows 2,406 events from 1/4/18 1:00:00.000 PM to 1/5/18 1:36:10.000 PM. The 'Events (2,406)' tab is selected. The 'Format Timeline' dropdown is set to 'List'. The 'Fields' sidebar is open, showing 'Selected Fields' and 'Interesting Fields'. Annotations include:

- A yellow box with the text 'click to view all fields' pointing to the 'All Fields' link.
- A green box around the 'a' icon in the 'Selected Fields' list, with a callout indicating it means the field's values are alpha-numeric.
- A green box around the '2' in the '# date\_mday' field, with a callout indicating it shows the number of unique values for the field.
- A green box around the '#' icon in the 'Interesting Fields' list, with a callout indicating it means the majority of the field values are numeric.

Field	Count
host	4
source	4
sourcetype	1
action	1
app	1
date_hour	17
date_mday	2
date_minute	60

# Describe Selected Fields

- Selected fields and their values are listed under every event that includes those fields
- By default, the selected fields are:
  - host
  - source
  - sourcetype
- You can choose any field and make it a selected field

**New Search** Save As Close

action=purchase Yesterday Q

✓ 392 events (1/4/18 12:00:00.000 AM to 1/5/18 12:00:00.000 AM) No Event Sampling Job || ■ → ⌵ ⌵ Smart Mode

**Events (392)** Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection × Deselect 1 hour per column

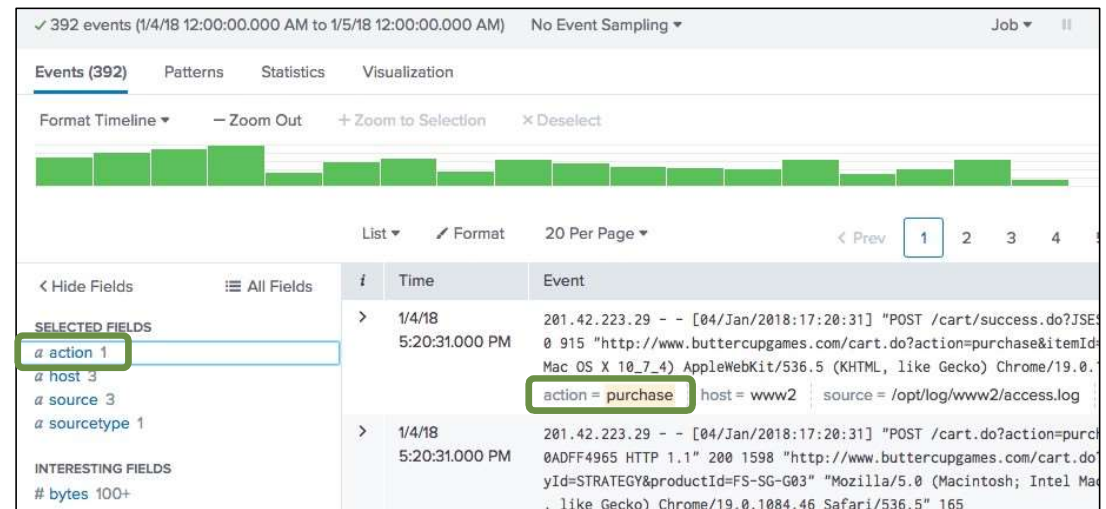
List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 Next >

< Hide Fields All Fields

	i	Time	Event
	>	1/4/18 5:20:31.000 PM	201.42.223.29 - - [04/Jan/2018:17:20:31] "POST /cart/success.do?JSESSIONID=SD1SL8FF10ADFF4965 HTTP 1.1" 200 915 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-11" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 118
<b>SELECTED FIELDS</b> a host 3 a source 3 a sourcetype 1			host = www2   source = /opt/log/www2/access.log   sourcetype = access_combined

# Make an Interesting Field a Selected Field

- You can modify selected fields
  - 1 Click a field in the Fields sidebar
  - 2 Click **Yes** in the upper right of the field dialog
- Note that a selected field appears:
  - In the Selected Fields section of the Fields sidebar
  - Below each event where a value exists for that field



# Make Any Field Selected

You can identify other fields as selected fields from All Fields (which shows all of the discovered fields)

**Select Fields**

Select All Within Filter   Deselect All   Coverage: 1% or more   Filter   + Extract New Fields

	Field	# of Values	Event Coverage	Type
<input checked="" type="checkbox"/>	action	1	100%	String
<input checked="" type="checkbox"/>	host	3	100%	String
<input checked="" type="checkbox"/>	source	3	100%	String
<input checked="" type="checkbox"/>	sourcetype	1	100%	String
<input type="checkbox"/>	JSESSIONID	>100	100%	String
<input type="checkbox"/>	bytes	>100	100%	Number
<input type="checkbox"/>	categoryId	8	50.77%	String

**SELECTED FIELDS**

- a action 1
- a host 3
- a source 3
- a sourcetype 1

5:20:31.000 PM 0 915 "http://www.butte Mac OS X 10\_7\_4) AppleW action = purchase host

1/4/18 201.42.223.29 - - [04/]

# The Field Window

Select a field from the Fields sidebar, then:

Narrow the search to show only results that contain this field

**action = \*** is added to the search criteria

Get statistical results

Click a value to add the field/value pair to your search – in this case, **action = addtocart** is added to the search criteria

Top 10 Values	Count	%
failure	1,942	49.923%
view	440	11.311%
purchase	392	10.077%
addtocart	377	9.692%
success	230	5.912%
TCP_REFRESH_HIT	189	4.859%
remove	189	4.859%
TCP_DENIED	43	1.105%

# Using Fields in Searches

- Efficient way to pinpoint searches and refine results

141.146.8.66	clientip=141.146.8.66	status=404	area_code=404
--------------	-----------------------	------------	---------------

- Field names ARE case sensitive; field values are NOT

–Example:

host=www3	host=WWW3	HOST=www3
✓ 323 events 1/9/14 12:00:00.000 AM to	✓ 323 events 1/9/14 12:00:00.000 AM to	✓ 0 events 1/9/14 12:00:00.000 AM to

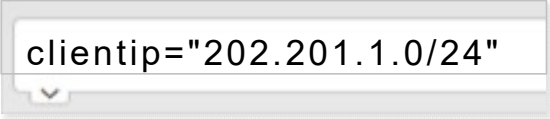
These two searches return results

This one does not return results



# Using Fields in Searches (cont.)

- For IP fields, Splunk is subnet/CIDR aware

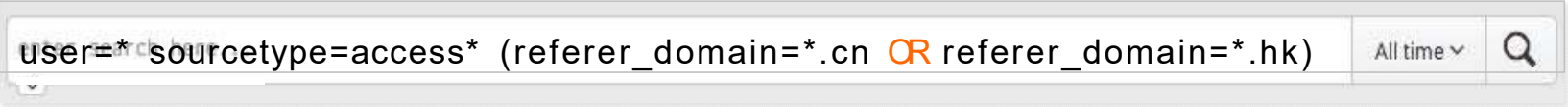


```
clientip="202.201.1.0/24"
```



```
clientip="202.201.1.*"
```

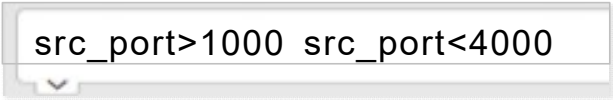
- Use wildcards to match a range of field values
  - Example: **user=\*** (to display all events that contain a value for user)



```
user=* sourcetype=access* (referer_domain=*.cn OR referer_domain=*.hk)
```

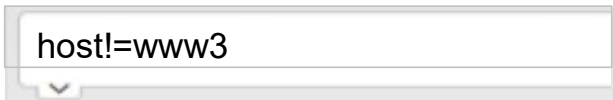
- Use relational operators

With numeric fields



```
src_port>1000 src_port<4000
```

With alphanumeric fields

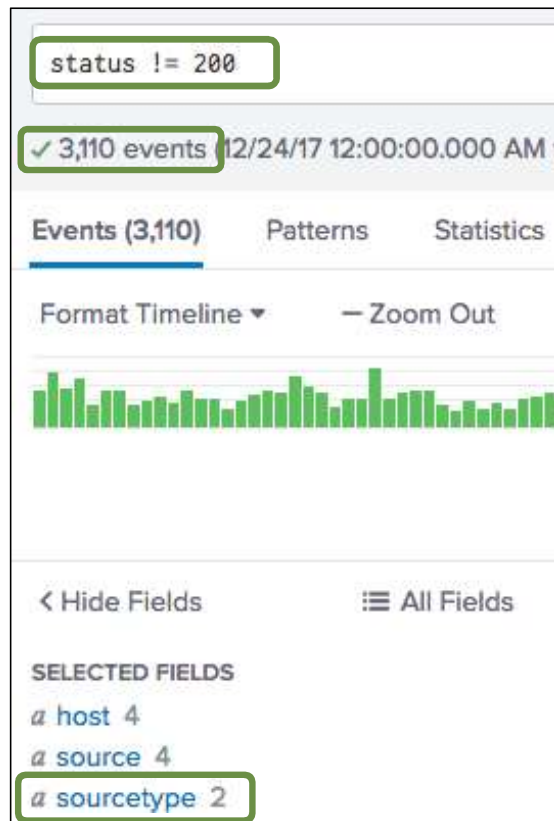


```
host!=www3
```

# != vs. NOT

- Both != field expression and NOT operator exclude events from your search, but produce different results
- Example: status != 200
  - Returns events where status field exists and value in field doesn't equal 200
- Example: NOT status = 200
  - Returns events where status field exists and value in field doesn't equal 200 -- **and** all events where status field **doesn't** exist

# != vs. NOT(cont.)



In this example:

- `status != 200` returns **3,110** events from **2** sourcetypes
- `NOT status=200` returns **66,855** events from **9** sourcetypes

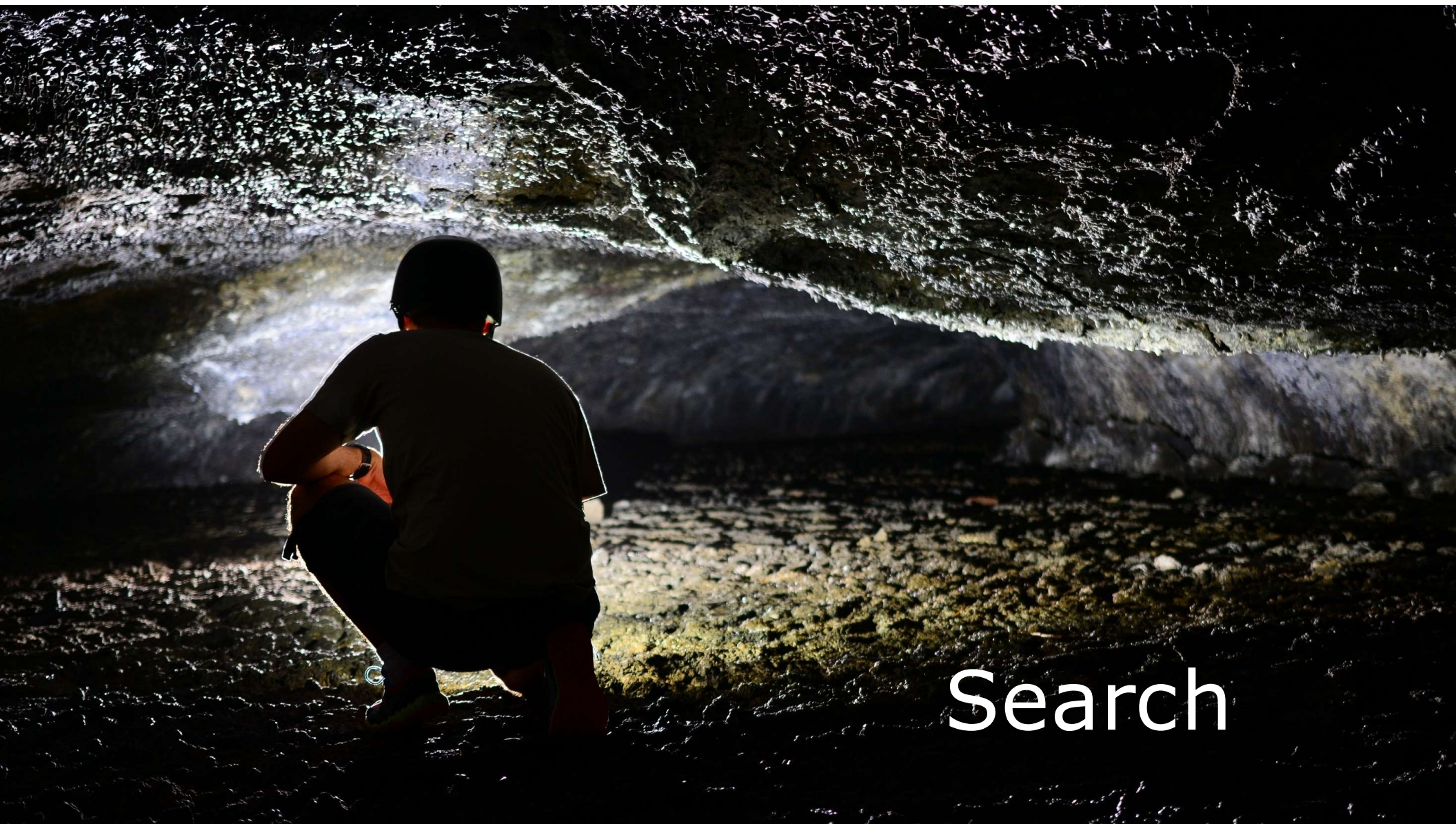
## Note

The results from a search using `!=` are a **subset** of the results from a similar search using `NOT`.



# != vs. NOT(cont.)

- Does != and NOT ever yield the same results?
  - Yes, if you know the field you're evaluating always exists in the data you're searching
  - For example:
    - ❑ index=web sourcetype=access\_combined status!=200
    - ❑ index=web sourcetype=access\_combined NOT status=200yields same results because status field always exists in access\_combined sourcetype



Search



Mining



Mining



Analyze data

- Date Time
- Event IDs
- Etc



### Ongoing Analysis

- Trends
- Daily Awareness

### Management

- Status
- Patterns





### Warnings

- Real-time
- Scheduled

### Problems

- Quicker resolution
- Actionable

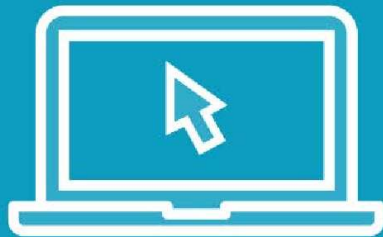
# Demo



Windows System Logs

Windows Security Logs

# Demo



Developing saved reports

# Summary



Added more data from local machine

Understanding of search