

# Best Practices and Better Practices for Users

...while you get settled...

## ▶ Latest Slides:

- <https://splunk.box.com/v/blueprints-practices-user>

## ▶ Collaborate: #bestpractices

- Sign Up @ <http://splk.it/slack>

## ▶ Load Feedback ----->

The screenshot shows a mobile application interface with the following elements:

- Header:** "Best Practices and Better Prac..." with a back arrow and a share icon.
- Navigation:** "Description" and "Notes" tabs.
- Content:**
  - Administrator (150)
  - Role: Architect (130)
  - Skill Level: Beginner (23)
  - Feedback section with a "SHOW 6 MORE" dropdown arrow.
  - Two 5-point rating scales:
    - "How would you rate this session content: (Rate 1 to 5)" with radio buttons for 1-5.
    - "How would you rate the session speaker(s): (Rate 1 to 5)" with radio buttons for 1-5.
  - "General Feedback: (Open Text Area)" with a text input field.
  - "Submit Feedback" button at the bottom.

A red arrow points from the "Feedback" section header to the "SHOW 6 MORE" dropdown arrow.

# Best Practices and Better Practices for Users

Presented by Splunk Blueprints

Burch | Senior Best Practices Engineer

.conf2017 | Version 0.0

# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk<, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

```
130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=3-3w03-4004"
128.241.230.02 - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FLD5H-01&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
096.NT 5.1:160.0.0 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/product.screen?product_id=FLD5H-01&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
//buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=MV-CE-0&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=MV-CE-0&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
//buttercup-shopping.com/rp-li-02" 468 125.17 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
//buttercup-shopping.com/rp-li-02" 468 125.17 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
//buttercup-shopping.com/rp-li-02" 468 125.17 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
//buttercup-shopping.com/rp-li-02" 468 125.17 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
//buttercup-shopping.com/rp-li-02" 468 125.17 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61f75&jsessionid=SD55L9FF1ADF3 HTTP 1.1"
```

# “Scale customer success through the automation of adoption services and best practices”

---

Blueprint's Mission

# What's a “Burch”?

Senior Best Practices Engineer

- ▶ Was a Senior Sales Engineer
- ▶ Before that, Splunk **Customer**
- ▶ Before that, Middleware Eng
- ▶ Before that, Computer Science
- ▶ Before that, an idea of my parents



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f75&SESSIONID=5D55LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=F3-3w03- "
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7F6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-6&product_id=H0-1374- "
Oms NT 5:1:160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7F6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-6&product_id=H0-1374- "
item_id=EST-10&product_id=RP-L1-02" 468 125.17 "GET /cart.do?action=remove&item_id=EST-10&product_id=RP-L1-02" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-6&product_id=H0-1374- "
/buttercup-shopping.com/n- "GET /category.screen?category_id=61f75&SESSIONID=5D55LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=F3-3w03- "
opping.com/purchase&item_id=EST-6&product_id=H0-1374- "GET /category.screen?category_id=61f75&SESSIONID=5D55LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=F3-3w03- "
/buttercup-shopping.com/n- "GET /category.screen?category_id=61f75&SESSIONID=5D55LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=F3-3w03- "

```

# Agenda

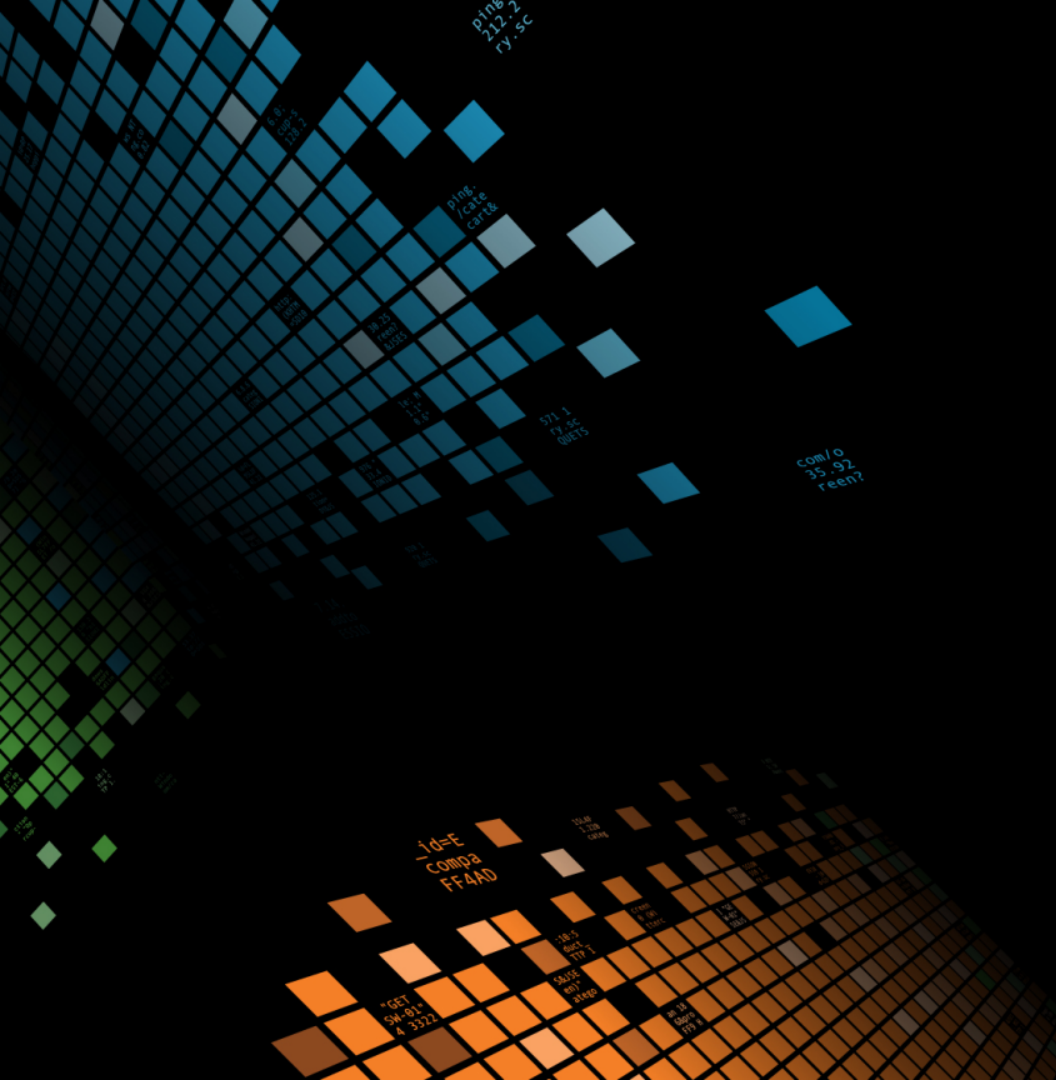
Coo wit u?

## 1. How I Learned

## 2. Searching

- Pretty Searches
- Search Performance
- Accuracy

## 3. Evolved Ideas



# How I Learned

---

Now this is a story all about how...

# Search Tutorial

Free Search Tutorial -> docs.splunk.com -> Search Tutorial

The screenshot shows the Splunk documentation website. The navigation bar includes links for PRODUCTS, SOLUTIONS, CUSTOMERS, COMMUNITY, and SPLEXICON. A search bar is visible in the top right. The main content area features three columns: Developer tools (with links to SDKs and Web Framework), Community (with links to Ponydocs and Answers), and Legacy (with a link to Legacy products). Below this, there are sections for 'Docs Latest' and 'Splunk Docs on Twitter'. A red arrow points to the 'Search Tutorial' link in the 'Docs Latest' section.

- ▶ Downloads & Installs Splunk
- ▶ Add tutorial data
- ▶ Local sandbox



# Quick Reference Guide

## Search “splunk quick reference guide”

splunk&gt;

QUICK REFERENCE GUIDE

### Concepts

#### Events

An event is a set of values associated with a timestamp. It is a single entry of data and can have one or multiple lines. An event can be a text document, a configuration file, an entire stack trace, and so on. This is an example of an event in a web activity log:

```
10.14.0.172 - - [01/
Mar/2015:12:05:27 -0700] "GET /
trade/app?action=logout HTTP/1.1"
200 2953
```

You can also define transactions to search for and group together events that are conceptually related but span a duration of time. Transactions can represent a multistep business-related activity, such as all events related to a single customer session on a retail website.

#### Host, Source, and Source Type

A *host* is the name of the physical or virtual device where an event originates. The *host* field provides an easy way to find all data originating from a specific device. A *source* is the name of the file, directory, data stream, or other input from which a particular event originates. Sources are classified into *source types*, which can be either well known formats or formats defined by the user. Some common source types are HTTP web server logs and Windows event logs.

Events with the same source types can come from different sources. For example, events from the file `source=/var/log/messages` and from a syslog input port `source=UDP:514` often share the source type, `sourcetype=linux_syslog`

At search-time, indexed events that match a specified search string can be categorized into event types.

#### Indexes

When data is added, Splunk software parses the data into individual events, extracts the timestamp, applies line-breaking rules, and stores the events in an *index*. You can create new indexes for different inputs. By default, data is stored in the “main” index. Events are retrieved from one or more indexes during a search.

#### Index-Time and Search-Time

During *index-time* processing, data is read from a source on a host and is classified into a source type. Timestamps are extracted, and the data is parsed into individual events. Line-breaking rules are applied to segment the events to display in the search results. Each event is written to an index on disk, where the event is later retrieved with a search request.

When a *search* starts, referred to as *search-time*, indexed events are retrieved from disk. *Fields* are extracted from the raw text for the event.

### Core Features

#### Search

Search is the primary way users navigate data in Splunk software. You can write a search to retrieve events from an index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. You transform the events using the Splunk Search Process Language (SPL™). Searches can be saved

### Additional Features (Splunk Enterprise only)

#### Data Model

A *data model* is a hierarchically-organized collection of datasets that Pivot uses to generate reports. Data model objects represent individual datasets, which the data model is composed of.

#### Pivot

Pivot refers to the table, chart, or other visualization you create using the Pivot Editor. You can map attributes defined by data model objects to data visualizations, without manually writing the searches. Pivots can be saved as reports and used to power dashboards.

#### Apps

Apps are a collection of configurations, knowledge objects, and customer designed views and dashboards. Apps extend the Splunk environment to fit the specific needs of organizational teams such as Unix or Windows system administrators, network security specialists, website managers, business analysts, and so on. A single Splunk Enterprise or Splunk Cloud installation can run multiple apps simultaneously.

#### Distributed Search

A *distributed search* provides a way to scale your deployment by separating the search management and presentation layer from the indexing and search retrieval layer. You use search to facilitate horizontal scaling for enhanced performance, to control access to indexed data, and to manage geographically

# Search Command Reference

docs.splunk.com -> Splunk Enterprise -> Search and report -> Search Reference -> Commands by category

☰ Hide Contents ▾
Documentation / Splunk® Enterprise / Search Reference / Commands by category

**Search Reference**

- Introduction
- Quick Reference
- Splunk Enterprise Quick Reference Guide
- Command quick reference
- Commands by category
- Command types
- Splunk for SQL users
- SPL data types and clauses
- Functions
- Time Format Variables and Modifiers
- Search Commands
- Internal Commands
- Search in the CLI

## Commands by category

The following tables list all the search commands, categorized by their usage. Some commands fit into more than one category based on the options that you specify.

### Correlation

These commands can be used to build correlation searches.

Command	Description
<a href="#">append</a>	Appends subsearch results to current results.
<a href="#">appendcols</a>	Appends the fields of the subsearch results to current results, first results to first result, second to second, etc.
<a href="#">appendpipe</a>	Appends the result of the subpipeline applied to the current result set to results.
<a href="#">arules</a>	Finds association rules between field values.
<a href="#">associate</a>	Identifies correlations between fields.
<a href="#">contingency, counttable, ctable</a>	Builds a contingency table for two fields.
<a href="#">correlate</a>	Calculates the correlation between different fields.
<a href="#">diff</a>	Returns the difference between two search results.
<a href="#">join</a>	Combines the of results from the main results pipeline with the results from a subsearch.
<a href="#">lookup</a>	Explicitly invokes field value lookups.

### Commands by category

- Correlation
- Data and indexes
- Fields
- Find anomalies
- Geographic and location
- Prediction and trending
- Reports
- Results
- Search
- Subsearch
- Time

# Splunk! The Book

[www.splunk.com/goto/book](http://www.splunk.com/goto/book)



## Exploring Splunk

SEARCH PROCESSING LANGUAGE (SPL)  
PRIMER AND COOKBOOK

By David Carasso, Splunk's Chief Mind



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_3=61F5&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=F-3W-03-...
128.241.230.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-03&SESSIONID=SD5L7FFGADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-6&product_id=F-3W-03-...
Owens NT 5.1: Svi: [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"
http://buttercup-shopping.com/ - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-76&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1301 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1"

```

# Splunk User Groups

usergroups.splunk.com

splunk>usergroups

FIND MORE GROUPS

50m ▾

# Find a Splunk User Group

Connect with like-minded people who are passionate about Splunk technology

# Free Education!

splunk.com/education

## Splunk Fundamentals 1

Take this course, get Splunk User certified, and be eligible to win up to \$4500!

Once you complete and pass this course, you are eligible to take the Splunk Certified User certification exam. The person or persons with the highest score on the certification exam by August 31st, 2017 will win the prize. In the event of a tie the \$4,500 will be shared among the winners. Must not have any other Splunk Certification. One passing entry per person. Competition closes on August 31st, 2017.

This course teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts. It will also introduce you to Splunk's datasets features and Pivot interface.



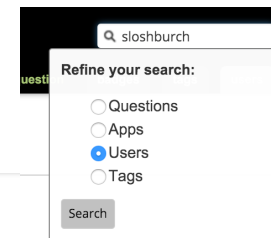
# But now I have questions...



# answers.splunk.com



## Community Q&A

- ▶ E-mail notifications
- ▶ Fast answers
- ▶ Larger distribution



### Karma Leaderboard

last week   last 2 weeks   current month   **quarter to date**   all time

Rank	Change <b>↑</b>	User <b>↑</b>	Karma <b>↓</b>
18	39 <b>↑</b>	 <a href="#">SloshBurch</a>	533
101,108	42,782 <b>↑</b>	 <a href="#">SloshBurch</a>	



**SloshBurch**  
Boston, MA

+ Follow

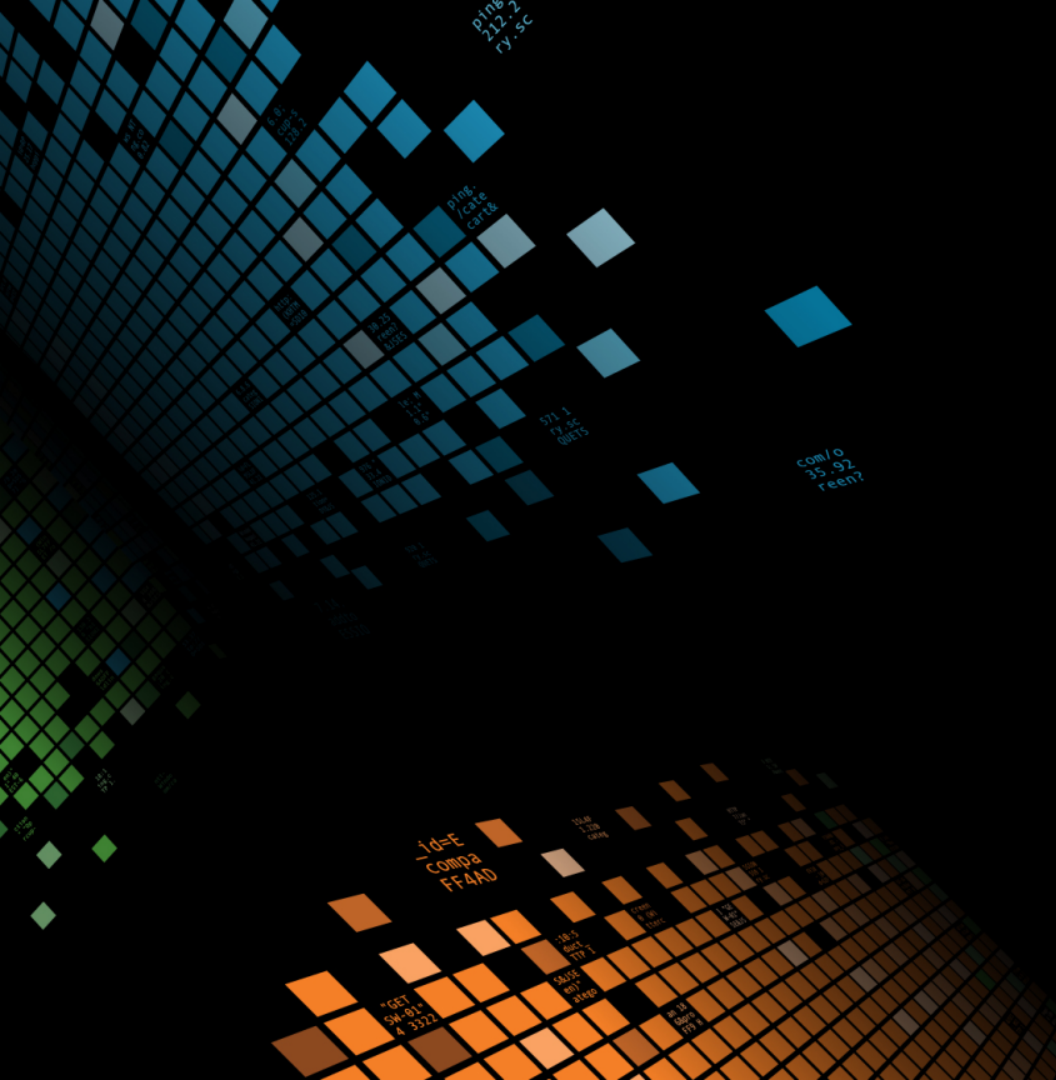
**1422**  
Reputation

**226**  
Posts

**38**  
Following

**7**  
Followers

**11/11**  
Joined



# Searching

---



# Pretty Searches

I feel pretty, oh so pretty...







# Ninja: Debug This

Where's ~~Waldo~~ eval max\_runtime?!

```
`dmc_audit_get_searches(*)` | stats min(_time) as _time, values(user) as user, max(total_run_time) as
total_run_time, first(search) as search, first(search_type) as search_type, first(apiStartTime) as
apiStartTime, first(apiEndTime) as apiEndTime by search_id | where isnotnull(search) AND search_type
="ad hoc" | search user="*" | stats count median(total_run_time) as median_runtime max(total_run_time)
as max_runtime values(user) as user by search | eval median_runtime=if(isnotnull(median_runtime),
median_runtime, "-") | eval max_runtime=if(isnotnull(max_runtime), max_runtime, "-") | sort - count |
rename search as "Search", count as "Count", median_runtime as "Median Runtime", max_runtime as "Max
Runtime", user as User | fieldformat "Median Runtime" = `dmc_convert_runtime('Median Runtime')` |
fieldformat "Max Runtime" = `dmc_convert_runtime('Max Runtime')`
```

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f75&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=60-CW-01"
OwS NT 5.1: 160.0.0 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=60-CW-01"
//buttercup-160: - NET CLR 1.1.4322) 468 125.17 /category.screen?category_id=61f75&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=60-CW-01"
buttercup-shopping.com/n-11-02" 468 125.17 /category.screen?category_id=61f75&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=60-CW-01"
opping.com/purchase&id=1" 468 125.17 /category.screen?category_id=61f75&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=60-CW-01"
/buttercup-160: -
```

# n00b: Debug This

Keyboard Command: Ctrl + \ or Command + \

```

1 `dmc_audit_get_searches(3ae8d0022f51)`
2 | stats min(_time) as _time, values(user) as user, max(total_run_time) as total_run_time, first(search) as search, first
   (search_type) as search_type, first(apiStartTime) as apiStartTime, first(apiEndTime) as apiEndTime by search_id
3 | where isnotnull(search) AND search_type="ad hoc"
4 | search user="*"
5 | stats count median(total_run_time) as median_runtime max(total_run_time) as max_runtime values(user) as user by search
6 | eval median_runtime=if(isnotnull(median_runtime), median_runtime, "-")
7 | eval max_runtime=if(isnotnull(max_runtime), max_runtime, "-")
8 | sort - count
9 | rename search as "Search", count as "Count", median_runtime as "Median Runtime", max_runtime as "Max Runtime", user as User
10 | fieldformat "Median Runtime" = `dmc_convert_runtime('Median Runtime')`
11 | fieldformat "Max Runtime" = `dmc_convert_runtime('Max Runtime')`

```

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f5e&SESSIONID=5D51L4FF1ADDF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68&product_id=F3-3w03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f5e&SESSIONID=5D51L4FF1ADDF10 HTTP/1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-68&product_id=60-CW00"
Owe NT 5.1: 160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-81&SESSIONID=5D51L9FF1ADDF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=5D185L8FF2ABF0"
itemid=EST-16&product_id=RP-L1-02" 468 125.17 /category.screen?category_id=61f5e&SESSIONID=5D51L4FF1ADDF10 HTTP/1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-L1-02"
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-L1-02" 468 125.17 /category.screen?category_id=61f5e&SESSIONID=5D51L9FF1ADDF3 HTTP/1.1" 200 1318 "GET /oldlink?item_id=EST-26&SESSIONID=5D51L9FF1ADDF3 HTTP/1.1" 200 1318 "GET /oldlink?item_id=EST-26&SESSIONID=5D51L9FF1ADDF3 HTTP/1.1" 200 1318 "GET /category.screen?category_id=61f5e&SESSIONID=5D51L4FF1ADDF10 HTTP/1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16&product_id=RP-L1-02"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16&product_id=RP-L1-02"

```

# Search Interface Improvements

## ► Default

### Search

Use these properties for assistance with command syntax including examples in different colors.

Search assistant

- Compact
- Full
- None

Syntax highlighting

Light theme

Search auto-format

- On
- Off

Show line numbers

- On
- Off

## ► Suggestion

### Search

Use these properties for assistance with command syntax including examples in different colors.

Search assistant

- Compact
- Full
- None

Syntax highlighting

Dark theme

Search auto-format

- On
- Off

Show line numbers

- On
- Off

# What the?!

## Speaking of UI...

### Soooo sssllllloooowwww

1 index=\_internal  
2 | stats count

353 of 353 events matched No Event Sampling

Events (353) Patterns Statistics (1)

20 Per Page Format Preview

count
353

### Dude! Where's my fields?!

1 index=\_internal

928,453 of 928,453 events matched No Event Sampling

Events (928,453) Patterns Statistics Visualization

Format Timeline List Format 20 Per Page

< Hide Fields All Fields

	i	Time	Event
>		9/23/17 11:59:59.995 PM	127.0.0.1 - splunk-system-HTTP/1.0" 200 364 - - - 11:59:59.995 PM
>		9/23/17 11:59:59.976 PM	09-23-2017 23:59:59.976 -0.oad from='ds.splunk.aws.th
>		9/23/17 11:59:59.976 PM	2017-09-23 23:59:59.976 IN 23:54:58+0000)
>		9/23/17 11:59:59.976 PM	2017-09-23 23:59:59.975 IN 23:54:58.2017"

Selected Fields

- a host 13
- a source 51
- a sourcetype 39

Interesting Fields

- a index 1
- # linecount 9
- a splunk\_server 3

# Search Mode

## Speaking of UI...

Soooo sssllllll

What's my fields?!

```

1 index=_internal
2 | stats count

```

353 of 353 events matched


Events (353) Patterns



20 Per Page Format


count

353

Job [ ] [ ] [ ] [ ] [ ] Smart Mode

 **Fast Mode**  
Field discovery off for event searches. No event or field data for stats searches.

  **Smart Mode**  
Field discovery on for event searches. No event or field data for stats searches.

 **Verbose Mode**  
All event & field data.

Sampling

Statistics Visualization

t Format 20 Per Page

Time	Event
9/23/17 11:59:59.995 PM	127.0.0.1 - splunk-system-HTTP/1.0" 200 364 - - - 11:59:59.995 PM host = boba source = /opt/splunk
9/23/17 11:59:59.976 PM	09-23-2017 23:59:59.976 - 09-23-2017 23:59:59.976 oad from='ds.splunk.aws.th host = chewbacca source = /opt/splunk
9/23/17 11:59:59.976 PM	2017-09-23 23:59:59.976 IN 2017-09-23 23:54:58+0000) host = boba source = /opt/splunk
9/23/17 11:59:59.976 PM	2017-09-23 23:59:59.975 IN 2017-09-23 23:54:58+0000) host = boba source = /opt/splunk

# linecount 9  
a splunk\_server 3



# Event Types & Tags

Weak:

```
index=oidemo host=dmzlog.splunktel.com sourcetype=access_combined
source=/opt/apache/log/access_combined.log iphone
user_agent="*iphone*"
| stats count by action
```

Strong:

```
tag=iphone_event
```

or

```
eventtype=web_logs
```

# Dereference Finesse

## Weak:

```
index=internal
| eval ERROR = case( log_level == "ERROR" , message )
| eval WARN = case( log_level == "WARN" , message )
| eval INFO = case( log_level == "INFO" , message )
```

## Strong:

```
index=_internal
| eval {log_level} = message
```

### Selected Fields

a **ERROR** 100+

a **INFO** 100+

a **WARN** 100+

a **WARNING** 92

# Pretty Searches: coalesce’s cooler than if

## Weak:

```
...| eval size = if( isnull(bytes) , if( isnull(b) , "N/A" , b ) , bytes )
```

## Strong:

```
...| eval size = coalesce( bytes , b , "N/A" )
```

130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=61f75&sessionid=5d5154f1f10adff3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F3-5w03-9680r/0-20  
128.241.230.82 - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-DSH-81&sessionid=5d517ff6adff9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product\_id=K0-1280-CW40-C600/0-20  
1317.27.160.0 - [07/Jan 18:10:57:156] "GET /oldlink?product\_id=FL-DSH-81&sessionid=5d517ff6adff9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product\_id=K0-1280-CW40-C600/0-20  
vitemid=EST-1&SVI: NET CLR 1.1.4322" 468 125.17 "GET /oldlink?item\_id=EST-2&sessionid=5d519ff1adff3 HTTP/1.1" 500 1871 "GET /category.screen?category\_id=61f75&sessionid=5d5154f1f10adff3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product\_id=K0-1280-CW40-C600/0-20  
0:buttercup-shopping\_id=RP-LI-02" 468 125.17 "GET /category.screen?category\_id=61f75&sessionid=5d5154f1f10adff3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product\_id=K0-1280-CW40-C600/0-20  
shopping.com/purchase&t

# Macros

Keyboard Shortcut: Control-Shift-E or Command-Shift-E

## Repeatable Code

### Definition \*

Enter the string the search macro expands to when it is referenced in another

```
`HandleInfoMaxTime` | head _time>(info_max_time - $
alert_value_window=if(_time<(info_max_time-$search_
$entity_statop$( $threshold_field$) AS alert_value b
$service_statop$(alert_value) AS alert_value by ale
alert_value_window="current_window" | eval window_d
"none")) | `gettime`
```

Use eval-based definition?

### Arguments

Enter a comma-delimited string of argument names. Argument names may c

entity\_statop, service\_statop, threshold\_field, entity\_field, search\_alert

## Expand in UI

The screenshot shows the Splunk search interface. At the top, there are tabs for 'Overview' and 'Health'. Below that, a search bar contains 'New Search'. A dropdown menu is open, showing two search queries: '1 `dmc\_license`' and '2 `| `dmc\_license`'. The second query is selected. Below the dropdown, it says '406 events (before)'. To the right, a panel titled 'Expanded Search String' displays the full search string for the selected query:

```
1 index=_internal host=leah source=*license_usage.log
2 | eval _time=_time - 43200
3 | bin _time span=1d
4 | stats latest(b) AS b by slave, pool, _time
5 | timechart span=1d sum(b) AS "volume" fixedrange=f
6 | join type=outer _time
7 [ search index=_internal host=leah source=*lice
   =-30d@d
```

[docs.splunk.com "Help reading searches"](https://docs.splunk.com/HowTo/Help%20reading%20searches)

# Time and Units

## Weak:

```
...| eval new_time = <ridiculous string edits>
```

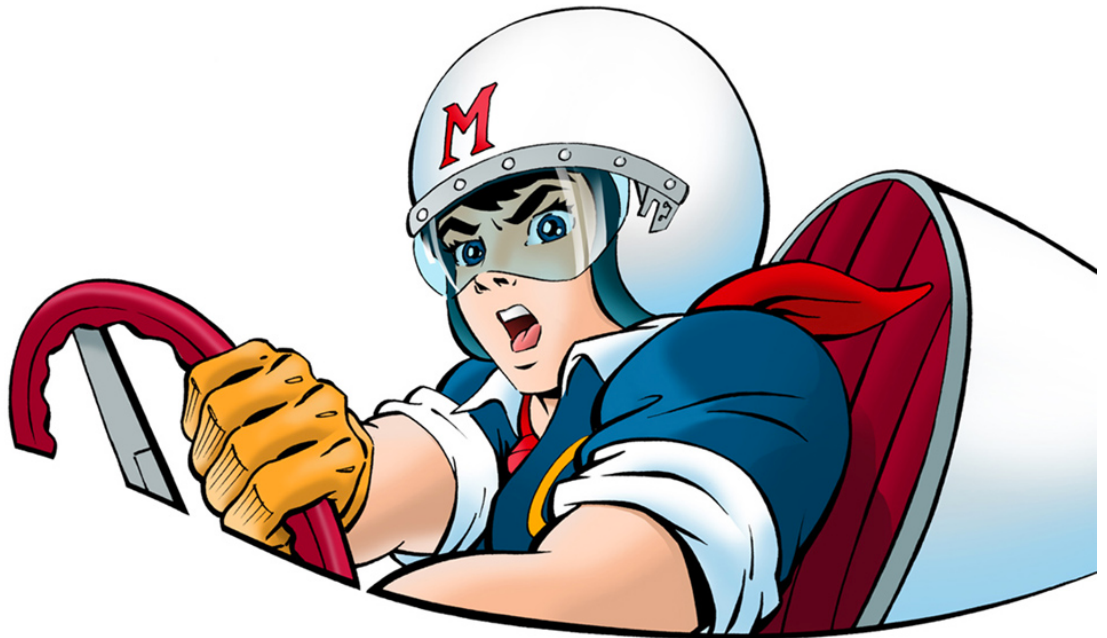
## Strong:

```
...| convert ctime(duration) ...| bin span=1h _time
...| eval pause = tostring( pause , "duration" )
...| rename new_time as _time
```



# Search Performance

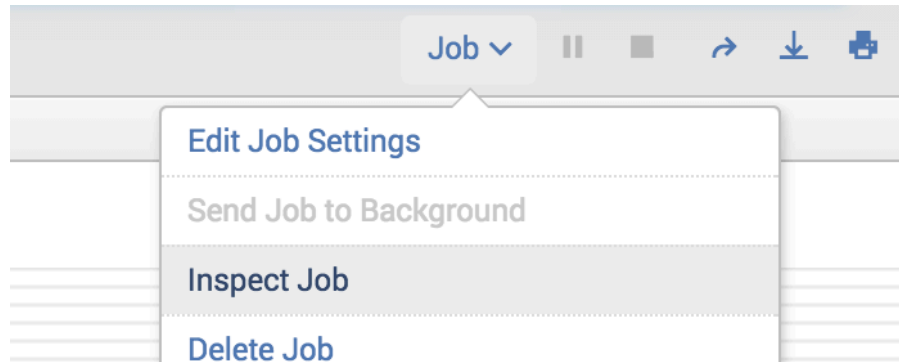
He's a demon on wheels



# Search Performance Improvement

docs.splunk.com “Search Job Inspector”

- ▶ events per second = events / seconds
- ▶ results per second = results / seconds



This search has completed and has returned **1,000** results by scanning **22,696** events in **1.049** seconds.





# NOT NOTs

Weak:

index=burch NOT blah=yay blah=cool

Strong:

index=burch blah=duh

index=burch blah!=yay

Implies ( blah!=yay blah=\* )

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=61F7S&SESSIONID=5D5L4FF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"  
 1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-5SH-01&SESSIONID=5D5L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=F1-5W03- "burch/duh"

# stats vs dedup/transaction

## Weak:

```
... phone=*
| dedup phone
| table phone
| sort phone
```

```
... phone=*
| transaction host
| table host, phone
```

## Strong:

```
... phone=*
| stats count by phone, host
| fields - count
```

## Pro Tip:

- Table is cosmetic
- Fields is reducing

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW-03-18062020"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW-03-18062020"
OwS NT 5.1: 160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=F3-SW-03-18062020"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW-03-18062020"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW-03-18062020"
OwS NT 5.1: 160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=F3-SW-03-18062020"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW-03-18062020"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW-03-18062020"
OwS NT 5.1: 160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=F3-SW-03-18062020"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW-03-18062020"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW-03-18062020"
OwS NT 5.1: 160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 2823 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=F3-SW-03-18062020"
```

# Avoid Subsearches

Weak:

```
index=burch | eval blah=yay
| append [ search index=simon | eval blah=duh ]
```

Strong:

```
( index=burch ... ) OR ( index=simon ... )
| eval blah=case( index=="burch" , "yay" , index=="simon" ,
"duh" )
```

(format and return commands for returning results)

# foreach FTW!

## Weak:

```
...| timechart span=1h limit=0 sum(eval(b/pow(1024,3))) as size
by st
```

## Strong:

```
...| timechart span=1h limit=0 sum(b) by st
| foreach * [ eval <<FIELD>> = '<<FIELD>>' / pow( 1024 , 3 ) ]
```

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F75&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68&product_id=F3-5W03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-68&product_id=F3-5W03"
1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-68&product_id=F3-5W03"
Oms NT S:1: SVI: [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F75&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68&product_id=F3-5W03"
/buttercup-shopping.com/nr-11-4322" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1"
/buttercup-shopping.com/nr-11-4322" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1"
shopping.com/purchase&itemId=EST-18&product_id=V-C-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1"
/buttercup-shopping.com/nr-11-4322" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=5D5154FF1ADFF10 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D5154FF1ADFF10 HTTP/1.1"
```





# eventcount

Weak:

```
index=*
| stats count by index
```

Strong:

```
| eventcount summarize=false index=*
```

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F7S&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW03" "buttercup-shopping.com"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=00-CW00" "buttercup-shopping.com"
1317.27.160.0 - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=0V-CB-01&SESSIONID=COMW00" "buttercup-shopping.com"
1317.27.160.0 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-6&SESSIONID=SD185L9FF2ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/n-1-4322" "buttercup-shopping.com"
1317.27.160.0 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 125.17 "http://buttercup-shopping.com/n-1-02" "buttercup-shopping.com"
1317.27.160.0 - - [07/Jan 18:10:57:156] "GET /cart.do?action=remove&itemId=EST-1&product_id=0V-CB-01&SESSIONID=COMW00" "buttercup-shopping.com"
1317.27.160.0 - - [07/Jan 18:10:57:156] "GET /category.screen?category_id=SURF&SESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/n-1-02" "buttercup-shopping.com"
```

# Dashboard Performance

## If your dashboard...

- ▶ ...has many similar searches
- ▶ ...is viewed by many
- ▶ ...is viewed by few

## Then use...

- ▶ “Post-process”
- ▶ Scheduled report (cache)
- ▶ Inline Searches



# Pretty SimpleXML

Keyboard Command: CTRL + Shift + F or Command + Shift + F

```
<form refresh="600">
<label>Launchpad</label>
<fieldset submitButton="false" autoRun="true">
<input type="time" searchWhenChanged="true">
<label>Specify preferred time window</label>
<default>
<earliest>@d</earliest>
<latest>now</latest>
</default>
</input>
<input type="dropdown" token="percentageFilter" searchWhenChanged="true">
<label>Select a cut-off percentage</label>
<choice value="0">0%</choice>
<choice value="25">25%</choice>
<choice value="50">50%</choice>
<choice value="75">75%</choice>
<choice value="85">85%</choice>
<choice value="90">90%</choice>
<choice value="95">95%</choice>
<default>0</default>
</input>
</fieldset>
<row>
<panel>
<html>
<h1>Learning Splunk</h1>
```

```
<form refresh="600">
<label>Launchpad</label>
<fieldset submitButton="false" autoRun="true">
<input type="time" searchWhenChanged="true">
<label>Specify preferred time window</label>
<default>
<earliest>@d</earliest>
<latest>now</latest>
</default>
</input>
<input type="dropdown" token="percentageFilter" searchWhenChanged="true">
<label>Select a cut-off percentage</label>
<choice value="0">0%</choice>
<choice value="25">25%</choice>
<choice value="50">50%</choice>
<choice value="75">75%</choice>
<choice value="85">85%</choice>
<choice value="90">90%</choice>
<choice value="95">95%</choice>
<default>0</default>
</input>
</fieldset>
<row>
<panel>
<html>
<h1>Learning Splunk</h1>
<ul>
<li>
```

# Metrics Explorer for Splunk

<https://splunkbase.splunk.com/app/3726/>



## Metrics Explorer for Splunk

### Metrics Explorer

Select Metrics Index(s)

Last 24 hours

All

Available Metrics from index: "\*"

metric\_name

cpu.idle.value

cpu.interrupt.value

cpu.nice.value

cpu.percent.idle.value

cpu.percent.interrupt.value

cpu.percent.nice.value

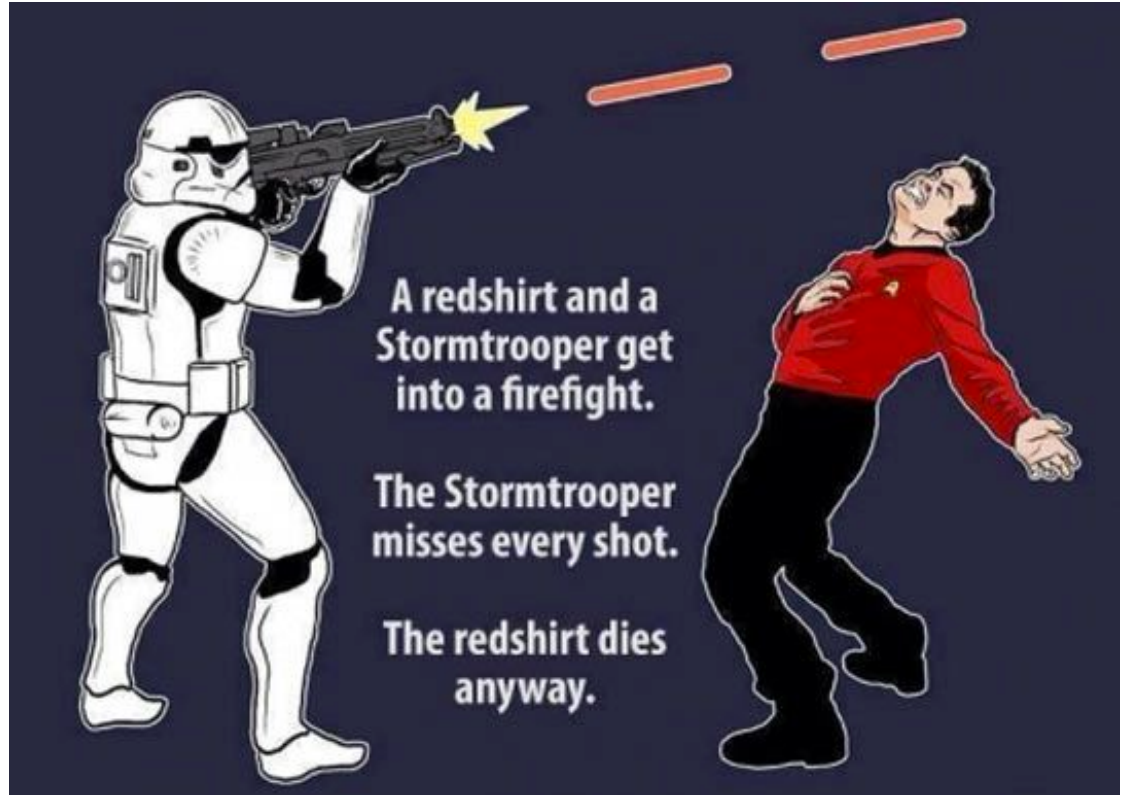
cpu.percent.softirq.value

cpu.percent.steal.value

cpu.percent.system.value

cpu.percent.user.value

# Accuracy





# Be specific

## Time Selector!

**Weak:**

iphone

| stats count by action

**Strong:**

index=oidemo host=dmzlog.splunktel.com

sourcetype=access\_combined

source=/opt/apache/log/access\_combined.log iphone

user\_agent="\*iphone\*"

| stats count by action

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f75&SESSIONID=5D55L4FF1ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-5W03- "
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=61f75&SESSIONID=5D55L4FF1ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03- "
OwS NT 5.1: SV: [07/Jan 18:10:57:153] "GET /category.screen?category_id=61f75&SESSIONID=5D55L4FF1ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-5W03- "
/vitemId=EST-16&product_id=RP-LI-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D55L4FF1ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03- "
action=shopping.com/n-net CLR 1.1.4322" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D55L4FF1ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03- "
shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=V-C-01&SESSIONID=5D55L4FF1ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03- "
```



# Create New Fields?! rex different for each person

## Interesting Fields

- a component 49
- # date\_hour 1
- # date\_mday 1
- # date\_minute 16
- a date\_month 1
- # date\_second 60
- a date\_wday 1
- # date\_year 1
- # date\_zone 1
- a eventtype 3
- a group 37
- a idx 100+
- a index 1
- # ingest\_pipe 2



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F5t&SESSIONID=5D5L9FF1ADF3 HTTP/1.1" 404 720
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FLD5H-81&SESSIONID=5D5L9FF1ADF3 HTTP/1.1" 200 1318
317.27.160.0 - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FLD5H-81&SESSIONID=5D5L9FF1ADF3 HTTP/1.1" 200 1318
One NT 5.1: SVI: - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F5t&SESSIONID=5D5L9FF1ADF3 HTTP/1.1" 404 720
//buttercup-shopping.com/n-1-02" 468 125.17
action=purchase&it
```

# Extract Fields

Search: docs.splunk.com field extractor

More values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression. You can also indicate values in the sample event to modify them. [Learn more](#)

2014 14:46:01 Sent to **checkout** TransactionID=107387

2014 14:46:03 Sent to **Accounting System** 100303

Field Name:

Sample Value: **Accounting System**

2014 14:46:03 Sent to **Accounting** System 100303

2014 14:46:03 TransactionID=107387 AcctCode=4400-4383

2014 14:46:01 ecomm engine **response** TransactionID=107387 CustomerID=5i31kpk5 accepted

# timestartpos 7		
a uri 100+	>	9/8/14 6:08:44
a uri_path 14		
a uri_query 100+		
a user 1		
a useragent 25	>	9/8/14 6:08:44
# version 1		
4 more fields		
<a href="#">Extract New Fields</a>	>	9/8/14 6:08:44

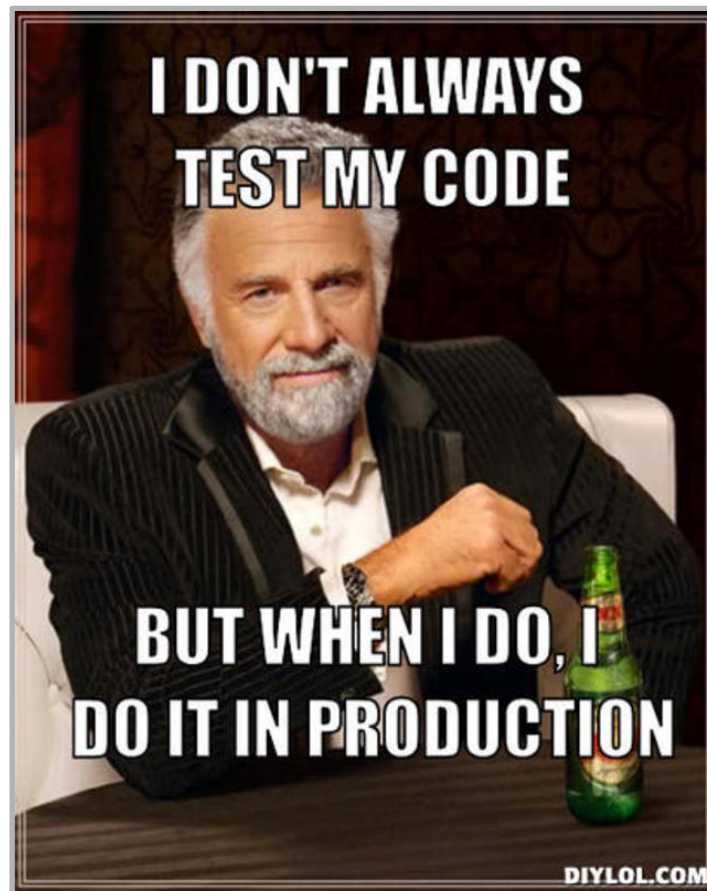


# Play it Safe

## Hands-on Labs

### Sandboxing with Splunk (with Docker)

Accept it. You're afraid to take risks in Splunk. So was I. That is, until Docker changed my life. Join the cult and learn how to rapidly create disposable Splunk sandboxes in mere minutes!



# Hidden Fields: Time

docs.splunk.com Search Time Modifiers

Event Time	Index Time
<u>_time</u>	<u>_indextime</u>

## What does a big difference mean?

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW03-18069420"
128.241.230.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"
OwS NT 5.1.160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"
/vitemId=EST-5VI: - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"
//buttercup-shopping.com/n- - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"
buttercup-shopping.com/n- - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"
shopping.com/n- - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"
/buttercup-shopping.com/n- - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GLF7S&SESSIONID=SD5SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-SW03-18069420"

```

# Hidden Fields: Time

docs.splunk.com Search Time Modifiers

Event Time	Index Time
<code>_time</code>	<code>_indextime</code>
<code>earliest</code>	<code>_index_earliest</code>
<code>latest</code>	<code>_index_latest</code>

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLFTS&SESSIONID=SD5SL4FF1ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=K1-L1"
Ows NT 5.1:160.0.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=K1-L1"
item_id=EST-10&product_id=RP-L1-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=K1-L1"
//buttercup-shopping.com/n/en?category_id=GLFTS&SESSIONID=SD5SL4FF1ADFF10 HTTP 1.1" 200 2823 "http://buttercup-shopping.com/category.screen?category_id=K1-L1"
action=changequantity&itemId=EST-10&product_id=RP-L1-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=K1-L1"
action=purchase&itemId=EST-10&product_id=RP-L1-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=K1-L1"

```

# Snap-To Times

## Weak:

### Time range

Start time

Finish time

Time specifiers: y, mon, d, h, m, s

[Learn more](#)

### Acceleration

Accelerate this search

### Schedule and alert

Schedule this search

Schedule type \*

Run every \*

## Strong:

### Time range

Start time

Finish time

Time specifiers: y, mon, d, h, m, s

[Learn more](#)

### Acceleration

Accelerate this search

### Schedule and alert

Schedule this search

Schedule type \*

Run every \*

# Time Fields

## Weak:

Search

```
earliest=-24hours latest=now|
```

```
...
```

## Strong:

### Time range

Start time

Finish time

Time specifiers: y, mon, d, h, m, s

[Learn more](#)

### Acceleration

Accelerate this search

### Schedule and alert

Schedule this search

Schedule type \*

Basic

Run every \*

hour

# Alerts

## Blueprints for Actionable Alerts

Wednesday, September 27, 2017 | 3:30 PM-4:15 PM

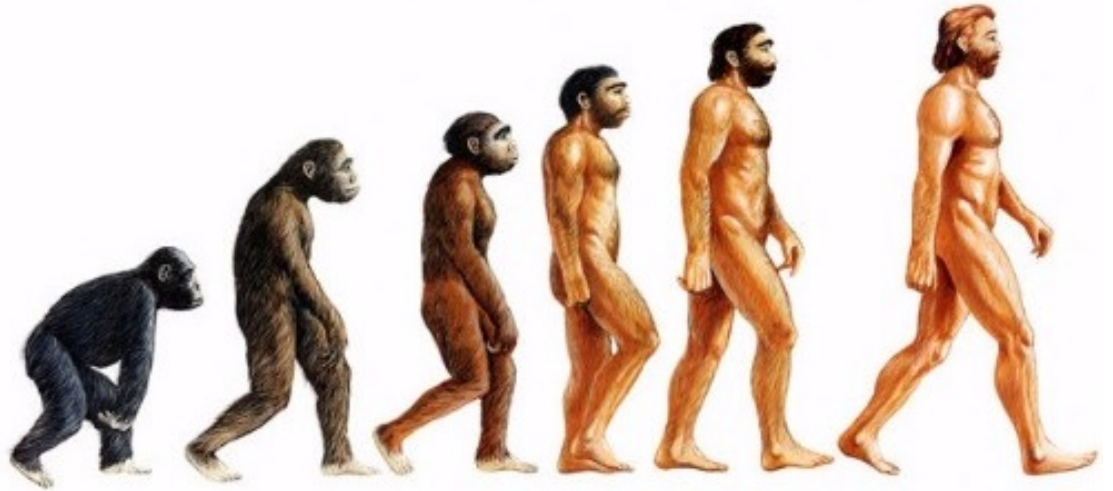
GOOD FOR ALL SKILL LEVELS

**Burch !**, Senior Best Practices Engineer, Splunk Inc.

Do you receive too many alerts from your Splunk environment and don't know which to focus on? Do you have so many alerts that you no longer see through the noise? Do you fear that your Splunk investment is losing its purpose and value because users have no choice but to ignore it? I've been there. I inherited a system like that. This is an updated version of the popular session from .conf2016 covering the evolution of how I improved those alerts and shifted Splunk from spam to glam. Come to this session to learn from my experiences and approaches, which will provide you with more confidence and actionable alerts.

# Evolved Ideas

**BOSH! -> BOSCH!  
-> BORCH! -> BURCH!**



# Acceleration Options

Knowledge Manager Manual > Use data summaries to accelerate searches > Manage report acceleration

	Summary Indexing	Report Acceleration	Data Model Acceleration
Benefits	<ul style="list-style-type: none"> <li>Save disk space</li> <li>Control on impact to system</li> </ul>	<ul style="list-style-type: none"> <li>Backfill</li> <li>Simple</li> </ul>	<ul style="list-style-type: none"> <li>Backfill</li> <li>Simple</li> <li>Extensible</li> <li>Search Agnostic</li> </ul>
Limits	<ul style="list-style-type: none"> <li>Gaps</li> <li>Intellectually difficult</li> <li>Backfill</li> </ul>	<ul style="list-style-type: none"> <li>Requires transforming</li> <li>Specific to search</li> </ul>	<ul style="list-style-type: none"> <li>Massive if misused</li> </ul>



# Don't Scare Your Admins

## Impress Them!

- ▶ Accelerations
- ▶ Scheduled Searches
- ▶ Real Time Searches
- ▶ Search Limits

© 2017 SPLUNK INC.

### Selection of Impacting Capabilities

<http://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities>


Group	Capabilities	Why
Accelerations	<ul style="list-style-type: none"> <li>• <a href="#">accelerate_datamodel</a></li> <li>• <a href="#">accelerate_search</a></li> <li>• <a href="#">output_file</a></li> </ul>	<ul style="list-style-type: none"> <li>• Compute &amp; Storage costs</li> <li>• Rarely cleaned up</li> </ul>
Scheduled Searches	<ul style="list-style-type: none"> <li>• <a href="#">schedule_search</a></li> <li>• <a href="#">schedule_rtsearch</a></li> </ul>	<ul style="list-style-type: none"> <li>• Compute and concurrent load</li> <li>• Rarely cleaned up</li> </ul>
Real Time Searches	<ul style="list-style-type: none"> <li>• <a href="#">rtsearch</a></li> <li>• <a href="#">schedule_rtsearch</a></li> </ul>	<ul style="list-style-type: none"> <li>• Rarely necessary</li> <li>• Impact on SH + ALL Indexers</li> <li>• Proliferation to dashboards</li> </ul>
Search Limits	<ul style="list-style-type: none"> <li>• <a href="#">srchJobsQuota</a></li> <li>• <a href="#">srchMaxTime</a></li> <li>• <a href="#">srchTimeWin</a></li> <li>• <a href="#">srchDiskQuota</a></li> <li>• <a href="#">rtSrchJobsQuota</a></li> </ul>	<ul style="list-style-type: none"> <li>• Boundaries</li> </ul> <p>Careful, could be annoying</p>

splunk> .conf2017



# Search Consumption

## Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
<p align="center"><b>Unaware Issue Exists</b></p>	<p><b>Screens (Dashboards/GT)</b></p> <ul style="list-style-type: none"> <li>• Changes in behavior</li> <li>• Data Driven KPIs</li> <li>• Notice patterns</li> </ul>	
<p align="center"><b>Aware Issue Exists</b></p>	<p><b>Investigations (SPL)</b></p> <ul style="list-style-type: none"> <li>• Go Spelunking!</li> </ul>	<p><b>Alerts until Fixed</b></p> <ul style="list-style-type: none"> <li>• Monitor for known symptoms</li> <li>• Adaptive Response</li> <li>• Actionable</li> </ul>


```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLFTS&SESSIONID=SD5SL9FFADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W63"
128.241.230.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-5SH-81&SESSIONID=SD5SL7FFADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=GL-403"
Ows NT 5.1: SVI: - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FFADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=GL-403"
10.10.10.10 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-5SH-81&SESSIONID=SD5SL7FFADFF9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=GL-403"
//buttercup-shopping.com/n/-LI-02" 468 125.17 "GET /category.screen?category_id=GLFTS&SESSIONID=SD5SL9FFADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=GL-403"
http://buttercup-shopping.com/n/-LI-02" 468 125.17 "GET /category.screen?category_id=GLFTS&SESSIONID=SD5SL9FFADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=GL-403"
http://buttercup-shopping.com/n/-LI-02" 468 125.17 "GET /category.screen?category_id=GLFTS&SESSIONID=SD5SL9FFADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=GL-403"

```

# Search Consumption

## Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
<p><b>Unaware Issue Exists</b></p>	<p><b>Screens (Dashboards/GT)</b></p> <ul style="list-style-type: none"> <li>Changes in behavior</li> <li>Data Driven KPIs</li> <li>Notice patterns</li> </ul>	
<p><b>Aware Issue Exists</b></p>	<p><b>Investigations (SPL)</b></p> <ul style="list-style-type: none"> <li>Go Spelunking!</li> </ul>	<p><b>Alerts until Fixed</b></p> <ul style="list-style-type: none"> <li>Monitor for known symptoms</li> <li>Adaptive Response</li> <li>Actionable</li> </ul>




```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F75&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-SW-03"
128.241.230.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=00-CW-00"
OwS NT 5.1: 160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=00-CW-00"
itemId=EST-16&product_id=RP-LI-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "GET /cart.do?action=changequantity&itemId=EST-1&product_id=00-CW-00"
//buttercup-shopping.com/n/-LI-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "GET /cart.do?action=changequantity&itemId=EST-1&product_id=00-CW-00"
opping.com/purchase&item_id=EST-1&product_id=00-CW-00" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "GET /cart.do?action=changequantity&itemId=EST-1&product_id=00-CW-00"

```

# Search Consumption

## Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
<b>Unaware Issue Exists</b>	<b>Screens (Dashboards/GT)</b> <ul style="list-style-type: none"> <li>Changes in behavior</li> <li>Data Driven KPIs</li> <li>Notice patterns</li> </ul>	
<b>Aware Issue Exists</b>	<b>Investigations (SPL)</b> <ul style="list-style-type: none"> <li>Go Spelunking!</li> </ul>	<b>Alerts until Fixed</b> <ul style="list-style-type: none"> <li>Monitor for known symptoms</li> <li>Adaptive Response</li> <li>Actionable</li> </ul>

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLF7S&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F3-5W03"
128.241.230.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-81&SESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
OwS NT 5.1: Svi: - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-81&SESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
//buttercup-shopping.com/n/-LI-02" 468 125.17 "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"
action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=F3-5W03"

```

# Wrap Up

## 1. How I Learned

## 2. Searching

- Pretty Searches
- Search Performance
- Accuracy

## 3. Evolved Ideas

# What Now?



8DEC0D

1. Rate this! (be honest)
2. Collaborate: #bestpractices
  - Sign Up @ <http://splk.it/slack>
3. Customer Success Studio
4. More talks, search for
  - Blueprints
  - Burch
  - Champagne
  - Delaney
  - Optimization
  - Best Practices
  - Veuve

# Questions & Discussion?

Don't forget to **rate this session** in the  
.conf2017 mobile app







# Search with Burch: Index



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GLF7S&SESSIONID=5D5SL9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=31-w-03-10894/0-20-1  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=5D5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=31-w-03-10894/0-20-1  
317.2.160.0.0 - - [07/Jan 18:10:57:156] "GET /category.screen?category\_id=GLF7S&SESSIONID=5D5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=31-w-03-10894/0-20-1  
vitemid=EST-10&product\_id=RP-LI-02" 468 125.17 "c:tcp" "GET /category.screen?category\_id=FL-DSH-01&SESSIONID=5D5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=31-w-03-10894/0-20-1  
shopping.com/n-LI-02" 468 125.17 "c:tcp" "GET /category.screen?category\_id=GLF7S&SESSIONID=5D5SL9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=31-w-03-10894/0-20-1  
http://buttercup-shopping.com/n-LI-02" 468 125.17 "c:tcp" "GET /category.screen?category\_id=GLF7S&SESSIONID=5D5SL9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product\_id=31-w-03-10894/0-20-1