

splunk>

.conf2017

© 2017 SPLUNK INC.

# Power Of SPL

Stephen Luedtke | Sr. Technical Marketing Manager

September 27, 2017 | Washington, DC

# 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.

# Agenda

## 1. Overview & Anatomy of a Search

- Quick refresher on search language and structure

## 2. SPL Commands and Examples

- Searching, charting, converging, mapping, transactions, anomalies, exploring

## 3. Custom Commands

- Extend the capabilities of SPL

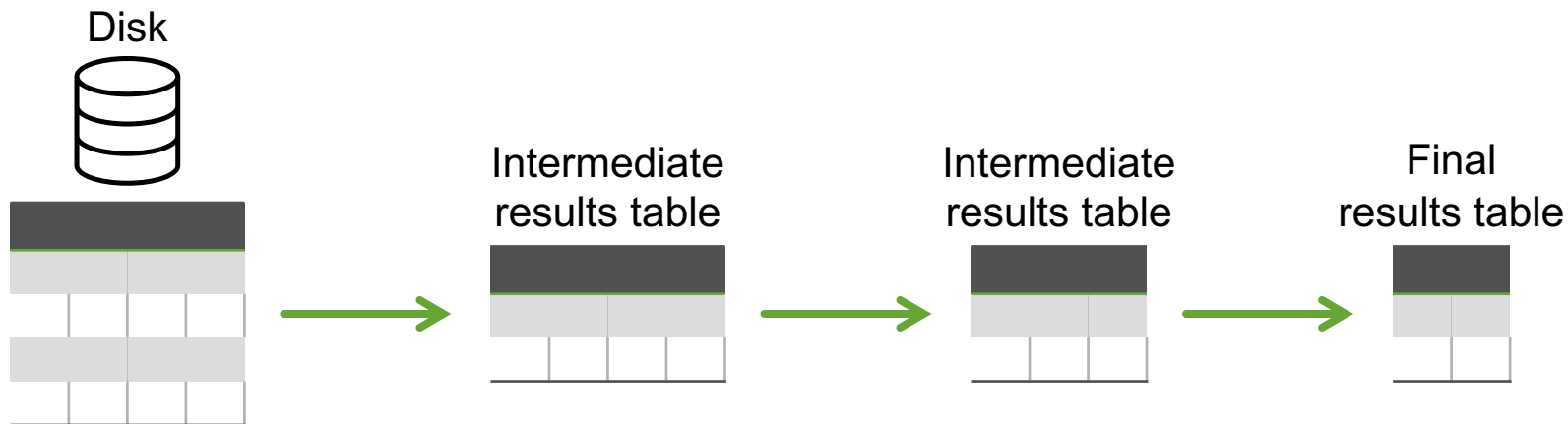
## 4. Q&A

# SPL Overview

---

# SPL Overview

- ▶ Over 140 search commands
- ▶ Syntax was originally based upon the **Unix pipeline** and **SQL** and is optimized **for time-series data**
- ▶ The scope of SPL includes data searching, filtering, modification, manipulation, enrichment, insertion and deletion
- ▶ Includes machine learning such as anomaly detection



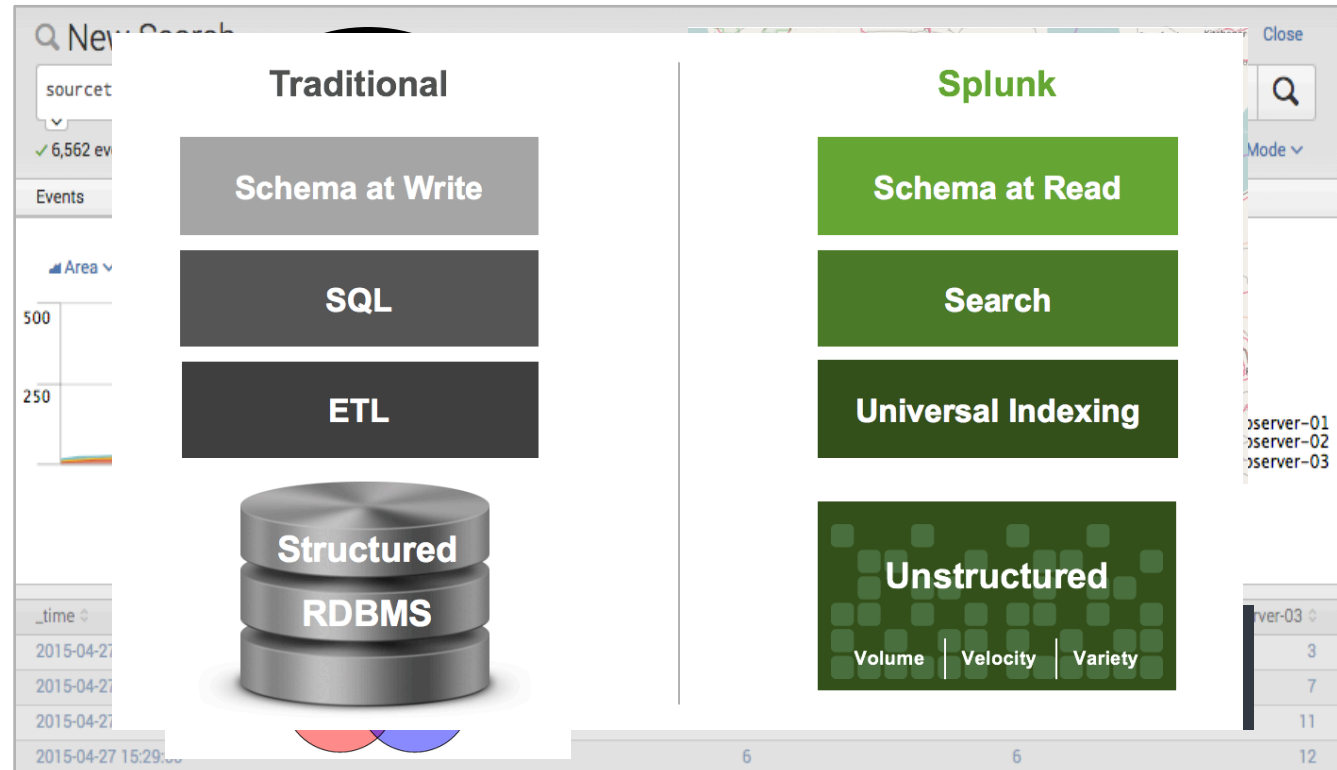
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L4FF10ADFF10"
10.2.1.1:51; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
10.2.1.1:51; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
10.2.1.1:51; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"

```

# Why Create A New Query Language?

- ▶ Flexibility and effectiveness on *small* and ***big*** data
- ▶ Late-binding schema
- ▶ More/better methods of correlation
- ▶ Not just analyze, but visualize



# SPL Basic Structure

search and filter | munge | report | cleanup

```
sourcetype=access*
```

```
| eval KB=bytes/1024
```

```
| stats sum(KB) dc(clientip)
```

```
| rename sum(KB) AS "Total KB" dc(clientip) AS "Unique Customers"
```

# SPL Examples

---



# SPL Examples And Recipes

- ▶ Find the needle in the haystack
- ▶ Charting statistics and predicting values
- ▶ Enriching and converging data sources
- ▶ Map geographic data in real time
- ▶ Identifying anomalies
- ▶ Transactions
- ▶ Data exploration & finding relationships between fields
- ▶ Custom commands

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
10.0.0.0 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
```

# SPL Examples And Recipes

- ▶ Find the needle in the haystack
- ▶ Charting statistics and predicting values
- ▶ Enriching and converging data sources
- ▶ Map geographic data in real time
- ▶ Identifying anomalies
- ▶ Transactions
- ▶ Data exploration & finding relationships between fields
- ▶ Custom Commands

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
ows NT 5.1; SV1; - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14.1.1.1 (189) "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"
```

# Search And Filter

## Examples

- ▶ **Keyword search:**  
sourcetype=access\* http
- ▶ **Filter:**  
sourcetype=access\* http  
host=webserver-02
- ▶ **Combined:**  
sourcetype=access\* http  
host=webserver-02 (503 OR 504)

**New Search**

sourcetype=access\* http

**Matching terms**

- 120,976 **http**
- 2,154 <http://m.acme.com/>
- 4,308 <http://m.acme.com/search.php>
- 22,184 <http://shop.acme.com/cart.do>
- 20,055 <http://shop.acme.com/category.screen>
- 13,808 <http://shop.acme.com/oldlink>
- 28,299 <http://shop.acme.com/product.screen>
- 798 <http://www.google.com/bot.html>
- 517 \*[http\\_ops=23](http://http_ops=23)
- 554 \*[http\\_ops=28](http://http_ops=28)
- 517 \*[http\\_ops\\_2=23](http://http_ops_2=23)
- 554 \*[http\\_ops\\_2=28](http://http_ops_2=28)
- 557 [httpjspbase.java:87](http://httpjspbase.java:87)
- 15,727 [http](http://http)
- 557 [httpervlet.java:856](http://httpervlet.java:856)

**How to Search**

**Step 1: Retrieve Events**  
The simplest searches return events that match terms you type into the search bar:  
terms: error login  
quoted phrases: "database error"  
boolean operators: login NOT (error OR fail)  
wildcards: fail\*  
field values: status=404, status!=404, or status>200

**Step 2: Use Search Commands**  
More advanced searches use commands to transform, filter, and report on the events you retrieved. Use the vertical bar "|" , or pipe character, to apply a command to the retrieved events.

# Search And Filter

## Examples

### ► Keyword search:

`sourcetype=access* http`

### ► Filter:

`sourcetype=access* http`  
`host=webserver-02`

### ► Combined:

`sourcetype=access* http`  
`host=webserver-02 (503 OR 504)`

The screenshot shows the Splunk Search interface. At the top, there is a search bar with the query `sourcetype=access_combined host=web*`. Below the search bar, it indicates that 8,839 events were found for the time range 4/7/15 8:49:00.000 AM to 4/7/15 9:49:08.000 AM. The interface includes tabs for Events (8,839), Patterns, Statistics, and Visualization. A timeline visualization is shown below the tabs. At the bottom, there is a table of search results with columns for Time and Event. The table shows several events from 4/7/15, including POST requests to /search.php and GET requests to /product.screen and /oldlink.

i	Time	Event
>	4/7/15 9:49:07.088 AM	175.45.177.187 - - [07/Apr/2015 09:49:07:088873] "POST /search.php?uid=1 AND (SELECT * FROM information_schema.tables WHERE table_name = 'users' AND table_schema = 'users') '1FF7ADFF9 HTTP 1.1' 503 45052 "http://m.acme.com/search.php?uid=1 AND (SELECT * FROM information_schema.tables WHERE table_name = 'users' AND table_schema = 'users') '6 (KHTML, like Gecko) Version/5.1 Mobile/9A334 Safari/7534.48.3" 8038 host = webserver-03   source = /opt/apache/log/access_combined.log   sourcetype = access_combined
>	4/7/15 9:49:07.070 AM	175.45.177.13 - - [07/Apr/2015 09:49:07:070283] "POST /search.php?uid=01226056-999 "http://m.acme.com/<script type='text/javascript'>alert('test');</script>" AppleWebKit (KHTML, like Gecko) Mobile [FBAN/FBForiPhone;FBAV/4.0.3;FBBV/4030.0;FBDV;FBLC/en_US;FBSF/1.0]" 11725 host = webserver-03   source = /opt/apache/log/access_combined.log   sourcetype = access_combined
>	4/7/15 9:49:07.067 AM	175.45.177.188 - - [07/Apr/2015 09:49:07:067717] "POST /search.php?uid=b066eae631978 "http://m.acme.com/<script type='text/javascript'>alert('pwd');</script>" AppleWebKit/528.18 (KHTML, like Gecko) Mobile/7E18" 9475 host = webserver-02   source = /opt/apache/log/access_combined.log   sourcetype = access_combined
>	4/7/15 9:49:07.046 AM	175.45.177.13 - - [07/Apr/2015 09:49:07:046441] "POST /search.php? (SELECT password FROM users WHERE username = 'admin') '9b04682d2&JSESSIONID=SD35L1FF7ADFF9 HTTP 1.1' 503 48015 "http://m.acme.com/search.php?uid=01226056-999 "http://m.acme.com/<script type='text/javascript'>alert('test');</script>" AppleWebKit/534.46 (KHTML, like Gecko) Mobile/9A334 Safari/7534.48.3" 8038 host = webserver-03   source = /opt/apache/log/access_combined.log   sourcetype = access_combined

# Search And Filter

## Examples

### ► Keyword search:

`sourcetype=access* http`

### ► Filter:

`sourcetype=access* http`  
`host=webserver-02`

### ► Combined:

`sourcetype=access* http`  
`host=webserver-02 (503 OR 504)`

New Search

sourcetype=access\* host=webserver-02 (503 OR 504)

✓ 1,965 events (4/7/15 8:53:00.000 AM to 4/7/15 9:53:06.000 AM)

Events (1,965) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

i	Time	Event
>	4/7/15 9:52:52.018 AM	144.185.205.147 - - [07/Apr/2015 09:52:52:018196] "GET /oldlink?item_id=WPSS-2&JS...duct.screen?product_id=WPSS-2" "mozilla/5.0 (iPad; U; CPU iPhone OS 5_0_1 like Mac...one; FBAV/4.0.3; FBBV/4030.0; FBDV/iPad2,1; FBMD/iPad; FBSN/iPhone OS; FBSV/5.0.1; FBSS/...
>	4/7/15 9:52:51.200 AM	175.45.177.187 - - [07/Apr/2015 09:52:51:200299] "POST /search.php?=1 AND (SELECT 1FF7ADFF9 HTTP 1.1" 504 53332 "http://m.acme.com/search.php?=1 AND (SELECT * FROM 22) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" 9877
>	4/7/15 9:52:51.172 AM	175.45.177.17 - - [07/Apr/2015 09:52:51:172965] "POST /search.php?=1 AND (SELECT FF7ADFF9 HTTP 1.1" 503 48362 "http://m.acme.com/search.php?=1 AND (SELECT * FROM ppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0 Mobile Safari/531.21
>	4/7/15 9:52:51.013 AM	175.45.177.13 - - [07/Apr/2015 09:52:51:013986] "POST /search.php?uid=497625e1-61648 "http://m.acme.com/<script type='text/javascript'>alert('pwnd');</script>" "r...pleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" 10071

Selected Fields  
a host 1  
a source 1  
a sourcetype 1

Interesting Fields  
# bytes 100+  
a category 1  
a clientip 100+  
# cost 8  
# date\_hour 2  
# date\_mday 1  
# date\_minute 60  
a date\_month 1

# Eval – Modify or Create New Fields and Values

## Examples

### ► Calculation:

```
sourcetype=access*
| eval KB=bytes/1024
```

### ► Evaluation:

```
sourcetype=access*
| eval http_response =
if(status != 200, "Error", "OK")
```

### ► Concatenation:

```
sourcetype=access*
| eval connection = device." - ".clientip
```

New Search

```
sourcetype=access*
| eval KB=bytes/1024
```

✓ 10,189 events (7/7/14 3:26:00.000 PM to 7/7/14 4:26:23.000 PM)

Events (10,189) | Statistics | Visualization

Format Timeline ▾ | Zoom Out

KB

>100 Values, 99.98% of events

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 1.989513 | Min: 0.097656 | Max: 3.906250 | Std Dev: 1.086884

Top 10 Values	Count	%
3.766602	11	0.108%
0.677734	8	0.078%

Selected Fields

- a host 2
- # KB 100+
- a source 2
- a sourcetype 2

# Eval – Modify or Create New Fields and Values

## Examples

### ► Calculation:

```
sourcetype=access*
| eval KB=bytes/1024
```

### ► Evaluation:

```
sourcetype=access*
| eval http_response =
if(status != 200, "Error", "OK")
```

### ► Concatenation:

```
sourcetype=access*
| eval connection = device." - ".clientip
```

New Search

```
sourcetype=access*
| eval http_response = if(status == 200, "OK", "Error")
```

10,323 events (6/27/14 11:58:00.000 AM to 6/27/14 12:58:58.000 PM)

Events (10,323) | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

List | Format | 20 Per Page

< Hide Fields | All Fields

Selected Fields

- # bytes 100+
- a clientip 100+
- a host 2
- a http\_response 2**
- # status 40
- a status\_description 40

Interesting Fields

- a action 5
- a bc\_uri 100+
- a category\_id 9

http\_response

2 Values, 100% of events

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Values	Count	%
OK	7,013	67.936%
Error	3,310	32.064%

12:58:53.562 PM LE-5WL&JSESSIONID=SD5SL1FF1ADFF9 HTTP 1.1" 200 474 "http://shop.splu

# Eval – Modify or Create New Fields and Values

## Examples

### ► Calculation:

```
sourcetype=access*
| eval KB=bytes/1024
```

### ► Evaluation:

```
sourcetype=access*
| eval http_response =
if(status != 200, "Error", "OK")
```

### ► Concatenation:

```
sourcetype=access*
| eval connection = device." - ".clientip
```

New Search

```
sourcetype=access*
| eval connection = clientip."." .port
```

✓ 10,330 events (6/27/14 12:03:00.000 PM to 6/27/14 1:03:52.000 PM)

Events (10,330) | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

connection

>100 Values, 26.941% of events

Selected

Reports

Top values | Top values by time | Rare values

Events with this field

Top 10 Values	Count	%
10.120.37.110:80	17	0.611%
10.122.183.49:80	13	0.467%
10.187.165.92:80	13	0.467%
10.169.199.125:80	11	0.395%

Selected Fields

- # bytes 100+
- a clientip 100+
- a connection 100+
- a host 2
- # status 40
- a status\_description 40



# Eval – Just Getting Started!

## Splunk Search Quick Reference Guide

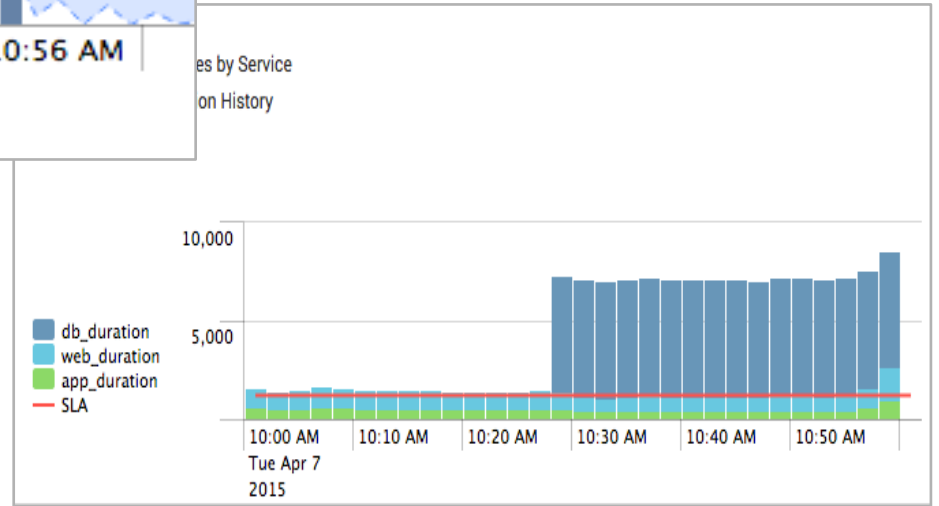
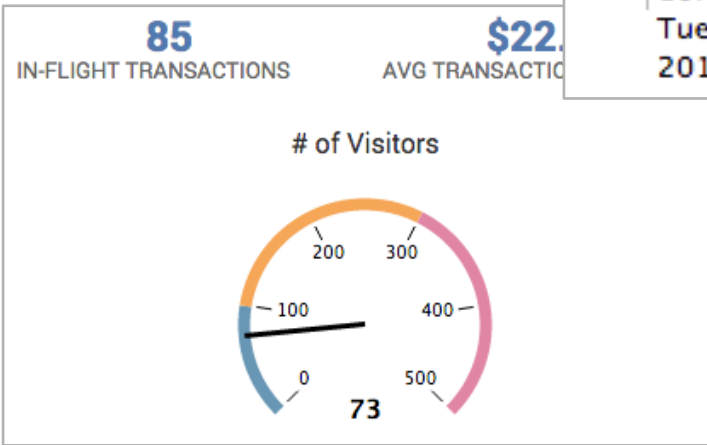
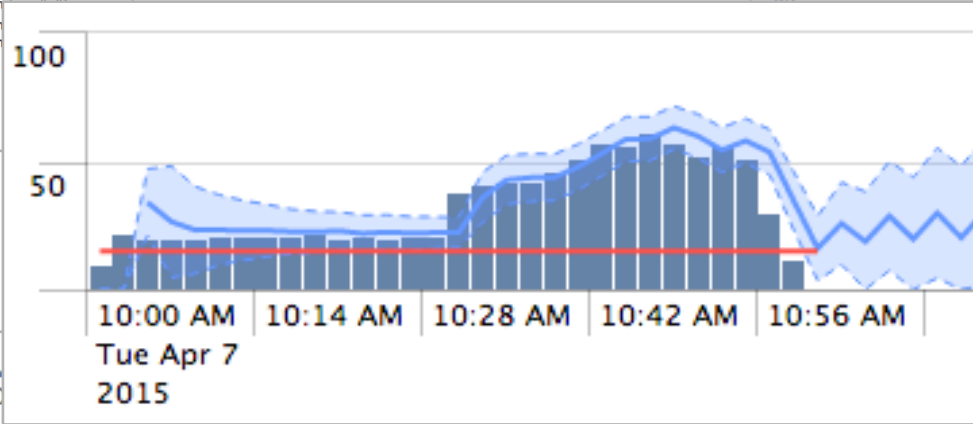
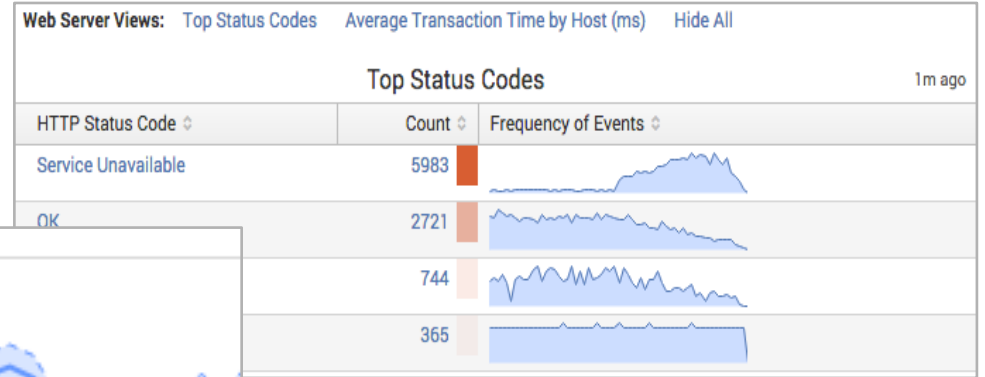
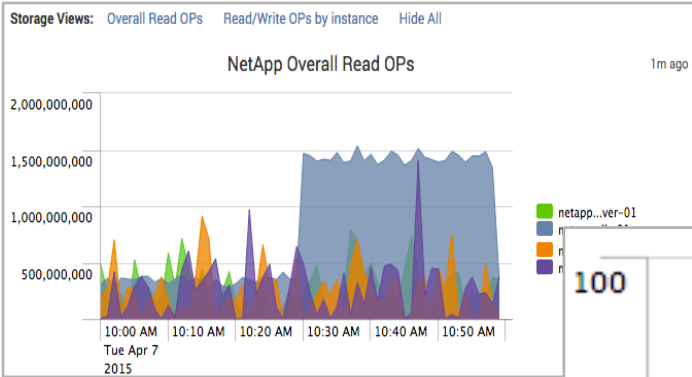
Common Eval Functions		The eval command calculates an expression and puts the resulting value into a field (e.g. "...  eval force = mass * acceleration"). The following table lists some of the functions used with the eval command. You can also use basic arithmetic operators (+ - * / %), string concatenation (e.g., "...  eval name = last . "," . first"), and Boolean operations (AND OR NOT XOR < > <= >= != == LIKE).
Function	Description	Examples
<b>abs(X)</b>	Returns the absolute value of X.	abs(number)
<b>case(X, "Y", ...)</b>	Takes pairs of arguments X and Y, where X arguments are Boolean expressions. When evaluated to TRUE, the arguments return the corresponding Y argument.	case(error == 404, "Not found", error == 500, "Internal Server Error", error == 200, "OK")
<b>ceil(X)</b>	Ceiling of a number X.	ceil(1.9)
<b>cidrmatch("X", Y)</b>	Identifies IP addresses that belong to a particular subnet.	cidrmatch("123.132.32.0/25", ip)
<b>coalesce(X, ...)</b>	Returns the first value that is not null.	coalesce(null(), "Returned val", null())
<b>cos(X)</b>	Calculates the cosine of X.	n=cos(0)
<b>exact(X)</b>	Evaluates an expression X using double precision floating point arithmetic.	exact(3.14*num)
<b>exp(X)</b>	Returns eX.	exp(3)
<b>if(X, Y, Z)</b>	If X evaluates to TRUE, the result is the second argument Y. If X evaluates to FALSE, the result evaluates to the third argument Z.	if(error==200, "OK", "Error")
<b>isbool(X)</b>	Returns TRUE if X is Boolean.	isbool(field)
<b>isint(X)</b>	Returns TRUE if X is an integer.	isint(field)
<b>isnull(X)</b>	Returns TRUE if X is NULL.	isnull(field)
<b>isstr()</b>	Returns TRUE if X is a string.	isstr(field)
<b>len(X)</b>	This function returns the character length of a string X.	len(field)
<b>like(X, "Y")</b>	Returns TRUE if and only if X is like the SQLite pattern in Y.	like(field, "addr%")

# SPL Examples And Recipes

- ▶ Find the needle in the haystack
- ▶ **Charting statistics and predicting values**
- ▶ Enriching and converging data sources
- ▶ Map geographic data in real time
- ▶ Identifying anomalies
- ▶ Transactions
- ▶ Data exploration & finding relationships between fields
- ▶ Custom commands

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14 "screen?category_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=EST-14" 404 1088 "http://buttercup-shopping.com/category.screen?category_id=EST-14"
10 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=EST-14" 404 1088 "http://buttercup-shopping.com/category.screen?category_id=EST-14"
```

# Stats, Timechart, Eventstats, Streamstats



130.60.4... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 317.27.160.0... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...  
 128.241.220.82... [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" Mozilla/5.0...

# Stats – Calculate Statistics Based on Field Values

## Examples

### ► Calculate stats and rename

Index=power\_of\_spl

| stats avg(bytes) AS “Avg Bytes”

### ► Multiple statistics

index=power\_of\_spl | stats avg(bytes) AS bytes  
sparkline(avg(bytes)) AS  
Bytes\_Trend min(bytes) max(bytes)

### ► By another field

index=power\_of\_spl  
| stats avg(bytes) AS avg\_bytes  
sparkline(avg(bytes)) AS Bytes\_Trend  
min(bytes) max(bytes) by clientip | sort -  
avg\_bytes

The screenshot shows the Splunk search interface. At the top, there are navigation tabs for Search, Walkthrough, and Dashboards. The current dashboard is titled "Power of SPL". A search bar contains the query: `index=power_of_spl | stats avg(bytes) AS "Avg Bytes"`. Below the search bar, it indicates that 18,076 events were found before 11/1/16 6:03:27.000 PM. The search results are displayed in a table with one row: "Avg Bytes" with a value of 4973.068212. The interface also shows options for "20 Per Page", "Format", and "Preview".

# Stats – Calculate Statistics Based on Field Values

## Examples

- ▶ Calculate stats and rename

```
index=power_of_spl
```

```
| stats avg(bytes) AS "Avg Bytes"
```

- ▶ Multiple statistics

```
index=power_of_spl | stats avg(bytes) AS
bytes sparkline(avg(bytes)) AS
Bytes_Trend min(bytes) max(bytes)
```

- ▶ By another field

```
index=power_of_spl
| stats avg(bytes) AS avg_bytes
sparkline(avg(bytes)) AS Bytes_Trend
min(bytes) max(bytes) by clientip | sort -
avg_bytes
```

The screenshot shows the Splunk search interface. The search bar contains the query: `index=power_of_spl | stats avg(bytes) AS bytes sparkline(avg(bytes)) AS Bytes_Trend min(bytes) as Min max(bytes) as Max`. The search results show 18,076 events. The results table is displayed in the 'Statistics (1)' view, showing a single row with the following values:

bytes	Bytes_Trend	Min	Max
4973.068212		100	59994

# Stats – Calculate Statistics Based on Field Values

## Examples

- ▶ Calculate stats and rename

Index=power\_of\_spl

| stats avg(bytes) AS “Avg Bytes”

- ▶ Multiple statistics

index=power\_of\_spl | stats avg(bytes) AS bytes  
sparkline(avg(bytes)) AS  
Bytes\_Trend min(bytes) max(bytes)

- ▶ By another field

index=power\_of\_spl  
| stats avg(bytes) AS avg\_bytes  
sparkline(avg(bytes)) AS Bytes\_Trend  
min(bytes) max(bytes) by clientip | sort -  
avg\_bytes

The screenshot shows the Splunk search interface with the following search query:

```
index=power_of_spl
| stats avg(bytes) AS avg_bytes sparkline(avg(bytes)) AS Bytes_Trend min(bytes) as Min max(bytes) as Max by clientip
| sort - avg_bytes
```

The search results show 1,009 events. The table below displays the first 10 results:

clientip	avg_bytes	Bytes_Trend	Min	Max
175.45.177.7	46638.013793		30198	59951
175.45.177.11	46343.569343		30539	59994
175.45.177.17	46043.953333		30143	59859
183.97.189.111	45766.188312		31479	59983
175.45.177.189	45471.924812		30430	59917
175.45.177.15	45246.281690		30108	59866
175.45.177.13	45079.918919		30398	59965
175.45.177.188	44702.584416		30065	59895
175.45.177.187	44306.079470		30130	58856
244.79.226.145	998.000000		998	998
166.105.65.33	903.666667		848	995

# Timechart – Visualize Statistics Over Time

## Examples

### ► Visualize stats over time

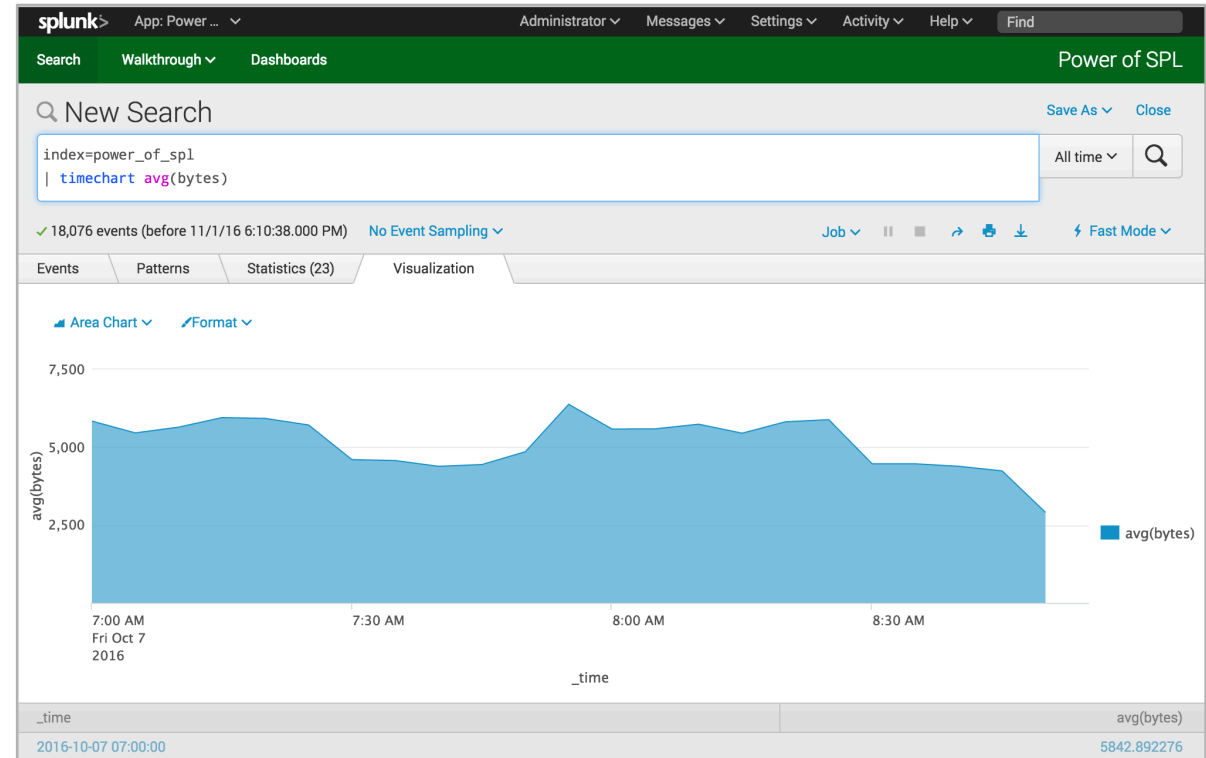
```
index=power_of_spl
| timechart avg(bytes)
```

### ► Add a trendline

```
index=power_of_spl
| timechart avg(bytes) as bytes
| trendline sma5(bytes)
```

### ► Add a prediction overlay

```
index=power_of_spl
| timechart avg(bytes) as bytes
| predict future_timespan=5 bytes
```



# Timechart – Visualize Statistics Over Time

## Examples

### ► Visualize stats over time

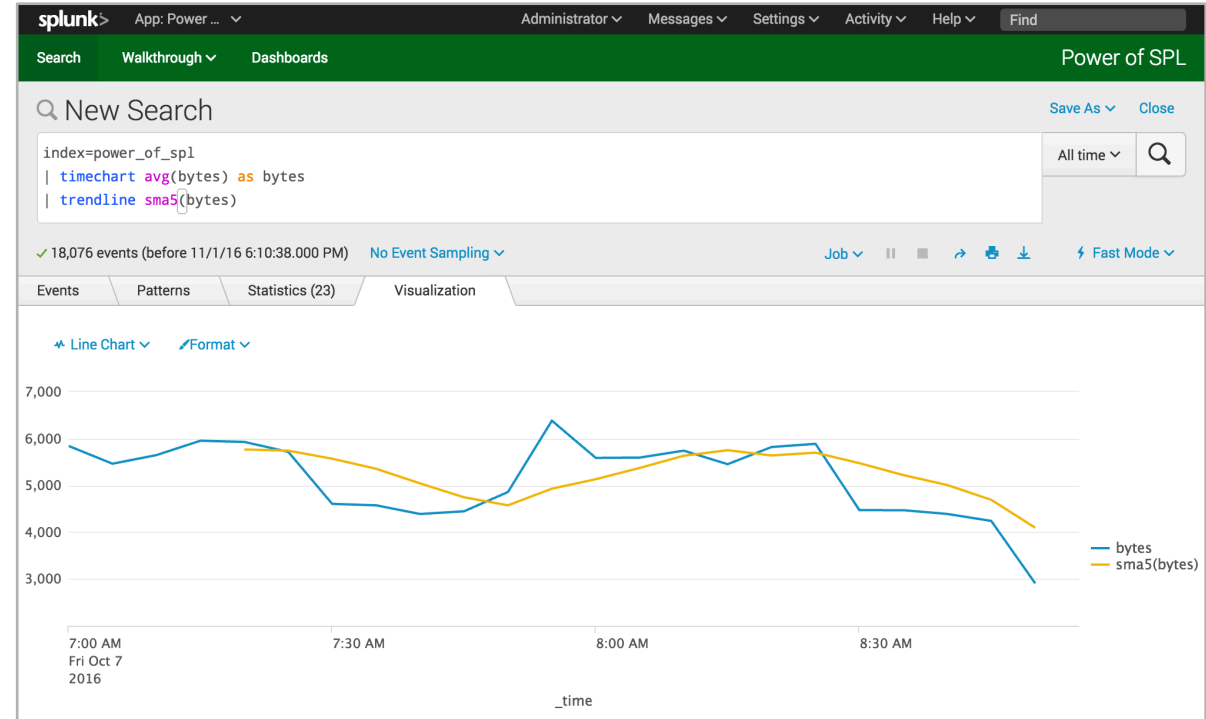
```
index=power_of_spl
| timechart avg(bytes)
```

### ► Add a trendline

```
index=power_of_spl
| timechart avg(bytes) as bytes
| trendline sma5(bytes)
```

### ► Add a prediction overlay

```
index=power_of_spl
| timechart avg(bytes) as bytes
| predict future_timespan=5 bytes
```





# Timechart – Visualize Statistics Over Time

## Examples

### ▶ Visualize stats over time

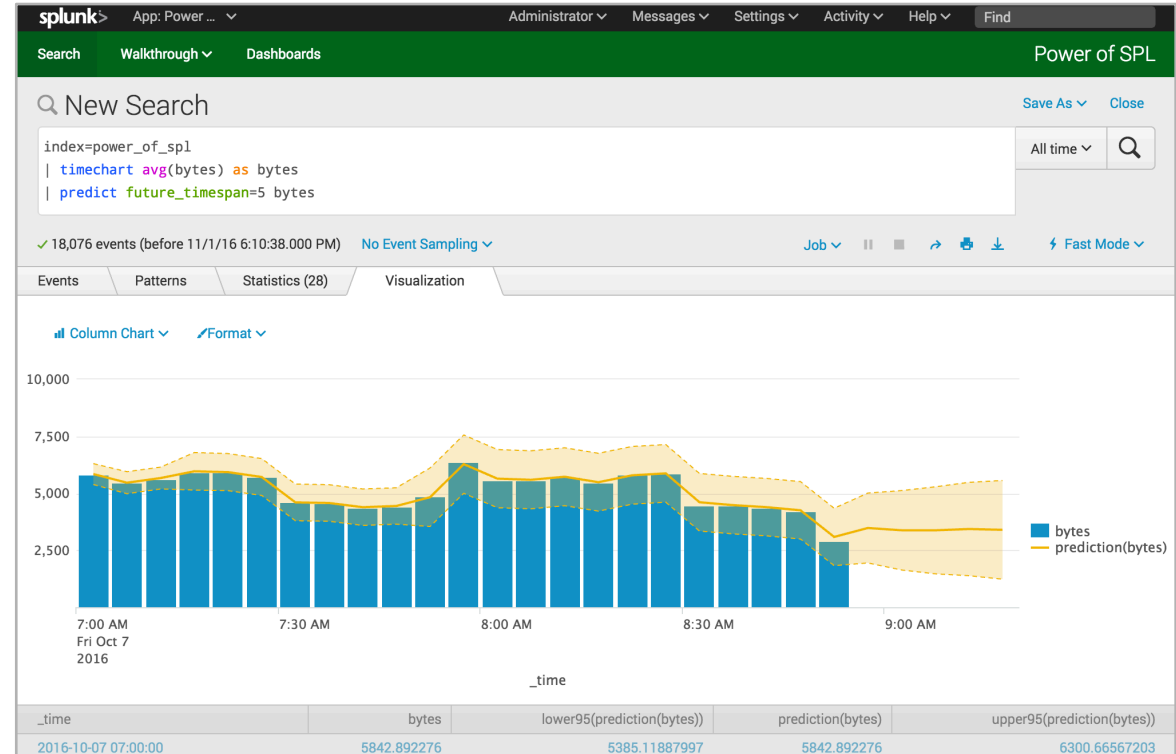
```
index=power_of_spl
| timechart avg(bytes)
```

### ▶ Add a trendline

```
index=power_of_spl
| timechart avg(bytes) as bytes
| trendline sma5(bytes)
```

### ▶ Add a prediction overlay

```
index=power_of_spl
| timechart avg(bytes) as bytes
| predict future_timespan=5 bytes
```



# Streamstats – Cumulative/Running Totals Statistics

## Examples

### ► Cumulative/Running Totals

**index=power\_of\_spl**

**| reverse**

**| streamstats sum(bytes) AS sum\_bytes**

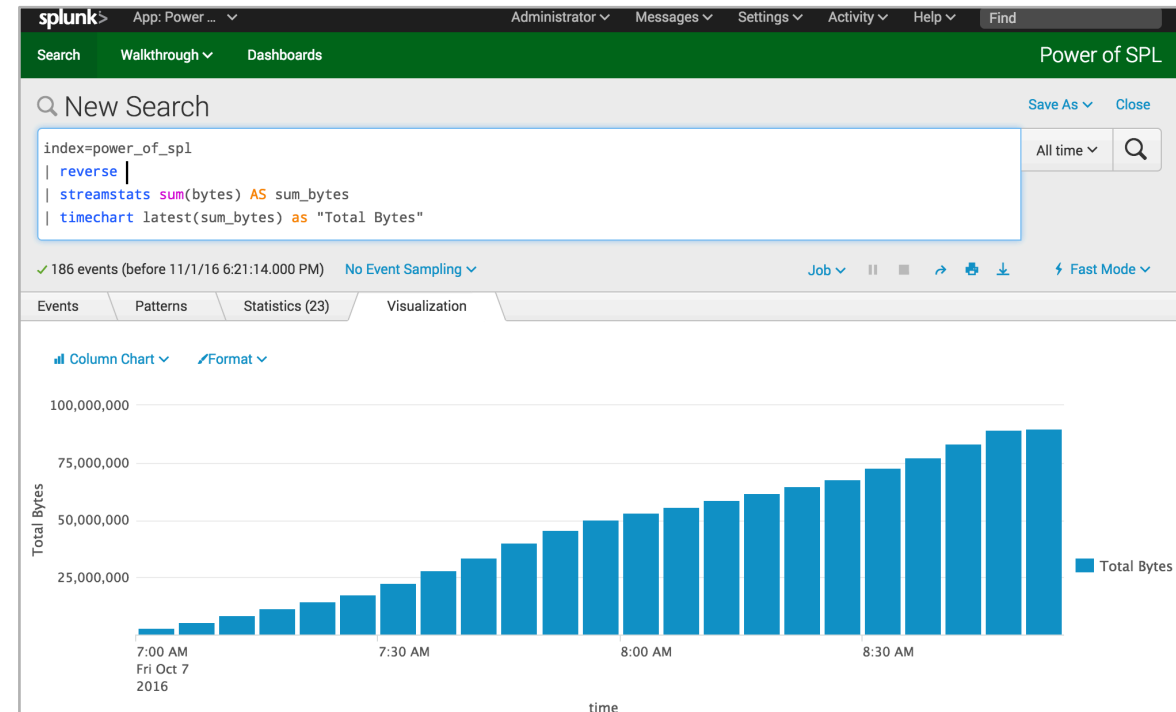
**| timechart latest(sum\_bytes) as "Total Bytes"**

### ► Summary Statistics

**index=power\_of\_spl**

**| eventstats avg(bytes) AS overall\_avg\_bytes**

**| stats avg(bytes) as clientip\_avg\_bytes by  
clientip overall\_avg\_bytes**



# Streamstats – Cumulative/Running Totals Statistics

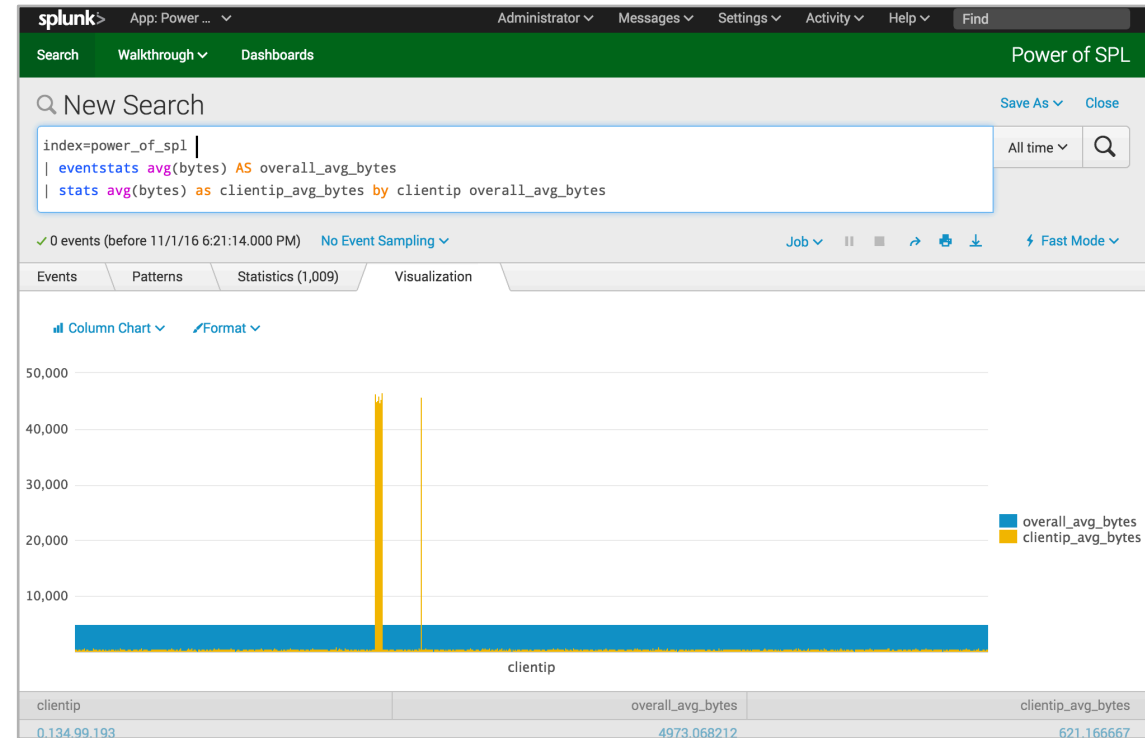
## Examples

### ► Cumulative/Running Totals

```
index=power_of_spl
| reverse
| streamstats sum(bytes) AS sum_bytes
| timechart latest(sum_bytes) as "Total Bytes"
```

### ► Summary Statistics

```
index=power_of_spl
| eventstats avg(bytes) AS overall_avg_bytes
| stats avg(bytes) as clientip_avg_bytes by clientip overall_avg_bytes
```



# Stats/Timechart – But Wait, There’s More!

## Splunk Search Quick Reference Guide

Common Stats Functions	
Common statistical functions used with the chart, stats, and timechart commands. Field names can be wildcarded, so avg(*delay) might calculate the average of the delay and xdelay fields.	
<b>avg(X)</b>	Returns the average of the values of field X.
<b>count(X)</b>	Returns the number of occurrences of the field X. To indicate a specific field value to match, format X as eval(field="value").
<b>dc(X)</b>	Returns the count of distinct values of the field X.
<b>earliest(X)</b>	Returns the chronologically earliest seen value of X.
<b>latest(X)</b>	Returns the chronologically latest seen value of X.
<b>max(X)</b>	Returns the maximum value of the field X. If the values of X are non-numeric, the max is found from alphabetical ordering.
<b>median(X)</b>	Returns the middle-most value of the field X.
<b>min(X)</b>	Returns the minimum value of the field X. If the values of X are non-numeric, the min is found from alphabetical ordering.
<b>mode(X)</b>	Returns the most frequent value of the field X.
<b>perc&lt;X&gt;(Y)</b>	Returns the X-th percentile value of the field Y. For example, perc5(total) returns the 5th percentile value of a field "total".
<b>range(X)</b>	Returns the difference between the max and min values of the field X.
<b>stdev(X)</b>	Returns the sample standard deviation of the field X.
<b>stdevp(X)</b>	Returns the population standard deviation of the field X.
<b>sum(X)</b>	Returns the sum of the values of the field X.
<b>sumsq(X)</b>	Returns the sum of the squares of the values of the field X.
<b>values(X)</b>	Returns the list of all distinct values of the field X as a multi-value entry. The order of the values is alphabetical.
<b>var(X)</b>	Returns the sample variance of the field X.



# Converging Data Sources

Index Untapped Data: Any Source, Type, Volume



Ask Any Question

Application Delivery

IT Operations

Security, Compliance and Fraud

Business Analytics

Industrial Data and the Internet of Things



# Lookup – Converging Data Sources

## Examples

### ► Enrich data with lookups

```
index=power_of_spl status!=200
| lookup customer_info uid
| stats count by customer_value
```

### ► Search Inception!

```
index=power_of_spl
[ search index=power_of_spl | stats sum(bytes)
as total_bytes by clientip
| sort - total_bytes | head 1 | return clientip ]
| stats count by clientip status uri | sort - count
```

### ► Append multiple searches

```
index=power_of_spl
| timechart span=15s avg(bytes) as avg_bytes
| appendcols [ search index=power_of_spl
| stats stdev(bytes) as stdev_bytes ] | eval 2stdv_upper = avg_bytes +
stdev_bytes*2 | filldown 2stdv_upper | eval 2stdv_lower = avg_bytes -
stdev_bytes*2 | filldown 2stdv_lower
| eval 2stdv_lower = if('2stdv_lower' <0,0,'2stdv_lower') | fields -
stdev_bytes
```

Enrich Data Through Lookups (Open me in search and remove stats command to show fields added!)

```
index=power_of_spl status!=200
| lookup customer_info uid
| stats count by customer_value
```

customer_value	count
high	143
low	2562
med	174

Lookup Table (.csv OR database)						Raw Data w/ "uid"	
uid	city	state	customer_value	customer_segment	er	i	Event
41b30a94-70ef-4c43-b6a6-04fb71a1ce9	Portland	OR	low	C3	sf	>	213.93.208.187 - - [07/Oct/2016 08:50:00:329932] "GET /product.screen?product_id=BW-3&SESSIONID=SD25CL9FF7ADFF7 HTTP 1.1" 404 246 "http://shop.acme.com/category.screen?uid=5f995bbf-25b6-45f4-950e-8c80f094577d&category=Misc" "mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3" 3659
4934d9b7-546f-437d-a272-4ac2a8c00f62	New Orleans	LA	low	C3	cs	>	63.28.124.107 - - [07/Oct/2016 08:49:46:006891] "GET /cart.do?action=view&item_id=MCB-5&product_id=MCB-5&SESSIONID=SD10SL4FF3ADFF5 HTTP 1.1" 404 941 "http://shop.acme.com/category.screen?uid=62c3f72a-2dcc-4b98-92c8-4ab329a93697&category=Misc" "mozilla/5.0 (Linux; U; Android 3.2.1; en-us; Xoom Build/HTK75D) AppleWebKit/534.13 (KHTML, like Gecko) Version/4.0 Safari/534.13" 3936
8f20e339-f80a-4e9a-af74-1e0d9a808204	Paterson	NJ	low	C3	rv	>	197.56.99.63 - - [07/Oct/2016 08:49:39:004604] "GET /category.screen?uid=e792db7d-5fe2-4080-bae4-3e0a07601028&category=Misc&SESSIONID=SD55L3FF3ADFF4 HTTP 1.1" 503 713 "http://shop.acme.com/cart.do?action=view&item_id=MCB-6&product_id=MCB-6" "mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) 1Password/3.6.1/361009 (like Mobile/8C148 Safari/6533.18.5)" 2886
43c43e89-12ff-4ed7-a375-3d488684714b	Rockville	MD	low	C3	ar	>	240.1.18.177 - - [07/Oct/2016 08:49:24:108329] "POST /category.screen?uid=105f1740-157-0ad-0-57-361601028&category=Misc&SESSIONID=SD55L3FF3ADFF4 HTTP 1.1" 503 713 "http://shop.acme.com/cart.do?action=view&item_id=MCB-6&product_id=MCB-6" "mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) 1Password/3.6.1/361009 (like Mobile/8C148 Safari/6533.18.5)" 2886
84157348-f3d3-4241-8f78-803a362e0739	Roanoke	VA	med	C2	kj	>	240.1.18.177 - - [07/Oct/2016 08:49:24:108329] "POST /category.screen?uid=105f1740-157-0ad-0-57-361601028&category=Misc&SESSIONID=SD55L3FF3ADFF4 HTTP 1.1" 503 713 "http://shop.acme.com/cart.do?action=view&item_id=MCB-6&product_id=MCB-6" "mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) 1Password/3.6.1/361009 (like Mobile/8C148 Safari/6533.18.5)" 2886

# Converging Data Sources

## Examples

### ▶ Enrich data with lookups

```
index=power_of_spl status!=200
| lookup customer_info uid
| stats count by customer_value
```

### ▶ Search Inception!

```
index=power_of_spl
[ search index=power_of_spl | stats sum(bytes)
as total_bytes by clientip
| sort - total_bytes | head 1 | return clientip ]
| stats count by clientip status uri | sort - count
```

### ▶ Append multiple searches

```
index=power_of_spl
| timechart span=15s avg(bytes) as avg_bytes
| appendcols [ search index=power_of_spl
| stats stdev(bytes) as stdev_bytes ] | eval 2stdv_upper = avg_bytes +
stdev_bytes*2 | filldown 2stdv_upper | eval 2stdv_lower = avg_bytes -
stdev_bytes*2 | filldown 2stdv_lower
| eval 2stdv_lower = if('2stdv_lower' <0,0,'2stdv_lower') | fields -
stdev_bytes
```

The screenshot shows the Splunk search interface. The search query is:

```
index=power_of_spl
[ search index=power_of_spl
| stats sum(bytes) as total_bytes by clientip
| sort - total_bytes
| head 1
| return clientip ]
| stats count by clientip status uri
| sort - count
```

The results table shows the following data:

clientip	status	uri	count
183.97.189.111	504	/search.php?=1	56
183.97.189.111	503	/search.php? (SELECT	26
183.97.189.111	503	/search.php?=1	19
183.97.189.111	504	/search.php?uid=86b88499-797b-47d9-90f8-b4081028dfdc&JSESSIONID=SD3SL1FF7ADFF9	2
183.97.189.111	503	/search.php?uid=0188e7df-3e1c-4ac4-a215-86bb0a18fdc8&JSESSIONID=SD3SL1FF7ADFF9	1
183.97.189.111	503	/search.php?uid=031c0ac7-bdf4-4dbc-978d-3a5351018a2f&JSESSIONID=SD3SL1FF7ADFF9	1
183.97.189.111	503	/search.php?uid=048708b6-3fe3-470d-82e1-f1fa98afa636&JSESSIONID=SD3SL1FF7ADFF9	1



# appendcols - Converging Data Sources

## Examples

### ▶ Enrich data with lookups

```
index=power_of_spl status!=200
| lookup customer_info uid
| stats count by customer_value
```

### ▶ Search Inception!

```
index=power_of_spl
[ search index=power_of_spl | stats sum(bytes)
as total_bytes by clientip
| sort - total_bytes | head 1 | return clientip ]
| stats count by clientip status uri | sort - count
```

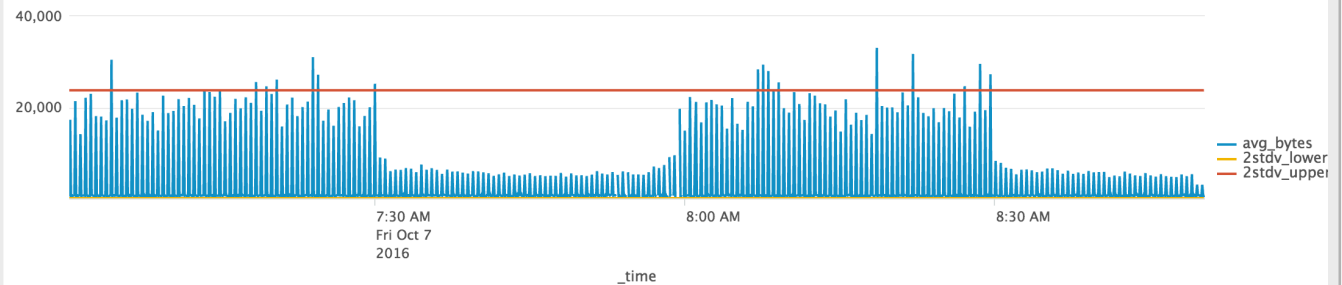
### ▶ Append multiple searches

```
index=power_of_spl
| timechart span=15s avg(bytes) as avg_bytes
| appendcols [ search index=power_of_spl
| stats stdev(bytes) as stdev_bytes ] | eval 2stdv_upper = avg_bytes +
stdev_bytes*2 | filldown 2stdv_upper | eval 2stdv_lower = avg_bytes
- stdev_bytes*2 | filldown 2stdv_lower
| eval 2stdv_lower = if('2stdv_lower' < 0, '2stdv_lower') | fields -
stdev_bytes
```

#### Append Multiple Searches to Create Custom Thresholds

(Note we could use eventstats for this example, but if you wanted to substitute different time ranges to calculate the threshold appendcols could be used like so)

```
index=power_of_spl
| timechart span=15s avg(bytes) as avg_bytes
| appendcols
[ search index=power_of_spl
| stats stdev(bytes) as stdev_bytes ]
| eval 2stdv_upper = avg_bytes + stdev_bytes*2 | filldown 2stdv_upper
| eval 2stdv_lower = avg_bytes - stdev_bytes*2 | filldown 2stdv_lower
| eval 2stdv_lower = if('2stdv_lower' < 0, '2stdv_lower')
| fields - stdev_bytes
```



# SPL Examples And Recipes

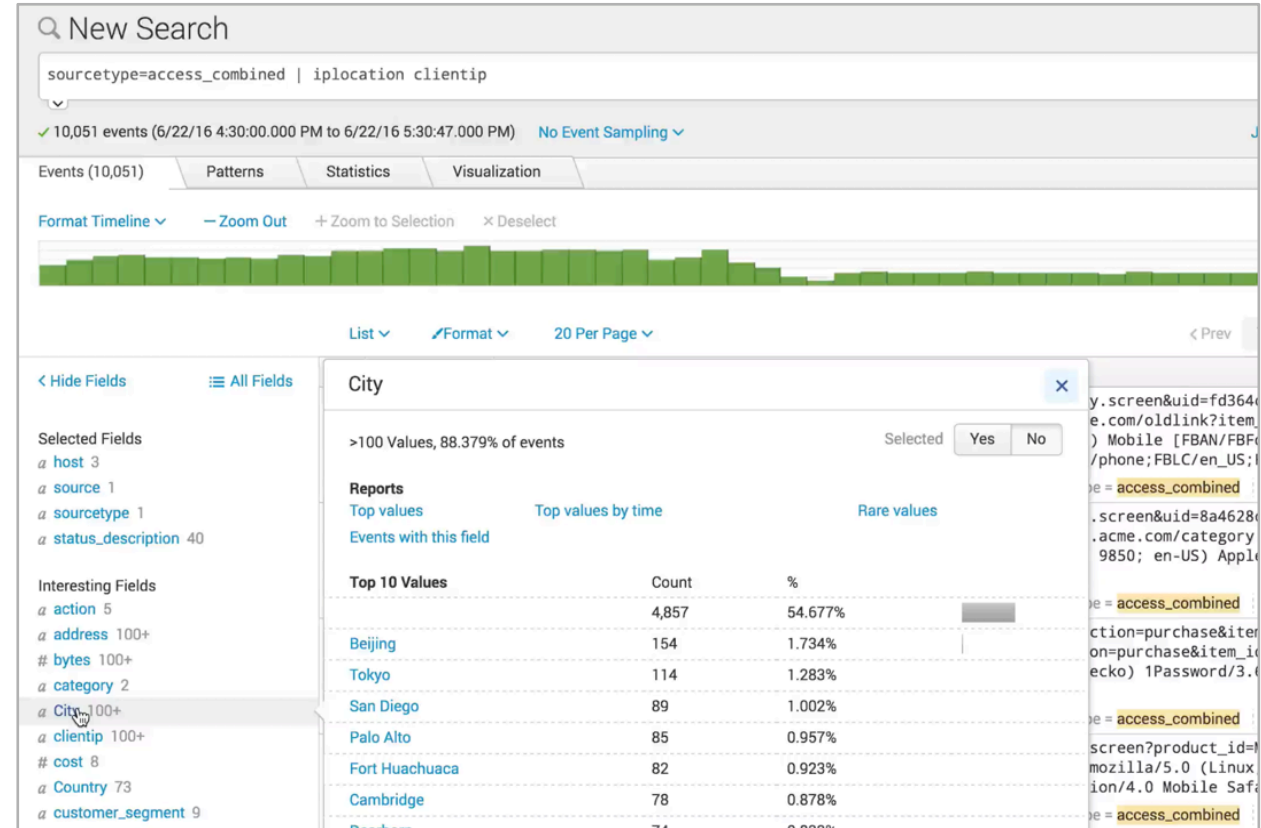
- ▶ Find the needle in the haystack
- ▶ Charting statistics and predicting values
- ▶ Enriching and converging data sources
- ▶ **Map geographic data in real time**
- ▶ Identifying anomalies
- ▶ Transactions
- ▶ Data exploration & finding relationships between fields
- ▶ Custom commands

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=CP-01"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=CP-01"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=CP-01"
```

# iplocation – Geographic Data

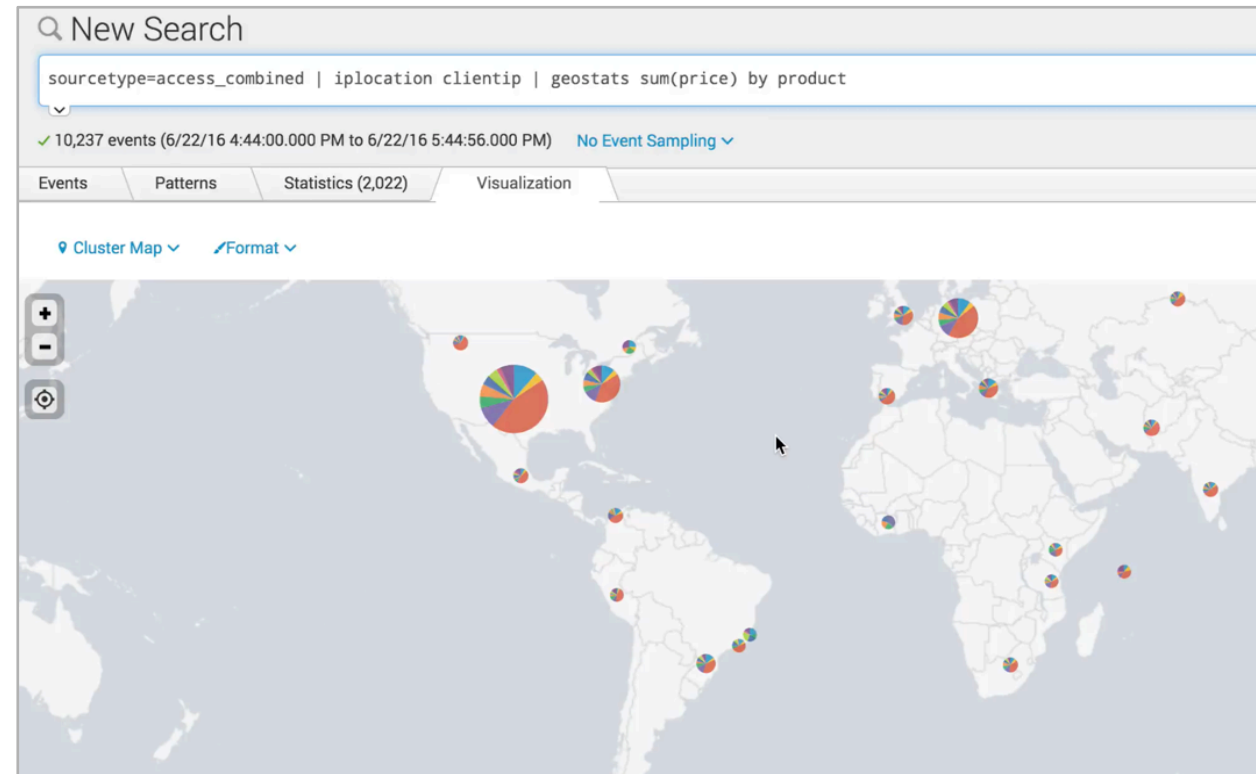
## Examples

- ▶ **Assign Lat/Lon to IP addresses**  
... | iplocation clientip
- ▶ **Visualize statistics geographically**  
... | geostats sum(price) by product
- ▶ **Use custom choropleths**  
... | geom <featureCollection> <featureId>
- ▶ **Track object movements**  
... | table \_time latitude longitude vehicleId



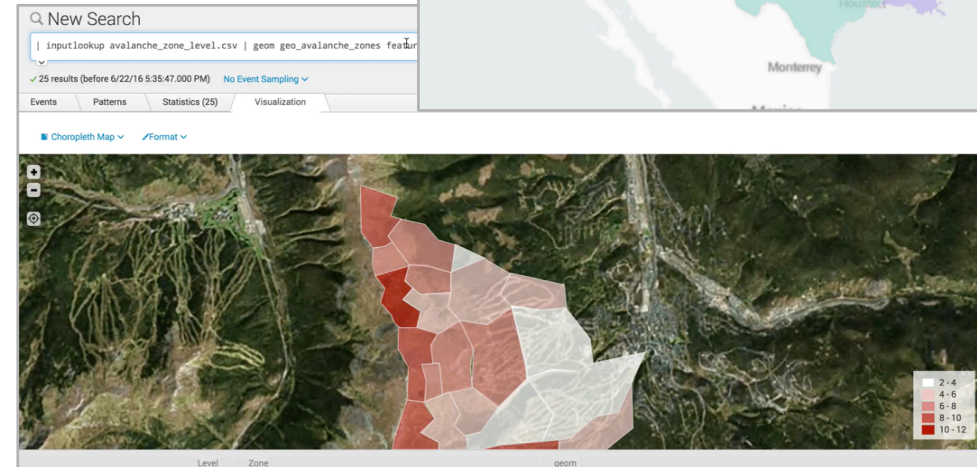
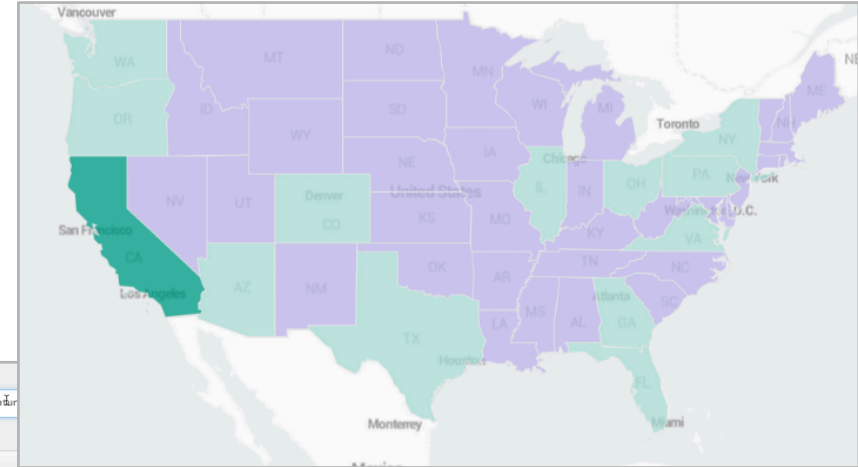
# geostats – Geographic Data Examples

- ▶ Assign Lat/Lon to IP addresses  
... | iplocation clientip
- ▶ Visualize statistics geographically  
... | geostats sum(price) by product
- ▶ Use custom choropleths  
... | geom <featureCollection> <featureId>
- ▶ Track object movements  
... | table \_time latitude longitude vehicleId



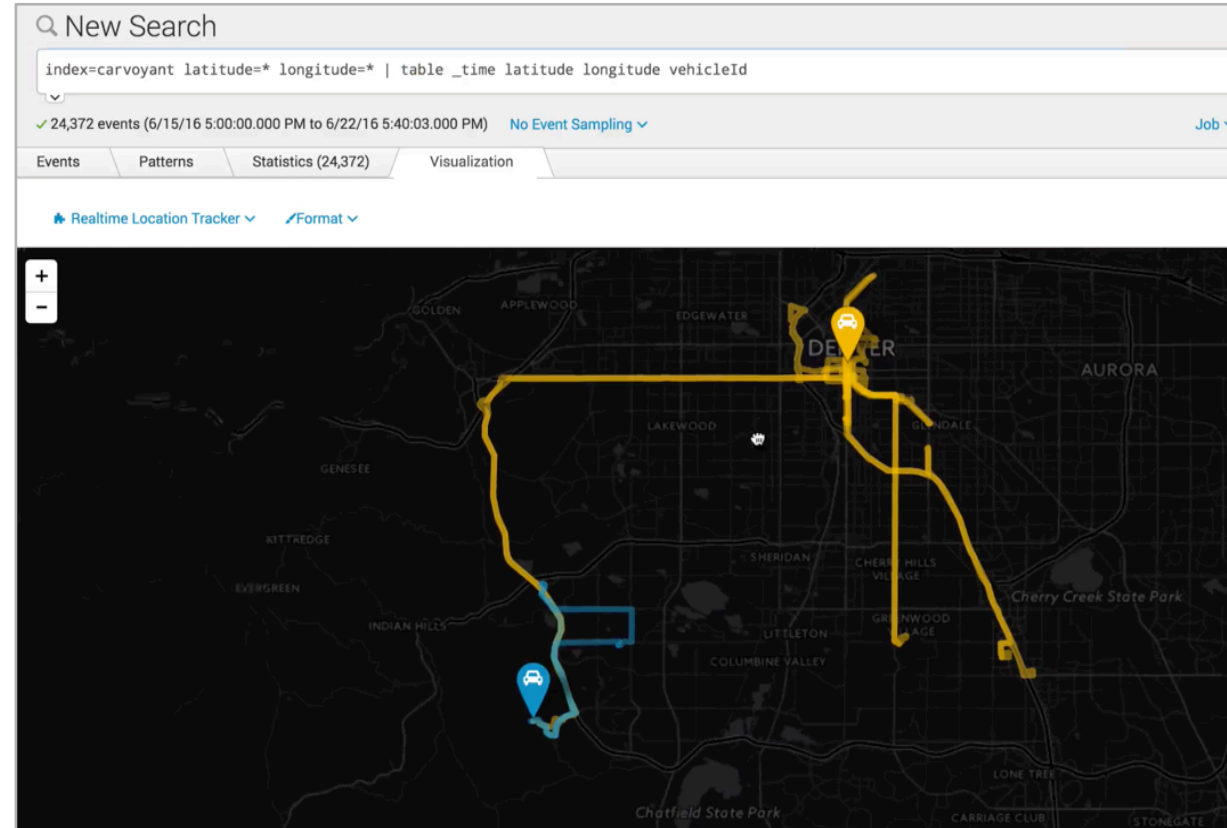
# geom – Geographic Data Examples

- ▶ Assign Lat/Lon to IP addresses  
... | iplocation clientip
- ▶ Visualize statistics geographically  
... | geostats sum(price) by product
- ▶ Use custom choropleths  
... | geom <featureCollection> <featureId>
- ▶ Track object movements  
... | table \_time latitude longitude vehicleId



# table – Geographic Data Examples

- ▶ Assign Lat/Lon to IP addresses  
... | iplocation clientip
- ▶ Visualize statistics geographically  
... | geostats sum(price) by product
- ▶ Use custom choropleths  
... | geom <featureCollection> <featureId>
- ▶ Track object movements  
... | table \_time latitude longitude vehicleId



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "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-18&product_id=AV-CB-01&SESSIONID=SD5L9FF1ADFF3"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01"
10.0.0.0 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01"

```

# SPL Examples And Recipes

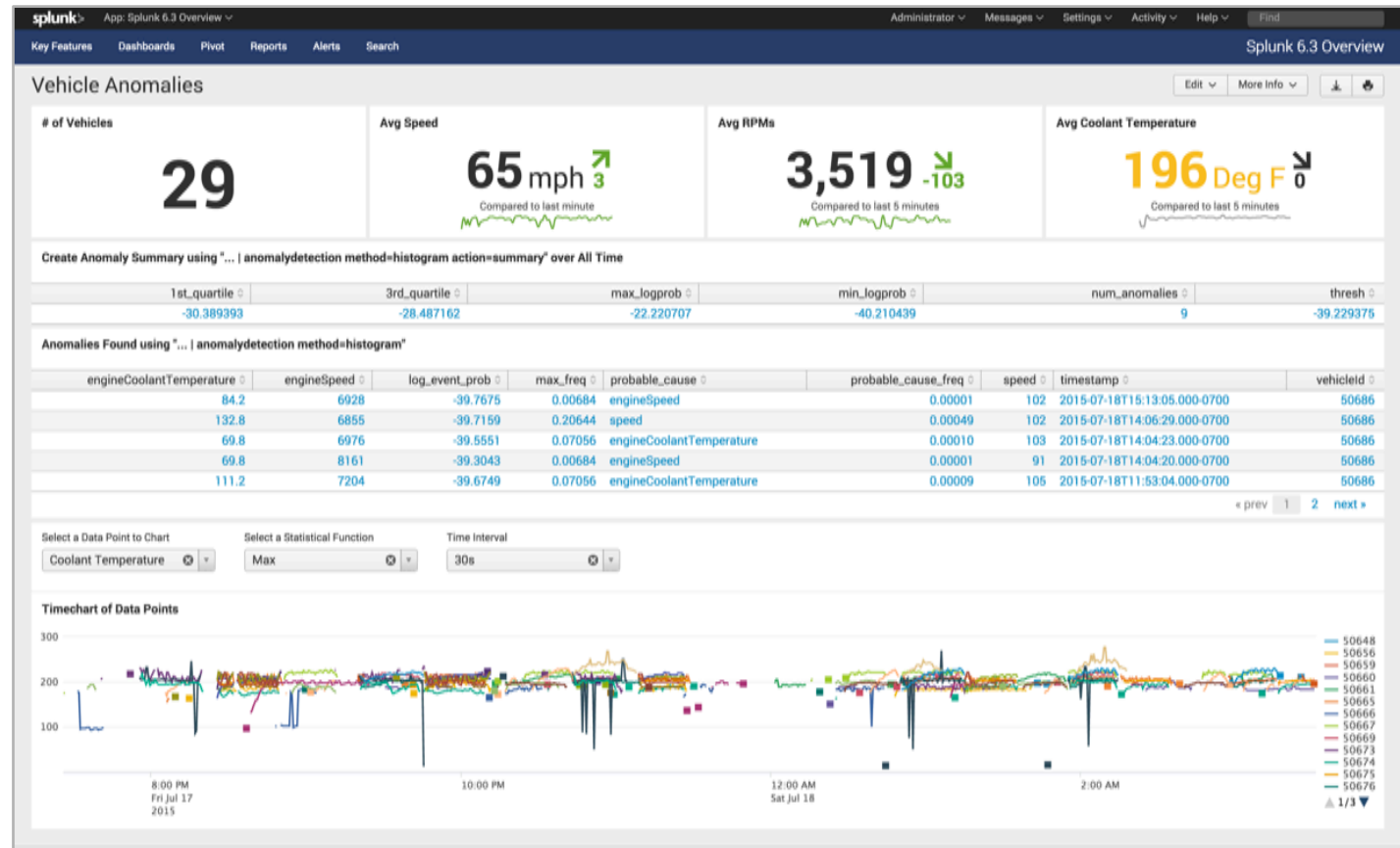
- ▶ Find the needle in the haystack
- ▶ Charting statistics and predicting values
- ▶ Enriching and converging data sources
- ▶ Map geographic data in real time
- ▶ **Identifying anomalies**
- ▶ Transactions
- ▶ Data exploration & finding relationships between fields
- ▶ Custom commands

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-01"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category\_id=GIFTS"  
ows NT 5.1; SV1: - - [07/Jan 18:10:56:156] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product\_id=KQ-CW-01"  
://buttercup-shopping.com/oldlink?item\_id=EST-268&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1"  
:/buttercup-shopping.com/oldlink?item\_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18"  
/buttercup-shopping.com/oldlink?item\_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/category.screen?category\_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18"

# Anomaly Detection – Find anomalies in your data

## Examples

- ▶ Find anomalies  
| inputlookup car\_data.csv | anomalydetection
- ▶ Summarize anomalies  
| inputlookup car\_data.csv | anomalydetection action=summary
- ▶ Use IQR and remove outliers  
| inputlookup car\_data.csv | anomalydetection method=iqr action=remove







# Transaction – Group Related Events Spanning Time

## Examples

- ▶ **Group by session ID**  
sourcetype=access\*  
| transaction JSESSIONID
- ▶ **Calculate session durations**  
sourcetype=access\*  
| transaction JSESSIONID  
| stats min(duration) max(duration)  
avg(duration)
- ▶ **Stats is better**  
sourcetype=access\*  
| stats min(\_time) AS earliest max(\_time)  
AS latest by JSESSIONID  
| eval duration=latest-earliest  
| stats min(duration) max(duration)  
avg(duration)

New Search

sourcetype=access\*  
| transaction JSESSIONID

247 events (7/1/14 1:15:00.000 PM to 7/1/14 2:15:08.000 PM)

Events (247) | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect | 1 minute per column

i	Time	Event
>	7/1/14 1:27:34.844 PM	10.2.1.33 128.241.220.82 - - [01/Jul/2014 13:27:34:844341] "GET /cart.do?action=purchase&itemId=EST-15&product_id=MC-SANDISK-M 10.2.1.34 62.216.64.19 - - [01/Jul/2014 13:29:41:906225] "GET /cart.do?action=changequantity&itemId=EST-16&product_id=BT-SP-JA 10.2.1.33 12.130.60.4 - - [01/Jul/2014 13:31:59:986518] "GET /cart.do?action=purchase&itemId=EST-16&product_id=CH-APPLE-SWL&JS 10.2.1.35 90.205.111.169 - - [01/Jul/2014 13:33:36:049273] "GET /cart.do?action=remove&itemId=EST-12&product_id=DP-HTCREZOUND& 10.2.1.34 62.216.64.19 - - [01/Jul/2014 13:39:29:250254] "GET /cart.do?action=view&itemId=EST-26&product_id=MC-SANDISK-MICROSD Show all 20 lines
		JSESSIONID = SD10SL5FF8ADFF1   action = addtocart action = changequantity action = purchase action = remove action = view   clientip = 1.16.0.0 clientip = status = 100 status = 200 status = 404 status = 503   status_description = Conflict status_description = Continue status_description = Not Found sta
>	7/1/14 1:27:21.837 PM	10.2.1.33 141.146.8.66 - - [01/Jul/2014 13:27:21:837389] "POST /product.screen?product_id=AC-ASSTCHARMS&JSESSIONID=SD6SL5FF2AD 10.2.1.33 12.130.60.5 - - [01/Jul/2014 13:32:05:991006] "POST /product.screen?product_id=CH-APPLE-10WL&JSESSIONID=SD6SL5FF2ADF 10.2.1.34 10.2.1.44 - - [01/Jul/2014 13:36:02:119] "POST /product.screen?product_id=CC-T10-RIM-BBERRYPLAY&JSESSIONID=SD6SL5FF2 10.2.1.34 130.253.37.97 - - [01/Jul/2014 13:40:47:290948] "POST /product.screen?product_id=AC-SAMS-NETEXTEND&JSESSIONID=SD6SL5 10.2.1.35 131.178.233.243 - - [01/Jul/2014 13:41:19:308722] "POST /product.screen?product_id=DP-NOKLUMIA&JSESSIONID=SD6SL5FF2A Show all 14 lines
		JSESSIONID = SD6SL5FF2ADFF3   clientip = 10.2.1.44 clientip = 12.130.60.4 clientip = 12.130.60.5 clientip = 125.17.14.100 clientip = 128.241.220.82 clientip = 1 status_description = Bad Request status_description = Continue status_description = Not Found status_description = OK status_description = Service Unavailable

# Transaction – Group Related Events Spanning Time

## Examples

- ▶ Group by session ID  
sourcetype=access\*  
| transaction JSESSIONID
- ▶ Calculate session durations  
sourcetype=access\*  
| transaction JSESSIONID  
| stats min(duration) max(duration)  
avg(duration)
- ▶ Stats is better  
sourcetype=access\*  
| stats min(\_time) AS earliest max(\_time)  
AS latest by JSESSIONID  
| eval duration=latest-earliest  
| stats min(duration) max(duration)  
avg(duration)

New Search

Save As Close

sourcetype=access\*  
| transaction JSESSIONID  
| stats min(duration) max(duration) avg(duration)

Last 60 minutes

247 events (7/1/14 2:10:00.000 PM to 7/1/14 3:10:59.000 PM)

Job Visualization

20 Per Page Format Preview

min(duration)	max(duration)	avg(duration)
2661.620435	3645.120123	3413.271055

# Transaction – Group Related Events Spanning Time

## Examples

- ▶ Group by session ID  
sourcetype=access\*  
| transaction JSESSIONID
- ▶ Calculate session durations  
sourcetype=access\*  
| transaction JSESSIONID  
| stats min(duration) max(duration)  
avg(duration)
- ▶ Stats is better  
sourcetype=access\*  
| stats min(\_time) AS earliest max(\_time)  
AS latest by JSESSIONID  
| eval duration=latest-earliest  
| stats min(duration) max(duration)  
avg(duration)

New Search

Save As ▾ Close

sourcetype=access\*  
| stats min(\_time) AS earliest max(\_time) AS latest by JSESSIONID  
| eval duration=latest-earliest  
| stats min(duration) max(duration) avg(duration)

Last 60 minutes ▾ 🔍

✓ 10,078 events (7/1/14 3:54:00.000 PM to 7/1/14 4:54:17.000 PM) Job ▾ ⏸ ⏹ ↶ ↷ ⏴ ⏵ ⚙ Smart Mode ▾

Events Statistics (1) Visualization

20 Per Page ▾ Format ▾ Preview ▾

min(duration) ⌵	max(duration) ⌵	avg(duration) ⌵
2593.070572	3605.554687	3380.481692



# Data Exploration

| **analyzefields**

| **anomalies**

| **arules**

| **associate**

| **cluster**

| **contingency**

| **correlate**

| **fieldsummary**

# Cluster – Exploring Your Data

## Examples

### ► Find most/least common events

```
* | cluster showcount=t t=.1
| table _raw cluster_count
```

### ► Display Summary of Fields

```
sourcetype=access_combined
| fields – date* source* time*
| fieldsummary maxvals=5
```

### ► Show patterns of co-occurring fields

```
sourcetype=access_combined
| fields – date* source* time* | correlate
```

### ► View field relationships

```
sourcetype=access_combined
| contingency uri status
```

### ► Find predictors of fields

```
sourcetype=access_combined
| analyzefields classfield=status
```

Q New Search Save As ▾ Close

\* | cluster showcount=t t=.1 | table \_raw cluster\_count | sort - cluster\_count Last 60 minutes ▾ Q

✓ 51 events (4/9/15 9:13:00.000 AM to 4/9/15 10:13:57.000 AM) Job ▾ || ▢ ↶ ⬇ 🗑 Smart Mode ▾

Events	Patterns	Statistics (51)	Visualization
20 Per Page ▾	Format ▾	Preview ▾	< Prev 1 2 3 Next >
_raw ↕			cluster_count ^
09-Apr-2015 09:40:42:088731 [CRITICAL] /opt/mysql/bin/mysqld: Disk is full writing '/mysqllog/binlog/localhost-3306-bin.000020' (Errcode: 28). Waiting for someone to free space... Retry in 60 secs			2
SPL_Prod_Net_Range,192.168.10.84,192.168.10.84,nCircle IP360 VnE Manager,923,SSL Server Supports Weak MAC Algorithms for TLSv1,2701,04/09/2015 09:26:33 AM,0			25
SPL_Prod_Net_Range,192.168.10.4,192.168.10.4,Cisco IOS 12.0,30621,Cisco IOS Software Multiple Features Crafted UDP Packet Denial of Service Vulnerability,161,04/09/2015 09:26:33 AM,1261			35
04/09/2015 09:33:55 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Type=Information ComputerName=file_1 TaskCategory=Logon OpCode=Info RecordNumber=462368778 Keywords=Audit Failure Message=An account failed to log on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: Logon Type: 3 Account For Which Logon Failed: Security ID: acme\adm_jerry\ Account Name: adm_jerry\ Account Domain: acme Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xc000006d Sub Status: 0xc000006a Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: yqerexyno_wkstn_348 Source Network Address: 10.152.11.14 Source Port: 53775 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.			70
04-09-2015 10:13:50 severity=MEDIUM search_name='Identity - Activity from Expired User Identity - Rule','orig_raw='netapp_appserver-01 auth:security:info: su: [ID 366847 auth:info] 'su dmsys' succeeded for root on /dev/???' user=dmsys info='Activity from Expired User Identity' search_name='Identity - Activity from Expired User Identity - Rule'			88
04-09-2015 10:11:06 info='Key Logger' severity=HIGH search_name='Endpoint - Outbreak Observed - Rule' signature='Key logger'			92

# fieldsummary – Exploring Your Data

## Examples

- Find most/least common events

```
* | cluster showcount=t t=.1
| table _raw cluster_count
```

- Display Summary of Fields

```
sourcetype=access_combined
| fields – date* source* time*
| fieldsummary maxvals=5
```

- Show patterns of co-occurring fields

```
sourcetype=access_combined
| fields – date* source* time* | correlate
```

- View field relationships

```
sourcetype=access_combined
```

```
| contingency uri status
```

- Find predictors of fields

```
sourcetype=access_combined
```

```
| analyzefields classfield=status
```

Q New Search Save As ▾ Close

\* sourcetype=access\_combined | fields - date\* source\* time\* | fieldsummary maxvals=5 Date time range ▾ Q

✓ 12,688 events (11/4/15 4:00:43.000 PM to 11/4/15 5:00:43.000 PM) Job ▾ || ↶ ↷ ↵ ↶ ↷ Smart Mode ▾

Events Patterns Statistics (75) Visualization

20 Per Page ▾ Format ▾ Preview ▾ < Prev 1 2 3 4 Next >

field	count	distinct_count	is_exact	max	mean	min	numeric_count	stdev	values
bytes	12688	25	0	59998	3990.820460	100	12688	12070.309129	[[{"value":"821","count":1247}, {"value":"566","count":1239}, {"value":"765","count":1193}, {"value":"505","count":1152}, {"value":"428","count":1137}]]
linecount	12688	2	1	2	1.778925	1	12688	0.414987	[[{"value":"2","count":9883}, {"value":"1","count":2805}]]
rack	12688	3	1	4	2.637216	1	12688	1.232783	[[{"value":"3","count":4514}, {"value":"1","count":4259}, {"value":"4","count":3915}]]
status	12688	25	0	505	403.843632	100	12688	135.400514	[[{"value":"503","count":7191}, {"value":"200","count":3634}, {"value":"404","count":954}, {"value":"504","count":500}, {"value":"410","count":19}]]
cost	9494	8	0	40.29	6.960321	0.70	9494	11.342524	[[{"value":"2.21","count":2810}, {"value":"0.70","count":976}, {"value":"3.71","count":964}, {"value":"6.20","count":958}, {"value":"1.03","count":956}]]
price	9494	7	0	97.50	22.329912	4.99	9494	25.614479	[[{"value":"12.70","count":2810}, {"value":"9.99","count":1920}, {"value":"4.99","count":976}, {"value":"25.70","count":958}, {"value":"15.21","count":949}]]
other	6748	25	0	11997	3223.880113	200	6748	3003.130581	[[{"value":"1125","count":7}, {"value":"2246","count":7}, {"value":"3344","count":7}, {"value":"3524","count":7}, {"value":"3527","count":7}]]
version	6748	1	1	1.1	1.100000	1.1	6748	0.000000	[[{"value":"1.1","count":6748}]]
JSESSIONID	12688	25	0				0		[[{"value":"SD8LS5FF10ADFF9","count":1245}, {"value":"SD3SL1FF7ADFF8","count":1242}, {"value":"SD1SL7FF2ADFF3","count":1189}, {"value":"SD10SL9FF10ADFF7","count":1149}, {"value":"SD5SL5FF4ADFF6","count":1144}]]
action	4500	5	0				0		[[{"value":"addtocart","count":955}, {"value":"view","count":937}, {"value":"purchase","count":881}, {"value":"remove","count":870}, {"value":"changequantity","count":857}]]
address	3936	25	0				0		[[{"value":"5 Northview Point","count":12}, {"value":"7930 Charing Cross Hill","count":12}, {"value":"50 Granby Street","count":11}, {"value":"7 Wayridge Drive","count":11}, {"value":"9 Fuller Circle","count":11}]]
app	0	0	1				0		[[{"value":"","count":0}]]
category	11630	2	1				0		[[{"value":"Misc","count":11537}, {"value":"category","count":93}]]
category_id	1236	1	1				0		[[{"value":"Misc","count":1236}]]
change_type	0	0	1				0		[[{"value":"","count":0}]]
clientip	12688	25	0				0		[[{"value":"175.45.177.111","count":117}, {"value":"175.45.177.13","count":113}, {"value":"175.45.177.15","count":113}, {"value":"175.45.177.189","count":112}, {"value":"175.45.177.7","count":107}]]
cookie	0	0	1				0		[[{"value":"","count":0}]]
customer_segment	3936	9	0				0		[[{"value":"C3","count":2045}, {"value":"B3","count":1082}, {"value":"A3","count":375}, {"value":"C2","count":155}, {"value":"C1","count":102}]]
customer_value	3936	3	1				0		[[{"value":"low","count":3502}, {"value":"med","count":262}, {"value":"high","count":172}]]



# Correlate – Exploring Your Data

## Examples

- Find most/least common events

```
* | cluster showcount=t t=.1
| table _raw cluster_count
```

- Display Summary of Fields

```
sourcetype=access_combined
| fields – date* source* time*
| fieldsummary maxvals=5
```

- Show patterns of co-occurring fields

```
sourcetype=access_combined
| fields – date* source* time* | correlate
```

- View field relationships

```
sourcetype=access_combined
| contingency uri status
```

- Find predictors of fields

```
sourcetype=access_combined
| analyzefields classfield=status
```

New Search

sourcetype=access\_combined | fields - date\* source\* time\*  
| correlate

10,490 events (4/8/15 5:56:00.000 PM to 4/8/15 6:56:46.000 PM)

Events Patterns Statistics (60) Visualization

20 Per Page Format Preview

RowField	JSESSIONID	action	address	bytes	category	category_id	clientip	cost	customer_segment	customer_value	customer_wallet
JSESSIONID	1.00	0.34	0.28	1.00	0.76	0.10	1.00	0.76	0.28	0.28	0.28
action	0.34	1.00	0.17	0.34	0.45	0.00	0.34	0.45	0.17	0.17	0.17
address	0.28	0.17	1.00	0.28	0.16	0.00	0.28	0.16	1.00	1.00	1.00
bytes	1.00	0.34	0.28	1.00	0.76	0.10	1.00	0.76	0.28	0.28	0.28
category	0.76	0.45	0.16	0.76	1.00	0.00	0.76	1.00	0.16	0.16	0.16
category_id	0.10	0.00	0.00	0.10	0.00	1.00	0.10	0.00	0.00	0.00	0.00
clientip	1.00	0.34	0.28	1.00	0.76	0.10	1.00	0.76	0.28	0.28	0.28
cost	0.76	0.45	0.16	0.76	1.00	0.00	0.76	1.00	0.16	0.16	0.16
customer_segment	0.28	0.17	1.00	0.28	0.16	0.00	0.28	0.16	1.00	1.00	1.00
customer_value	0.28	0.17	1.00	0.28	0.16	0.00	0.28	0.16	1.00	1.00	1.00
customer_wallet	0.28	0.17	1.00	0.28	0.16	0.00	0.28	0.16	1.00	1.00	1.00
description	0.76	0.45	0.16	0.76	1.00	0.00	0.76	1.00	0.16	0.16	0.16
device	0.59	0.54	0.30	0.59	0.63	0.00	0.59	0.63	0.30	0.30	0.30
email	0.28	0.17	1.00	0.28	0.16	0.00	0.28	0.16	1.00	1.00	1.00

# Contingency – Exploring Your Data

## Examples

- ▶ Find most/least common events  
\* | cluster showcount=t t=.1  
| table \_raw cluster\_count
- ▶ Display Summary of Fields  
sourcetype=access\_combined  
| fields – date\* source\* time\*  
| fieldsummary maxvals=5
- ▶ Show patterns of co-occurring fields  
sourcetype=access\_combined  
| fields – date\* source\* time\* | correlate
- ▶ View field relationships  
sourcetype=access\_combined  
| contingency uri status
- ▶ Find predictors of fields  
sourcetype=access\_combined  
| analyzefields classfield=status

Q New Search Save

sourcetype=access\_combined | contingency uri status Last 60 min

✓ 10,100 events (4/8/15 5:47:00.000 PM to 4/8/15 6:47:14.000 PM) Job ▾ || ■ ↶ ↷ ⬇ ⬆ ⬇

Events Patterns Statistics (1,001) Visualization

20 Per Page ▾ Format ▾ Preview ▾ < Prev 1 2 3 4 5 6 7 8

uri	503	200	404	504	415	100	303	405	401	201	411	409	403	206
/search.php?=1	119	0	0	238	0	0	0	0	0	0	0	0	0	0
/search.php? (SELECT	119	0	0	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=13ecd676-1aac-489c-9273-64f05beaded3&category=Misc&JSESSIONID=SD7SL7FF6ADFF5	0	4	3	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=aa310182-8593-4092-8587-5508a01f3901&category=Misc&JSESSIONID=SD2SBL2FF1ADFF4	0	5	1	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=efd2eb40-2ef3-418f-9173-6ce44112c842&category=Misc&JSESSIONID=SD1SBL2FF7ADFF8	0	5	0	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=c2ee77ba-f435-470e-9d5e-bfd5862000&category=Misc&JSESSIONID=SD9SL7FF2ADFF9	0	2	3	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=a222c3c7-4803-44fd-a6c9-00f795f1462a&category=Misc&JSESSIONID=SD7SL5FF9ADFF3	0	1	4	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=a1395aac-e835-4f42-89ae-a659b89919c7&category=Misc&JSESSIONID=SD1SBL1FF6ADFF2	0	5	0	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=7a47ef03-64ac-40db-8f9b-c549698d30b9&category=Misc&JSESSIONID=SD5SBL1FF1ADFF8	0	4	0	0	0	0	0	0	0	0	0	0	0	0
/category.screen&uid=10c1fd9c-d2a3-48da-9fb1-29f59d52bd3d&category=Misc&JSESSIONID=SD1SCL1FF10ADFF6	0	5	0	0	0	0	0	0	0	0	0	0	0	0

# analyzefields – Exploring Your Data

## Examples

- ▶ Find most/least common events
  - \* | cluster showcount=t t=.1
  - | table \_raw cluster\_count
- ▶ Display Summary of Fields
  - sourcetype=access\_combined
  - | fields – date\* source\* time\*
  - | fieldsummary maxvals=5
- ▶ Show patterns of co-occurring fields
  - sourcetype=access\_combined
  - | fields – date\* source\* time\* | correlate
- ▶ View field relationships
  - sourcetype=access\_combined
  - | contingency uri status
- ▶ Find predictors of fields
  - sourcetype=access\_combined
  - | analyzefields classfield=status

New Search

sourcetype=access\_combined | associate uri status | Last 60 minutes

10,221 events (4/8/15 5:46:00.000 PM to 4/8/15 6:46:48.000 PM)

Events Patterns Statistics (3) Visualization

20 Per Page Format Preview

Reference_Key	Reference_Value	Target_Key	Support	Unconditional_Entropy	Conditional_Entropy	Entropy_Improvement	Top_Conditional_Value
status	404	uri	28.57%	11.278	9.441	1.836670	/category.screen&uid=a222c3c7-4803-44fd-a6c9-00f795f1462a&category=Misc&JSESSIONID=SD7SL5FF9ADFF3 (0.10% -> 0.55%)
status	503	uri	36.71%	11.278	8.051	3.227311	/search.php?i=1 (7.13% -> 12.90%)
status	504	uri	14.71%	11.278	3.403	7.875187	/search.php?i=1 (7.13% -> 64.36%)

# Machine Learning Toolkit And Showcase

## Examples

- ▶ Predict Numeric Fields
- ▶ Predict Categorical Fields
- ▶ Detect Numerical Outliers
- ▶ Detect Categorical Outliers
- ▶ Forecast Time Series
- ▶ Cluster Events

Welcome to the Machine Learning Toolkit and Showcase. Click on the dashboards or examples below to explore the kinds of analytics this app enables. Each dashboard includes both end-to-end examples with datasets we have provided, as well as the ability to apply the dashboard to your own data. You can inspect the dashboard panels and other code to see how each one works and then create custom dashboards to suit your needs. Everything you see was implemented on the Splunk platform using public interfaces, so you can bring similar functionality to your own organization's Splunk instance; there's nothing hidden up our sleeves.

### Predict Numeric Fields

Predict the value of a numeric field using a weighted combination of the values of other fields in that event. A common use of these predictions is to identify anomalies: predictions that differ significantly from the actual value may be considered anomalous. IT admins could predict the values of sensors that were malfunctioning, security analysts could predict how much data a user is likely to transfer and flag unusually high prediction errors, and business analysts could predict the likely spending habits of customers.

Algorithm: Linear Regression

Examples:

- Predict Median House Value
- Predict Baseball Runs
- Predict App Usage from Other Apps

### Predict Categorical Fields

Predict the value of a categorical field using the values of other fields in that event. A common use of these predictions is to identify anomalies: high-confidence predictions that turn out to be incorrect may be considered anomalous. IT admins could predict the correct values of missing configuration variables, security analysts could predict what actions a user is likely to perform and raise an alert when the user behaves unexpectedly, and business analysts could predict customer churn based on other factors.

Algorithm: Logistic Regression

Examples:

- Predict Telecom Customer Churn
- Predict Species of Iris from Physical Measurements
- Predict Incidence of Diabetes from Health Metrics

### Detect Numeric Outliers

Find values that are far from previous values. IT admins could look for machines with unusually high resource utilization; security analysts could look for employees transferring unusually large amounts of data; and business analysts could identify big spenders.

Algorithm: Distribution statistics

Examples:

- Detect Outliers in Server Response Time

### Detect Categorical Outliers

Find events that contain unusual combinations of values. IT admins could look for unusual machine configurations; security analysts could look for employees performing an atypical combination of activities; and business analysts could identify rare purchasing habits.

Algorithm: Probabilistic measures

Examples:

- Detect Outliers in Mortgage Contract Data
- Detect Outliers in Congressional Voting Records

# SPL Examples And Recipes

- ▶ Find the needle in the haystack
- ▶ Charting statistics and predicting values
- ▶ Enriching and converging data sources
- ▶ Map geographic data in real time
- ▶ Identifying anomalies
- ▶ Transactions
- ▶ Data exploration & finding relationships between fields
- ▶ **Custom commands**

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
0- - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
0- - [07/Jan 18:10:55:189] "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"

```

# Custom Commands

- ▶ What is a Custom Command?
  - “| **haversine** origin="47.62,-122.34" outputField=dist lat lon”
- ▶ Why do we use Custom Commands?
  - Run other/external algorithms on your Splunk data
  - Save time munging data (see Timewrap!)
  - Because you can!
- ▶ Create your own or download as Apps
  - [Haversine](#) (Distance between two GPS coords)
  - [Timewrap](#) (Enhanced Time overlay)
  - [Levenshtein](#) (Fuzzy string compare)
  - [Base64](#) (Encode/Decode)

# Custom Commands – Haversine

## Examples

### ► Download and install App

[Haversine](#)

### ► Read documentation then use in SPL!

```
sourcetype=access*
```

```
| iplocation clientip
```

```
| search City=A*
```

```
| haversine origin="47.62,-122.34" units=mi  
outputField=dist lat lon
```

```
| table clientip, City, dist, lat, lon
```

The screenshot shows the Splunkbase interface for the 'haversine' app. At the top, there are navigation links for 'CATEGORIES', 'TECHNOLOGIES', and 'FOR DEVELOPERS', along with a search bar. The app name 'haversine' is prominently displayed with a green 'DOWNLOAD' button. Below the app name, there are tabs for 'OVERVIEW' and 'DOCUMENTATION'. The 'OVERVIEW' tab is active, showing a description: 'Calculates the distance between two points represented via latitude and longitude. Augments each relevant event with the resultant distance, stored in a field named 'distance' or another field as specified. Latitude and longitude for input must be represented in decimal degree format, though separate input fields may be specified for each. Units are in kilometers by default, but optionally represented in miles.' To the right of the description, there are 6 ratings, a 'Rate this app' button, 398 downloads, and options to 'Subscribe' and 'Share this app'. Below the description, there is a 'VERSION: 2.0' dropdown menu. The 'RELEASE NOTES' section indicates a new release with bugfixes and documentation updates, dated March 20, 2015, and notes it is 'Platform Independent' and compatible with versions 6.2, 6.1, 6.0, and 5.0. At the bottom right, there is a 'COMMUNITY SUPPORTED' section with an 'Ask a Question' button and links to 'Questions on SplunkAnswers' and 'Flag as inappropriate'.

# Custom Commands – Haversine

## Examples

- ▶ Download and install App [Haversine](#)
- ▶ **Read documentation then use in SPL!**

**sourcetype=access\***

**| iplocation clientip**

**| search City=A\***

**| haversine origin="47.62,-122.34" units=mi  
outputField=dist lat lon**

**| table clientip, City, dist, lat, lon**

New Search Save As Close

sourcetype=access\*  
| iplocation clientip  
| search City=A\*  
| haversine origin="47.615,-122.336" units=mi outputField=dist lat lon  
| table clientip, City, dist, lat, lon

Last 60 minutes Q

✓ 68 events (4/8/15 4:33:00.000 PM to 4/8/15 5:33:27.000 PM) Job || → ↓ ↻ Smart Mode

Events Patterns Statistics (68) Visualization

20 Per Page Format Preview < Prev 1 2 3 4 Next >

clientip	City	dist	lat	lon
35.150.128.238	Ann Arbor	1903.9630892460589	42.27340	-83.71330
204.148.241.222	Ashburn	2296.60342464036	39.03350	-77.48380
68.136.248.200	Ashburn	2296.60342464036	39.03350	-77.48380
88.197.116.23	Athens	6164.047108275602	37.98330	23.73330
68.136.248.200	Ashburn	2296.60342464036	39.03350	-77.48380
97.75.108.67	Austin	1770.0203563672421	30.26720	-97.74310
35.189.121.104	Ann Arbor	1903.9630892460589	42.27340	-83.71330
63.17.3.219	Ashburn	2296.60342464036	39.03350	-77.48380
189.135.204.185	Alvaro Obregon Borough	2342.8992471298166	19.37330	-99.22500
68.136.248.200	Ashburn	2296.60342464036	39.03350	-77.48380



# For More Information

► Additional information can be found in:

- [Power of SPL App!](#)
- [Search Manual](#)
- [Blogs](#)
- [Answers](#)
- [Exploring Splunk](#)

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-5W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=K0-CW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0"  
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0"  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0"

# Join The Pony Poll



[ponypoll.com/](http://ponypoll.com/)\*\*\*

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.111 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.111 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.111 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
```

# Q&A

---

# Thank You

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

splunk> .conf2017