



splunk>

# How to Lose a Friend in 3 Days

## Using Splunk to crown the king of the hill

Brett Roberts | @bretts2261

Cory Minton | @cory\_minton

October 2018



# 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. © 2018 Splunk Inc. All rights reserved.

# Who Will be the King of the Hill?



# The Competitors



Brett “Black Diamond” Roberts

Favorite SPL Command = Eval



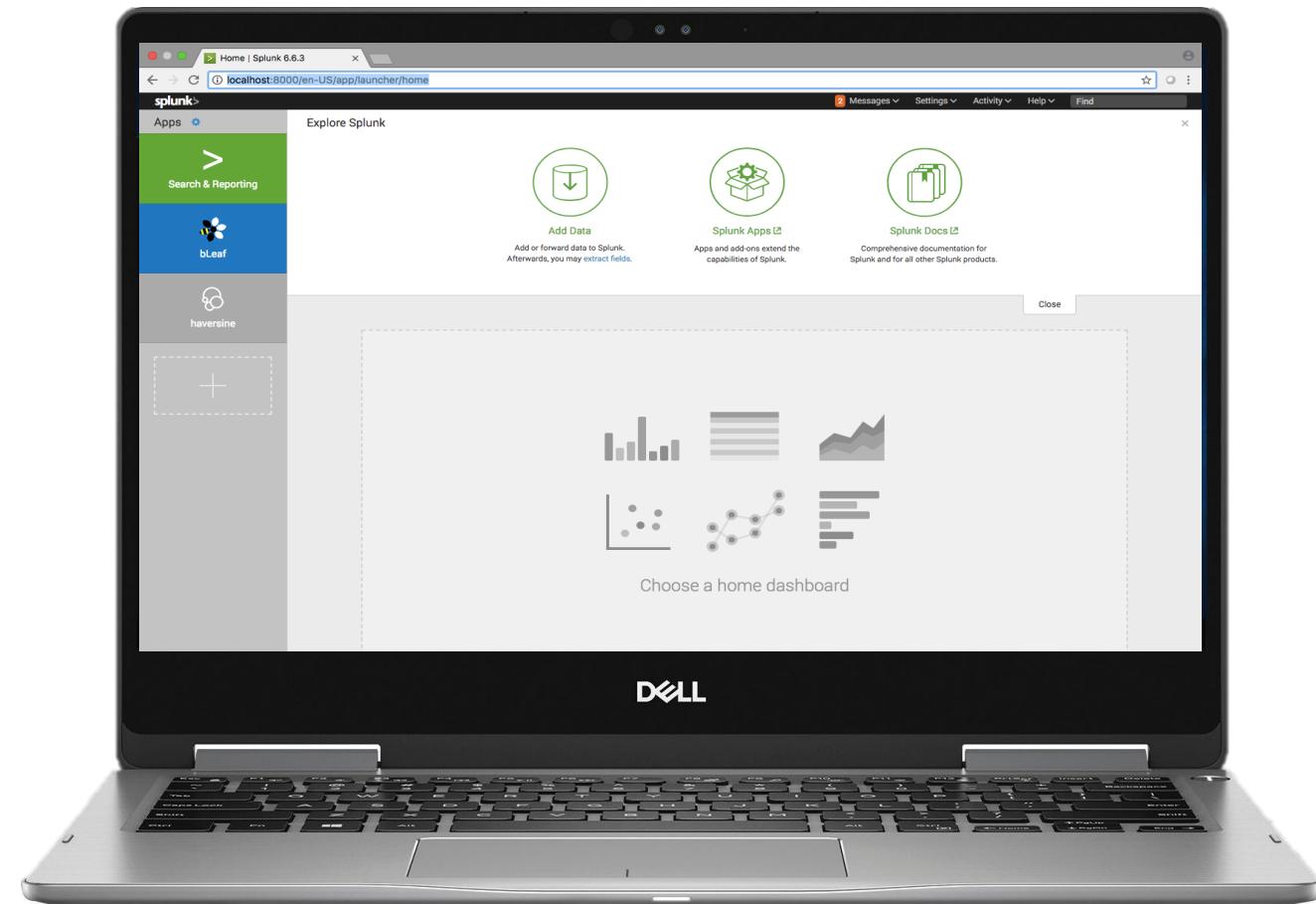
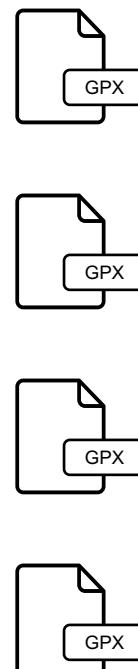
Cory “Bunny Slope” Minton

Favorite SPL Command = “What is SPL?”

# Technologies that We Used



# Snoww Mobile App



Splunk Enterprise 6.6.3



# haversine

The screenshot shows a laptop screen displaying the SplunkBase app page for the 'haversine' app. The page has a dark header with the Splunkbase logo and a search bar. Below the header, the app's name 'haversine' is displayed with a large, bold, white font. A 5-star rating with 6 ratings is shown. The main content area has tabs for 'Overview' (which is selected) and 'Details'. The 'Overview' tab contains a brief description of the app's function: '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.' Below this is a 'Release Notes' section for Version 2.0 (March 20, 2015), which states: 'This new release provides a bugfix or two, a bit more flexibility in syntax, and documentation updates.' To the right of the description, there are stats: '16 Installs' and '1,780 Downloads', with a prominent green 'LOGIN TO DOWNLOAD' button. At the bottom, it shows the app's version as '2.0', built by 'Steven Maresca', and its category as 'Utilities' under 'Category & Contents'.

- ▶ Free app in SplunkBase
  - Calculates the distance between two points represented via latitude and longitude
    - Built by Steven Maresca

# Using the Haversine App...

<span style="font-size: 2em;">&gt;</span> <u>3/20/18</u> <u>3:32:26.000 PM</u>	<pre>&lt;time&gt;2018-03-20T15:32:26&lt;/time&gt; &lt;bounds maxlat="39.196370537429" maxlon="0" minlat="0" minlon="-120.27697560389"/&gt; &lt;/metadata&gt; &lt;trk&gt; &lt;name&gt;&lt;/name&gt;</pre> <p>Show all 9 lines</p> <p>host = Bretts-MacBook-Air.local   source = 65245_activity.gpx   sourcetype = Ski_Data_Brett</p>
--	---

5 | **haversine originField=first\_loc second\_loc**

<span style="font-size: 2em;">&gt;</span> <u>1/24/18</u> <u>11:51:00.000 PM</u>	<pre>&lt;time&gt;2018-01-24T23:51:00.000000&lt;/time&gt; &lt;/trkpt&gt;&lt;trkpt lat="39.280684143341" lon="-120.12390537199"&gt; &lt;ele&gt;1956.79&lt;/ele&gt; &lt;time&gt;2018-01-24T23:51:13.000000&lt;/time&gt; &lt;/trkpt&gt;&lt;trkpt lat="39.280640222169" lon="-120.12395197537"&gt;</pre> <p>Show all 6 lines</p> <p>distance = 0.0039270113   host = Bretts-MacBook-Air.local   source = 66587_activity.gpx   sourcetype = Ski_Data_Brett</p>
---	--



# haversine

The screenshot shows a laptop displaying the SplunkBase app page for 'haversine'. The page has a dark theme. At the top, there's a navigation bar with links for 'My Account', 'Support & Services', and a search bar. Below the header, the app name 'haversine' is displayed with a large, light gray '>' icon to its left. It shows a 5-star rating with 6 ratings. The 'Overview' tab is selected, showing a brief 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.' Below this, there's a 'Release Notes' section for Version 2.0 (March 20, 2015) and a 'Details' section with version 2.0, built by Steven Maresca, and categories Utilities/Add-on. A prominent green 'LOGIN TO DOWNLOAD' button is centered below the stats. The Dell logo is visible at the bottom of the laptop.

## ► Free app in SplunkBase

- Calculates the distance between two points represented via latitude and longitude
  - Built by Steven Maresca

**Now we have distance and time...  
we can get SPEED**

```

1 sourcetype="ski_data_brett" date_mday!=25
2 | eval latlon=lat.",".lon
3 | transaction maxspan=7h maxevents=2 | eval first_loc=mvindex(latlon, 0)
4 | eval second_loc=mvindex(latlon, 1)
5 | haversine originField=first_loc second_loc
6 | eval distance = (distance * .62137119)
7 | where distance!=9.8250112
8 | stats sum(distance) as "Total Distance"

```

# What Questions Did we Ask?



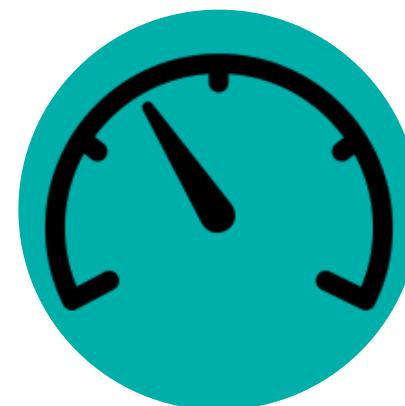
# Total Runs



# Daily Runs



## Distance



## Average Speed



# Top Speed

# The Results

Who will be the king of the hill



# Total Runs

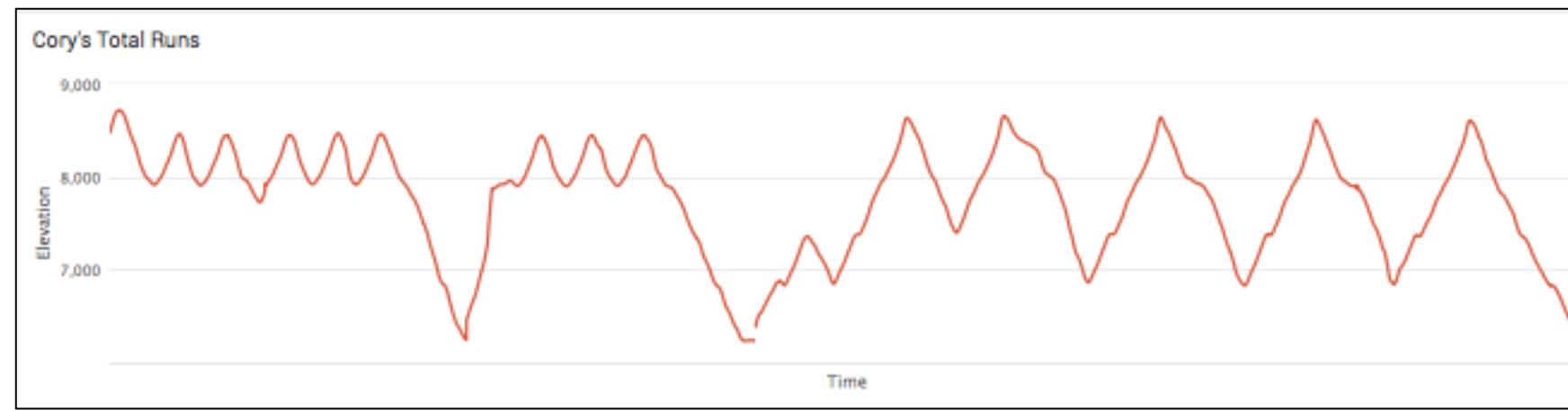
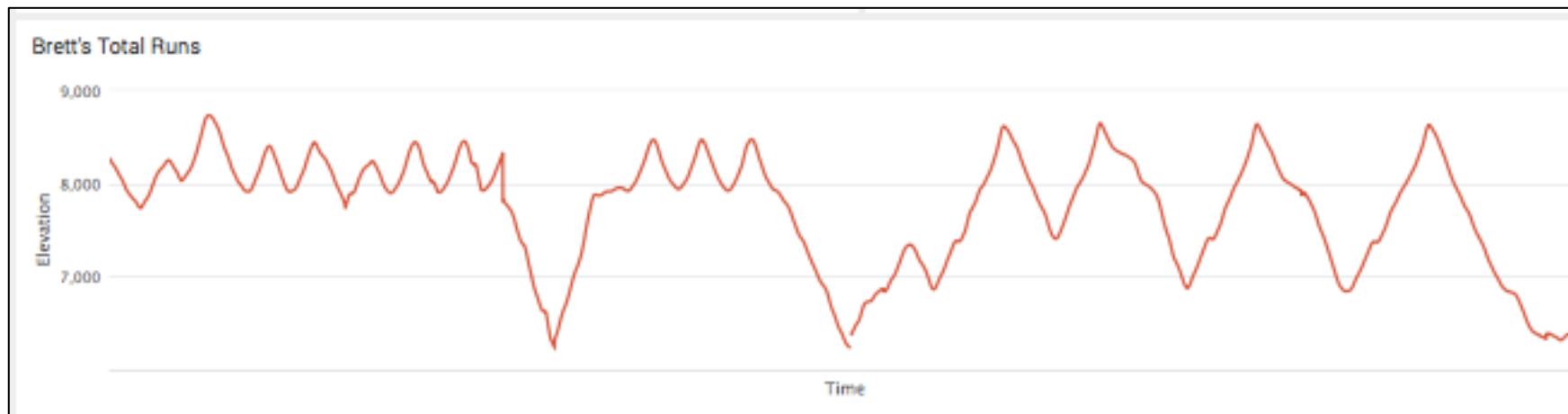
## SPL Query

```
1 sourcetype="ski_data_brett" _time="1516751022.999000" OR _time="1516750994.999000" OR _time="1516751710.997000" OR _time="1516752307.999000" OR _time="1516753283.999000"  
OR _time="1516753958.001000" OR _time="1516754762.997000" OR _time="1516755338.999000" OR _time="1516767929.999000" OR _time="1516768502.998000" OR _time="1516769099  
.997000" OR _time="1516838812.996000" OR _time="1516840050.000000" OR _time="1516841322.997000" OR _time="1516843320.999000" OR _time="1516852016.998000" OR _time  
="1516749607.011000"  
2 | stats count as elevation
```

## Results



# Plotting Our Runs



# # Of Runs by Day

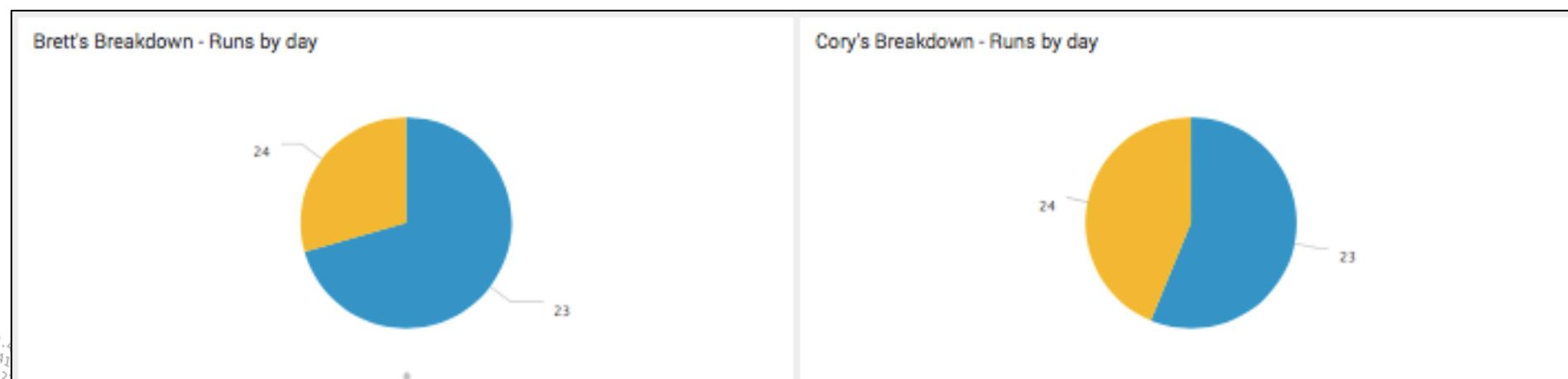
## SPL Query

```

1 sourcetype="ski_data_cory" _time="1516750895.998000" OR _time="1516751698.000000" OR _time="1516752215.000000" OR _time="1516753975.000000" OR _time="1516754749.998000" OR
 _time="1516755512.999000" OR _time="1516768030.000000" OR _time="1516768631.999000" OR _time="1516769198.998000" OR _time="1516837986.999000" OR _time="1516838769
 .998000" OR _time="1516840125.998000" OR _time="1516841325.999000" OR _time="1516843264.998000" OR _time="1516845188.000000" OR _time="1516851491.999000"
2 | stats count by date_mday
3 | rename date_mday as "date"

```

## Results



# Total Distance

# SPL Query

```
1 sourcetype="ski_data_cory"
2 | eval latlon=lat.",.lon
3 | transaction maxspan=7h maxevents=2 | eval first_loc=mvindex(latlon, 0)
4 | eval second_loc=mvindex(latlon, 1)
5 | haversine originField=first_loc second_loc
6 | eval distance = (distance * .62137119)
7 | where distance!=25.462668
8 | stats sum(distance) as "Total Distance"
```

## Results

### Brett's Total Distance

**20.31 Miles**

### Cory's Total Distance

# 20.79 Miles

# Avg Distance Per Run

# SPL Query

```
1 sourcetype="ski_data_brett" date_mday!=25
2 | eval latlon=lat.",".lon
3 | transaction maxspan=7h maxevents=2 | eval first_loc=mvindex(latlon, 0)
4 | eval second_loc=mvindex(latlon, 1)
5 | haversine originField=first_loc second_loc
6 | eval distance = (distance * .62137119)
7 | where distance!=9.8250112
8 | eval distance = (distance / 17)
9 | stats sum(distance) as "Total Distance"
```

## Results

### Brett's Avg Distance per Run

**1.194 Miles**

### Cory's Avg Distance per Run

**1.30 Miles**

# Average Speed

## SPL Query

```

1 sourcetype="ski_data_brett" date_hour!=0
2 | eval latlon=lat.",.lon | transaction maxspan=7h maxevents=2
3 | eval first_loc=mvindex(latlon, 0)
4 | eval second_loc=mvindex(latlon, 1)
5 | where first_loc!=second_loc
6 | havesine originField=first_loc second_loc | eval speed=distance/(duration/60/60) | where speed != 14230.640620214393
7 | stats avg(speed) AS avgSpeed
8 | eval "avgSpeed"=round(avgSpeed,2)
9 | rename avgSpeed as "Average Speed"

```

## Results

Brett's Trip Average Speed



Cory's Trip Average Speed



# Top Speed

## SPL Query

```
1 index="ski_data_brett_northstar" sourcetype="ski_data_brett" | eval latlon=lat.".lon | transaction maxspan=1h maxevents=2 | eval first_loc=mvindex(latlon, 0) | eval second_loc=mvindex(latlon, 1) | where first_loc!=second_loc | haversine originField=first_loc second_loc | eval speed=distance/(7/30/60) | eval speed=speed *.62137119223733 | stats max(speed) AS maxSpeed | eval "Max Speed"=round(maxSpeed,2) | fields "Max Speed"
```

## Results

Brett's Top Speed



Cory's Top Speed



# Time to Crown the "King of the Hill"

# Let's Use Splunk...

- ▶ Go to this website →
  - ▶ In field 2, under “Name or Team” put either:
    - “Brett” if you think he is king.
    - “Cory” if you think he is king.
  - ▶ SHAKE YOUR PHONE!!!
  - ▶ Highest shake velocity wins!

[www.Splunk.com/shake](http://www.Splunk.com/shake)

# Our Takeaways

- ▶ Splunk allows incredible exploration of data
- ▶ You can enrich data well in Splunk
- ▶ If we can do this goofy thing, imagine what you can do!
- ▶ Have fun!
- ▶ Keep learning
- ▶ Find your use case!

# Don't Forget to Attend Our Other Sessions

1. Master The Dark Arts: Demystifying Splunk Architecture –
  - October 3<sup>rd</sup> from 2-2:45pm
2. Choosing the Right Infrastructure for Your Splunk Deployment
  - October 4th from 11:00-11:45am
3. Splunk for IT Ops: A Storage Perspective
  - October 4th from 11:00-11:45am
  - Splunk Theater

*Stop by the Dell EMC booth (P1)  
to learn more*

# Thank You

Don't forget to rate this session  
in the .conf18 mobile app

