

Big Dating: Using Splunk to Fall in Love

Kelly Kitagawa | Sales Engineer, Splunk
Keegan Dubbs | Product Marketing, Splunk

September 26, 2017 | Washington, DC

Agenda

- ▶ Background
- ▶ The Social Experiment
- ▶ Field Extractions
- ▶ The Results
- ▶ Best Practices

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D5SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D5SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D5SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"

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.

**No
thanks**



How Does Bumble Work?



Match!

- Both parties swipe yes

Hi!

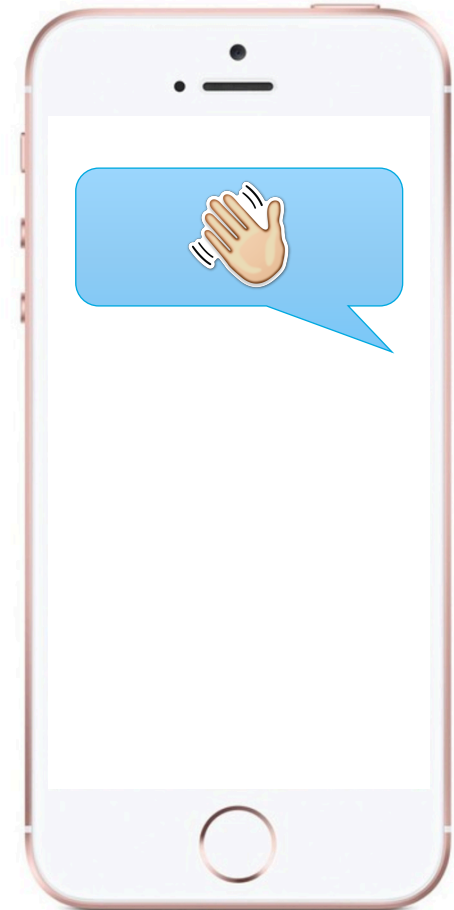
- Females have **24 hours** to write first message

Hey ;)

- Males have 24 hours to respond

The Social Experiment

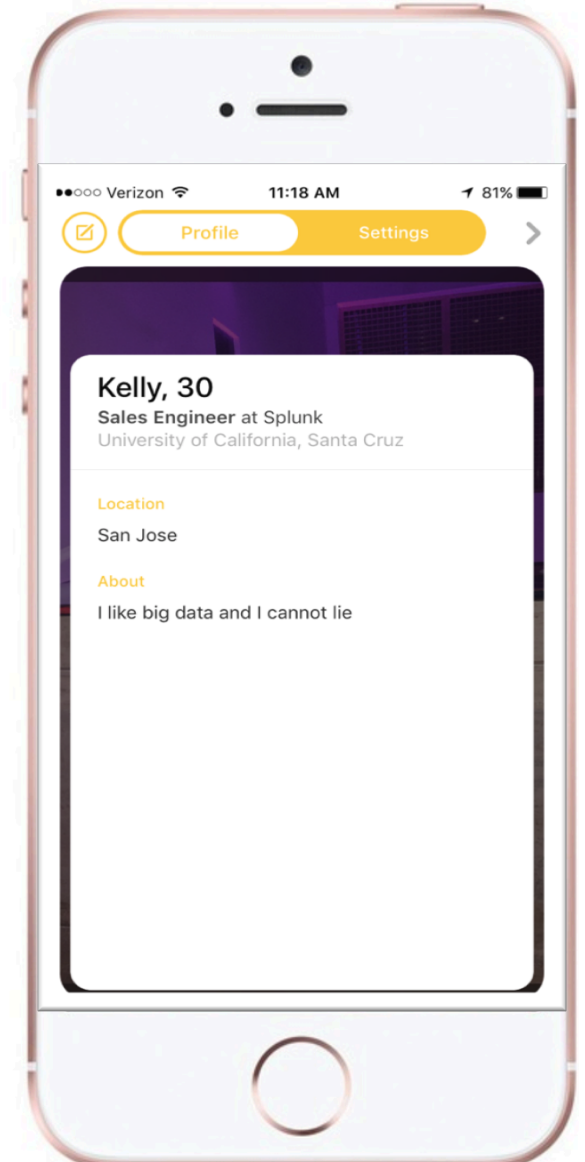
What first message gets the most responses?



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 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=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 10.0.0.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 10.0.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 10.0.0.0 - - [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=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 10.0.0.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 10.0.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0" 10.0.0.0 - - [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=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0"

Controlled Variables

- ▶ 50 matches each
- ▶ 5:00pm-9:00pm PST swipe time
- ▶ 6 photos
- ▶ Profile tagline: *I like big data and I cannot lie*



Gathering the Data

Favorite replies

Ur hawt

U2

Actually, I'm more of a Sting fan, but the reference was appropriate.....

Hey Chris, how's it going?

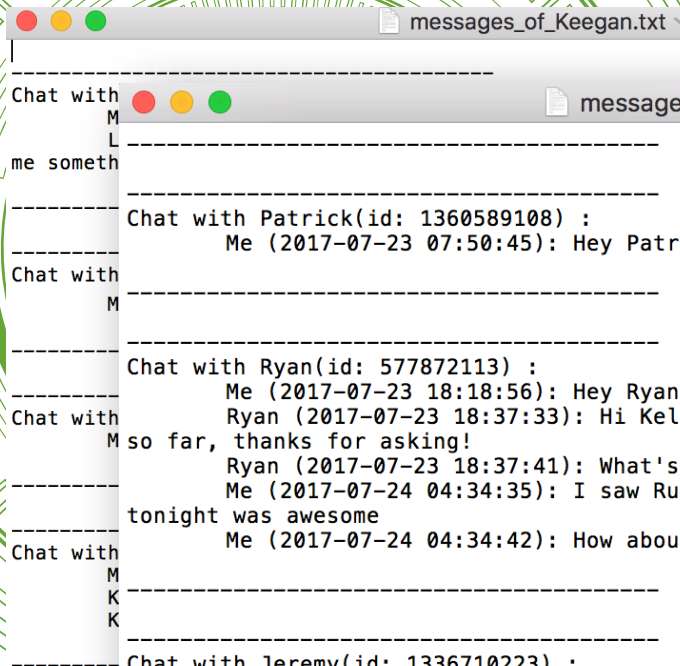
So wait you can't lie

Or you're not lying about the fact that you like big data

Ur hawt

Thanks! If only someone would use me for my mind though!

Gathering the Data



```

messages_of_Keegan.txt
-----
Chat with M
L
me someth
-----
Chat with Patrick(id: 1360589108) :
Me (2017-07-23 07:50:45): Hey Patrick. How's it going?
-----
Chat with M
-----
Chat with Ryan(id: 577872113) :
Me (2017-07-23 18:18:56): Hey Ryan. How's it going?
Chat with Ryan (2017-07-23 18:37:33): Hi Kelly, how are you doing? I'm having a great weekend
M so far, thanks for asking!
Ryan (2017-07-23 18:37:41): What's been the highlight of your weekend so far?
Me (2017-07-24 04:34:35): I saw Run The Jewels at BillG last night. GOT episode
tonight was awesome
Me (2017-07-24 04:34:42): How about yourself?
-----
Chat with M
K
K
-----
Chat with Jeremy(id: 1336710223) :
Me (2017-07-24 04:43:18): 🍷
-----
Chat with
-----
Chat with Dashiell(id: 1367769625) :
Me (2017-07-24 04:43:29): 🍷
-----
Chat with Straten(id: 1366466647) :
Me (2017-07-24 08:03:45): 🍷
-----

```

**Text file (.txt) of
chat records**

Step 1: Transforming the Data

Parse data for proper line breaking, and create custom source type

splunk> Apps

Add Data Next >

Select Source Set Source Type Input Settings Review Done

Set Source Type

This page lets you see how Splunk sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **messages_of_Keegan.txt**

Source type: **bumble_data** Save As

Event Breaks

Timestamp

Extraction Auto Current time Advanced...

Advanced

Name	Value	
CHARSET	UTF-8	x
BREAK_ONLY_BEFOI	(-){40}[\r\n]+	x
EXTRACT-future_hus	^(w+ s+)+(?<future	x
LINE_BREAKER	(-){40}[\r\n]+	x
NO_BINARY_CHECK	true	x
SHOULD_LINEMERG	false	x
category	Custom	x
description	bumble	x
disabled	false	x
pulldown_type	true	x

[New setting](#) [Copy to clipboard](#) Apply settings

	Time	Event
1	8/24/17 11:58:22.000 AM	timestamp = none
2	7/21/15 4:47:34.000 AM	Chat with Lucas(id: 1334123772) : Me (2015-07-21 04:47:34): Hi there Lucas (2015-07-21 06:22:42): Well hello there Keegan. How's i
3	7/21/15 4:48:01.000 AM	Chat with Ben(id: 1333692836) : Me (2015-07-21 04:48:01): Hi there 🤔
4	7/22/15 3:15:35.000 AM	Chat with Ryan(id: 1334067317) : Me (2015-07-22 03:15:35): Hi!
5	7/22/15 3:16:17.000 AM	Chat with Kyle(id: 1336968773) : Me (2015-07-22 03:16:17): Hi! Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week going Kyle (2015-07-24 23:33:04): What are you up to tonight/this w
6	7/22/15 3:29:11.000 AM	Chat with Brandon(id: 1322733585) : Me (2015-07-22 03:29:11): Hi!
7	7/22/15 11:28:27.000 PM	Chat with Samwise(id: 1335783455) : Me (2015-07-22 23:28:27): Hi!
8	8/18/15 4:06:43.000 AM	Chat with Dylan(id: 1341692307) : Me (2015-08-18 04:06:43): Soooo what would you say is the spa Dylan (2015-08-18 04:15:29): Hahahah can anything compare to Dylan (2015-08-18 04:16:20): I honestly don't think there is Me (2015-08-18 04:37:56): I mean I'm a big fan of comet in ca Show all 11 lines
9	8/18/15 4:07:33.000 AM	Chat with Nick(id: 1341080931) : Me (2015-08-18 04:07:33): Hayyy

Step 2: Extracting Fields

Extract fields using
regex and/or the
field extractor utility

splunk> App: Search & Reporting Administrator

Search Datasets Reports Alerts Dashboards

Extract Fields

Select sample Select method Select fields Validate Save

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

future_husband_name

Chat with Pete(id: 1330399597) :
Me (2017-08-05 22:53:44):

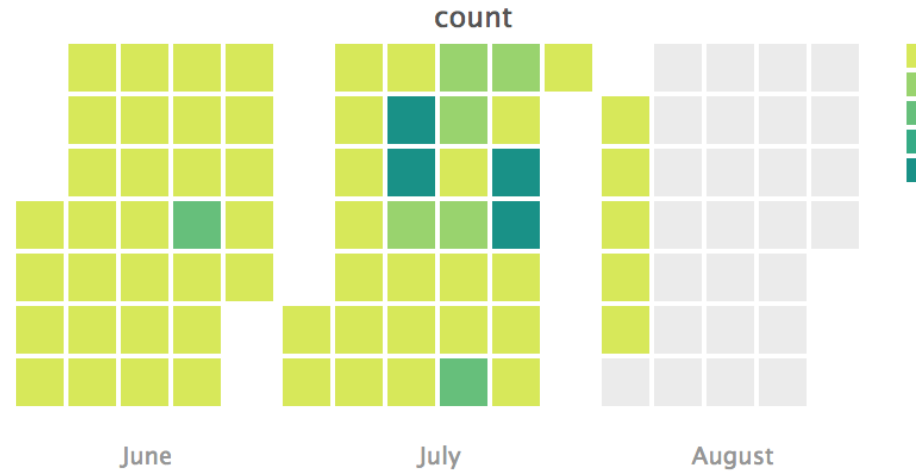
Step 3: Create Dashboards

The Results: What get's the most responses?

The screenshot displays the Splunk web interface. At the top, the navigation bar shows the Splunk logo and the application name 'App: Using Splunk to Fall In Love'. Below this, a secondary navigation bar contains links for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'Using Splunk to Fall in Love' and features three panels: 'Success Rate: Hey X Hows it Going', 'Success Rate: Ur Hawt', and 'Success Rate: hand Emoji'. Below these panels is a section titled 'Average Number of Messages within a Chat' and another titled 'Avg. TTR'. The interface also includes buttons for 'Edit', 'Export', and a menu icon in the top right corner of the dashboard area.

Custom Visualizations

Messages Heat Map by Day

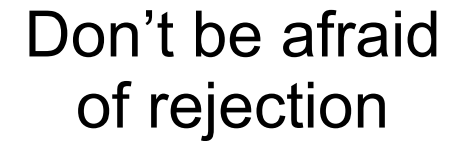
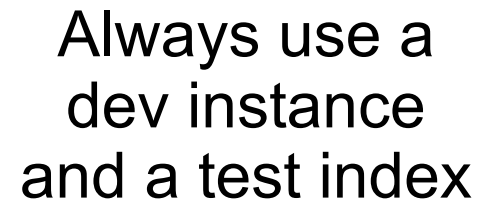
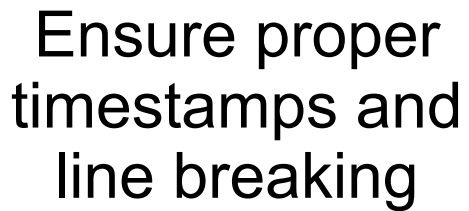


Most Frequent Names

Tag Cloud Visualization



Key Learning



**“Make machine data accessible,
usable and valuable to
everyone.”**

Ur hawt.

Kelly Kitagawa | Sales Engineer

Keegan Dubbs | 925-286-9779