splunk> .conf2017

# 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



splunk

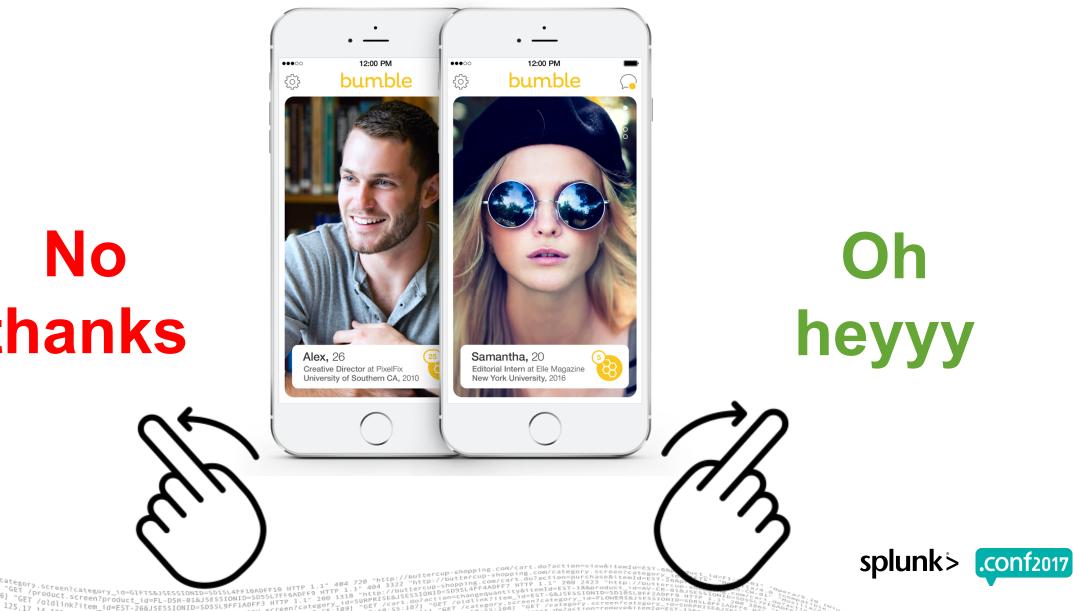
### **Forward-Looking Statements**

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.

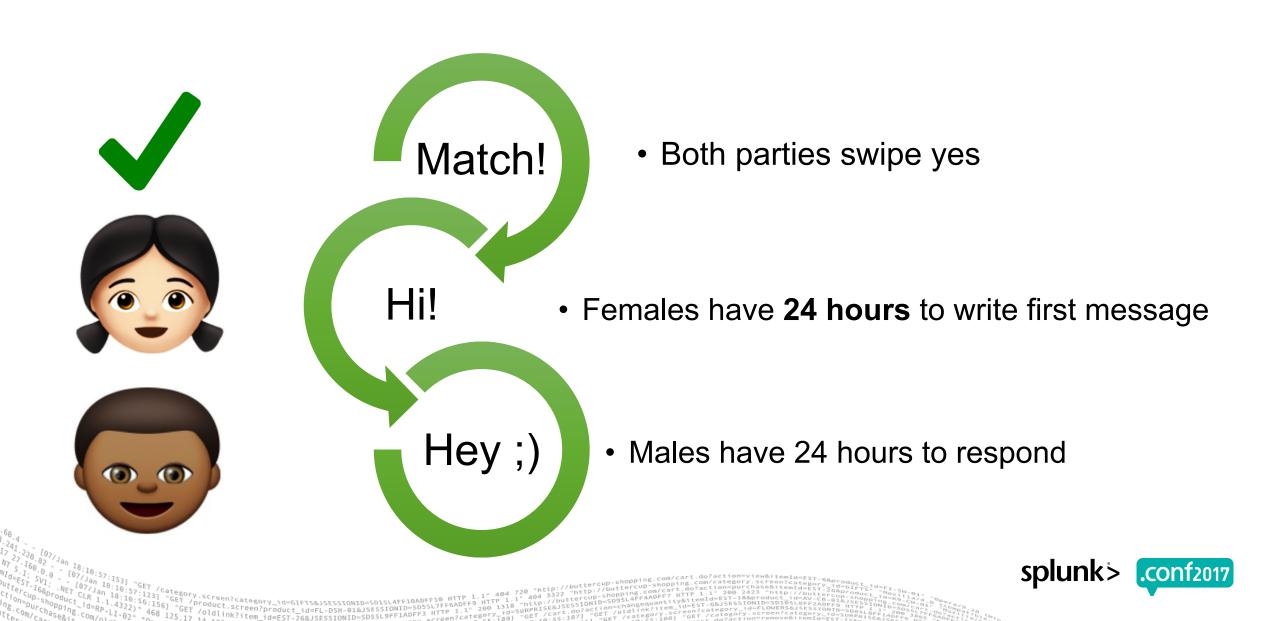
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk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

### **How Does Bumble Work?**

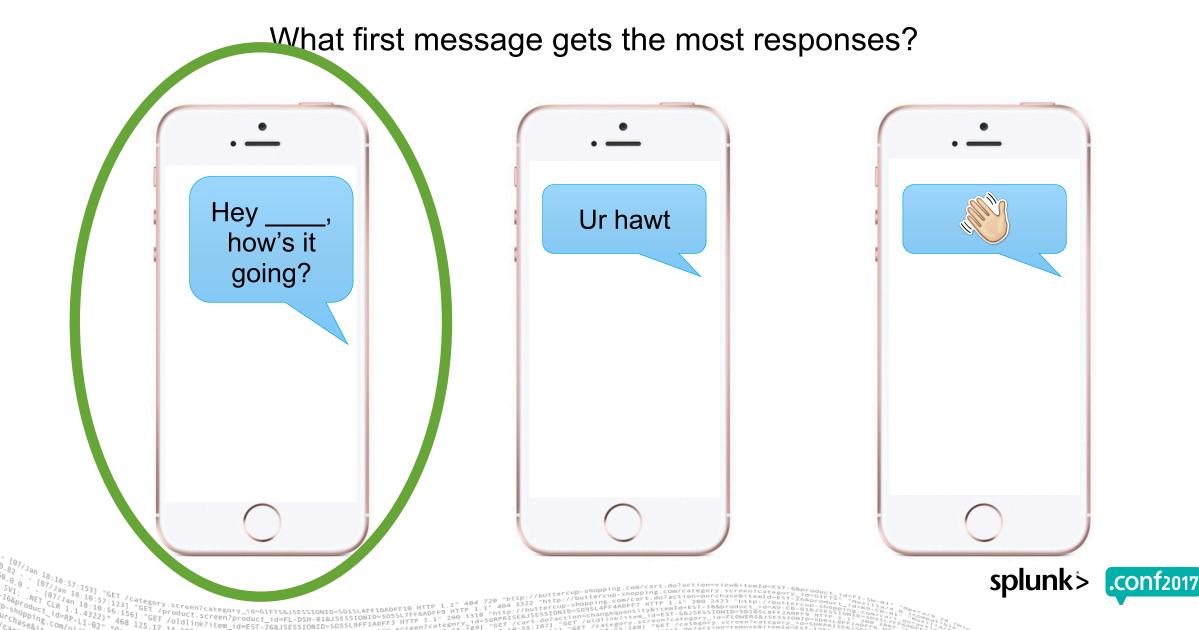


No thanks

### **How Does Bumble Work?**



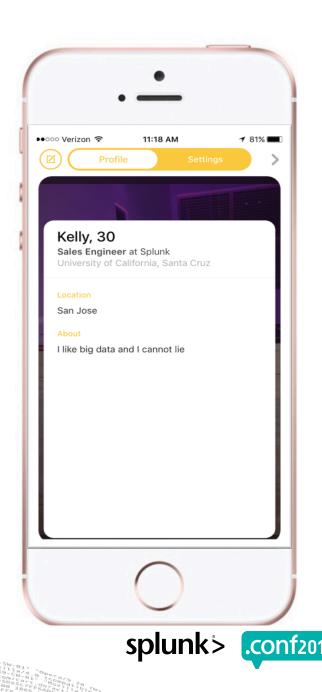
### **The Social Experiment**



### **Controlled Variables**

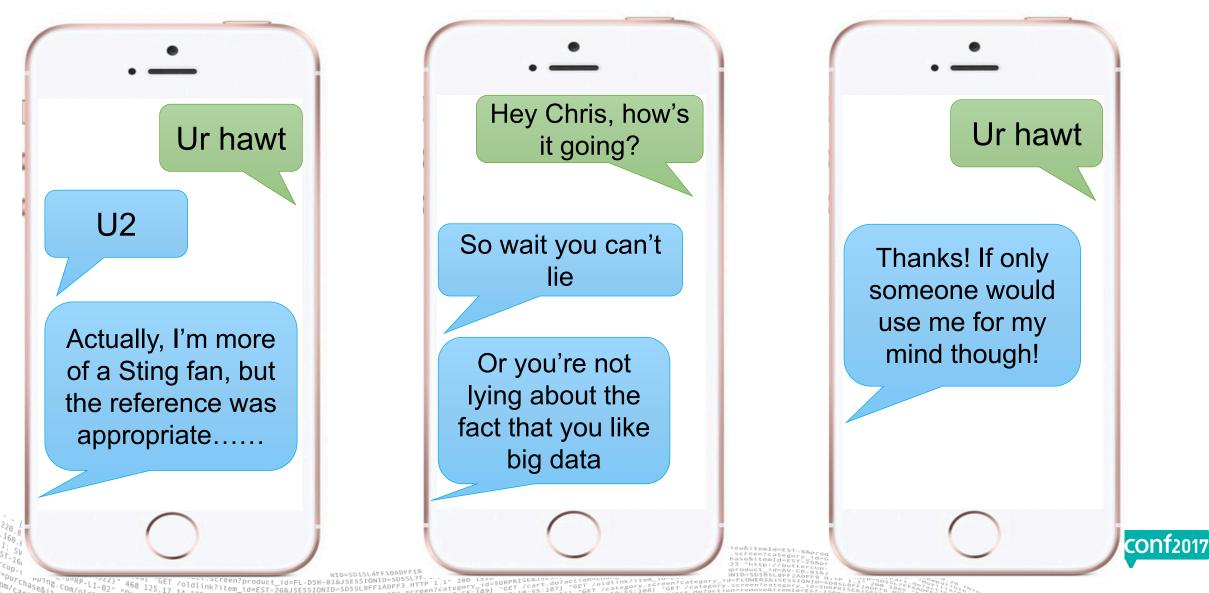
- ▶ 50 matches each
- ► 5:00pm-9:00pm PST swipe time
- ► 6 photos
- Profile tagline: I like big data and I cannot lie

Screen?product id=FL-DSH-01&JSESSIONID=SD5



### **Gathering the Data**

**Favorite replies** 



#### Gathering the Data UNNUNNUNNUNN messages\_of\_Keegan.txt Chat with messages\_of\_1335631403.txt ~ me someth Chat with Patrick(id: 1360589108) : Me (2017-07-23 07:50:45): Hey Patrick. How's it going? \_\_\_\_ Chat with Chat with Ryan(id: 577872113) : Me (2017-07-23 18:18:56): Hey Ryan. How's it going? Ryan (2017-07-23 18:37:33): Hi Kelly, how are you doing? I'm having a great weekend Chat with 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 - 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



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

Add Data       Select Source Type       Input Settings       Review       Dore       Next>         Select Source Type       This page lets you set how Splurk sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options blow 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:       Save As         Source type:       Save As         List        Format         2       Time         Timestamp       1         2       More timestamp         2       Time         2       True time         4/4734.000 AM       Chart with Lucas(1d: 1334123772) : Me (2015-07-21 04:7340) : Here there         Varianced       2       T/21/15         4/4724.000 AM       Chart with Lucas(1d: 13340237317) : Me (2015-07-22 04:7340) : Here there for the event interation of the cost of the c			/			
Selict Source     Set Source Type     Input Settings     Review     Done       Set Source Types     This page lets you see how Splunk sees you data before indoxing. If the events look correct and have the right limestamps, 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:     Source type:     Save As     List      / Format     20 Per Page        Source:     Save As     Image Vent     8/24/17       * Unrestamp     1     8/24/17     11.5822.200.0AM     timestamp = none       2     7/21/15     Chat with Lucas(1d: 1334123772) :     H. there       * Advanced     2     7/21/15     Chat with Lucas(1d: 1334023737) :     H. there       * Advanced     3     4/721/15     Chat with Mayn(1d: 133402737) :     H. there       * Manne     Value     4     7/22/15     Chat with Mayn(1d: 1334067317) :     H. there       © HARSET     UTF-B     ×     5     7/22/15     Chat with Mayn(1d: 1334067317) :     H. there       BREAK.ONLY_BEFOL     (400)(Vn0)/1)     ×     5     7/22/15     Chat with Mayn(1d: 1334067317) :     H. there       INE.BREAKER     (400)(Vn0)/1)     ×     6     7/22/15     Chat with Magn(1d: 1334067317) :     H. there       IND.	splunk> Apps ~		/			
This page lets you see how "Splunk sees your data before indexing. If the events look correct and have the right timestamp: divergences of the proper vertex that and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As". Source type: bumble_data  Source type: bumble_data Source type: b		Select Source Set S	Source Type Inpu	ıt Settings	Review Done	< Next>
Source type: bumble_data        Save As         Source type: bumble_data        Ime       Event         > Event Breaks       1       Br24/17         * Timestamp       1       Br24/17         * Timestamp       2       7/21/15         & Advanced       2       7/21/15         * Advanced       3       7/21/15         * Advanced       3       7/21/15         * Mame       Value       4         HARSET       UTF-8       ×         BREAK_ONLY_BEFOI       (440)[\vn]+)       ×         S16:17.000 AM       Chat with Ben(id: 1334067317) : Me (2015-07-22 03:15:35) : H1!         We (2015-07-22 03:15:37) : H1       Me (2015-07-22 03:15:37) : Me (2015-07-22 03:15:37) : H1         Kyle (2015-07-22 03:15:37) : H1       S16:17.000 AM         * Mone       *       6         MOLBINARY_CHECK       fue         NO_BINARY_CHECK       fue         NO_BINARY_CHECK       fue         Kyle (2015-07-22 03:28:37) : H1         Kyle (2015-07-22 03:28:37) : H1         Kyle (2015-07-22 03:28:17)	This page lets you see ho options below to define p	w Splunk sees your dat roper event breaks and				
> Event Breaks       1       ▲       B/24/17 11:5822.000 AM       timestamp = none         • Timestamp       2       7/21/15 4/3734.000 AM       Chat with Lucas(id: 1334123772) : 4/4734.000 AM       Chat with Lucas(id: 1334123772) : We (2015-07-21 04:47:34): Hi there Lucas (2015-07-21 04:47:34): Hi there Lucas (2015-07-21 04:47:34): Hi there         • Advanced       3       7/21/15 4/4801.000 AM       Chat with Ben(id: 1333692836) : Me (2015-07-21 04:47:34): Hi there ●         • Mame       Value       4       7/22/15 3:15:35.000 AM       Chat with Ryan(id: 1334067317) : Me (2015-07-22 03:15:17): Hi there ●         • CHARSET       UTF-8       ×       5       7/22/15 3:15:35.000 AM       Chat with Kyle(id: 136968773) : Me (2015-07-22 03:16:17): Hi there ●         • EXTRACT-future_hus       ^(\we+\se)+\te(?P-future x       5       7/22/15 3:29:11.000 AM       Chat with Kyle(id: 136968773) : Me (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hi there we (2015-07-22 03:28:39): Hi there we (2015-07-22 03:28:39): Hi there Me (2015-07-22 03:28:27): Hi there Me (2015-07-22 03:28:27): Hi there Me (2015-08-18 04:65:43): Soooo what would you say is the Dylan (2015-08-18 04:65:43): Soooo what would you say is the Dylan (2015-08-18 04:65:43): Soooo what would you say is the Dylan (2015-08-18 04:65:43): Soooo what would you say is the Dylan (2015-08-18 04:65:43): Soooo what would you say is the Dylan (2015-08-18 04:65:43): Soooo	Source type: bumble_da	ata 🗸	Save As	List 🗸	Format 20	Per Page 🗸
<ul> <li></li></ul>					Time	Event
Extraction       Auto       Current time       Advanced.       2       7/21/15       Chat with Lucas(id: 1334123772): Me (2015-07-21 06:22:42): Well hello there Keegan. How         V Advanced       3       7/21/15       Chat with Ben(id: 1333692836): Me (2015-07-21 06:22:42): Well hello there Keegan. How         CHARSET       UTF-8       ×         BREAK_ONLY_BEFOI       (+40)[hr/n]+)       ×         5       7/22/15       Chat with Ryan(id: 1334692373): Me (2015-07-22 03:15:35): Hi!         EXTRACT-future_hus       *(W+ts+)+(2P <future td="" x<="">         LINE_BREAKER       (+40)[hr/n]+)         X       5         MOLBINARY_CHECK       true         VOLD_LLINEMERG       false         Gescription       bumble         Molegate       8         8       8/18/15         4       7/22/15         Chat with Dandinid: 1321733585):         MOLD_LINEMERG       false         X       7         Me (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:17): Hi!         Me (2015-07-22 03:28:27): Hi!       11:28:27:000 PM         Me (2015-07-22 23:28:27): Hi!       11:28:27:000 PM         Me (2015-08-18 04:66:39): Soooo what would you say is the Dylan (2015-08-18 04:66:43): Soooo what would you say is the Dylan (2015-08-18 04:16:20): I</future>				1 🔺		timestamp = none
✓ Advanced       4:48:01.000 AM       Me (2015-07-21 04:48:01): Hi there ♥         Mame       Value       4       7/22/15       Chat with Ryan(id: 1334067317): Me (2015-07-22 03:15:35): Hi!         BREAK_ONLY_BEFOI       (-(40){\r/n}+)       ×       5       7/22/15       Chat with Kyle(id: 1336968773): Me (2015-07-22 03:28:39): Hi!         EXTRACT-future_hus       ^(\w+\s+)+(?P-future ×       5       7/22/15       Chat with Kyle(id: 1326968773): Me (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g Kyle (2015-07-22 03:28:17): Hi!         NO_BINARY_CHECK       true       ×       6       7/22/15       Chat with Brandon(id: 1322733585) : Me (2015-07-22 03:29:11): Hi!         SHOULD_LINEMERG       false       ×       7       7/22/15       Chat with Samwise(id: 1335783455) : Me (2015-07-22 23:28:27): Hi!         description       bumble       ×       8       8/18/15       Chat with Dylan(id: 1341692307) : Me (2015-08-18 04:06:32): Sooo what would you say is the Dylan (2015-08-18 04:06:43): Sooo what would you say is the Dylan (2015-08-18 04:06:43): Sooo what would you say is the Dylan (2015-08-18 04:06:16:20): I mean I'm a big fan of comet i Show all 11 lines         New setting       9       8/18/15       Chat with Nick(id: 134		Current time	Advanced	2		Me (2015-07-21 04:47:34): Hi there
CHARSET       UTF-8       ×         BREAK_ONLY_BEF0       ({40}{\runny})       ×         EXTRACT-future_hus       *(\w+\s+)+(?P <future td="" ×<="">         LINE_BREAKER       ({40}{\runny})         CHARSET       T/22/15         Chat with Kyle(id: 1336968773) :         S1:5:35.000 AM         Mc (2015-07-22 03:16:17) : Hi!         K(w+\s+)+(?P<future td="" ×<="">         LINE_BREAKER       ({40}{\runny})         NO_BINARY_CHECK       true ×         SHOULD_LINEMERG       false         Gategory       Custom         description       bumble         disabled       false         pulldown_type       true ×         9       8/18/15         New setting       9         9       8/18/15         Chat with Nick(id: 1341080931) :         We (2015-08-18 04:15:20) : I mean I'm a big fan of comet i         Show all 11 lines</future></future>	∽ Advanced			3		
CHARSET       UTF-8       ×         BREAK_ONLY_BEFOI       ({40}(\r/n)+)       ×         STRACT-future_hus       *(\w+\s+)+(?P-future ×         STRACT-future_hus       *(\w+\s+)+(?P-future ×         LINE_BREAKER       ({40}(\r/n)+)         LINE_BREAKER       ({40}(\r/n)+)         NO_BINARY_CHECK       true         X       6         7       7/22/15         Category       Custom         description       bumble         disabled       false         pulldown_type       true         x       8         8/18/15       Chat with Dylan(id: 1341692307) : Me (2015-08-18 04:16:20) : I honestly don't thick there Dylan (2015-08-18 04:15:29) : Habahah can anything compare Dylan (2015-08-18 04:15:20) : I man I'm a big fan of comet i Show all 11 lines         9       8/18/15       Chat with Nick(id: 1341080931) :         9       8/18/15       Chat with Nick(id: 1341080931) :	Name	Value		4	7/00/15	Chat with Dura/id: 1224067247) .
EXTRACT-future_hus       *(\w+\s+)+(?P-future x         EXTRACT-future_hus       *(\w+\s+)+(?P-future x         LINE_BREAKER       (:40)[\v/\n]+)         NO_BINARY_CHECK       true         XNO_BINARY_CHECK       true	CHARSET	UTF-8	×	4		
EXTRACT-future_hus       *(\w+\s+)+(?P <future td="" x<="">         INE_BREAKER       (-{40}}\v/n)+)         NO_BINARY_CHECK       true         XHOULD_LINEMERG       false         x       6         7       7/22/15         Category       Custom         description       bumble         bumble       x         8       8/18/15         Chat with Dylan(id: 1341692307) :         Me (2015-08-18 04:15:29) : Hapkab can anything compare Dylan (2015-08-18 04:15:29) : Haphab can anything compare Dyla</future>	BREAK_ONLY_BEFOI	(-{40}[\r\n]+)	×	5	7/22/15	(hat with Kula(id: 1336068773) .
LINE_BREAKER       (-{40}}\vn]+)       ×         NO_BINARY_CHECK       true       ×         SHOULD_LINEMERG       false       ×         category       Custom       ×         description       bumble       ×         disabled       false       ×         pulldown_type       true       ×         New setting       9       8/18/15         Chat with Namwise(id: 1341080931) :       Show all 11 lines	EXTRACT-future_hus	^(\w+\s+)+(?P <future< td=""><td colspan="2">+(?P<future td="" ×<=""><td></td><td>Me (2<mark>015-07-22 03:16:17)</mark>: Hi! Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g</td></future></td></future<>	+(?P <future td="" ×<=""><td></td><td>Me (2<mark>015-07-22 03:16:17)</mark>: Hi! Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g</td></future>			Me (2 <mark>015-07-22 03:16:17)</mark> : Hi! Kyle (2015-07-22 03:28:39): Hey Keegan. How's your week g
NO_BINARY_CHECK       true       ×       3:29:11.000 AM       Me (2015-07-22 03:29:11): Hi!         SHOULD_LINEMERG       false       ×       7       7/22/15       Chat with Samwise(id: 1335783455) : Me (2015-07-22 23:28:27): Hi!         description       bumble       ×       8       8/18/15       Chat with Dylan(id: 1341692307) : Me (2015-08-18 04:05:43): Sooo what would you say is the Dylan (2015-08-18 04:15:29): Hahahah can anything compare Dylan (2015-08-18 04:15:20): I honestly don't think there Me (2015-08-18 04:15:20): I mean I'm a big fan of comet i Show all 11 lines         New setting       9       8/18/15       Chat with Nick(id: 134180931) : How cometable and the samwing compare Dylan (2015-08-18 04:15:20): I mean I'm a big fan of comet i Show all 11 lines	LINE_BREAKER	(-{40}[\r\n]+)	×			Kyle (2015-07-24 23:33:04): What are you up to tonight/th
Category       Custom       x       7       7/22/15       Chat with Samwise(id: 1335783455):         Category       Custom       x       11/28:27.000 PM       Me (2015-07-22 23:28:27): Hi!         description       bumble       x       8       8/18/15       Chat with Dylan(id: 1341692307): Me (2015-08-18 04:06:43): Soooo what would you say is the Dylan (2015-08-18 04:16:20): I honestly don't think there Dylan (2015-08-18 04:16:20): I mean I'm a big fan of comet in Show all 11 lines         New setting       9       8/18/15       Chat with Nick(id: 134180931): May meree	NO_BINARY_CHECK	true	×	6		
category       Custom       x       11:28:27:000 PM       Me (2015-07-22 23:28:27): Hi!         description       bumble       x       8       8/18/15       Chat with Dylan(id: 1341692307): Me (2015-08-18 04:05:43): Soooo what would you say is the Dylan (2015-08-18 04:15:29): Hahahah can anything compare Dylan (2015-08-18 04:15:29): Hahahah can anything compare Dylan (2015-08-18 04:15:20): I honestly don't think there we we (2015-08-18 04:15:20): I honestly don't there we we (2015-08-18 04:15:20): I honestly don't think there we we (2015-08-18 04:15:20): I honestly don't think there we we conclude the don't don't there we we have a set of 2016 2016 2016 2016 2016 2016 2016 2016	SHOULD_LINEMERG	false	×	_		
disabled     false     x     4:06:43.000 AM     Me (2015-08-18 04:06:43): Soooo what would you say is the Dylan (2015-08-18 04:15:29): Hahahah can anything compare Dylan (2015-08-18 04:15:29): Honestly don't think there Me (2015-08-18 04:15:20): I honestly don't think there Me (2015-08-18 04:37:56): I mean I'm a big fan of comet i Show all 11 lines       New setting     9     8/18/15     Chat with Nick(id: 1341080931):	category	Custom	×	7		
disabled     false     x     Dylan (2015-08-18 04:15:29): Hahahah can anything compare Dylan (2015-08-18 04:16:20): I honestly don't think there we (2015-08-18 04:37:56): I mean I'm a big fan of comet in Show all 11 lines       New setting     9     8/18/15     Chat with Nick(id: 1341080931) : 407070 000 When the table of the table of table	description	bumble	×	8		
pulldown_type         true         ×         Show all 11 lines           New setting         9         8/18/15         Chat with Nick(id: 1341080931) :           Operate lightered         9         8/18/15         Chat with Nick(id: 1341080931) :	disabled	false	×		AN A	Dylan (2015-08-18 04:15:29): Hahahah can anything compare Dylan (2015-08-18 04:16:20): I honestly don't think there
407/02 000 AM	pulldown_type	true	×			
cheby country				9		

Step 1: Transforming the Data

### **Step 2: Extracting Fields**

### Extract fields using regex and/or the field extractor utility

Search Datasets	Reports	Alerts	Dashboards				
Extract Fields	Select sa	ample	Select method	Select fields	Validate	Save	lext >
elect Fields							
ighlight one or more val	g <mark>ht te</mark> xt that i						
Select Fields Highlight one or more val o modify them. To highlight future_husband_r Chat with Pete(id	ght text that i name	is already					

HULLIN ..

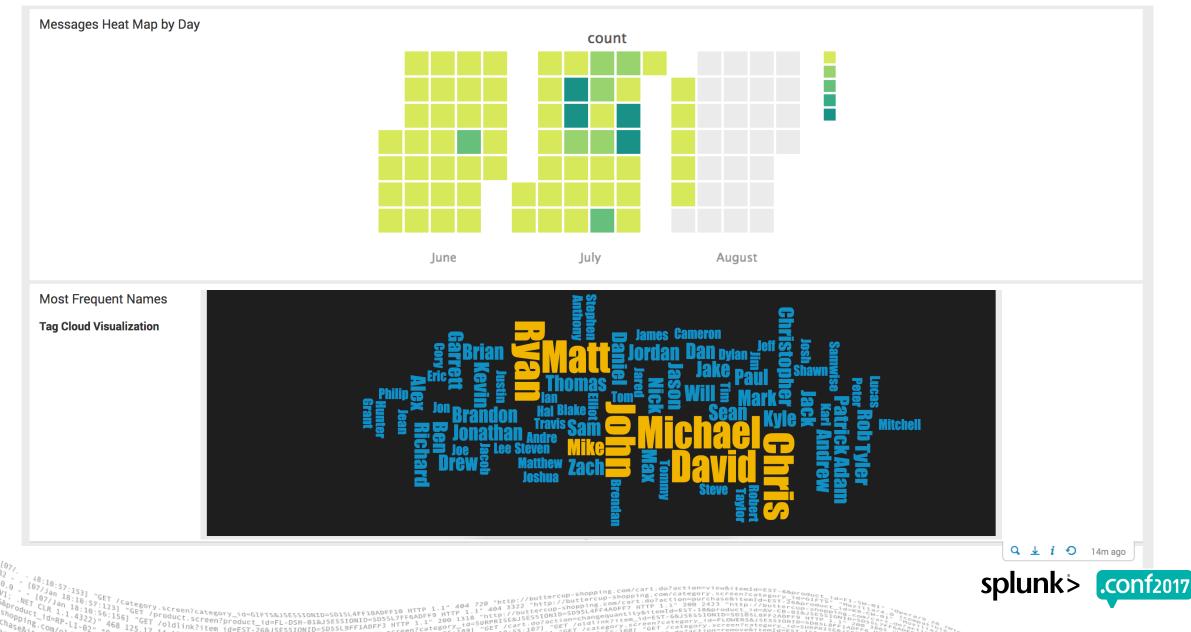


### **Step 3: Create Dashboards**

The Results: What get's the most responses?

splunk > App: Using Splunk to Fall In Love ~	Administrator 🗸	Messages → Settings → Activity →	Help∨ Find
Search Datasets Reports Alerts Dashboards			Using Splunk to Fall In Love
Using Splunk to Fall in Love			Edit Export ~
Success Rate: Hey X Hows it Going	Success Rate: Ur Hawt	Success Rate: hand Emoji	
Average Number of Messages within a Chat			
Avg. TTR			
".220 [07/Jan 2720.82	10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId= 10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cartegory.screen?cat. 10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cartHttp:// 10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/erHttp://	537-6&productd=r1-5W-01. =557id=52FTE.u=r1-5W-01. Duttor5&productMox12.64/4.20pn_	splunk'> .conf201

### **Custom Visualizations**



### **Best Practices**

Key Learning



timestamps and line breaking

friend

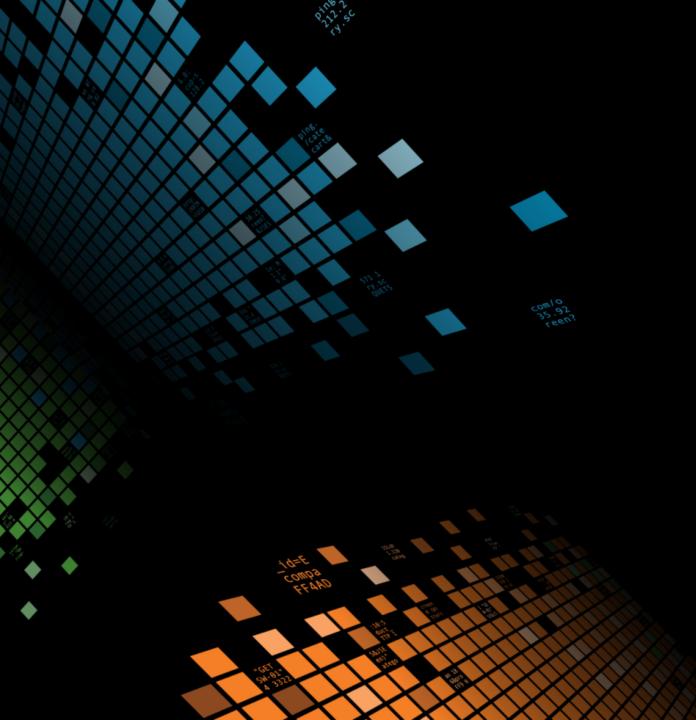
dev instance and a test index of rejection



© 2017 SPLUNK INC

### "Make machine data accessible, usable and valuable to everyone."





# Ur hawt.

Kelly Kitagawa | Sales Engineer Keegan Dubbs | 925-286-9779

