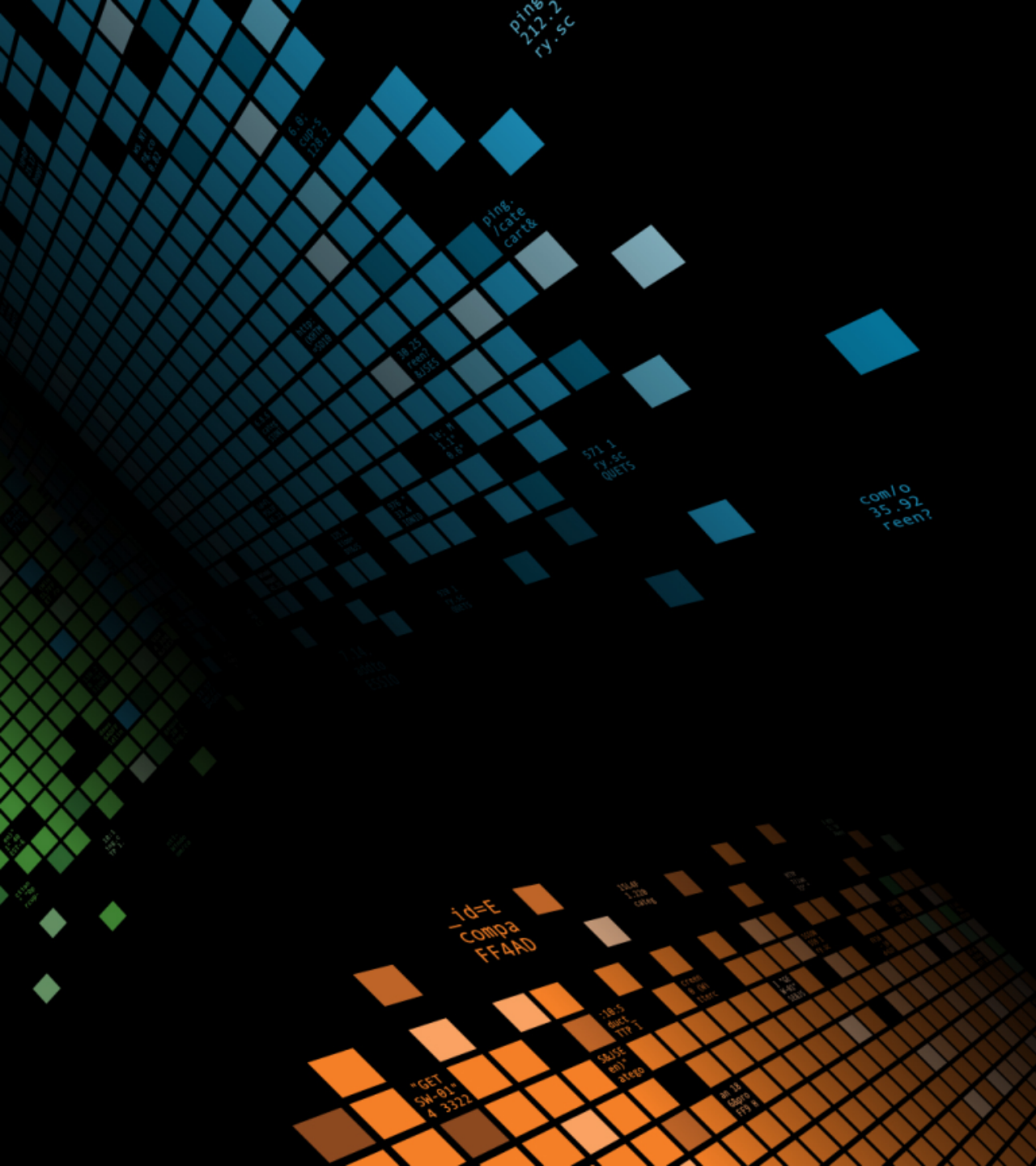


splunk> .conf2017

Beyond “Regular” Regular Expressions

Cary Petterborg | Splunk Architect | LDS Church

August 8, 2017



Boilerplate

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.

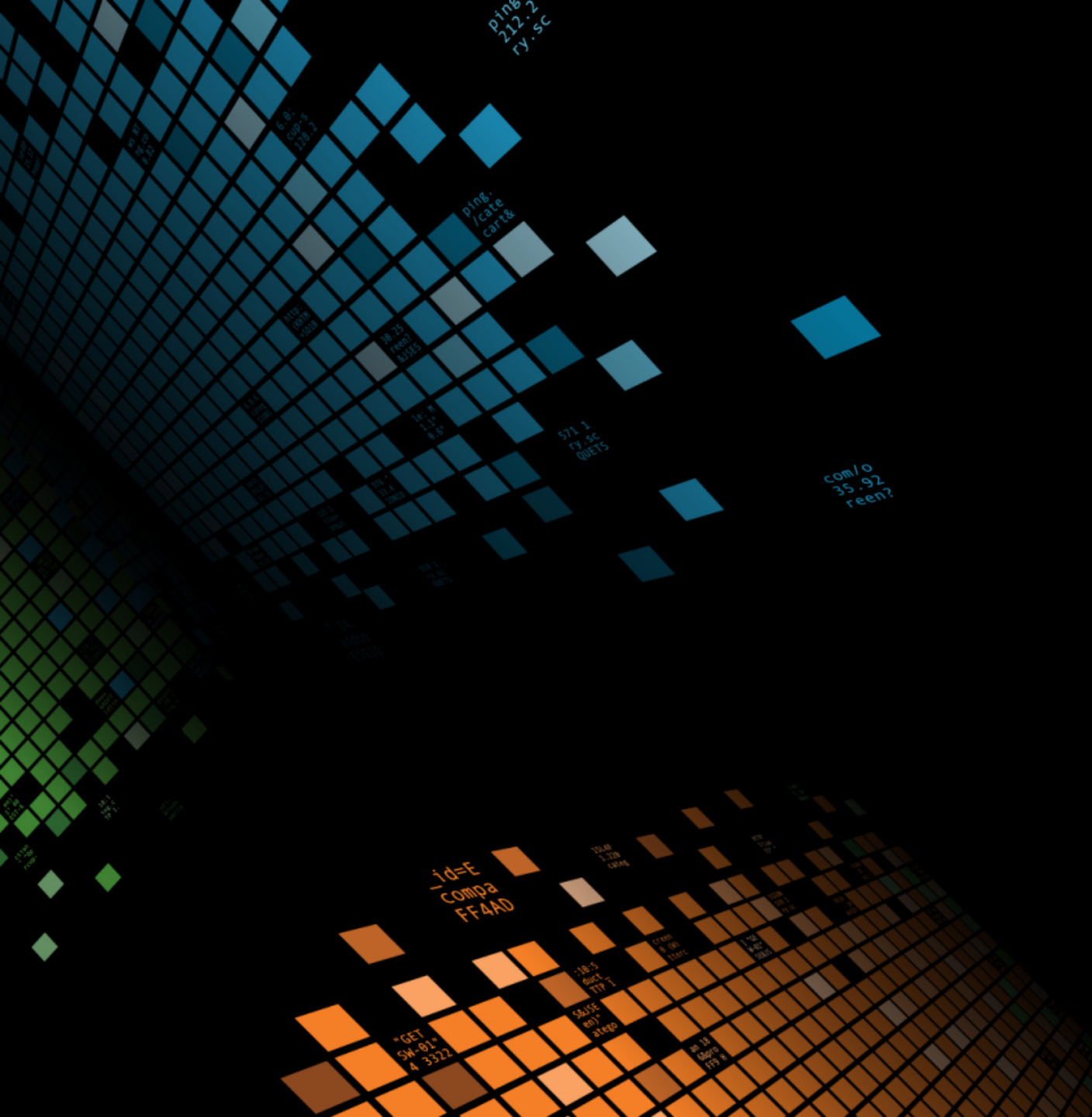
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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.

My Disclaimer

During the course of this presentation, I may make references to my employer, The Church of Jesus Christ of Latter-day Saints. This should not be taken as an endorsement of Splunk or Splunk products by the LDS Church.



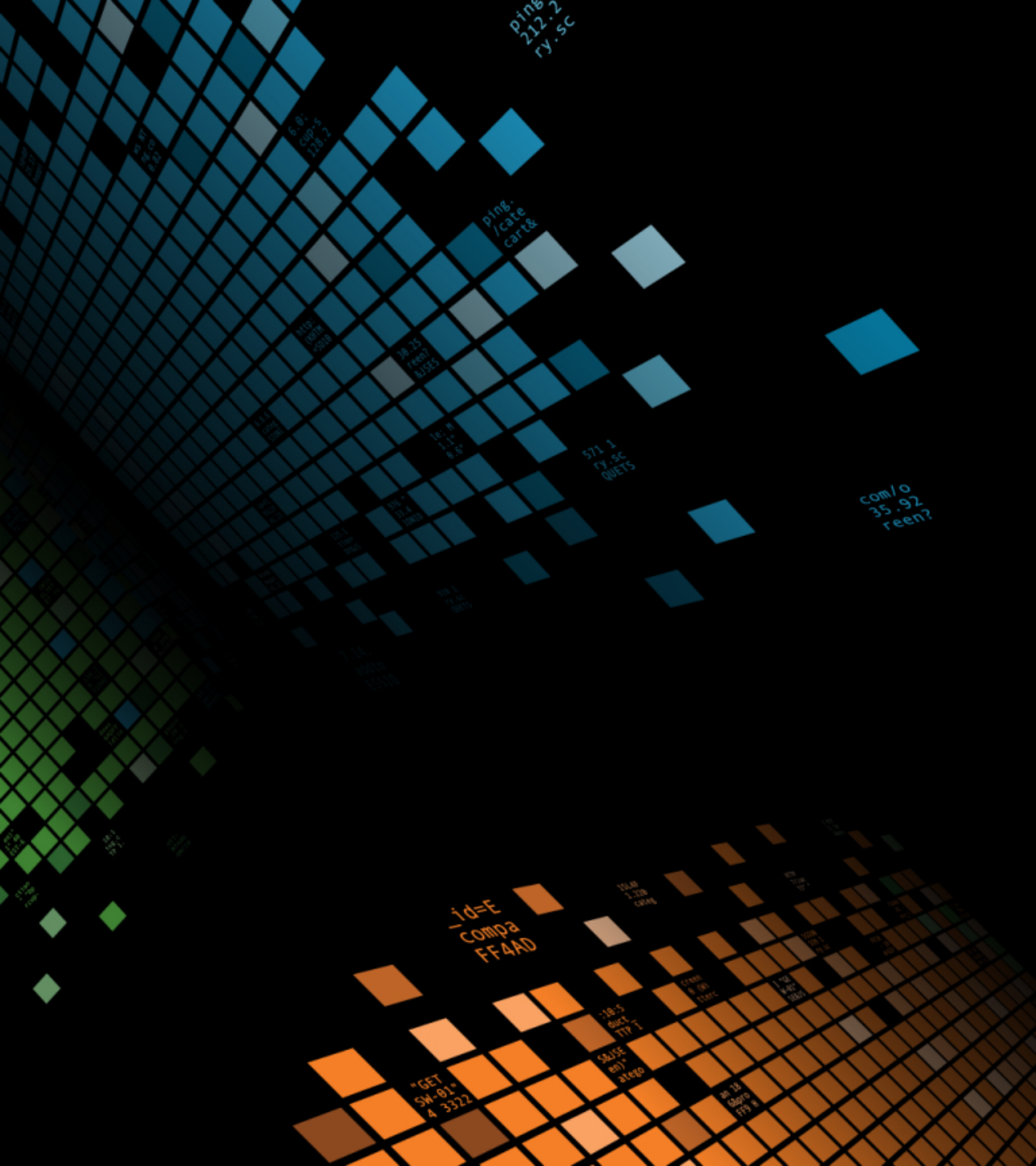


About Me

Who is Cary Petterborg

- ▶ Splunk user and administrator for 5.5 years
- ▶ Monitoring Engineer for 10 years
- ▶ Web developer for 23 years
- ▶ Software engineer for 37 years
- ▶ Many languages from assembly to Ruby
- ▶ Application development including Flight Sim, DB systems, and Web
- ▶ Works for the LDS Church in Salt Lake City
- ▶ Speaker at .conf 201[567]
- ▶ SplunkTrust Member 2018





Purpose

My purpose here today is to...

- ▶ Help you **control your data** instead of letting your data control you
- ▶ Regular expressions give you that control



Why Do I Like Regular Expressions?

- ▶ Using Regular Expressions since the mid 80's
- ▶ Started using regex with lex/yacc/sed/grep for software development
- ▶ Realized the power of regex quickly
- ▶ Taught classes on regex
- ▶ Love working with regex stuff in Splunk and other utilities
- ▶ **Regex is an important skill, and I want to share my knowledge**
- ▶ **Have Rex – Will Conquer**



One day, you too...

REGULAR EXPRESSION

1 MATCH - 9799 STEPS

```
/ ^\w{3}\s\d\d \d\d:\d\d:\d\d (?P<host>\w+).*Description=\s*(?P<descr>[\s\S]+20\d\d):[\s\S]*(MediaResourceList  
Name\s+:\s+(?P<media_res_list_name>\w+)[\s\S]*MediaResourceType\s+:\s+(?P<media_res_type>\d+)|RouteListName\  
s+:\s+(?P<route_list_name>[\^,;]+)[,;\s]*Reason=(?P<reason>\d+)[,;\s]*RouteGroups\((?P<route_grps>[\^\\]+)\)|T  
imeStamp\s+:\s+(?P<timestamp>\d+\d+\d+\s+\d+:\d+\s+\w+)\s+LoginFrom\s+:\s+(?P<login_from>[\^.\d]+)\s+Inter  
face\s+:\s+(?P<interface>\w+)\s+UserID\s+:\s+(?P<user_id>\w+)[\s\S]+AppID\s+:\s+(?P<app_id>[\w\s]+)[\s\S]*C  
lusterID\s+:\s+(?P<cluster_id>[\w-]*)[\s\S]+NodeID\s+:\s+(?P<node_id>\w+)[\s\S]+TimeStamp\s+:\s+(?P<ts>\w{3}  
[\w{3}]\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\d+)[\s\S]*::Status=(?P<status>\d+,[a-z]+)^Severity=(?P<severity>\w+)^  
Acknowledged=(?P<acked>\w+)^CUSTOMER=(?P<customer>[\^\\]+)^Private IP Address=(?P<priv_ip>[\^\\]+)^Default  
Alarm Name=(?P<def_alarm_name>[\^\\]+)^Managed Object=(?P<object>[\^\\]+)^Managed Object Type=(?P<obj_type>[\  
\^\\]+)^MODE=(?P<mode>[\^;]+);Alarm ID=(?P<alarm_id>\d+)^Component=(?P<component>[\^\\]+)\x0000
```

gmiXsuUAJ ?

TEST STRING

```
Jan 14 11:18:46 h32467 CPCMh32467: %local7-2-ALARM: 16$Description= Number of MediaResourceListExhausted events exceeds confi  
gured threshold during configured interval 5 within 60 minutes on cluster US-UT-DIR-Production. There are 6 MediaResourceLis  
tExhausted events (up to 30) received during the monitoring interval From Thu Jan 14 10:50:52 MST 2016 to Thu Jan 14 11:50:52  
MST 2016: MediaResourceListName : US-UT-DIR-Campus-NoVideo MediaResourceType : 2 AppID : Cisco CallManager ClusterID : US-UT  
-DIR-Production NodeID : dirvp211a TimeStamp : Thu Jan 14 11:17:53 MST 201::Status=1,active^Severity=minor^Acknowledged=no^CU  
STOMER=Cisco Prime Collaboration^Private IP Address=10.308.5.22^Default Alarm Name=MediaListExhausted^Managed Object=10.308.5.  
22^Managed Object Type=Communications Manager^MODE=2;Alarm ID=659201239^Component=dirvp212a.wh.hamsterfarm.net\x0000
```

One day, you too...

Regular Expression

[Regular Expression Reference](#) [View in Search](#)

```
^\\w{3}\\s\\d{4}\\s\\d{4}\\s\\d{4}\\s(?!P<host>\\w+) *Description=\\s*(?!P<descr>[\\s\\d]+20\\d\\d)[\\s\\d]*(MediaResourceListName\\s+\\s+(?!P<media_res_list_name>\\w+)[\\s\\d]*MediaResourceType\\s+\\s+(?!P<media_res_type>\\d+)[RouteListName\\s+\\s+(?!P<route_list_name>[\\s\\d]+)[\\s\\d]*Reason=(?!P<reason>\\d+)[\\s\\d]*RouteGroups((?!P<route_grps>[\\s\\d]+))\\s+Timestamp\\s+\\s+(?!P<timestamp>\\d+\\d+\\d+\\d+\\d+\\s+\\w+)[\\s\\d]*LoginFrom\\s+\\s+(?!P<login_from>[\\s\\d]+)[\\s\\d]*Interface\\s+\\s+(?!P<interface>\\w+)[\\s\\d]*UserID\\s+\\s+(?!P<user_id>\\w+)[\\s\\d]*AppID\\s+\\s+(?!P<app_id>[\\w\\s]+)[\\s\\d]*ClusterID\\s+\\s+(?!P<cluster_id>[\\w\\s]+)[\\s\\d]*NodeID\\s+\\s+(?!P<node_id>\\w+)[\\s\\d]*TimeStamps+\\s+(?!P<ts>\\w{3})\\s+\\d+\\s+\\d+\\s+\\d+\\s+\\d+\\s+\\w+\\s+\\d+)[\\s\\d]*Status=(?!P<status>\\d+)[\\s\\d]*Severity=(?!P<severity>\\w+)[\\s\\d]*Acknowledged=(?!P<acked>\\w+)[\\s\\d]*CUSTOMER=(?!P<customer>[\\s\\d]+)[\\s\\d]*Private IP Address=(?!P<priv_ip>[\\s\\d]+)[\\s\\d]*Default Alarm Name=(?!P<def_alarm_name>[\\s\\d]+)[\\s\\d]*Managed Object=(?!P<object>[\\s\\d]+)[\\s\\d]*Managed Object Type=(?!P<obj_type>[\\s\\d]+)[\\s\\d]*MODE=(?!P<mode>[\\s\\d]+)[\\s\\d]*Alarm ID=(?!P<alarm_id>\\d+)[\\s\\d]*Component=(?!P<component>[\\s\\d]+)[\\s\\d]*\\x00000
```

Preview Save

Events	host	descr	media_res_list_name	media_res_type	route_list_name	reason	route_grps	timestamp	login_from	interface	user_id	app_id	cluster_id	node_id	ts	status	severity	acked
--------	------	-------	---------------------	----------------	-----------------	--------	------------	-----------	------------	-----------	---------	--------	------------	---------	----	--------	----------	-------

✓ 10 events (before 7/11/16 4:29:50.000 PM) Original search included: 20 per page ▾

filter Apply Sample: 1,000 events ▾ All events ▾ All Events Matches Non-Matches

✓	Jan 14 11:18:46	h32467	CPCMH32467: %Local7-2-ALARM: 16\$Description=	h32467	Number of MediaResourceListExhausted events exceeds configured threshold during configured interval 5 within 60 minutes on cluster US-UT-DIR-Production. There are 6 MediaResourceListExhausted events (up to 30) received during the monitoring interval From Thu Jan 14 10:50:52 MST 2016 to Thu Jan 14 11:50:52 MST 2016: MediaResourceListName: US-UT-DIR-Campus-NoVideo MediaResourceType: 2 AppID: Cisco CallManager ClusterID: US-UT-DIR-Production NodeID: dirvp211a Timestamp: Thu Jan 14 11:17:53 MST 2016::Status=1,active^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime Collaboration^Private IP Address=10.308.5.22^Default Alarm Name=MediaListExhausted^Managed Object=10.308.5.22^Managed Object Type=Communications Manager^MODE=2;Alarm ID=659201239^Component=dirvp212a.wh.hamsterfarm.net \x00000
✓	Jan 14 10:58:14	h32467	CPCMH32467: %Local7-2-ALARM: 16\$Description=	h32467	Number of RouteListExhausted events exceeds configured threshold during configured interval 0 within 60 minutes on cluster BRVP. There are 1 RouteListExhausted events (up to 30) received during the monitoring interval From Thu Jan 14 15:48:46 BRST 2016 to Thu Jan 14 16:48:46 BRST 2016: RouteListName: Local Route Group No Translations; Reason=41; RouteGroups(BR-SP-Brazil-TPL-A0) AppID: Cisco CallManager ClusterID: BRVP NodeID: BRVP2 Timestamp: Thu Jan 14 15:54:45 BRST 2016::Status=1,active^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime Collaboration^Private IP Address=10.555.41.20^Default Alarm Name=RouteListExhausted^Managed Object=10.555.41.20^Managed Object Type=Communications Manager^MODE=2;Alarm ID=659617997^Component=BRVP1.heavensgate.org \x00000
✓	Jan 14 10:53:27	h32467	CPCMH32467: %Local7-2-ALARM: 16\$Description=	h32467	Number of MediaResourceListExhausted events exceeds configured threshold during configured interval 5 within 60 minutes on cluster US-UT-DIR-Production.\x00012\x00012There are 6 MediaResourceListExhausted events (up to 30) received during the monitoring interval From Thu Jan 14 09:50:51 MST 2016 to Thu Jan 14 10:50:51 MST 2016: \x00012\x00012MediaResourceListName: NULL_LIST \x00012MediaResourceType: 1 \x00012AppID: Cisco CallManager \x00012ClusterID: US-UT-DIR-Production \x00012NodeID: dirvp211b \x00012 Timestamp: Thu Jan 14 10:13:44 MST 2016 \x00012\x00012MediaResourceL::Status=2,cleared^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime Collaboration^Private IP Address=10.308.5.22^Default Alarm Name=MediaListExhausted^Managed Object=10.308.5.22^Managed Object Type=Communications Manager^MODE=2;Alarm ID=659201239^Component=dirvp212a.wh.hamsterfarm.net \x00000
✓	Jan 14 10:53:06	h32467	CPCMH32467: %Local7-2-ALARM: 16\$Description=	h32467	Number of MediaResourceListExhausted events exceeds configured threshold during configured interval 0 within 60 minutes on cluster ARVP. There are 1 MediaResourceListExhausted events (up to 30) received during the monitoring interval From Thu Jan 14 14:48:15 ART 2016 to Thu Jan 14 15:48:15 ART 2016: MediaResourceListName: UV-MO-MNTVD-TPLCMLX MediaResourceType: 7 AppID: Cisco CallManager ClusterID: ARVP NodeID: ARVP2 Timestamp: Thu Jan 14 14:51:15 ART 2016::Status=1,active^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime Collaboration^Private IP Address=10.555.72.21^Default Alarm Name=MediaListExhausted^Managed Object=10.555.72.21^Managed Object Type=Communications Manager^MODE=2;Alarm ID=659600865^Component=ARVP2.LDSChurch.org \x00000
✓	Jan 14 10:28:15	h32467	CPCMH32467: %Local7-2-ALARM: 16\$Description=	h32467	Number of RouteListExhausted events exceeds configured threshold during configured interval 0 within 60 minutes on cluster DE-HE.\x00012\x00012There are 1 RouteListExhausted events (up to 30) received during the monitoring interval From Thu Jan 14 17:22:58 CET 2016 to Thu Jan 14 18:22:58 CET 2016: \x00012\x00012RouteListName: LocalRouteGroupOnly, Reason=41; RouteGroups(FR-J-Torcy-SE) \x00012AppID: Cisco CallManager \x00012ClusterID: DE-HE \x00012NodeID: eadebhgscvp002 \x00012 Timestamp: Thu Jan 14 17:38:52 CET 2016 \x00012\x00012::Status=2,cleared^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime Collaboration^Private IP Address=10.277.4.21^Default Alarm Name=RouteListExhausted^Managed Object=10.277.4.21^Managed Object Type=Communications Manager^MODE=2;Alarm ID=658775520^Component=eadebhgscvp002.heavensgate.org \x00000

130.60.4 - - [07/Jan 18:10:57:153] "GET /c/128.241.220.02 - - [07/Jan 18:10:57:123] "ows NT 5.1: 5V1; NET CLR 1.1.4322)" 468] /buttercup-shopping_id=RP-LI-02" "0 /buttercup-purchase.com/01 /buttercup-purchase.com/01





Splunk and Regular Expressions

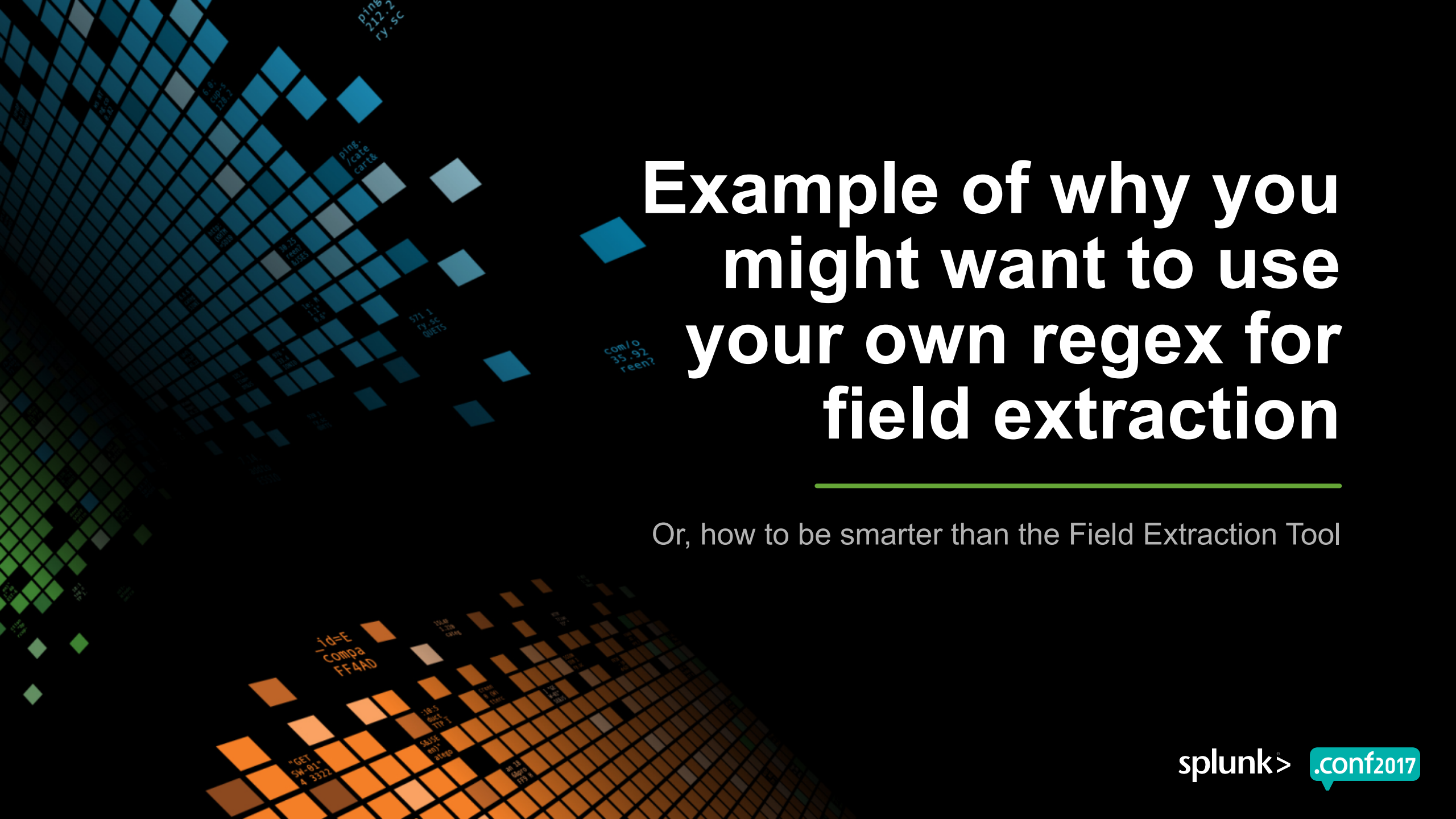
Where do you use regular expression in Splunk?

- ▶ Field extractions
- ▶ The **rex** and **regex** search commands
- ▶ In *props.conf*, *transforms.conf* and other *.conf* files
- ▶ Data feeds (probably external to Splunk itself)
- ▶ Note: Splunk regular expressions are PCRE (Perl Compatible Regular Expressions) and use the PCRE C library.





Splunk Field Extraction Tool



Example of why you might want to use your own regex for field extraction

Or, how to be smarter than the Field Extraction Tool

Multi-format Security Data in...

```
secure.log
1 Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.241.220.82 port 2253 ssh2-
2 Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user administrator from 128.241.220.82 port 1715 ssh2-
3 Mon Jun 06 2016 02:29:44 www1 sshd[5001]: Failed password for invalid user george from 128.241.220.82 port 2212 ssh2-
4 Mon Jun 06 2016 02:30:13 www1 sshd[1638]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)-
5 Mon Jun 06 2016 02:30:13 www1 sshd[1480]: Failed password for invalid user yp from 128.241.220.82 port 2808 ssh2-
6 Mon Jun 06 2016 02:30:22 www1 sshd[2291]: Failed password for invalid user email from 128.241.220.82 port 4995 ssh2-
7 Mon Jun 06 2016 02:30:26 www1 sshd[4761]: Failed password for invalid user local from 128.241.220.82 port 1271 ssh2-
8 Mon Jun 06 2016 02:30:50 www1 sshd[4986]: Failed password for invalid user mysql from 128.241.220.82 port 2076 ssh2-
9 Mon Jun 06 2016 02:31:19 www1 sshd[81145]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)-
10 Mon Jun 06 2016 02:31:19 www1 sshd[2021]: Failed password for myuan from 10.1.10.172 port 4468 ssh2-
11 Mon Jun 06 2016 02:31:28 www1 sshd[1155]: Failed password for invalid user yp from 10.1.10.172 port 1822 ssh2-
12 Mon Jun 06 2016 02:31:32 www1 sshd[1632]: Failed password for invalid user elena_andubasquet from 10.1.10.172 port 2074 ssh2-
13 Mon Jun 06 2016 02:31:54 www1 sshd[4333]: Failed password for root from 10.1.10.172 port 2772 ssh2-
14 Mon Jun 06 2016 02:32:00 www1 sudo: djohnson ; TTY=pts/0 ; PWD=/home/djohnson ; USER=root ; COMMAND=/bin/su-
15 Mon Jun 06 2016 02:32:00 www1 sshd[3697]: Failed password for invalid user whois from 10.1.10.172 port 1246 ssh2-
16 Mon Jun 06 2016 02:32:19 www1 sshd[5985]: Failed password for invalid user testuser from 10.1.10.172 port 2597 ssh2-
```

130.60.4 - - [07/Jun 2016 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=F1-5W-01" Moz/5.0 (Macintosh; Intel Mac OS X 10_7_0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6.0
128.241.220.82 - - [07/Jun 2016 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6.0
137.27.160.0 - - [07/Jun 2016 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://shopping.com/cart.do?action=remove&itemId=EST-18" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6.0
130.60.4 - - [07/Jun 2016 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://shopping.com/cart.do?action=remove&itemId=EST-18" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6.0
130.60.4 - - [07/Jun 2016 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://shopping.com/cart.do?action=remove&itemId=EST-18" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6.0

Simple FET extraction of Port

This is what the FET gives you:

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 for the regular expression

```
Wed Jun 08 2016 09:39:12 www1 sshd[4092]: Failed password for invalid user local from 109.169.32.135 port 2172 ssh2
```

Hide Regular Expression ▾

```
^(?:[^\.\n]*\.)?(3)\d+\s+\w+\s+(?P<port>\d+)
```



Notes on Named Capture Groups

- ▶ (?P<name>...) === (?<name>...)
- ▶ The **P** is optional (came from **P**ython), but it is usually considered more correct
- ▶ Splunk FET will use (?P<name>...), so why not make things similar?

BUT

- ▶ Do it the way you feel most comfortable



FET Failed


Gets wrong values from some events

```
: Failed password for invalid user local from 109.169.32.135 port 22
]: Failed password for nsharpe from 10.2.10.163 port 8317 ssh2
: Failed password for invalid user dean from 109.169.32.135 port 3822
: Failed password for invalid user operator from 109.169.32.135 port 22
: Failed password for invalid user itmadmin from 109.169.32.135 port 22
: Failed password for mail from 84.34.159.23 port 1190 ssh2
: Failed password for sync from 84.34.159.23 port 2530 ssh2
: Failed password for invalid user inet from 10.3.10.46 port 1516 ssh2
]: pam_unix(sshd:session): session closed for user myuan by (uid=0)
: Failed password for invalid user administrator from 10.3.10.46 port 22
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.14.14
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&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=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.14.14
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.14.14
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&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=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.14.14
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.14.14
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&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=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.14.14

FET Failed After More Lines Added


Trying to add an additional line and extracting *user* doesn't work

 The extraction failed. If you are extracting multiple fields, try removing one or more fields. Start with extractions that are embedded within longer text strings.

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 for the regular expression to match. Click on highlighted v

Wed Jun 08 2016 09:39:12 www1 sshd[4092]: Failed password for invalid user local from 109.169.32.135 port 2172 ssh2

 Wed Jun 08 2016 09:39:12 www1 sshd[38618]: Failed password for nsharpe from 10.2.10.163 port 8317 ssh2

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

130.60.4 - - [07/Jun 08 2016 09:39:12] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0; rv:53.0) Gecko/20100801 Firefox/53.0

My tool of choice: regex101.com

regular expressions 101 @regex101 donate contact bug reports & feedback wiki

SAVE & SHARE
save regex ⌘+S

FLAVOR
pcre (php) ✓
javascript
python
golang

TOOLS
code generator
regex debugger

REGULAR EXPRESSION no match
:// insert your regular expression here /g

TEST STRING SWITCH TO UNIT TESTS
insert your test string here

EXPLANATION
An explanation of your regex will be automatically generated as you type.

MATCH INFORMATION
Detailed match information will be displayed here automatically.

QUICK REFERENCE

SUBSTITUTION

Add the data and a regex

REGULAR EXPRESSION

:/ for (?P<user>\S+) from

TEST STRING

```
Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.2
Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user ad
Mon Jun 06 2016 02:29:44 www1 sshd[5001]: Failed password for invalid user ge
Mon Jun 06 2016 02:30:13 www1 sshd[1638]: pam_unix(sshd:session): session ope
Mon Jun 06 2016 02:30:13 www1 sshd[1480]: Failed password for invalid user yp
Mon Jun 06 2016 02:30:22 www1 sshd[2291]: Failed password for invalid user er
Mon Jun 06 2016 02:30:26 www1 sshd[4761]: Failed password for invalid user lo
Mon Jun 06 2016 02:30:50 www1 sshd[4986]: Failed password for invalid user my
Mon Jun 06 2016 02:31:19 www1 sshd[81145]: pam_unix(sshd:session): session op
Mon Jun 06 2016 02:31:19 www1 sshd[2021]: Failed password for myuan from 10.1
Mon Jun 06 2016 02:31:28 www1 sshd[1155]: Failed password for invalid user yp
Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.2
Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user ad
```

Refine the regex – better matches, but not all

REGULAR EXPRESSION

```
! / for (invalid user )?(?P<user>\S+) from
```

TEST STRING

```
Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.241.220.82 port 2253
Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user administrator from 12
Mon Jun 06 2016 02:29:44 www1 sshd[5001]: Failed password for invalid user george from 128.241.2
Mon Jun 06 2016 02:30:13 www1 sshd[1638]: pam_unix(sshd:session): session opened for user djohns
Mon Jun 06 2016 02:30:13 www1 sshd[1480]: Failed password for invalid user yp from 128.241.220.8
Mon Jun 06 2016 02:30:22 www1 sshd[2291]: Failed password for invalid user email from 128.241.22
Mon Jun 06 2016 02:30:26 www1 sshd[4761]: Failed password for invalid user local from 128.241.22
Mon Jun 06 2016 02:30:50 www1 sshd[4986]: Failed password for invalid user mysql from 128.241.22
Mon Jun 06 2016 02:31:19 www1 sshd[81145]: pam_unix(sshd:session): session opened for user djohr
Mon Jun 06 2016 02:31:19 www1 sshd[2021]: Failed password for myuan from 10.1.10.172 port 4468 s
Mon Jun 06 2016 02:31:28 www1 sshd[1155]: Failed password for invalid user yp from 10.1.10.172 p
Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.241.220.82 port 2253
Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user administrator from 12
Mon Jun 06 2016 02:29:44 www1 sshd[5001]: Failed password for invalid user george from 128.241.2
Mon Jun 06 2016 02:30:13 www1 sshd[1638]: pam_unix(sshd:session): session opened for user djohns
Mon Jun 06 2016 02:30:13 www1 sshd[1480]: Failed password for invalid user yp from 128.241.220.8
Mon Jun 06 2016 02:30:22 www1 sshd[2291]: Failed password for invalid user email from 128.241.22
Mon Jun 06 2016 02:30:26 www1 sshd[4761]: Failed password for invalid user local from 128.241.22
Mon Jun 06 2016 02:30:50 www1 sshd[4986]: Failed password for invalid user mysql from 128.241.22
Mon Jun 06 2016 02:31:19 www1 sshd[81145]: pam_unix(sshd:session): session opened for user diohr
```


And FINALLY – we got them all

Four different formats – all four user field types found!

REGULAR EXPRESSION

```
:/ ((for ((invalid user ))|(user ))?)|(sudo: ))(?P<user>\S+) (from|by)?
```

TEST STRING

```
Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user administrator from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:29:44 www1 sshd[5001]: Failed password for invalid user george from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:30:13 www1 sshd[1638]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Mon Jun 06 2016 02:30:13 www1 sshd[1480]: Failed password for invalid user yp from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:30:22 www1 sshd[2291]: Failed password for invalid user email from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:30:24 www1 sudo: djohnson ; TTY=pts/0 ; PWD=/home/djohnson ; USER=root ; COMMAND=/bin/bash
Mon Jun 06 2016 02:30:26 www1 sshd[4761]: Failed password for invalid user local from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:30:50 www1 sshd[4986]: Failed password for invalid user mysql from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:31:19 www1 sshd[81145]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Mon Jun 06 2016 02:31:19 www1 sshd[2021]: Failed password for myuan from 10.1.10.172 port 4468 ssh2
Mon Jun 06 2016 02:31:28 www1 sshd[1155]: Failed password for invalid user yp from 10.1.10.172 port 1821 ssh2
Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.241.220.82 port 2253 ssh2
```




How'd He Do That?

Tricks for getting it right

One named capture group with a single name

More than one instance of the same name will fail

- ▶ (for invalid user (?P<user>\S+))|(for (?P<user>\S+))
- ▶ Capture group names must be unique:

EXPLANATION

▼ / (for invalid user (?P<user>\S+))|(for (?P<user>\S+)) / g

All the errors detected are listed below, from left to right, as they appear in the pattern.

(?P<user> A subpattern name must be unique

) A subpattern name must be unique

How do you eat an elephant?

Bite by bite is better than trying to stuff the whole elephant in your mouth at once

- ▶ Start with one format
- ▶ Try to find similarities and differences between the formats
- ▶ Add a new format to your data and check your updated regex
- ▶ Keep a copy of the last one that worked!!
- ▶ Add additional formats and check ALL matches for ALL examples

```
130.60.4 - - [07/Jan 18:10:57:123] "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-SW-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://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
317.27.160.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D18L9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D55L7FF6ADFF0 HTTP/1.1"
200.131.200.198 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=KQ-CW-01"
125.17.14.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D18L9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=KQ-CW-01"
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 468 125.17.14.1 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D18L9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=KQ-CW-01"
```

Alternate: Do one for each format

Then you can try combining

- ▶ This can be more difficult with simpler regexes
- ▶ Can be easier for more complex regexes
- ▶ Combine two of the regexes that are similar
- ▶ Try to keep the things that are the same in both, making the changes to the original only where there is a difference
- ▶ Remember – **ONE instance of a name per regex**



Use Parentheses!

Make it easier to come back to later

((for ((invalid user)|(user))?)(sudo:))(?P<user>\S+) (from|by)?

- ▶ Using parentheses for clarity is helpful:
- ▶ They make it possible to see the separate parts and their relationships with each other
- ▶ Don't overdo the parentheses



Use the Best Character Class

Use the right tool for the job

- ▶ Sometimes a field regex must be able to match data that hasn't been seen in the data yet, so in this case **be as general as possible**
- ▶ In the previous example, the **\S** is best because **\s** will be the delimiter (a space in this case) because you want to catch any potential case that you don't see in the data, yet.

\S+

- ▶ If you have a delimiter that you can count on, use something like this to match the field value (**in this case be specific** about what it is NOT):

[^,]+

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=FI-SW-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.10) Gecko/20100101 Firefox/3.0.10" [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.10) Gecko/20100101 Firefox/3.0.10" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.10) Gecko/20100101 Firefox/3.0.10" [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.10) Gecko/20100101 Firefox/3.0.10" [07/Jan 18:10:55:188] "GET /category.action=remove&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.10) Gecko/20100101 Firefox/3.0.10"

If you have a definite delimiter, take advantage

Examples:

- ▶ Data: "contents of quoted string"
 - Use: "(?P<contents>[^\"]+)"

- ▶ Data: User:carypetterborg Dept:ICS
 - Use: User:(?P<user>\S+)\s

- ▶ Data: Salt Lake City, Utah 84117-6403
 - Use: ^(?P<city>[^,]+),\s+(?P<state>.\s+)\s+(?P<zip>[-\d]*)\$





REX and REGEX Commands

The most common use for regular expressions is in SPL with *rex* and *regex*

REX Example

`index=voice sourcetype=voice* Description | rex "Description=(?P<description>[^\^]+)"
| rex field=description "From (?P<start>.+) to (?P<end>.+?):\s"`

Aug 2 20:32:28 I13772 CPCMI13772: %local7-2-ALARM: 16\$Description= Number of AuthenticationFailed events exceeds configured threshold during configured interval of time 1 within 3 minutes on cluster StandAloneCluster. There are 2 AuthenticationFailed events (up to 30) received during the monitoring interval From **Wed Aug 03 10:25:00 PHT 2016** to **Wed Aug 03 10:28:00 PHT 2016**: TimeStamp : 8/3/16 10:26 AM LoginFrom : 172.12.34.40 Interface : VMREST UserID : JacobMD AppID : Cisco Tomcat ClusterID : NodeID : APPHMANAOVM001 TimeStamp : Wed Aug 03 10:26:13 PHT 2016 TimeStam::Status=2,cleared^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime Collaboration^Private IP Address=172.16.17.24^Default Alarm Name=AuthenticationFailed^Managed Object=10.160.17.24^Managed Object Type=Unity Connection^MODE=2;Alarm ID=343815480^Component=10.160.17.24\x00000

REX Commands

It takes two:

- ▶ index=voice sourcetype=voice* Description
| rex "Description=(?P<description>[^\^]+)"
| rex field=description "From (?P<start>.+) to (?P<end>.+?):\s"

- ▶ SYNTAX:
| rex [field=*fieldname*] "regex"

- ▶ Also available:
| rex mode=sed

```
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=5D35L7FF6ADFF0 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 14.189 "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=5D185L9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=KQ-CB-01"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
action=purchase&is.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
```

First rex – get the description

REGULAR EXPRESSION

1 match, 23 steps (~5ms)

```
/ Description=(?P<description>[^\^]+)
```

/g

TEST STRING

SWITCH TO UNIT TESTS ▶

```
Aug  2 20:32:28 l13772 CPCML13772: %local7-2-ALARM: 16$Description= Number of
AuthenticationFailed events exceeds configured threshold during configured interval of
time 1 within 3 minutes on cluster StandAloneCluster. There are 2
AuthenticationFailed events (up to 30) received during the monitoring interval From Wed
Aug 03 10:25:00 PHT 2016 to Wed Aug 03 10:28:00 PHT 2016:   TimeStamp : 8/3/16 10:26 AM
LoginFrom : 172.12.34.40 Interface : VMREST UserID : JacobMD AppID : Cisco Tomcat
ClusterID : NodeID : APPHMANAOVM001 TimeStamp : Wed Aug 03 10:26:13 PHT 2016
TimeStam::Status=2,cleared^Severity=minor^Acknowledged=no^CUSTOMER=Cisco Prime
Collaboration^Private IP Address=172.16.17.24^Default Alarm
Name=AuthenticationFailed^Managed Object=10.160.17.24^Managed Object Type=Unity
Connection^MODE=2;Alarm ID=343815480^Component=10.160.17.24\x00000
```

Second rex – get the Start and End

REGULAR EXPRESSION 1 match, 1016 steps (~16ms)

```
:/ From (?P<start>.+ ) to (?P<end>.+?):\s /g
```

TEST STRING SWITCH TO UNIT TESTS ▶

```
Number of AuthenticationFailed events exceeds configured threshold
during configured interval of time 1 within 3 minutes on cluster
StandAloneCluster. There are 2 AuthenticationFailed events (up to 30)
received during the monitoring interval From Wed Aug 03 10:25:00 PHT
2016 to Wed Aug 03 10:28:00 PHT 2016: TimeStamp : 8/3/16 10:26 AM
LoginFrom : 172.12.34.40 Interface : VMREST UserID : JacobMD AppID :
Cisco Tomcat ClusterID : NodeID : APPHMANAOVM001 TimeStamp : Wed Aug
03 10:26:13 PHT 2016 TimeStam::Status=2,cleared
```


Regex example

Only get events with internal addresses

New Search Save As Close

sourcetype="linux_secure" | regex "10\.\\d+\\.\\d+\\.\\d+\\.\\d+" All time Q

✓ 289 events (before 7/17/17 1:20:53.000 PM) No Event Sampling Job || ■ ↶ ↷ ⬇ Smart Mode

Events (289) Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection × Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields	f	Time	Event
Selected Fields a host 1 a source 1 a sourcetype 1	>	6/8/16 9:39:12.000 AM	Wed Jun 08 2016 09:39:12 www1 sshd[38618]: Failed password for nsharp from 10.2.10.163 port 8317 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
Interesting Fields # date_hour 17 # date_mday 3 # date_minute 55 a date_month 1 # date_second 59 a date_wday 3 # date_year 1 a date_zone 1 a index 1	>	6/8/16 2:14:45.000 AM	Wed Jun 08 2016 02:14:45 www3 sshd[3957]: Failed password for invalid user inet from 10.3.10.46 port 1516 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
	>	6/8/16 2:14:41.000 AM	Wed Jun 08 2016 02:14:41 www3 sshd[4461]: Failed password for invalid user administrator from 10.3.10.46 port 2108 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
	>	6/8/16 2:14:23.000 AM	Wed Jun 08 2016 02:14:23 www3 sshd[3256]: Failed password for invalid user jetty from 10.3.10.46 port 3759 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
	>	6/8/16 2:13:52.000 AM	Wed Jun 08 2016 02:13:52 www3 sshd[4725]: Failed password for invalid user ubuntu from 10.3.10.46 port 4940 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
	>	6/8/16 2:13:48.000 AM	Wed Jun 08 2016 02:13:48 www3 sshd[5405]: Failed password for invalid user oracle from 10.3.10.46 port 4544 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
	>	6/8/16 2:13:48.000 AM	Wed Jun 08 2016 02:13:48 www3 sshd[68976]: Accepted password for djohnson from 10.3.10.46 port 1790 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure
	>	6/8/16 2:13:20.000 AM	Wed Jun 08 2016 02:13:20 www3 sshd[58151]: Failed password for djabbar from 10.3.10.46 port 3715 ssh2 host = Carys-MacBook-Pro-2.local source = secure.log sourcetype = linux_secure

Breakdown

- ▶ Search:
`sourcetype=linux_secure | regex "10\.\d+\.\d+\.\d+"`
- ▶ Only internal (10.*) IP addresses make it through the **regex** filter
- ▶ Search produces events, regex then limits those results passed on through the pipeline by a fancy regular expression
- ▶ *Yes, there are other ways to do this, but this is a regex example*



Rex vs Regex

- ▶ Use **rex** to extract fields
- ▶ Use **regex** to limit results
- ▶ Yes, you can use them in the same search:

```
sourcetype=linux_secure | rex "from (?P<src_ip>\d+\.\d+\.\d+\.\d+)" | regex  
src_ip="(?!10)\.\d+\.\d+\.\d+"
```





Index Time Regular Expression Usage

The Problem

- ▶ You can't index Social Security Numbers
- ▶ How do you distinguish a Social Security Number from other numbers?
- ▶ Obfuscate ONLY SSNs, but leave other things alone.



SSN vs Phone

Regex distinctions

SSN

▶ 123-45-6789

▶ `\d{3}-\d{2}-\d{4}`

Phone

▶ 800-123-4567

▶ `\d{3}-\d{3}-\d{4}`

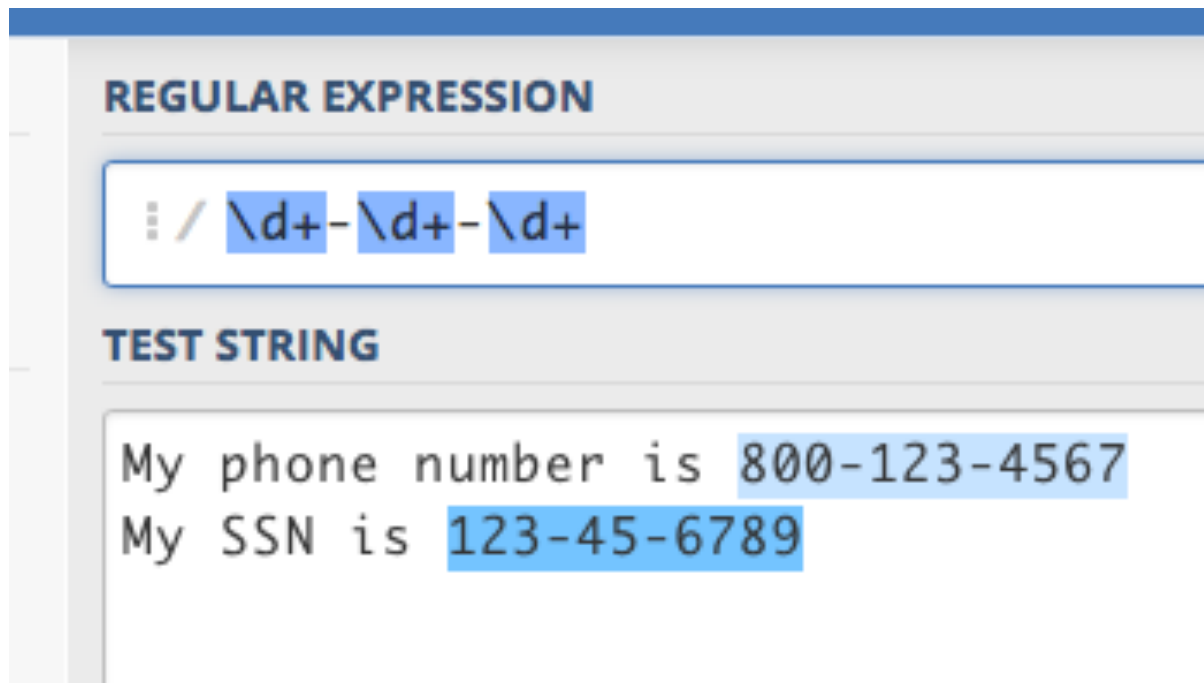


Be as specific in your matches as possible

- ▶ You could use something simple like:

`\d+-\d+-\d+`

- ▶ But it will mistake a phone number for a SSN:



A Better Match

- ▶ New regex:

`\d+-\d\d-\d+`

- ▶ Gets rid of Phone #'s, but what about other data?

REGULAR EXPRESSION

`:/ \d+-\d\d-\d+`

TEST STRING

My phone number is 800-123-4567
My SSN is 123-45-6789
My birthday is 12-25-1960
I need part # 71-34-912

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-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-268product_id=K0-CW-01"
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"
10.55.187.1 - - [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=purchase&itemId=EST-268product_id=K0-CW-01"
10.55.187.1 - - [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=purchase&itemId=EST-268product_id=K0-CW-01"

We're now so close

- ▶ This is exactly what a properly formatted SSN looks like:

`\d{3}-\d{2}-\d{4}`

- ▶ This defines a SSN, but it matches other things, too:

The screenshot shows a web-based interface for testing regular expressions. It has two main sections: 'REGULAR EXPRESSION' and 'TEST STRING'. In the 'REGULAR EXPRESSION' section, the text `\d{3}-\d{2}-\d{4}` is entered and highlighted in blue. In the 'TEST STRING' section, there are four lines of text: 'My phone number is 800-123-4567', 'My SSN is 123-45-6789', 'My birthday is 12-25-1960', and 'I need part # 8871-34-91268'. The SSN '123-45-6789' and the part number '8871-34-91268' are highlighted in blue, demonstrating that the regex matches any three-digit number followed by a hyphen, two digits, another hyphen, and four digits.

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-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CW-01"
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"
10.55.187.1 - - [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-108"
10.55.187.1 - - [07/Jan 18:10:55:188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-108"

Let's get REAL specific

- ▶ Best definition:

`(?<!\d)(?P<ssn>\d{3}-\d{2}-\d{4})(?!\\d)`

- ▶ The SSN match can be found *anywhere* in the event, and only the SSN:

The screenshot shows a Splunk interface with a 'REGULAR EXPRESSION' field containing the regex `(?<!\d)(?P<ssn>\d{3}-\d{2}-\d{4})(?!\\d)`. Below it, the 'TEST STRING' field contains several lines of text. The SSN '123-45-6789' and '987-65-4321' are highlighted in green, indicating a successful match. The other lines, 'My phone number is 800-123-4567.' and 'My birthday is 12-25-1960.', are not highlighted.

```
REGULAR EXPRESSION
: / (?<!\d)(?P<ssn>\d{3}-\d{2}-\d{4})(?!\\d)

TEST STRING
My phone number is 800-123-4567.
My SSN is 123-45-6789.
My birthday is 12-25-1960.
I need part # 8871-34-91268.
987-65-4321
```

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-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=5D15L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
10.0.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-3"
10.0.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-3"
10.0.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-3"
10.0.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-3"
```

So let's make it work in transforms.conf

- ▶ Grab the beginning and ending text of the event:

```
(.*)(?<!\d)(\d{3}-\d{2}-\d{4})(?!\\d)(.*)
```

The screenshot shows a Splunk interface with a 'REGULAR EXPRESSION' field containing the regex `:/ (.*)(?<!\d)(\d{3}-\d{2}-\d{4})(?!\\d)(.*)`. Below it, the 'TEST STRING' field contains the text: `My phone number is 800-123-4567.
My SSN is 123-45-6789.
My birthday is 12-25-1960.
I need part # 8871-34-91268.
987-65-4321`. The regex highlights the phone number, SSN, and birthday in the test string.

Index-time conversion

Conditions and Limitations

- ▶ This regex can't be done with SEDCMD in props.conf alone
 - The regex uses regex features not found in SED format
- ▶ Using a simple custom sourcetype, but it can be made a general transform
- ▶ Must capture all parts of the event.
- ▶ Will obfuscate only one SSN per event.



The transforms.conf

[nossn]

REGEX=(?m)(.*)(?<!\d)(\d{3}-\d{2}-\d{4})(?!\\d)(.*)

FORMAT = \$1###-##-#####\$3

DEST_KEY = _raw

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
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-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
317.27.160.0 - - [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 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
10.0.55.187 - - [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&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"

New regex features shown

- ▶ **(?m)** – perform the regex on multi-line events
- ▶ **(?<!\\d)** - Negative Lookbehind – *not preceded by a digit* – no net character
- ▶ **(?!\\d)** – Negative Lookahead – *not followed by a digit* – no net character



How the FORMAT works

- ▶ **FORMAT = \$1###-##-###\$3**
- ▶ **\$1** and **\$3** are capture group matches – from **(.*)** at beginning and end
- ▶ **\$2** is not used in the FORMAT, but it's the capture group for the SSN – from:
(\d{3}-\d{2}-\d{4})



After bringing in the data:

List Format 20 Per Page

i	Time	Event
>	7/18/17 2:16:51.000 PM	###-###-#### host = Carys-MacBook-Pro-2.local source = ssn.log sourcetype = testssn
>	7/18/17 2:16:51.000 PM	I need part # 8871-34-91268. host = Carys-MacBook-Pro-2.local source = ssn.log sourcetype = testssn
>	7/18/17 2:16:51.000 PM	My birthday is 12-25-1960. host = Carys-MacBook-Pro-2.local source = ssn.log sourcetype = testssn
>	7/18/17 2:16:51.000 PM	My SSN is ###-###-####. host = Carys-MacBook-Pro-2.local source = ssn.log sourcetype = testssn
>	7/18/17 2:16:51.000 PM	My phone number is 800-123-4567. host = Carys-MacBook-Pro-2.local source = ssn.log sourcetype = testssn

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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=5D55L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
 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-16&product_id=RP-LI-02"
 10 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-189"



Greedy vs. Lazy Matches

Greedy vs Lazy

REGULAR EXPRESSION

`\\d+6`

TEST STRING

12345678901234567890

REGULAR EXPRESSION

`\\d+?6`

TEST STRING

12345678901234567890

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=F1-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CW-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
10.0.0.1:5V1: - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
10.0.0.1:5V1: - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"

What is the difference?

Subtle difference, but big effect

- ▶ **Greedy** – Grab as much as you can
- ▶ **Lazy** – Grab as little as you can
- ▶ The lazy match will continue only as far as it needs to, no further
 - `<.+?>` will match `<12345>`, while
 - `<.+>` will match both `<12345>` and `<12345><67890>`

SYNTAX: place a **?** After a ***** or **+**

The lazy match only goes to the first instance of a match following a multiple match



Greedy Example

```
REGULAR EXPRESSION  
:: / \((?P<cmd>.* )session|
```

```
led password for invalid user geo  
_unix(sshd:session): session open  
led password for invalid user yp  
led password for invalid user ema  
led password for invalid user loc  
led password for invalid user mys  
im_unix(sshd:session): session ope  
led password for myuan from 10.1.  
...
```

```
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=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-26&product_id=KQ-CU-01"  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1 "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-CU-01&JSESSIONID=5D185L9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"  
item_id=EST-16&product_id=RP-LI-02)" 0  
do?action=purchase&itemId=EST-16&product_id=RP-LI-02)" 0  
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02)" 0
```


Second Look - Greedy

REGULAR EXPRESSION 1 match, 689 steps (~31ms)

```
:/ From (?P<start>.+ ) to (?P<end>.+): \s
```

TEST STRING SWITCH TO UNIT TESTS >

```
Number of AuthenticationFailed events exceeds configured threshold during  
configured interval of time 1 within 3 minutes on cluster StandAloneCluster.  
There are 2 AuthenticationFailed events (up to 30) received during the  
monitoring interval From Wed Aug 03 10:25:00 PHT 2016 to Wed Aug 03 10:28:00  
PHT 2016: TimeStamp : 8/3/16 10:26 AM LoginFrom : 172.12.34.40 Interface :  
VMREST UserID : JacobMD AppID : Cisco Tomcat ClusterID : NodeID :  
APPHMANAOVM001 TimeStamp : Wed Aug 03 10:26:13 PHT 2016  
TimeStam::Status=2,cleared
```

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KV-CB-01" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0
317.27.160.0 - - [07/Jun 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=remove&itemId=EST-149" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0
10 - - [07/Jun 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=remove&itemId=EST-149" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0
10 - - [07/Jun 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=remove&itemId=EST-149" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0

Second Look - Lazy

REGULAR EXPRESSION 1 match, 1016 steps (~8ms)

/ From (?P<start>.+) to (?P<end>.+?): \s / g

TEST STRING SWITCH TO UNIT TESTS ▶

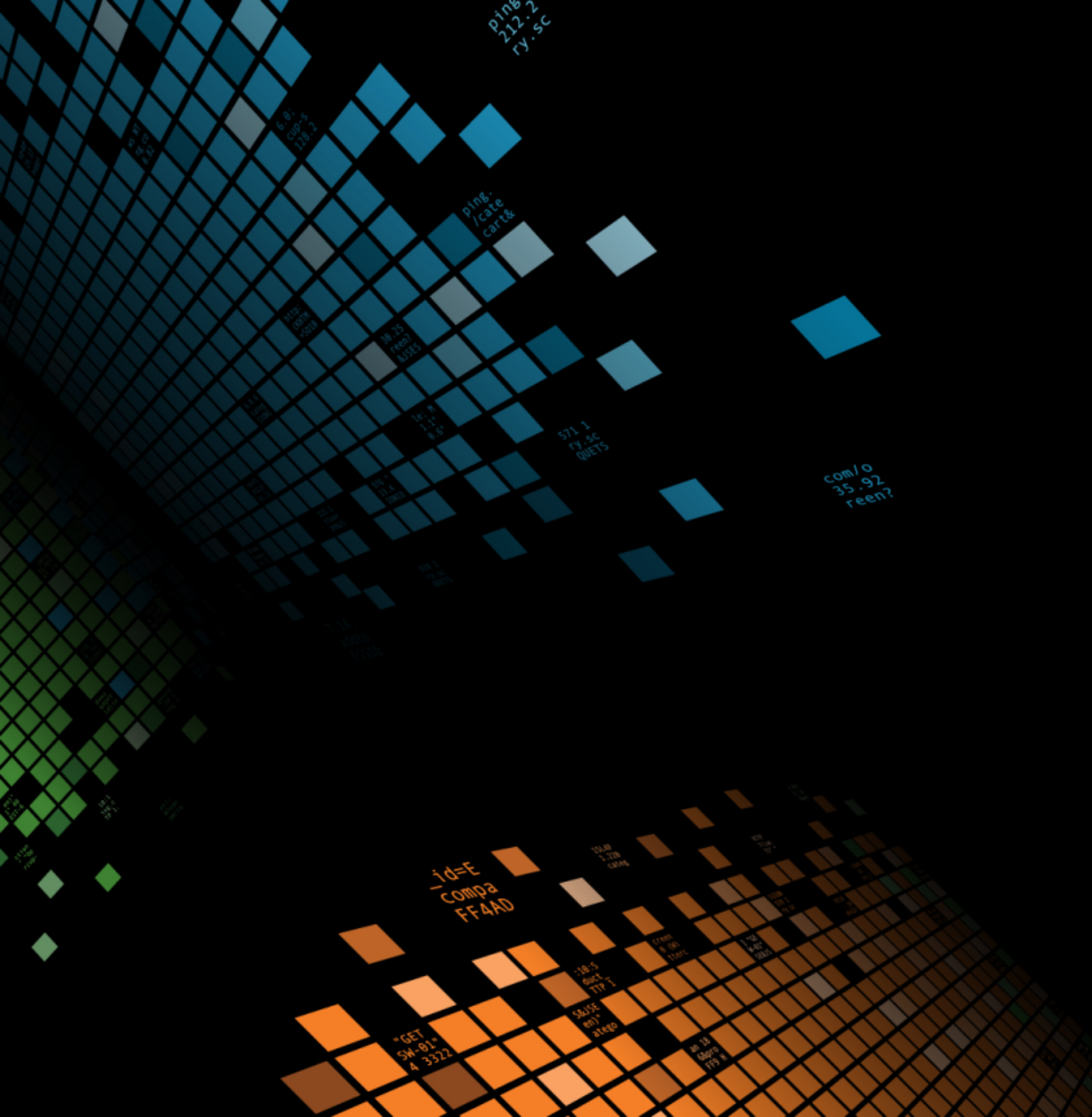
Number of AuthenticationFailed events exceeds configured threshold during configured interval of time 1 within 3 minutes on cluster StandAloneCluster. There are 2 AuthenticationFailed events (up to 30) received during the monitoring interval From Wed Aug 03 10:25:00 PHT 2016 to Wed Aug 03 10:28:00 PHT 2016: TimeStamp : 8/3/16 10:26 AM LoginFrom : 172.12.34.40 Interface : VMREST UserID : JacobMD AppID : Cisco Tomcat ClusterID : NodeID : APPHMANAOVM001 TimeStamp : Wed Aug 03 10:26:13 PHT 2016 TimeStamp::Status=2,cleared

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1

Choose Wisely

- ▶ Greedy may cross long segments
- ▶ Lazy may stop prematurely
- ▶ **Try it on various data sets** to make sure it will do what you want

```
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=FI-SW-01"
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"
ows NT 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=5D15L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-11&product_id=KQ-CW-01"
:/buttercup-shopping_id=RP-LI-02" 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-11&product_id=KQ-CW-01"
action=purchase&itemId=EST-11&product_id=KQ-CW-01" 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-11&product_id=KQ-CW-01"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=KQ-CW-01" 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-11&product_id=KQ-CW-01"
```



Embedding

Multiple field extractions from one piece of data

► Problem:

- Extract two different fields from the **exact same piece of data**
- Only want to use **one regex** – for efficiency if nothing else
- Need both the **Domain** only and the **whole URL** from an access log

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.130 Safari/537.36"
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" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.130 Safari/537.36"
ows NT 5.1; SV1; .NET CLR 1.1.4322)" "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 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.130 Safari/537.36"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14.1.1.1 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.130 Safari/537.36"
opping.com/cart.do?action=remove&itemId=EST-18" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.130 Safari/537.36"
```

Source and Results

► Data:

- 1501408932.060 16922 108.65.113.83 TCP_REFRESH_HIT/200 474 GET <http://damtare.by.ru/id.txt> myuan@buttercupgames.com DIRECT/damtare.by.ru text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-DefaultRouting <IW_scty,-6.9,0,-,-,-,-,0,-,-,-,-,-,-, IW_scty,-> - -

► Desired Fields:

- Domain: damtare.by.ru
- URL: <http://damtare.by.ru/id.txt>

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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&JSESSIONID=5D55L7FF6ADFF0 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
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"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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&JSESSIONID=5D55L7FF6ADFF0 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
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"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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&JSESSIONID=5D55L7FF6ADFF0 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
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"
```

Regex

REGULAR EXPRESSION

28 matches, 439 steps (~26ms)

:/ (?P<URL>http: \\ \\ (?P<domain> [^\\ /] +) \\ S +) / g

TEST STRING

SWITCH TO UNIT TESTS

1501400746.799 563 89.11.192.18 TCP_MISS/403 4206 GET http://www.hybridarcade.com/ pbunch@buttercupgames.com DIRECT/www.hybridarcade.com text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-DefaultRouting <IW_game,ns,0,-,-,-,0,-,-,-,-,IW_game,-> - - 1501401212.060 16922 173.192.201.242 TCP_REFRESH_HIT/200 474 GET http://damtare.by.ru/id.txt pcallahan@buttercupgames.com DIRECT/damtare.by.ru text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-DefaultRouting <IW_scty,-6.9,0,-,-,-,0,-,-,-,-,IW_scty,-> - - 1501402224.788 931 112.111.162.4 TCP_REFRESH_HIT/200 3227 GET http://www.goppo.com/ acurry@buttercupgames.com DIRECT/www.goppo.com text/html DEFAULT_CASE-DefaultGroup-

130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" Mozillia/7.0 "Comp... 128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=K9-CW-01" Mozilla/7.0 "Comp... 317 27.160.0.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 468 125.17 14... "/buttercup-shopping_id=RP-LI-02" "0-... /buttercup-shopping_id=RP-LI-02" "/buttercup-purchase&is.com/ol...

Regex101.com vs Splunk

- ▶ Slashes need escaping in regex101, but not in Splunk:

(?P<URL>http:**V**(?P<domain>[**^V**]+\b)\bS+)

VS

(?P<URL>http://(?P<domain>[**^/**]+\b)\bS+)



What? ... Oh, now I see.

(?P<URL>http://(?P<domain>[^/]+)\S+)

^

^

^

^

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=FI-5W-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1
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 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1
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" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1
100.100.100.100 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1
100.100.100.100 - - [07/Jan 18:10:55:188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1

Results in Splunk

You can't do this in the FET without doing your own regex!

Regular Expression

[Regular Expression Reference](#) [View in Search](#)

(?P<URL>http://(?P<domain>[^/]+\S+)

Preview

Save

Events	URL	domain
--------	-----	--------

✓ 30 events (before 8/31/17 4:37:35.000 PM)

Original search included:

20 per page

< Prev 1 2 Next >

filter

Apply

Sample: 1,000 events

All events

All Events

Matches

Non-Matches

_raw	URL	domain
✓	http://damtare.by.ru/id.txt	damtare.by.ru
✓	http://www.lowermybills.com/images/home_banner/home_auto_insurance.jpg	www.lowermybills.com
✓	http://www.lowermybills.com/dwr/engine.js	www.lowermybills.com
✓	http://www.lowermybills.com/dwr/interface/RemoteLogger.js	www.lowermybills.com
✓	http://www.lowermybills.com/	www.lowermybills.com
✓	http://damtare.by.ru/id.txt	damtare.by.ru

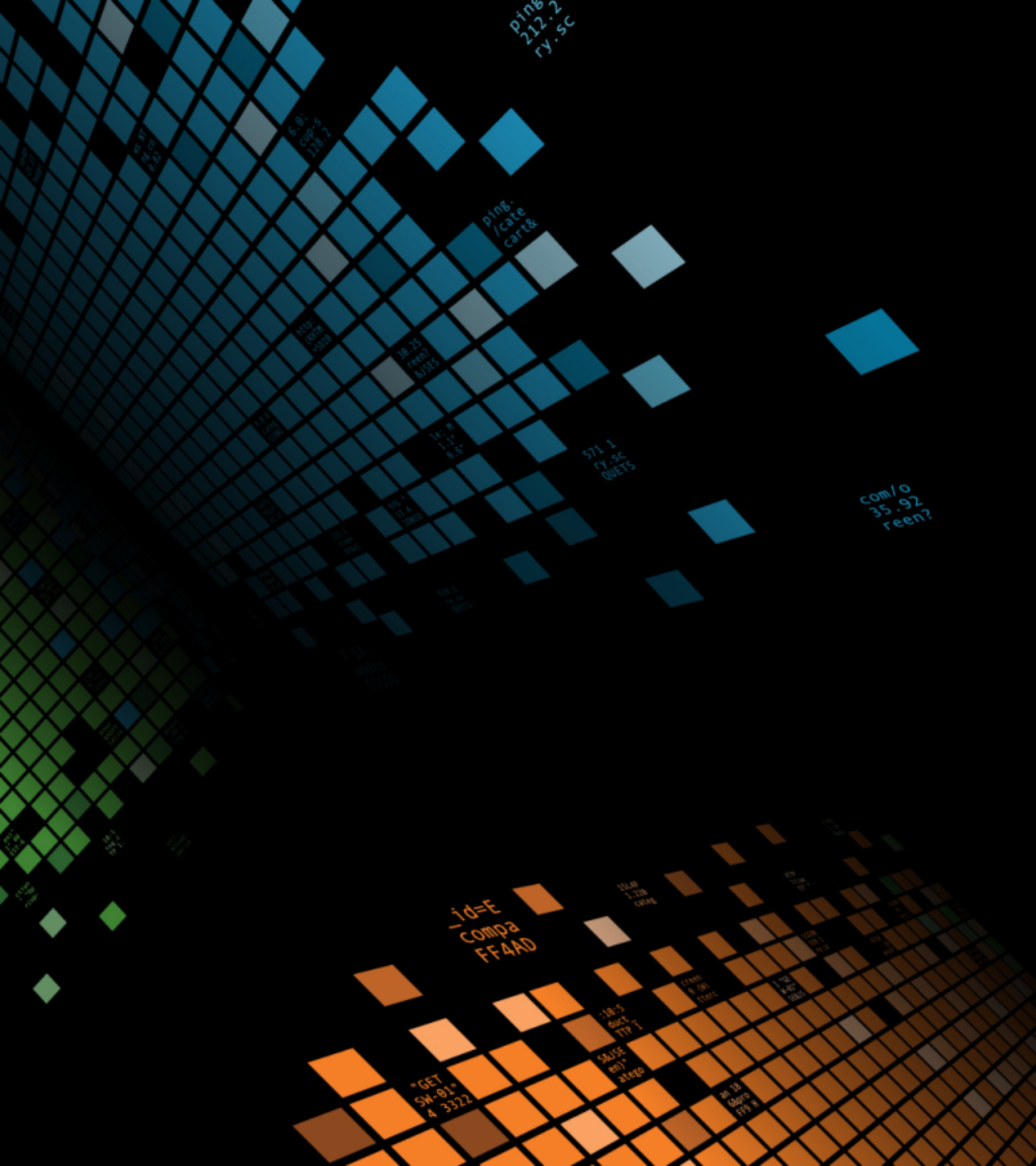


Other Notes

Performance Considerations

- ▶ Some complex field extractions can be costly
- ▶ Some complex regular expressions can be costly
- ▶ **Use the Job Inspector** to see if there is a difference in doing on complex field extraction vs many simple field extractions (| **rex** | **vs** | **rex** | **rex** | **rex**)
- ▶ **Sometimes the readability is more important** than the performance

```
130.60.4 ... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FFIA0FF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; 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=SD35L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=AV-CB-01&JSESSIONID=SD55L9FFIA0FF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L9FFIA0FF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.189 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FFIA0FF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L9FFIA0FF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
doaction=purchase&itemId=EST-16&product_id=RP-LI-02" 0 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FFIA0FF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.action=remove&itemId=EST-108" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
opping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 0 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FFIA0FF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.action=remove&itemId=EST-108" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
```

Tools

Regex101 Web Page

<http://regex101.com>

The screenshot displays the regex101.com interface. At the top, the site name "regular expressions 101" is visible. The main area is divided into three columns: "SAVE & SHARE" on the left, "REGULAR EXPRESSION" in the center, and "EXPLANATION" on the right. The "REGULAR EXPRESSION" column shows the pattern `i / ((for ((invalid user)|(user|sudo:))((sudo:)?P<user>S+) (from|by)?) /g` with 47 matches and 23269 steps. The "TEST STRING" column contains a log of SSH sessions with various users and actions. The "EXPLANATION" column details the structure of the regex, including capturing groups and alternatives. Below the explanation is a "MATCH INFORMATION" section showing the first two matches with their full matches and group contents. A "QUICK REFERENCE" section at the bottom right provides a search reference for various regex tokens.

REGULAR EXPRESSION
47 matches, 23269 steps (~22ms)
`i / ((for ((invalid user)|(user|sudo:))((sudo:)?P<user>S+) (from|by)?) /g`

TEST STRING
SWITCH TO UNIT TESTS

Mon Jun 06 2016 02:29:19 www1 sshd[3849]: Failed password for root from 128.241.220.82 port 2253 ssh2
Mon Jun 06 2016 02:29:24 www1 sshd[4267]: Failed password for invalid user administrator from 128.241.220.82 port 1715 ssh2
Mon Jun 06 2016 02:29:44 www1 sshd[5001]: Failed password for invalid user george from 128.241.220.82 port 2212 ssh2
Mon Jun 06 2016 02:30:13 www1 sshd[1638]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Mon Jun 06 2016 02:30:13 www1 sshd[1480]: Failed password for invalid user yp from 128.241.220.82 port 2808 ssh2
Mon Jun 06 2016 02:30:22 www1 sshd[2291]: Failed password for invalid user email from 128.241.220.82 port 4995 ssh2
Mon Jun 06 2016 02:30:26 www1 sshd[4761]: Failed password for invalid user local from 128.241.220.82 port 1271 ssh2
Mon Jun 06 2016 02:30:50 www1 sshd[4986]: Failed password for invalid user mysql from 128.241.220.82 port 2076 ssh2
Mon Jun 06 2016 02:31:19 www1 sshd[81145]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Mon Jun 06 2016 02:31:19 www1 sshd[2021]: Failed password for myuan from 10.1.10.172 port 4468 ssh2
Mon Jun 06 2016 02:31:28 www1 sshd[1155]: Failed password for invalid user yp from 10.1.10.172 port 1822 ssh2
Mon Jun 06 2016 02:31:32 www1 sshd[1632]: Failed password for invalid user elena_andubasquet from 10.1.10.172 port 2074 ssh2
Mon Jun 06 2016 02:31:54 www1 sshd[4333]: Failed password for root from 10.1.10.172 port 2772 ssh2
Mon Jun 06 2016 02:32:00 www1 sudo: djohnson ; TTY=pts/0 ; PWD=/home/djohnson ; USER=root ; COMMAND=/bin/su
Mon Jun 06 2016 02:32:00 www1 sshd[3697]: Failed password for invalid user whois from 10.1.10.172 port 1246 ssh2
Mon Jun 06 2016 02:32:19 www1 sshd[5985]: Failed password for invalid user testuser from 10.1.10.172 port 2597 ssh2
Mon Jun 06 2016 02:32:24 www1 sshd[3987]: Failed password for invalid user irc from 10.1.10.172 port 4012 ssh2
Mon Jun 06 2016 02:32:53 www1 sshd[1028]: Failed password for invalid user art from 10.1.10.172 port 1027 ssh2
Mon Jun 06 2016 02:33:15 www1 sshd[52866]: Server listening on :: port 22.
Mon Jun 06 2016 02:33:15 www1 sshd[4488]: Failed password for invalid user festina from 10.1.10.172 port 4216 ssh2

EXPLANATION

- 1st Capturing Group `((for ((invalid user)|(user|sudo:))((sudo:)?P<user>S+) (from|by)?)`
 - 1st Alternative `((for ((invalid user)|(user|sudo:))`
 - 2nd Capturing Group `((for ((invalid user)|(user|sudo:))`
 - 3rd Capturing Group `((invalid user)|(user|sudo:))`
- Quantifier — Matches between zero and one times, as many times as possible, giving back as needed (greedy)

MATCH INFORMATION

Match 1

Full match	58-71	`for root from`
Group 1.	58-62	`for `
Group 2.	58-62	`for `
Group `user`	62-66	`root`
Group 8.	67-71	`from`

Match 2

Full match	160-195	`for invalid user administrator from`
Group 1.	160-177	`for invalid user `
Group 2.	160-177	`for invalid user `
Group 3.	164-177	`invalid user `

QUICK REFERENCE

Search reference	a single character of: a, b or c <code>[abc]</code>
all tokens	a character except: a, b or c <code>[^abc]</code>
common tokens	a character in the range: a-z <code>[a-z]</code>
general tokens	a character not in the ran... <code>[^a-z]</code>
anchors	a character in the rang... <code>[a-zA-Z]</code>
meta sequences	any single character <code>.</code>
quantifiers	any whitespace character <code>\s</code>
group constructs	any non-whitespace character <code>\S</code>
character classes	any digit <code>\d</code>

Regexr Web Page

<http://regexr.com> - Doesn't do PCRE!!

The screenshot shows the RegExr v2.1 web interface. The top navigation bar includes the site name, user 'gskinner', and links for 'RegExr v1', 'GitHub', and 'Tutorial'. A sidebar on the left contains a 'Library' section with links to 'Help', 'Reference', 'Cheatsheet', 'Examples', 'Community', and 'Favourites'. The main content area features a text input field with the regex pattern `/((for ((invalid user)|(user)))|(sudo:))(\S+) (from|by)?/g`, which has 47 matches. Below the input is a 'Text' section displaying a list of log entries with the regex matches highlighted in blue. At the bottom, a 'Tools' section includes 'Replace', 'List', 'Details', and 'Explain' options, with a list of matches including 'root', 'administrator', 'george', 'djohnson', 'yp', 'email', 'local', 'mysql', 'djohnson', 'myuan', and 'vn'. A footer on the left contains a list of bullet points describing the tool's features.

RegExr v2.1 by gskinner RegExr v1 GitHub Tutorial

Library

- Help
- Reference
- Cheatsheet
- Examples
- Community
- Favourites

Expression share save flags

```
/((for ((invalid user)|(user)))|(sudo: ))(\S+) (from|by)?/g 47 matches
```

Text

```
Mon Jun 06 2016 11:04:54 www1 sudo: nsharpe ; TTY=pts/0 ; PWD=/home/nsharpe ; USER=root ; COMMAND=/bin/su
Mon Jun 06 2016 11:04:54 www1 sshd[2572]: Failed password for ncsd from 10.2.10.163 port 3894 ssh2
Mon Jun 06 2016 11:05:20 www1 sshd[3053]: Failed password for invalid user administrator from 10.2.10.163 port 1662
ssh2
Mon Jun 06 2016 11:06:12 www1 sshd[5350]: Failed password for invalid user administrator from 10.2.10.163 port 3666
ssh2
Mon Jun 06 2016 11:06:44 www1 sshd[4115]: Failed password for invalid user administrator from 10.2.10.163 port 3568
ssh2
Mon Jun 06 2016 11:07:24 www1 sshd[22652]: Accepted password for djohnson from 10.3.10.46 port 9128 ssh2
Mon Jun 06 2016 11:07:24 www1 sshd[5331]: Failed password for invalid user administrator from 10.2.10.163 port 4762
ssh2
```

Tools Replace List Details Explain

```
$? \n
root
administrator
george
djohnson
yp
email
local
mysql
djohnson
myuan
vn
```

RegExr is an online tool to learn, build, & test Regular Expressions (RegEx / RegExp).

- Results update in real-time as you type.
- Roll over a match or expression for details.
- Save & share expressions with others.
- Use Tools to explore your results.
- Browse the Library for help & examples.
- Undo & Redo with Cmd-Z / Y.
- Search for & rate Community patterns.

Just for fun:

Try your regex prowess

► Regex Golf

- <https://alf.nu/RegexGolf>
- <https://www.oreilly.com/learning/regex-golf-with-peter-norvig>

► Regex Crosswords

- <https://regexcrossword.com>
- <https://mariolurig.com/crossword/>



Splunk Answers and Docs

Learn from others – ask questions – get answers

► <http://answers.splunk.com/>

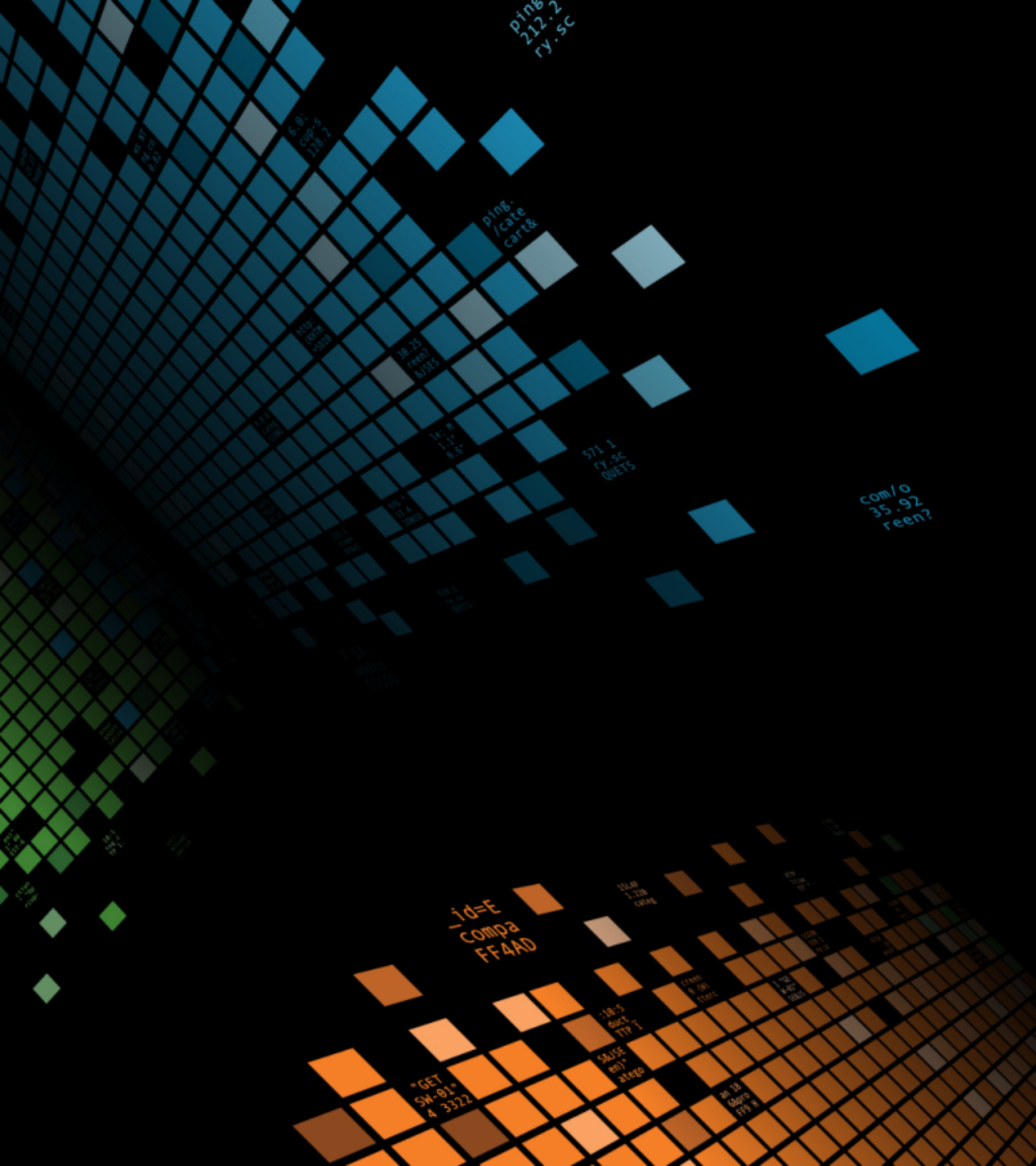
Splunk Documentation

► <https://docs.splunk.com/Documentation/Splunk/6.4.3/Knowledge/AboutSplunkregularexpressions>

► Splunk **regex** Slack channel

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-01"
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://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CU-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"
://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CU-01"
://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CU-01"
://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CU-01"

THE CHURCH OF
JESUS CHRIST
OF LATTER-DAY SAINTS



Questions?
