

Creating Field Extractions – Lab Guide

Overview

Welcome to the Splunk Education lab environment. These lab exercises will have you create Regular Expression (regex) field extractions and delimited field extractions.

Scenario

You will use data from the international video game company, Buttercup Games. A list of source types is provided below.

NOTE: This is a lab environment driven by data generators with obvious limitations. This is not a production environment. Screenshots approximate what you should see, not the **exact** output.

Index	Type	Sourcetype	Interesting Fields
web	Online sales	access_combined	<code>action, bytes, categoryId, clientip, itemId, JSESSIONID, price, productId, productName, referer, referer_domain, sale_price, status, user, userAgent</code>
games	Game logs	SimCubeBeta	<code>date_hour, date_mday, date_minute, date_month, date_second, data_wday, data_year, date_zone, eventtype, index, linecount, punct, splunk_server, timeendpos, timestampstartpos</code>

Lab Connection Info

Access labs using the server URL, user name, and password shown in your lab environment.

The screenshot shows a web interface for connecting to a lab environment. At the top, there are four buttons: 'SERVERS' (highlighted in pink), 'LAB DOCUMENT', 'CHECK MY WORK', and 'HELP'. Below these are sections for 'Lab Server Info' and 'Deployment Status'.

SERVER URL	PUBLIC IP	SPLUNK USER NAME	PASSWORD	DOWNLOAD	STATUS
https://11-195-15-aio.class.splunk.com	3.23.114.109	powerUser	wrarug8hlkozuBa	link	DEPLOYED

Common Commands and Functions

These commands and statistical functions are commonly used in searches but may not have been explicitly discussed in the module. Please use this table for quick reference. Click on the hyperlinked SPL to be taken to the Search Manual for that command or function.

SPL	Type	Description	Example
sort	command	Sorts results in descending or ascending order by a specified field. Can limit results to a specific number.	<i>Sort the first 100 src_ip values in descending order</i> <code>sort 100 -src_ip</code>
where	command	Filters search results using eval-expressions.	<i>Return events with a count value greater than 30</i> <code>where count > 30</code>
rename	command	Renames one or more fields.	<i>Rename SESSIONID to 'The session ID'</i> <code>rename SESSIONID as "The session ID"</code>
fields	command	Keeps (+) or removes (-) fields from search results.	<i>Remove the host field from the results</i> <code>fields - host</code>
stats	command	Calculates aggregate statistics over the results set.	<i>Calculate the total sales, i.e. the sum of price values</i> <code>stats sum(price)</code>
eval	command	Calculates an expression and puts the resulting value into a new or existing field.	<i>Concatenate first_name and Last_name values with a space to create a field called "full_name"</i> <code>eval full_name=first_name." ".last_name</code>
table	command	Returns a table.	<i>Output vendorCountry, vendor, and sales values to a table</i> <code>table vendorCountry, vendor, sales</code>
sum()	statistical function	Returns the sum of the values of a field. Can be used with <code>stats</code> , <code>timechart</code> , and <code>chart</code> commands.	<i>Calculate the sum of the bytes field</i> <code>stats sum(bytes)</code>
count_or_count()	statistical function	Returns the number of occurrences of all events or a specific field. Can be used with <code>stats</code> , <code>timechart</code> , and <code>chart</code> commands.	<i>Count all events as "events" and count all events that contain a value for action as "action"</i> <code>stats count as events, count(action) as action</code>

Refer to the [Search Reference Manual](#) for a full list of commands and functions.

Lab Exercise 1 – Create Regex Field Extractions

Description

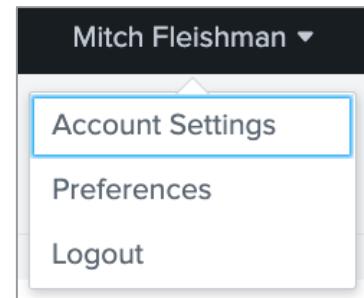
Configure the lab environment user account. Then, create field extractions based on Regular Expression (regex).

Steps

Task 1: Log into Splunk and change the account name and time zone.

Set up your lab environment to fit your time zone. This also allows the instructor to track your progress and assist you if necessary.

1. Log into your Splunk lab environment using the username and password provided to you.
2. You may see a pop-up window welcoming you to the lab environment. You can click **Continue to Tour** but this is not required. Click **Skip** to dismiss the window.
3. Click on the username you logged in with (at the top of the screen) and then choose **Account Settings** from the drop-down menu.
4. In the **Full name** box, enter your first and last name.
5. Click **Save**.
6. Reload your browser to reflect the recent changes to the interface. (This area of the web interface will be referred to as **user name**.)



After you complete step 6, you will see your name in the web interface.

NOTE: Sometimes there can be delays in executing an action like saving in the UI or returning results of a search. If you are experiencing a delay, please allow the UI a few minutes to execute your action.

7. Navigate to **user name > Preferences**.
8. Choose your local time zone from the **Time zone** drop-down menu.
9. Click **Apply**.
10. (Optional) Navigate to **user name > Preferences > SPL Editor > Search auto-format** and click on the toggle to activate auto-formatting. Then click **Apply**. When the pipe character is used in search, the SPL Editor will automatically begin the pipe on a new line.

index=web sourcetype=access_combined | stats count by action Last 24 hours

Search auto-format disabled (default)

index=web sourcetype=access_combined
| stats count by action Last 24 hours

Search auto-format enabled

Task 2: Use the Field Extractor (FX) to extract the IP address and transaction ID fields using the Regular Expression method.

11. Navigate to the search app by clicking **Apps > Search & Reporting** in the upper left corner of Splunk Web.

a. If a welcome message appears, click **Skip**.

12. Use this search to search the **web** index for all events in the **last 24 hours** for the **access_combined** sourcetype that contain the keyword **mobile**:

```
index=web sourcetype=access_combined mobile
```

13. View the event details to see all the extracted fields, by clicking the arrow (>) under the information icon (i) in the first event that contains an IP address value, a timestamp, and either a GET or POST operation

14. Click **Event Actions > Extract Fields**.

15. Configure a regular expression extraction method.

- Click on the **Regular Expression** selection.
- Click **Next** to begin selecting fields.

The screenshot shows the 'Extract Fields' interface with the 'Select Method' step selected. A sample event is shown in a code block:

```
91.199.80.24 - - [07/Jun/2022:16:49:22] "POST /cart/success.do?JSESSIONID=SD10SL3FF7ADFF206911 HTTP 1.1" 200 1881 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.46.3" 310
```

Two extraction methods are presented:

- Regular Expression:** Shows the pattern `(.*?)`. Description: Splunk Enterprise will extract fields using a Regular Expression.
- Delimiters:** Shows the pattern `x|y|z`. Description: Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

16. Add an extracted field for the IP address value.

- Highlight the IP address value, which appears as the very first field, in the sample event.
- In the **Field Name** field, type: `src`

NOTE: To view the pop-up box with the **Field Name** field, you may need to click on the highlighted IP address.

- Click **Add Extraction**.

The screenshot shows the 'Extract Fields' interface with the 'Select Fields' step selected. A sample event is shown in a code block:

```
91.199.80.24 - - [07/Jun/2022:16:49:22] "POST /cart/success.do?JSESSIONID=SD10SL3FF7ADFF206911 HTTP 1.1" 200 1881 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.46.3" 310
```

A tooltip for the `src` field is open, showing the **Field Name** as `src` and the **Sample Value** as `91.199.80.24`. The **Add Extraction** button is highlighted.

17. Scroll down to the **Preview** section and verify that the correct information is being extracted.

- Click **Matches** to verify results.

The screenshot shows the Splunk interface with the 'Preview' tab selected. At the top, there are buttons for 'filter', 'Apply', 'Sample: 1,000 events', 'All events', 'All Events', 'Matches' (which is highlighted with a red box), and 'Non-Matches'. Below these, a table displays two log entries:

	_raw	src
✓	91.199.80.24 - - [07/Jun/2022:16:49:22] "POST /cart/success.do?JSESSIONID=SD10SL3FF7ADFF206911 HTTP 1.1" 200 1881 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 310	91.199.80.24
✓	91.199.80.24 - - [07/Jun/2022:16:49:21] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD10SL3FF7ADFF206911 HTTP 1.1" 200 3955 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&category1=ACCESSORIES&productId=WC-SH-A02" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 473	91.199.80.24

- Click **Non-Matches** to verify any incorrect results. You should see "No results found."

The screenshot shows the Splunk interface with the 'Preview' tab selected. At the top, there are buttons for 'filter', 'Apply', 'Sample: 1,000 events', 'All events', 'All Events', 'Matches' (which is highlighted with a red box), and 'Non-Matches'. Below these, a message states: '✓ 438 events (3/9/22 12:00:00.000 AM to 6/7/22 12:04:50.000 PM)' and '20 per page ▾'. A message at the bottom says 'No results found.'

- Click **All Events**.

18. Back at the top of the screen under **Select Fields**, highlight the last number in the event.

- In the **Field Name** box, type: **transactionId**
- Click **Add Extraction**.

The screenshot shows the 'Select Fields' configuration page. It has a title 'Select Fields' and a note: '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 values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more ↗'. Below this, a sample event is shown: '91.199.80.24 - - [07/Jun/2022:16:49:22] "POST /cart/success.do?JSESSIONID=SD10SL3FF7ADFF206911 HTTP 1.1" 200 1881 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 310'. The 'transactionId' field is highlighted in blue. On the left, there are sections for 'S' (Selected Fields) and 'P' (Previously Selected). In the 'Selected Fields' section, there is a table with columns 'Field Name' (containing 'transactionId'), 'Sample Value' (containing '310'), and 'Actions' (containing 'Extract' and 'Require' buttons). A button 'Add Extraction' is also present. On the right, there is a note: 'Optional 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.' A 'View in Search' button is located at the bottom right.

19. Click on the **Show Regular Expression >** link to review the regex syntax.

- If the regular expression matches all events, it should look relatively simple in structure and looks similar to the highlighted expression below. **If this is the case, move on to step 20.**

The screenshot shows the regular expression editor with a 'Hide Regular Expression ▾' button. Below it is a text input field containing the regular expression: '^?P<src>[^]+)?(:[^"\n"]*)(6)\s+(?P<transactionId>.+)'. This expression is highlighted with a red box.

- b. In some cases, the regular expression does not match all events, resulting in a more complex and inaccurate regular expression:

- c. Scroll down to the Preview section and verify that not all events are matching correctly.

filter	Apply	Sample: 1,000 events ▾	All events ▾	All Events	Matches	Non-Matches
_raw ▾				src ▾		transactionId ▾
✓	211.25.254.234 - - [27/Jul/2021:08:34:54] "GET /oldlink?itemId=EST-16&JSESSIONID=SD0SL3FF4ADFF203410 HTTP 1.1" 200 2028 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5"	211.25.254.234	361			
✗	211.25.254.234 - - [27/Jul/2021:08:34:52] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD0SL3FF4ADFF203410 HTTP 1.1" 200 1457 "http://www.buttercupgames.com/category.screen?categoryId=ACCESSORIES" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 680					

- d. Add a missing sample event by hovering over an event that shows the missing red "x" symbol to the left and click + **Add sample event**.

✓	211.25.254.234 - - [27/Jul/2021:08:34:54] "GET /oldlink?itemId=EST-16&JSESSIONID=SD0SL3FF4ADFF203410 HTTP/1.1"	211.25.254.234	403 2028	"http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 361
✗	211.25.254.234 - - [27/Jul/2021:08:34:52] "GET /category.screen?			+ Add sample event

- e. In the newly added sample event, which now appears towards the top of the screen, highlight the IP address value.

 - In the **Field Name** box, under the **Select a Field** drop-down list, select **src**.
 - Click **Add Extraction**.

211.25.254.234	- - [27/Jul/2021:08:34:54] "GET /oldlink?itemId=EST-16&JSESSIONID=SD0SL3FF4ADFF203410 HTTP 1.1" 403 2028
"http://www.buttercupgames.com/product.screen?productId=SFBVS-G01"	"Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en- (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 361
211.25.254.234	- - [27/Jul/2021:08:34:52] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD0SL3FF4ADFF203410 H
Field Name	Select a Field ▾
Sample Value	src transactionId
	<input type="button" value="Add Extraction"/>

- f. In the second sample event, highlight the last number.

 - Verify that the **Field Name** lists transactionId.
 - Click **Add Extraction**.

20. Scroll down to the **Preview** section and verify that the correct information is being extracted.

 - Click **Matches** to verify results.
 - Click **Non-Matches** to verify that it returns with “No results found”.

NOTE: If there are any results under **Non-Matches**, repeat steps 19c to 19f, until there are no results under **Non-Matches**.

 - Click **Next** to proceed to validate the extracted fields.

21. In the **Validate** step, click on the **Show Regular Expression >** link (if it is hidden) and look at the syntax. Then click **Next**.

22. Review the **Extraction Name** and click **Finish**.

NOTE: If there are any results under **Non-Matches**, repeat steps 19c to 19f, until there are no results under **Non-Matches**.

- c. Click **Next** to proceed to validate the extracted fields.

Save

Name the extraction and set permissions.

Extractions Name	EXTRACT-	src,transactionId	
Owner	poweruser		
App	search		
Permissions	Owner	App	All apps
<hr/>			
Source type	access_combined		
Sample event	91.199.80.24 - - [07/Jun/2022:16:49:22] "POST /cart/success.do?JSESSIONID=SD10SL3FF7ADFF206911 HTTP/1.1" 200 1881 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 310		
Fields	src,transactionId		
Regular Expression	^(?P<src>[^]+)(?:[^"\n"]"(6)\s+(?P<transactionId>.+)?)		

23. On the final **Success!** screen, click on **Explore the fields I just created in Search.**

- In the Fields sidebar, under **Interesting Fields**, verify that your newly added fields appear (**src** and **transactionId**).
- Click on the **src** field to explore the values.

Top 10 Values	Count	%
211.166.11.101	132	2.477%
87.194.216.51	129	2.421%
109.169.32.135	107	2.008%
175.44.24.82	77	1.445%
91.205.189.27	73	1.37%
195.216.243.24	72	1.351%
209.114.36.109	70	1.314%
210.192.123.204	69	1.295%
194.146.236.22	67	1.258%
196.28.38.71	61	1.145%

24. Search for events in the **access_combined** sourcetype in the **last 24 hours**. List the top **transactionId**'s by IP address using this search:

```
index=web sourcetype=access_combined | top transactionId by src
```

src	transactionId	count	percent
107.3.146.207	972	1	2.127660
107.3.146.207	928	1	2.127660
107.3.146.207	904	1	2.127660
107.3.146.207	876	1	2.127660
107.3.146.207	831	1	2.127660
107.3.146.207	785	1	2.127660

25. Save your search as a report with the name **L1S1**.

- Click **Save As > Report**
- For **Title**, enter **L1S1**.
- Save**.
- You can **View** your report or exit out of the **Your Report Has Been Created** window by clicking the **X** in the upper-right corner.
- You can access your saved reports using the **Reports** tab in the application bar.

The screenshot shows the Splunk interface with the 'Reports' tab selected. At the top, there are navigation links: Search, Analytics, Datasets, Reports (highlighted in green), Alerts, and Dashboards. To the right is a search bar labeled 'Search & Reporting' with a magnifying glass icon.

The main area is titled 'Reports' and contains a message: 'Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.' Below this is a table titled '6 Reports'.

The table has columns: i, Title (sorted by title), Actions, Next Scheduled Time, Owner, App, and Sharing. The rows list the following reports:

i	Title	Actions	Next Scheduled Time	Owner	App	Sharing
>	Bucket Merge Retrieve Conf Settings	Open in Search Edit	None	nobody	search	App
>	Errors in the last 24 hours	Open in Search Edit	None	nobody	search	App
>	Errors in the last hour	Open in Search Edit	None	nobody	search	App
>	L1S1	Open in Search Edit	None	poweruser	search	Private
>	License Usage Data Cube	Open in Search Edit	None	nobody	search	App
>	Orphaned scheduled searches	Open in Search Edit	None	nobody	search	App

A note at the bottom states: 'Your recently saved L1S1 report will be visible in the Reports tab.'

Lab Exercise 2 – Create Delimited Field Extractions

Description

This lab exercise walks you through the process of creating delimited field extractions. Additionally, field extractions based on Regular Expression (regex) are used to capture additional fields.

Steps

Scenario: The engineering team launched the beta of a new game called SimCube. To make improvements to the game, engineers want to see how users are playing the game. However, the log file doesn't contain headers and the fields are not automatically extracted.

Task 1: Use the Field Extractor (FX) to extract fields using the delimiters method.

1. Re-initialize the search window by clicking **Search** in the application bar.
 2. Search for all events in the **last 30 days** for the SimCubeBeta sourcetype in the games index using this search:

index=games sourcetype=SimCubeBeta

- a. Click the arrow (>) under the information icon (**i**) in the first event to see which fields are extracted.

i	Time	Event																
	6/7/22 1:12:09.000 PM	07/Jun/2022:19:12:09 , 148.107.2.20 , v2.003B , User:'tmcbrean@mhcable.com' CharacterName:'Kooby' Action:'Joined Union' CurrentStanding:'Office Joke'																
▼ <div style="display: flex; align-items: center;"> Event Actions ▾ </div>																		
	<div style="border: 1px solid #ccc; padding: 5px; width: 150px;"> Type <input checked="" type="checkbox"/> Field Selected <input checked="" type="checkbox"/> host ▾ <input checked="" type="checkbox"/> source ▾ <input checked="" type="checkbox"/> sourcetype ▾ Time <input style="border: none; border-bottom: 1px solid #ccc; padding: 0 5px;" type="button" value="time"/> <input style="border: none; border-bottom: 1px solid #ccc; padding: 0 5px;" type="button" value="ago"/> Default <input type="checkbox"/> index ▾ <input type="checkbox"/> linecount ▾ <input type="checkbox"/> punct ▾ </div>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 5px;">Value</th> <th style="text-align: right; padding: 5px;">Actions</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">sim_cube_server</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> <tr> <td style="padding: 5px;">/opt/log/SIMlog/simgame.log</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> <tr> <td style="padding: 5px;">SimCubeBeta</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> <tr> <td style="padding: 5px;">2022-06-07T13:12:09.000-06:00</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> <tr> <td style="padding: 5px;">games</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> <tr> <td style="padding: 5px;">1</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> <tr> <td style="padding: 5px;">://...-...-'@!`"!_!`!</td> <td style="text-align: right; padding: 5px;">▼</td> </tr> </tbody> </table>	Value	Actions	sim_cube_server	▼	/opt/log/SIMlog/simgame.log	▼	SimCubeBeta	▼	2022-06-07T13:12:09.000-06:00	▼	games	▼	1	▼	://...-...-'@!`"!_!`!	▼
Value	Actions																	
sim_cube_server	▼																	
/opt/log/SIMlog/simgame.log	▼																	
SimCubeBeta	▼																	
2022-06-07T13:12:09.000-06:00	▼																	
games	▼																	
1	▼																	
://...-...-'@!`"!_!`!	▼																	

3. In the Fields sidebar, underneath the **Interesting Fields** section, click **+ Extract New Fields**.
 - a. On the **Select Sample Event** screen, click the first event to select it as a sample event.

Events
✓ 172 events (3/9/22 12:00:00.000 AM to 6/7/22 1:15:19.000 PM)
20 per page ▾
< Prev
1 2 3 4 5 6 7 8 9 Next >
<input type="button" value="filter"/> <input type="button" value="Apply"/> Sample: 1,000 events ▾ <input type="button" value="All events"/>
_raw ▾
07/Jun/2022:19:12:09 , 148.107.2.20 , v2.003B , User:'tmcbreen@mhcable.com' CharacterName:'Kooby' Action:'Joined Union' CurrentStanding:'Office Joke'
07/Jun/2022:19:11:08 , 121.9.245.177 , v2.002B , User:'danny_girl8@hotmail.com' CharacterName:'pixie' Action:'Promoted' CurrentStanding:'Supervisor'
07/Jun/2022:19:11:06 , 128.241.220.72 , v2.002B , User:'kealvhoghart@live.com' CharacterName:'madtoker' Action:'Made Deadline' CurrentStanding:'Worker'

- b. Verify that the event now appears towards the top as a sample event.

The screenshot shows a Splunk search interface. At the top, it says "Source type SimCubeBeta" and "Time Range Last 90 days". Below this, there is a single event listed in a dark blue box:

```
07/Jun/2022:19:12:09 , 148.107.2.20 , v2.003B , User:'tmcbreen@mhcable.com' CharacterName:'Kooby' Action:'Joined Union' CurrentStanding:'Office Joke'
```

NOTE: The first few fields for this sourcetype appear to be separated with a comma symbol (,). This includes a timestamp, an IP address (in IP version 4 format), a software version (for example "v2.002B"), and then some miscellaneous information.

The miscellaneous information at the end of the event appears to be separated by spaces, which includes fields such as the **User**, **CharacterName**, **Action**, and **CurrentStanding**.

- c. Click the **Next** button at the top of the screen.
4. Select the **Delimiters** method and click **Next**.
a. For the **Delimiter type**, select **Comma**.

The screenshot shows the "Rename Fields" page. It has a "Delimiter" section with tabs for Space, Comma (which is selected and highlighted in blue), Tab, Pipe, and Other. Below this, there are four fields labeled field1, field2, field3, and field4. Under each field is its corresponding value from the event: 07/Jun/2022:19:12:09, 148.107.2.20, v2.003B, and User:'tmcbreen@mhcable.com' CharacterName:'Kooby' Action:'Joined Union' CurrentStanding:'Office Joke'.

- b. Rename all the fields as follows (in this order):
– field1 > **time**
– field2 > **src**
– field3 > **version**
– field4 > **misc**

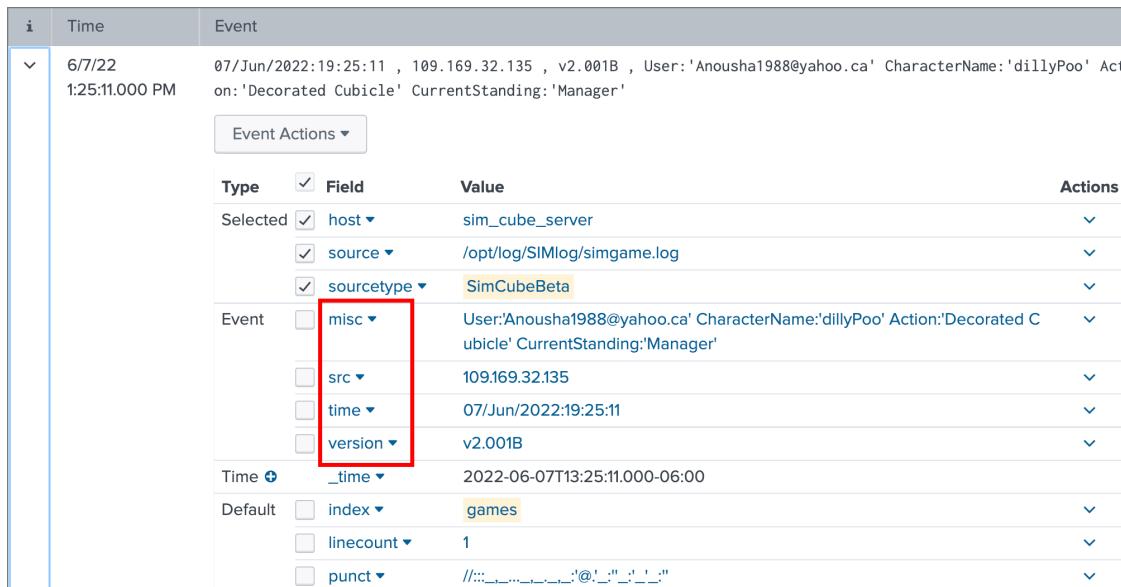
The screenshot shows the same "Rename Fields" page after renaming. The fields are now labeled time, src, version, and misc. The values remain the same: 07/Jun/2022:19:12:09, 148.107.2.20, v2.003B, and User:'tmcbreen@mhcable.com' CharacterName:'Kooby' Action:'Joined Union' CurrentStanding:'Office Joke'.

NOTE: For the time being, the **misc** field contains all the information at the end of the event. Those fields are separated by spaces. You will create individual fields for this data using a regular expression later in this lab.

- c. After all the fields are renamed, click **Next**.
5. For Extractions Name, enter **simgame_log** and click **Finish>**

6. On the final **Success!** screen, click on **Explore the fields I just created in Search**. (Alternatively, return to the search app and repeat the search you performed in step 2.)

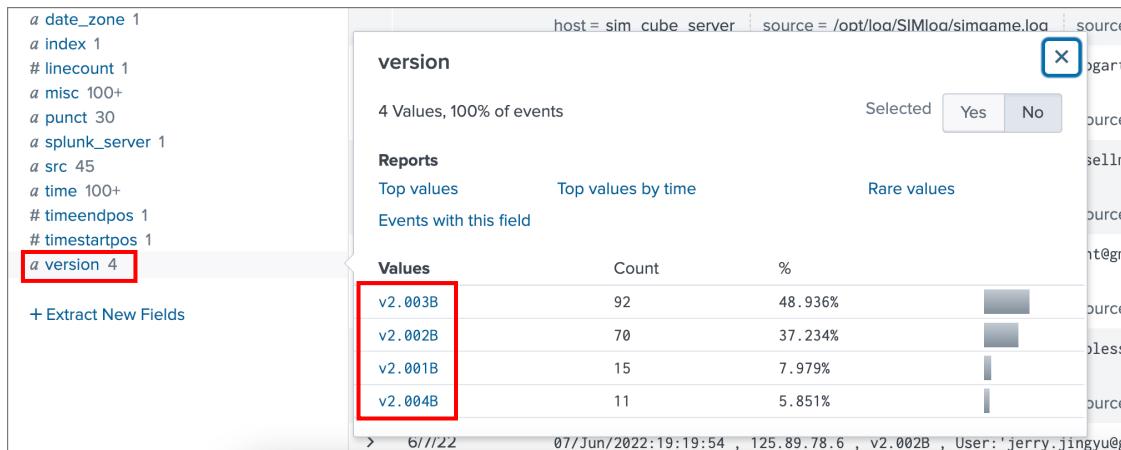
- a. In the Fields sidebar, under **Interesting Fields**, verify that your newly added fields appear (**misc**, **src**, **time**, and **version**).



The screenshot shows the Splunk interface with the Fields sidebar open. Under the 'Interesting Fields' section, the following fields are listed:

Type	Field	Value	Actions
Selected	host	sim_cube_server	▼
	source	/opt/log/SIMlog/simgame.log	▼
	sourcetype	SimCubeBeta	▼
Event	misc	User:'Anousha1988@yahoo.ca' CharacterName:'dillyPoo' Action:'Decorated Cubicle' CurrentStanding:'Manager'	▼
	src	109.169.32.135	▼
	time	07/Jun/2022:19:25:11	▼
	version	v2.001B	▼
Time	_time	2022-06-07T13:25:11.000-06:00	▼
Default	index	games	▼
	linecount	1	▼
	punct	://.....@'`-`-`-	▼

- b. Click on the **version** field to explore the values.



The screenshot shows the Splunk interface with the 'version' field selected. The details pane displays the following information:

- version**: 4 Values, 100% of events
- Reports**: Top values, Top values by time, Rare values
- Events with this field**

Values	Count	%
v2.003B	92	48.936%
v2.002B	70	37.234%
v2.001B	15	7.979%
v2.004B	11	5.851%

- c. Click on the **misc** field to explore the values. Notice that the **misc** field consists of a long string with multiple game-related values that you may wish to consider as separate fields.

New Search

index=_* OR index=_* sourcetype=SimCubeBeta

188 events (6/6/22 1:00:00.000 PM to 6/6/22 1:00:00.000 PM)

Events (188) Patterns Statistics

Format Timeline - Zoom Out

Reports Top values Top values by time Rare values Events with this field

Top 10 Values

	Count	%
User: 'Bob@rjhtrading.com'	2	1.064%
CharacterName: 'BeefCake' Action: 'Cleaned Desk'		
CurrentStanding: 'Director'		
User: 'Anousha1988@yahoo.ca'	1	0.532%
CharacterName: 'dillyPoo' Action: 'Decorated Cubicle'		
CurrentStanding: 'Manager'		
User: 'Anousha1988@yahoo.ca'	1	0.532%
CharacterName: 'dillyPoo' Action: 'Made Deadline'		
CurrentStanding: 'Mid-Manager'		
User: 'Bob@rjhtrading.com'	1	0.532%
CharacterName: 'BeefCake' Action: 'Got A Case Of The Mondays'		
CurrentStanding: 'Grunt'		
User: 'Bob@rjhtrading.com'	1	0.532%
CharacterName: 'BeefCake' Action: 'Looked At Inappropriate WebSite'		
CurrentStanding: 'Grunt'		
User: 'CEDWARDS@napavalleycomputers.com'	1	0.532%
CharacterName: 'Dash' Action: 'Did Not File TPS Report'		
CurrentStanding: 'Manager'		

< Hide Fields : All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # date_hour 4
- # date_mday 1
- # date_minute 60
- a date_month 1
- # date_second 58
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- # filecount 1

Use the regex method to extract additional fields found in the new misc field.

7. In the Fields sidebar, underneath the **Interesting Fields** section, click **+ Extract New Fields**.

- On the **Select Sample Event** screen, click the first event to select it as a sample event.
- Verify that the event now appears towards the top as a sample event.
- Click the **Next** button at the top of the screen.

8. Select the **Regular Expression** method and click **Next**.

9. Add extracted fields for the string data that we previously added to the **misc** field.

- Highlight the name of the user after the word "User:" as it appears between the single quotes. Do not include the single quotes in the highlight selection.

NOTE: Be sure to capture all the characters **between** the single quotes, but **not** the single quotes themselves. Some versions of Internet Explorer won't allow you to exclude the single quotes. Switch to another browser to complete the exercise.

- Give it a **Field Name of User**.
- Click **Add Extraction**.

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 values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more [?!](#)

07/Jun/2022:19:25:11 , 109.169.32.135 , v2.001B , User: 'Anousha1988@yahoo.ca' CharacterName: 'dillyPoo' Action: 'Decorated Cubicle' CurrentStanding: 'Manager'

Preview

If you see incorrect results below, click an additional event step.

Events

Field Name: User

Sample Value: Anousha1988@yahoo.ca

Add Extraction

188 events (3/9/22 12:00:00.000 AM to 6/7/22 2:29:12.000 PM)

20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

filter Apply Sample: 1,000 events ▾ All events ▾

- d. Repeat steps a-c to create fields for **CharacterName**, **Action**, and **CurrentStanding** fields.
- e. Click on the **Show Regular Expression** link to view the regex expression.

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 values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

07/Jun/2022:19:25:11 , 109.169.32.135 , v2.001B , User: 'Anousha1988@yahoo.ca' CharacterName:'dillyPoo' Action:'Decorated Cubicle' CurrentStanding:'Manager'

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

```
^{^\n}*(?P<User>[^]+)(?:^\n)*(2)?P<CharacterName>[^]+|^:\n":(?P<Action>[^]+)[^\n]:*(?P<CurrentStanding>[^]+)
```

[Edit the Regular Expression](#)

10. While still on the **Select fields** step (before the validation stage), click on **Non-Matches** to see whether any relevant events are being excluded. (If no events display when you click **Non-Matches**, proceed to step 11.)

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 values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

07/Jun/2022:19:25:11 , 109.169.32.135 , v2.001B , User: 'Anousha1988@yahoo.ca' CharacterName:'dillyPoo' Action:'Decorated Cubicle' CurrentStanding:'Manager'

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

```
^{^\n}*(?P<User>[^]+)(?:^\n)*(2)?P<CharacterName>[^]+|^:\n":(?P<Action>[^]+)[^\n]:*(?P<CurrentStanding>[^]+)
```

[Edit the Regular Expression](#)

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.

Events [User](#) [CharacterName](#) [Action](#) [CurrentStanding](#)

✓ 188 events (3/9/22 12:00:00.000 AM to 6/7/22 2:37:00.000 PM) 20 per page ▾

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

! No results found.

- a. If Non-Matches appear, hover your cursor over any listed event that you want to include and click **+ Add sample event**.

_raw ▾

28/Jul/2021:15:02:53 , 12.130.60.4 , v2.002B , User: 'csmail@sbcglobal.net' CharacterName:'dr.G' Action:'Looked At Inappropriate Web Content' CurrentStanding:'Manager'

[+ Add sample event](#)

- b. Highlight each relevant value in the sample event and click **Select a Field**. For each value, choose the field name you want associated with that value and click **Add Extraction**.

- c. Repeat step 10a-10b for each excluded event until there are no more **Non-Matches**.
d. Click **Next** to proceed to the **Validate** step.
11. On the **Validate** step, verify that the results below look correct by capturing all four fields for each event. When you're satisfied with your results, click **Next**.

Validate

Validate your field extractions and remove values that are incorrectly highlighted in the Events tab. In the field tabs, inspect the extracted values for each field, and optionally click a value to apply it as a search filter to the Events tab event list.

Hide Regular Expression View in Search

`^[\^n]*(?P<User>[^]+)(?:[\^n]*)(?P<CharacterName>[^]+)[\^n]*(?P<Action>[^]+)[\^n]*(?P<CurrentStanding>[^]+)`

Edit the Regular Expression

Events User CharacterName Action CurrentStanding

✓ 188 events (3/9/22 12:00:00.000 AM to 6/7/22 2:40:00.000 PM) 20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

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

_raw	User	CharacterName	Action	CurrentStanding
✓ 07/Jun/2022:19:25:11 , 109.169.32.135 , v2.001B , User: Anousha1988@yahoo.ca <input type="button" value="X"/>	Anousha1988@yahoo.ca	dillyPoo	Decorated Cubicle	Manager
CharacterName: 'dillyPoo' <input type="button" value="X"/>				
Action: 'Decorated Cubicle' <input type="button" value="X"/>				
CurrentStanding: 'Manager' <input type="button" value="X"/>				

NOTE: Be sure to thoroughly check your results. It's important to ensure you've captured all characters inside the single quotes for the fields you've extracted.

12. Accept the prefilled **Extractions Name** and click **Finish>** to save.

Extract Fields Select Sample Select Method Select Fields Validate Save < Back **Finish >**

Save

Name the extraction and set permissions.

Extractions Name EXTRACT-

Owner poweruser

App search

Permissions Owner App All apps

Source type SimCubeBeta

Sample event 07/Jun/2022:19:25:11 , 109.169.32.135 , v2.001B , User: 'Anousha1988@yahoo.ca' CharacterName: 'dillyPoo' Action: 'Decorated Cubicle' CurrentStanding: 'Manager'

Fields User,CharacterName,Action,CurrentStanding

Regular Expression `^[\^n]*(?P<User>[^]+)(?:[\^n]*)(?P<CharacterName>[^]+)[\^n]*(?P<Action>[^]+)[\^n]*(?P<CurrentStanding>[^]+)`

13. Click on the **Explore the fields I just created in Search** link on the **Success!** page.

- Click the arrow (>) under the information icon (i) in the first event to see which fields are extracted.
- Verify that in addition to the delimited fields we created earlier (**misc**, **src**, **time**, **version**), you also see the newly created fields using regular expressions (**Action**, **CharacterName**, **CurrentStanding**, **User**).

i	Time	Event
▼	6/7/22 2:46:35.000 PM	07/Jun/2022:20:46:35 , 121.254.179.199 , v2.002B , User:'chocolateswife@verizon.net' CharacterName:'nicea55' Action:'Got Drunk At Office Party' CurrentStanding:'Grunt'
Event Actions ▾		
Type	<input checked="" type="checkbox"/> Field	Value
Selected	<input checked="" type="checkbox"/> host ▾	sim_cube_server
	<input checked="" type="checkbox"/> source ▾	/opt/log/SIMlog/simgame.log
	<input checked="" type="checkbox"/> sourcetype ▾	SimCubeBeta
Event	<input type="checkbox"/> Action ▾	Got Drunk At Office Party
	<input type="checkbox"/> CharacterName ▾	nicea55
	<input type="checkbox"/> CurrentStanding ▾	Grunt
	<input type="checkbox"/> User ▾	chocolateswife@verizon.net
	<input type="checkbox"/> misc ▾	User:'chocolateswife@verizon.net' CharacterName:'nicea55' Action:'Got Drunk At Office Party' CurrentStanding:'Grunt'
	<input type="checkbox"/> src ▾	121.254.179.199
	<input type="checkbox"/> time ▾	07/Jun/2022:20:46:35
	<input type="checkbox"/> version ▾	v2.002B
Time +	_time ▾	2022-06-07T14:46:35.000-06:00
Default	<input type="checkbox"/> index ▾	games
	<input type="checkbox"/> linecount ▾	1
	<input type="checkbox"/> punct ▾	//:...:...:@'."'_'__'`"
	<input type="checkbox"/> splunk_server ▾	kstewart-1009-24-aio.class.splunk.com

NOTE: It may take a few minutes before the newly extracted fields appear in the search.