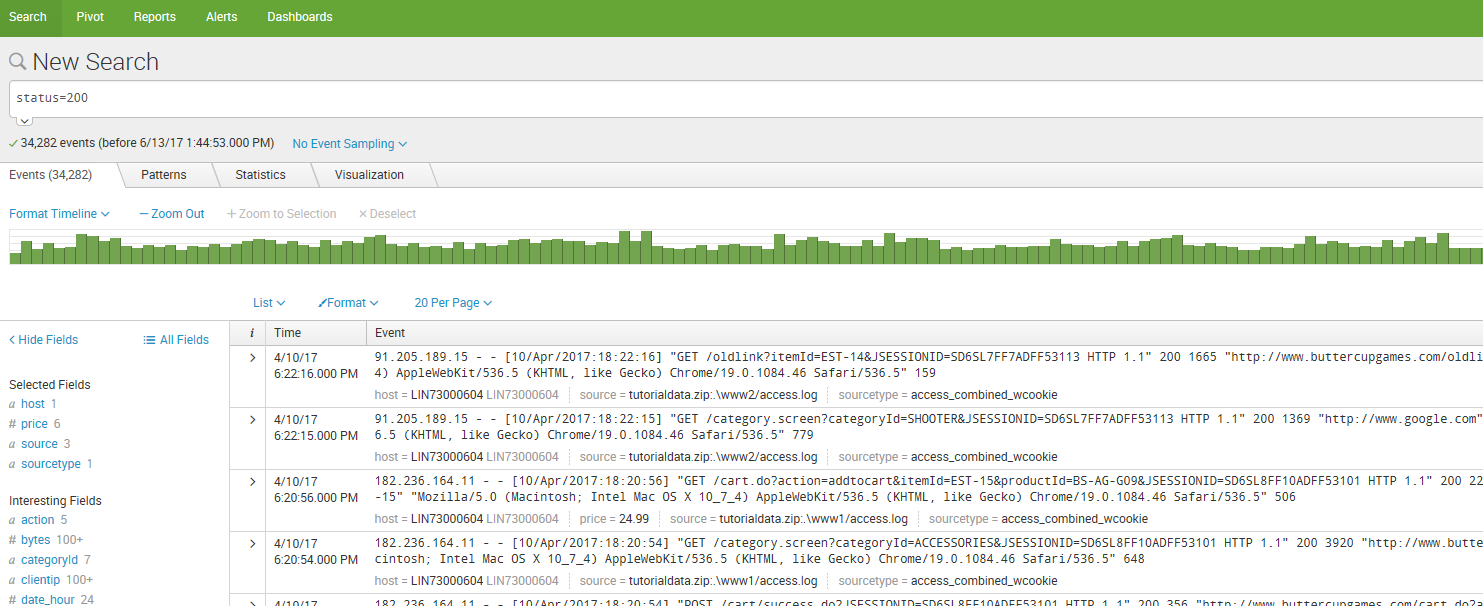
**Splunk Knowledge Objects**

Data Interpretations: Fields and Field Extractions

==========================================

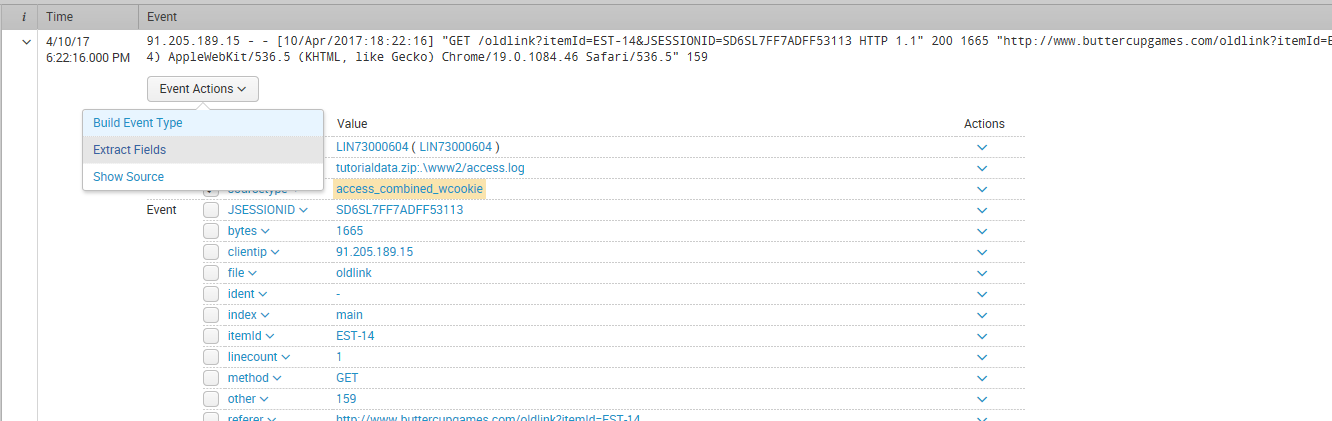
Search based on field:

====================

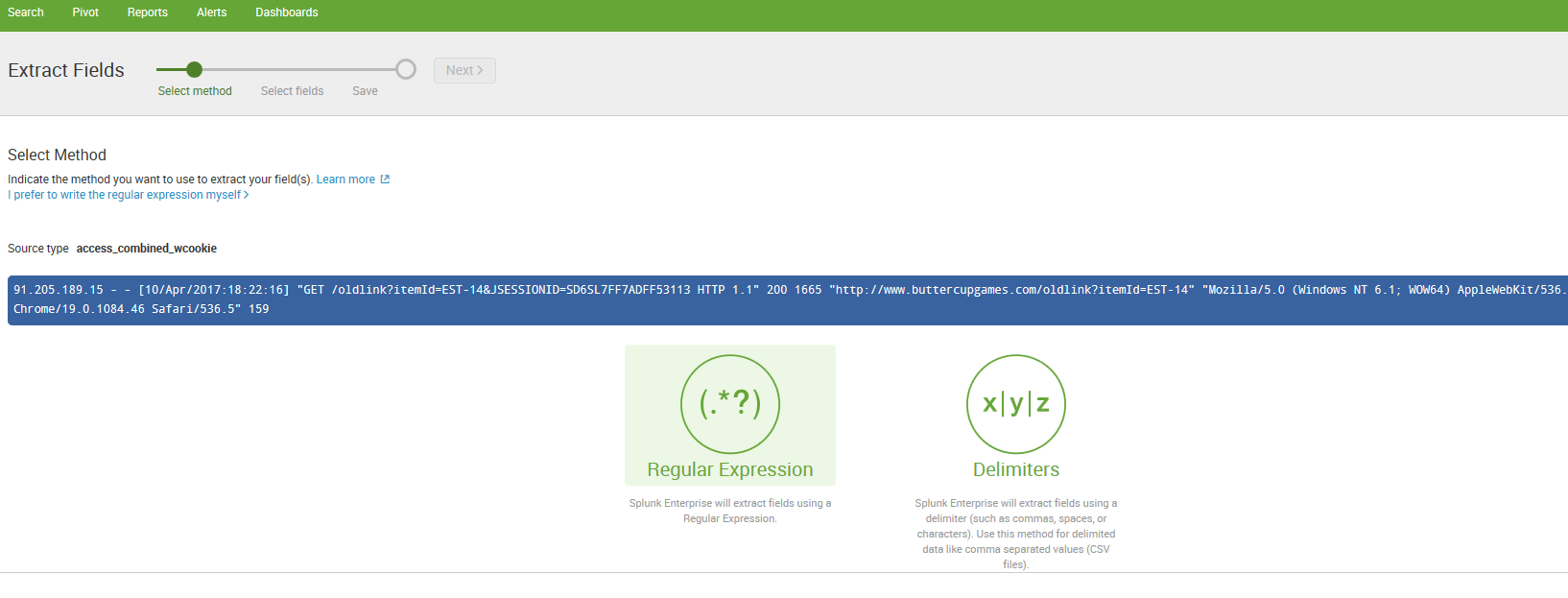


Field Extraction:

================

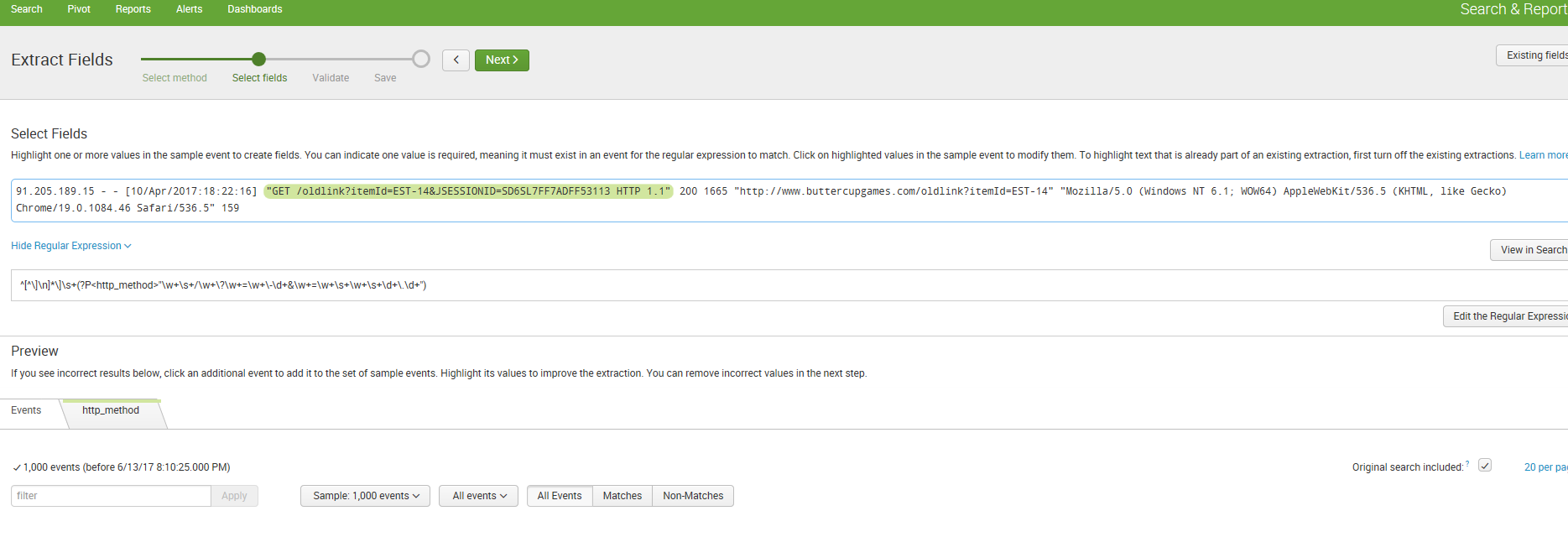


Select Extract fields tab

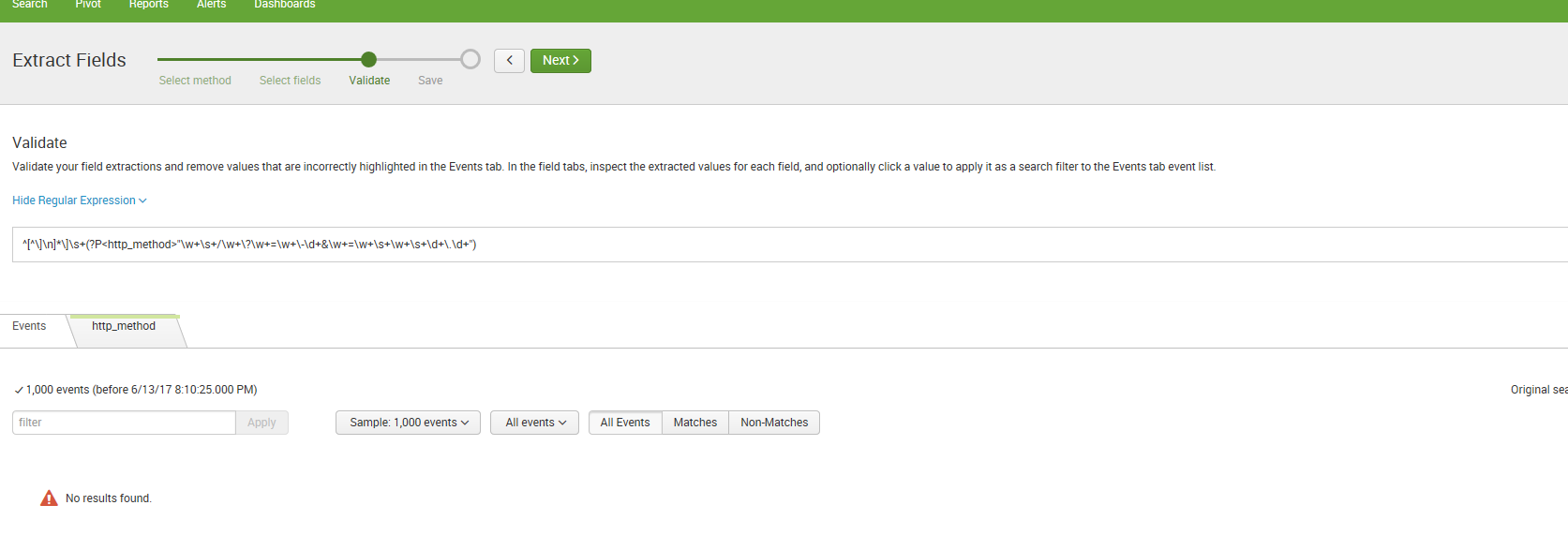


Click on Next 🡪

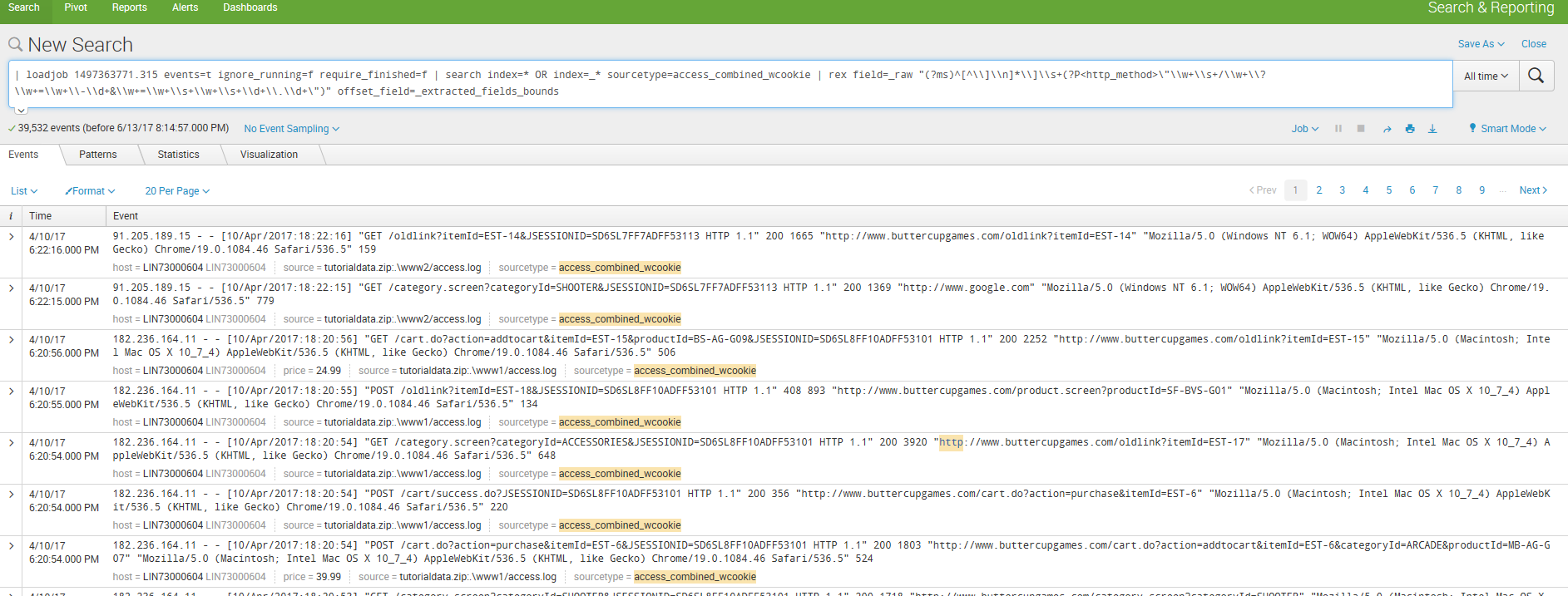
Highlight the fields in the event you want and supply the filed name



Click on Next 🡪 Validate



Click on view in search to see the events



Click on Next to save

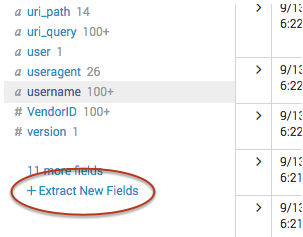


Access the field extractor from the bottom of the fields sidebar

When you use this method to access the field extractor it runs only against the set of events returned by the search that you have run. Run a search that returns events.

1. Scroll down to the bottom of the fields sidebar and click Extract New Fields.

The field extractor starts you at the [Select Sample step](http://docs.splunk.com/Documentation/Splunk/6.6.1/Knowledge/FXSelectSamplestep).

[](http://docs.splunk.com/File:Extract_new_fields.png)

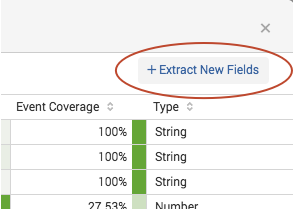
Access the field extractor from the All Fields dialog box

When you use this method to access the field extractor you can only extract fields from the data that has been returned by your search.

1. Run a search that returns events.

2. At the top of the fields sidebar, click **All Fields**.

3.In the All Fields dialog box, click **Extract new fields**.

[](http://docs.splunk.com/File:Field_extractor_extract_new_fields.png)

The field extractor starts you at the [at the Select Sample step](http://docs.splunk.com/Documentation/Splunk/6.6.1/Knowledge/FXSelectSamplestep).

Access the field extractor from a specific event

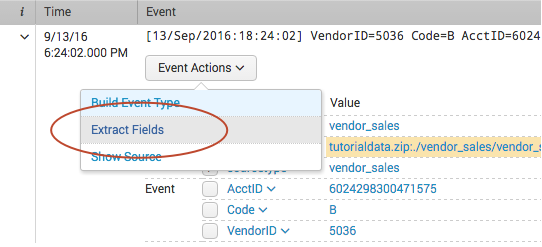
Use this method to select an event in your search results, and create a field extraction that:

* Extracts one or more fields found in that event.
* Is tied to the source type of that event.

When you use this method to access the field extractor, the field extractor runs against the set of events returned by the search that you have run.

1. Run a search that returns events.
2. Find an event that you want to extract fields from, and click the arrow symbol to the left of the timestamp to open it.
3. Click **Event Actions**, and select **Extract Fields.**

The field extractor starts you at the [Select Method step](http://docs.splunk.com/Documentation/Splunk/6.6.1/Knowledge/FXSelectMethodstep), in a new browser tab. You have already defined the source type and sample event.

[](http://docs.splunk.com/File:Field_extractor_access_search_event_actions.png)

Access the field extractor through the Field Extractions page in Settings

This entry method is available to all users.

1. Select **Settings > Fields > Field extractions**.
2. Click the **Open field extractor** button.

The field extractor starts you at the [Select Sample step](http://docs.splunk.com/Documentation/Splunk/6.6.1/Knowledge/FXSelectSamplestep).

Access the field extractor through the Home page

This entry method is available only to users whose roles have the edit\_monitor capability, such as Admin.

On the Home page, click the **extract fields** link under the **Add Data** icon.

The field extractor starts you at the [Select Sample step](http://docs.splunk.com/Documentation/Splunk/6.6.1/Knowledge/FXSelectSamplestep).

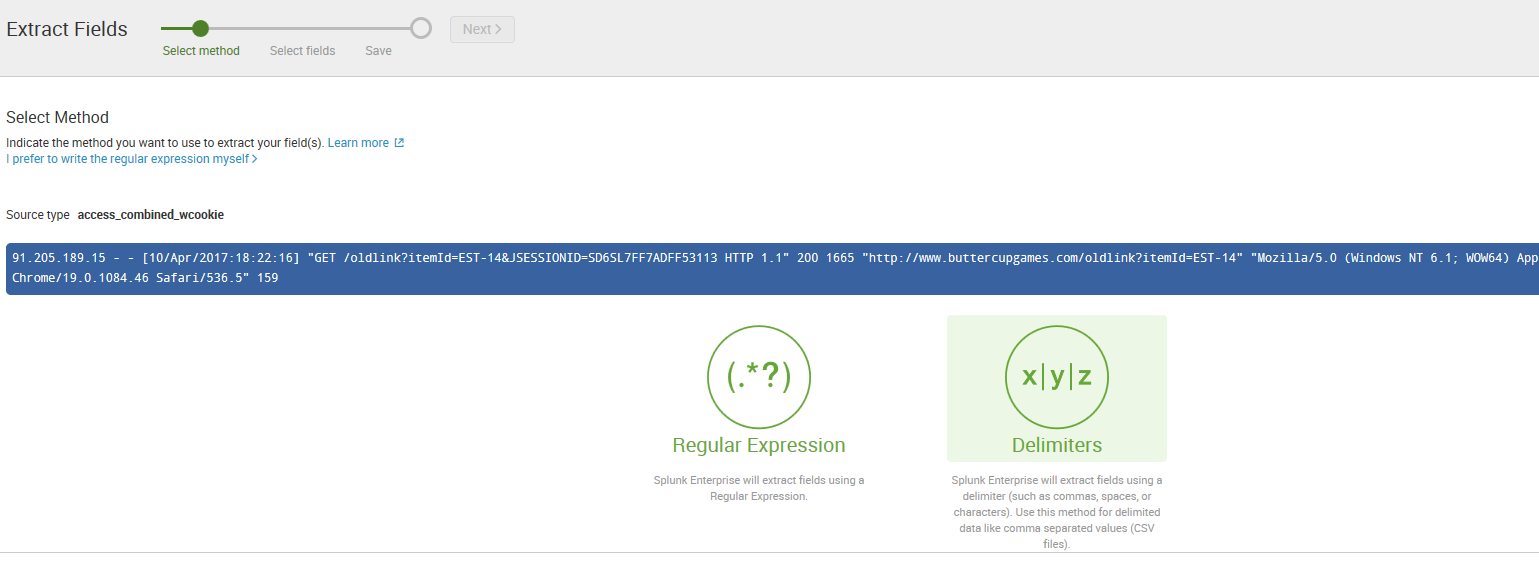
Access the field extractor after you add data

This entry method is available only to users whose roles have the edit\_monitor capability, such as Admin.

After you add data to Splunk Enterprise, use the field extractor to extract fields from that data, as long as it has a fixed source type.

For example: You add a file named vendors.csv to your Splunk deployment and give it the custom source type vendors. After you save this input, you can enter the field extractor and extract fields from the events associated with the vendors source type.

Click on delimiters

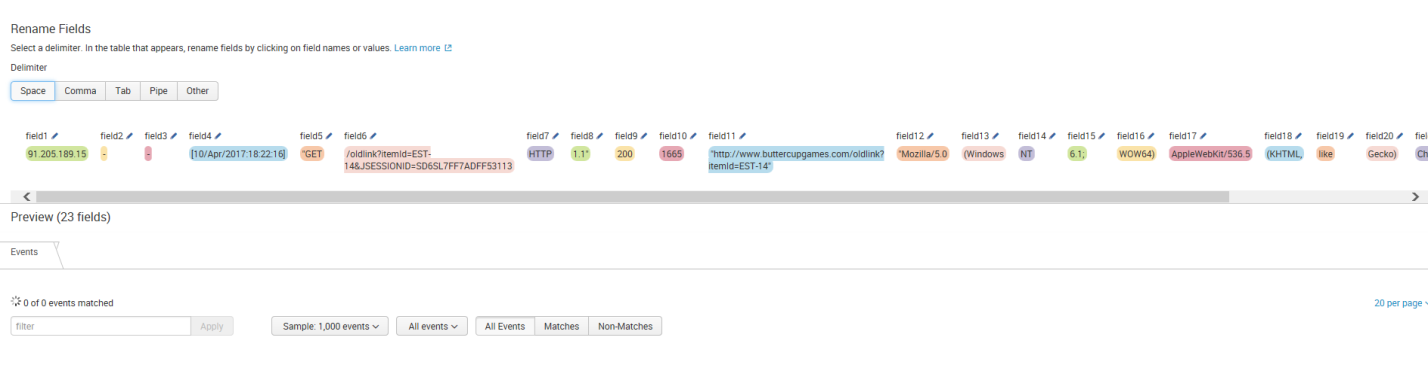


Click Next 🡪 Rename fields

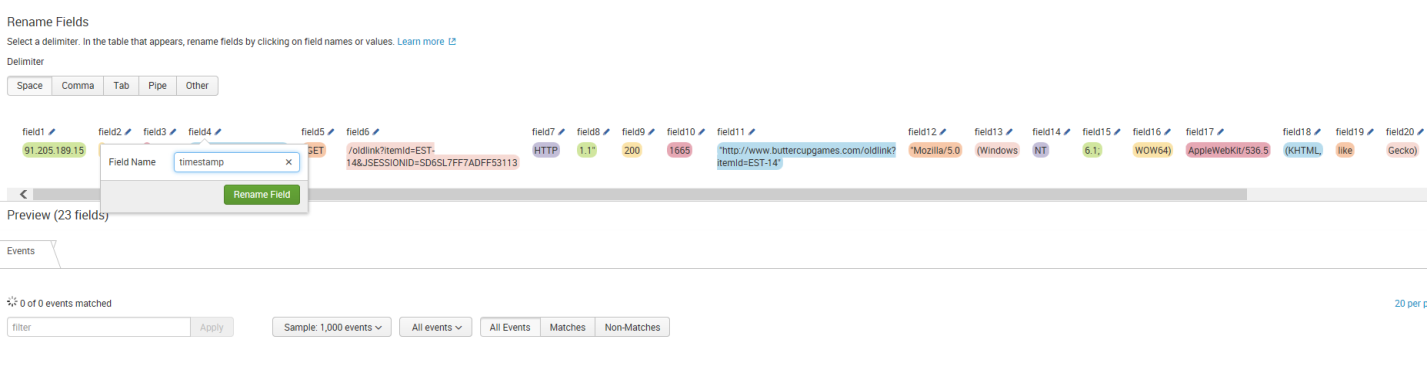


Select either comma or tab or pipe or space etc

Eg:

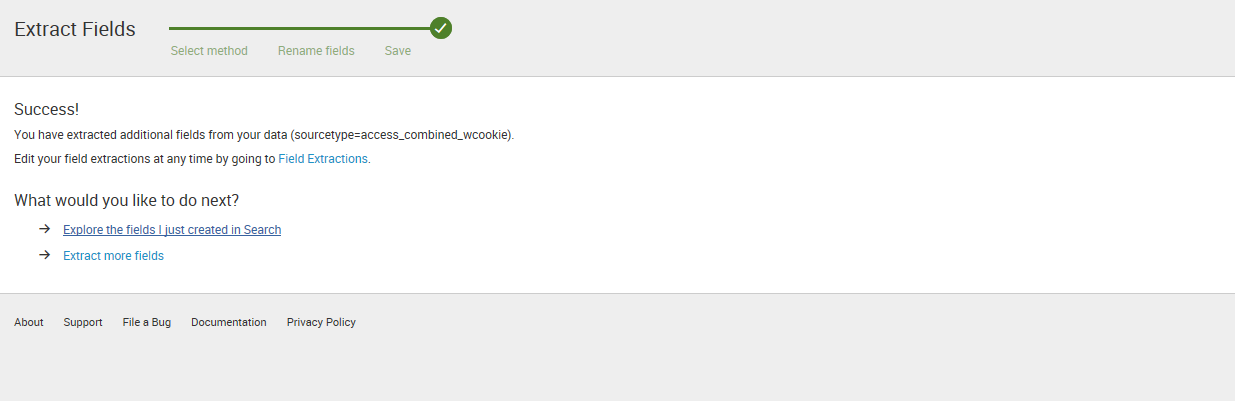


Click on a field name to rename it as shown below



Click next to save and click finish

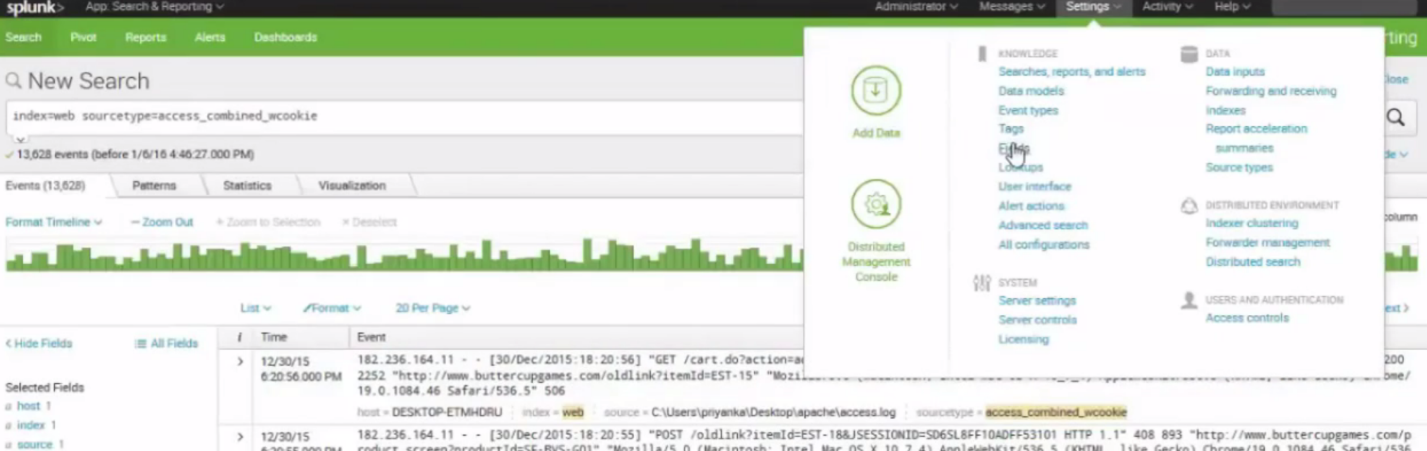




Add new Field extractions

====================

Click Settings 🡪 fields🡪 field Extractions



Click on field extractions

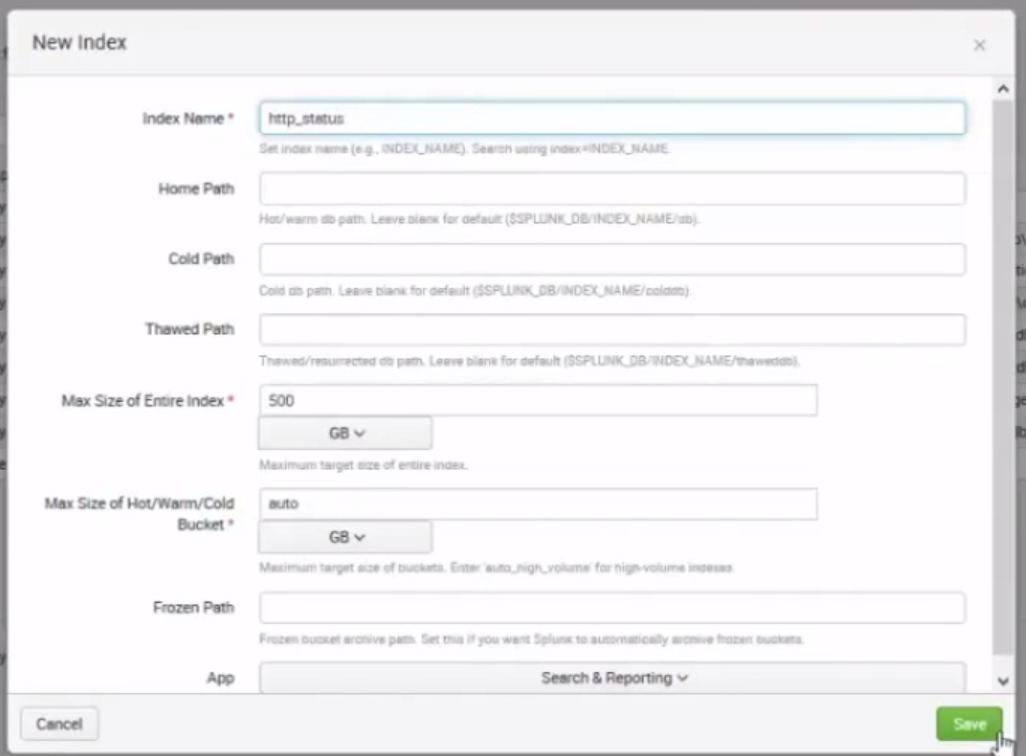
To start with lets create a status.txt file

Then create a new index

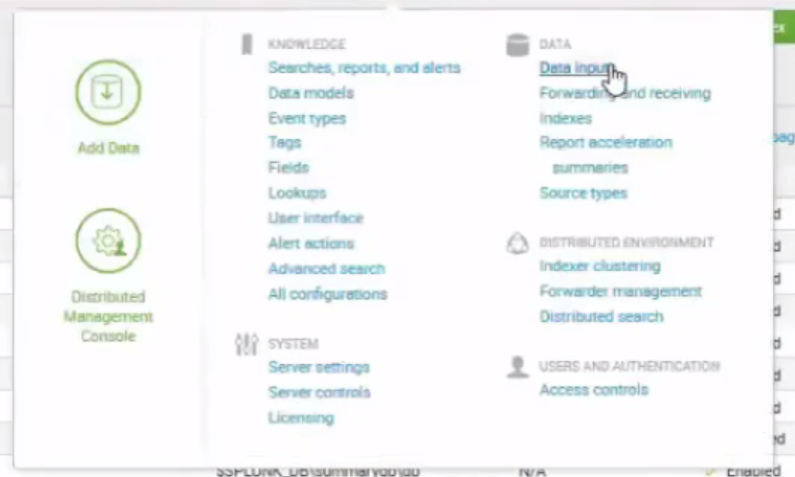
Go to Settings 🡪 Indexes



Click New Index



Go to Settings 🡪 click Data Inputs

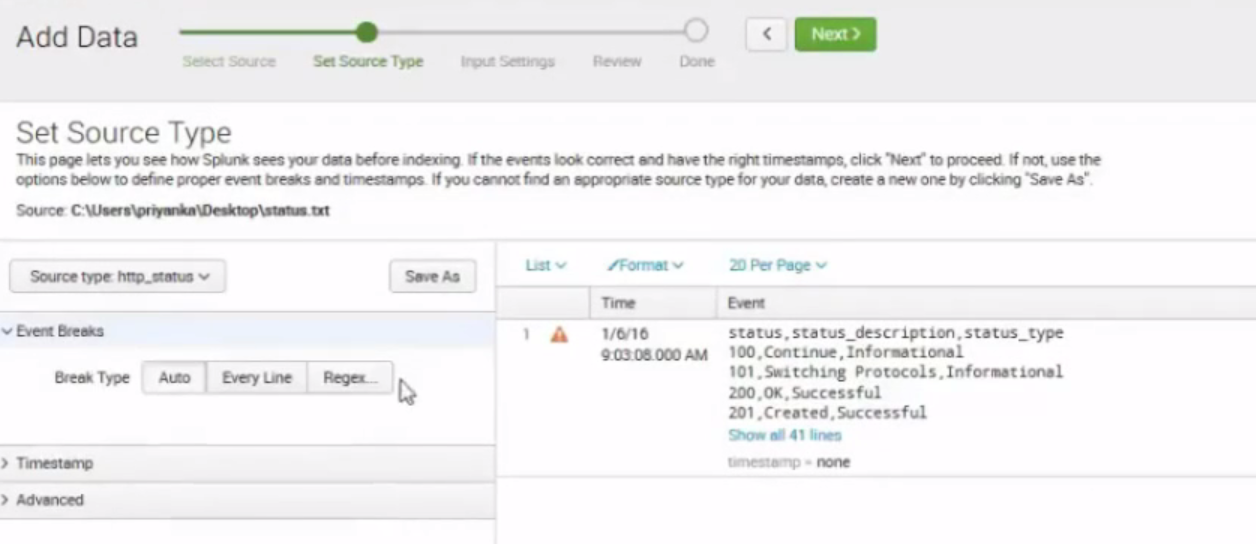


Click on File and directories 🡪 New 🡪Browse 🡪select file status.txt ->select > Next

Click save as

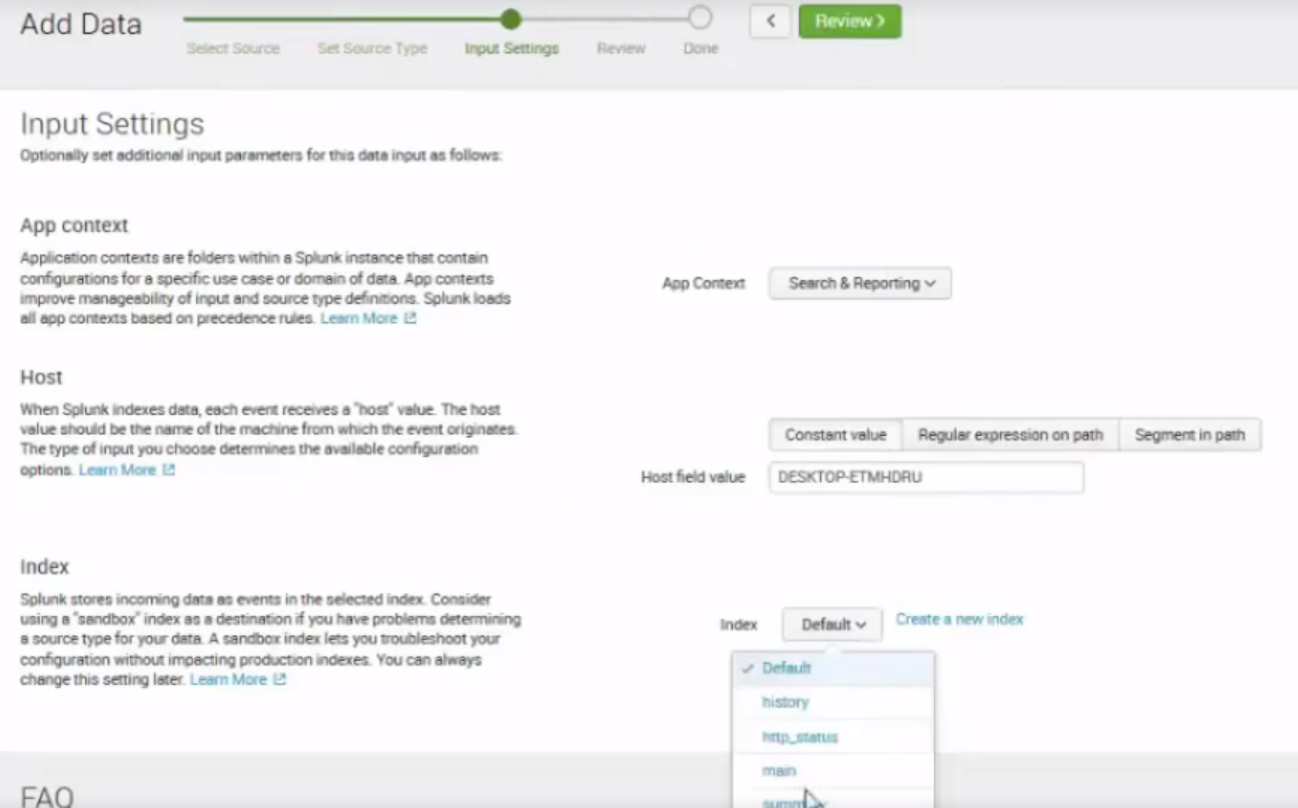


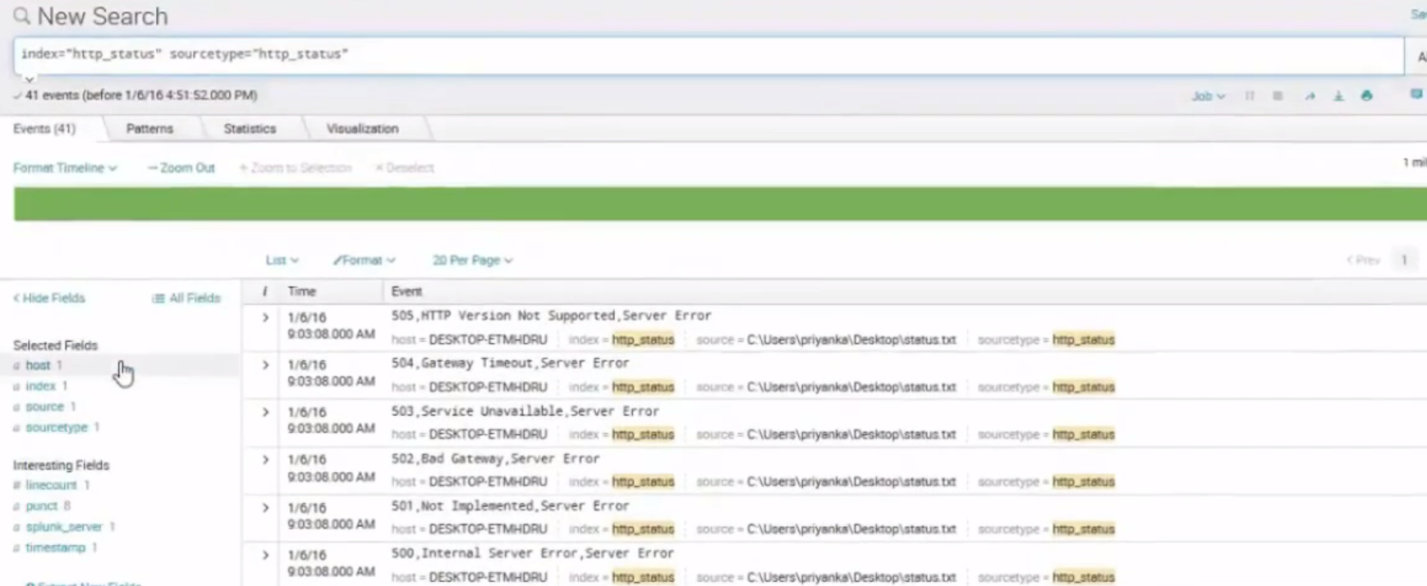
Click on Event break 🡪 every line



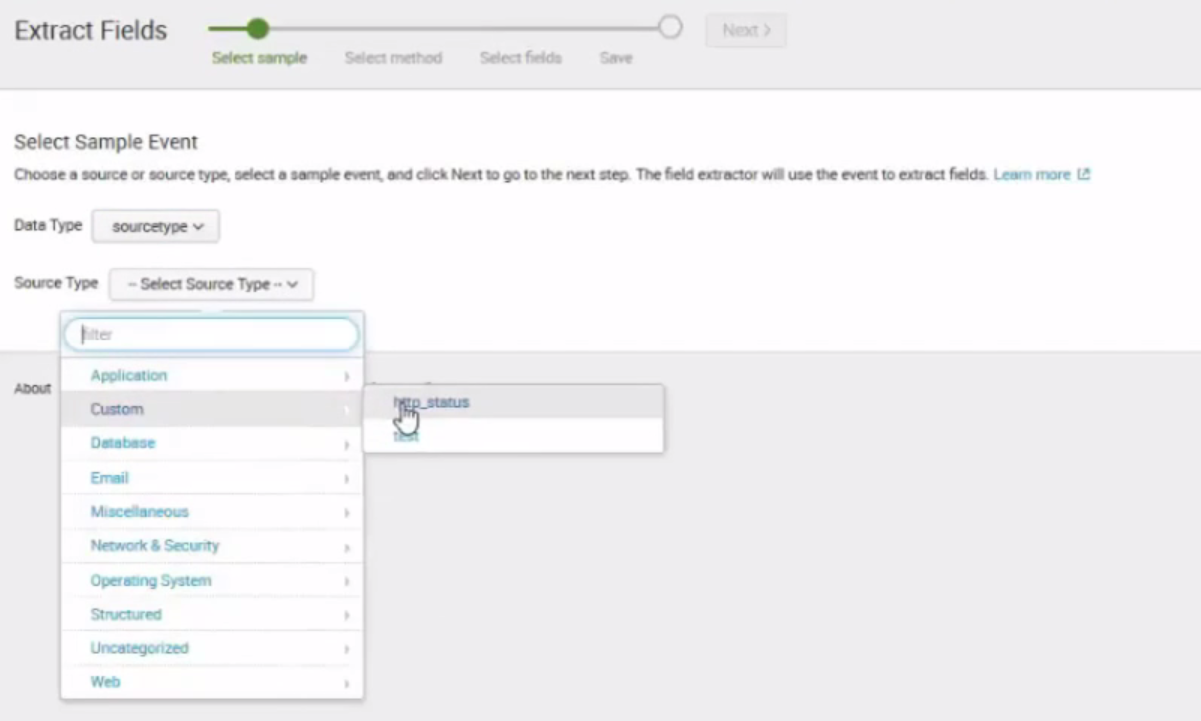
Click save as

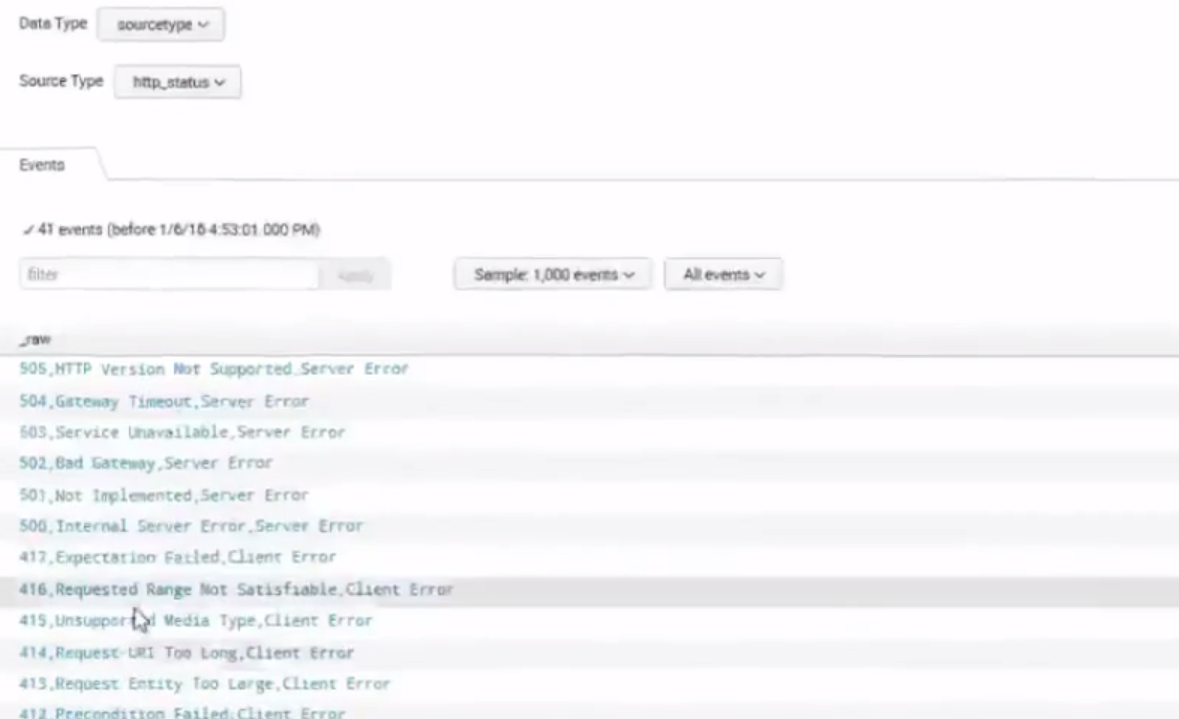
Click Next 🡪 choose Index 🡪http\_Status

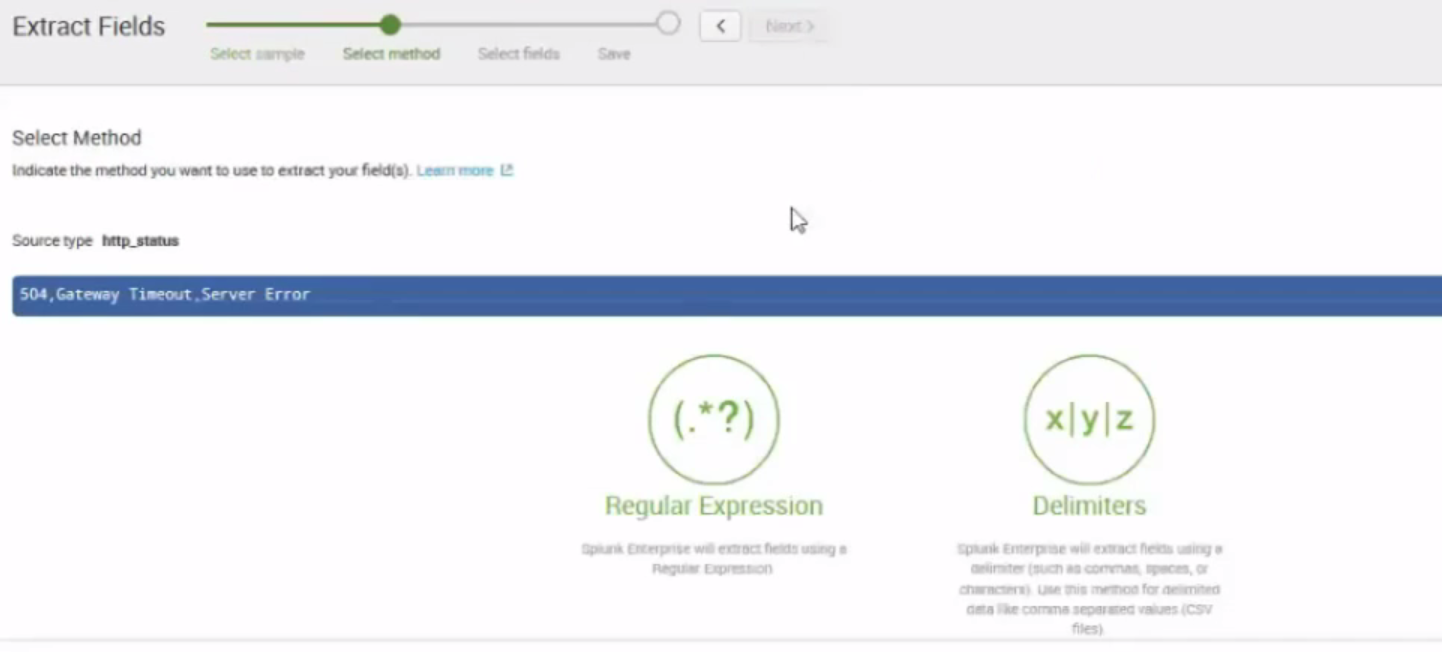
click review



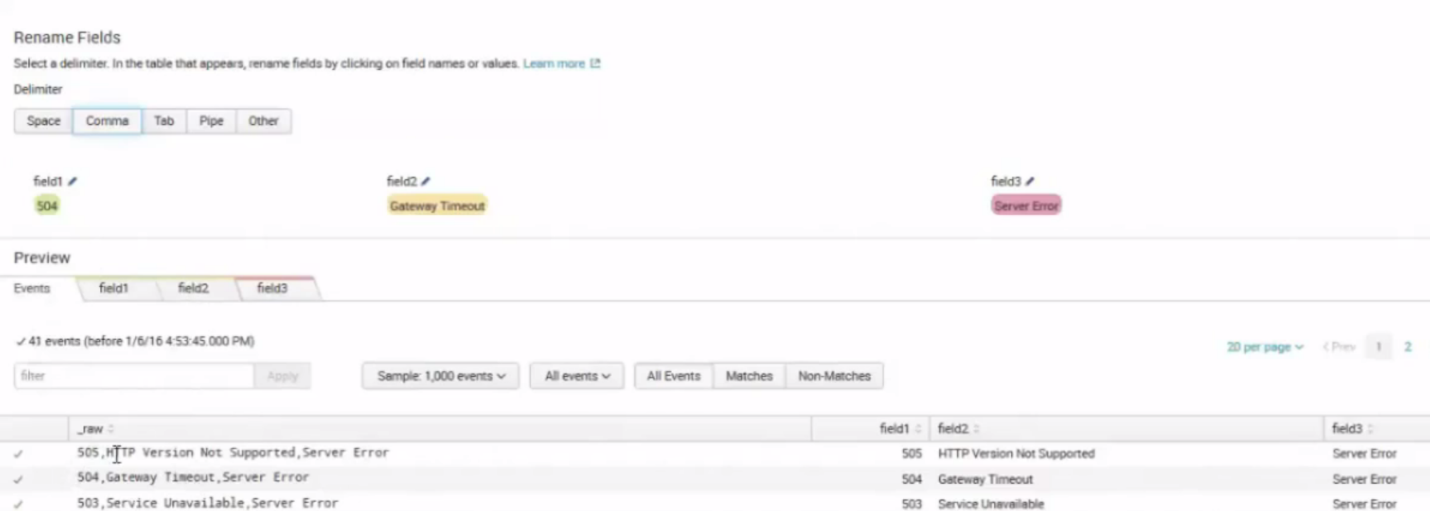
Click Settings 🡪 fields🡪field extractions -- > open Field Extractions



Click on any event 🡪click Next

Click delimiter 🡪 click Next

Choose tab or space or comma



Choose the field name and rename it

Click Save 🡪 give the name 🡪 click Finish

Go to Search and App 🡪 type index=”http\_status”

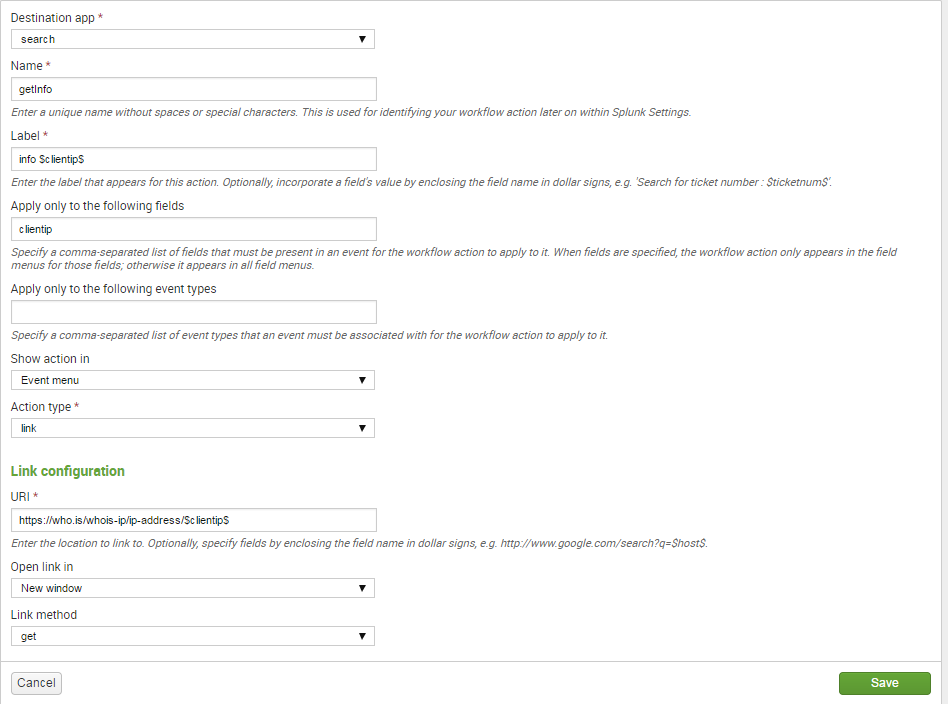
WorkFlow Actions

===============

To pass the clientip field and get the client ip value

Click on Settings 🡪fields 🡪workflow Actions





Click save

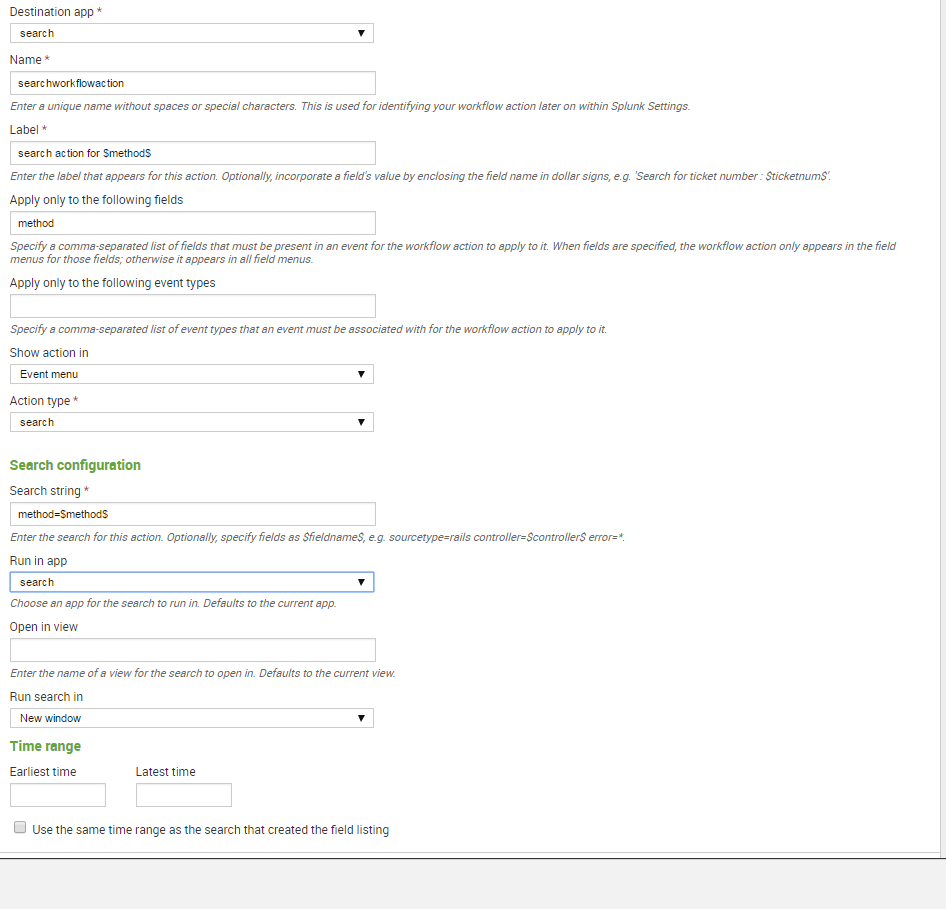
Change the permissions to 🡪 this app

Go to Search and Reporting App 🡪 type sourcetype=access\_combined\_wcookie

Expand >

Example 2: Passing the method

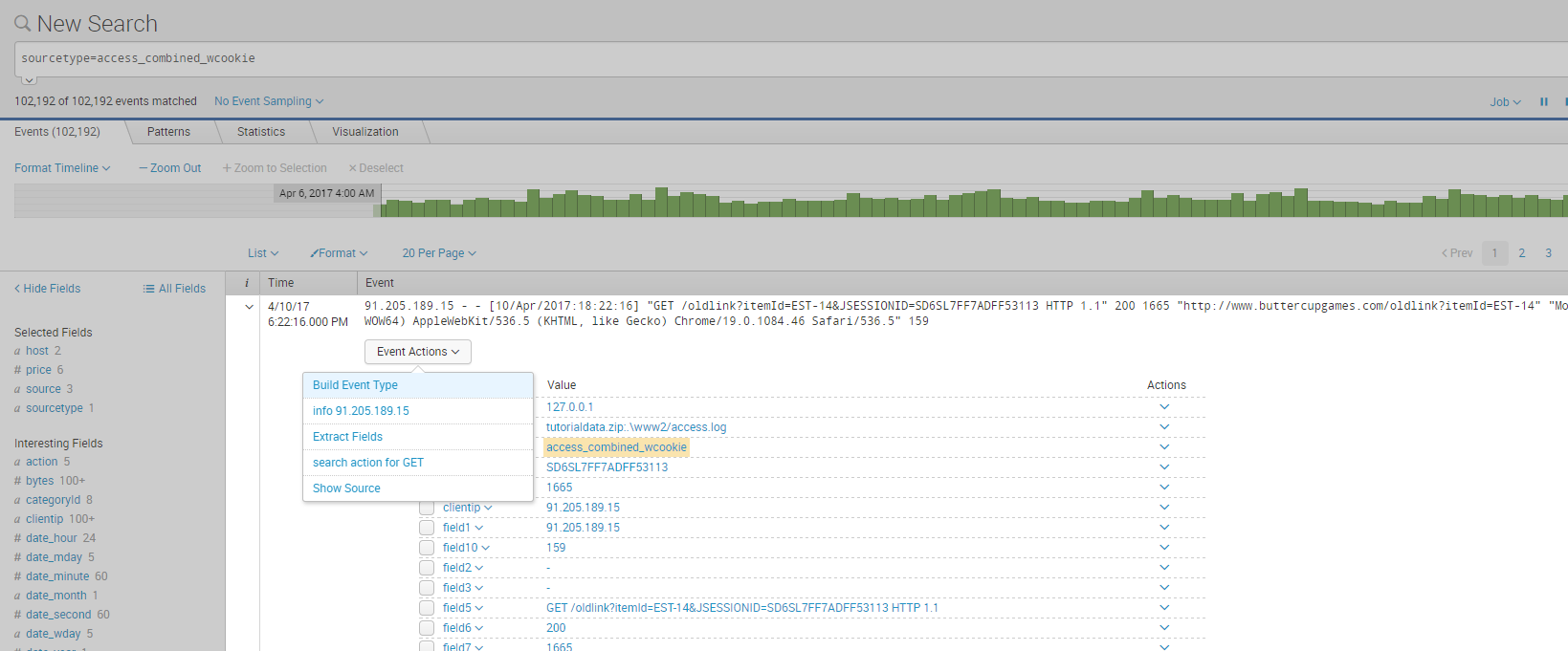
============================



Click on save .

Change permissions to 🡪this app

Click on search and reporting App



Under events expand the > and click on Event Actions to see

