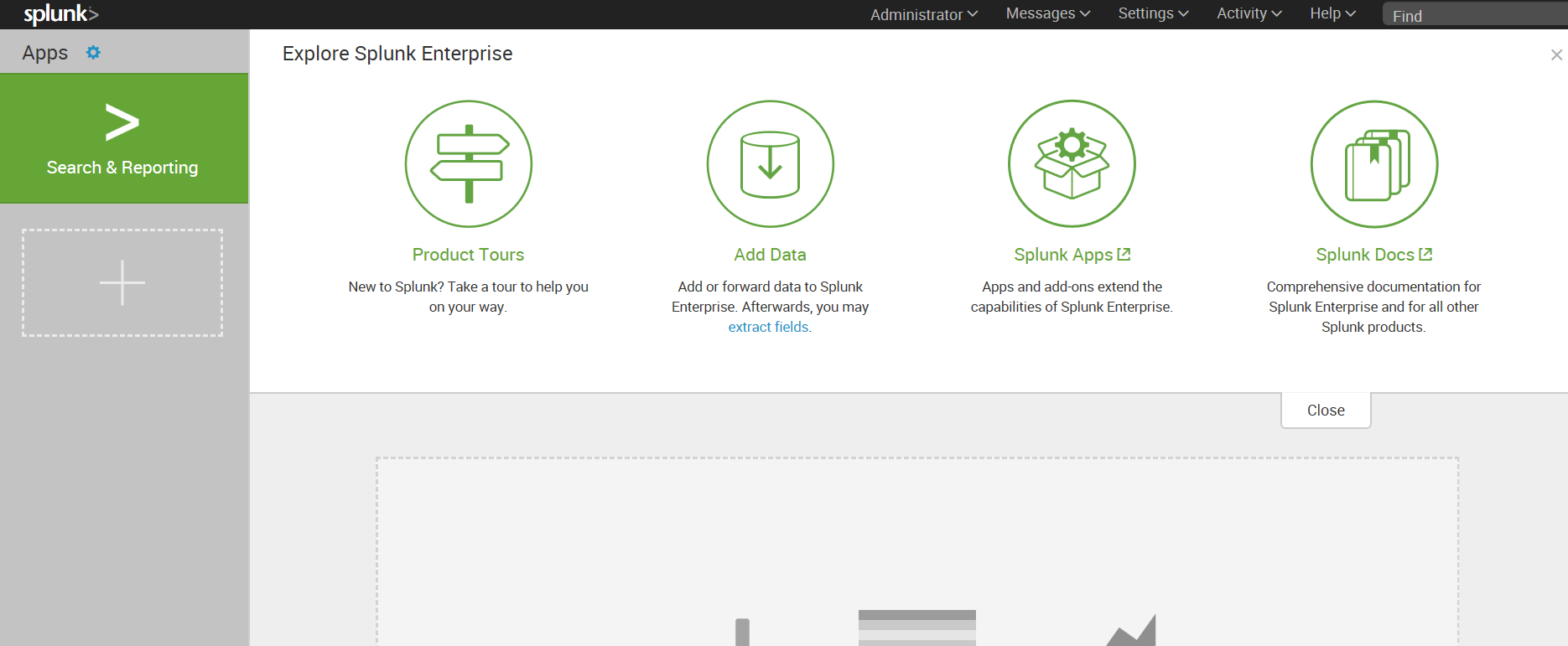
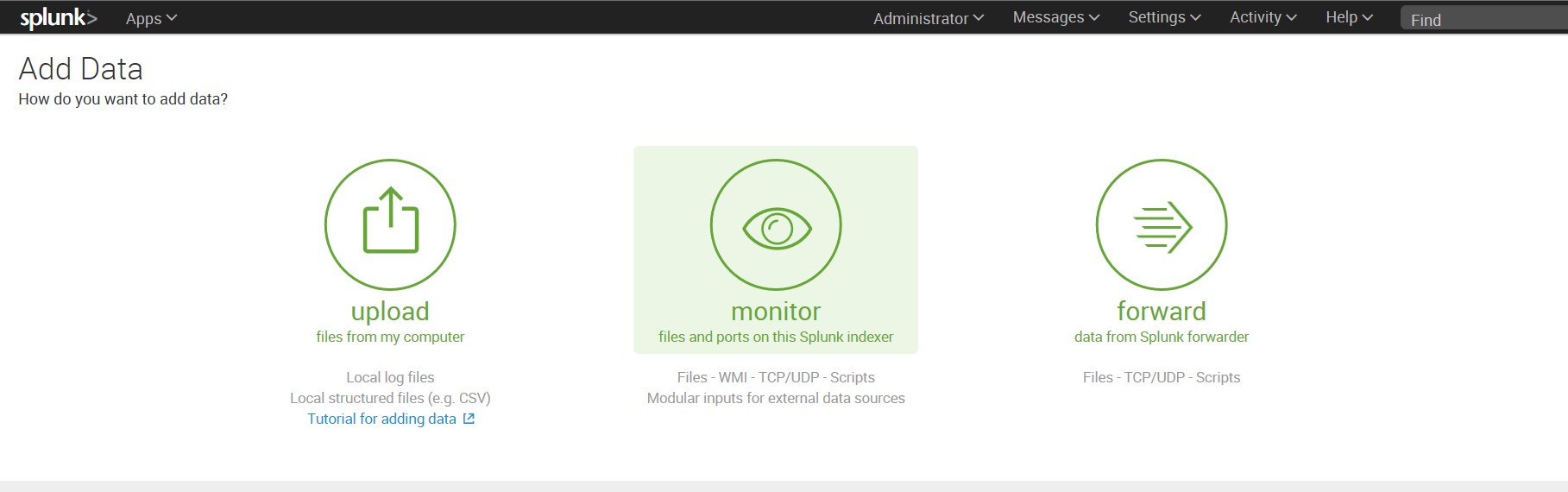
**Splunk Search - Demo**

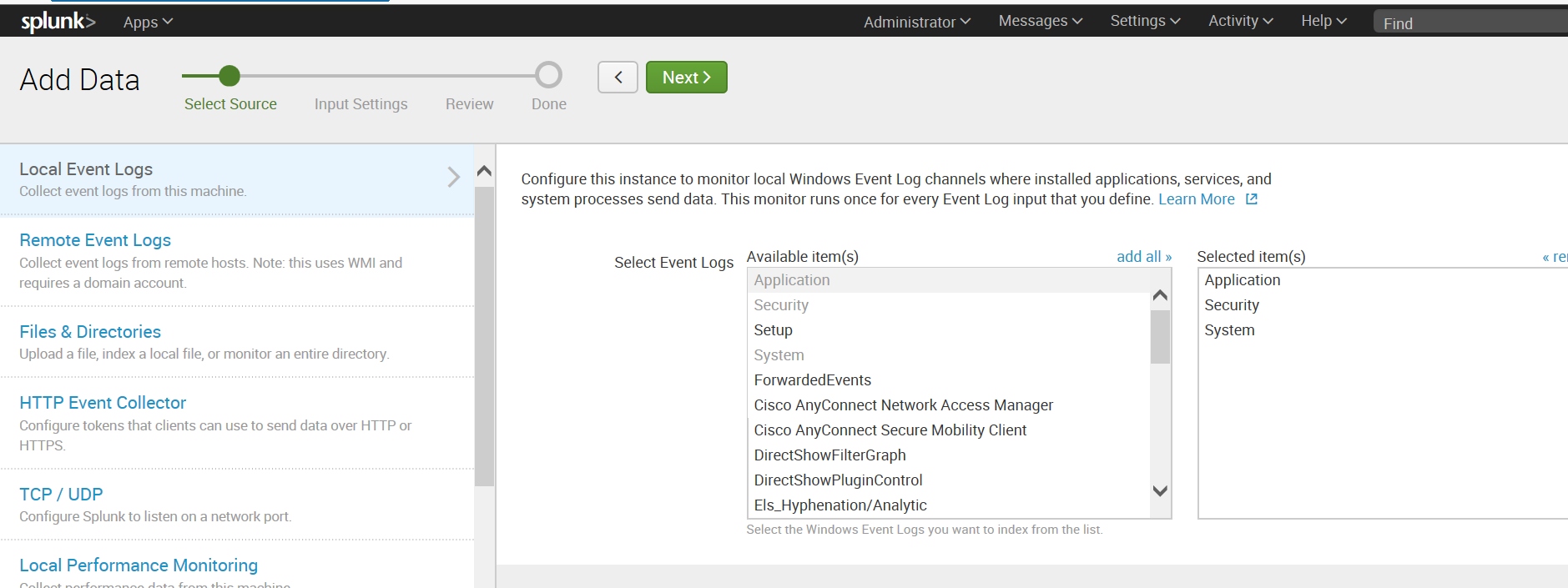
1. **Create a free account in** [**https://www.splunk.com/en\_us/download.html**](https://www.splunk.com/en_us/download.html)
2. **After creating an account , login to the account using the url** [**http://localhost:8000/en-US/app/launcher/home#en-US/app/launcher/home**](http://localhost:8000/en-US/app/launcher/home#en-US/app/launcher/home)
3. **View the page**

****

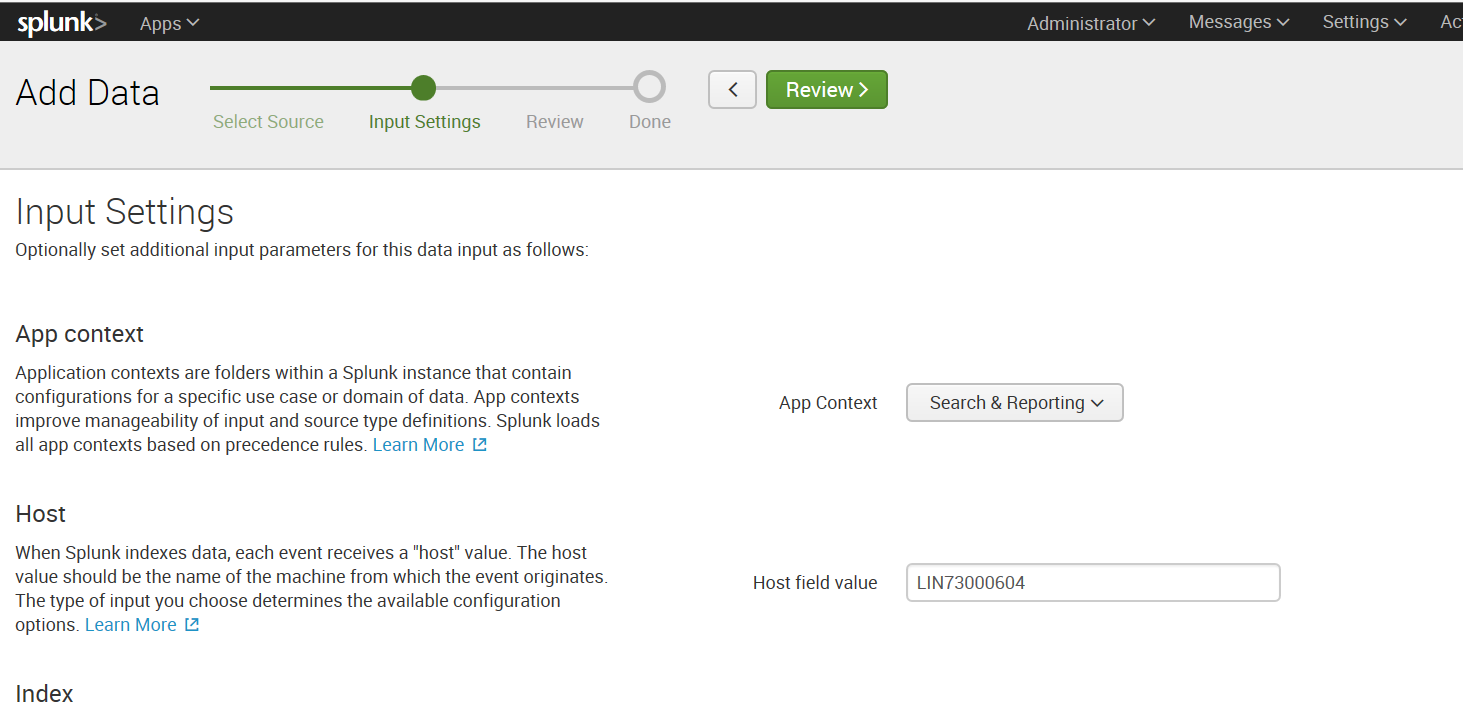
1. **Click on Add data**
2. **Click on monitor data to monitor real time data**

****

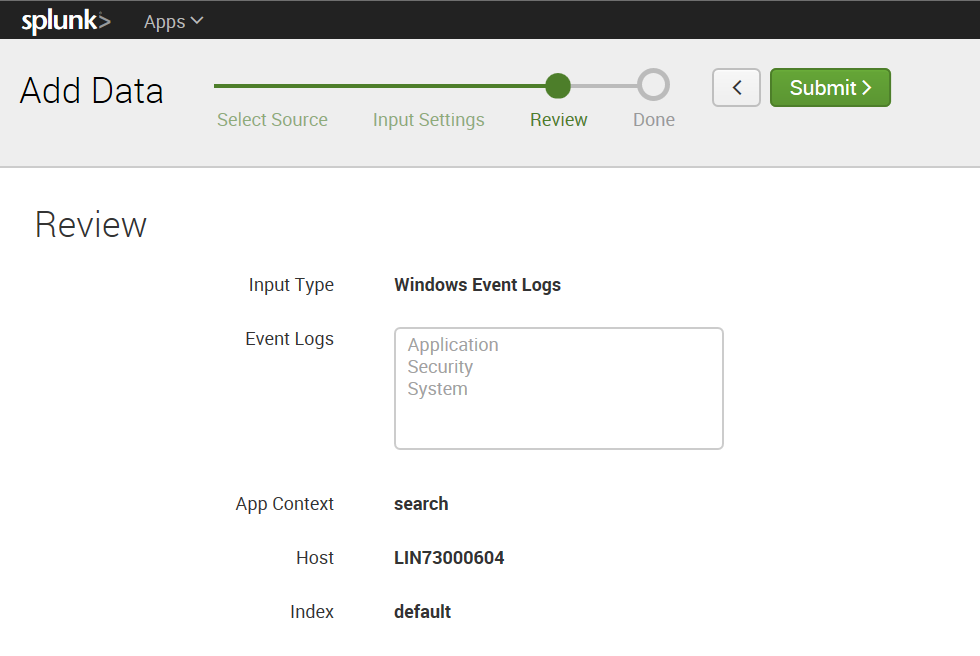
1. **Select the different types of logs**

****

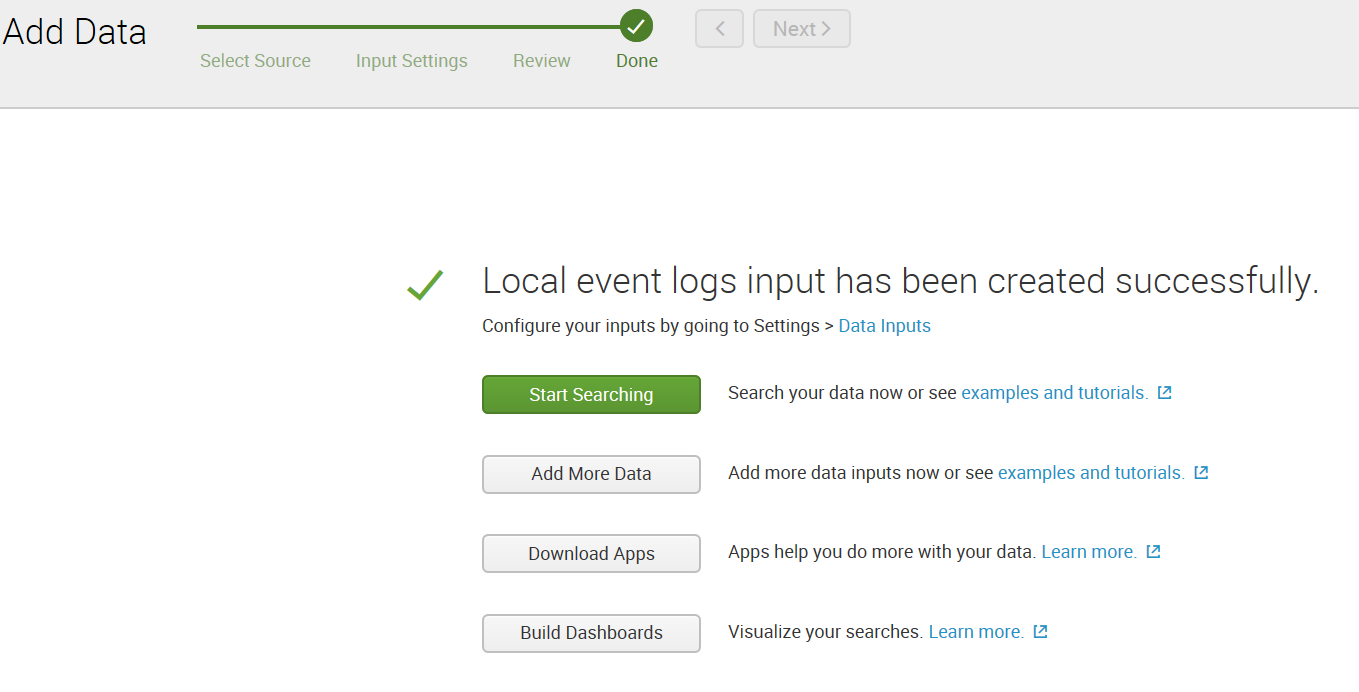
**Click on Next**

****

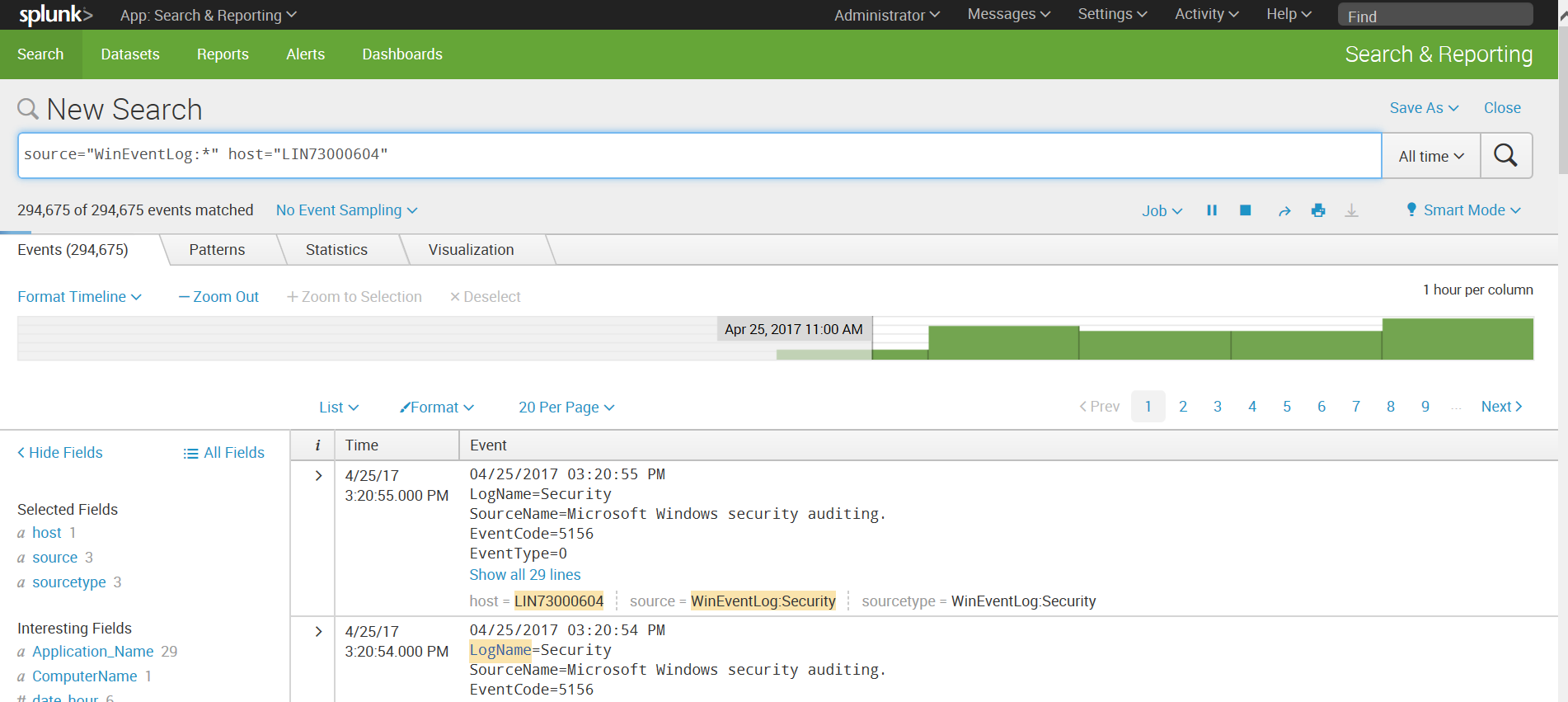
**Click on Review**

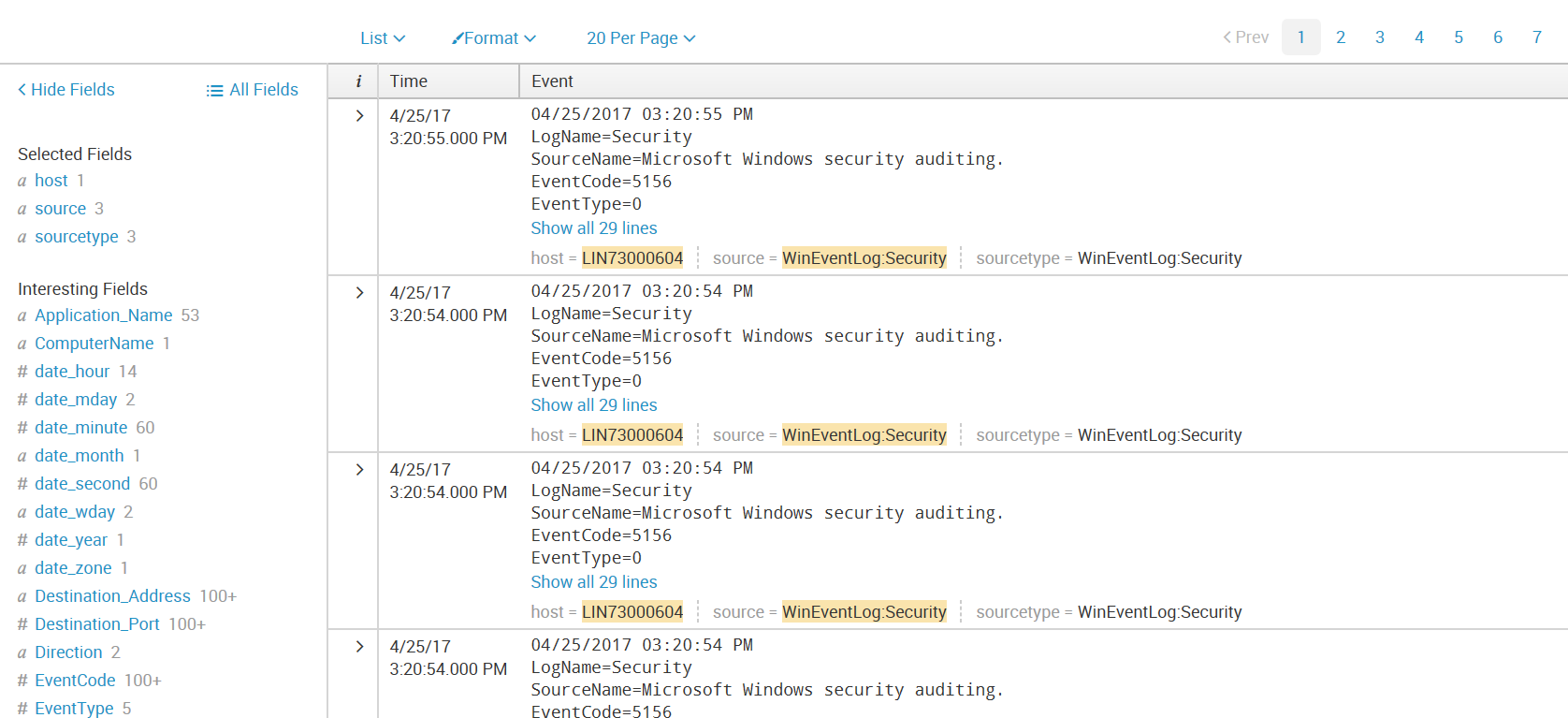
****

**Click on submit**

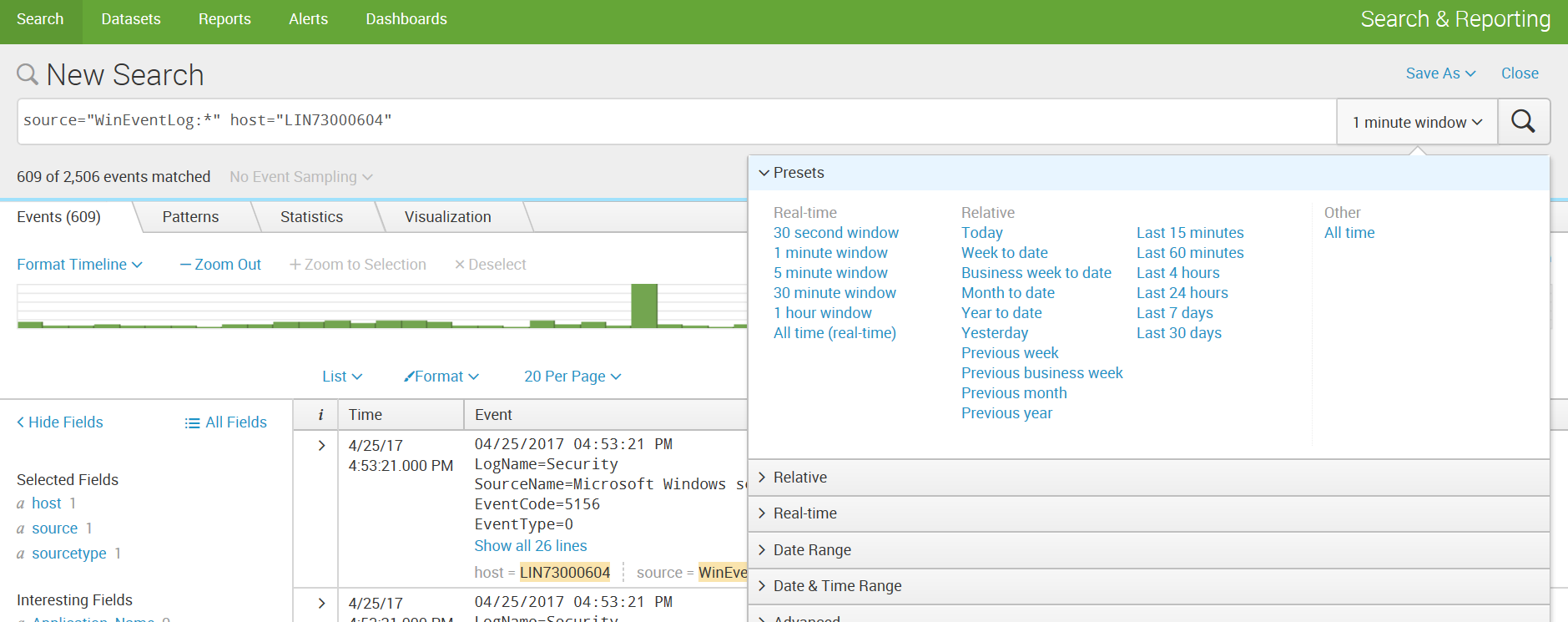
****

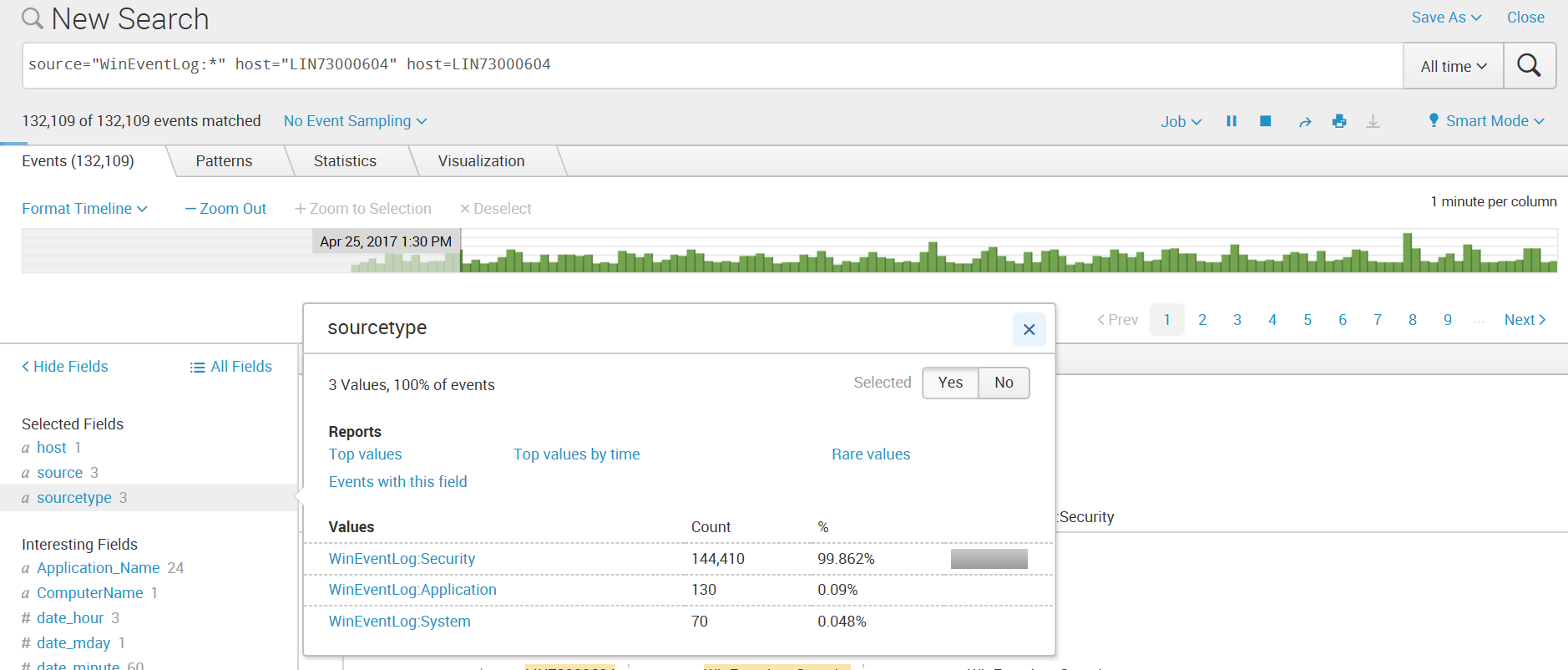
**Click on Searching**

****

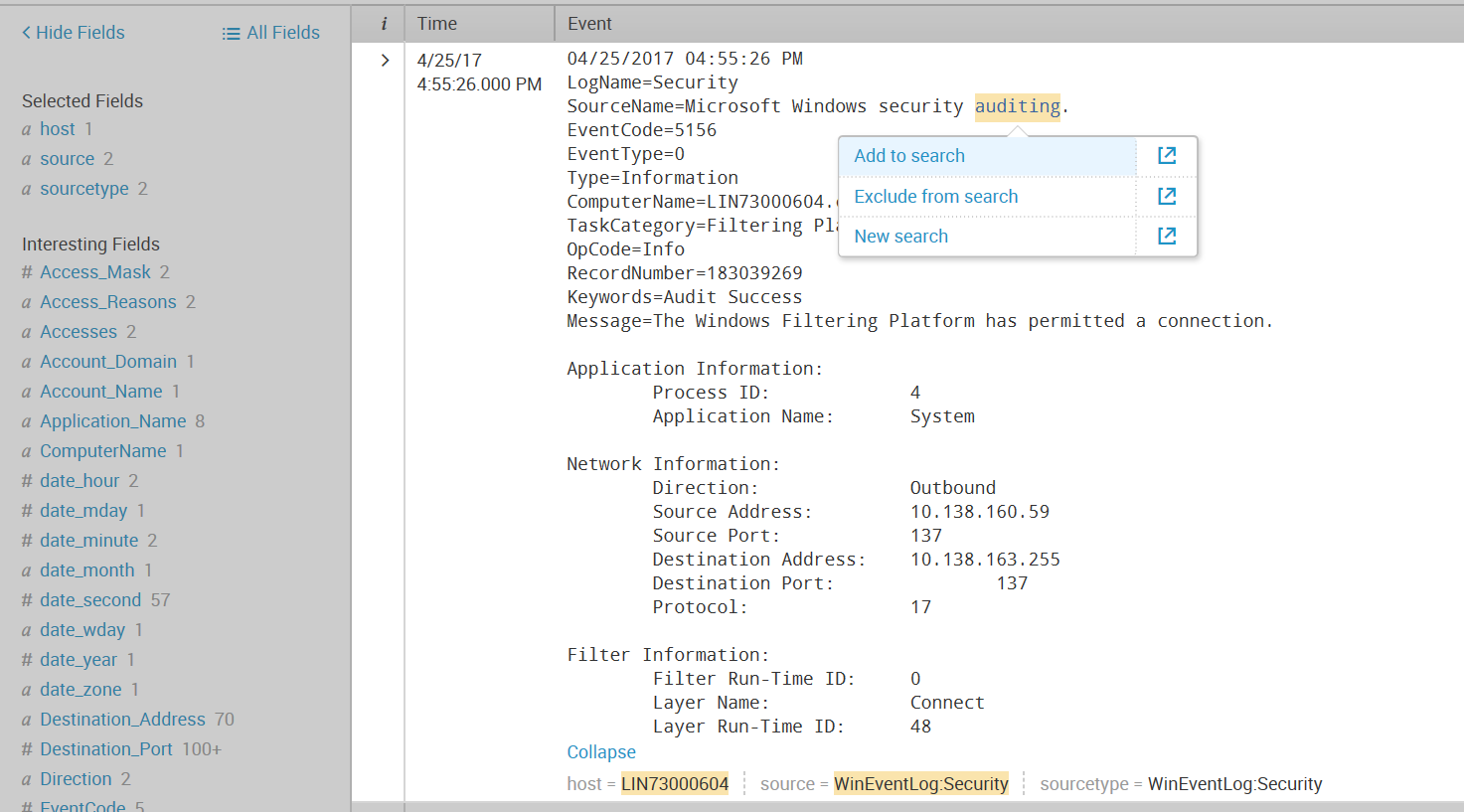
****

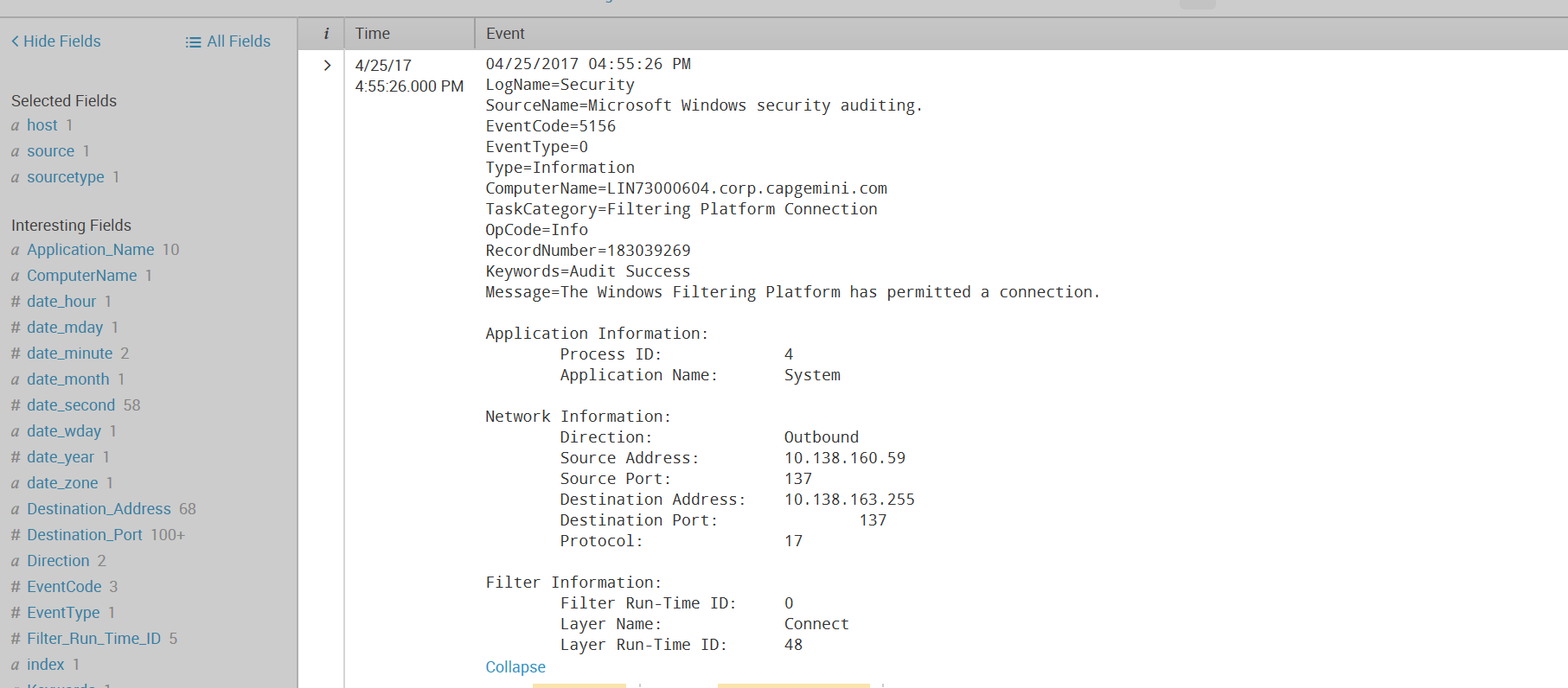
**Search by host, source, and sourcetype**

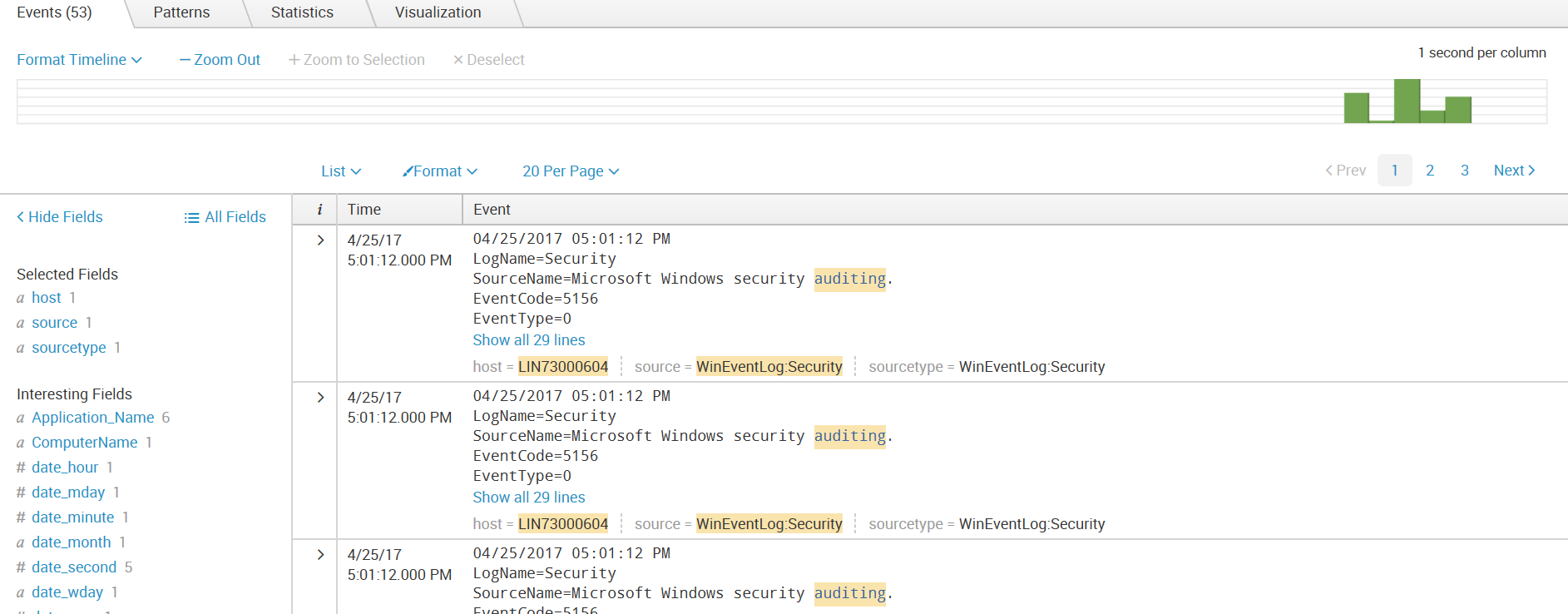
****

****

**Add to search**

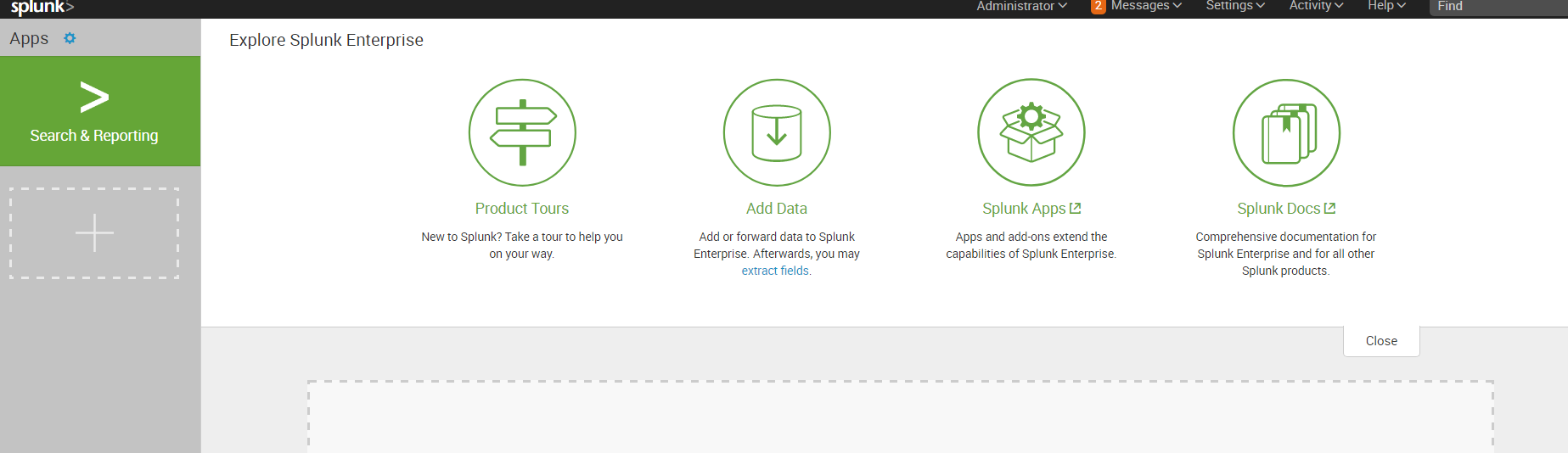


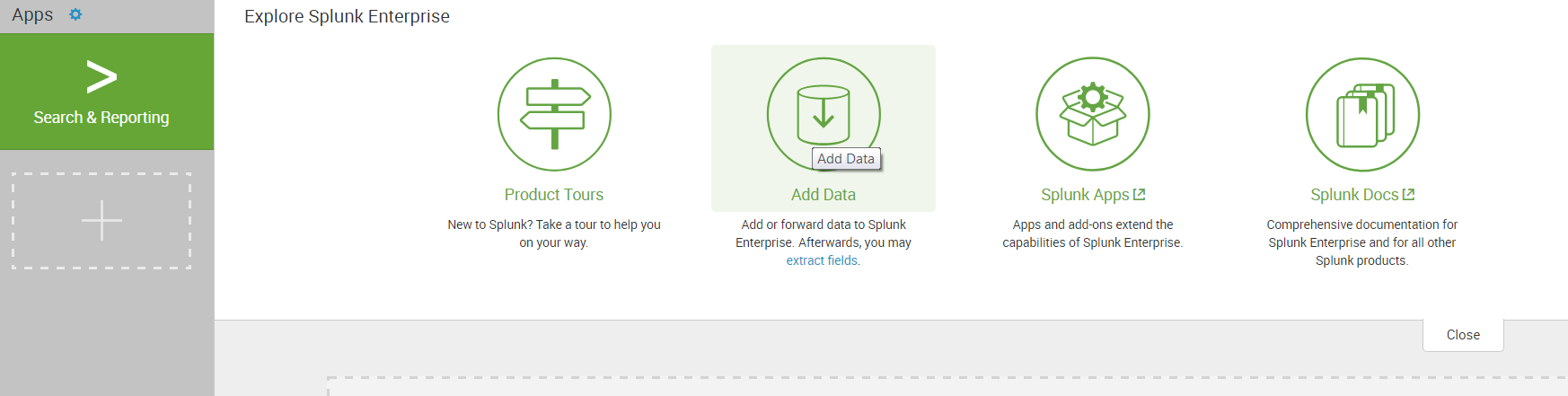
****

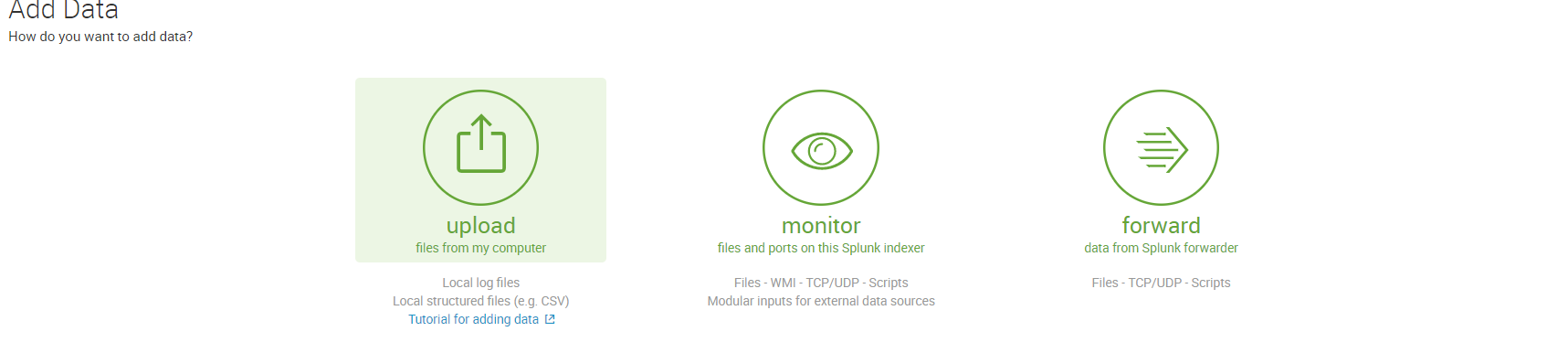


Upload sample data

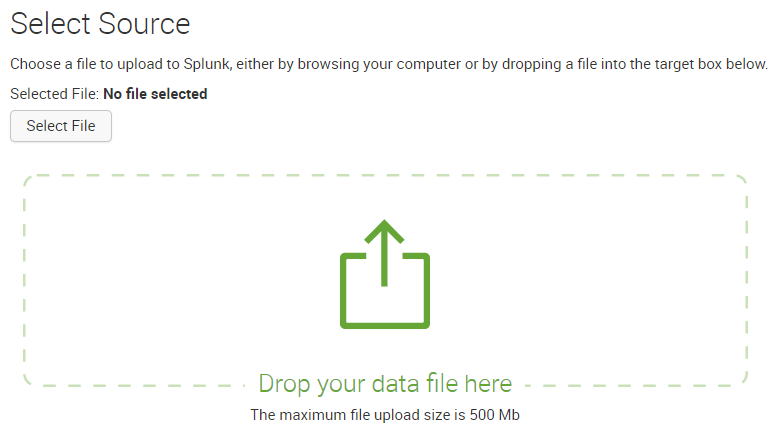
1. Click on Splunk 🡪 Add Data

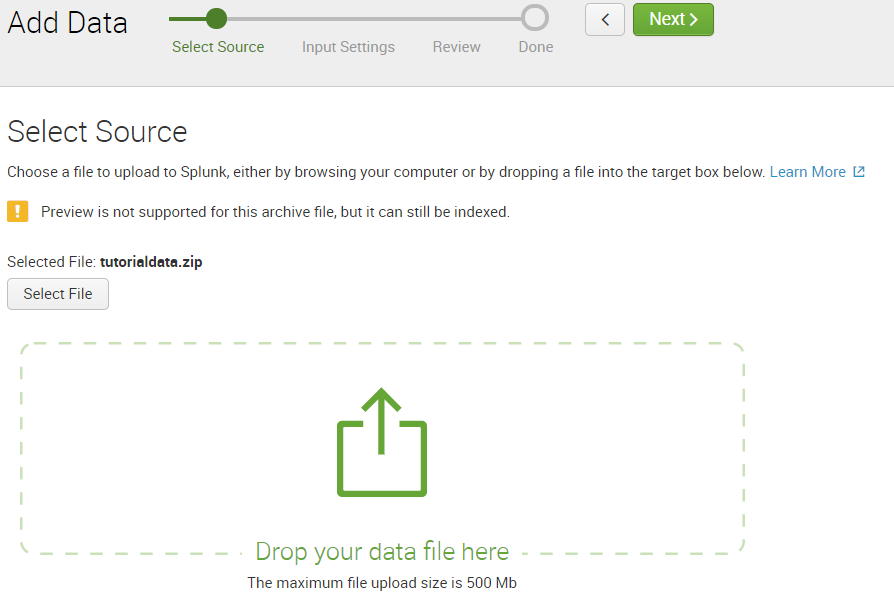




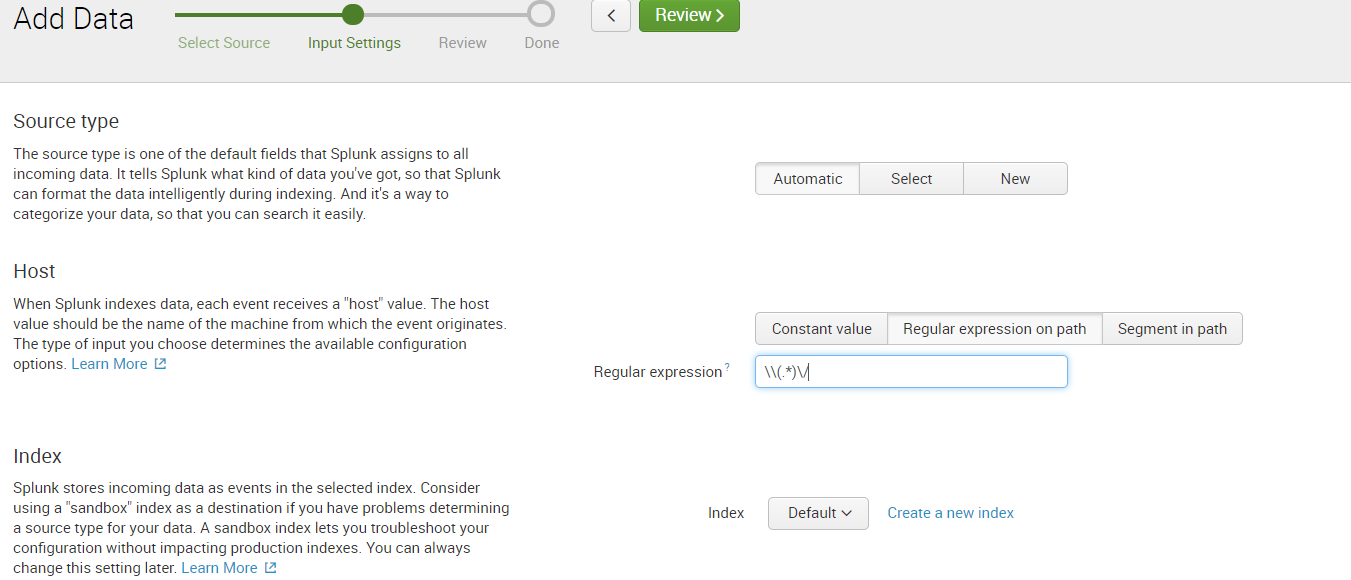


1. Under Select Source, click Select File to browse for the tutorialdata.zip file

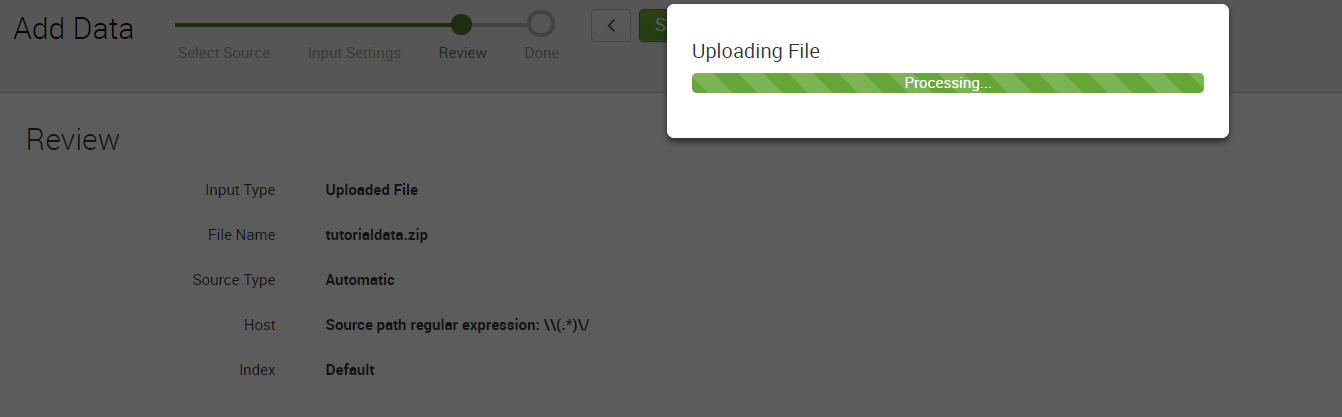


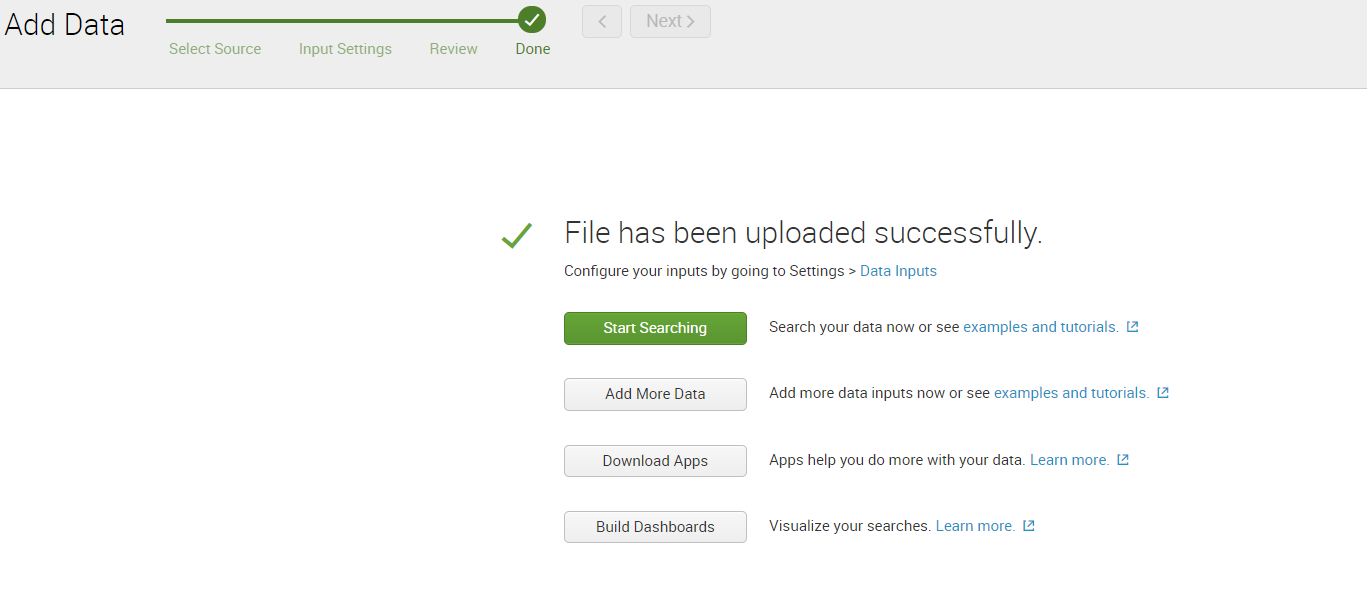


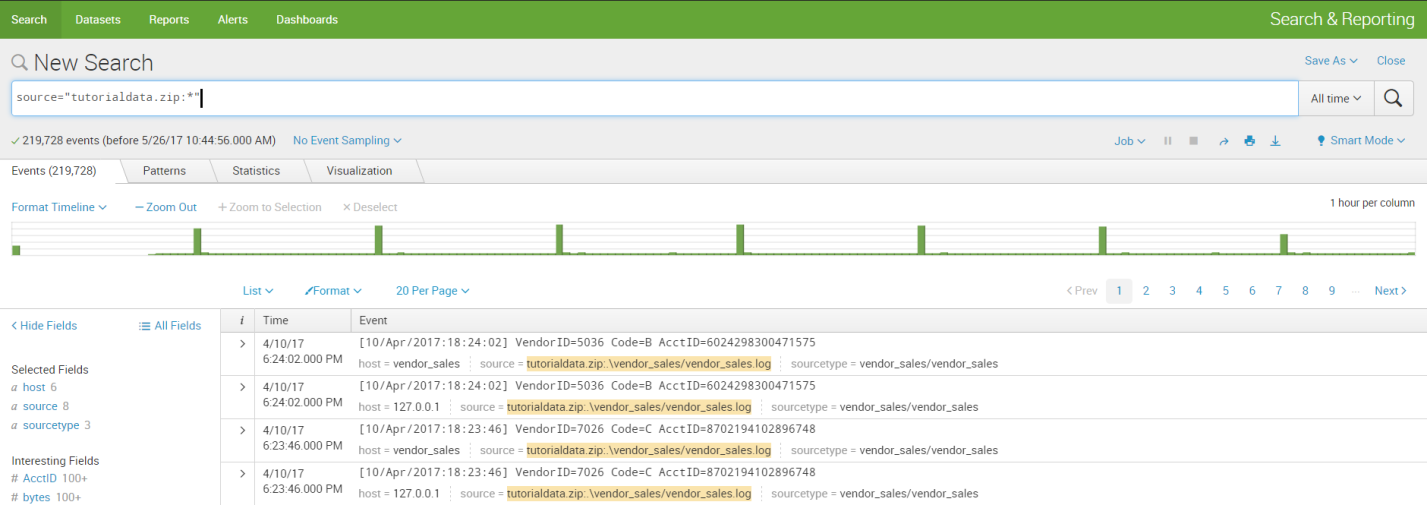
1. Select 🡪source type -> automatic, set the regular expression as given below , index -> default



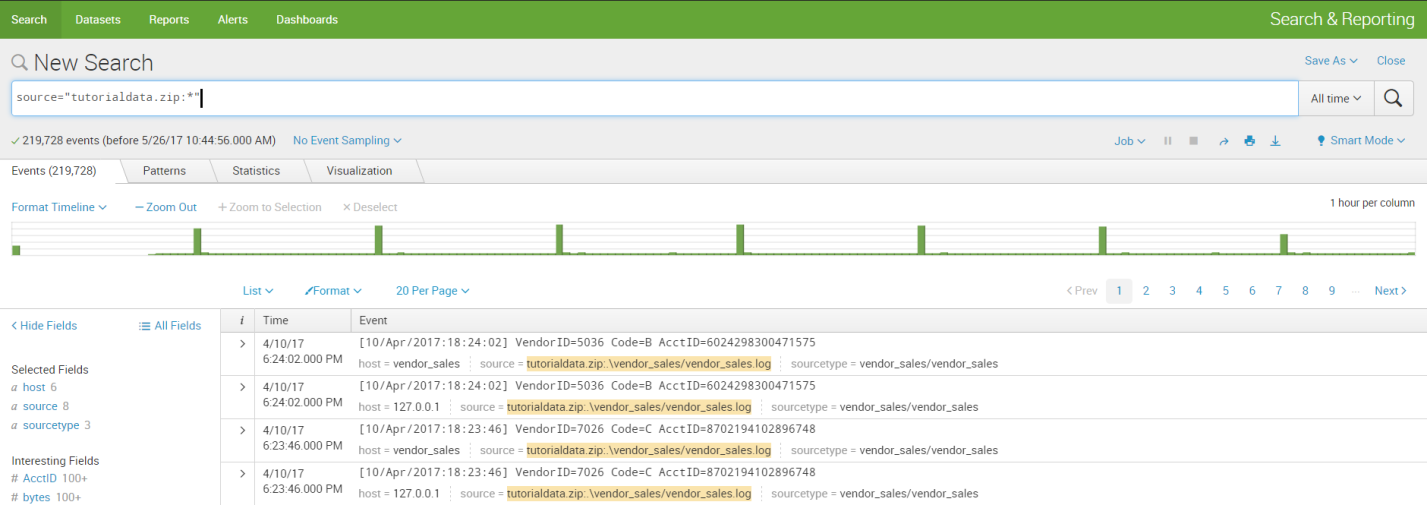
1. Click on Review 🡪 Next



 Click on start searching



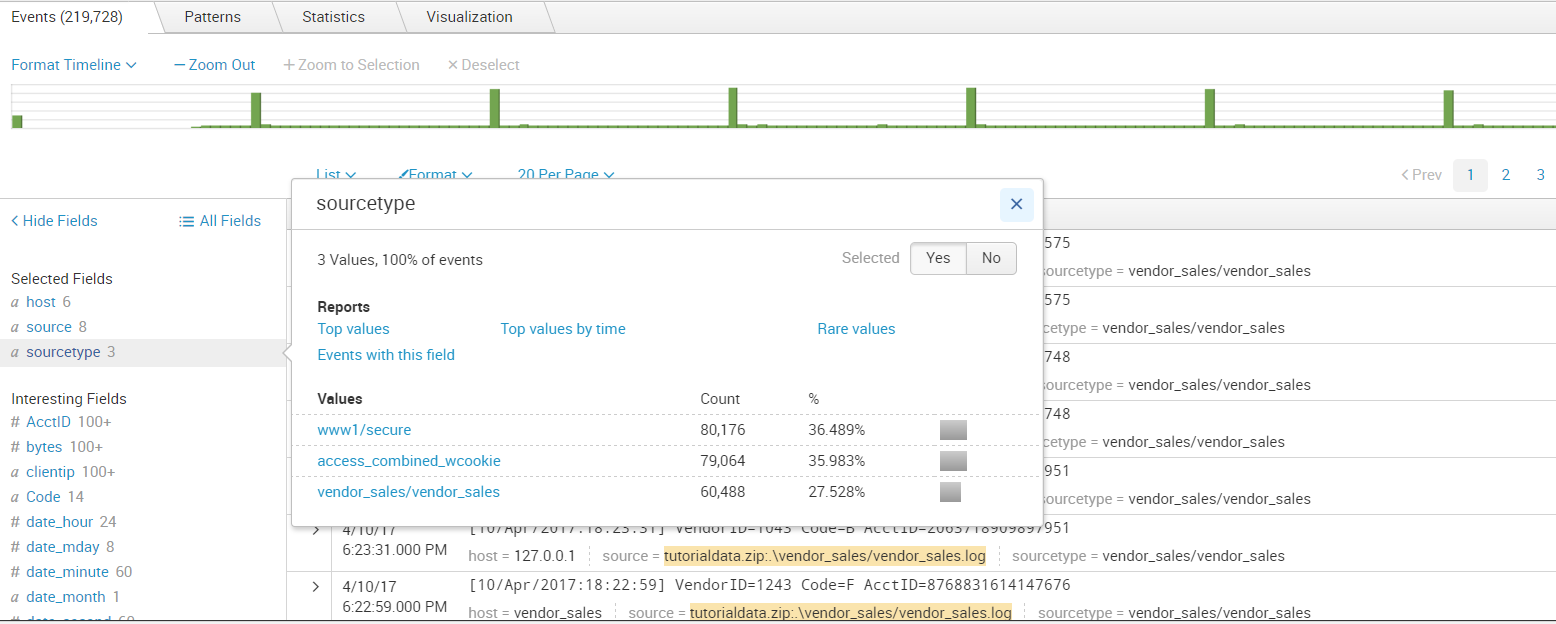
Click Splunk Home to return



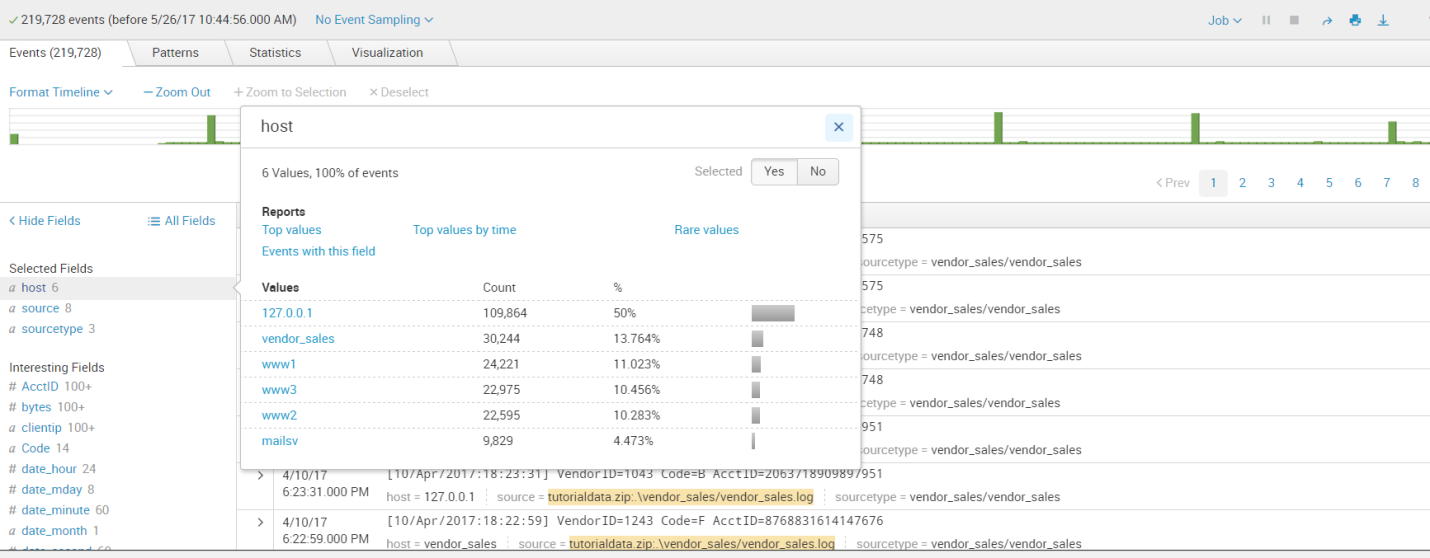
Click on Source tab to see the list of sources



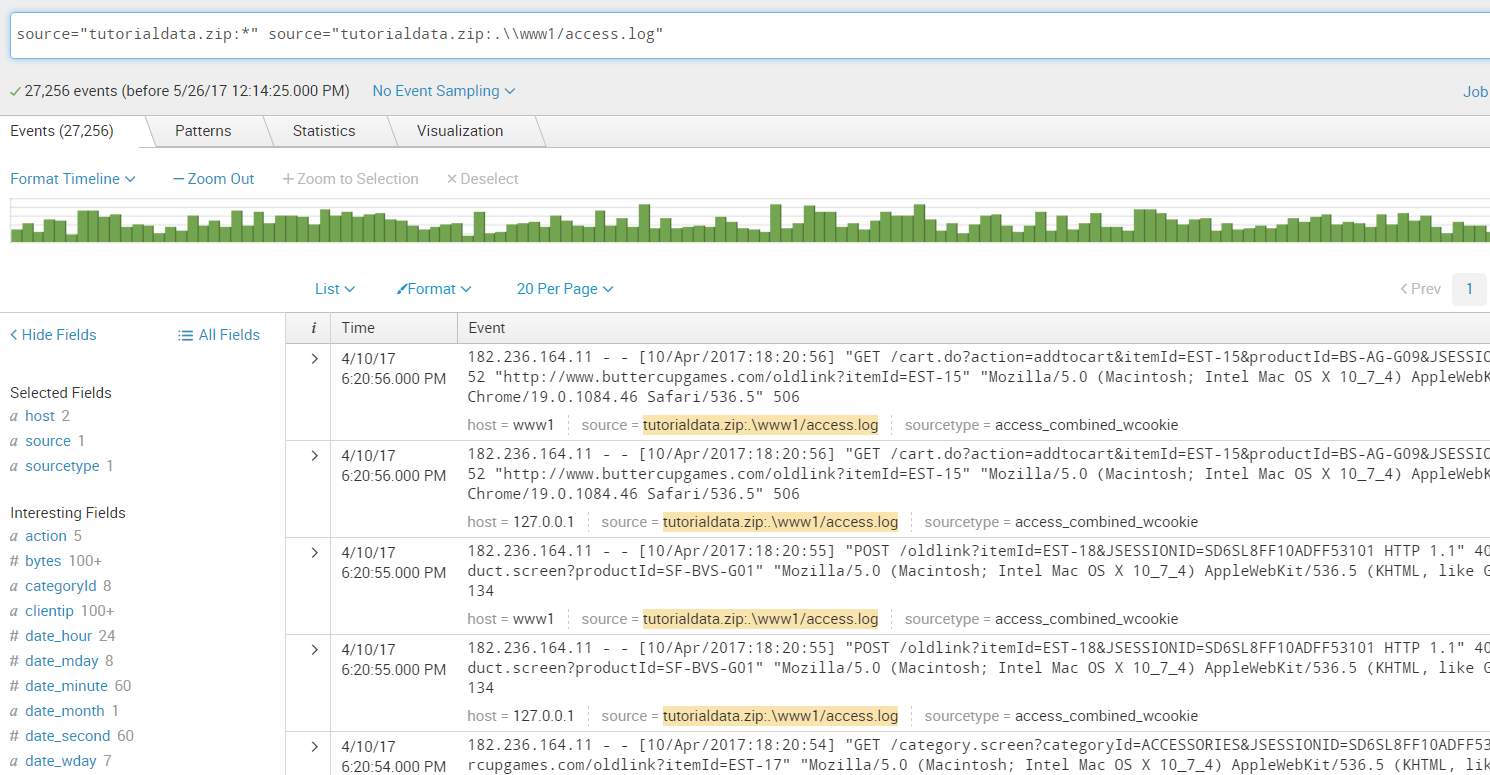
Click on Source type



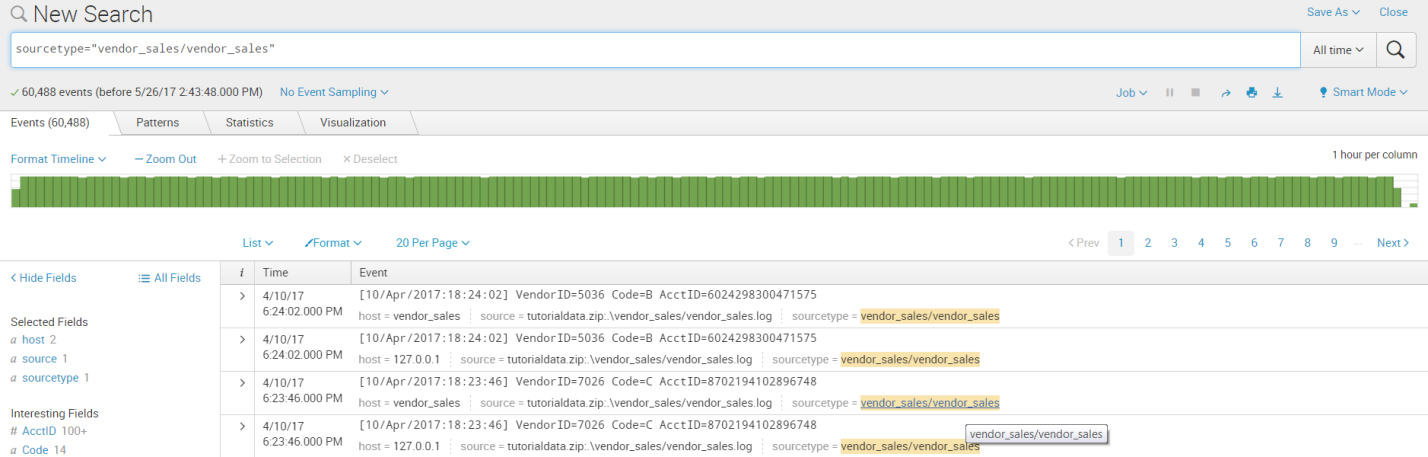
Click on host



Search for the sources

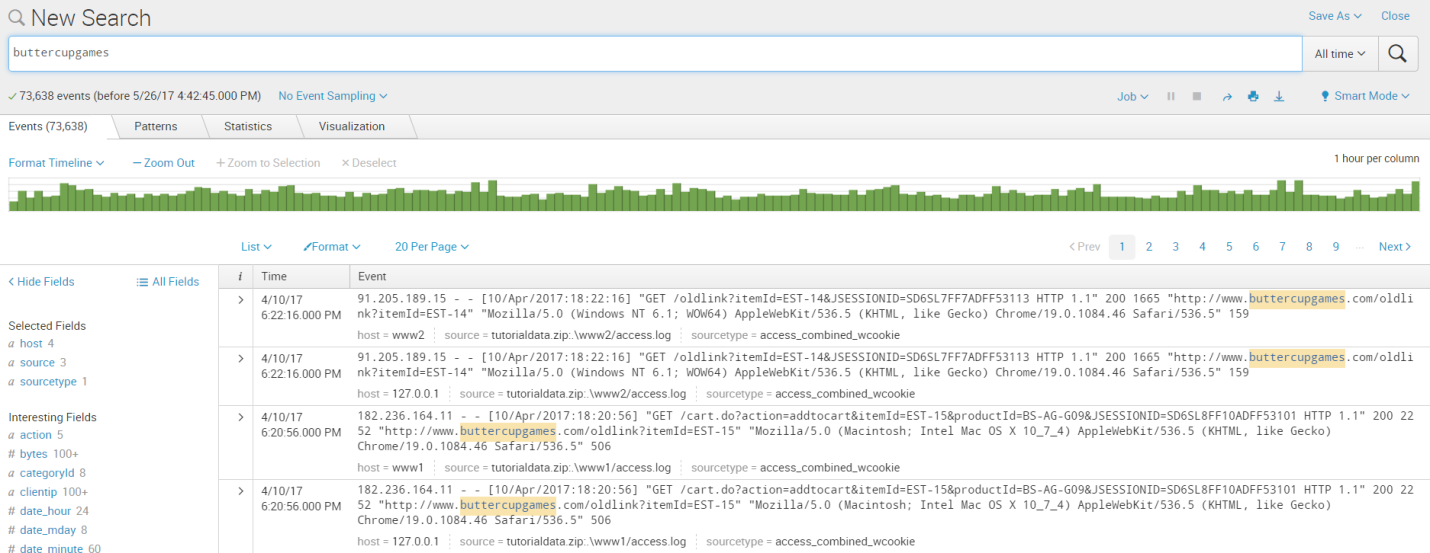


Click on sourcetype 🡪vendorsales

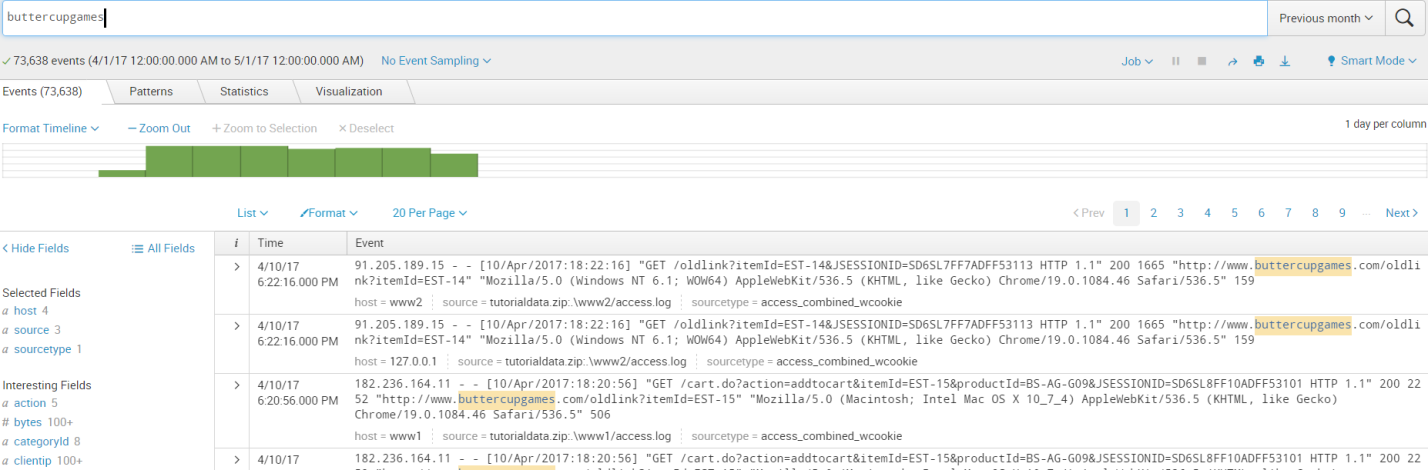


Searches based on time ranges

Exploring data from Buttercup games online store using different time ranges.



Click on Presets 🡪Relative 🡪yesterday

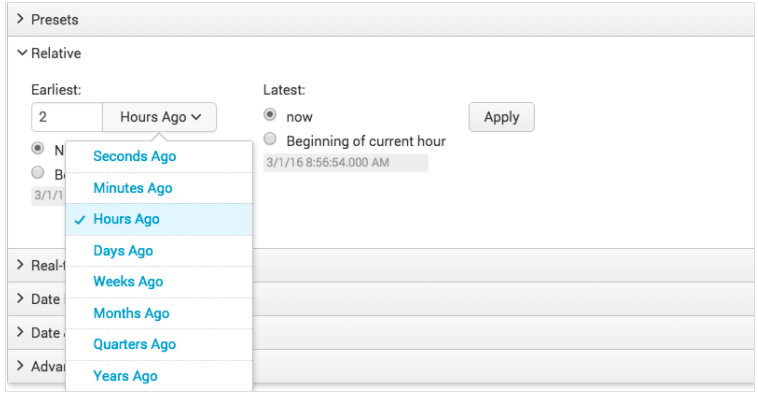


Specify relative time ranges

You can use the Relative option to specify a custom time range.

1. Open the time range picker.

2. To run a search over the last two hours, select the Relative time range option



**Specify date and time ranges**

You can also use the **Date Range** and **Date & Time Range** options to specify a custom time range.

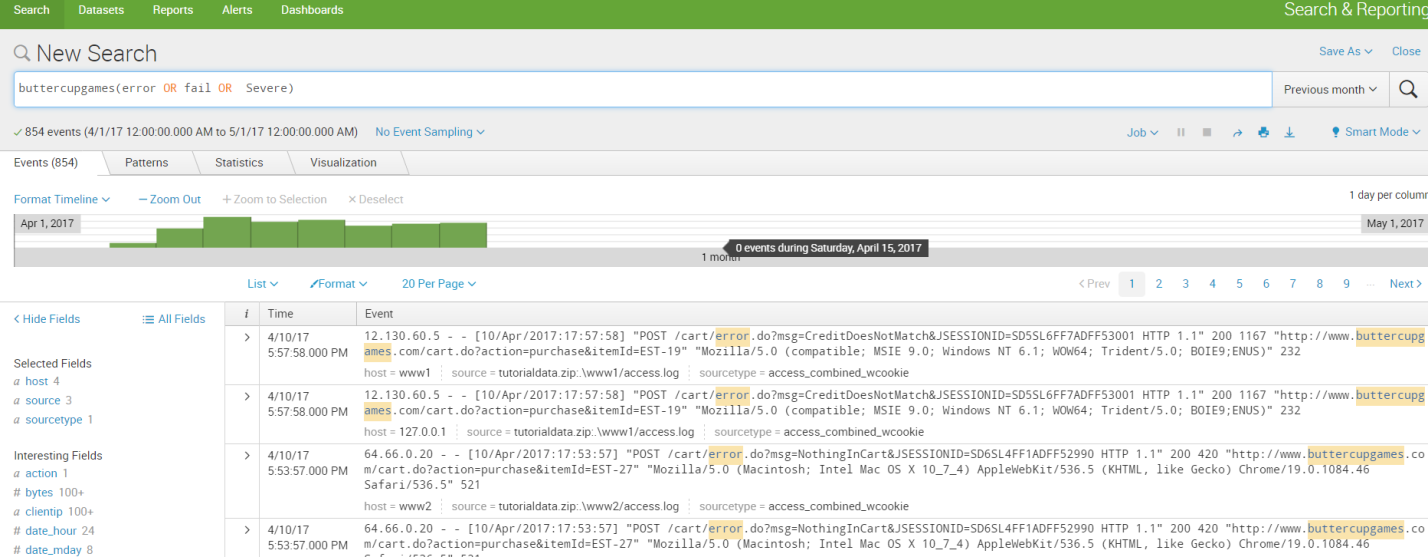
* Use **Between** to specify that events must occur between an earliest and latest date.
* Use **Before** to specify that events must occur before a date.
* Use **Since** to specify that events must occur after a date.

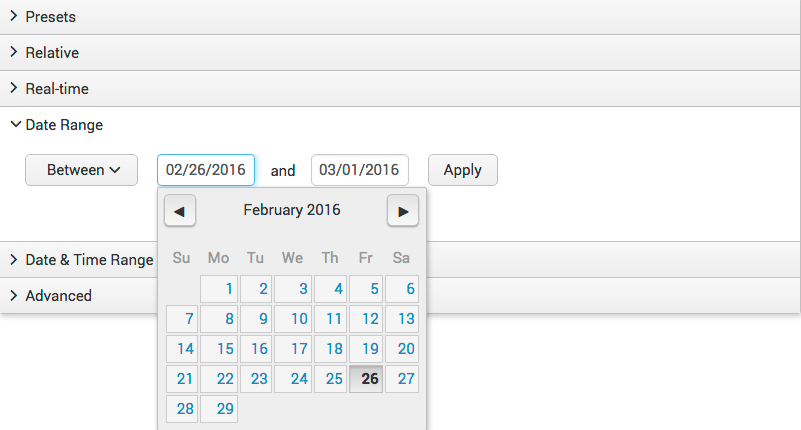
You use the **Date Range** option to specify dates. The following screen image shows the calendar that you can use to select a date.

To search for the terms error, fail, failure, failed, or severe, in the events that also mention buttercupgames, run the following search.

buttercupgames (error OR fail\* OR severe)

Tip: Instead of typing the search string, you can copy and paste the search Click the spyglass icon to the right of the time range picker to run the search.



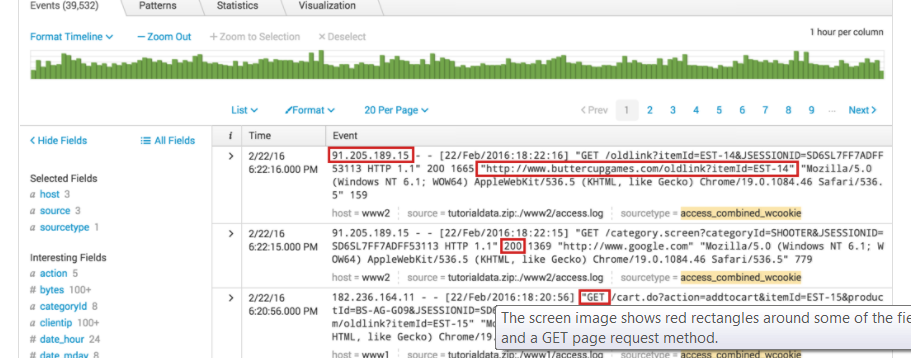
[](http://docs.splunk.com/File:6.4_timerange_daterange.png)

Search with filed name



Access combined format of Apache logs,

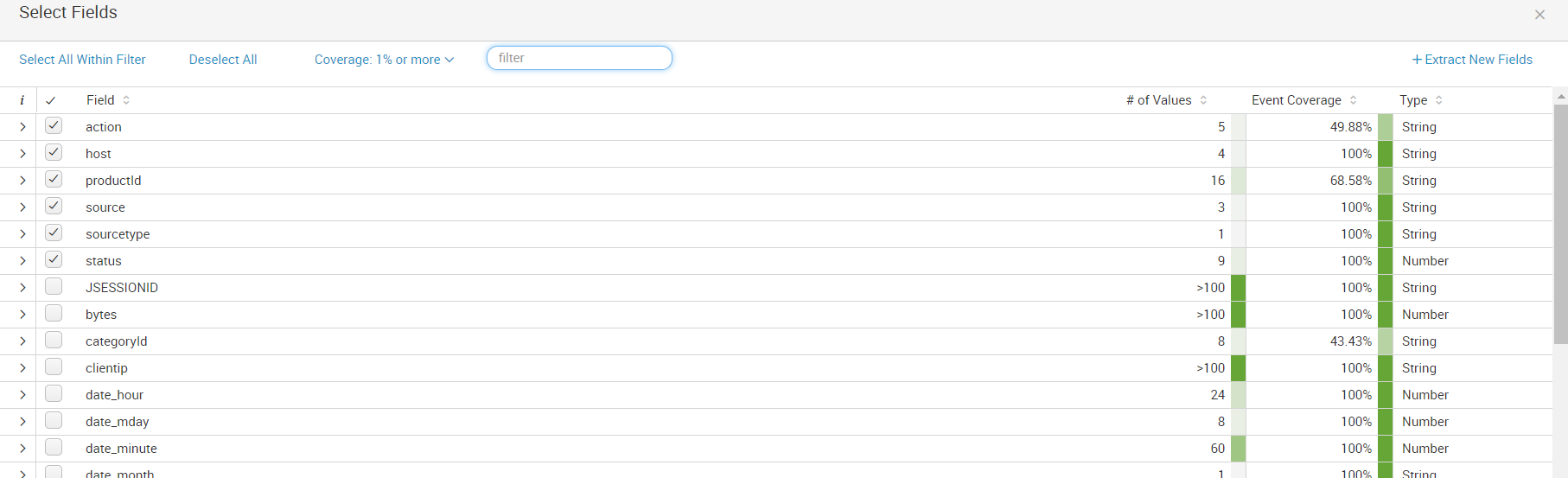
* IP addresses for the users accessing the website.
* URIs and URLs for the pages requested and referring pages.
* HTTP status codes for each page request.
* GET or POST page request methods.



Specify Selected Fields

To add fields to the Selected Fields list, click All Fields.

The Select Fields dialog box shows a list of fields in your events. The # of Values column shows the number of unique values for each field in the events. Because your search criteria specifies the source type, the sourcetype field has just 1 value.

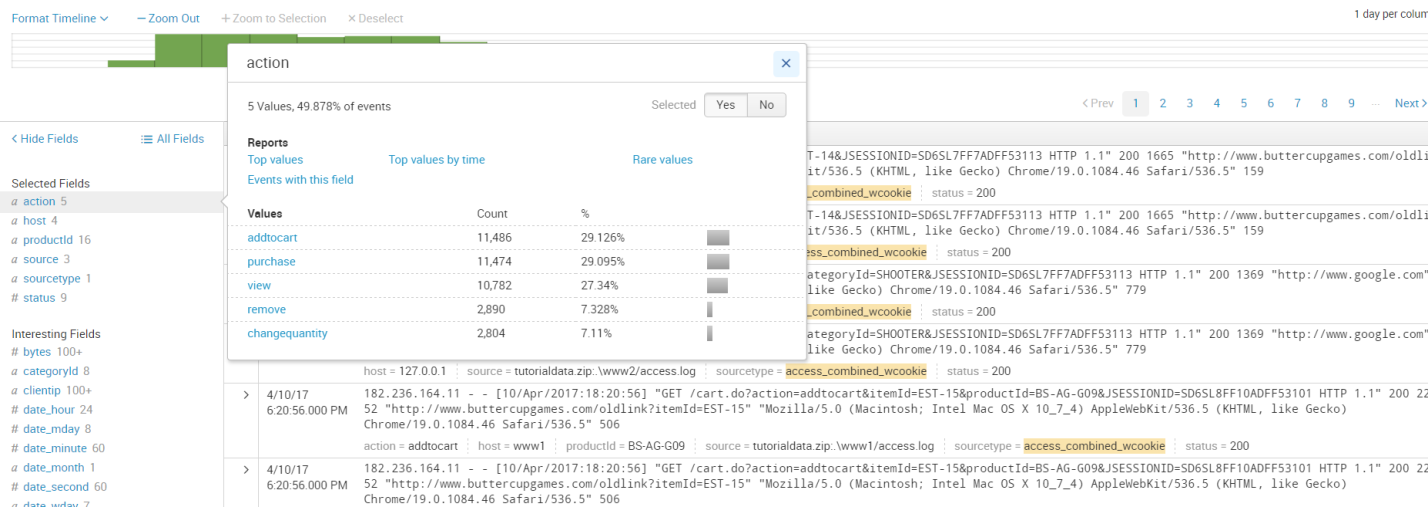


Identifying field values

The Fields sidebar displays the number of unique values for each field in the events. These are the same numbers that appear in the Select Fields dialog box.

1. Under Selected Fields, notice the number 5 next to the action field.

2. Click the action field.



Run targeted Searches

### Search for successful purchases

Search for successful purchases from the Buttercup Games store.

1. Start a new search.

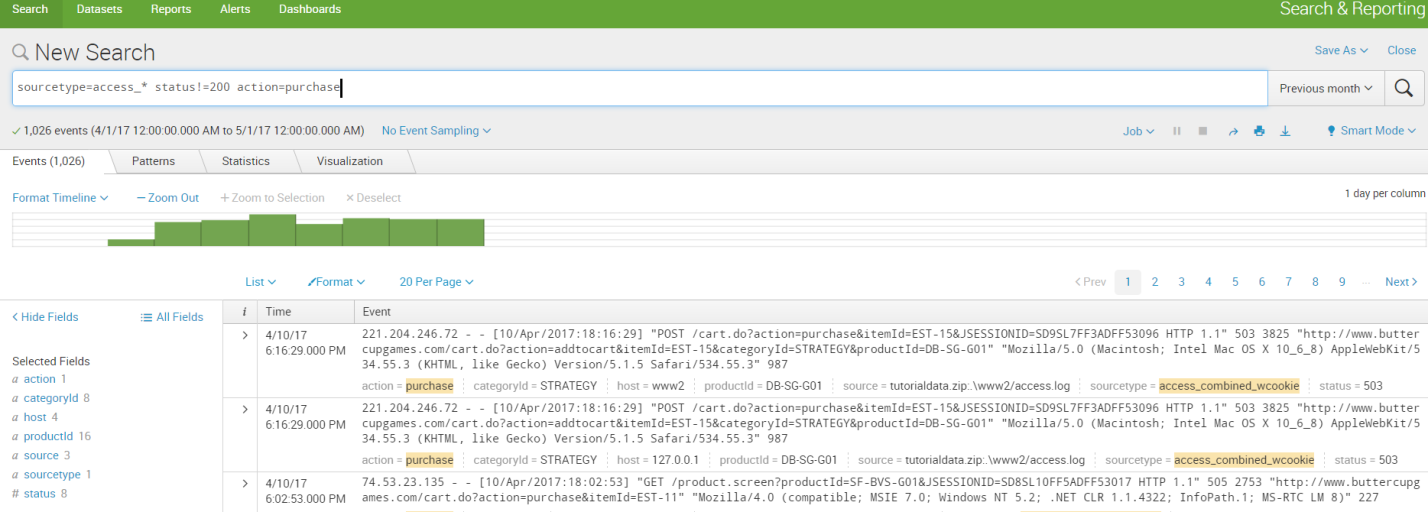
2. Run the following search.

sourcetype=access\_\* status=200 action=purchase



3. Change the status portion of the search and run the search again

sourcetype=access\_\* status!=200 action=purchase



Search for errors

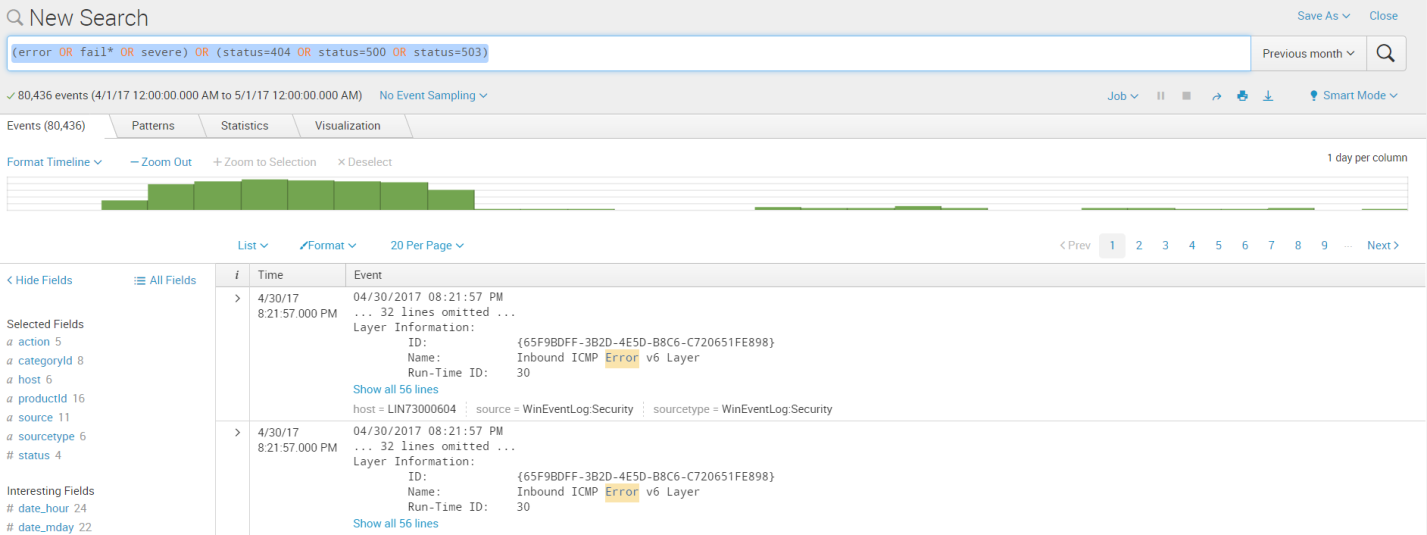
The way that errors are designed in events varies from source to source. To search for errors, your search must specify these different designations.

Use Boolean operators to specify different error criteria. Use parenthesis to group parts of your search string.

1. Start a new search.

2. Run the following search.

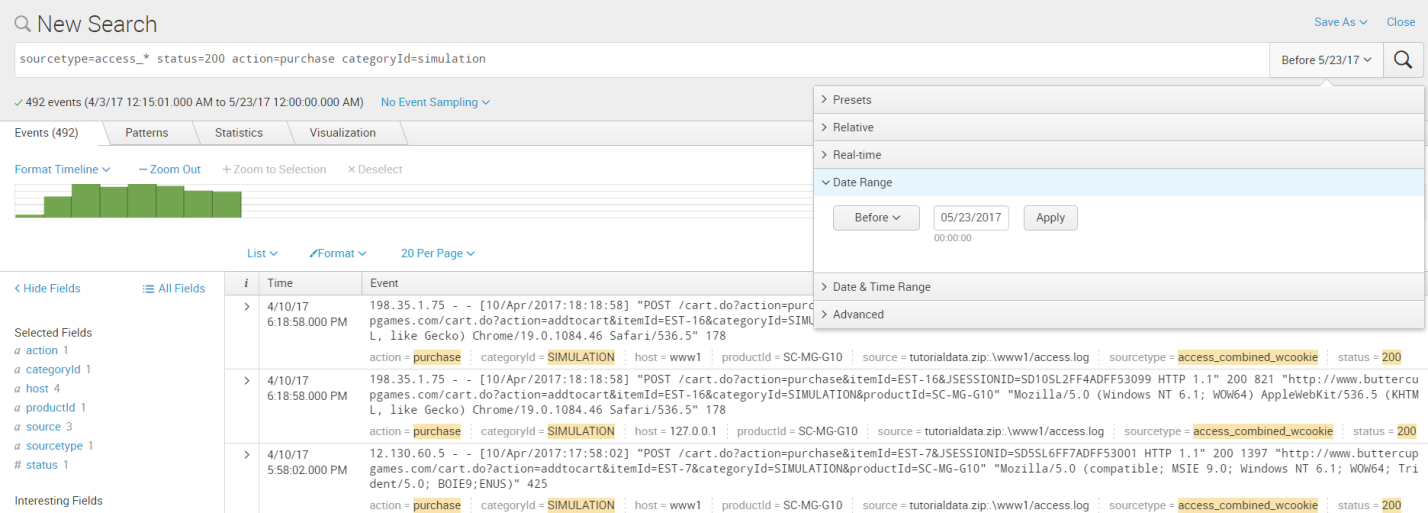
(error OR fail\* OR severe) OR (status=404 OR status=500 OR status=503)

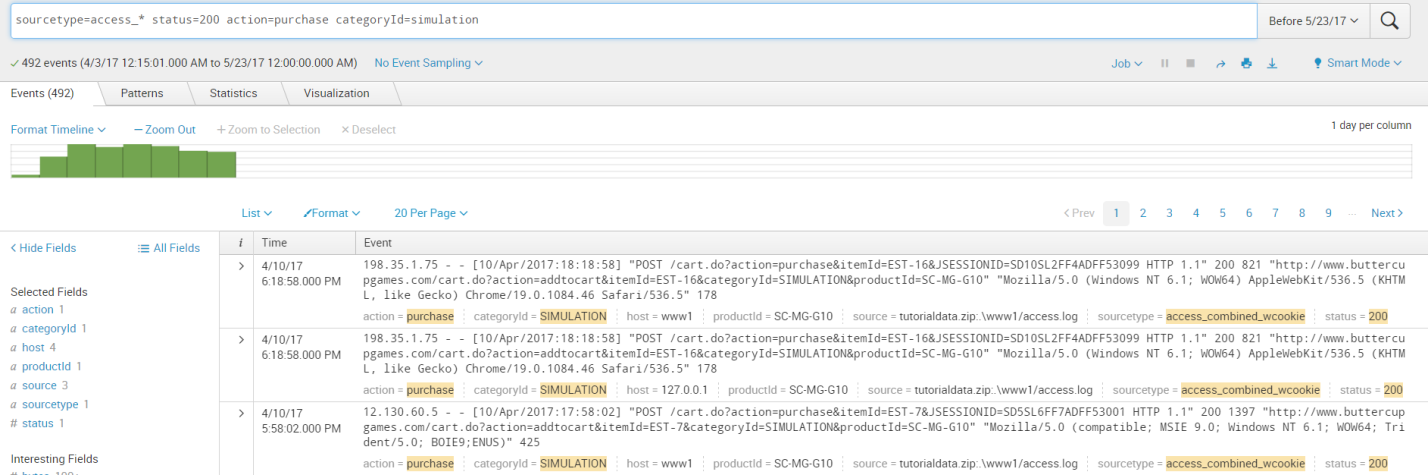


### Search for sales of a specific product

Search for how many simulation style games were bought yesterday.

1. In the time range picker,  presets 🡪All Time
2. Date Range 🡪 Before 05/23/2017





4. Find the number of purchases for each type of product sold at the shop.

a. Locate the unique categoryId values by clicking on the categoryId field in the Selected Fields list.

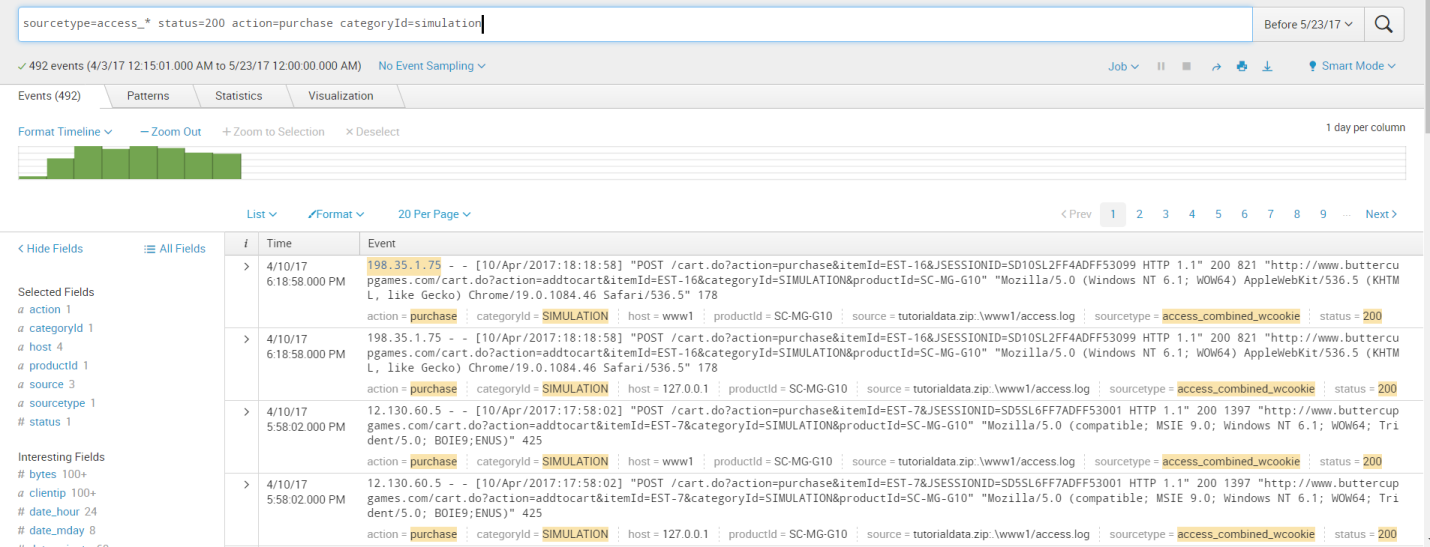
b. Run the search in step 2 for each unique categoryId value.

**Using the Search Language**

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

1. To know how many simulation games were purchased

sourcetype=access\_\* status=200 action=purchase categoryId=simulation

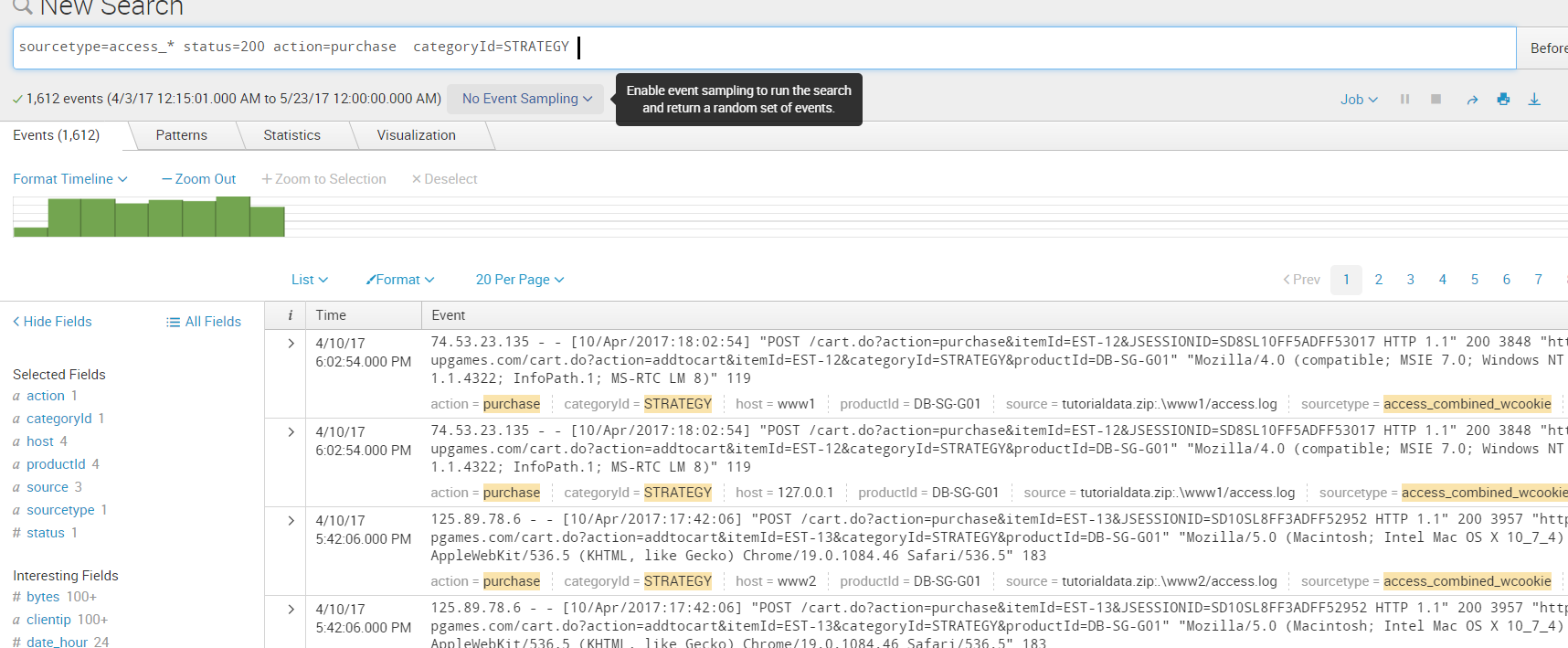


2. Start a new search and restrict your search to Yesterday.

 Type source in the Search bar.

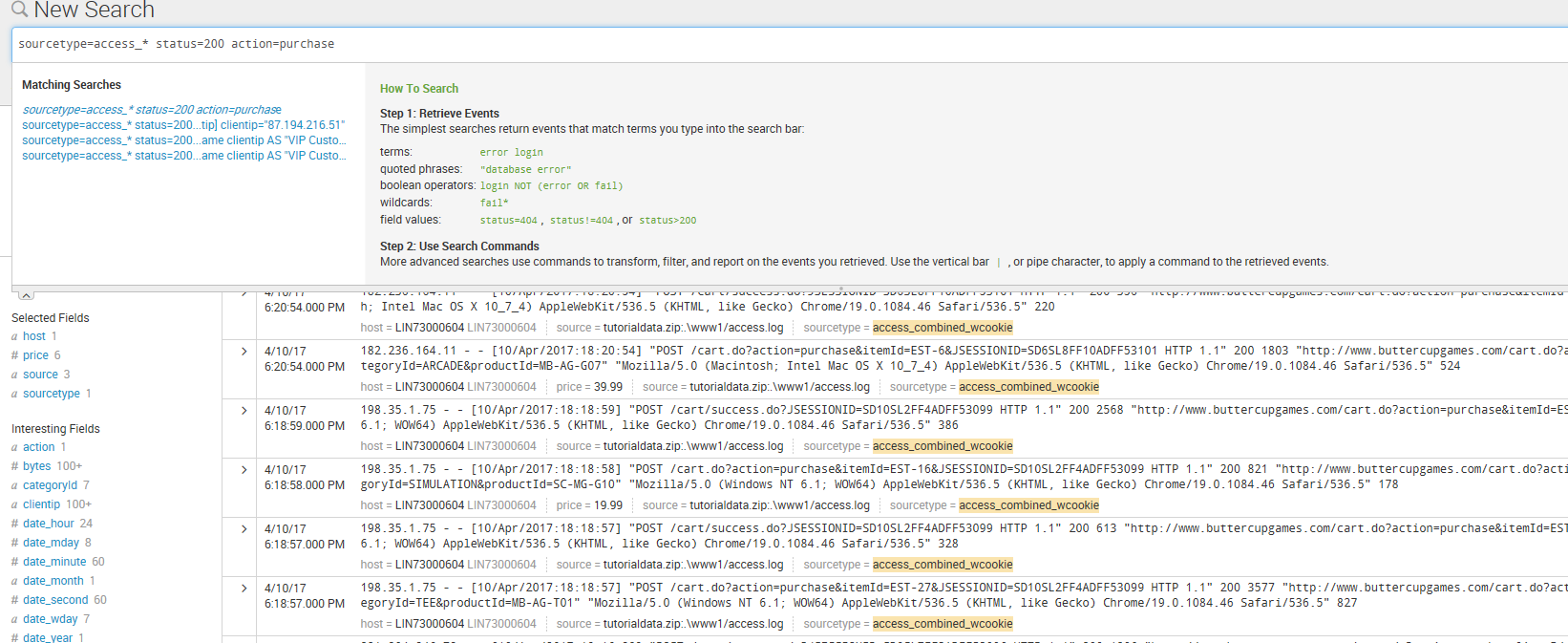
As you type in Search bar, the Search Assistant opens with a list of Matching Searches and the Matching Terms.

3. Select the following search from the Matching Searches, or type the search into the Search bar.



3. Select the following search from the **Matching Searches** list, or type the search into the Search bar.

sourcetype=access\_\* status=200 action=purchase



4.  Return the most popular items bought at the Buttercup Games online store.

sourcetype=access\_\* status=200 action=purchase | top categoryId

