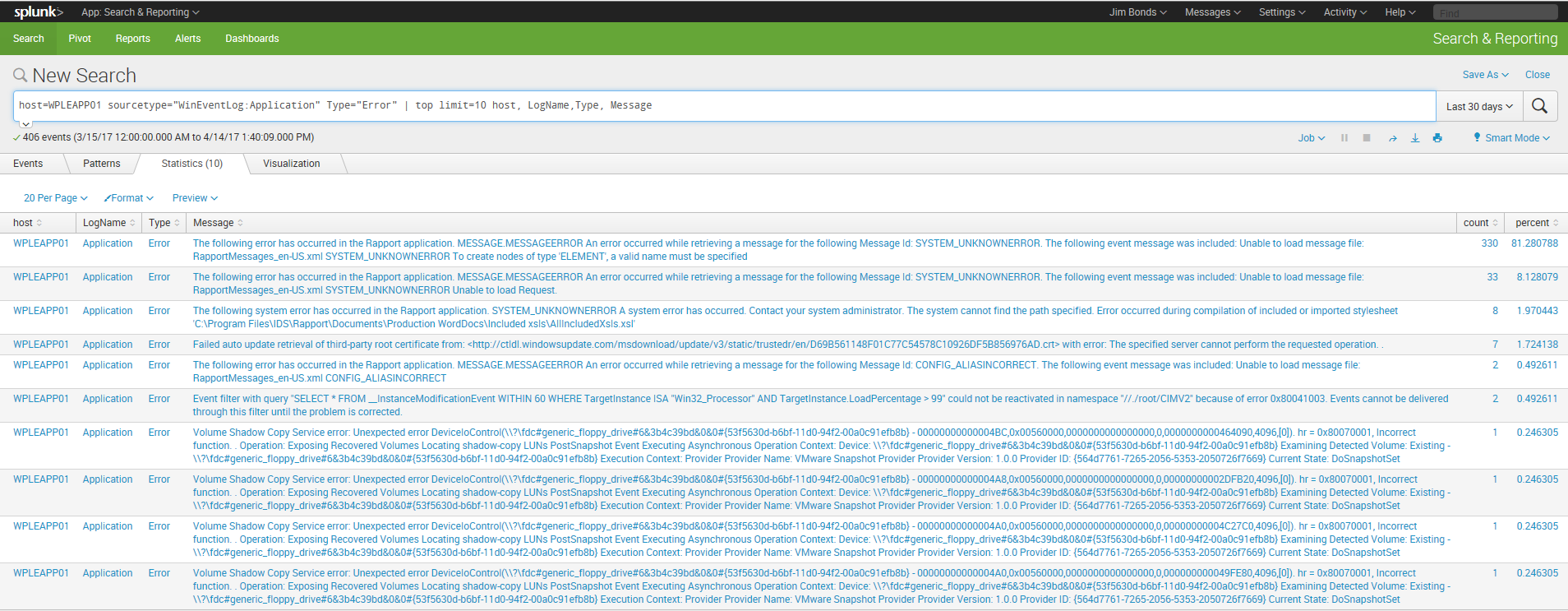
SplunK:



What is Splunk? It is a tool used for Data Analytics. We use Splunk to analyze machine data (log files). Splunk can be used to move, index and store machine data.

We will use the Splunk Web Browser to process data from different Splunk environments. Splunk instances can be set up in different locations (servers) and streamed up to one Splunk main environment.

Regions Splunk Web Page: <http://upsplnksch01:8000/en-US/account/> (login with Regions Id and password.)

Splunk vocabulary:

Index - put files into readable format.

Event - single row in event log that has a time stamp and is searchable.

Search - Look up by time stamp Id or event code Ids.

Pivot – not a pivot table, but any kind of table, charts or search we keep.

Dashboard – collection of Pivots.

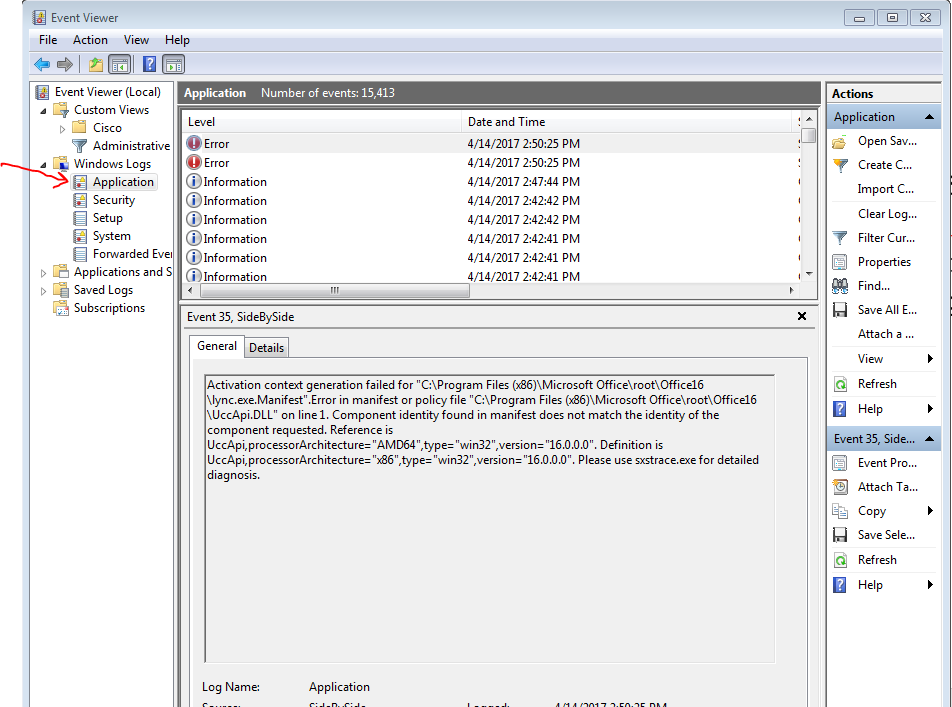
Forwarder – piece that sends data to our Splunk environment.

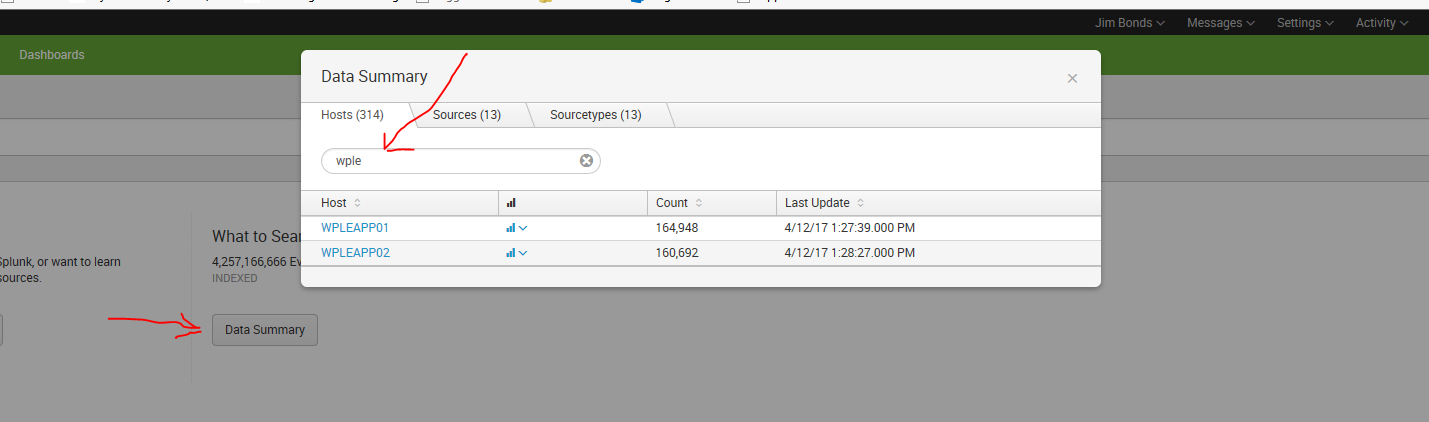
Basic Splunk Techniques:

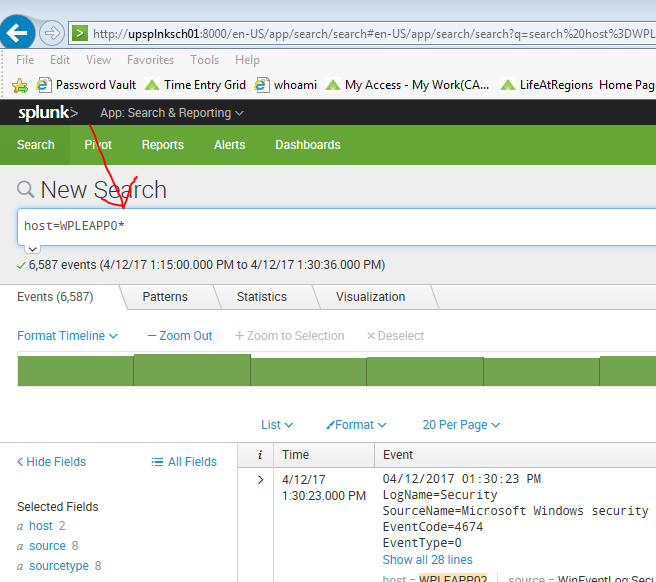
Add data:

The first thing you will need to do is Add data. To add data, click on Data Summary. This is a list of servers that have Splunk forwarders. If you don’t see your server, create a Landdesk (Software Distribution) ticket to have a Splunk forwarder installed.

When WPLEAPP0\* forewarders were set up to monitor windows loggs, you can request to monitor any of the logfiles on the server including vindor spacific.

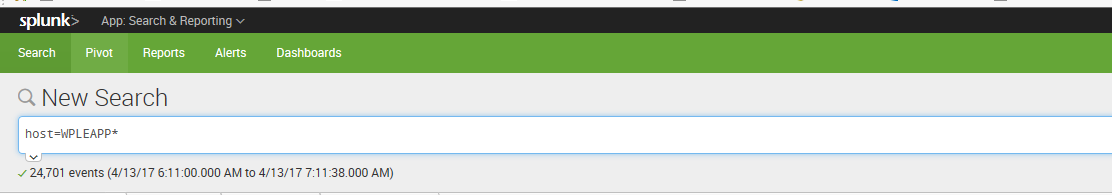




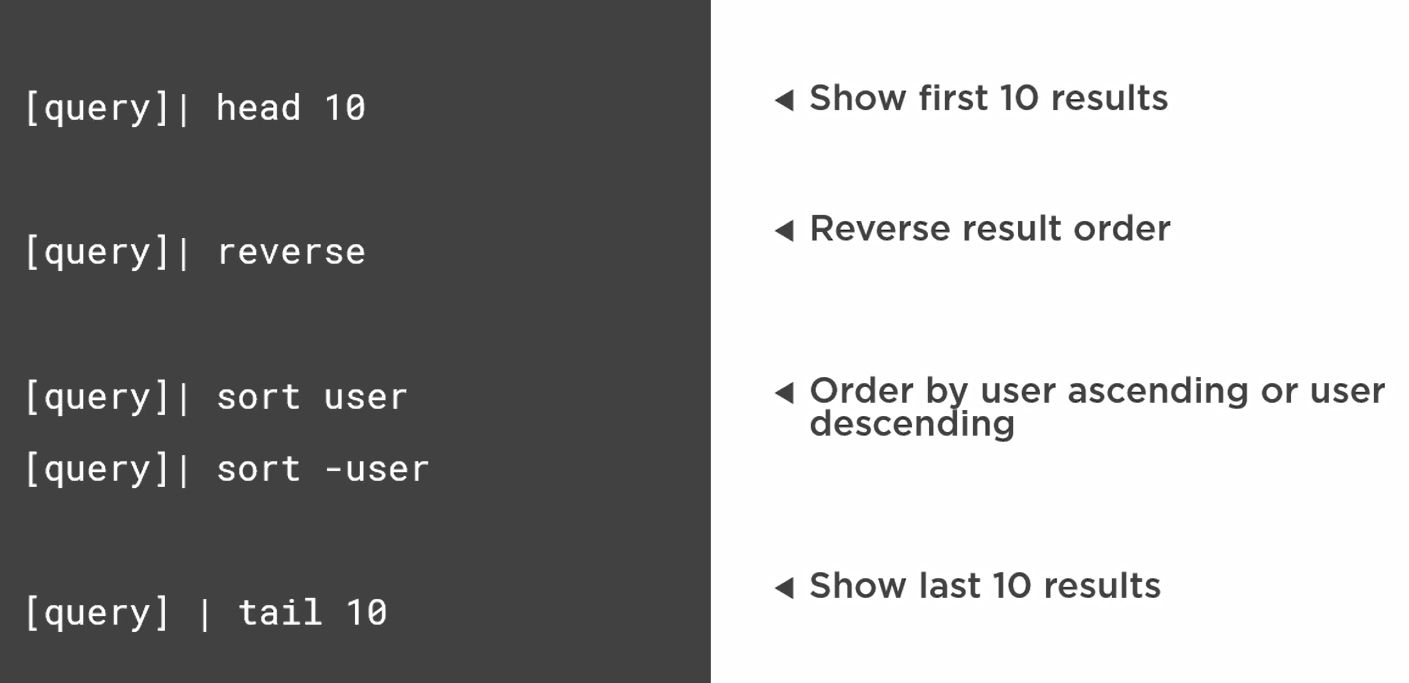
You can use wild cards (\*), to add more servers. Or, if it’s another server you add a second host=xyz\*

Search:

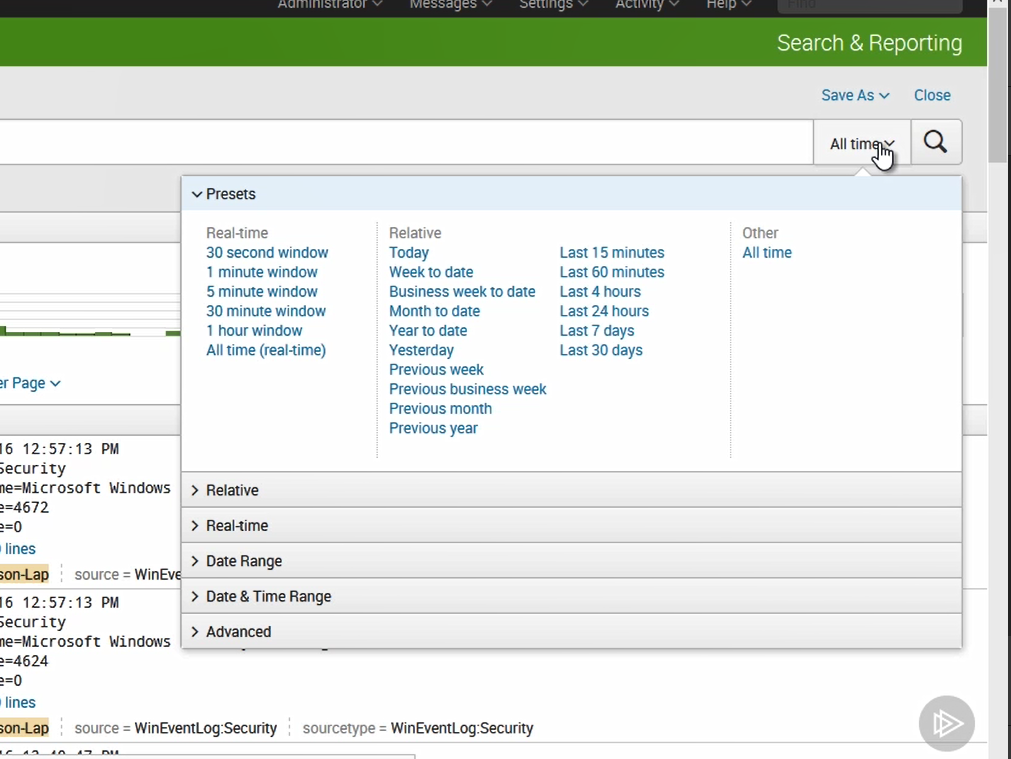
Once you have the server or servers selected you can begin to narrow your search. Search is a very powerful tool. You can search by Date Time, Event ID’s ETC. Then you can setup alerts and create dashboards.



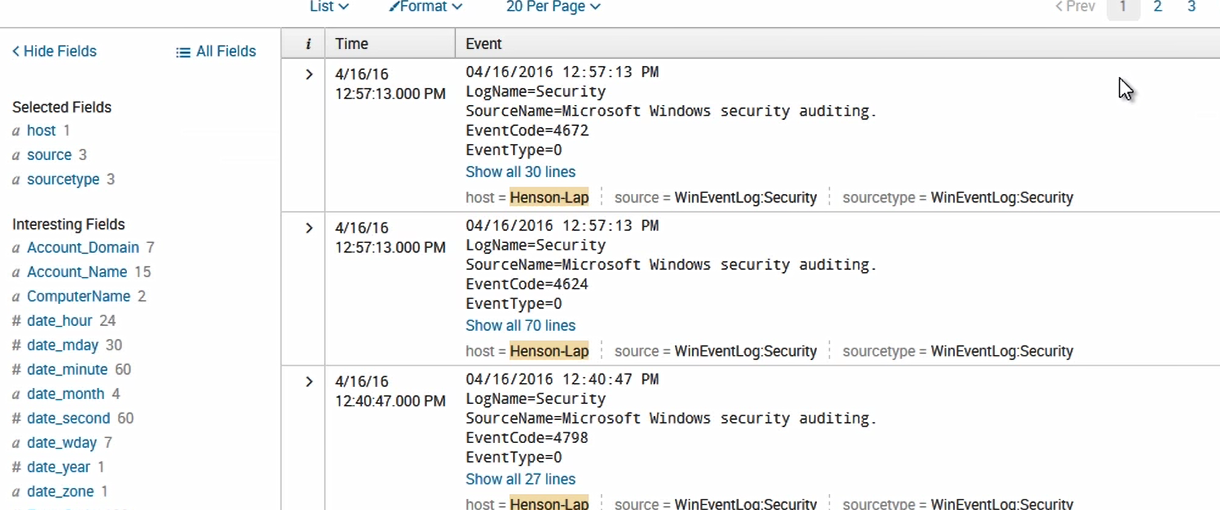
The Search Page is the first thing you see when you login. Its pulling everything from the forwarders set up on WPLEAPP\*. You can type into the Search Page to create your search. The Search Page uses Splunk Processing Language SPL. The following are examples of SPL commands.



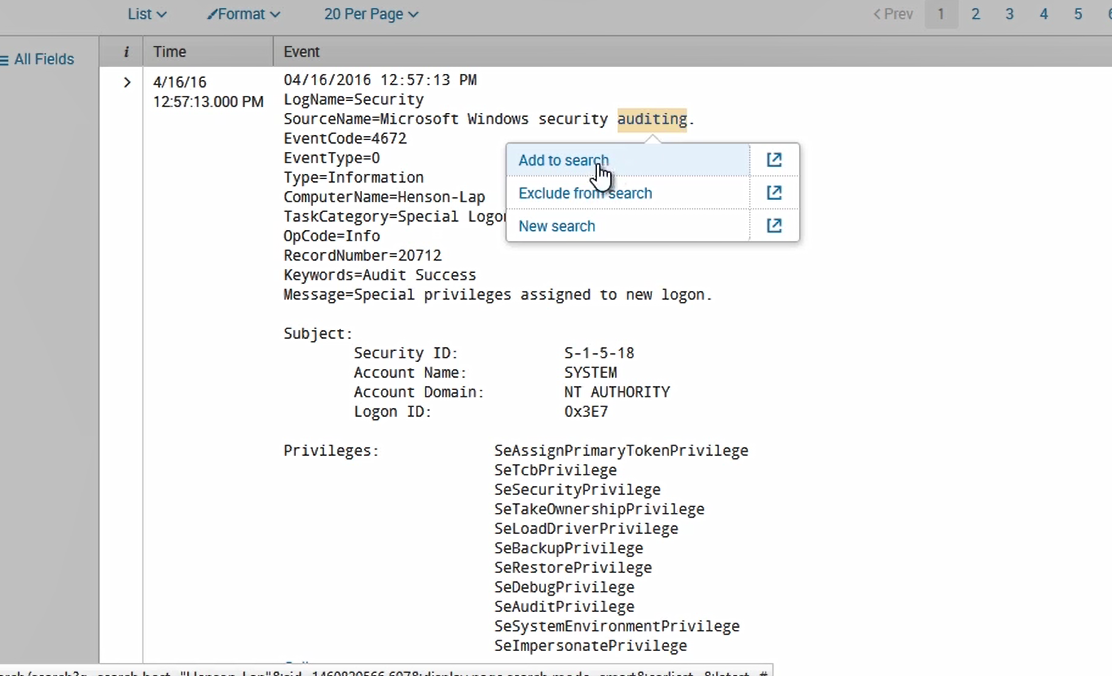
When you click around on the search page the query will be created for you. Next to the Search Bar is the Time Date Picker. You can use the preset times, and look at data as it comes in real time, setting it for a minute or five minutes. If you are looking for trends over time you can take it back a week or month. There are more tabs to give you more date search functionality.



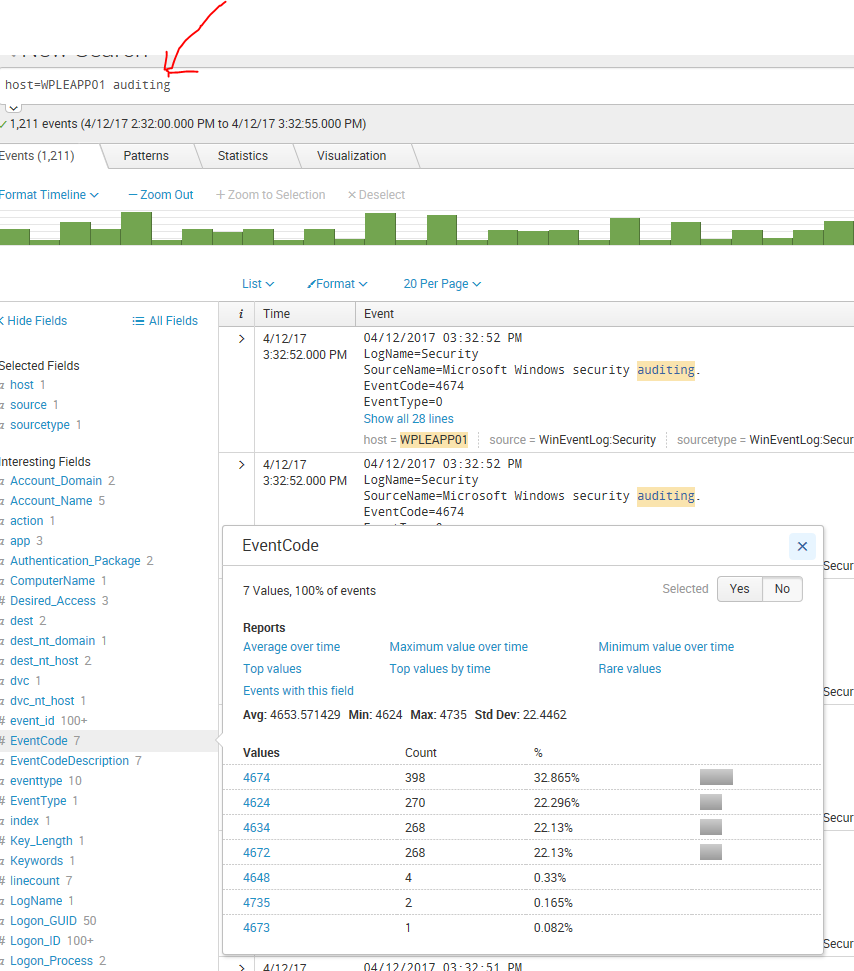
The results from your searches are in rows and listed by time by default. You can change that.



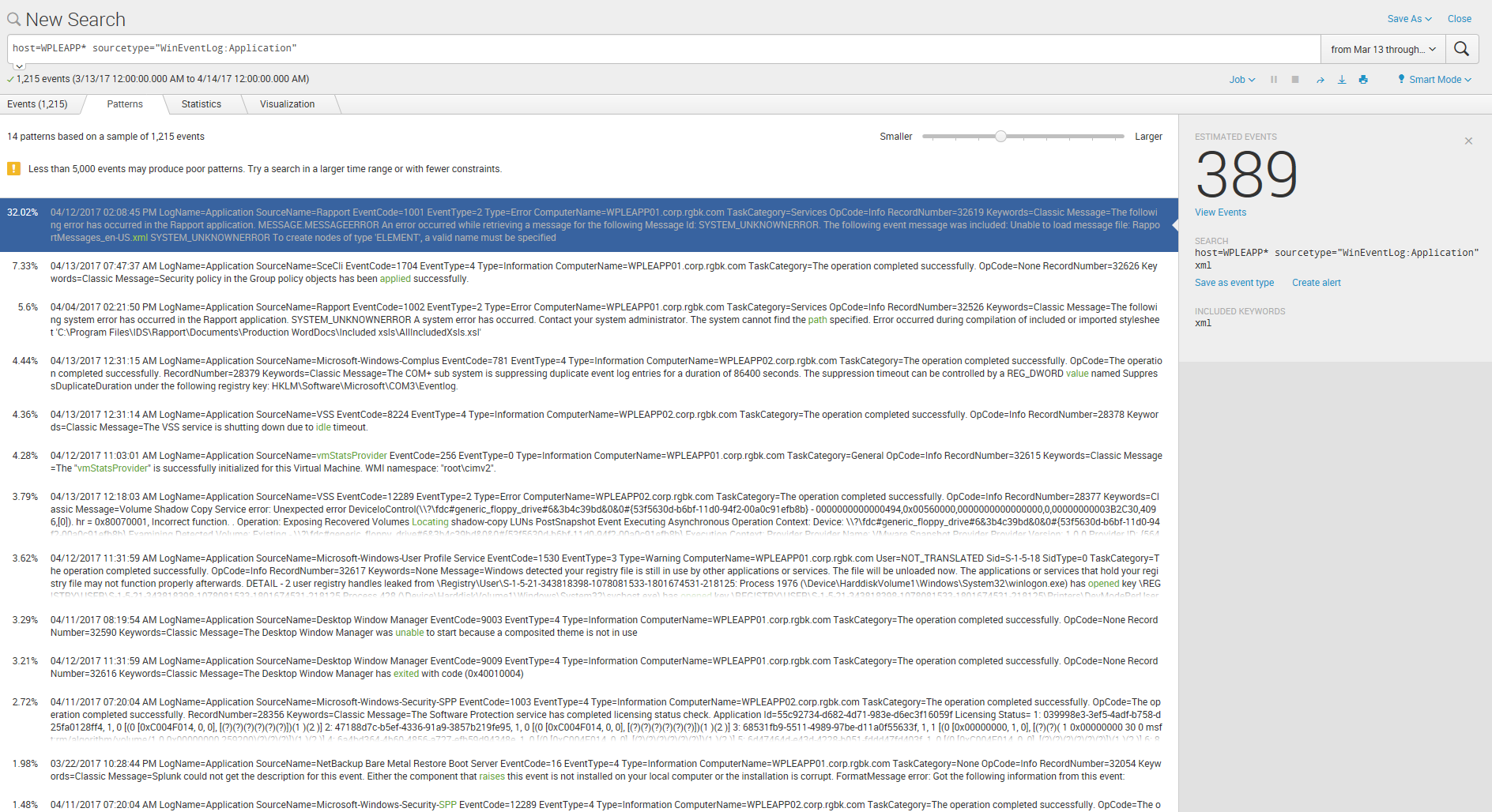
You can expand these rows out, and the fields are clickable. If the field is clickable, you can add or exclude then from the search by clicking on them.



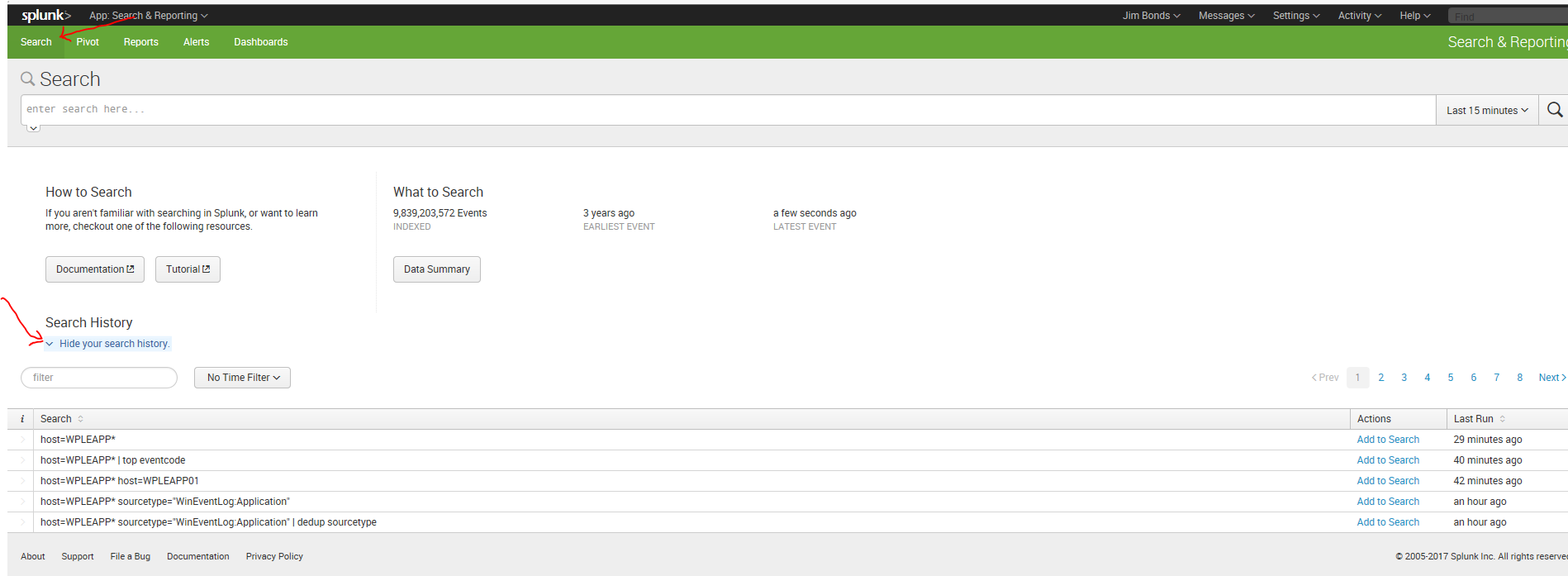
Another way to comb through events is with the field side bar. It gives you stats when you click on it. It gives us the top ten values. You can also click on the green time line bar and filter down to a date. If you filter down and want to remove the filter, you can back arrow on the browser, or change the query in the search bar. You can drill down into the search data without learning the search language.

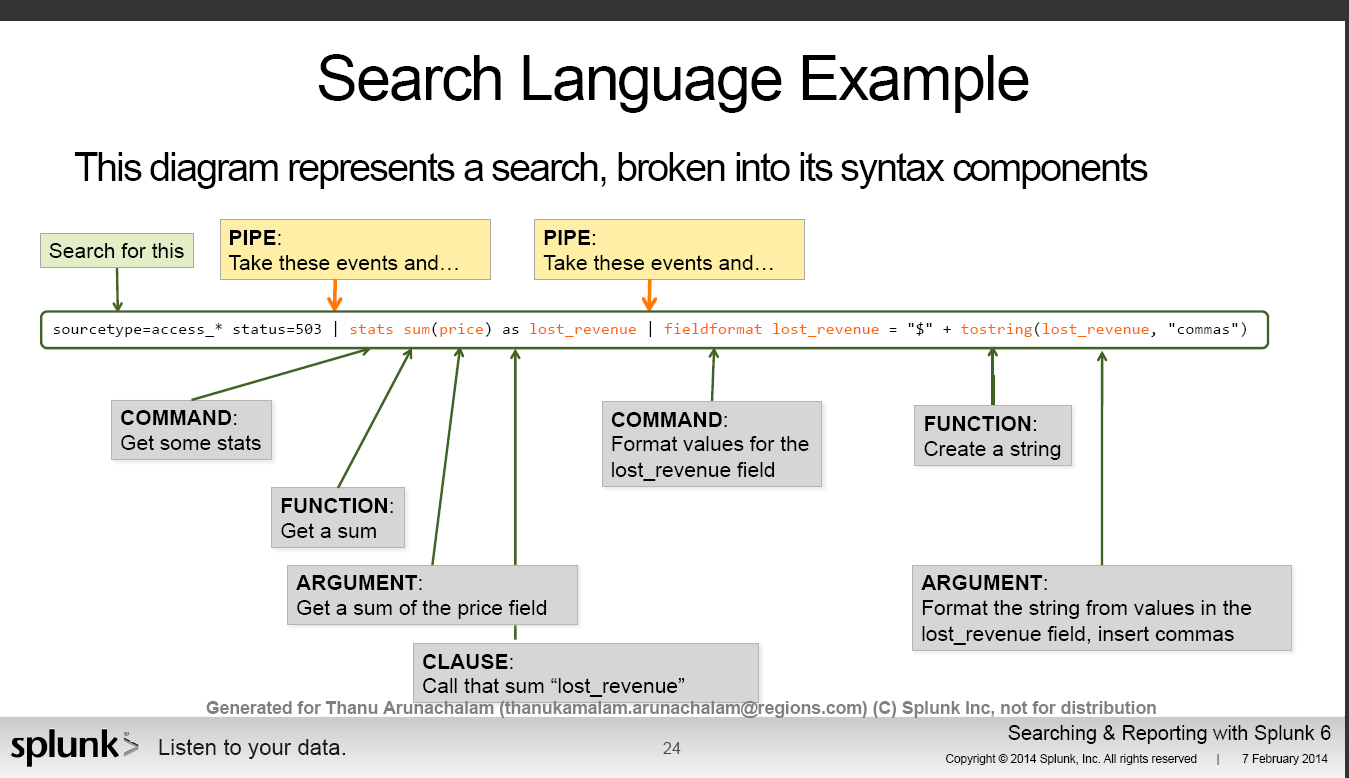


After you build and run your query you can go to the Patterns tab. The Patterns tab will show you patterns that are in your results. In the example below we see 14 patterns based on 1,215 events.



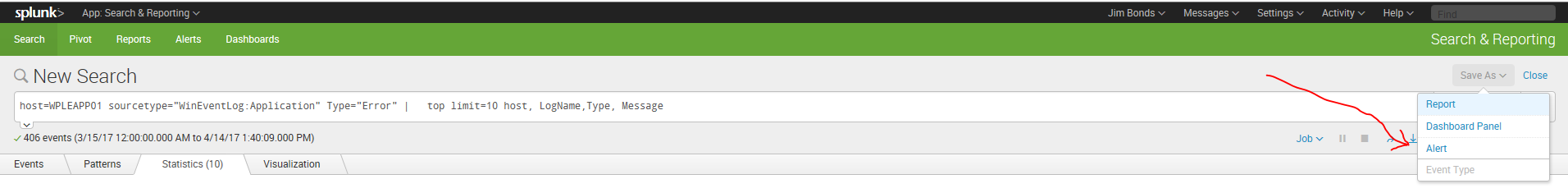
Another handy way to create a search is to click Search on the menu bar. On the initial search screen you can select the “Search History” link to see a list of your searches. Clicking on a search will recreate it.



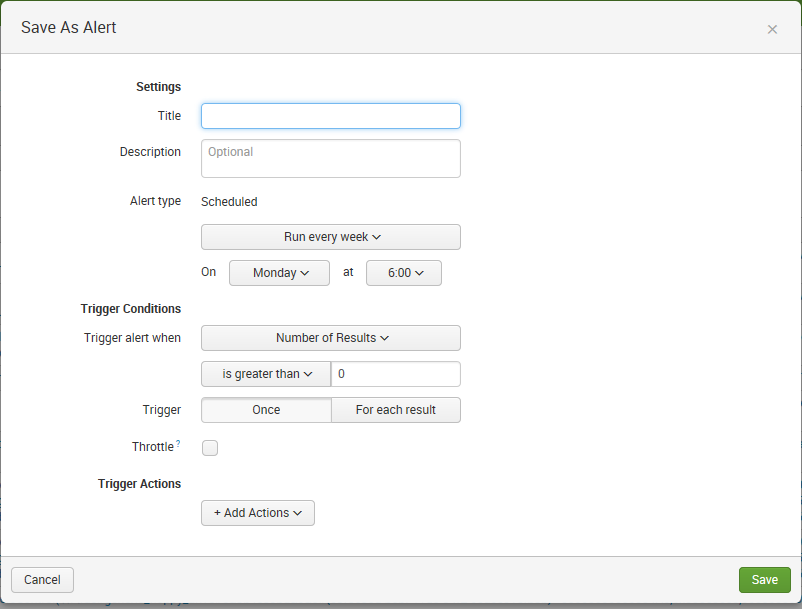


Alerts:

Search results trigger an alert action if they match the alert's conditions.



This form pops up. Create your alert here.



View and Edit your Alerts here.

