

SPLUNK ESSENTIALS

A SUMMARY BY DR. ALVIN ANG



Splunk Essentials

Leverage the power of Splunk to efficiently analyze machine, log, web, and social media data

Betsy Page Sigman

[PACKT] enterprise®

CONTENTS

Chapter 1: Introduction to Splunk.....	4
Part I: Theory	4
Functions of Splunk.....	4
Data Collection	4
Data Indexing.....	4
Data Searching.....	5
Data Analysis	5
Big Data	5
Three Vs:.....	5
Volume:.....	5
Variety:.....	5
Velocity:	6
Streaming Data	6
Latency of data	6
Sparseness of Data	6
Splunk Data Sources	7
Machine data.....	7
Web Logs	7
Data Files	8
Social Media Data.....	8
Splunk Events / Event Types / Source Types / Fields	8
Events	8
Event types	8
Source Types	9
Fields.....	9
Part II: Practice.....	11
Step 1: Install Splunk.....	11
Step 2: Download Tutorial Data.....	12
Step 3: Add Data Into Splunk	13
Step 4: Finding Your Way Back To The Search Box.....	21
Chapter 2: How to Delete Data from Splunk	24
Chapter 3: Search Processing Language (SPL)	28
Part I: Theory	28
Part II: Practical	29
Practice 1: Buttercupgames	29
Lesson Learnt: Search box is not Case Sensitive (caps lock).....	29
Practice 2: Buttercupgames date_wday="Wednesday"	30
Practice 3: Wild Card fail*	31
Lesson Learnt: Wild Card is represented by *	33
Practice 4: AND / OR.....	34

Lesson Learnt → There is an Implied “AND” between words in the search box	36
Practice 5: Creating a Count of Product IDs	37
Practice 6: Trying out the Eval and Stats function together	39
Practice 7: Trying out the Timechart command	42
Practice 8: Trying out the Visualization	43
Practice 9: Trying out the TOP Command	45
Practice 10: Another way of using the TOP Command	47
Practice 11: Day of the Week	49
Practice 12: Tagging.....	51
Practice 13: Saving Event Types	54
Practice 14: Deleting Event Types	57
Practice 15: Creating Reports	58
Practice 16: Creating Dashboards	62
Practice 17: Creating a Bar Chart.....	66
Practice 18: Creating a Stacked Bar Chart	71
Practice 19: How to Format the Legend	74
Practice 20: Creating a Sparkline Panel	75
Practice 21: Creating a Line Plot.....	76
Practice 22: Creating a Radial Gauge.....	78
Practice 23: Creating a Marker Gauge.....	79
Practice 24: Creating a Pivot Table.....	81
Appendix	87
Types of SPL Command.....	87
1. Filter	87
1a. search function.....	87
1b. where function	87
1c. dedup function	88
1d. head/tail function	88
2. Sort.....	89
2a. sort 0 anyfield.....	89
2b.sort 1000 fieldone -fieldtwo	89
2x.sort -fieldone, +fieldtwo.....	89
3. Group	90
4. Report	91
4a. top/rare function.....	91
4b. stats function	91
4c. chart function	92
4d. timechart function	92
5. Other	93
5a. field	93
5b. replace	93
5c. eval	93
5d. lookup	94
About the Author	95

PART I: THEORY

FUNCTIONS OF SPLUNK

Data Collection

- Splunk frequently collects Machine Data.
- Machine Data is streaming data and Splunk can handle it.
- Splunk can also collect data from many other sources.

Data Indexing

- Before data can be searched, it needs to be indexed.
- Creating an index requires two steps: **Parsing and Indexing**.
 - **Parsing = Separating** the data into events or breaking up chunks of data,
 - It adds Metadata (= data about data), such as:
 - Host = what device did the data come from,
 - Source = where did the event originate from
 - Source-type = the format of the data,
 - Timestamps
 - **Indexing** = breaks events into segments for easier searching.
 - Creates a structure for the index
 - Then writes the raw data and index files to disk.
 - With **indexing**, it's easier to search in Splunk for massive data.

Data Searching

- Since Splunk indexes data before it is searched, the search process goes very quickly.

Data Analysis

- Splunk has a variety of default data visualizations for reports and dashboards,

BIG DATA

Three Vs:

Volume:

- Small Volume
 - Millions of Data = Megabytes
 - Billions of Data = Gigabytes,
- Big Data
 - Terabytes of Data
 - Petabytes
 - Exabytes

Variety:

- Big data includes all kinds of data = Structured / Semi-Structured / Unstructured
- All data can be searched and processed quickly using the methods of Big Data.

Velocity:

- Speed at which data enters the system.
- Example every day one Petabyte of Data enters the system = requires quick processing.

Streaming Data

- Much of Big Data does not need to be kept.
- For example: Mechanical plant.
 - Many sensors that collect data on all parts of the assembly line.
 - Much of it does not need to be kept for long period of time.
 - Only use of it is to alert a possible problem through noticing a bad trend

Latency of data

- Latency = how quick the data enters the system for analysis.
- If detect anomalies, Splunk can immediately shut down the system (presuming no latency in the data).

Sparseness of Data

- Very Sparse = Finding a needle in a haystack.
- Rare = A handful of cases
- Sparse = 0.01 to 1%
- Dense = 10%
- Example: Retail Data is sparse.

- A store has many products but people buy very few items.
- The store's database will show that most of the fields would be empty.
- We would say then that the data is sparse.

SPLUNK DATA SOURCES

Machine data

- Much of Splunk's data is machine data.
- Machine Data = data created each time a machine does something.
 - From servers to
 - Operating Systems to
 - Controllers for robotic assembly arms.
- All machine data includes timestamp.
- If no timestamp is included, Splunk will find a date based on the file's last modification time.
- As a last resort, it will stamp the event with the time it was indexed into Splunk.

Web Logs

- Web Logs = How their website is used.
- Example:
 - Which pages are visited most?
 - Which pages have problems?
 - People leaving quickly
 - Discarded shopping carts,

- Other aborted actions

Data Files

- Splunk can read in data from all types of files.

Social Media Data

- Any Facebook (or any other social media) interaction creates a significant amount of data, even those that don't include many data-intensive acts, such as posting a picture, audio file, or a video.

SPLUNK EVENTS / EVENT TYPES / SOURCE TYPES / FIELDS

Events

- Events = a record of activity in a log file.
- Each Event has:
 - A timestamp
 - Information about the system being tracked
- Without Events, there would be nothing to search, of course.

Event types

- Event Type = Categorizing similar events.
- It is field-defined by the user.
- Event Types allow us to make meaningful searches easily and quickly.

- One common reason for setting up an Event Type is to examine why a system has failed.
- Example: Failed Logins categorized as 1 Event Type → a search for failed logins can help pinpoint problems.

Source Types

- Source Type = determines what type of data it is so that Splunk can format it appropriately as it indexes it.
- Examples of Source Types:
 - Access_Combined, for NCSA combined format HTTP web server logs
 - Apache_Error, for standard Apache web server error logs
 - Cisco_Syslog, for the standard syslog produced by Cisco network devices (including PIX firewalls, routers, and ACS), usually via remote syslog to a central log host
 - Websphere_Core, a core file export from WebSphere

Fields

- Fields are for Indexing and Searching.
- Every Event will create a number of Fields, example:
 - Host
 - Source
 - Source type
 - Timestamp
- Fields are extracted from events at multiple points in the data processing pipeline that Splunk uses, and each of these fields includes a

- Name → example: userid
- Value → example: susansmith

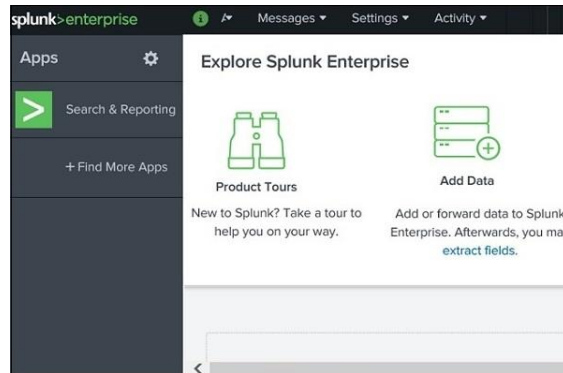
PART II: PRACTICE

STEP 1: INSTALL SPLUNK

- Go to <https://www.splunk.com/>
- Sign up and install the Free version of Splunk.



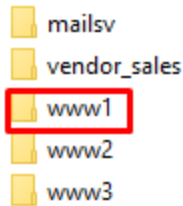
- Choose Local System.
- Key in your username / password... change them as you deem fit...



- After installation and running the software, it will open up in a browser and you will see the above picture.

STEP 2: DOWNLOAD TUTORIAL DATA

- Go to <https://www.alvinang.sg/publications-1>
- Scroll down all the way and find “Splunk Tutorial Files.zip”
- Download it.



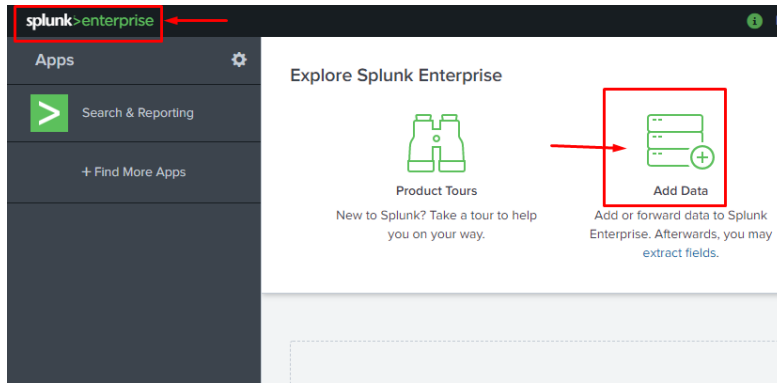
- Unzip the folder, open it and open “www1” on notepad.



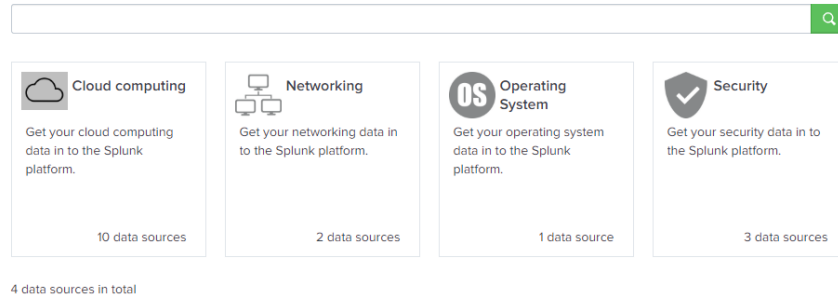
```
access - Notepad
File Edit Format View Help
209.160.24.63 - - [23/May/2020:18:22:16] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1748 "h
209.160.24.63 - - [23/May/2020:18:22:16] "GET /oldlink?itemId=EST-6&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1352 "h
209.160.24.63 - - [23/May/2020:18:22:17] "GET /product.screen?productId=BS-AG-G09&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1352 "h
209.160.24.63 - - [23/May/2020:18:22:19] "POST /category.screen?categoryId=STRATEGY&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1352 "h
209.160.24.63 - - [23/May/2020:18:22:20] "GET /product.screen?productId=FS-SG-G03&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1352 "h
209.160.24.63 - - [23/May/2020:18:22:20] "POST /cart.do?action=addtocart&itemId=EST-21&productId=FS-SG-G03&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3280 "http:
209.160.24.63 - - [23/May/2020:18:22:21] "POST /cart.do?action=purchase&itemId=EST-21&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3280 "http:
209.160.24.63 - - [23/May/2020:18:22:22] "POST /cart/success.do?JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3280 "http:
209.160.24.63 - - [23/May/2020:18:22:21] "GET /cart.do?action=remove&itemId=EST-11&productId=WC-SH-A01&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1352 "
209.160.24.63 - - [23/May/2020:18:22:22] "GET /oldlink?itemId=EST-14&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1352 "
112.111.162.4 - - [23/May/2020:18:26:36] "GET /product.screen?productId=WC-SH-G04&JSESSIONID=SD7SL8FF5ADFF4964 HTTP 1.1" 200 1352 "h
112.111.162.4 - - [23/May/2020:18:26:37] "POST /cart.do?action=addtocart&itemId=EST-18&productId=WC-SH-G04&JSESSIONID=SD7SL8FF5ADFF4964 HTTP 1.1" 200 1352 "h
112.111.162.4 - - [23/May/2020:18:26:38] "POST /cart.do?action=purchase&itemId=EST-18&JSESSIONID=SD7SL8FF5ADFF4964 HTTP 1.1" 200 1352 "h
112.111.162.4 - - [23/May/2020:18:26:38] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD7SL8FF5ADFF4964 HTTP 1.1" 200 1352 "h
112.111.162.4 - - [23/May/2020:18:26:37] "GET /category.screen?categoryId=NULL&JSESSIONID=SD7SL8FF5ADFF4964 HTTP 1.1" 200 1352 "h
112.111.162.4 - - [23/May/2020:18:26:38] "GET /oldlink?itemId=EST-7&JSESSIONID=SD7SL8FF5ADFF4964 HTTP 1.1" 503 1207 "h
74.125.19.106 - - [23/May/2020:18:32:15] "GET /cart.do?action=addtocart&itemId=EST-16&productId=DC-SG-G02&JSESSIONID=SD4SL7FF10ADFF4998 HTTP 1.1" 200 1352 "h
74.125.19.106 - - [23/May/2020:18:32:15] "GET /category.screen?categoryId=NULL&JSESSIONID=SD4SL7FF10ADFF4998 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:02] "POST /cart.do?action=changequantity&itemId=EST-21&productId=WC-SH-A01&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:03] "POST /cart.do?action=addtocart&itemId=EST-27&productId=DC-SG-G02&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:03] "GET /category.screen?categoryId=STRATEGY&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:03] "GET /cart.do?action=view&itemId=EST-19&productId=DB-SG-G01&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:05] "POST /product.screen?productId=DB-SG-G01&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:06] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:07] "GET /oldlink?itemId=EST-17&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 924 "
117.21.246.164 - - [23/May/2020:18:36:07] "GET /product.screen?productId=FI-AG-G08&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:07] "GET /category.screen?categoryId=NULL&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:08] "GET /product.screen?productId=WC-SH-G04&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
117.21.246.164 - - [23/May/2020:18:36:08] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD9SL6FF8ADFF5015 HTTP 1.1" 200 1352 "h
91.205.189.27 - - [23/May/2020:18:46:23] "GET /product.screen?productId=CU-PG-G06&JSESSIONID=SD8SL8FF3ADFF5080 HTTP 1.1" 200 1352 "h
91.205.189.27 - - [23/May/2020:18:46:24] "POST /cart.do?action=addtocart&itemId=EST-12&productId=CU-PG-G06&JSESSIONID=SD8SL8FF3ADFF5080 HTTP 1.1" 200 1352 "h
91.205.189.27 - - [23/May/2020:18:46:25] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD8SL8FF3ADFF5080 HTTP 1.1" 200 1352 "h
```

- You will see that the above .txt file is a log file containing the digital trail of a customer on the website www.buttercupgames.com .

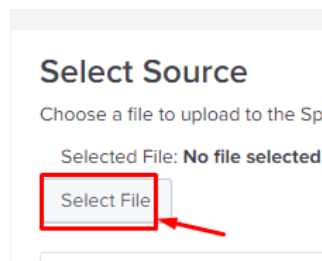
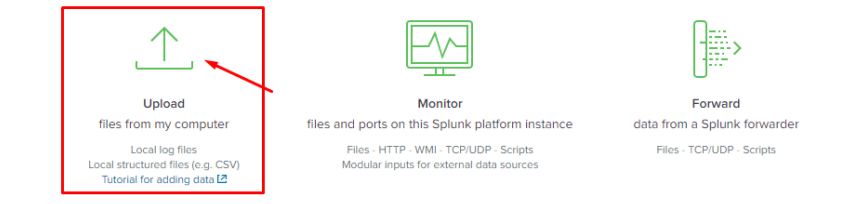
STEP 3: ADD DATA INTO SPLUNK





Follow guides for onboarding popular data sources



or get data in with the following methods



is PC > Desktop > Alvin's Works > Splunk Essentials > tutorialdata > www1

Name	Date modified	Type
 access	31-May-20 3:15 PM	Text Document
 secure	31-May-20 3:15 PM	Text Document

- Navigate to tutorialdata → www1 → access → upload it.

Add Data

Select Source
 Set Source Type
 Input Settings
 Review
 Done

[< Back](#) **Next >**

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **access.log**

Drop your data file here

The maximum file upload size is 500 Mb

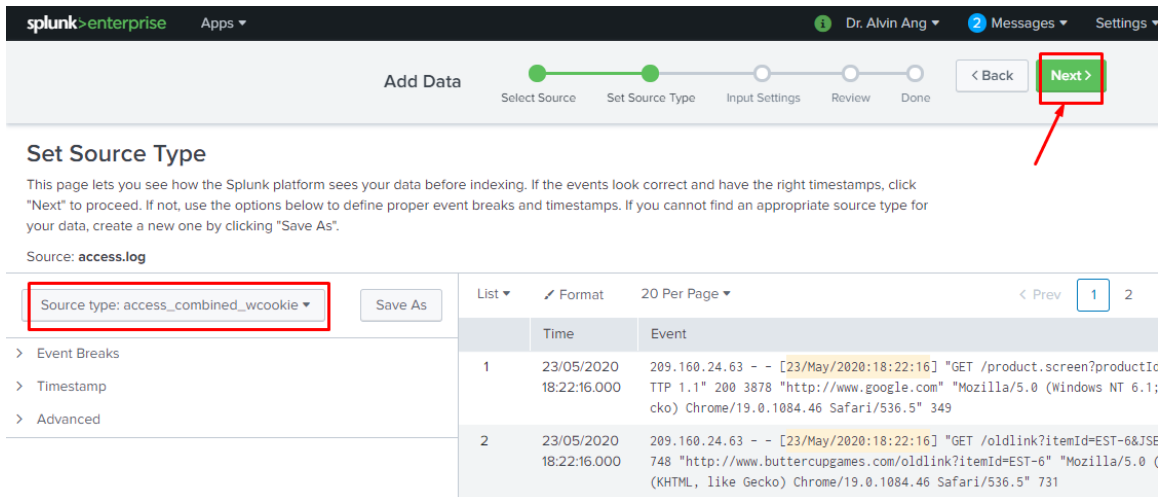


Figure 1: Automatic Source Type

- Figure 1 shows that the “Source Type” has been automatically selected for you.

Sourcetype	Used for
access_combined	A standardized format for text files used by HTTP web servers when generating server log files
cisco_syslog	Cisco standard system logs
apache_error	Errors

- The “access_combined_wcookie” indicates that each cookie set during an HTTP request is logged.
- By typing the following into the search bar (later on): **sourcetype=access_combined_wcookie** → This will pull up the web server logs with this sourcetype so you can then use them for analysis.

Add Data

Select Source Set Source Type **Input Settings** Review Done

< Back **Review >**

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Default Create a new index

Default
 history
 main
 summary

FAQ

- > How do indexes work?
- > How do I know when to create or use multiple indexes?

- Choose your Host Name and Index
 - Host Name = the name where you “host” your data. In this case, I host it on my laptop (choicetexts-PC)
 - Index = When the Splunk platform indexes raw event data, it transforms the data into searchable events and stores those events in the index.
 - When you add data to the Splunk platform, consider creating indexes for retention, or logical groupings.

Add Data

Select Source Set Source Type Input Settings Review Done

< Back **Submit >**

Review

Input Type	Uploaded File
File Name	access.log
Source Type	access_combined_wcookie
Host	choicetexts-PC
Index	Default

Add Data

Select Source Set Source Type Input Settings Review Done

< Back **Next >**

✓ **File has been uploaded successfully.**
Configure your inputs by going to [Settings > Data Inputs](#)

Start Searching	Search your data now or see examples and tutorials. ↗
Extract Fields	Create search-time field extractions. Learn more about fields. ↗
Add More Data	Add more data inputs now or see examples and tutorials. ↗
Download Apps	Apps help you do more with your data. Learn more. ↗
Build Dashboards	Visualize your searches. Learn more. ↗

The screenshot shows the Splunk Enterprise Search & Reporting interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'App: Search & Reporting'. Below that, a search bar contains the query: `source="access.log" host="choicetexts-PC" sourcetype="access_combined_wcookie"`. A red box highlights the search bar, and a red arrow points to it. Below the search bar, there's a bar chart visualization and a table of search results. The table has columns for Time and Event. The first row shows a GET request to /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 from Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5. The second row shows a POST request to /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 from http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5. The third row shows a GET request to /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 3920 from http://www.buttercupgames.com/oldlink?itemId=EST-17" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5. The fourth row shows a POST request to /cart/success.do?JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 356 from http://www.buttercupgame.com/cart.do?action=addtocart&itemId=EST-15" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5.

- After you click on “Start Searching”, you will come to this page above.
- Notice that in the search box:
 - `source="access.log"`
 - `host="choicetexts-PC"`
 - `sourcetype="access_combined_wcookie"`
- Has been typed out for you.
- Which also means that all events with
 - `source="access.log"`
 - `host="choicetexts-PC"`
 - `sourcetype="access_combined_wcookie"`
- will be searched out for you.

i	Time	Event
>	30/05/2020 18:20:56.000	182.236.164.11 - - [30/May/2020:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-TTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = choicetexts-PC ; source = access.log ; sourcetype = access_combined_wcookie
>	30/05/2020 18:20:55.000	182.236.164.11 - - [30/May/2020:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SDupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:41.0) Gecko/20100101 Firefox/41.0" 134 host = choicetexts-PC ; source = access.log ; sourcetype = access_combined_wcookie
>	30/05/2020 18:20:54.000	182.236.164.11 - - [30/May/2020:18:20:54] "GET /category.screen?categoryId=ACCESSORIES" "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:41.0) Gecko/20100101 Firefox/41.0" 648 host = choicetexts-PC ; source = access.log ; sourcetype = access_combined_wcookie
>	30/05/2020 18:20:54.000	182.236.164.11 - - [30/May/2020:18:20:54] "POST /cart/success.do?JSESSIONID=SD6SL8FFs.com/cart.do?action=purchase&itemId=EST-6" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:41.0) Gecko/20100101 Firefox/41.0" 220 host = choicetexts-PC ; source = access.log ; sourcetype = access_combined_wcookie

- Thus, note that:
 - Host here refers to the location which hosts the data → choicetexts-PC
 - Source refers to the file (access.log) notepad which stores the log information
 - Sourcetype is coined as “access_combined_wcookie” because it is the “type” of file for web logs.

Data Summary

Hosts (1) Sources (1) Sourcetypes (1)

filter

Host		Count	Last Update
choicetexts-PC	13,628	05/06/2020 15:08:24.000	

Data Summary

Hosts (1) Sources (1) Sourcetypes (1)

filter

Source		Count	Last Update
access.log	13,628	05/06/2020 15:08:24.000	

Data Summary

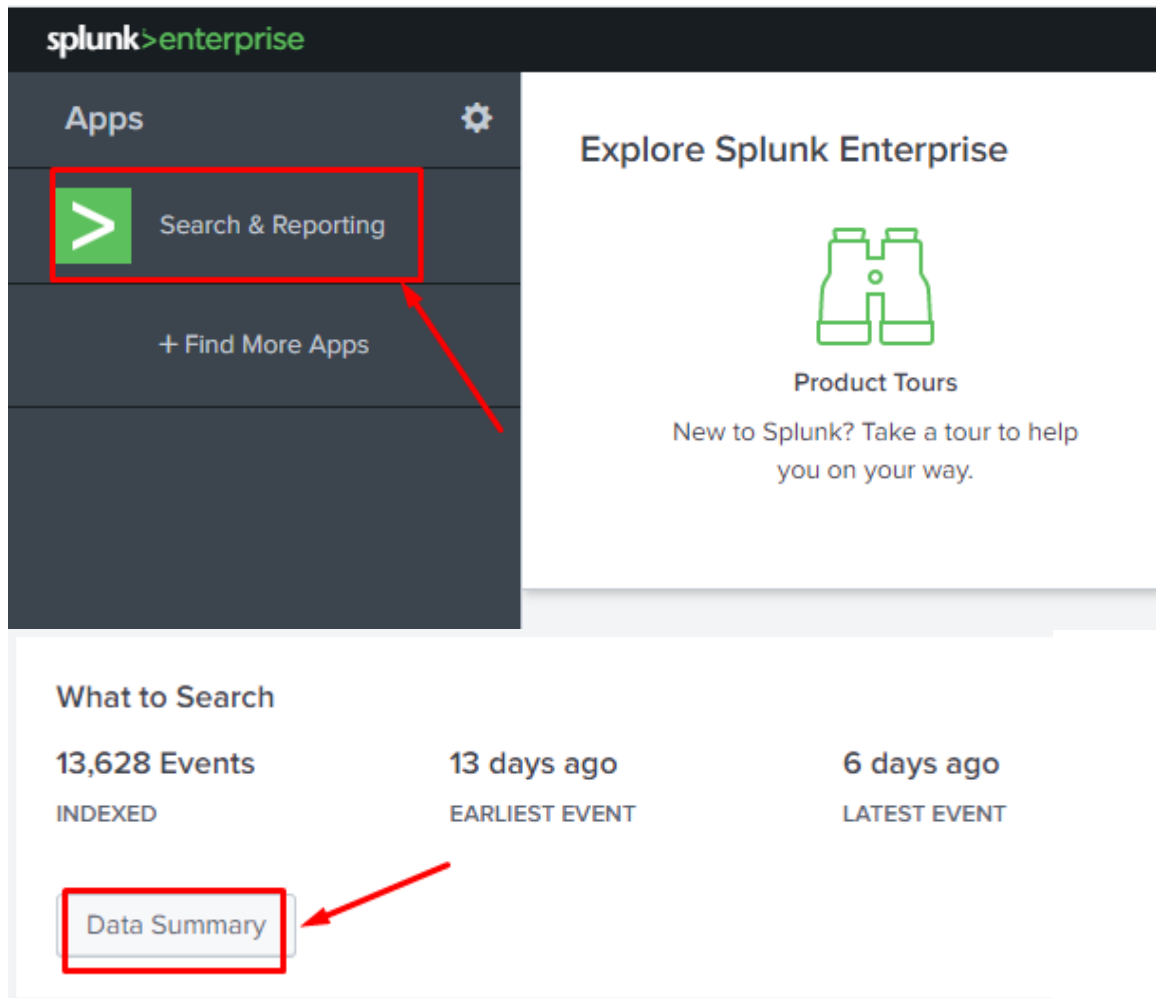
Hosts (1) Sources (1) Sourcetypes (1)

filter

Sourcetype		Count	Last Update
access_combined_wcookie	13,628	05/06/2020 15:08:24.000	

STEP 4: FINDING YOUR WAY BACK TO THE SEARCH BOX

- Presume you accidentally lost your way
- But you want to head back to the original search page which shows all results



Data Summary

Hosts (1) Sources (1) Sourcetypes (1)

filter

Host		Count	Last Update
choicetexts-PC		13,628	05/06/2020 15:08:24.000

splunk > enterprise App: S... dralvin... Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

host="choicetexts-PC"

Last 24 hours



0 events (04/06/2020 17:00:00.000 to 05/06/2020 17:00:00.000)

Events (0) Patterns Statistics

Presets

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

splunk>enterprise App: S... dralvin... 2 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Close

host="choicetexts-PC" New Search All time

✓ 13,628 events (before 05/06/2020 17:04:41.000) No Event Sampling Job

Events (13,628) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

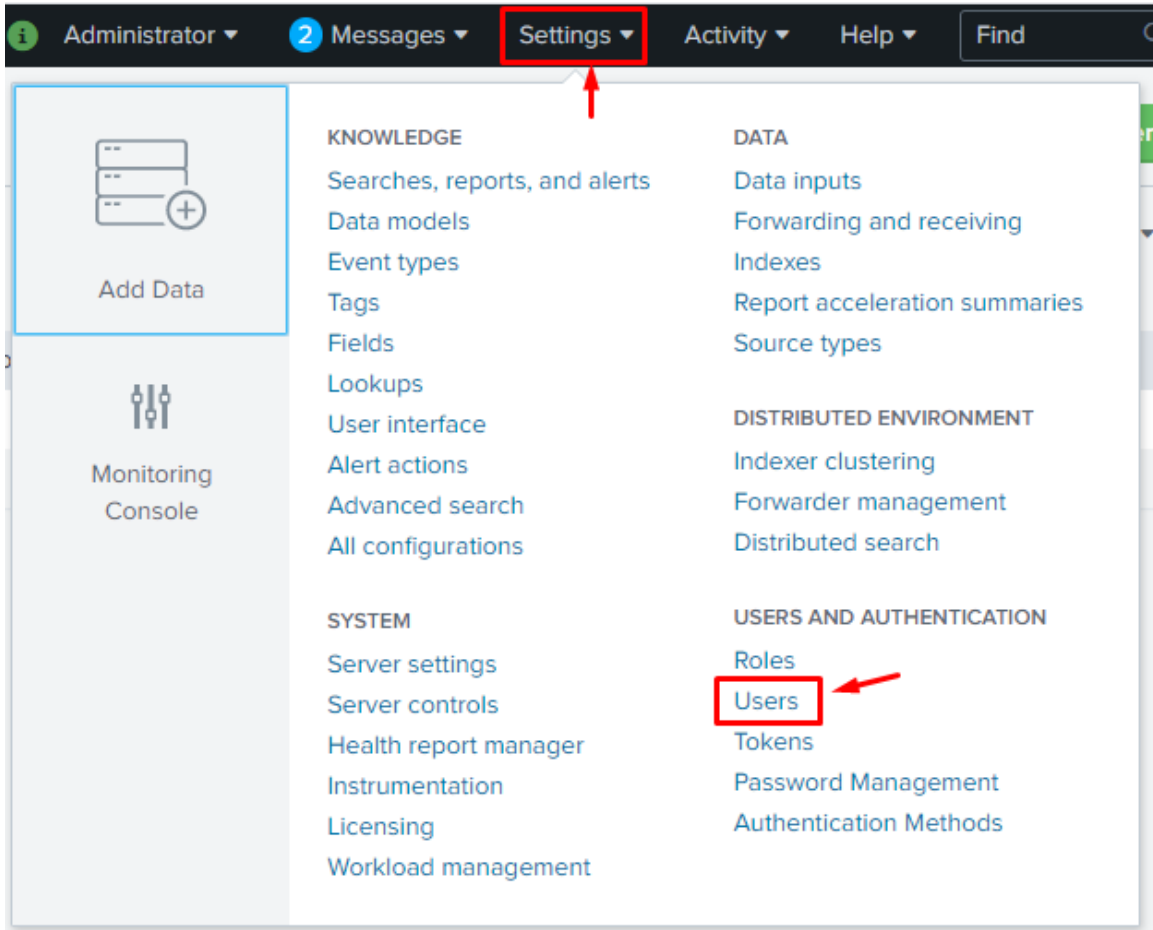
< Prev 1 2 3 4 5 6 7 8 ... Next >

i	Time	Event
>	30/05/2020 18:20:56.000	182.236.164.11 - - [30/May/2020:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = choicetexts-PC source = access.log sourcetype = access_combined_wcookie

SELETED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 5
butac 100%

- You will return to the original page with ALL data.



splunk>enterprise Apps ▾

Users

1 Users

Name ▲	Actions	Authentication system ⇅
dralvinang	View Capabilities Edit Clone	Splunk

Edit User: dralvinang ✕

Full name

Email address

Old password

Set password

Confirm password

Password must contain at least ?
8 characters

Time zone ?

Default app ?

Assign roles ?

Available item(s)	add all >	Selected item(s)	< remove all
admin		admin	
can_delete		can_delete	
power			
splunk-system-role			
user			

New Search

host="choicetexts-PC" | delete All time 

this will delete everything on the host type " | delete" after the "whatever you want to delete"

the moment you click this everything on the host gets deleted

✓ 13,628 events (before 05/06/2020 12:40:55.000) No Event Sampling Job [controls] Smart Mode

Events (13,628) Patterns Statistics Visualization



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

Hide Fields		All Fields	i	Time	Event
SELECTED FIELDS			>	30/05/2020 18:20:56.000	182.236.164.11 - - [30/May/2020:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = choicetexts-PC source = access.log sourcetype = test
INTERESTING FIELDS			>	30/05/2020 18:20:55.000	182.236.164.11 - - [30/May/2020:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = choicetexts-PC source = access.log sourcetype = test
			>	30/05/2020 18:20:54.000	182.236.164.11 - - [30/May/2020:18:20:54] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 3920 "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 648 host = choicetexts-PC source = access.log sourcetype = test

New Search Save As Close

host="choicetexts-PC" | delete All time

✓ 13,628 events (before 05/06/2020 12:46:16.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (2)** Visualization

20 Per Page

splunk_server	index	deleted	errors
choicetexts-PC	__ALL__	13628	0
choicetexts-PC	main	13628	0

All Splunk Files on the Host Computer Gets Deleted

PART I: THEORY

- In Chapter 1, we learnt how to Add Data into Splunk.
- In doing so, we have Indexed our Data.
- Now, we can begin to Search the Data.
- The default application for Splunk is the Search Application.
- Searches are made using the **Search Processing Language (SPL)**.

PART II: PRACTICAL

Practice 1: Buttercupgames

- Type 'buttercupgames' into the search box.
- All events with the word 'buttercupgames' will appear.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the text 'buttercupgames'. Below the search bar, a bar chart shows the distribution of events over time. The table below the chart displays search results for 'buttercupgames'. The first result is a GET request to a cart endpoint, and the second is a POST request to a product screen endpoint. Both results show the URL 'http://www.buttercupgames.com'.

i	Time	Event
>	30/05/2020 18:20:56.000	182.236.164.11 -- [30/May/2020:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&SESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = choicetexts-PC ; source = access.log ; sourcetype = access_combined_wcookie
>	30/05/2020 18:20:55.000	182.236.164.11 -- [30/May/2020:18:20:55] "POST /oldlink?itemId=EST-18&SESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgame.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = choicetexts-PC ; source = access.log ; sourcetype = access_combined_wcookie

Lesson Learn: Search box is not Case Sensitive (caps lock).

- In order to ensure Case Sensitivity....
 - CASE(Buttercup)
 - CASE(buttercup)
 - CASE (BUTTERCUP)

Practice 2: Buttercupgames date_wday="Wednesday"

The screenshot shows the Splunk Enterprise interface. At the top, the search bar contains the query `buttercupgames date_wday="wednesday"`. Below the search bar, it indicates that 1,799 events were found. The results are displayed in a table with columns for Time and Event. Two events are visible, both from 2020-05-27 at 23:52. The event at 23:52:17.000 shows a GET request to `http://www.buttercupgames.com/cart.do?action=add`. The event at 23:52:16.000 shows a GET request to `http://www.buttercupgames.com/cart.do?action=cha`. The word 'buttercupgames' is highlighted in red in both event descriptions. The interface also shows a timeline visualization and various search controls.

Time	Event
27/05/2020 23:52:17.000	221.207.229.6 - - [27/May/2020:23:52:17] "GET p://www.buttercupgames.com/cart.do?action=add eWebKit/536.5 (KHTML, like Gecko) Chrome/19.0 host = choicetexts-PC source = access.log sc
27/05/2020 23:52:16.000	221.207.229.6 - - [27/May/2020:23:52:16] "GET p://www.buttercupgames.com/cart.do?action=cha AppleWebKit/536.5 (KHTML, like Gecko) Chrome/ host = choicetexts-PC source = access.log sc

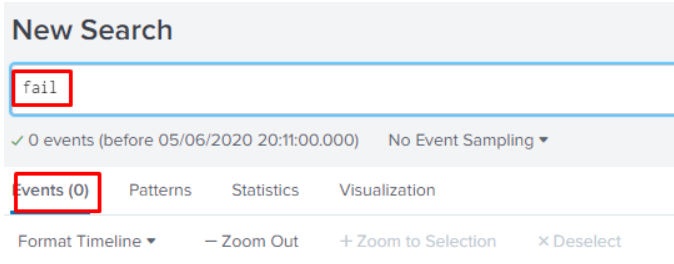
- Type 'buttercupgames date_wday="wednesday"' into the search box.
- All events with the word 'buttercupgames' AND appearing on Wednesdays will appear.

Practice 3: Wild Card fail*

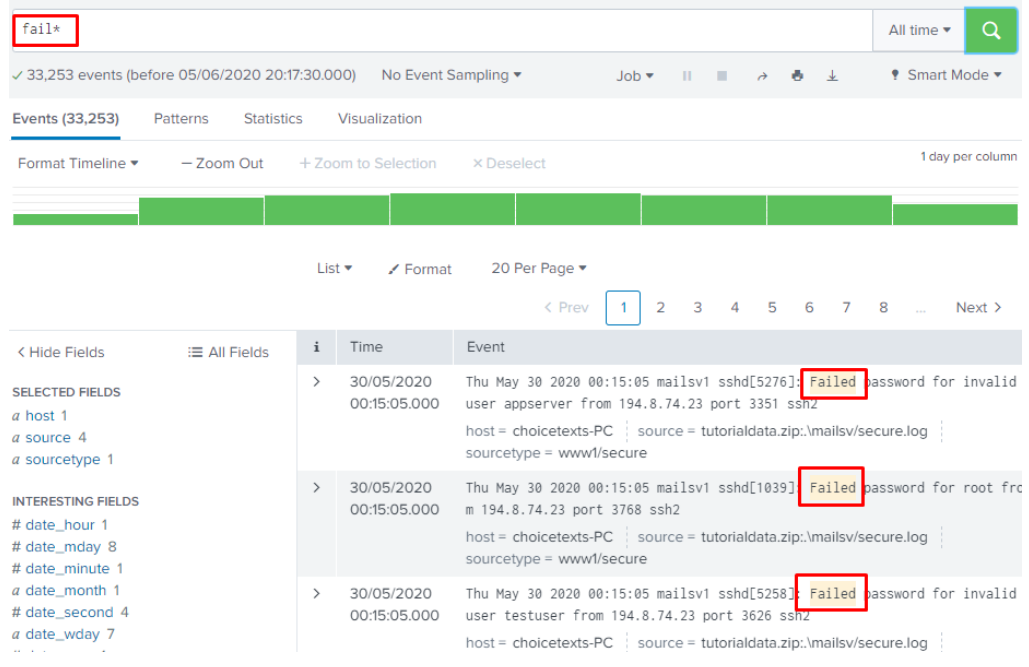
- From this Practice Onwards, we shall
 - Delete ALL data from Splunk (refer Chapter 2 on how to do this)
 - Add Data → the entire tutorial.zip into Splunk (refer Chapter 1 on how to do this)
- Presume that you have already Deleted ALL Data + Add the tutorial.zip entire folder into Splunk, you should now see this...there are 109,864 Events.

The screenshot shows the Splunk search interface. At the top, the search bar contains the query `host="choicetexts-PC"`. Below the search bar, it indicates that 109,864 events were found. The interface includes a timeline visualization and a table of search results. The table has columns for 'Time' and 'Event'. Three sample events are shown, all with a 'host' field value of 'choicetexts-PC'. The 'Event' field contains details such as timestamps, VendorID, Code, and AcctID. On the left side, there are sections for 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (AcctID, bytes, clientip, Code, date_hour, date_mday).

i	Time	Event
>	30/05/2020 18:24:02.000	[30/May/2020:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = choicetexts-PC source = tutorialdata.zip:\vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	30/05/2020 18:23:46.000	[30/May/2020:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = choicetexts-PC source = tutorialdata.zip:\vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	30/05/2020 18:23:31.000	[30/May/2020:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = choicetexts-PC source = tutorialdata.zip:\vendor_sales/vendor_sales.log



- If you were to type in just “fail” in the search box... you will realize that there are zero events.
- However, if you type in “fail*”, you get all events with the words “Failed” / “Failing” / “Fail”.
- In other words, the * behind the “fail” represents a *Wild Card* → Anything that comes after “fail” will be searched.



Lesson Learnt: Wild Card is represented by *

- Example: *log* will give all words that contain the 3 alphabets “log”
- Example ...logo...blog... will all be picked up by the search.

Practice 4: AND / OR

- We key in “fail* AND password” in the search box

The screenshot shows a search interface with the following elements:

- Search box: `fail* AND password` (highlighted with a red box and arrow)
- Time range: All time
- Event count: 33,253 events (before 05/06/2020 20:33:01.000)
- Visualization: Timeline view showing green bars representing events.
- Table view: A table with columns for Time and Event. The table is filtered to show 20 items per page. The 8th item is highlighted with a red box and arrow.

i	Time	Event
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[2900] Failed password for invalid user mysql from 175.44.1.122 port 4515 ssh2 host = choicetexts-PC source = tutorialdata.zip...mails/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1575] Failed password for mail from 175.44.1.122 port 1735 ssh2 host = choicetexts-PC source = tutorialdata.zip...mails/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1151] Failed password for root from 175.44.1.122 port 1202 ssh2 host = choicetexts-PC source = tutorialdata.zip...mails/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1845] Failed password for invalid user admin from 175.44.1.122 port 1718 ssh2 host = choicetexts-PC source = tutorialdata.zip...mails/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[4693] Failed password for invalid user irc from 175.44.1.122 port 4797 ssh2 host = choicetexts-PC source = tutorialdata.zip...mails/secure.log sourcetype = www1/secure

- Search results return Events that contain the words both “Failed” and “Password”.
- That means, should the Event only contain one word... either “Failed” or “Password”, it will not be shown.
- We take note of page 8 so that we can refer to it in the next few examples.

- We now key in “fail* password” in the search box

The screenshot shows the Splunk search interface. The search bar contains the query "fail* password". Below the search bar, there are 33,253 events. The results are displayed in a list view with 20 items per page. The first four results are highlighted in yellow, indicating they match the search criteria. The search results table is as follows:

i	Time	Event
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[2900]: Failed password for invalid user mysql from 175.44.1.122 port 4515 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1575]: Failed password for mail from 175.44.1.122 port 1735 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1151]: Failed password for root from 175.44.1.122 port 1202 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1845]: Failed password for invalid user admin from 175.44.1.122 port 1718 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure

- Notice that the results show that there is No difference between “fail* AND password” and “fail* password”?
- This means that Splunk understands the “space between words” are taken as “AND”.

Lesson Learnt → There is an Implied “AND” between words in the search box

- We now key in “fail* OR password” in the search box

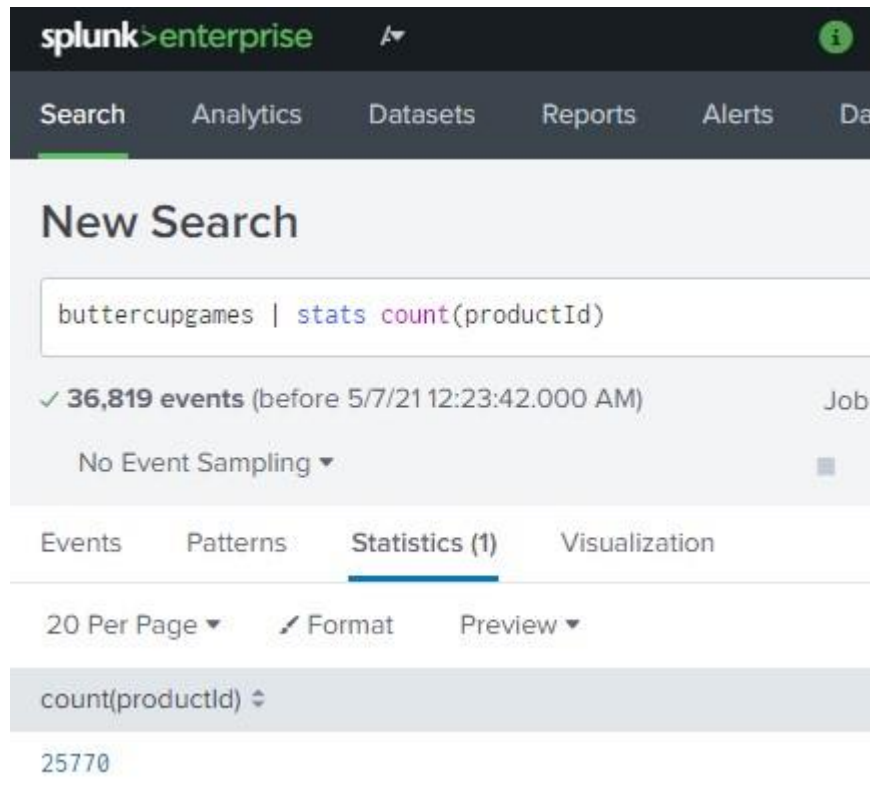
The screenshot shows a search interface with a search box containing the query "fail* OR password". Below the search box, there are navigation options like "All time" and a search icon. The interface displays 34,852 events. A timeline visualization is shown above a list of results. The list is on page 8, with page numbers 1 through 11 visible. The results table has columns for "i", "Time", and "Event".

i	Time	Event
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[1792]: Failed password for invalid user max from 223.205.219.67 port 4618 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[4157]: Failed password for invalid user irc from 223.205.219.67 port 3352 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure
>	30/05/2020 00:15:05.000	Thu May 30 2020 00:15:05 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = choicetexts-PC source = tutorialdata.zip:\mailsv/secure.log sourcetype = www1/secure

- Notice on Page 8, we now have Events that include either word “fail*” OR “password”.

Practice 5: Creating a Count of Product IDs

- Type `{ buttercupgames | stats count(productId)}` into the search box.



- We can see that the count of all the events with productId is shown.
- However, though useful, this is not what we are looking for here.

- Type {buttercupgames | stats count by productId} into the search box

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `buttercupgames | stats count by productId`. The search results show 36,819 events. The 'Statistics (16)' tab is selected, displaying a table with two columns: 'productId' and 'count'. The table lists 16 product IDs and their corresponding counts.

productId	count
BS-AG-G09	1227
CU-PG-G06	1271
DB-SG-G01	2129
DC-SG-G02	1855
FI-AG-G08	1397
FS-SG-G03	1681
MB-AG-G07	1725
MB-AG-T01	1844
PZ-SG-G05	1416

- We get the individual counts for each productId value, so we know precisely how many were sold during the time period.
- Refer to Appendix: 4b. stats function for more stats functions.

Practice 6: Trying out the Eval and Stats function together

- Refer to Appendix: 5c. eval to take a look at some Eval functions available, such as:

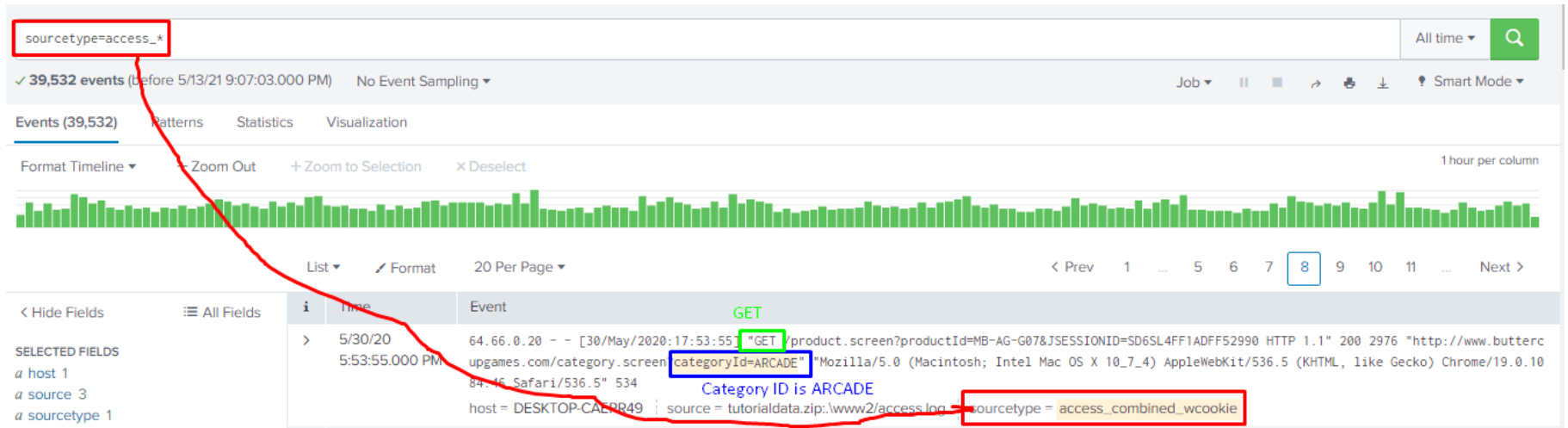
Eval function	Description	Example
case (X, "Y", . . .)	Using pairs of arguments, X and Y, where X is TRUE, return Y.	case(error == 404, "Not found", error == 200, "OK")
ceil (X)	Gives the ceiling of a number.	ceil(2.2)
if (X, Y, Z)	If X is TRUE, result is Y. If X is FALSE, result is Z.	if(error ==404, "Not found", "Found")
len (X)	Returns number of characters in the string field.	length(field)
lower (X), upper (X)	Returns lowercase, uppercase.	lower(username), upper(username)
round (X, Y)	Rounds X to Y decimal places. If no Y is given, round to integer.	round (3.5)

- Type into the search box
 - sourcetype=access_* | stats count(eval(method="GET")) as GET, count(eval(method="POST")) as POST by categoryId

The screenshot shows the Splunk Search & Reporting interface. At the top, there are navigation tabs: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A green arrow icon and the text 'Search & Reporting' are on the right. Below this is a 'New Search' header with 'Save As', 'Create Table View', and 'Close' options. The search query is entered in a text box: `sourcetype=access_* | stats count(eval(method="GET")) as GET, count(eval(method="POST")) as POST by categoryId`. To the right of the query is a search icon and 'All time'. Below the query bar, it shows '39,532 events (before 5/13/21 8:48:02.000 PM)' and 'No Event Sampling'. There are also icons for job management and 'Smart Mode'. Below the search bar, there are tabs for 'Events', 'Patterns', 'Statistics (8)', and 'Visualization'. Under 'Statistics (8)', there are options for '20 Per Page', 'Format', and 'Preview'. The main content is a table with the following data:

categoryId	GET	POST
ACCESSORIES	1425	718
ARCADE	1776	969
NULL	1660	381
SHOOTER	894	491
SIMULATION	935	510
SPORTS	512	281
STRATEGY	2971	1632
TEE	1288	725

- First, “sourcetype=access_*” brings up ALL sourcetypes with “access_***”



- Then, we extract all “GET” and “POST” PER Category ID (in the picture above, the categoryid=ARCADE).

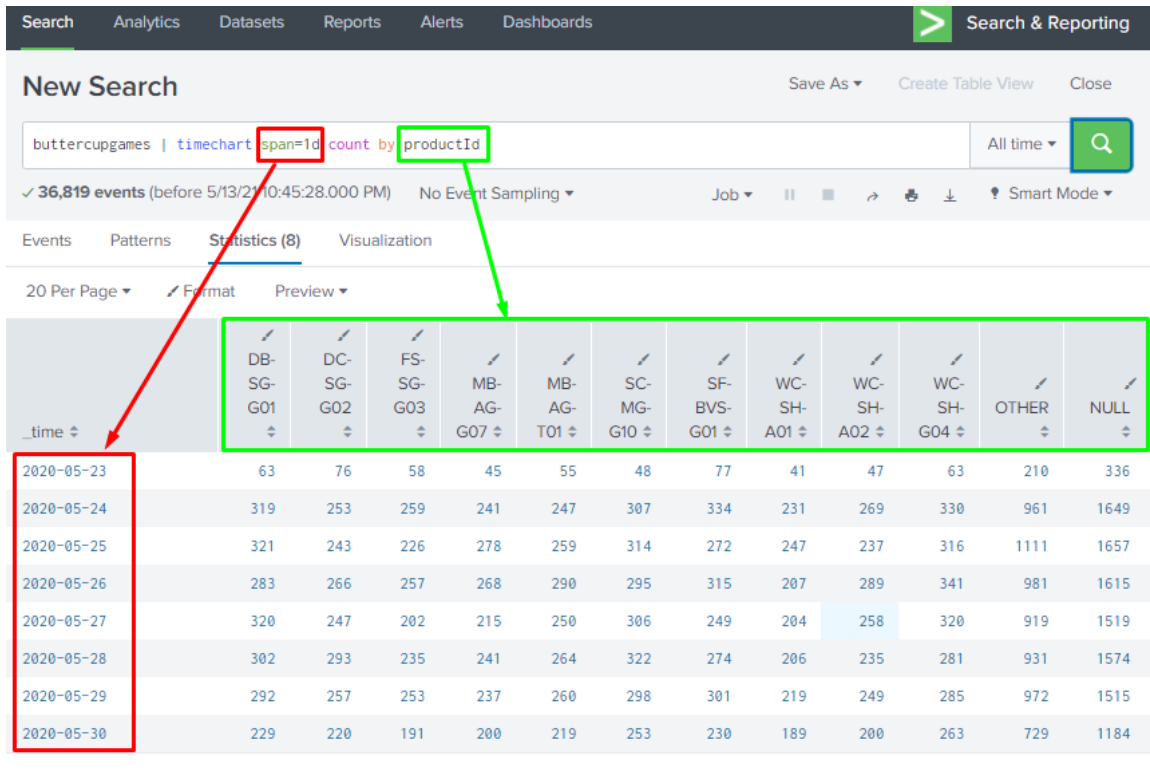
- Then, we COUNT them and place them under category id.

The screenshot shows a search interface with a query: `sourcetype=access_* | stats count(eval(method="GET")) as GET, count(eval(method="POST")) as POST by categoryId`. The query is executed for 39,532 events. The results are displayed in a table with columns for 'categoryId', 'GET', and 'POST'.

categoryId	GET	POST
ACCESSORIES	1425	718
ARCADE	1776	969
NULL	1660	381
SHOOTER	894	491
SIMULATION	935	510
SPORTS	512	281
STRATEGY	2971	1632
TEE	1288	725

Practice 7: Trying out the Timechart command

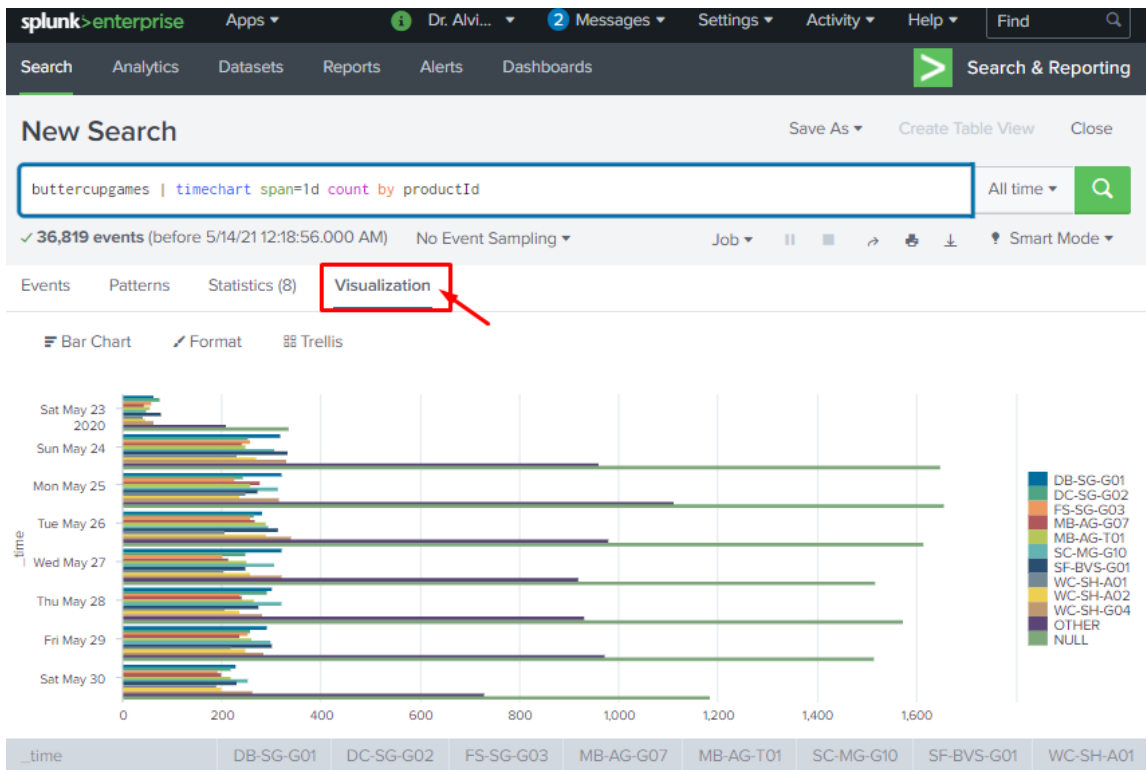
- Type into the search box:
 - buttercupgames | timechart span=1d count by productId



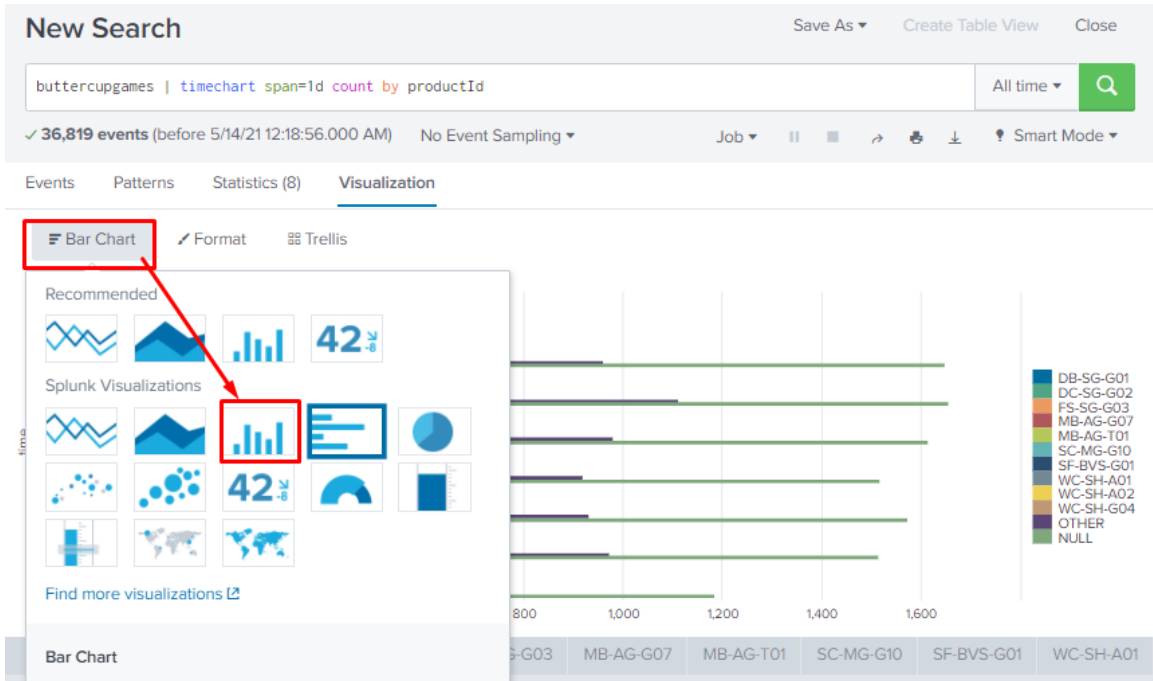
- We are trying to find out:
 - Which product IDs were sold?
 - When were they sold?
- `span=1d` is daily attribute.

Practice 8: Trying out the Visualization

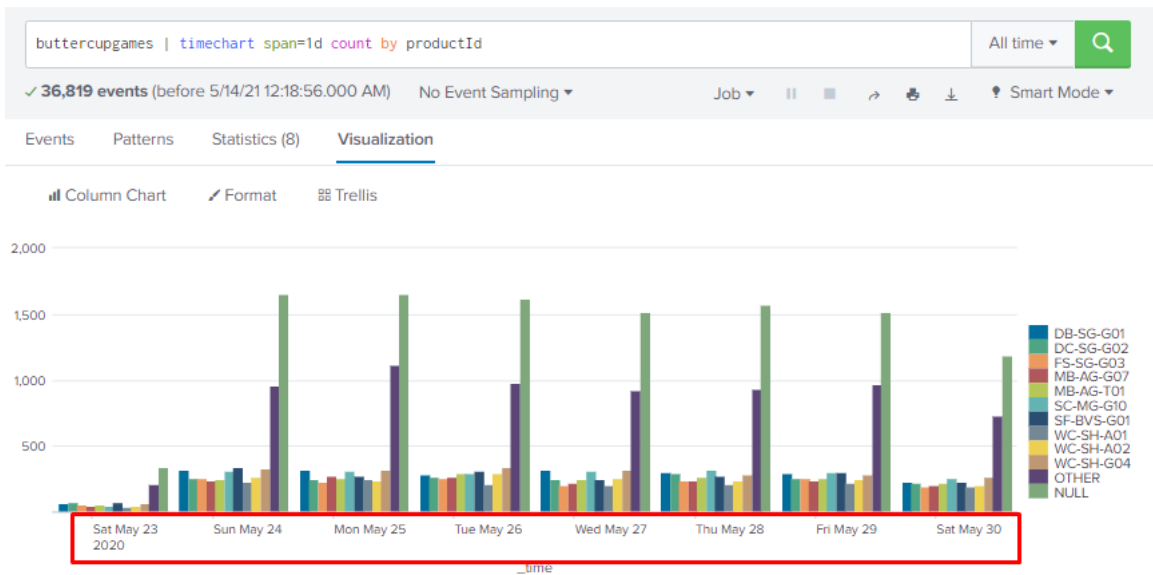
- After we have typed into the search box (following the previous Practice 7):
 - buttercupgames | timechart span=1d count by productId



- Click on the Visualization tab... you will see the following picture above...
- However, we can improve this by



- We will end up with a nicer daily column chart.



Practice 9: Trying out the TOP Command

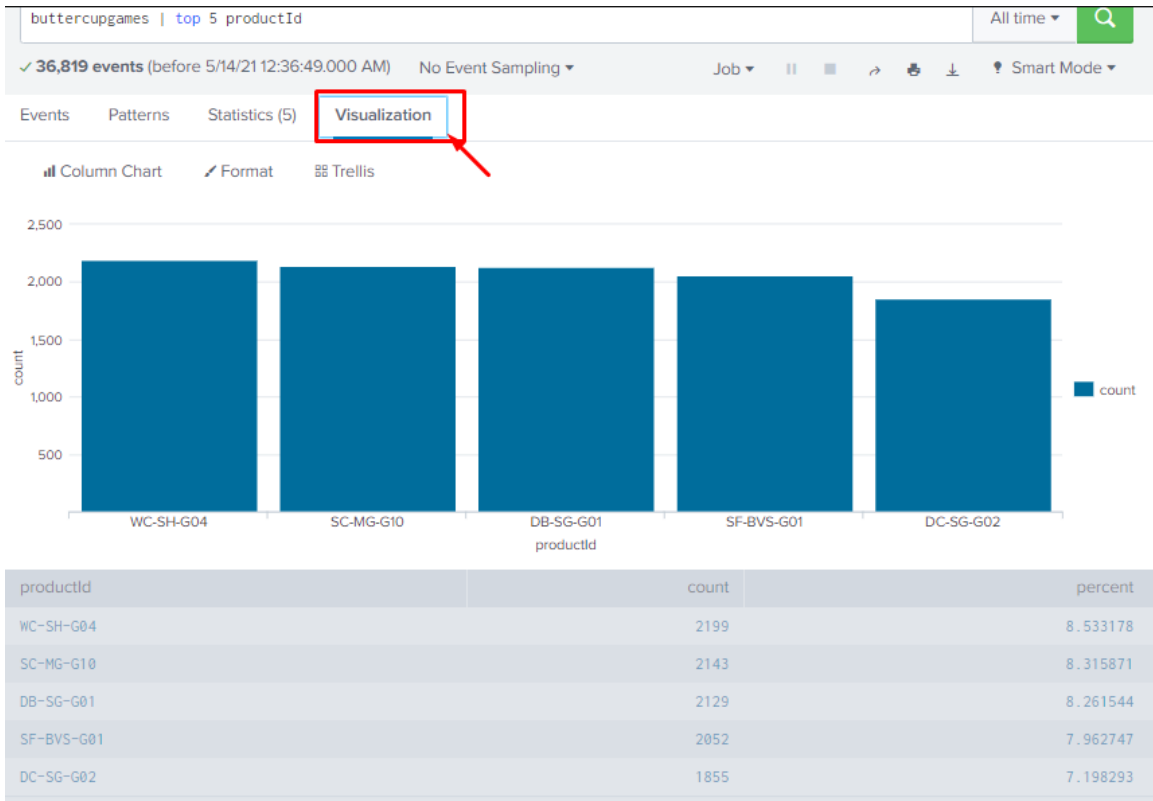
- Type in the following command:
 - buttercupgames | top 5 productId

The screenshot shows a search interface with a navigation bar at the top containing 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A 'Search & Reporting' button is on the right. Below the navigation bar is a 'New Search' section with a search input field containing 'buttercupgames | top 5 productId'. The search results show 36,819 events. The 'Statistics (5)' tab is selected, displaying a table with the following data:

productId	count	percent
WC-SH-G04	2199	8.533178
SC-MG-G10	2143	8.315871
DB-SG-G01	2129	8.261544
SF-BVS-G01	2052	7.962747
DC-SG-G02	1855	7.198293

- We are given the TOP 5 selling product IDs.

- We click on the Visualization tab, and we see this...



Practice 10: Another way of using the TOP Command

- Type in the following
 - `sourcetype=access_* | top 3 action by referer_domain`

The screenshot shows a Splunk search interface with the following search query: `sourcetype=access_* | top 3 action by referer_domain`. The search results are displayed in a table with columns for `referer_domain`, `action`, `count`, and `percent`. The top three results for `referer_domain` are `http://www.bing.com`, `http://www.buttercupgames.com`, and `http://www.google.com`. The top three actions for `http://www.bing.com` are `view`, `addtocart`, and `remove`. Red and blue boxes highlight these specific cells, with arrows pointing from the search query to the corresponding table cells.

referer_domain	action	count	percent
http://www.bing.com	view	46	51.111111
http://www.bing.com	addtocart	21	23.333333
http://www.bing.com	remove	12	13.333333
http://www.buttercupgames.com	purchase	5737	30.120229
http://www.buttercupgames.com	addtocart	5572	29.253951
http://www.buttercupgames.com	view	5054	26.534362
http://www.google.com	view	201	50.375940
http://www.google.com	addtocart	96	24.060150
http://www.google.com	remove	53	13.283208
http://www.yahoo.com	view	90	49.450549
http://www.yahoo.com	addtocart	54	29.670330
http://www.yahoo.com	remove	21	11.538462

- Type in the following
 - sourcetype=access_* | top 3 action by referer_domain countfield=Total

New Search

Save As Create Table View Close

sourcetype=access_* | top 3 action by referer_domain countfield=Total All time

✓ 39,532 events (before 5/14/21 12:49:25.000 AM) No Event Sampling Job

Events Patterns **Statistics (12)** Visualization

20 Per Page Format Preview

referer_domain	action	Total	percent
http://www.bing.com	view	46	51.111111
http://www.bing.com	addtocart	21	23.333333
http://www.bing.com	remove	12	13.333333
http://www.buttercupgames.com	purchase	5737	30.120229
http://www.buttercupgames.com	addtocart	5572	29.253951
http://www.buttercupgames.com	view	5054	26.534362
http://www.google.com	view	201	50.375940
http://www.google.com	addtocart	96	24.060150
http://www.google.com	remove	53	13.283208
http://www.yahoo.com	view	90	49.450549
http://www.yahoo.com	addtocart	54	29.670330
http://www.yahoo.com	remove	21	11.538462

- We are able to change the column named “count” to “total”.

Practice 11: Day of the Week

- Type in the following
 - buttercupgames | top 1 productId by date_wday

The screenshot shows a search tool interface with a search bar containing the query 'buttercupgames | top 1 productId by date_wday'. The results are displayed in a table with columns for 'date_wday', 'productId', 'count', and 'percent'. The 'date_wday' column is highlighted in a red box, and the 'Not In Order' message is visible below the table.

date_wday	productId	count	percent
friday	SF-BVS-G01	301	8.308032
monday	DB-SG-G01	321	8.394351
saturday	WC-SH-G04	326	8.796546
sunday	SF-BVS-G01	334	8.904292
thursday	SC-MG-G10	322	8.984375
tuesday	WC-SH-G04	341	8.992616
wednesday	WC-SH-G04	320	9.169054

Not In Order

- Now we have the top selling productId by day.
- Since it is not in order, we type in the following:
 - buttercupgames | eval DayOfWeekA=strftime(_time,"%A") | eval DayOfWeekN=strftime(_time,"%u") | top 1 productId by DayOfWeekN, DayOfWeekA

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Dr. Alvi...', 'Messages', 'Settings', 'Activity', 'Help', and a search box. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and a 'Search & Reporting' button.

The main content area is titled 'New Search'. It contains a search query: `buttercupgames | eval DayOfWeekA=strftime(_time,"%A") | eval DayOfWeekN=strftime(_time,"%u") | top 1 productId by DayOfWeekN, DayOfWeekA`. The search results show 36,819 events. Below the search bar, there are tabs for 'Events', 'Patterns', 'Statistics (7)', and 'Visualization'. The 'Statistics (7)' tab is active, displaying a table with 7 rows and 6 columns: DayOfWeekN, DayOfWeekA, productId, count, and percent.

DayOfWeekN	DayOfWeekA	productId	count	percent
1	Monday	DB-SG-G01	321	8.394351
2	Tuesday	WC-SH-G04	341	8.992616
3	Wednesday	WC-SH-G04	320	9.169054
4	Thursday	SC-MG-G10	322	8.984375
5	Friday	SF-BVS-G01	301	8.308032
6	Saturday	WC-SH-G04	326	8.796546
7	Sunday	SF-BVS-G01	334	8.904292

- Explanation:
 - We created two new fields:
 - DayOfWeekA : represents the alphabetic day of the week,
 - DayOfWeekN : represents the numerical day of the week.
 - We use a function, strftime, to evaluate the _time field and return the days of the week in the format we are looking for.
 - %A specifies the alphabetical day of the week
 - %u specifies the numerical day of the week
 - the combination here will give us our days in the proper order.

Practice 12: Tagging

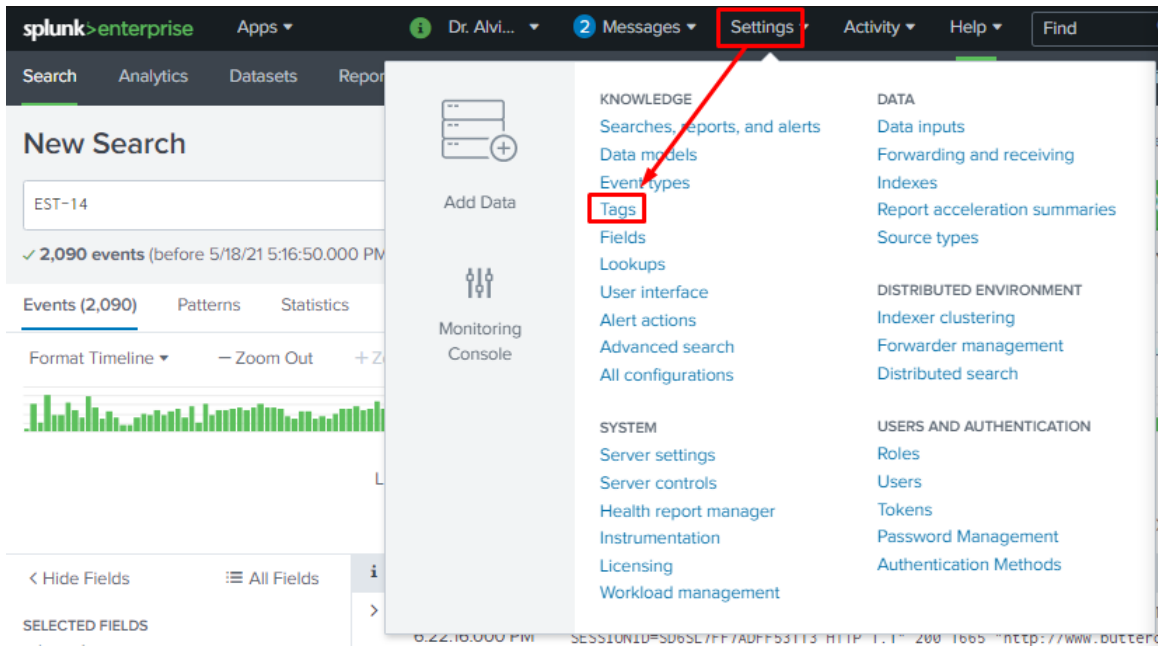
- Type in the following
 - EST-14

The screenshot shows the Splunk Enterprise interface. At the top, the search bar contains the text 'EST-14'. Below the search bar, a bar chart visualization shows the distribution of events over time. The main table displays two search results for the tag 'EST-14'. A red arrow points from the search bar to the 'itemId=EST-14' field in the first result, and another red arrow points from the same field to the 'itemId=EST-14' field in the second result.

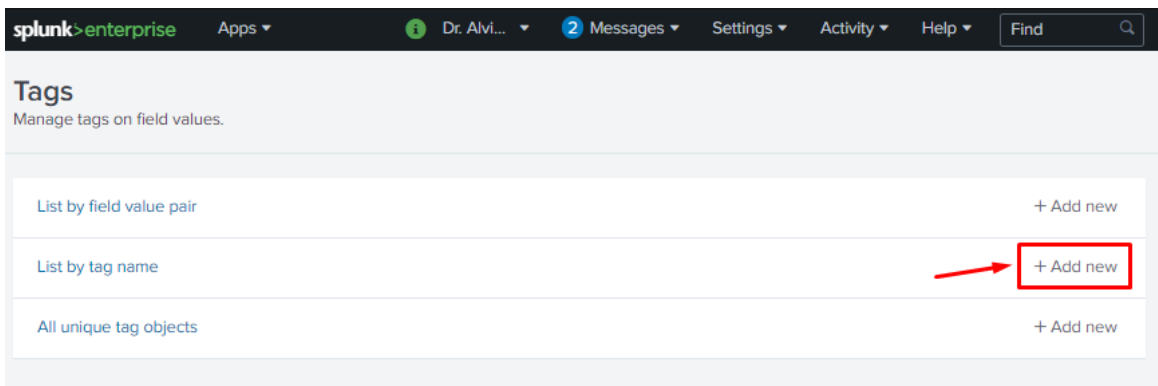
i	Time	Event
>	5/30/20 6:22:16.000 PM	91.205.189.15 - - [30/May/2020:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome host = DESKTOP-CAEPR49 source = tutorialdata.zip:\www2/access.log sourcetype = access_combined_wcookie
>	5/30/20 6:18:55.000 PM	198.35.1.75 - - [30/May/2020:18:18:55] "GET /product.screen?productId=SF-BVS-G018&JSESSIONID=SD10SL2FF4ADFFercupgames.com/cart.do?action=view&itemId=EST-14" Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (Fari/536.5" 370 host = DESKTOP-CAEPR49 source = tutorialdata.zip:\www1/access.log sourcetype = access_combined_wcookie

- All itemId=EST-14 will appear as shown.

- Go to Settings → Tags



- Click Add New



- Type in ITEM14 and itemId=EST-14... then click Save

The screenshot shows the 'Add new' page in Splunk. The 'Tag name' field is filled with 'ITEM14'. Below it, the 'Field value pair' section shows an example 'host=splunk.com' and a new entry 'itemId=EST-14'. A red box highlights the 'Save' button at the bottom right.

- You have tagged every itemId=EST-14 with the tag ITEM14.

The screenshot shows the 'List by tag name' page. It displays a table with one tag entry:

Tag name	Field value pair	Owner	App	Status	Actions
ITEM14	itemId=EST-14	dralvinang	search	Enabled Disable	Clone Delete

Practice 13: Saving Event Types

- Type in the following
 - `sourcetype="access_*" status=200 action=purchase`
- This searches for events where:
 - the sourcetype is an accessed web page,
 - the access was successful (`status=200`), and
 - it ended in a purchase

The screenshot shows the Splunk Search & Reporting interface. At the top, the search bar contains the query `sourcetype="access_*" status=200 action=purchase`. Below the search bar, a bar chart visualization shows the distribution of events over time. The event log below the chart displays a single event with the following details:

i	Time	Event
>	5/30/20 6:20:54.000 PM	182.236.164.11 - - [30/May/2020:18:20:54] "POST /cart/success.do?JSESSIONID=SD6SL8FF0ADFF53101 HTTP/1.1" 200 356 "http://www.buttercupgame.com/cart.do?action=purchase&itemId=EST-6" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 220 host = DESKTOP-CAEPR49 source = tutorialdata.zip:\www1/access.log sourcetype = access_combined_wcookie

Red arrows point from the search query to the corresponding fields in the event log: `sourcetype="access_*"` points to `sourcetype = access_combined_wcookie`, `status=200` points to the status code `200`, and `action=purchase` points to `action=purchase` in the event details.

Search Analytics Datasets Reports Alerts Dashboards

New Search

Save As ▾ Create Table View

sourcetype="access_*" status=200 action=purchase

✓ 5,224 events (before 5/18/21 7:13:59.000 PM) No Event Sampling ▾ Job ▾

Events (5,224) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection x Deselect

List ▾ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8

Hide Fields		All Fields	i	Time	Event
SELECTED FIELDS			>	5/30/20 6:20:54.000 PM	182.236.164.11 - - [30/May/2020:18:20:54] "POST /cart/su IONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 356 "http://www. s.com/cart.do?action=purchase&itemId=EST-6" "Mozilla/5.0 ntel Mac OS X 10_7_4 AppleWebKit/536.5 (KHTML, like Gec 0.1084.46 Safari/536.5" 220
INTERESTING FIELDS				host = DESKTOP-CAEPR49 ; source = tutorialdata.zip:www1/i	sourcetype = access_combined_wcookie

Save As Event Type

Name:

Tags:

Color:

Priority:

Determines which style wins, when an event has more than one event type.

Cancel Save

Your Event Type Has Been Created

You can edit this event type via [Event Types](#) in the Settings menu.

Done

Search Analytics Datasets Reports Alerts Dashboards > Search

New Search Save As ▾ Create Table View

sourcetype="access_*" status=200 action=purchase All time

✓ **5,224 events** (before 5/18/21 7:13:59.000 PM) No Event Sampling ▾ Job ▾ || ■ ↻ ⌵ ⌴ Smart M

Events (5,224) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1

List ▾ / Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 .

< Hide Fields		≡ All Fields	i	Time	Event
SELECTED FIELDS					
a host 1					
a source 3					
a sourcetype 1					
INTERESTING FIELDS					
a action 1					
				>	5/30/20 6:20:54.000 PM
		182.236.164.11 - - [30/May/2020:18:20:54] "POST /cart/suc IONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 356 "http://www.t s.com/cart.do?action=purchase&itemId=EST-6" "Mozilla/5.0 ntel Mac OS X 10_7_4 AppleWebKit/536.5 (KHTML, like Geck 0.1084.46 Safari/536.5" 220 host = DESKTOP-CAEPR49 source = tutorialdata.zip:\www1/a sourcetype = access_combined_wcookie			

- Recall earlier that the total number of events was 5,224. Now that you have stored the event type and labelled it "SUCCESS", you tally it and it also has 5224 counts.

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search Save As ▾ Create Table View Close

buttercupgames | stats count by eventtype All time 🔍

✓ **36,819 events** (before 5/18/21 8:43:11.000 PM) No Event Sampling ▾ Job ▾ || ■ ↻ ⌵ ⌴ Smart Mode ▾

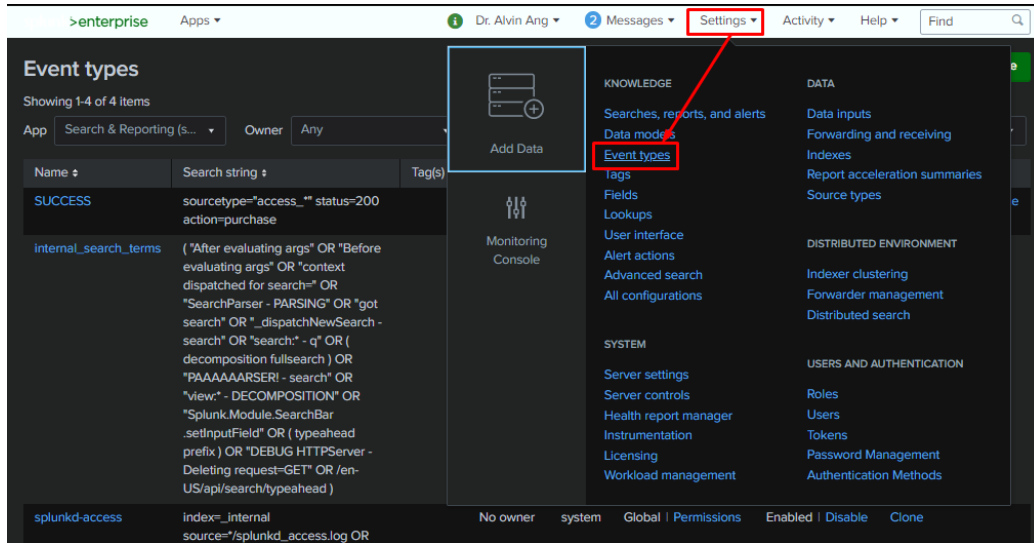
Events Patterns Statistics (1) Visualization

20 Per Page ▾ / Format Preview ▾

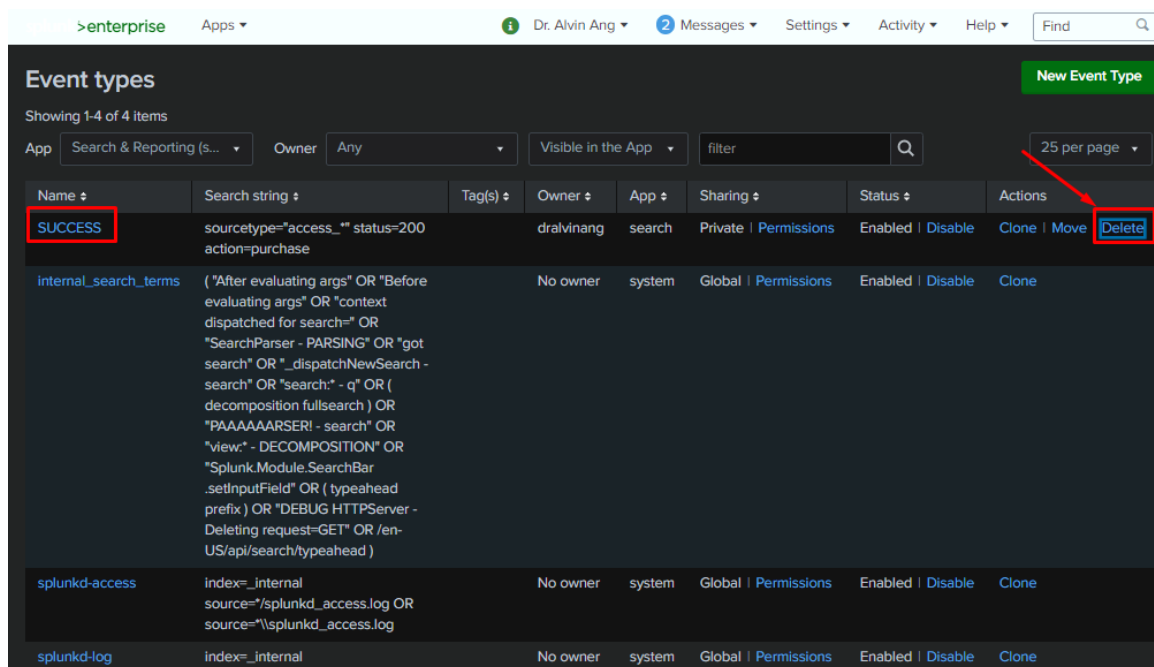
eventtype ↕	count ↕
SUCCESS	5224

Practice 14: Deleting Event Types

- Go to Settings → Event Types



- Choose “delete” the Event you want to delete.

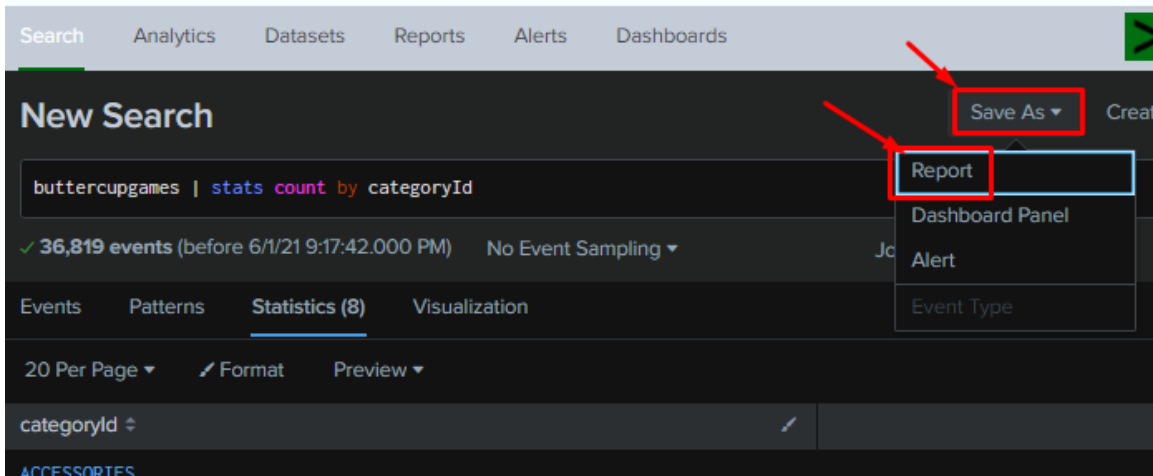


Practice 15: Creating Reports

- Type this in the search box:
 - buttercupgames | stats count by categoryId

The screenshot shows the Splunk Search & Reporting interface. The search query 'buttercupgames | stats count by categoryId' is entered in the search box. The results show 36,819 events. The 'Statistics (8)' tab is selected, displaying a table with the following data:

categoryId	count
ACCESSORIES	2035
ARCADE	2631
NULL	2041
SHOOTER	1323
SIMULATION	1375
SPORTS	763
STRATEGY	4399
TEE	1937



- Give the report a title “CateogryID Counts”

Save As Report [X]

Title:

Description:

Content: Statistics Table

Time Range Picker: Yes No

Your Report Has Been Created [X]

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- [Permissions](#)
- [Schedule](#)
- [Acceleration](#)
- [Embed](#)

enterprise Apps Dr. Alvi... Messages Settings Activity Help Find

Search Analytics Datasets **Reports** Alerts Dashboards Search & Reporting

CategoryID Counts

All time

✓ 36,819 events (before 6/1/21 9:17:42.000 PM)

8 results 20 per page

categoryId	count
ACCESSORIES	2035
ARCADE	2631
NULL	2041
SHOOTER	1323
SIMULATION	1375
SPORTS	763
STRATEGY	4399
TEE	1937

Search Analytics Datasets **Reports** Alerts Dashboards Search & Reporting

Reports

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.

7 Reports

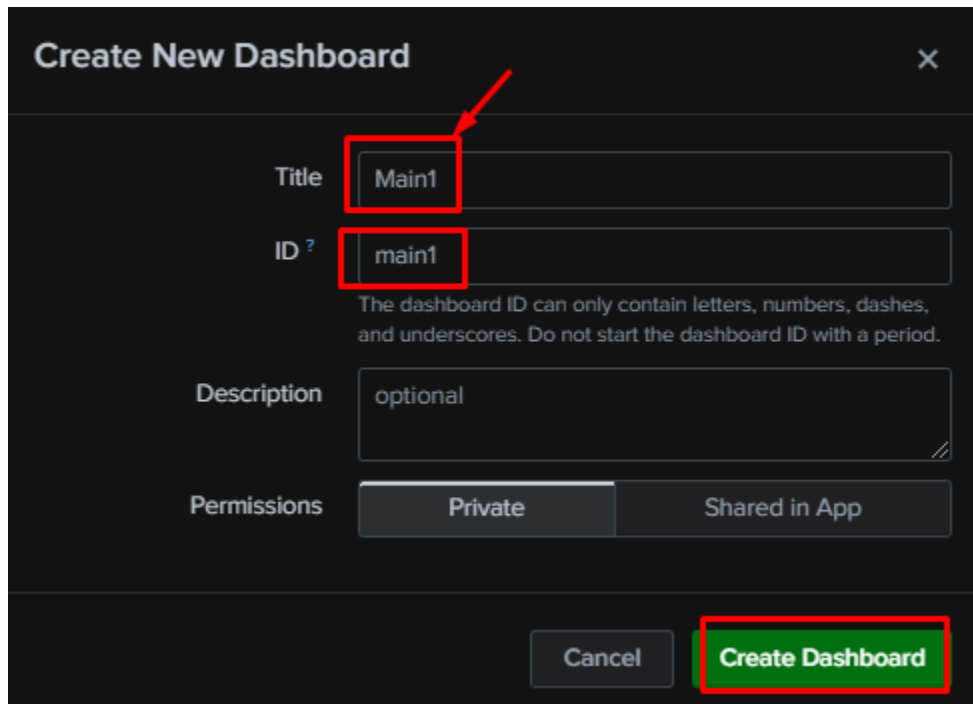
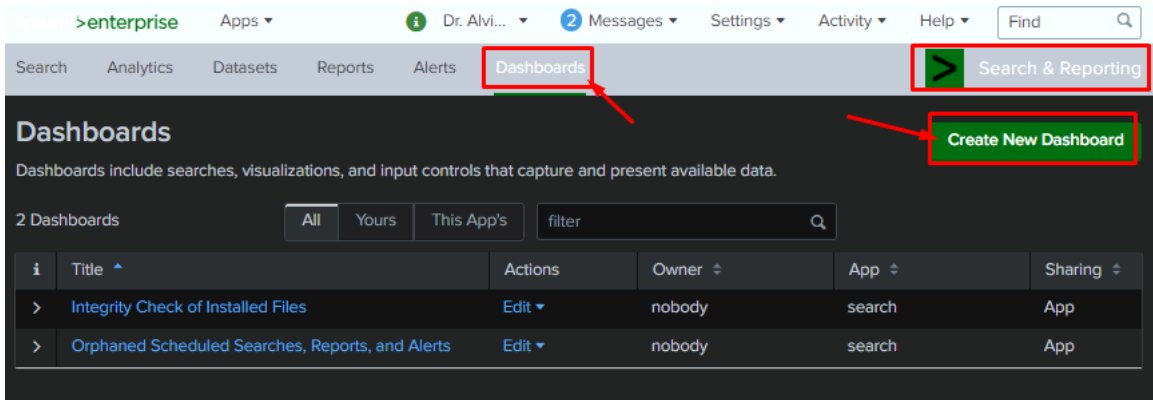
All Yours This App's filter

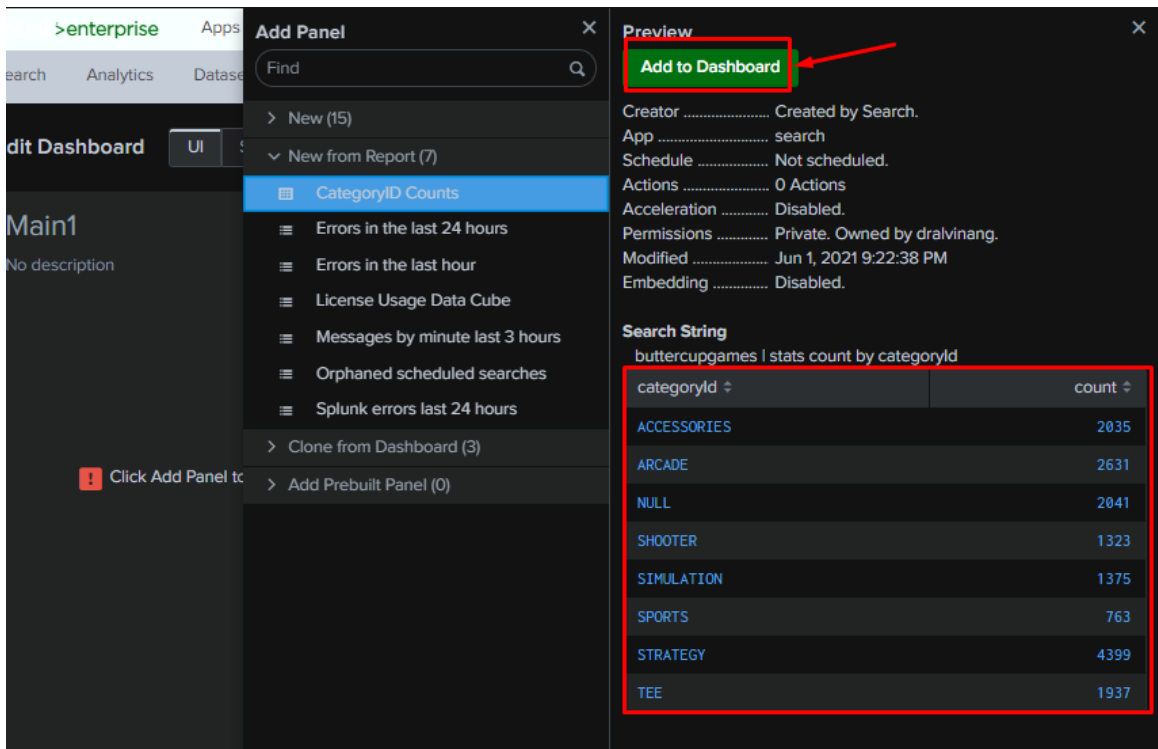
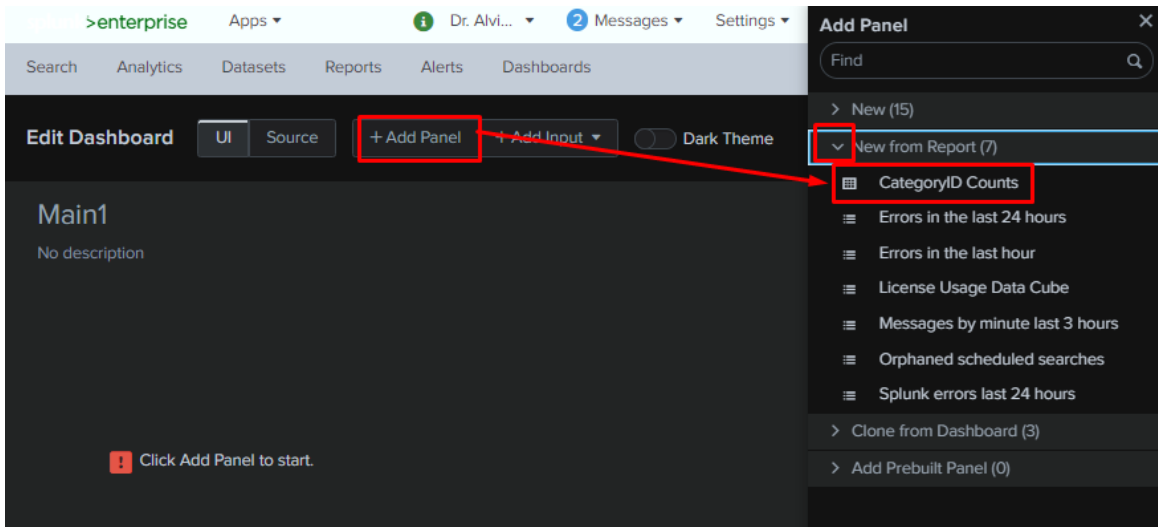
i	Title	Actions	Next Scheduled Time	Owner	App	Sharing
>	CategoryID Counts	Open in Search Edit	None	dralvinang	search	Private
>	Errors in the last 24 hours	Open in Search Edit Description Edit Permissions Edit Schedule Edit Acceleration	None	nobody	search	App
>	Errors in the last hour	Open in Search Edit Description Edit Permissions Edit Schedule Edit Acceleration	None	nobody	search	App
>	License Usage Data Cube	Open in Search Clone Embed Delete	None	nobody	search	App
>	Messages by minute last 3 ...	Open in Search	None	nobody	search	App
>	Orphaned scheduled search...	Open in Search Edit	None	nobody	search	App
>	Splunk errors last 24 hours	Open in Search Edit	None	nobody	search	App

- You may
 - Change the description
 - Edit permissions
 - Edit the schedule
 - schedule the report to be run (every hour, day, week, or month)
 - schedule an e-mail to alert you when the report runs
 - Edit acceleration
 - accelerate the development of the report
 - Clone the report
 - Embed the report in a website (However, the report has to be scheduled to do this.)
 - Delete the report

Practice 16: Creating Dashboards

- Under “Search and Reporting”, click the following





Main1
No description

No title

CategoryID Counts

categoryId	count
ACCESSORIES	2035
ARCADE	2631
NULL	2041
SHOOTER	1323
SIMULATION	1375
SPORTS	763
STRATEGY	4399
TEE	1937

Main1
No description

No title

CategoryID Counts

View report

Splunk Visualizations

- Table visualization (highlighted)
- Line chart
- Area chart
- Bar chart
- Number
- World map

Find more visualizations

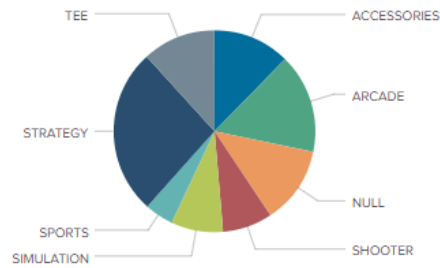
Statistics Table
Show results organized in rows and columns.

Main1

No description

No title

CategoryID Counts



Practice 17: Creating a Bar Chart

- Type the following into the search bar:
- `sourcetype=access* | timechart per_minute(eval(method="POST")) AS Views per_minute(eval(action="purchase")) AS Purchases`



- Click on Visualization → Bar Chart (and you will see the above)
- To break it down...
 - Step 1: sourcetype=access* |
 - Step 2: timechart per_minute(eval(method="POST")) AS Views
 - Step 3: per_minute(eval(action="purchase")) AS Purchases
- What we did:
 - Step 1: We begin by searching for all events with a *sourcetype* that begins with “access”.

```

> 5/30/20 12.130.60.5 - - [30/May/2020:17:57:58] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53001 HTTP 1.1" 200 1167 "http://www.but
5:57:58.000 PM tercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 232
host = DESKTOP-CAEPR49 | source = tutorialdata.zip:\www1/access.log | sourcetype = access_combined_wcookie

```

- Step 2: Then we use the *timechart command* and the *per_minute function* to give us a figure for the number of events per minute that use *method="POST"*, and then label it as *Views*.

INTERESTING FIELDS

- a action 5
- # bytes 100+
- a categoryId 8
- a clientip 100+
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 7
- # date_year 1
- a date_zone 1
- a file 14
- a ident 1
- a index 1
- a itemId 14
- a JSESSIONID 100+
- # linecount 1
- a method 2**
- # other 100+
- a productId 16
- a punct 98
- a referer 100+
- a referer_domain 4
- a req_time 100+
- a splunk_server 1

i	Time	Event
		host = DESKTOP-CAEPR49 source = tutorialdata.zip:\www1/access.log sourcetype = access_combined_wcookie
>	5/30/20 6:02:54.000 PM	74.53.23.135 - - [30/May/2020:18:02:54] "GET /oldlink?itemId=EST-17&JSESSIONID=SD8SL10FF5ADFF53017 HTTP 1.1" 200 2378 "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 822
>	5/30/20 6:02:54.000 PM	74.53.23.135 - - [30/May/2020:18:02:54] "POST /cart/success.do?JSESSIONID=SD8SL10FF5ADFF53017 HTTP 1.1" 200 2023 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 622
>	5/30/20 6:02:54.000 PM	74.53.23.135 - - [30/May/2020:18:02:54] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD8SL10FF5ADFF53017 HTTP 1.1" 200 3848 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=STRATEGY&productId=DB-SG-G01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 505 2753 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&productId=DB-SG-G01&JSESSIONID=SD8SL10FF5ADFF53017 HTTP 1.1" 200 3848 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-18&productId=MB-AG-G07" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 822

method

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
GET	24,866	62.901%
POST	14,666	37.099%

- Step 3: In addition, we use the *per_minute* function to find the number of events per minute that have *action="purchase"*, and then label the results as *Purchases*.

New Search Save As Create Table View Close

`sourcetype=access* | timechart per_minute(eval(method="POST")) AS Views per_minute(eval(action="purchase")) AS Purchases` All time 🔍

✓ 39,532 events (before 7/25/21 9:33:45.000 PM) No Event Sampling Job ⏸ 📄 ↶ 📄 ⏴ ⏵ 🔍 Smart Mode

Events Patterns Statistics (8) Visualization

20 Per Page 🔧 Format Preview

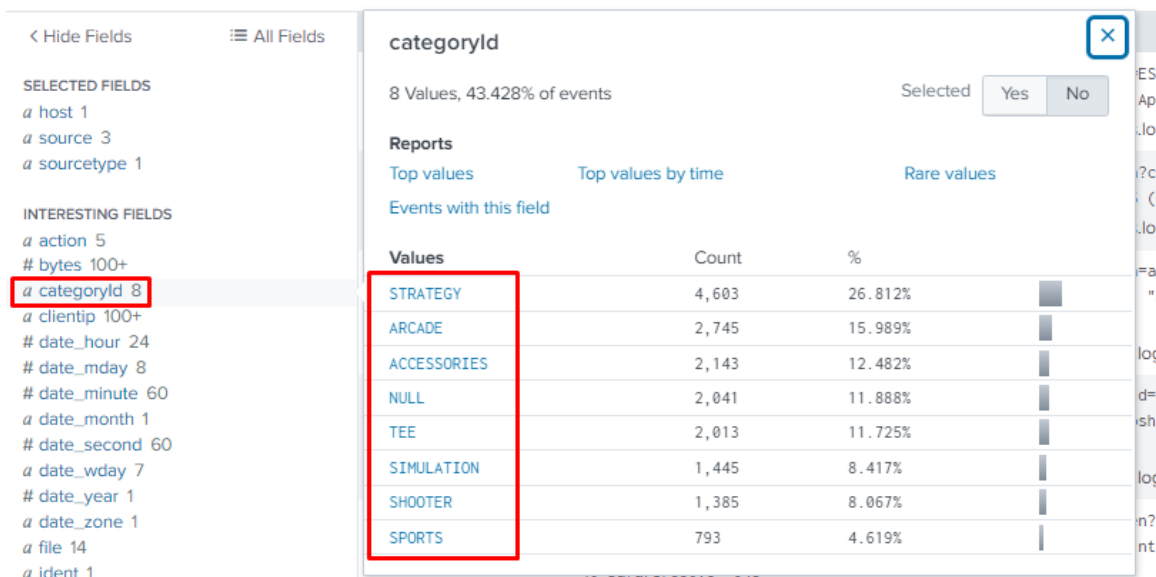
_time ↕	Views ↕	Purchases ↕
2020-05-23	0.297222	0.109028
2020-05-24	1.421528	0.543750
2020-05-25	1.588889	0.627083
2020-05-26	1.448611	0.575694
2020-05-27	1.381944	0.542361
2020-05-28	1.436111	0.550694
2020-05-29	1.411111	0.553472
2020-05-30	1.199306	0.481944

- And we get the end result... Views vs Purchases...

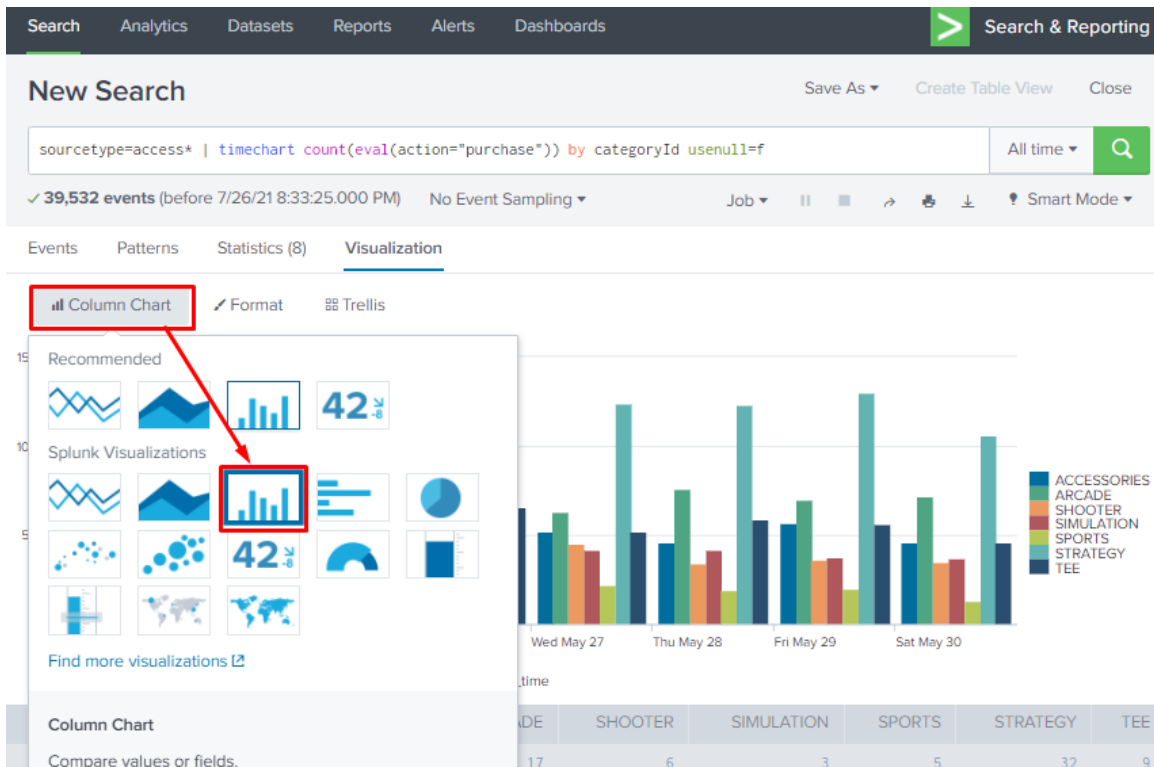
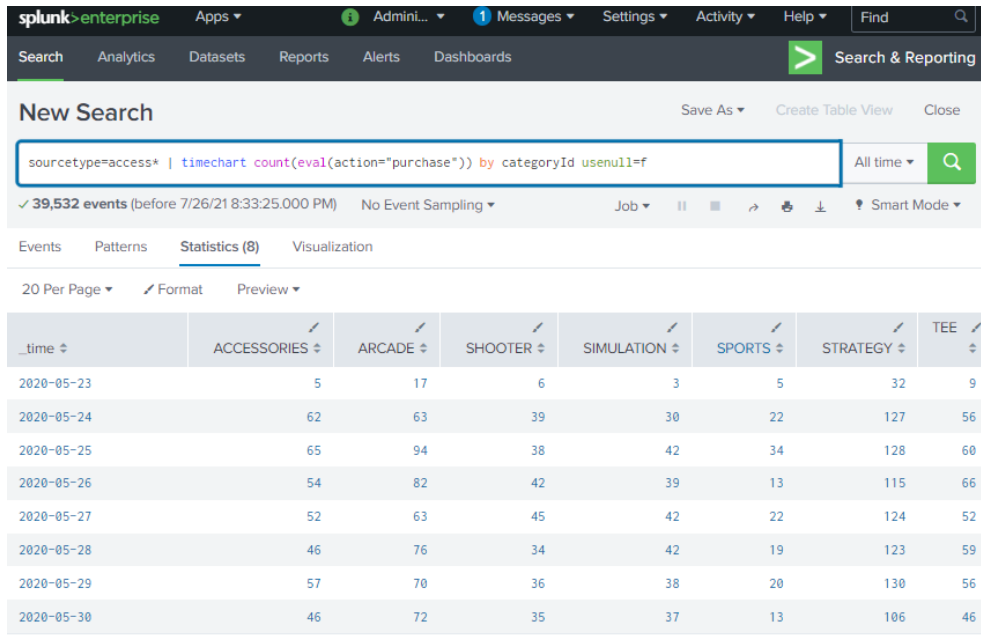


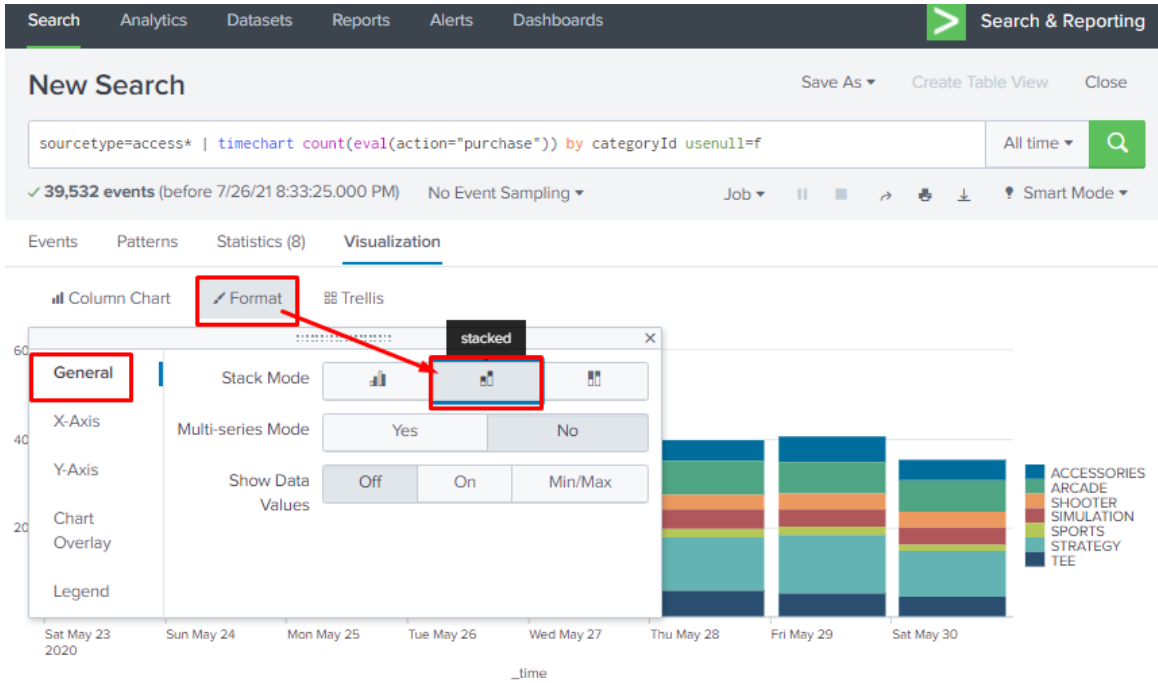
Practice 18: Creating a Stacked Bar Chart

- Type the following into the search bar:
- `sourcetype=access* | timechart count(eval(action="purchase")) by categoryId usenull=f`
- what this means...
 - First, we begin by searching for all events with a *sourcetype* that begins with “*access*”.
 - Then, we use the *timechart* command and the *count* function to give us the number of events that have *action="purchase"*, categorized by ID

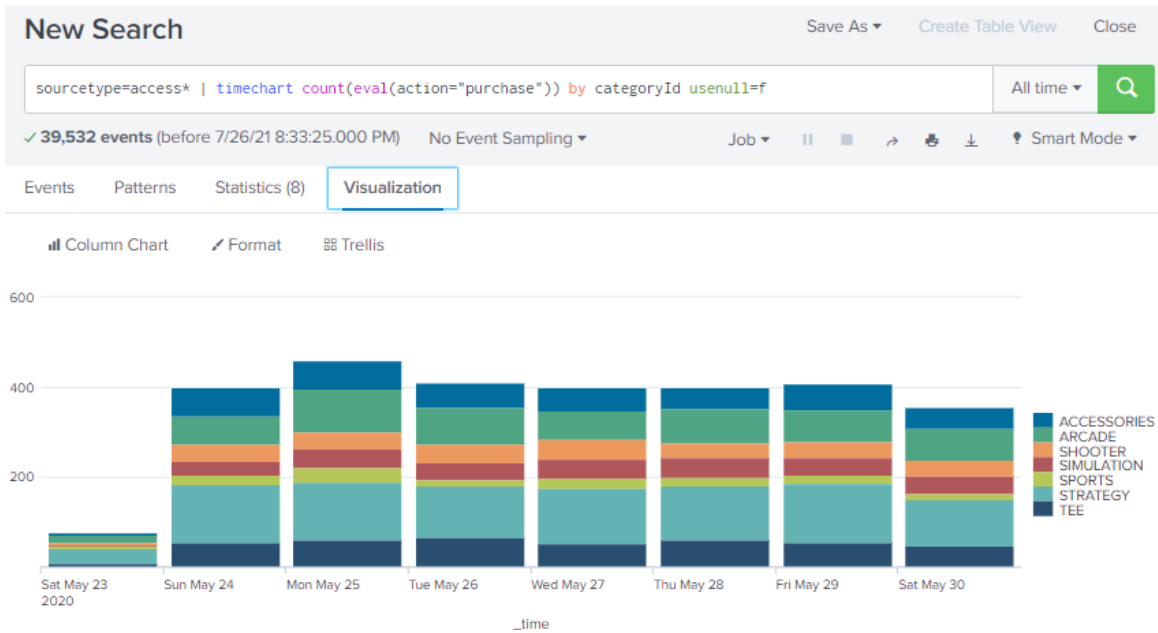


- The *usenull=f* piece indicates that you want to get rid of nulls for this analysis.



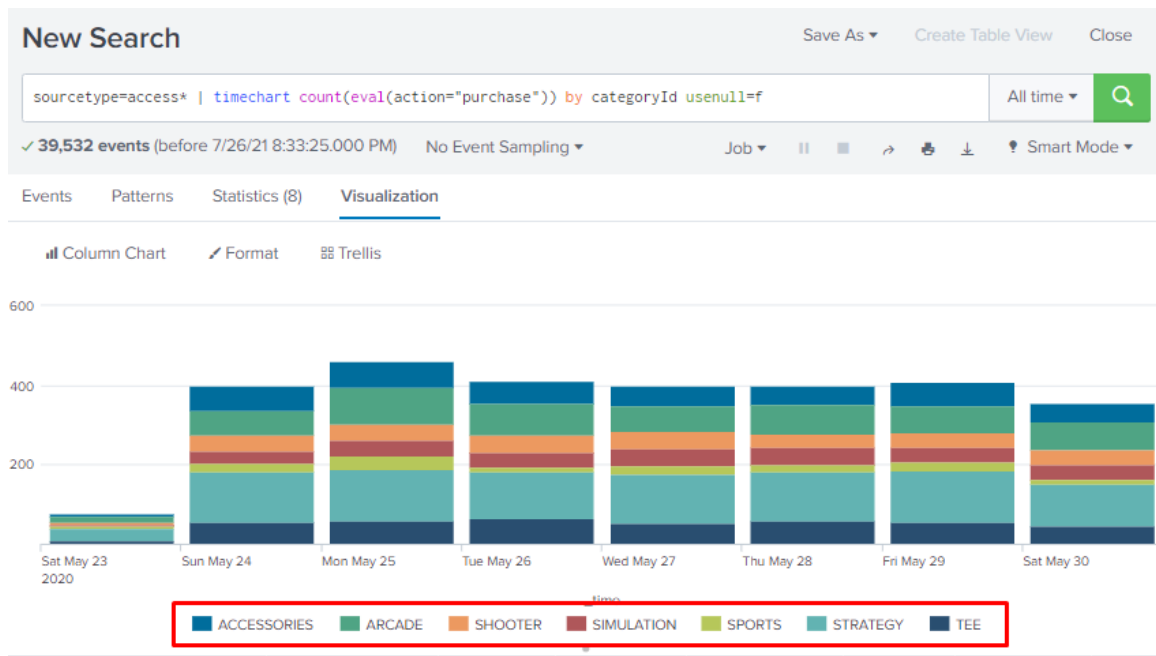
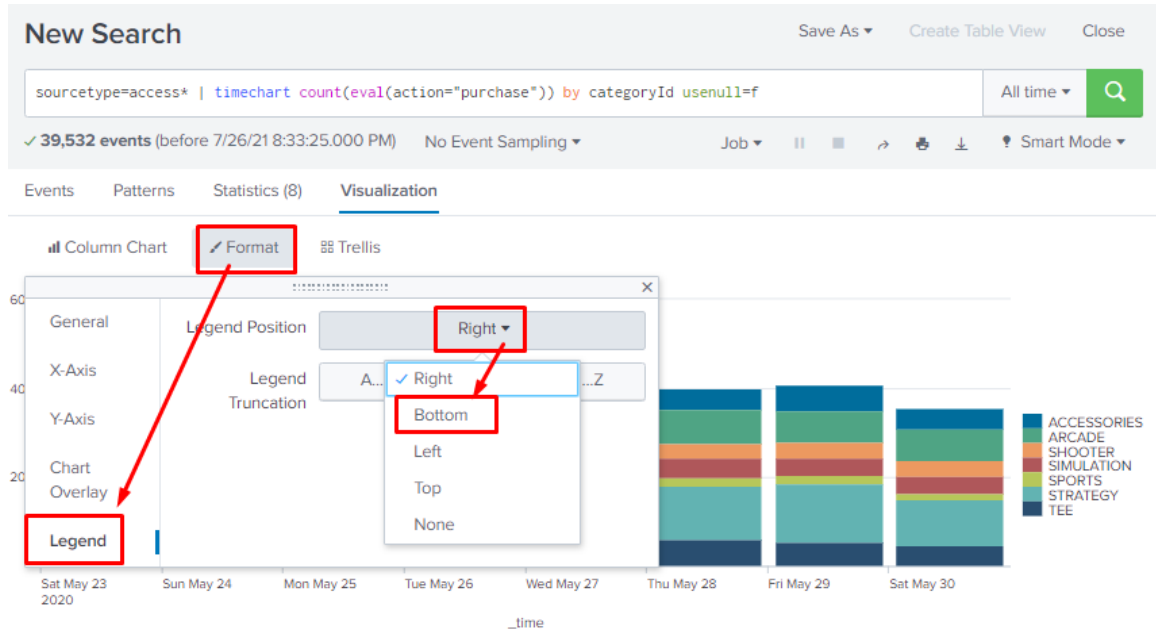


- And we finally end up with this stacked bar chart.



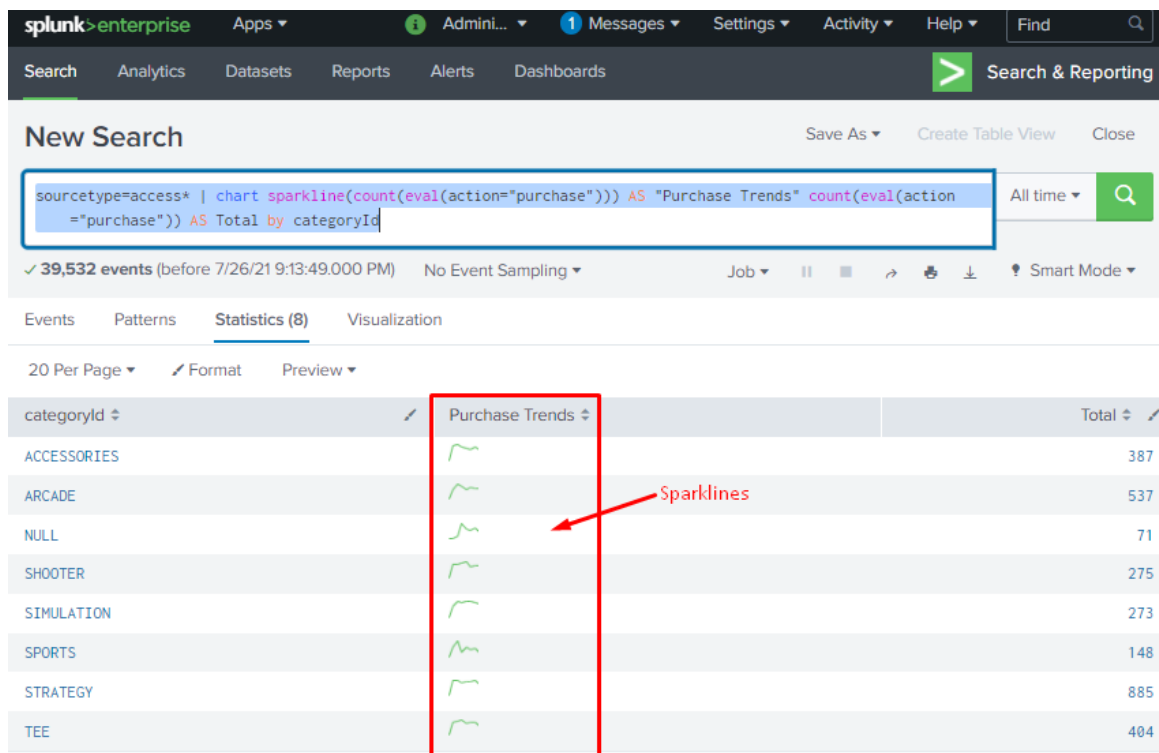
Practice 19: How to Format the Legend

- We continue from the previous practice. We shift the legend to the bottom.



Practice 20: Creating a Sparkline Panel

- Type this into the search box
 - `sourcetype=access* | chart sparkline(count(eval(action="purchase"))) AS "Purchase Trends" count(eval(action="purchase")) AS Total by categoryId`
- This statement is very similar to “Practice 18: Creating a Stacked Bar Chart”, which has already been explained earlier; thus it will not be reexplained here again.
- Sparklines have been created below.



Practice 21: Creating a Line Plot

- Type this into the search box
 - `buttercupgames | stats count(eval(action="purchase")) as Purchase by date_minute`
- What this means...
 - First, we begin by searching for all buttercupgames events.
 - Then, we use the *count command* to give us the number of events that have *action="purchase"*, and label the results as *Purchase*, and categorize by *date_minute*.

New Search

buttercupgames | stats count(eval(action="purchase")) as Purchase by date_minute

36,819 events (before 7/26/21 11:22:53.000 PM) No Event Sampling

Events Patterns **Statistics (60)** Visualization

20 Per Page Format Preview

date_minute	Purchase
0	113
1	94
10	89
11	93
12	122
13	85
14	103
15	70
16	70
17	98
18	101
19	75

New Search

Save As ▾ Create Table View Close

buttercupgames | stats count(eval(action="purchase")) as Purchase by date_minute

All time ▾ 🔍

✓ 36,819 events (before 7/26/21 11:33:15.000 PM) No Event Sampling ▾

Job ▾ || ■ ↶ ↷ ⏏ ⏴ ⏵ ⚙ Smart Mode ▾

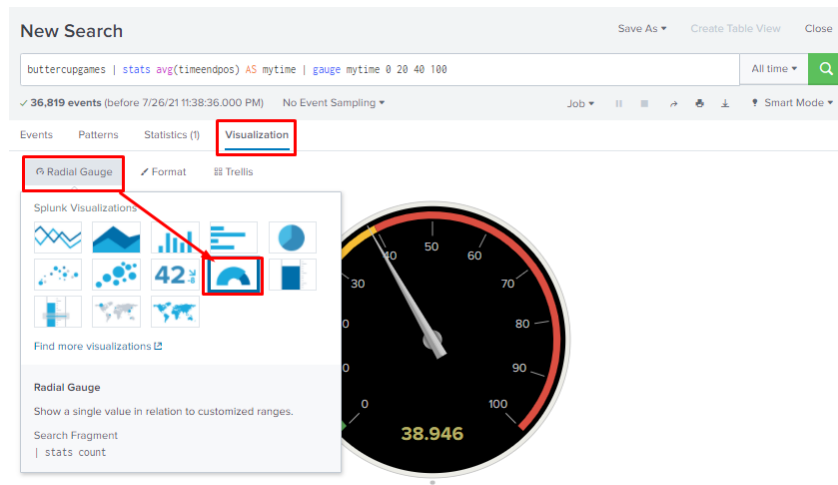
Events Patterns Statistics (60) **Visualization**

Line Chart ✓ Format Trellis

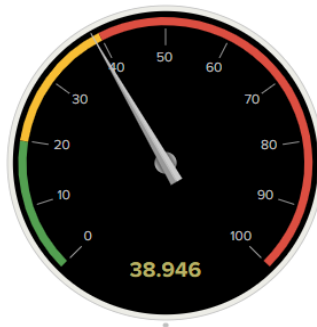


Practice 22: Creating a Radial Gauge

- Type this into the search box
 - `buttercupgames | stats avg(timeendpos) AS mytime | gauge mytime 0 20 40 100`



- We search the *buttercupgames events*, and measure the *average end time position* or *length of event* in seconds.
- Whenever the *average event time* goes over 40 seconds, the gauge that marks anything over 40 as red, and also has two categories for 0 to 20 and 20+ to 40.



Practice 23: Creating a Marker Gauge

- Type this into the search box
 - `buttercupgames | stats avg(timeendpos) AS mytime`

New Search

buttercupgames | stats avg(timeendpos) AS mytime

✓ 36,819 events (before 7/27/21 5:24:34.000 AM) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

100 Per Page ▾ ✓ Format Preview ▾

mytime ↕
38.94559873978109

the average end time position of each event, or rather, then average length of each event is 38.9 seconds

New Search

buttercupgames | stats avg(timeendpos) AS mytime

✓ 36,819 events (before 7/27/21 5:24:34.000 AM) No Event Sampling ▾

Events Patterns Statistics (1) **Visualization**

Marker Gauge ✓ Format Trellis

Splunk Visualizations

Find more visualizations ↗

Marker Gauge

Show a single value in relation to customized ranges.

Search Fragment

| stats count

New Search

buttercupgames | stats avg(timeendpos) AS mytime

✓ 36,819 events (before 7/27/21 5:24:34.000 AM) No Event Sampling ▾

Events Patterns Statistics (1) **Visualization**

Marker Gauge **Format** Trellis

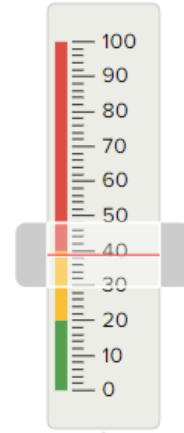
General

Color Ranges

Automatic Manual

Ranges from 0 to 20 40 100

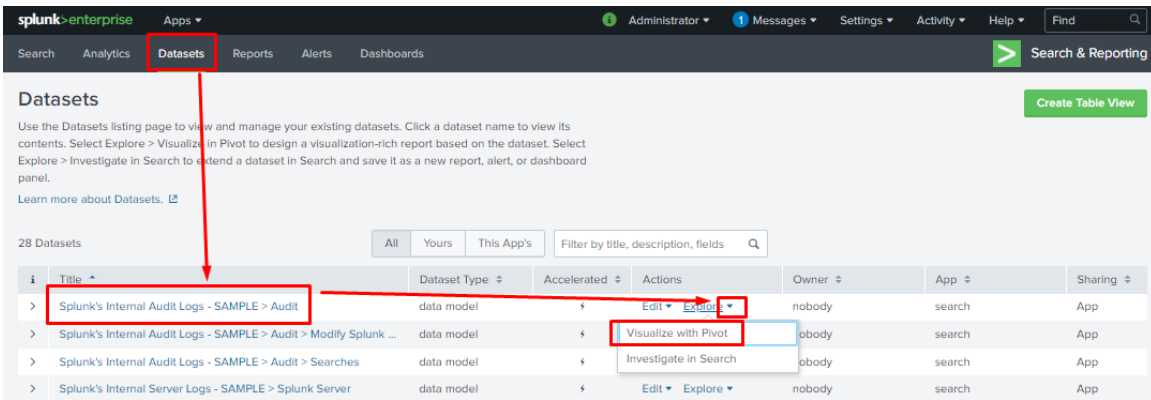
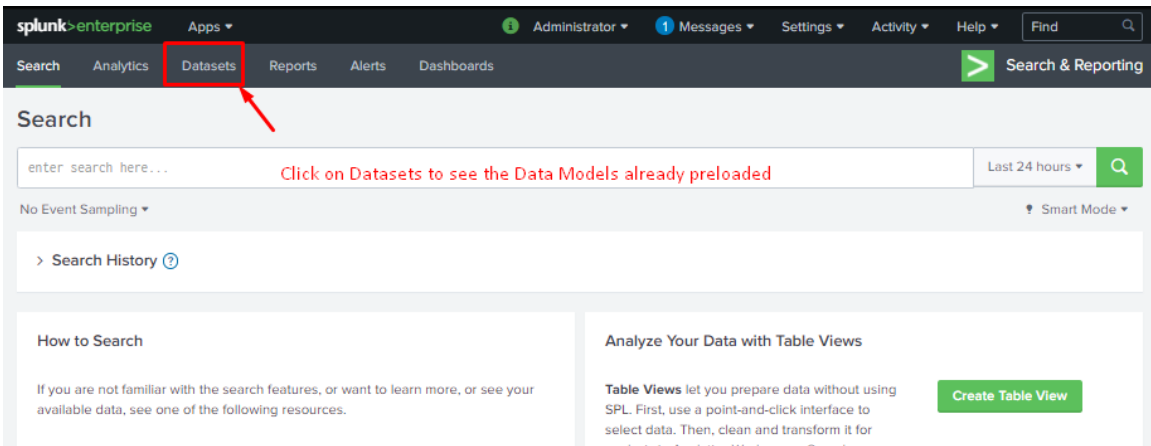
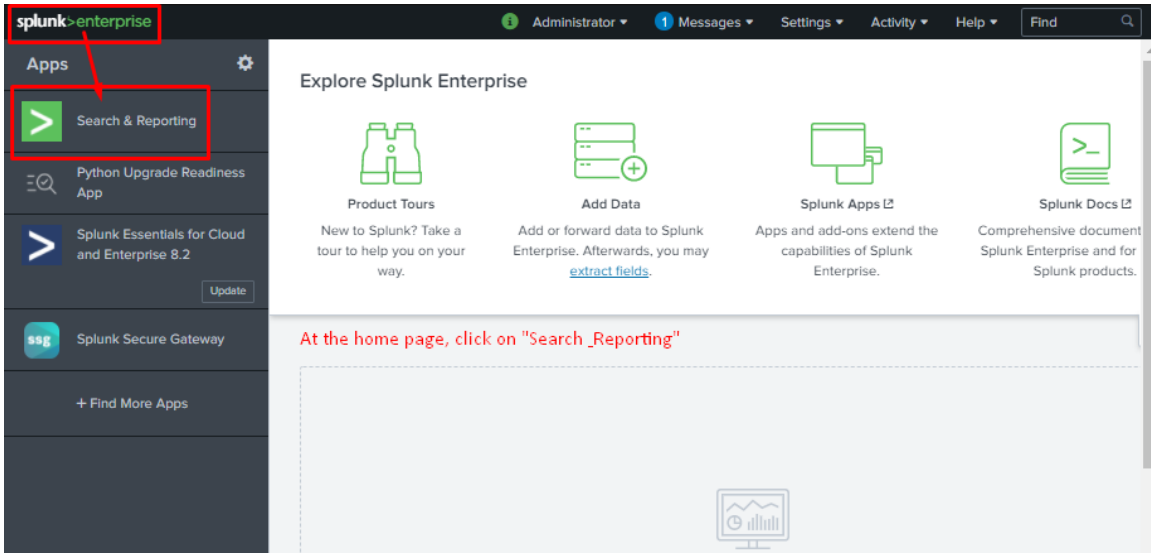
+ Add Range



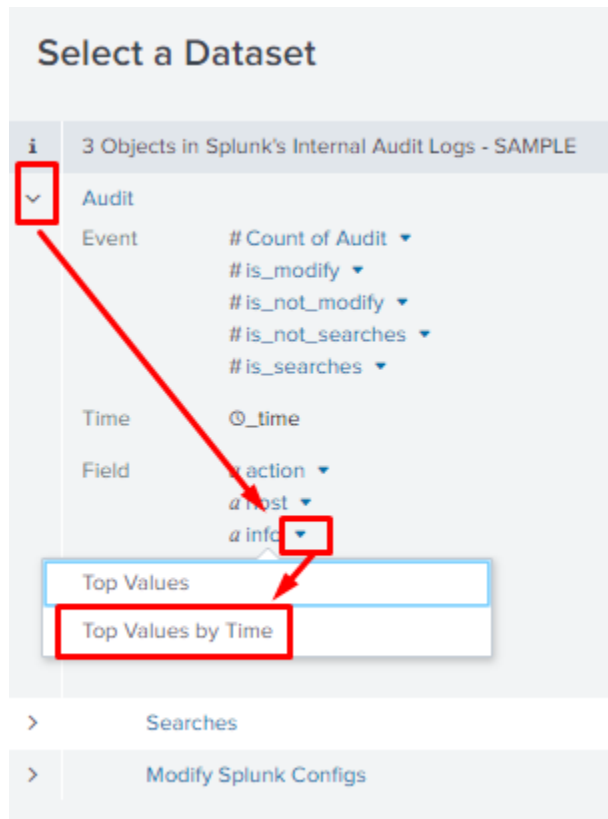
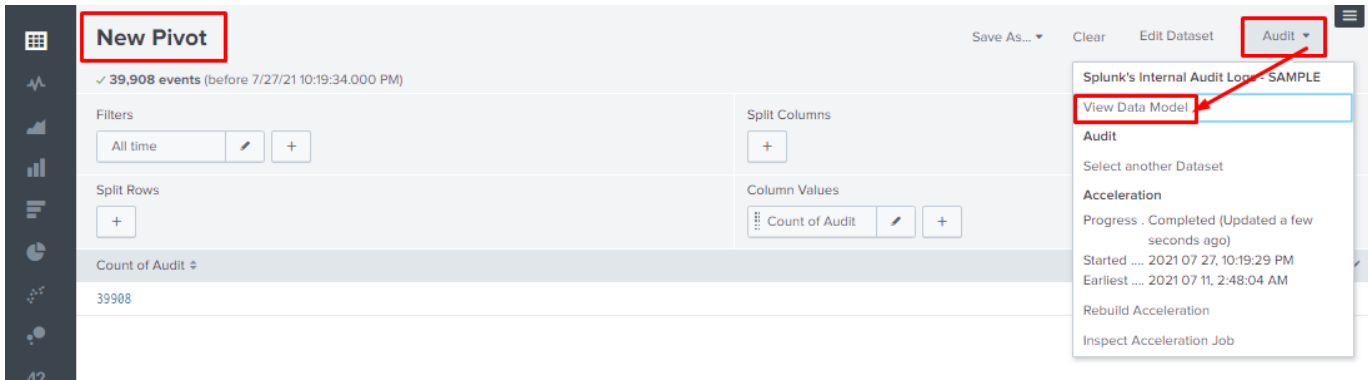
Practice 24: Creating a Pivot Table

- What is a Pivot Table?
 - A Pivot Table is used to summarise, sort, reorganise, group, count, total or average data stored in a table.
 - It allows us to transform columns into rows and rows into columns.
 - It allows grouping by any field (column)¹
 - Pivot tables allow you to view the data in many different ways.
- What is a Data Model?
 - To create a pivot table, you use a Data Model.
 - Data models allow you to structure the fields in objects that are easy to pull data from.
 - A model is set up by someone who has detailed knowledge of the data and its properties.
 - Here, we will use a model that is downloaded when you download Splunk.

¹ <https://www.lumeer.io/pivot-table-complete-guide/>



- Click on Splunk's Internal Audit Logs—SAMPLE.
- After you select the model, you will see a screen that shows the objects in the model



New Pivot Save As... Clear Edit Dataset Audit

✓ 40,116 events (before 7/27/21 10:21:54.000 PM)

Filters: All time

Split Columns: info

Split Rows: _time

Column Values: Count of Audit

_time	NULL	bad_request	cancel	canceled	completed	denied	expired	granted	n/a	pause	succeeded
2021-07-11	7166	0	0	0	79	553	25	1089	1	0	1
2021-07-12	6	0	0	0	48	524	0	26	0	0	0
2021-07-13	31	0	0	0	42	1177	0	42	0	0	0
2021-07-14	0	0	0	0	24	644	0	24	0	0	0
2021-07-15	0	0	0	0	34	933	0	34	0	0	0
2021-07-16	0	0	0	0	0	0	0	0	0	0	0
2021-07-17	0	0	0	0	36	986	0	36	0	0	0
2021-07-18	0	0	0	0	6	165	0	6	0	0	0
2021-07-19	7	0	0	0	25	1	0	24	1	0	0
2021-07-20	0	0	0	0	28	0	0	28	0	0	0

Save As Dashboard Panel ×

Dashboard New Existing

Dashboard Title

Dashboard ID ?
The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.

Dashboard Description

Dashboard Permissions Private Shared in App

Panel Title

Panel Powered By ?

Drilldown ?

Panel Content

Your Dashboard Panel Has Been Created ×

The panel has been created and added to splunks_internal_audit_logs__sample_. You may now view the dashboard.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Splunk's Internal Audit Logs — SAMPLE

Info - Top Values by Time

_time	NULL	bad_request	cancel	canceled	completed	denied	expired	granted	n/a	pause	succeeded
2021-07-11	7166	0	0	0	79	553	25	1089	1	0	1
2021-07-12	6	0	0	0	48	524	0	26	0	0	0
2021-07-13	31	0	0	0	42	1177	0	42	0	0	0
2021-07-14	0	0	0	0	24	644	0	24	0	0	0
2021-07-15	0	0	0	0	34	933	0	34	0	0	0
2021-07-16	0	0	0	0	0	0	0	0	0	0	0
2021-07-17	0	0	0	0	36	986	0	36	0	0	0
2021-07-18	0	0	0	0	6	165	0	6	0	0	0
2021-07-19	7	0	0	0	25	1	0	24	1	0	0
2021-07-20	0	0	0	0	28	0	0	28	0	0	0
2021-07-21	3	0	0	0	26	771	0	26	0	0	0
2021-07-22	0	0	0	0	44	1069	0	46	0	0	0
2021-07-23	39	0	0	0	64	302	0	689	0	0	0
2021-07-24	24	2	3	3	31	814	9	3059	0	0	2
2021-07-25	39	1	4	6	41	817	81	3098	0	1	3

- You end up with the dashboard above (with only 1 panel)
- You may choose to create another panel of your own choosing some other fields in a pivot table, then add the panel to your dashboard.

APPENDIX

TYPES OF SPL COMMAND

1. FILTER

Filter	Reduces results to a smaller set.	<code>search</code> <code>where</code> <code>dedup</code> <code>head</code> <code>tail</code>
--------	-----------------------------------	---

Types of Filter Commands:

1a. search function

<code>search</code>	This is the most important command Splunk has. It is the default command as well, so there is no need for you to type it in the search box. However, if you do another search after one or more pipes, you do need to include the word search in the command. We'll learn more about search in the section <i>How to perform simple searches</i> .
---------------------	--

1b. where function

<code>where</code>	This command takes an expression, such as <code>where monthly_sales > avg_mon_sales</code> , and evaluates it. If it is TRUE , it is kept in the search results.
--------------------	--

1c. dedup function

dedup	This command only keeps the first x results for each search. dedup source returns only the first result for each source. Building on this, dedup 3 source returns only the first three results for each source.
--------------	---

1d. head/tail function

head/tail	These commands look for a specified number of searched terms, counting from the top or bottom of the list of events. The head command returns the first x results. head 10 returns the first ten results. The tail command returns the last x results. Tail 10 returns the last ten results.
------------------	--

2. SORT

Sort	Orders the results and can also be used to limit the number of results.	<code>sort</code>
------	---	-------------------

Types of Filter Commands:

2a. `sort 0 anyfield`

<code>sort 0 anyfield</code>	This command sorts in ascending order by <code>userid</code> (A to Z, 1 to infinity, depending on whether the <code>anyfield</code> field is a number or name). The 0 means that all results are sorted, not just the default 10,000.
------------------------------	---

2b. `sort 1000 fieldone -fieldtwo`

<code>sort 1000 fieldone -fieldtwo</code>	Sorts by <code>fieldone</code> in ascending order, then by <code>fieldtwo</code> in descending order, and returns up to 1,000 results.
---	--

2x. `sort -fieldone, +fieldtwo`

<code>sort -fieldone, +fieldtwo</code>	Sorts by <code>fieldone</code> in descending order, and <code>fieldtwo</code> in ascending order. This command will return 10,000 results (the default).
--	--

3. GROUP

Command	What it Does
transaction	A transaction takes selected events and groups them together. transaction ipaddress host maxspan=60s groups together all events with the same combination of ipaddress and host , where the first and last event are no more than 60 seconds apart.

4. REPORT

4a. top/rare function

top/rare	The top command returns the values that occur most often, as well as their counts and percentages. The default is 10. top source returns a list of the top 10 sources, including their counts and percentages. top 15 source, host returns a list of the 15 most frequent source-host combinations.
-----------------	--

4b. stats function

stats	The stats command returns the results of statistical calculations. It can return a single number, as in stats dc(source) , which gives a distinct count that includes each different source. Or it can return a table, as in stats max(kbps) by host , which gives the maximum speed for each host.
--------------	--

Stats function	Description
avg(X)	Returns the average value of field X
dc(X)	Returns the distinct count of field X
earliest(X)	Returns the earliest value of field X, chronologically
last(X)	Returns the last seen value of field X
latest(X)	Returns the latest value of field X, chronologically
list(X)	Returns the list of all values of field X as a multi-value entry
max(X)	Returns the maximum value of field X
median(X)	Returns the middle value of all values of field X
min(X)	Returns the minimum value of field X
mode(X)	Returns the most frequent value of field X
perc<X>(Y)	Returns the X-th percentile value of field Y
range(X)	Returns the range (max-min) of field X
stdev(X)	Returns the standard deviation of field X
sum(X)	Returns the sum of all values of X
values(X)	Returns the list of all distinct values of field X as a multi-value entry
var(X)	Returns the sample variance of field X

4c. chart function

chart	<p>The chart command is used for creating tables of data. In each chart, the x-axis labels are indicated by either over or by.</p> <p>chart count(fail*) over host</p> <p>creates a chart showing the count of events that include the phrase "fail" plus anything after that (for example, "failed", "failure", and the like) for each value of host.</p> <p>For more on the chart command, go to http://docs.splunk.com/Documentation/Splunk/6.1.3/SearchReference/chart.</p>
--------------	--

4d. timechart function

timechart	<p>The timechart command produces a chart with time as the x-axis.</p> <p>timechart span=1d avg(delay) by host</p> <p>creates a chart showing the average delay by each host during a 1 day period.</p>
------------------	---

5. OTHER

5a. field

fields	The fields command is used to remove fields from a search. Thus, the command fields field1 field3 keeps only the fields labeled field1 and field3 .
---------------	---

5b. replace

replace	The replace command substitutes one value for another. In the statement replace 0 with Check, 9 with Warning in Status , status values of 0 are replaced with Check and status values of 9 are replaced with Warning .
----------------	--

5c. eval

eval	The eval command makes calculations and puts them into a new field. This code, eval Depth=case(depth<=3, "Low", depth>3 AND depth<=10, "Medium", depth>10, "High"), creates a new field, Depth , and uses the case function to assign the labels Low , Medium , or High , depending on the value.
-------------	--

Eval function	Description	Example
<code>case(X, "Y", . . .)</code>	Using pairs of arguments, X and Y, where X is TRUE, return Y.	<code>case(error == 404, "Not found", error == 200, "OK")</code>
<code>ceil(X)</code>	Gives the ceiling of a number.	<code>ceil(2.2)</code>
<code>if(X, Y, Z)</code>	If X is TRUE, result is Y. If X is FALSE, result is Z.	<code>if(error ==404, "Not found", "Found")</code>
<code>len(X)</code>	Returns number of characters in the string field.	<code>length(field)</code>
<code>lower(X), upper(X)</code>	Returns lowercase, uppercase.	<code>lower(username), upper(username)</code>
<code>round(X, Y)</code>	Rounds X to Y decimal places. If no Y is given, round to integer.	<code>round(3.5)</code>

5d. lookup

lookup	The lookup command calls up a lookup table that lets you add new field values. In the statement, lookup status_desc status OUTPUT description , the field, status , is looked up in the status_desc lookup table and the corresponding description is output.
---------------	--

ABOUT THE AUTHOR

Dr. Alvin Ang earned his Ph.D., Masters and Bachelor degrees from NTU, Singapore. He is a scientist, entrepreneur, as well as a personal/business advisor. More about him at www.AlvinAng.sg.