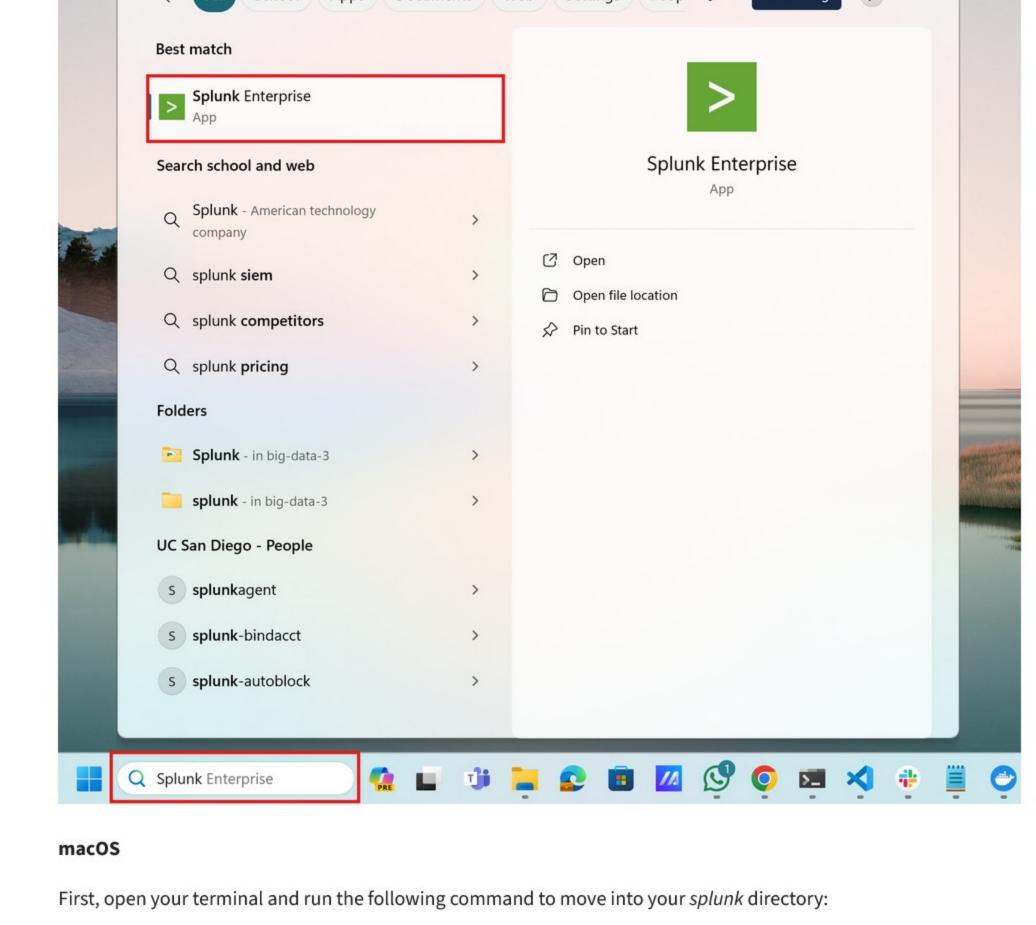
Exploring Splunk Queries

By the end of this activity, you will be able to:

- Import CSV files into Splunk.
- Query, filter, and plot data.
- Perform statistical calculations.

Step 1. Open Splunk. Windows

Go to the search menu, and search for Splunk. Once you locate the application, click on it, an you will be redirected



```
Then, run the following command to start Splunk:

1 ./bin/splunk start
```

•••••

Once you start Splunk, open your browser and go to http://localhost:8000/.

Step 2. Login. Login to Splunk by entering your credentials:

splunk>enterprise

cd /Applications/splunk



Sign In

Table ▼

Save As

_json

✓ Form

_time

4/16/24

11:48:4

4/16/24

Click on Select File:

Upload files from my computer

Selected File: No file selected

Select File

Navigate to your big-data-3/Splunk directory and select census.csv. Then click Next>:

data-3/Splunk directory and select census.csv. Then click Next>:

Source: census.csv

Source type: csv ▼

Source type: csv ▼

Default Settings

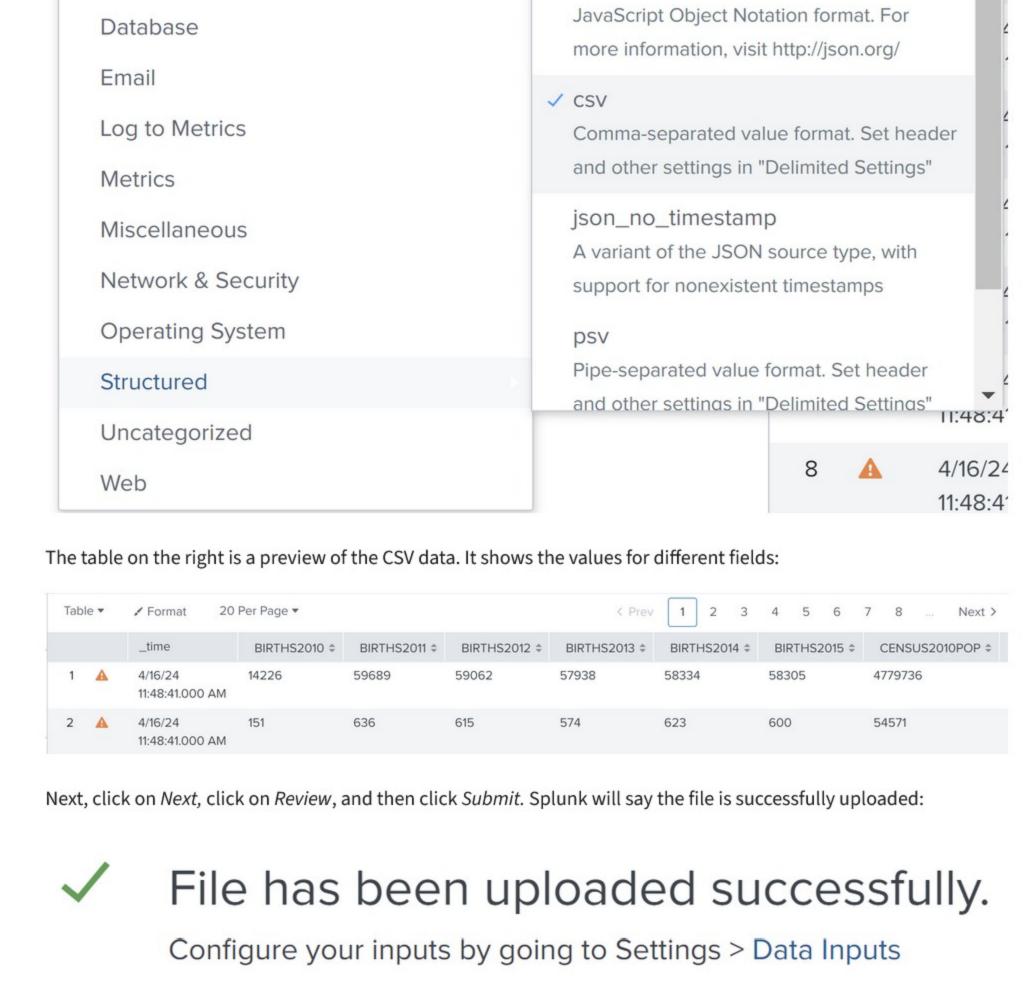
Application

Splunk's default source type settings

filter

On the left, make sure the Source type is csv:

If the Source type is not csv, click on Source type, go down to Structured, and select csv:



Splunk will enter a default query in the search box to show the data we just imported:

Step 4. View data. Click on Start Searching:

Start Searching

New Search

List v /Format v

1 STNAME="California"

query:

2 | table CTYNAME

1 STNAME="California" CENSUS2010POP>1000000

1 CENSUS2010POP>100000
2 | sort CENSUS2010POP desc
3 | table CENSUS2010POP, STNAME

STNAME="California" CENSUS2010POP>1000000

Events Patterns Statistics (10) Visualization

all Column Chart / Format 88 Trellis

1 STNAME="California" 2 | stats count

1 STNAME="California"

2 | stats sum(CENSUS2010POP)

√ 59 events (before 4/16/24 1:47:10.00

√ 59 events (before 4/16/24 1:48:50.00)

| table CTYNAME, CENSUS2010POP

above query.

using only the specified column name(s).

in ascending order you would replace "desc" with "asc"].

We can click on the *Visualization* tab to see a chart of the results:

the data. Let's count the results where the state is California:

we want to sort in descending order we would use " | sort -count".

Next, let's compute the total 2010 population for California:

> 7/25/16

source="census.csv" host="

The table shows the results matching this query:

host = florian | source = census.csv | sourcetype = csv

example, we can find the entries where the state is California:

20 Per Page ∨

√ 6,386 events (before 4/16/24 11:54:06.000 AM)

query from different file names, and sourcetype= to query from different formats.

49054,1.6822879116,-11.99012578,-1.182592242,-2.250384934,-18.02016827,1.4419610671

Step 5. Filtering for specific values. We can filter the results by looking for a field with a specific value. For

050,4,8,56,043,Wyoming,Washakie County,8533,8533,8545,8469,8443,8443,8316,8328,12,-76,-26,0,-127,12,26,108,90,95,96,90,34,79,105,77,70,79,-8,2

333018, 11.251924671, 11.456530819, 10.814708003, 9.2864699659, 12.417218543, 9.1199810494, 8.353720389, 9.4929103581, 3.4089573293, -1.773888363, 2.1319, 3.1028104302, 1.3217976448, -0.352650758, -0.354777673, -0.236882625, -0.238677725, -0.240326845, -11.63747502, -0.82781457, -2.01350231, -17.781, -1.63747502, -0.82781457, -2.01350231, -17.781, -1.63747502, -0.82781457, -2.01350231, -1.773888363, -1.7738888363, -1.7738888363, -1.7738888863, -1.7738888863, -1.7738888863, -1.7738888888888, -1.7738888888, -1.77388888888, -1.7738888888, -1.7

This query shows all the data from the census.csv file and whose data type is CSV. In general, we can use source= to

" sourcetype="csv"

No Event Sampling ▼

< Prev 1 2 3 4 5 6 7 8 9 -- Next>

CENSUS2010POP

The field STNAME contains the name of the state, and the above query only shows the results where the state is California. We can use an OR to search for multiple values on the same field:

1 STNAME="California" OR STNAME="Alaska"

We can search multiple fields with specific values by adding them to query. For example, let's search for state name California and 2010 population greater than one million people:

We can filter our results to just show a single column. For example, let's just show the county names of the previous

The | (pipe) is the syntax for sending the results from one query to the next, and the table command creates a table

We can sort the results based on any of the fields, such as population, and order them in either ascending or

descending order. The image below shows an example of a search for all items with a population greater than

100000, sorts the results in descending order, and creates a table containing the population and state name. [To sort

We can view plots of search results by clicking on the *Visualization* tab. For example, if we use our last query and add the 2010 population value to the table:

Instead of using "desc" you can use a dash before the sorting field, e.g. "...| sort -CENSUS2010POP | table ..." for the

Events Patterns Statistics (1)

20 Per Page ▼ ✓ Format Pre

count

59

We can sort based on the count by adding "| sort count" to the above query. This would sort in ascending order. if

Step 6. Perform statistical calculations. The Splunk stats command is used to perform statistical calculations on

Events Patterns Statistics (1)

20 Per Page ▼ Format Pre

sum(CENSUS2010POP) \$

74507912

Finally, let's compute the average 2010 population for California:

1 STNAME="California"
2 | stats mean(CENSUS2010POP)

✓ 59 events (before 4/16/24 1:47:58.000

Events Patterns Statistics (1)

splunk>enterprise Apps ▼

mean(CENSUS2010POP) \$

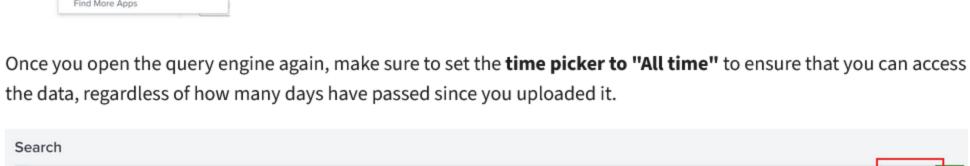
1262845.9661016949

Note: If you close Splunk and want to work with the data later, do not load the data again. Loading the data again

will create a duplicate version, causing all your queries to return doubled results.

the p Splunk Secure Gateway
Upgrade Readiness App
Manage Apps
Find More Apps

To access the data again, open Splunk, click *Apps* in the upper left corner, and select *Search and Reporting*.



Report an issue

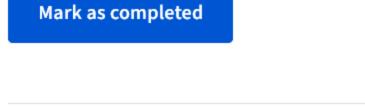
Search

1 enter search here...

No Event Sampling

* Smart Mode

* Smart Mode



√ Dislike

Like