Neeraj Agarwal

Mindtree Ltd

splunk implemetation (Employee data) certification project

**Problem Statement**

Objective: Implement a Splunk project for the Employee details. Under this project, you will have to work with the log files of employee data. Following parts should be covered

1. Log Files Creation

2. Data Inputs

3. Fields Extraction

4. Lookups

5. Alerts

6. Report

7. Dashboard

The following are the fields that are to be added in the log files:

1. Date

2. Time

3. Emp\_ID

4. Emp\_First\_Name

5. Emp\_Last\_Name

6. Emp\_Job\_Title

7. Emp\_Salary

**Abstract**

**This Document includes step by step procedure for monitoring set up of Employee data. This includes**

* **Creating an index**
* **Adding data sets**
* **Adding lookup tables**
* **Creating reports and alerts**
* **Creating dashboards**

Contents

[**Creating an index** 5](#_Toc19268305)

[**Adding data inputs** 6](#_Toc19268306)

[**Basic searches (Fields Extraction)** 7](#_Toc19268307)

[**Lookups** 12](#_Toc19268308)

[**Adding an alert** 15](#_Toc19268309)

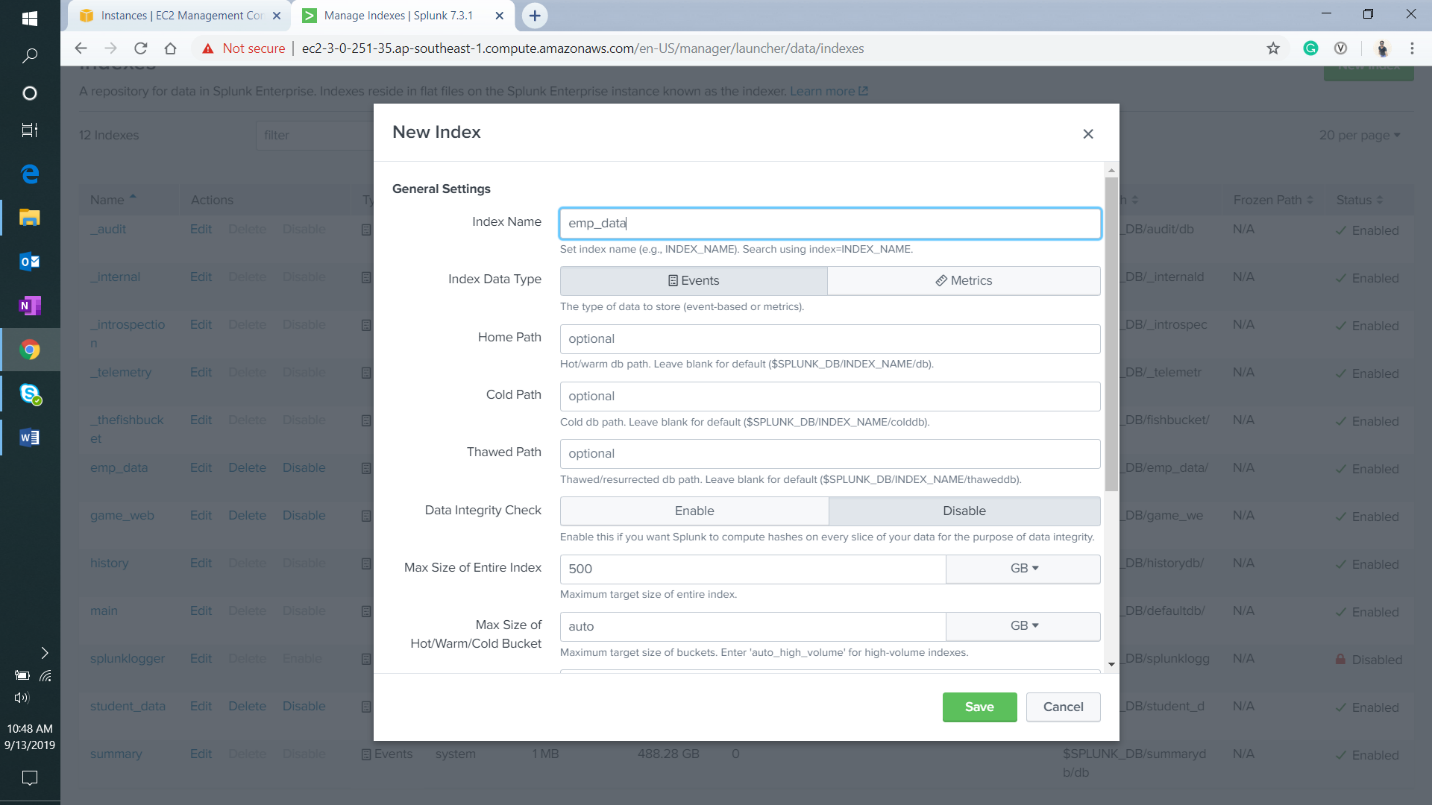
[**Creating Reports** 17](#_Toc19268310)

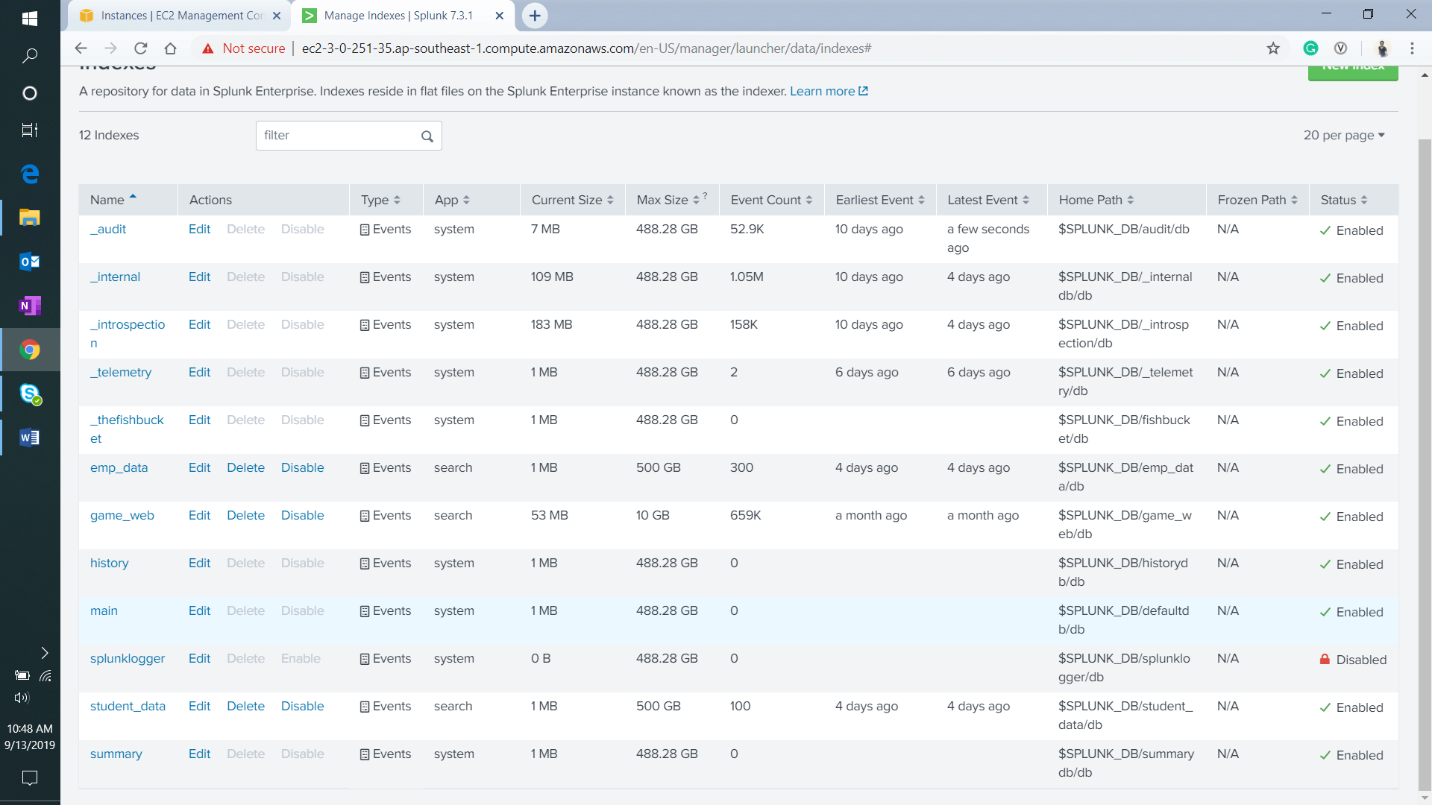
[**Creating A Dashboard** 21](#_Toc19268311)

[**Conclusion** 22](#_Toc19268312)

# **Creating an index**

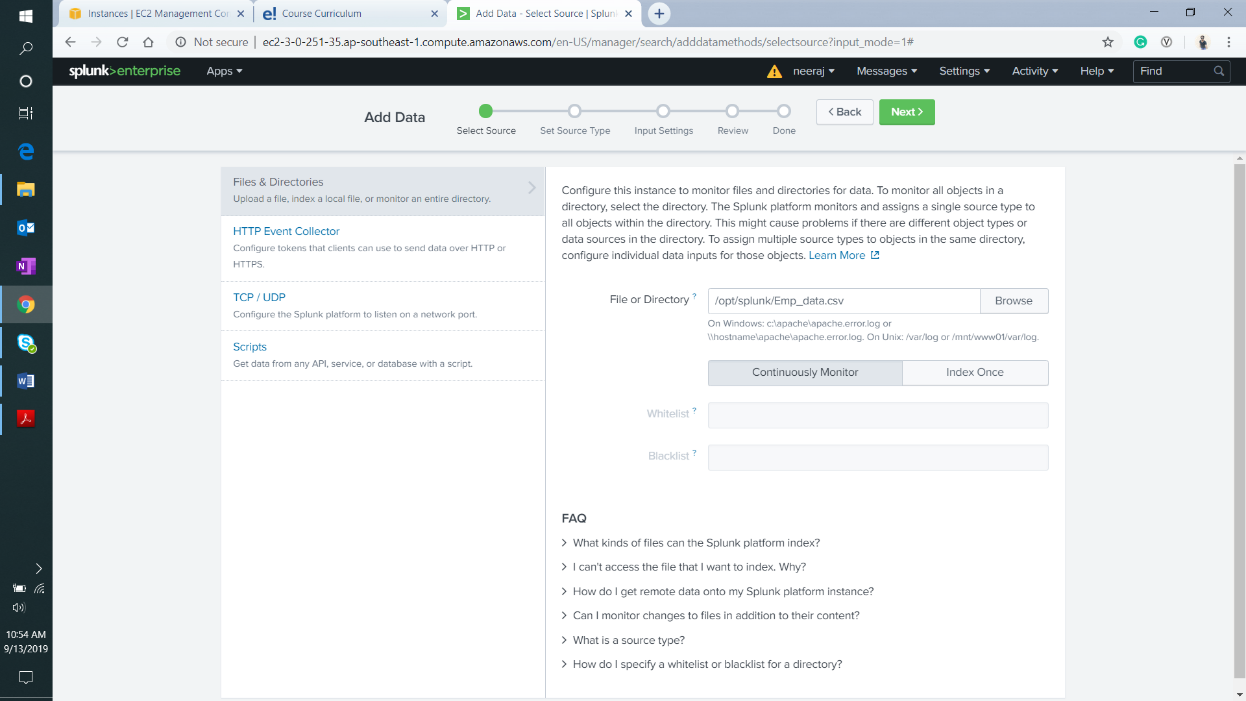
First I have created an index specifically for monitoring the employee data.

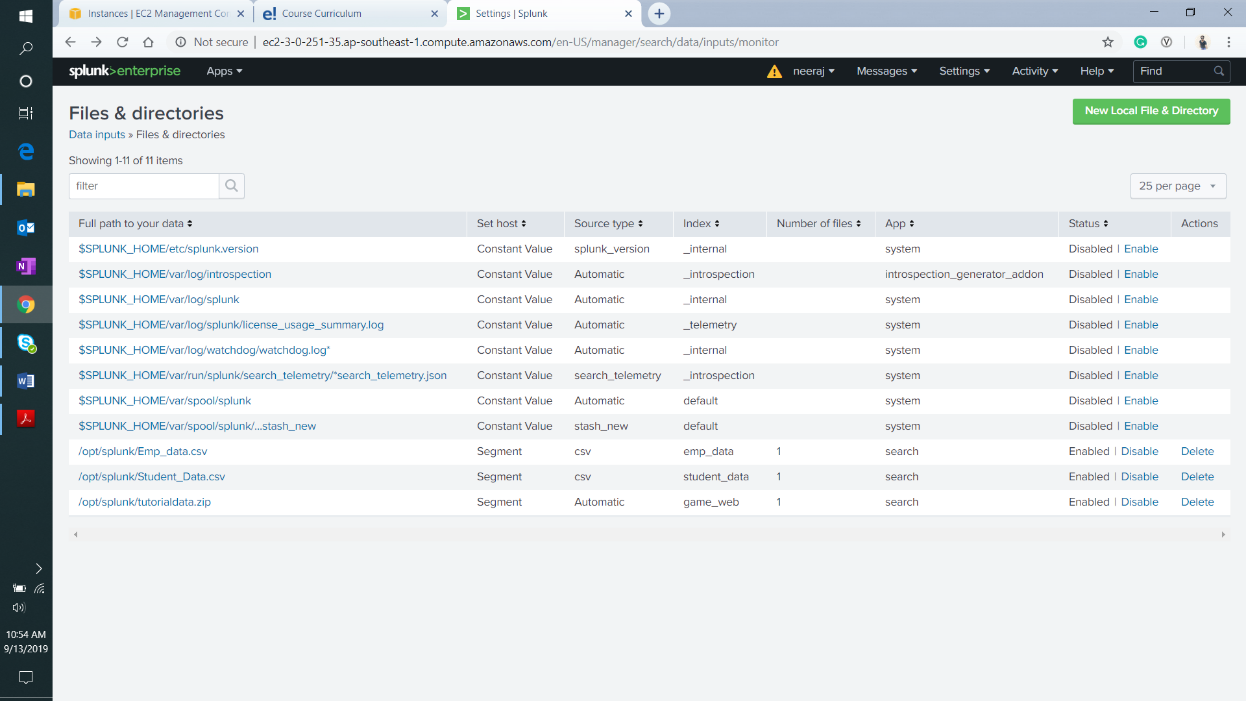




# **Adding data inputs**

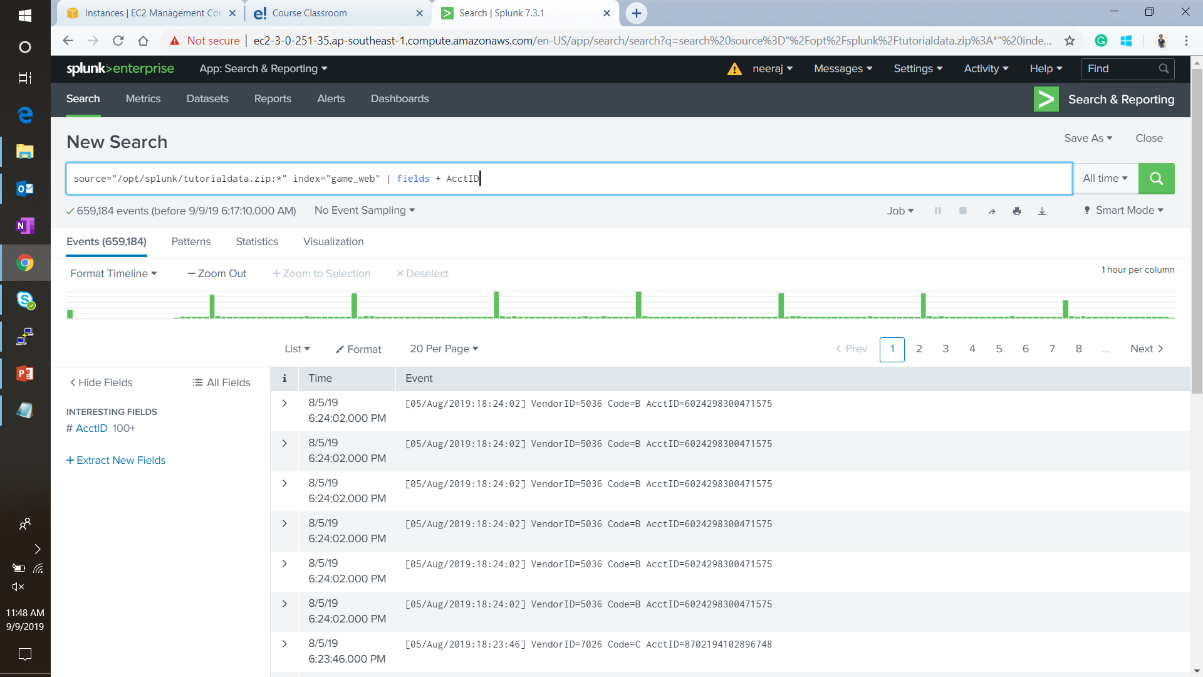
I have created a static csv file which contains details of 100 employees to add as a data set. I will add this file to monitor under the index created previously.





# **Basic searches (Fields Extraction)**

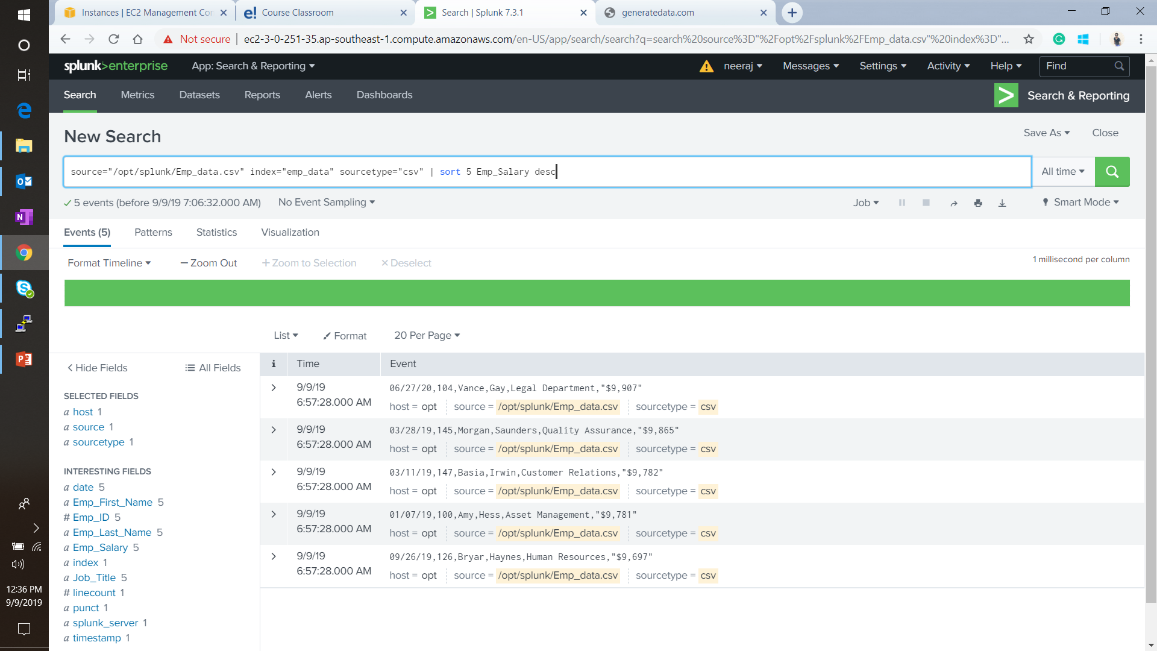
In this section, I have attached a few screenshots of the searches using various fields and commands.



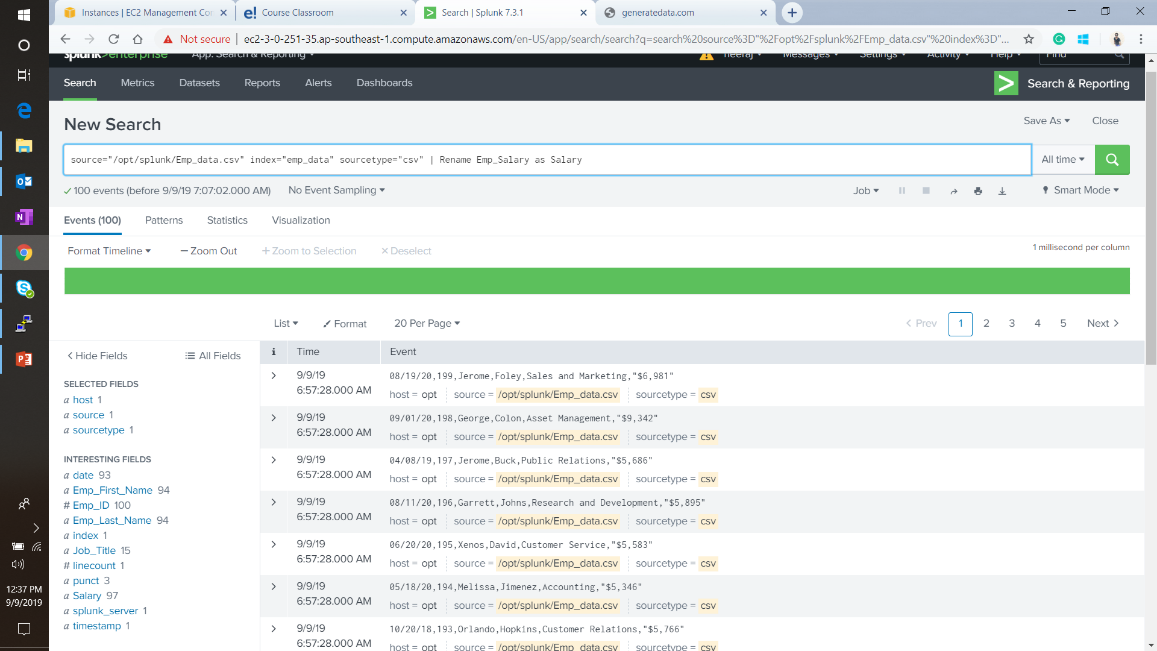
Field Extraction



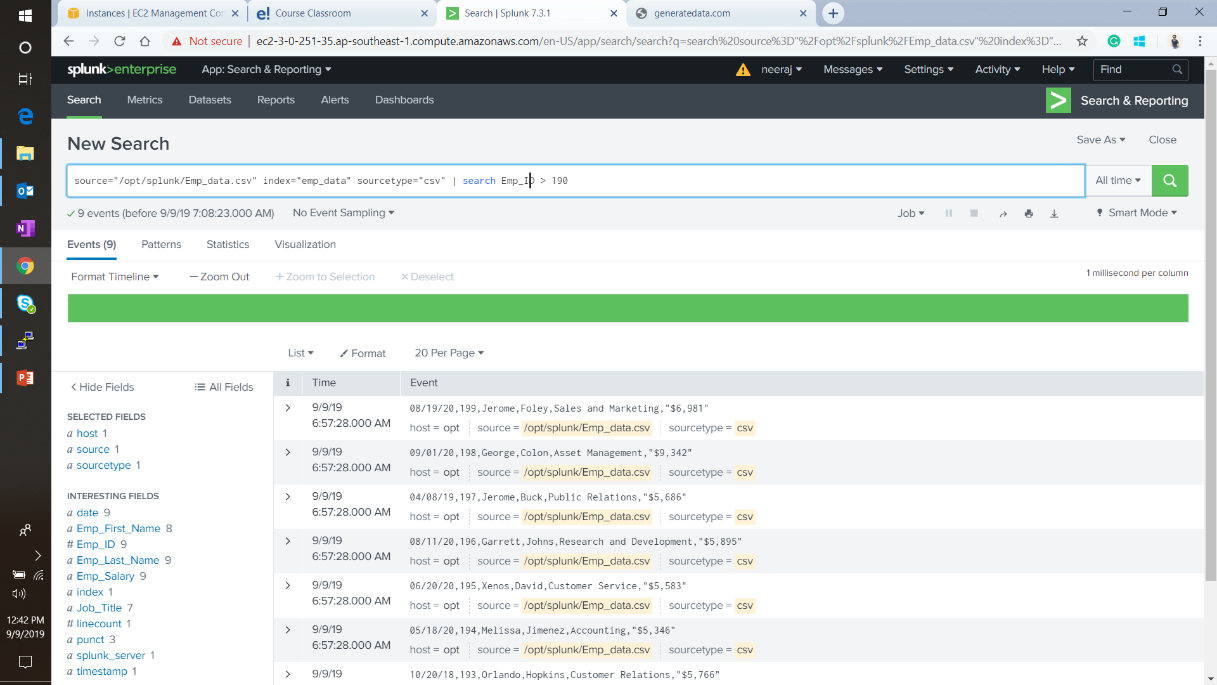
Example of “Table” command



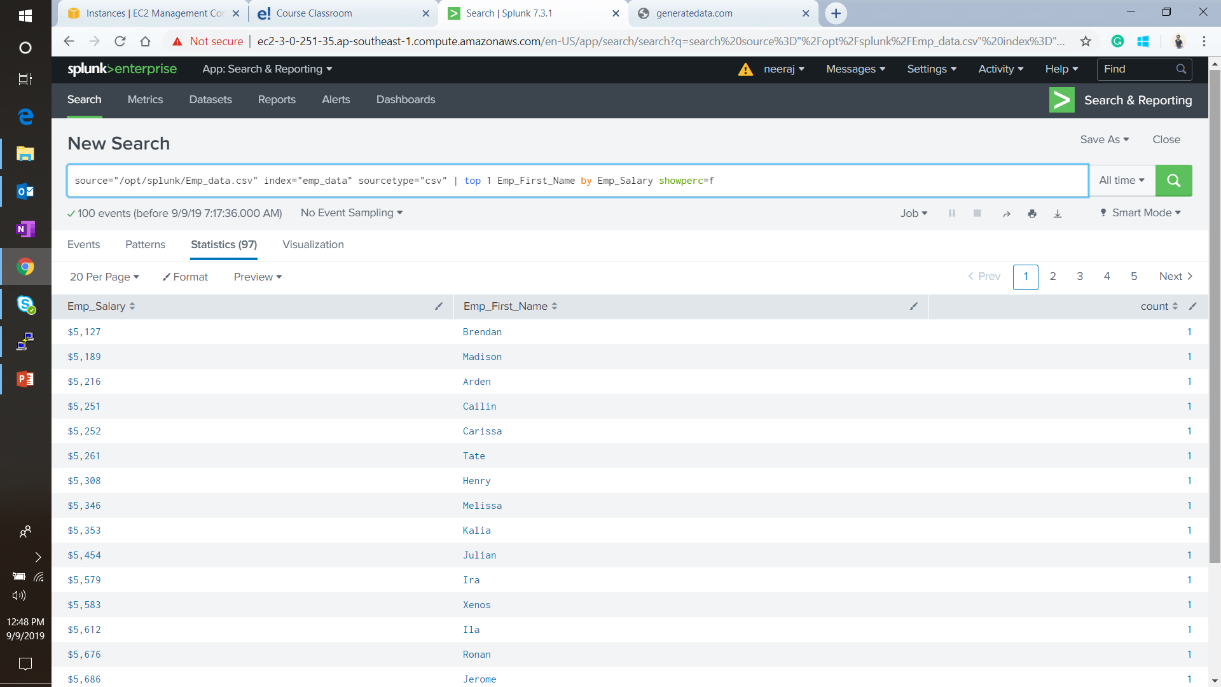
Example of “Sort” command



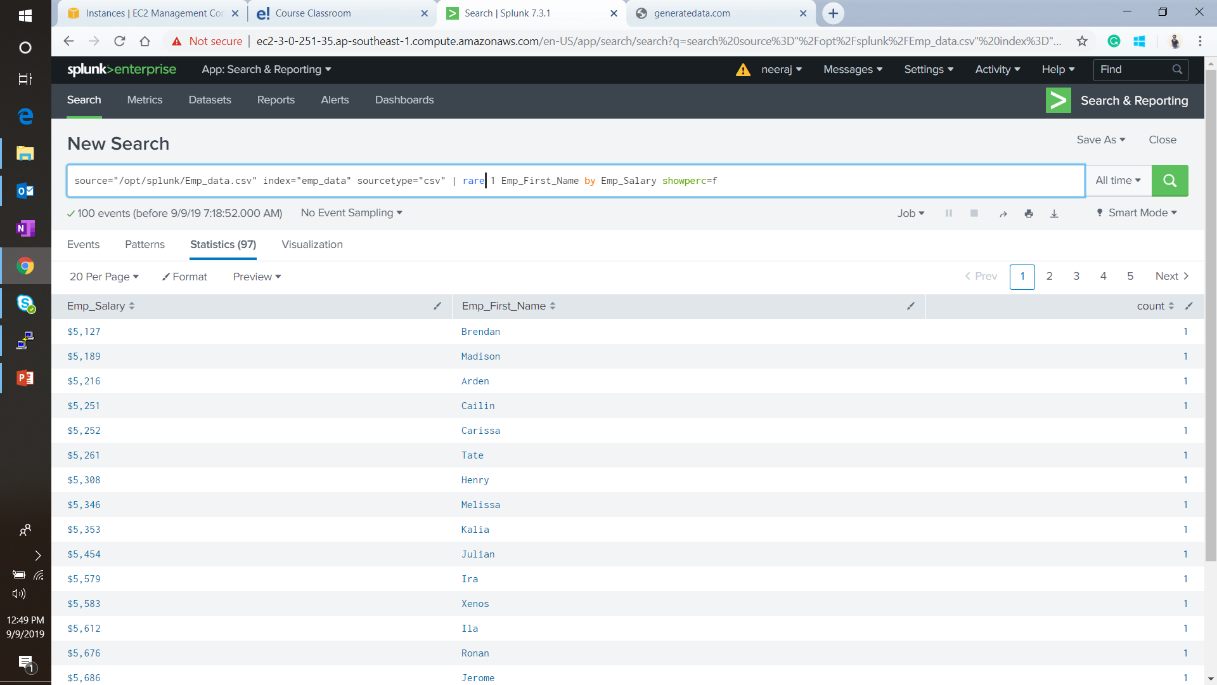
Example of “Rename” command



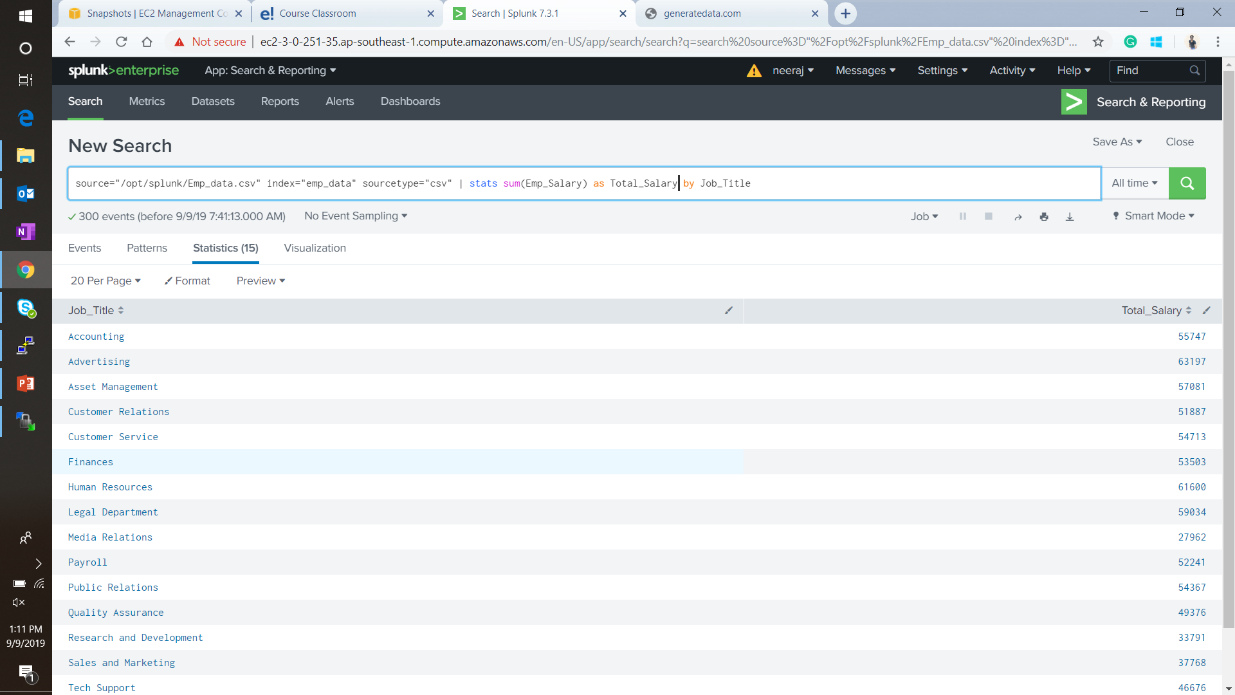
Example of “search” command



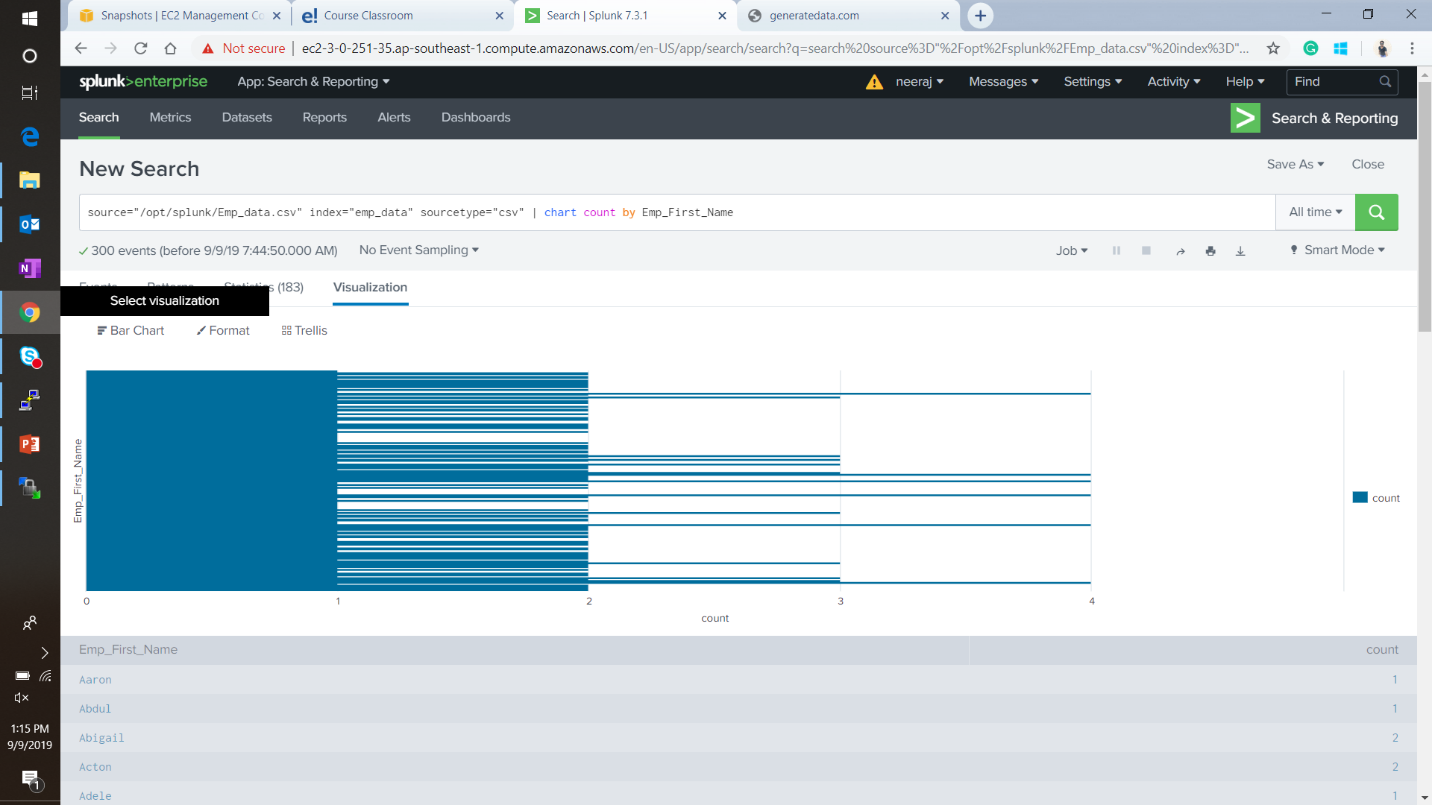
Example of “Top” command



Example of “Rare” command



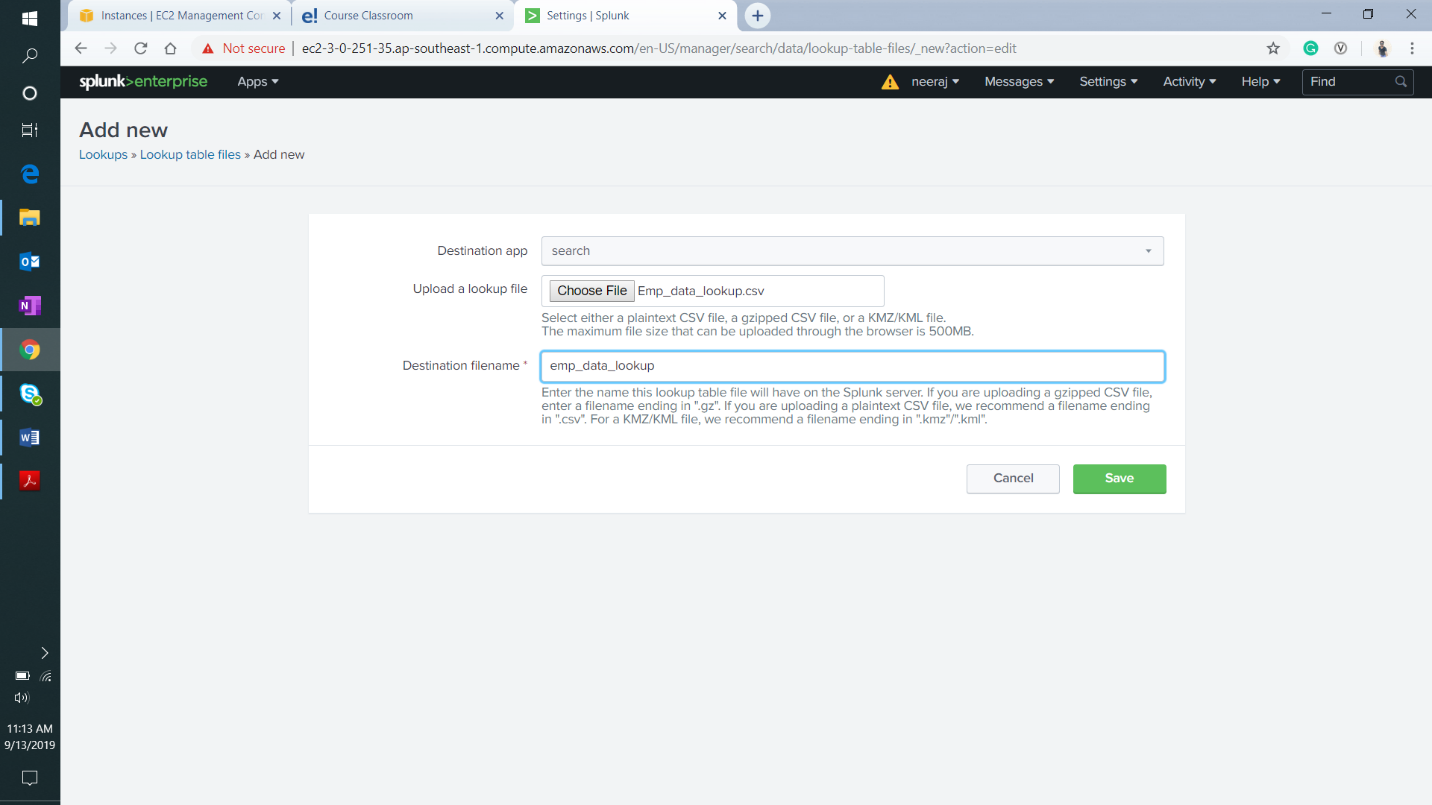
Example of “Stats” command



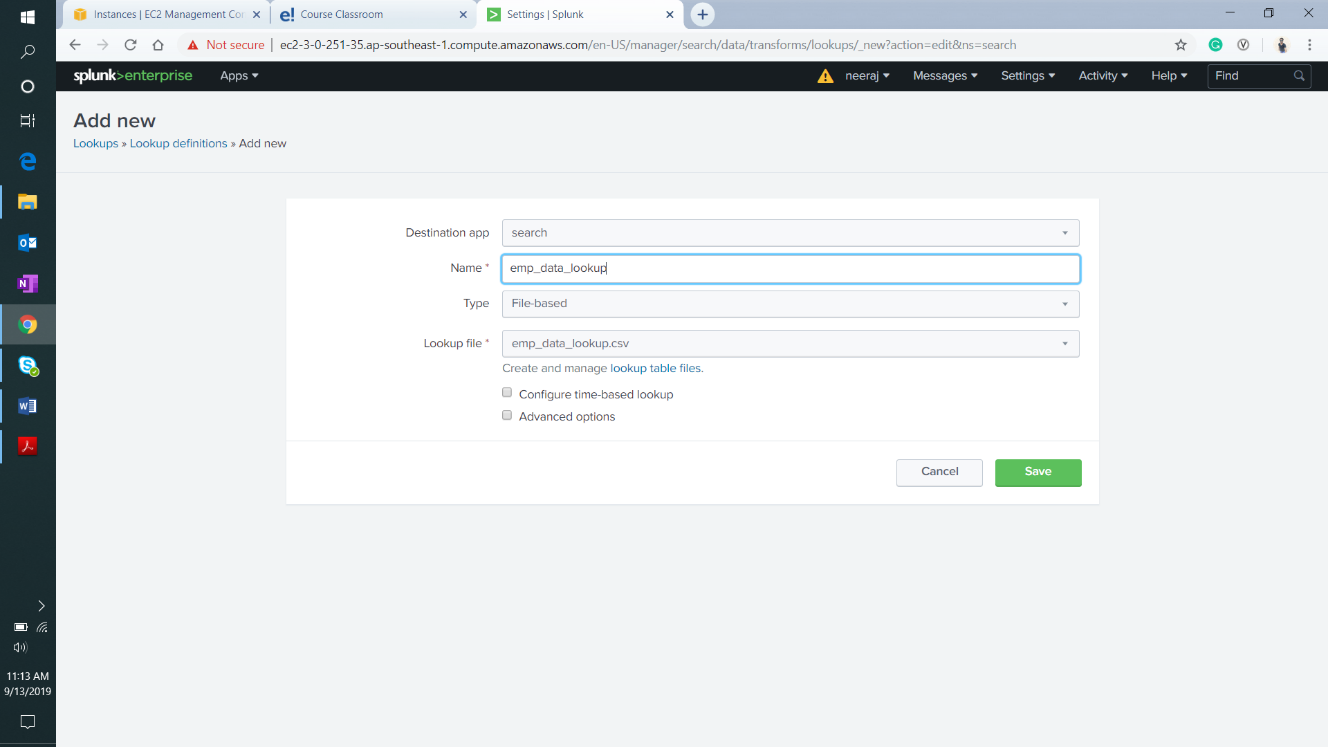
Example of “Chart” command

# **Lookups**

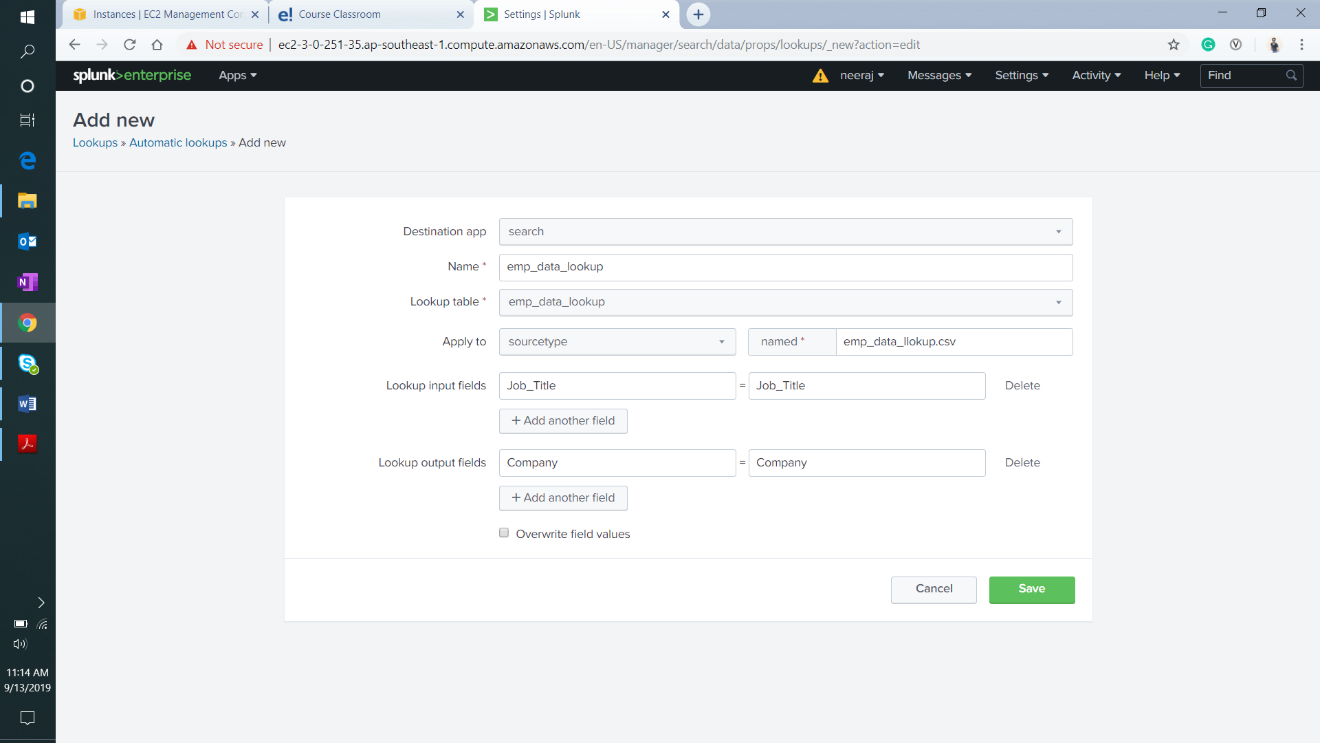
In this section, I will add a lookup table to map the employee’s job title to the company they are associated with. I have created a csv file with above-mentioned data.



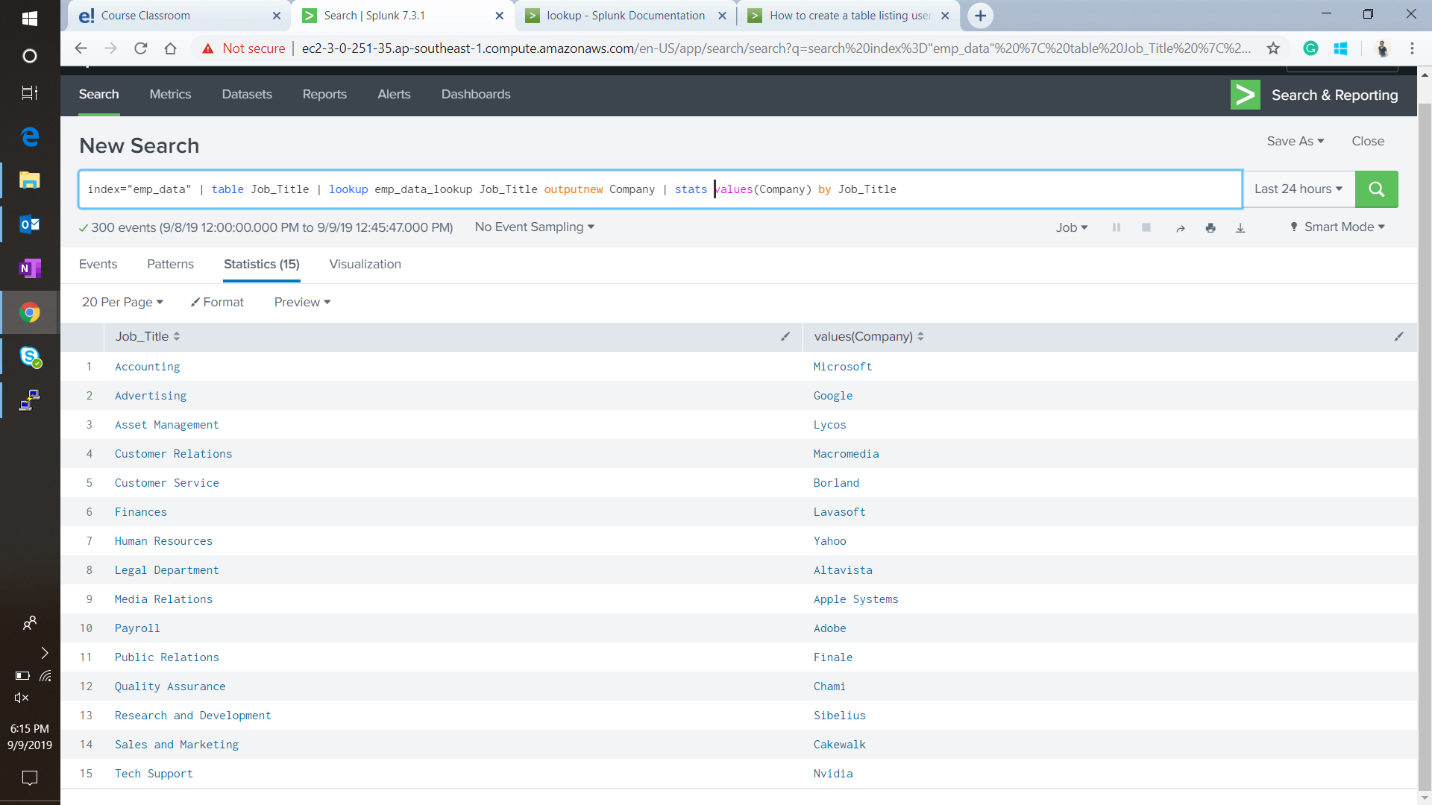
Adding the lookup file



Adding a new lookup definition



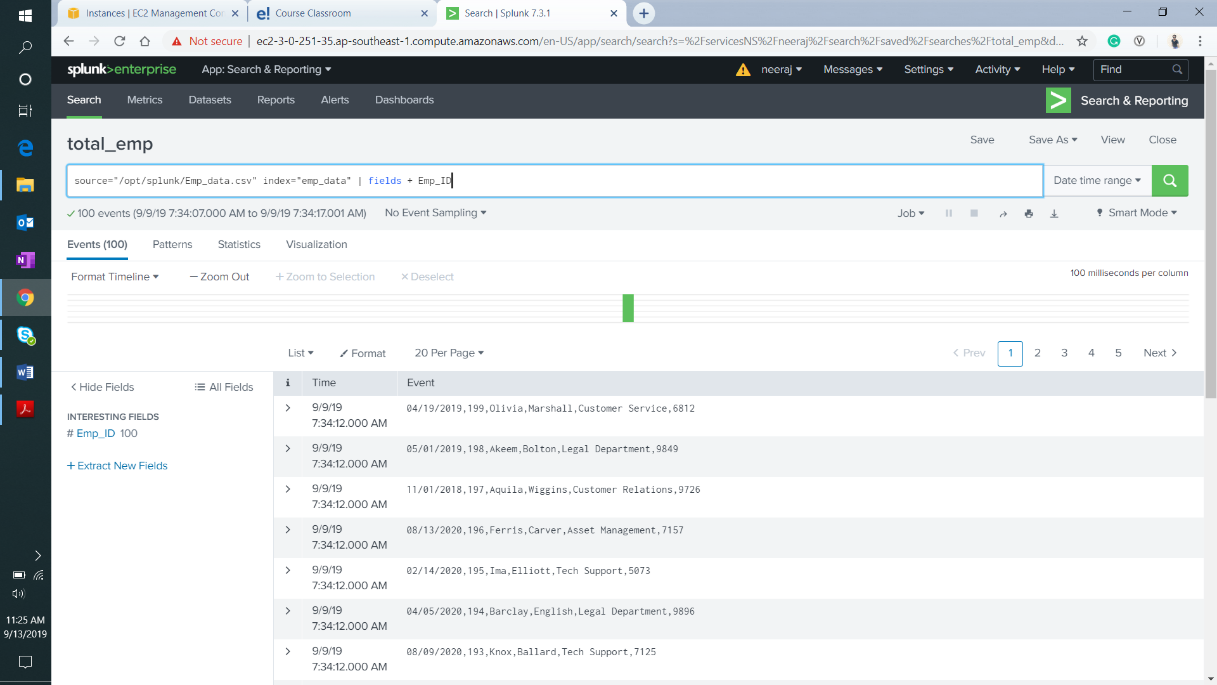
Adding automatic lookup



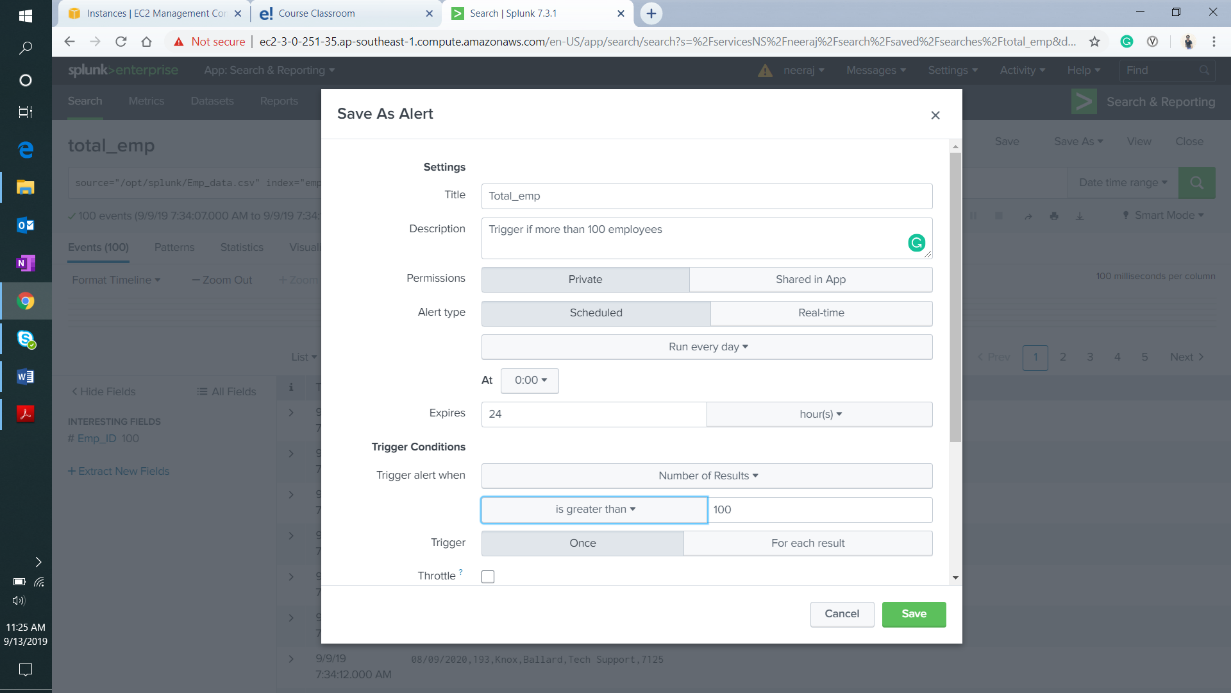
Example of a search which utilizes lookup

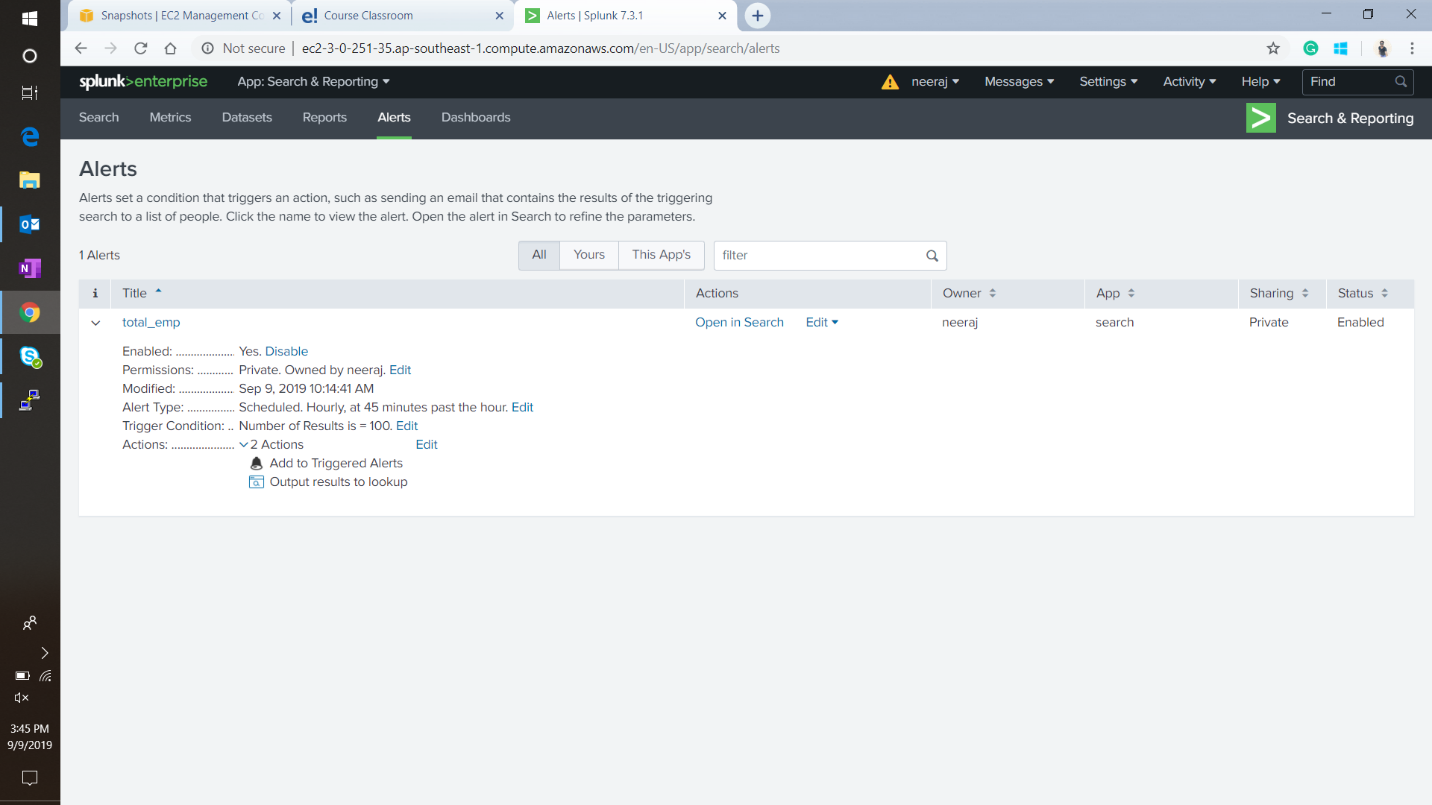
# **Adding an alert**

Here I am configuring an alert where if the search returns showing more than 100 employees in the organization data. This search runs every day at midnight and raises an alert, as well as outputs, result in lookup.



The search string to be configured as alert





The alert configured

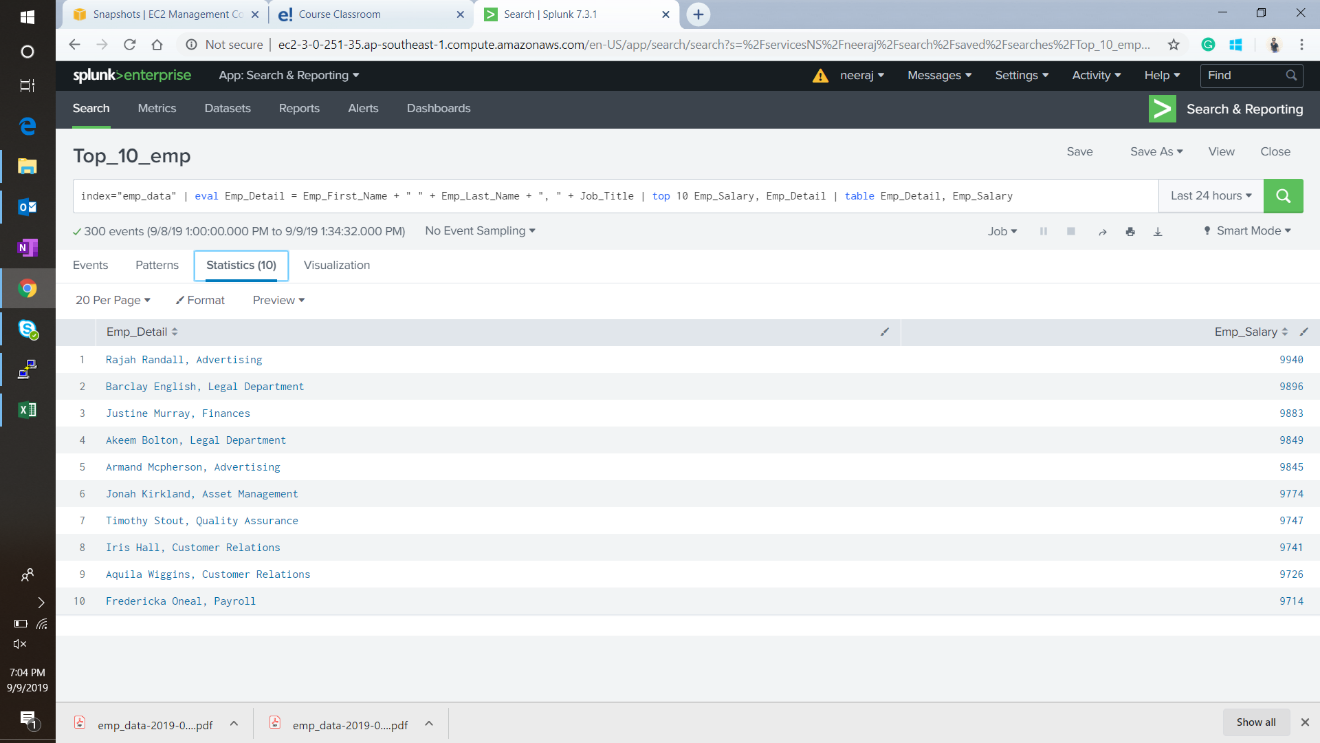
# **Creating Reports**

For this project, I have created four reports which will be used to create a dashboard in the next section. Below is the list of the reports

1. Top 10 earning employees

Search string :

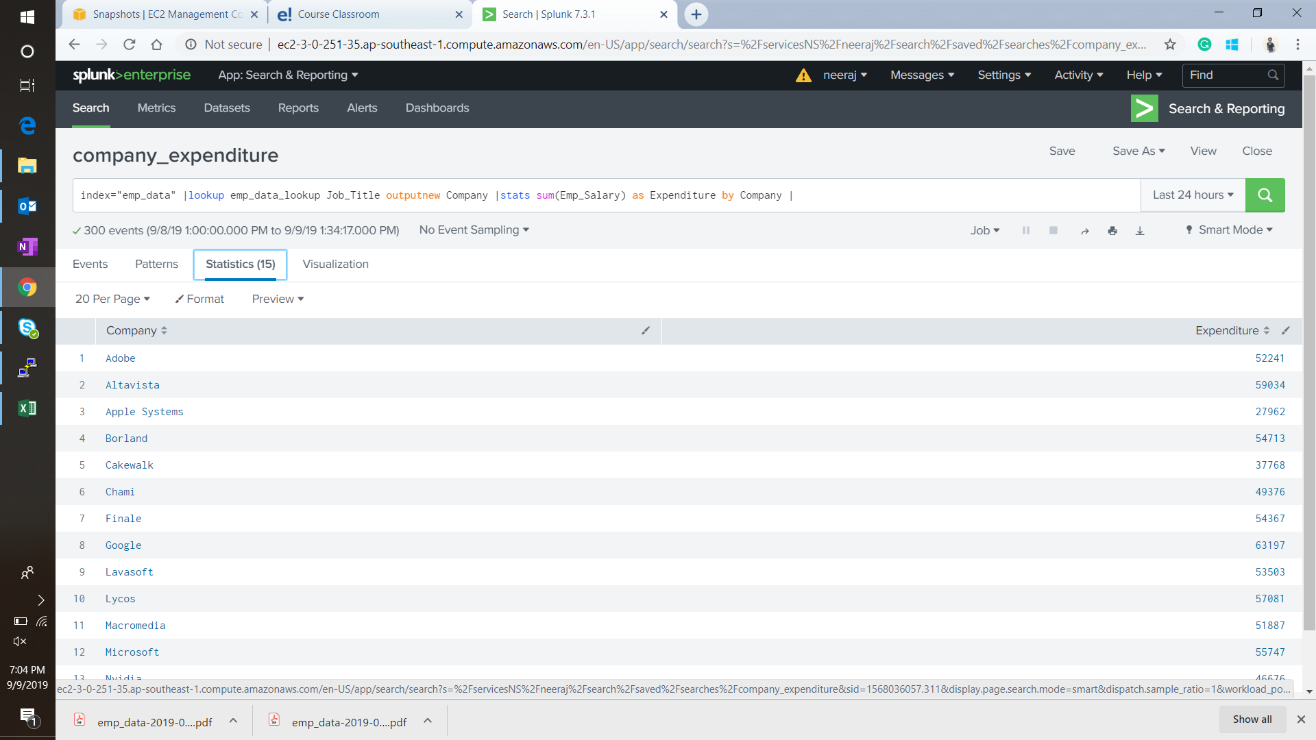
index="emp\_data" | eval Emp\_Detail = Emp\_First\_Name + " " + Emp\_Last\_Name + ", " + Job\_Title | top 10 Emp\_Salary, Emp\_Detail | table Emp\_Detail, Emp\_Salary



1. Expenditure of each company in employee salaries

Search string :

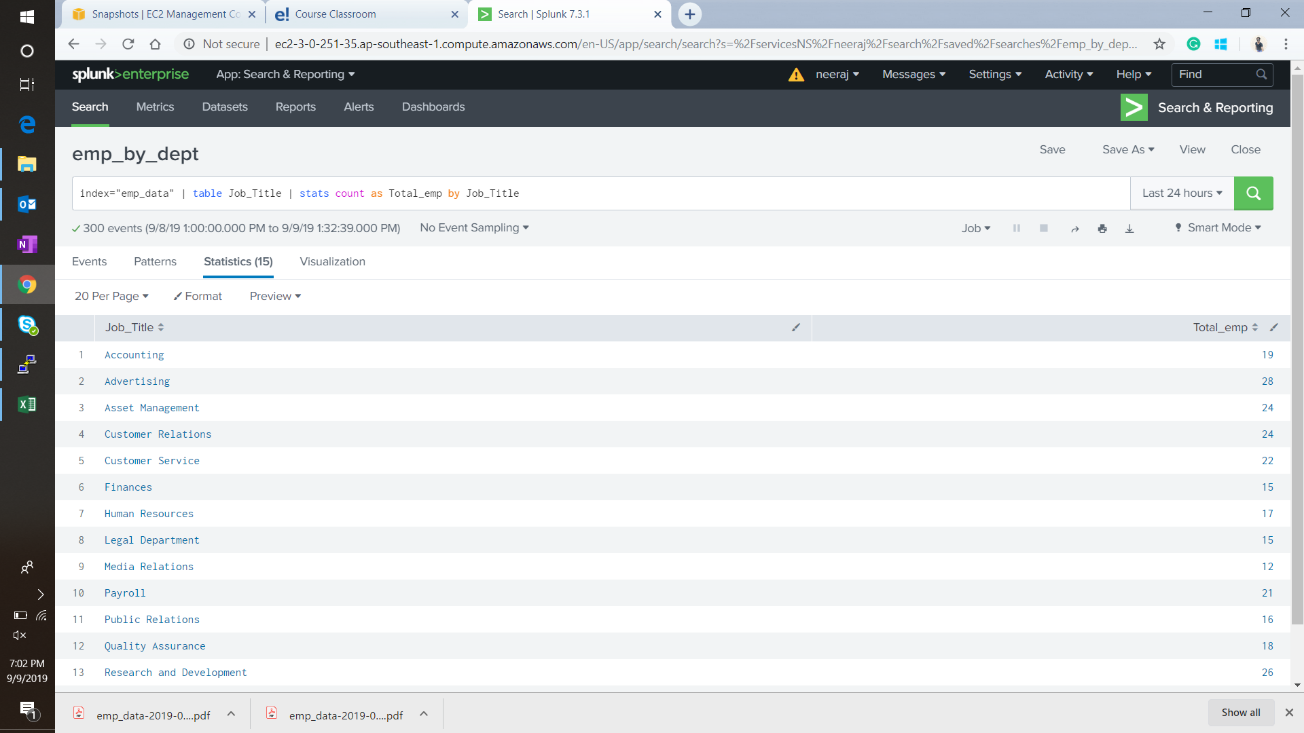
index="emp\_data" |lookup emp\_data\_lookup Job\_Title outputnew Company |stats sum(Emp\_Salary) as Expenditure by Company



1. Total employees in each department

Search string :

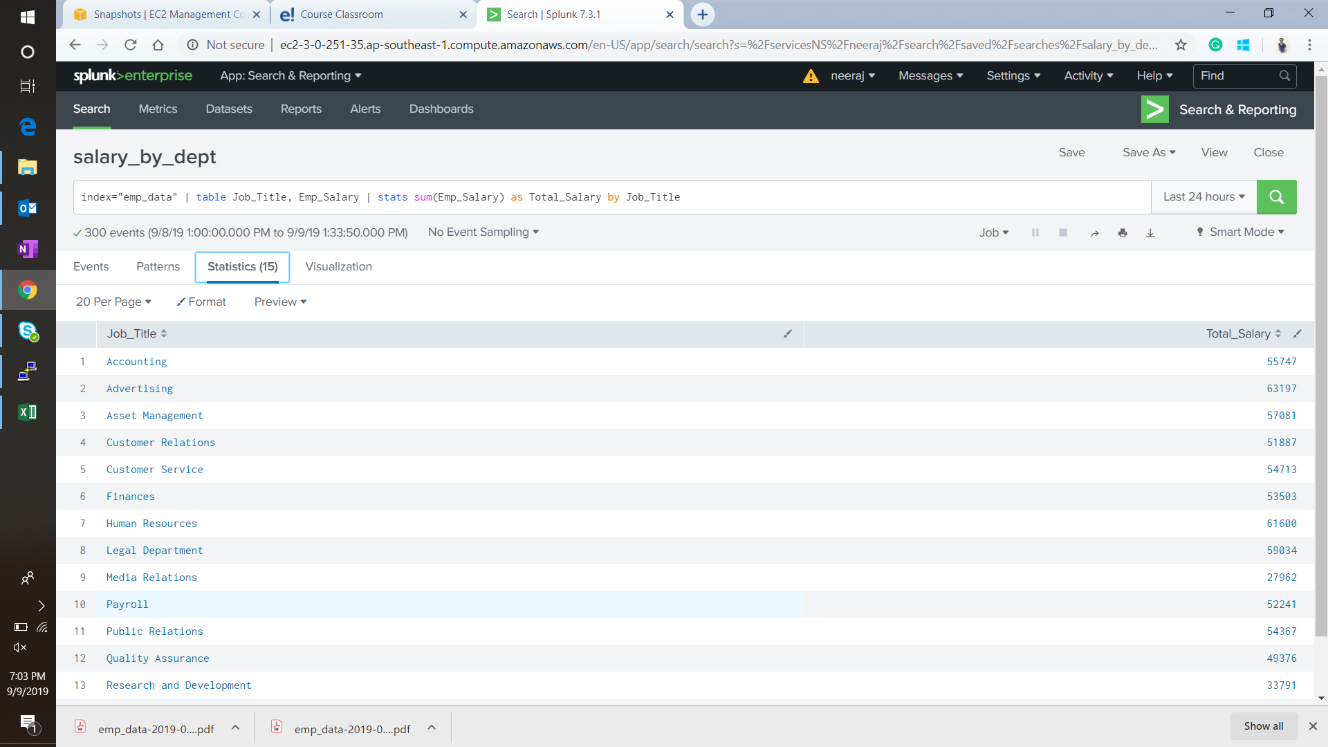
index="emp\_data" | table Job\_Title | stats count as Total\_emp by Job\_Title



1. Total salary spent in each department

Search String :

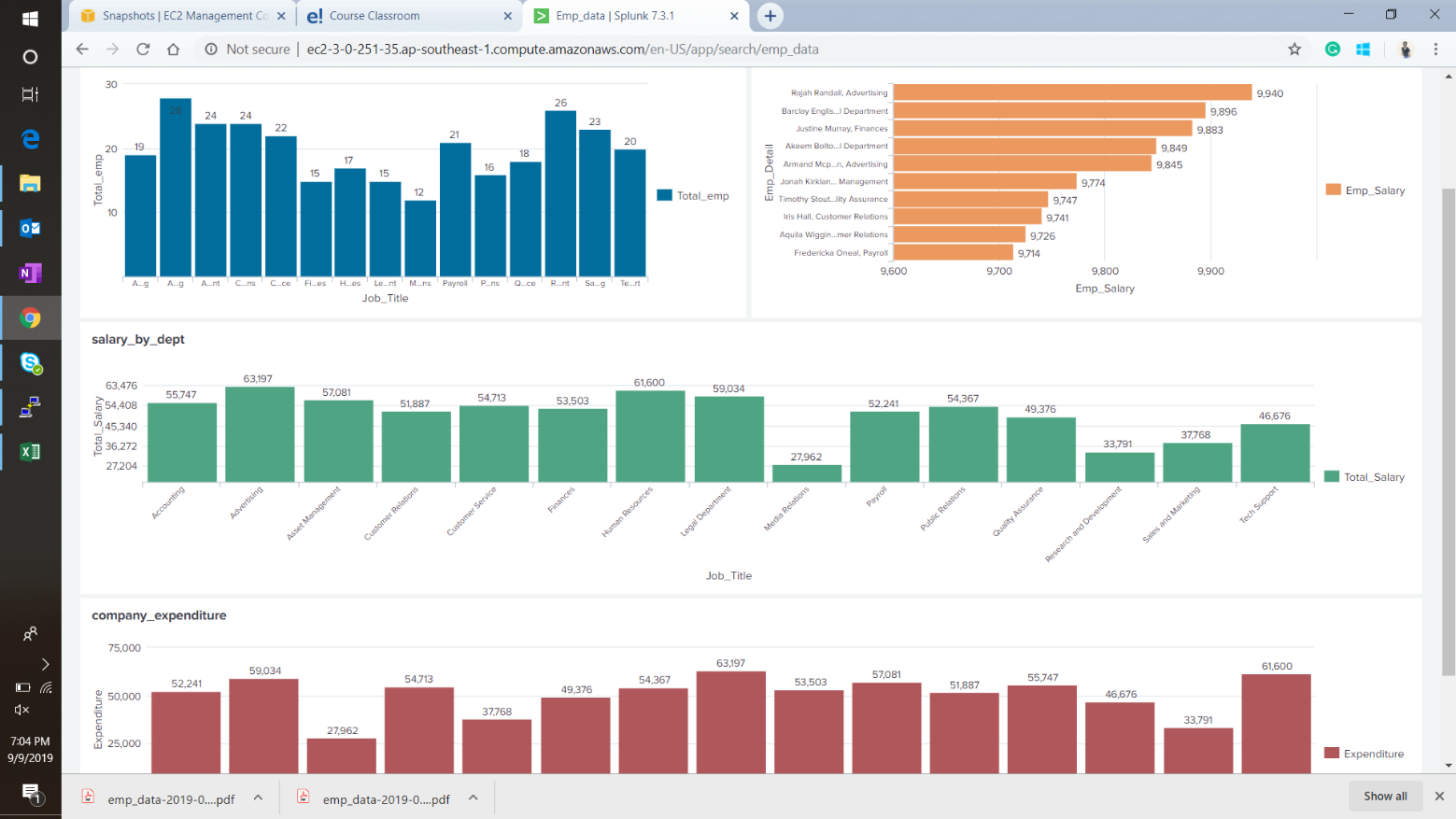
index="emp\_data" | table Job\_Title, Emp\_Salary | stats sum(Emp\_Salary) as Total\_Salary by Job\_Title



# **Creating A Dashboard**

Using the reports mentioned in the previous section I will create a simple dashboard consisting of bar charts to visualize the results of these searches instead of just a tabular form. I do this by creating a blank dashboard and selecting **add panel 🡪 new from reports**.

This is what we get after adding all 4 reports.



We can export it as pdf and share with other users as well.

# **Conclusion**

This concludes the technical documentation for the solution to the project statement given.

As required I have,

* Created a data file with all the required data
* Created an index and added data to it
* Performed various searches
* Added lookup table
* Configured alert
* Created reports
* Created Dashboard

All the required files including the original data file will be present along with this document of reference.