Question 1 (20 points): How many events are in ‘access.log’ and in ‘error.log’, respectively? How many events are in 'access.log' and in 'error.log' on April 2nd, 2017, respectively? You should explicitly provide the answer, then include one or several screenshot images showing where in Splunk software you get these numbers.

There are 41,483 events in access.log

There are 15,936 events in error.log



For 04/02/2017,

There are 52 events in access.log

There are 15,936 events in error.log

Graphical user interface, text, application

Description automatically generated

Question 2 (20 points): How many events happened between 04/01/2017 22:00:00 to 04/01/2017 23:00:00 (Note that the time referred here is the event log raw data time, it may or may not match with Splunk interpreted time)? Please also show the pie chart graph, and the statistics of the ‘status’ field for this time range events. You need to use screenshot image to show the pie chart graph and the statistics of the status field. (Note: the pie chart graph is about 'Top values', not 'Top values by time'. I have explained their differences in class)

Pie chart (top values):

Graphical user interface, application

Description automatically generated

Statistics of status field:

Background pattern

Description automatically generated

Question 3.

There are two versions of Mozilla from the log file. 4.0 and 5.0

The count of them is shown below.

A screenshot of a computer screen

Description automatically generated

Question 4 (30 points): In class I have demonstrated how to show geolocation graph based on client IP addresses, and how to add generated graph to dashboard. In this question, you are required to:

Show the search term you used to obtain the geolocation graph based on clientip field extracted by Splunk on the entire data log zip file (on ‘all time’ time range). The geostats command should be used with ‘count by method’ setting.

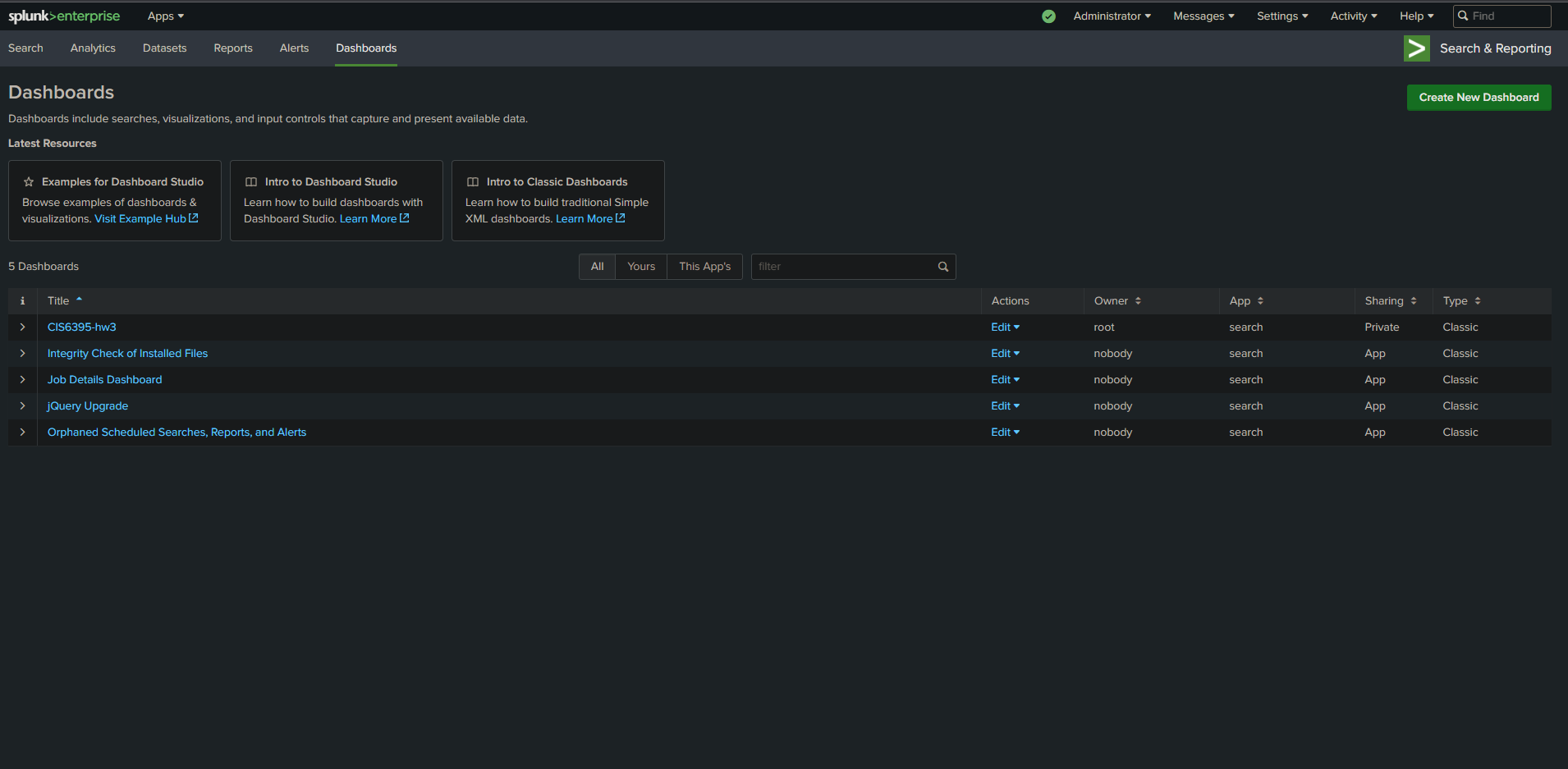
source="apache2.zip:\*" host="cis-6395hw3" | iplocation clientip | geostats count by method

Show the screenshot image of the generated ‘Cluster map’ of the geolocation graph.

A computer screen capture

Description automatically generated with medium confidence

Add this geolocation graph into a newly created dashboard titled ‘CIS6395-hw3’, with the panel title ‘client IP geolocation’. Show the screenshot image of the created dashboard, including the dashboard title and the panel title.



A screenshot of a map

Description automatically generated with medium confidence