**Practical Activity 9**

**Splunk-Enterprise SIEM Tool**



**Name**: Lamis Mohamed GabAllah

**Email**: [lamis.mohammed@womentechsters.org](mailto:lamis.mohammed@womentechsters.org)

**Date**: 1st August 2021

**Practical Task week 8 – Hands on experience with Splunk-Enterprise SIEM Tool**

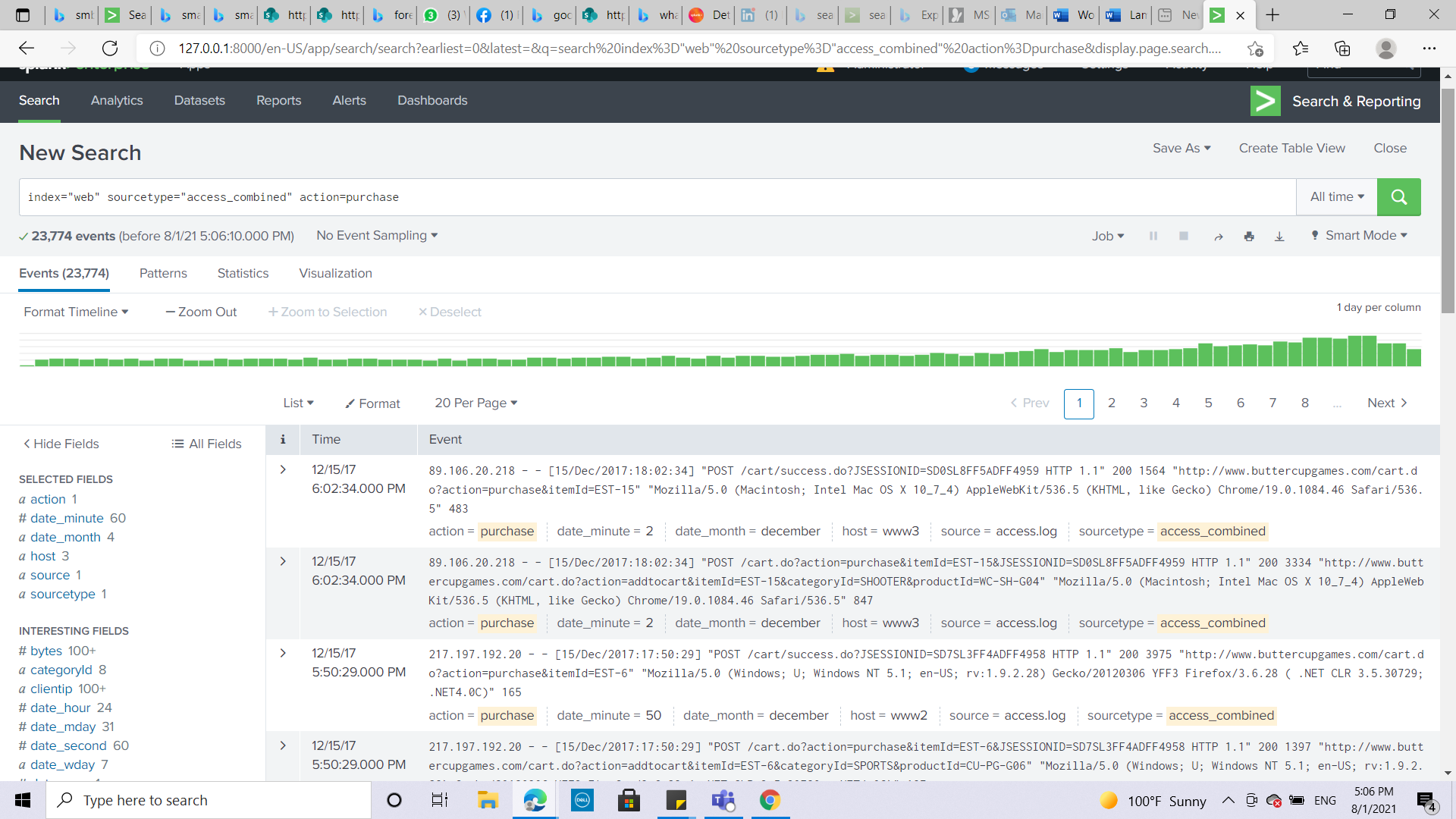
* The practical Activity will be based on Filtering Results and Manipulating of Data with eval, search and where commands of the dataset given.

**NB:** Please do not utilize any other dataset.

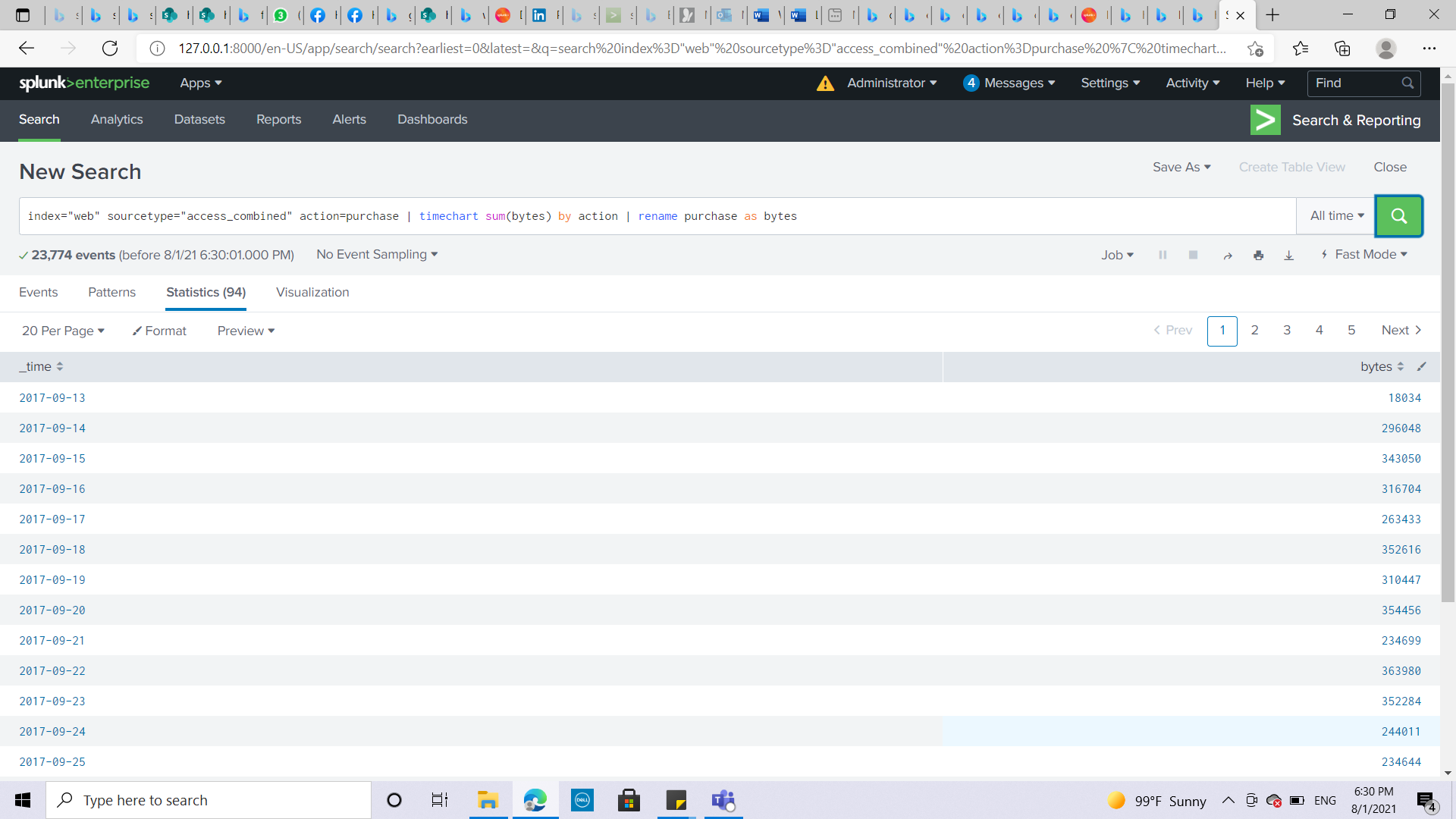
* The dataset is based on different web logs from linux server and Cisco WSA so before you start working on the task make sure you have Splunk Add-on for Unix and Linux and Splunk Add-on for Cisco WSA

**Task 1: Chart the total daily volume (in MB) of the web servers based on each week.**

1. Search online purchases [access\_combined] and answer with the query you have used.

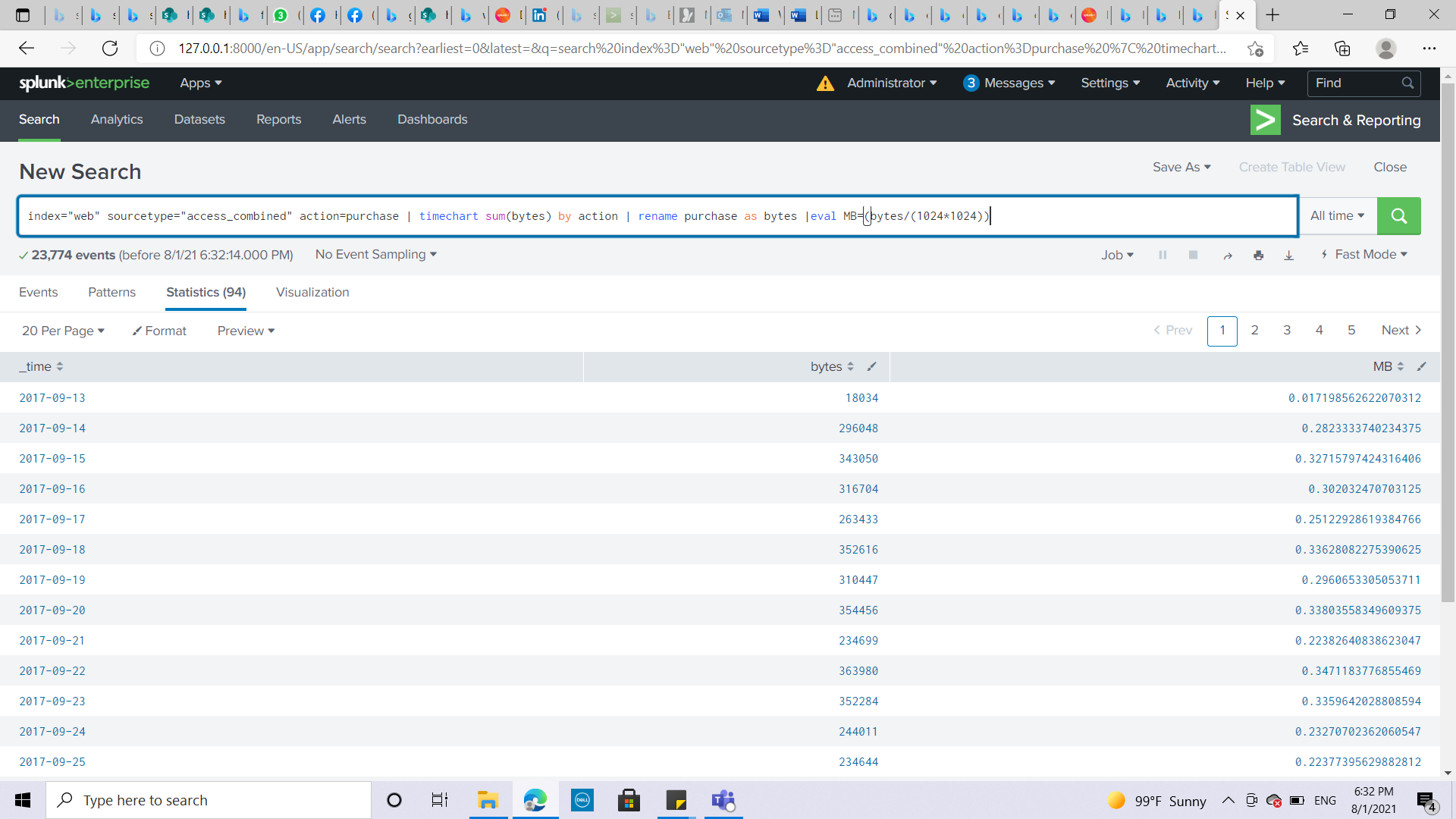


1. Use timechart to calculate the total bytes and name the field: bytes



1. Use eval to convert the bytes field to megabytes.

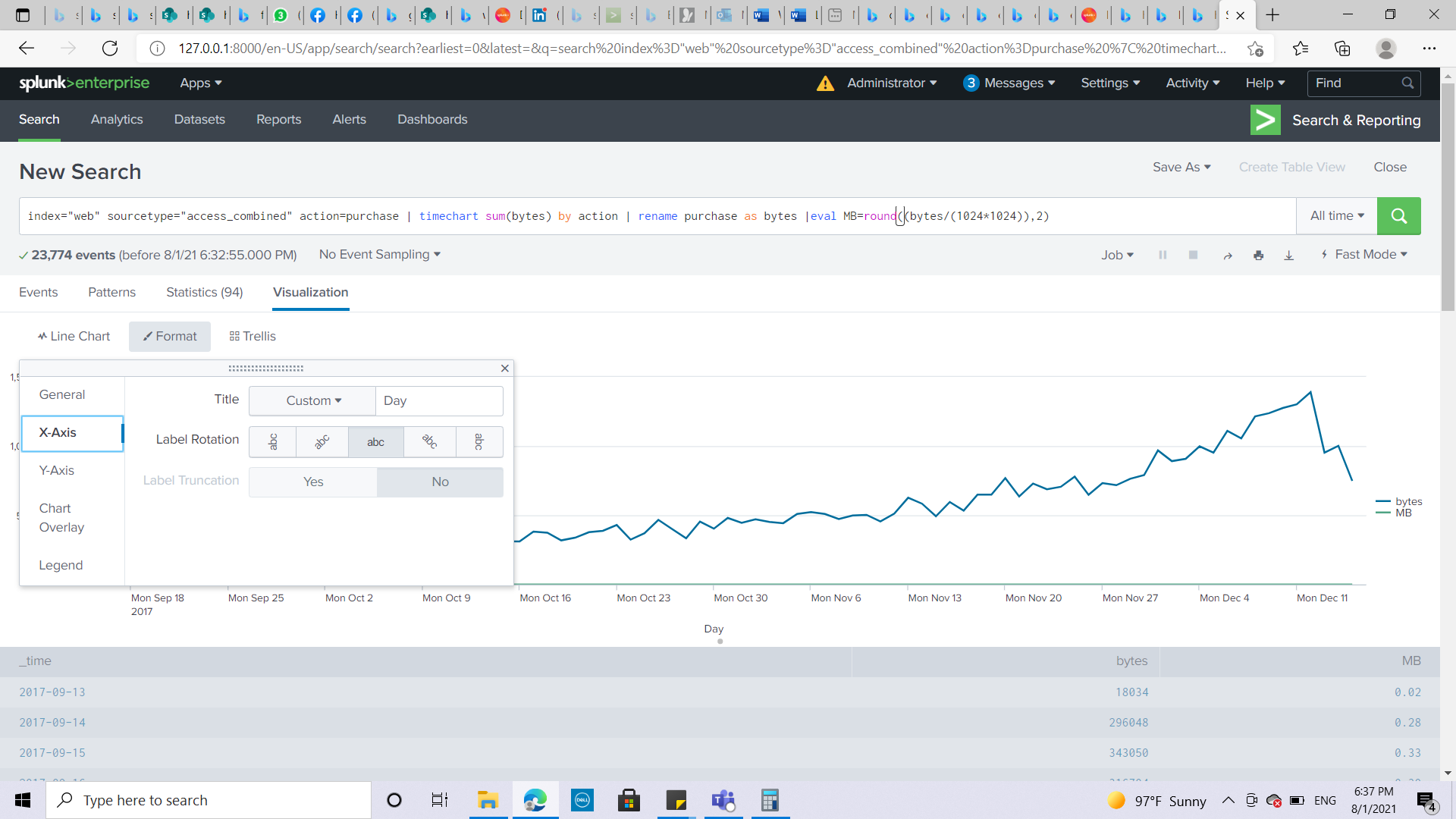
Hint: megabytes=bytes/(1024\*1024)



1. Use the round function to round the megabytes field values to two decimal places.

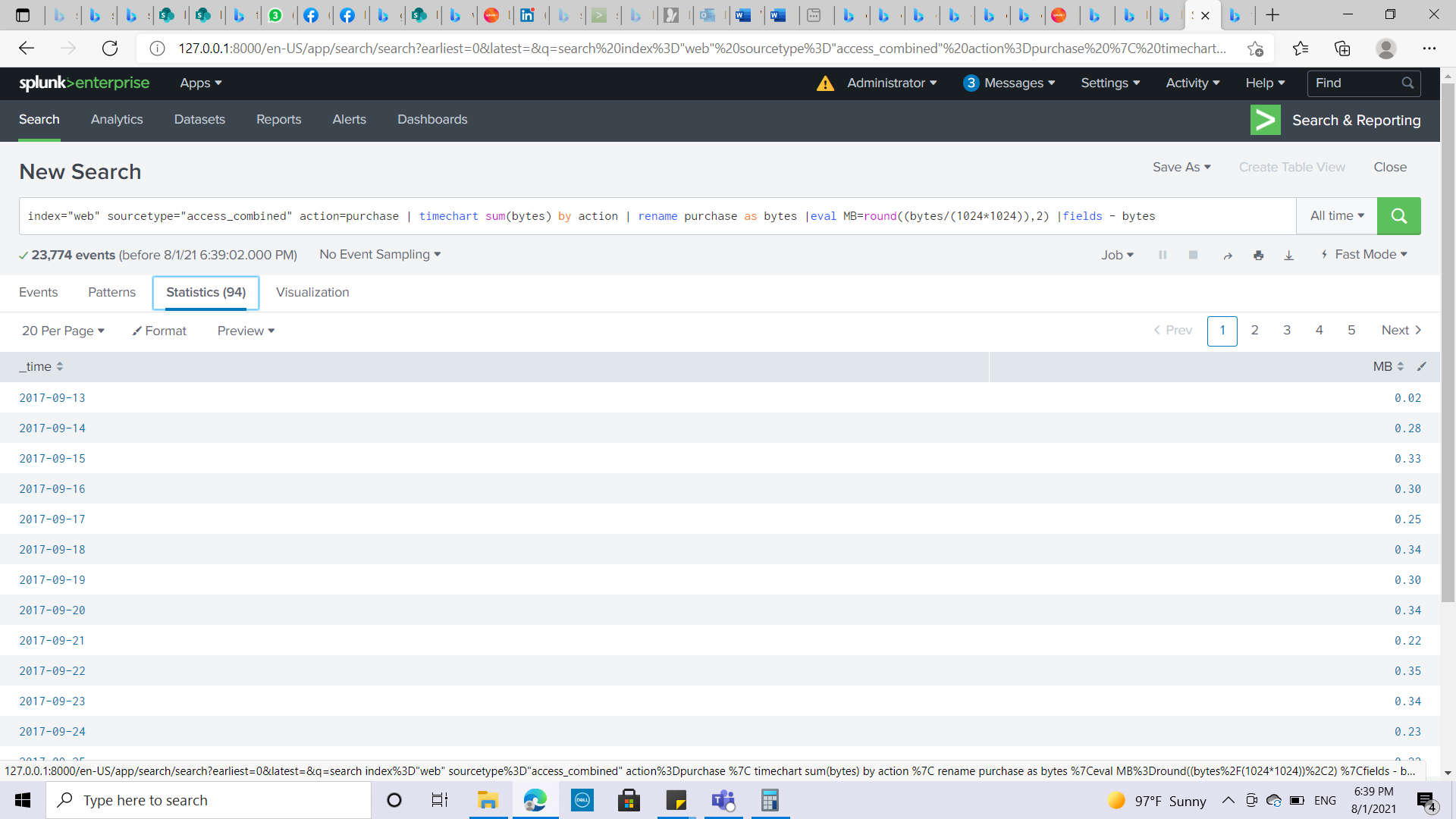


1. Switch to the Visualization tab and display the data as a Line Chart. Set the X-axis label to Day. Notice that the bytes field still displays.

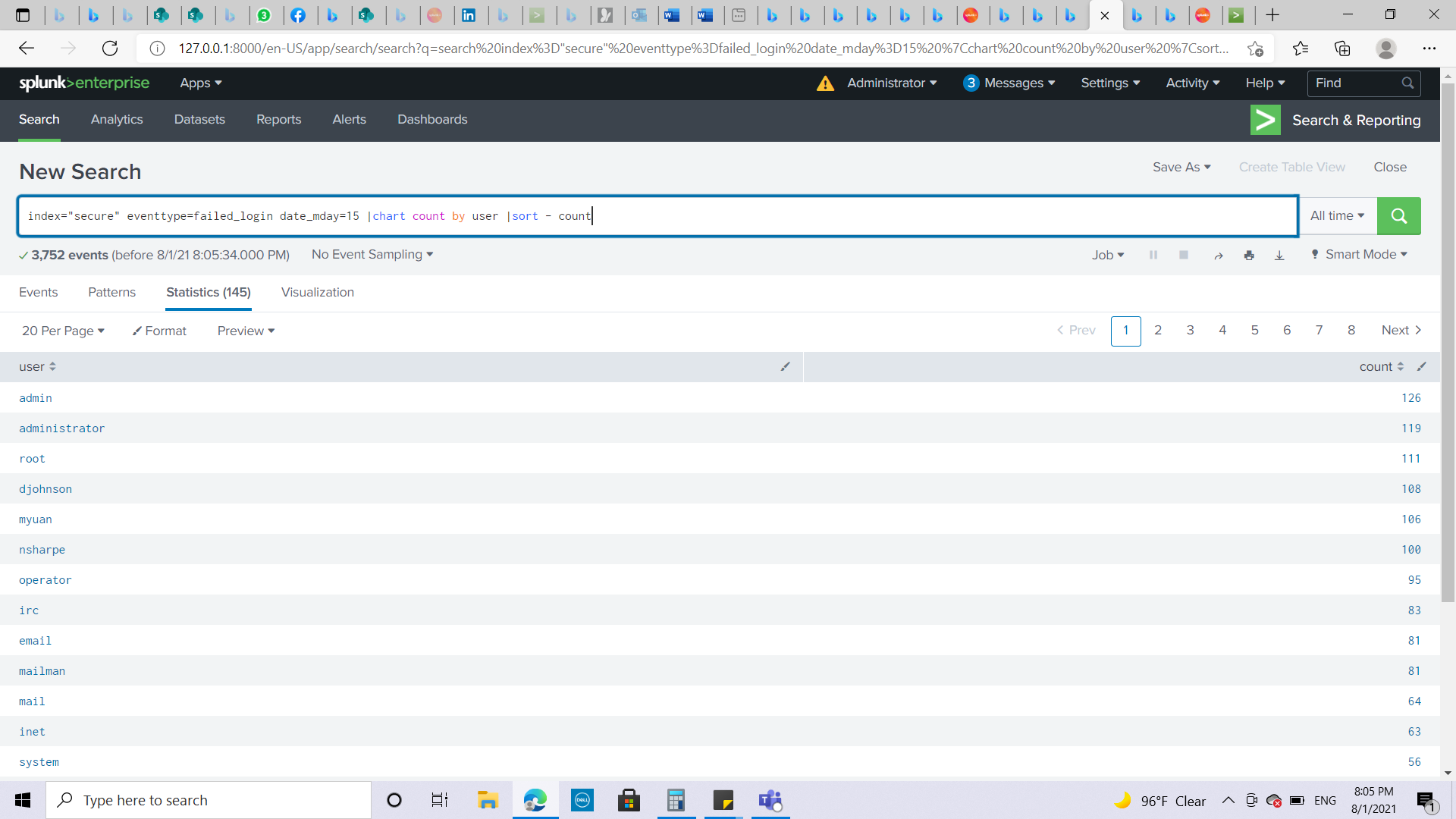


1. Use the fields command to remove the bytes field.





**Task 2: Identify users with more than 3 failed logins** on 15th Dec 2017 and sort in descending order. Or since our dataset is from December 2017 just display the highest failed login ins on 15th December 2017. And well sorted out in descending order.



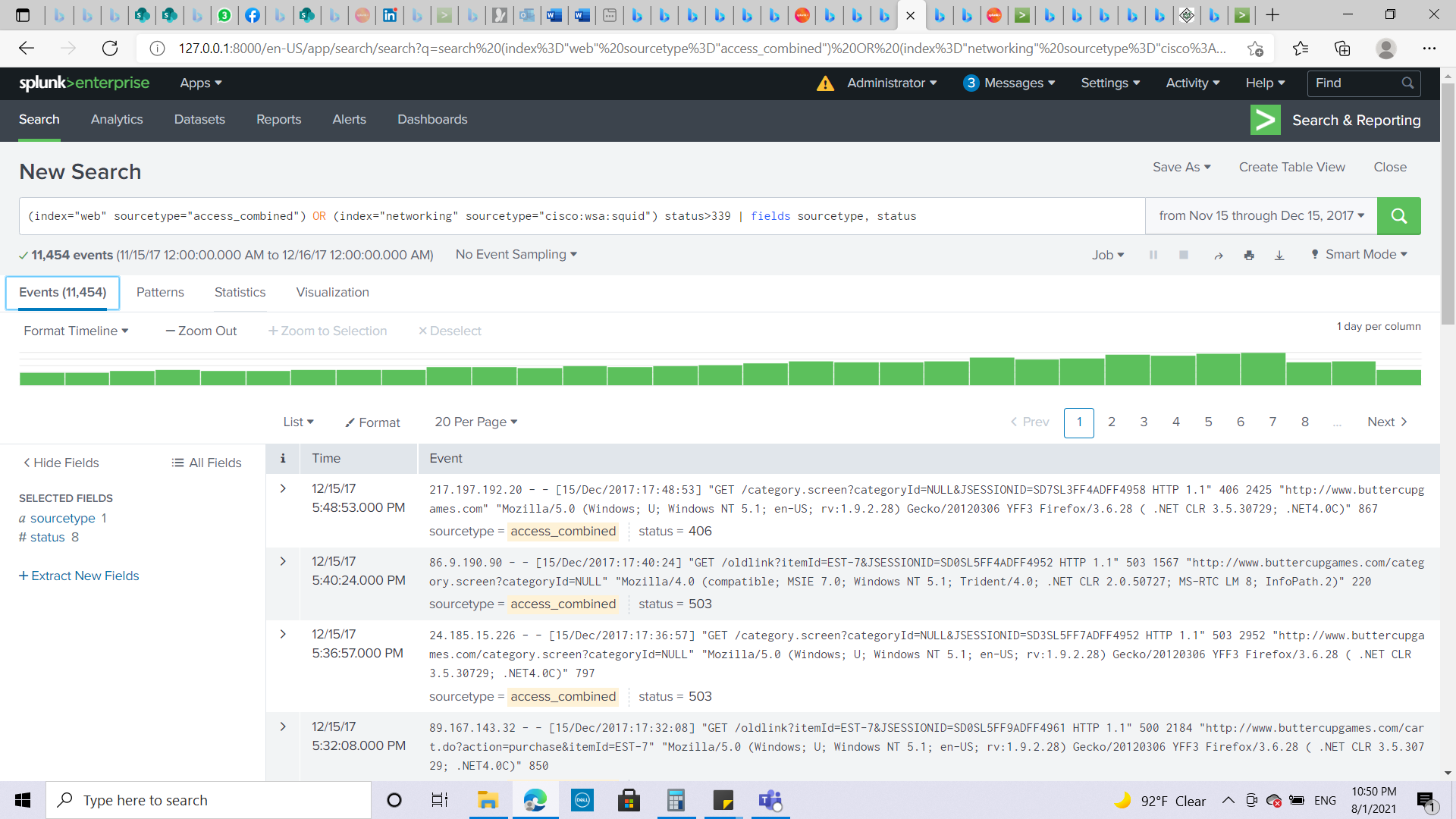
**Task 3: Report common HTTP status errors that occurred during that month in 2017 on the** online sales web servers and the internal web appliance within a proximity of 5 minutes or less. Only include days with more than 5 common errors.

1. Search HTTP status error events from the online sales web servers [access\_combined] and the web appliance [cisco\_wsa\_squid] during the last 30 days. For best performance, limit extracted fields to only sourcetype and status.

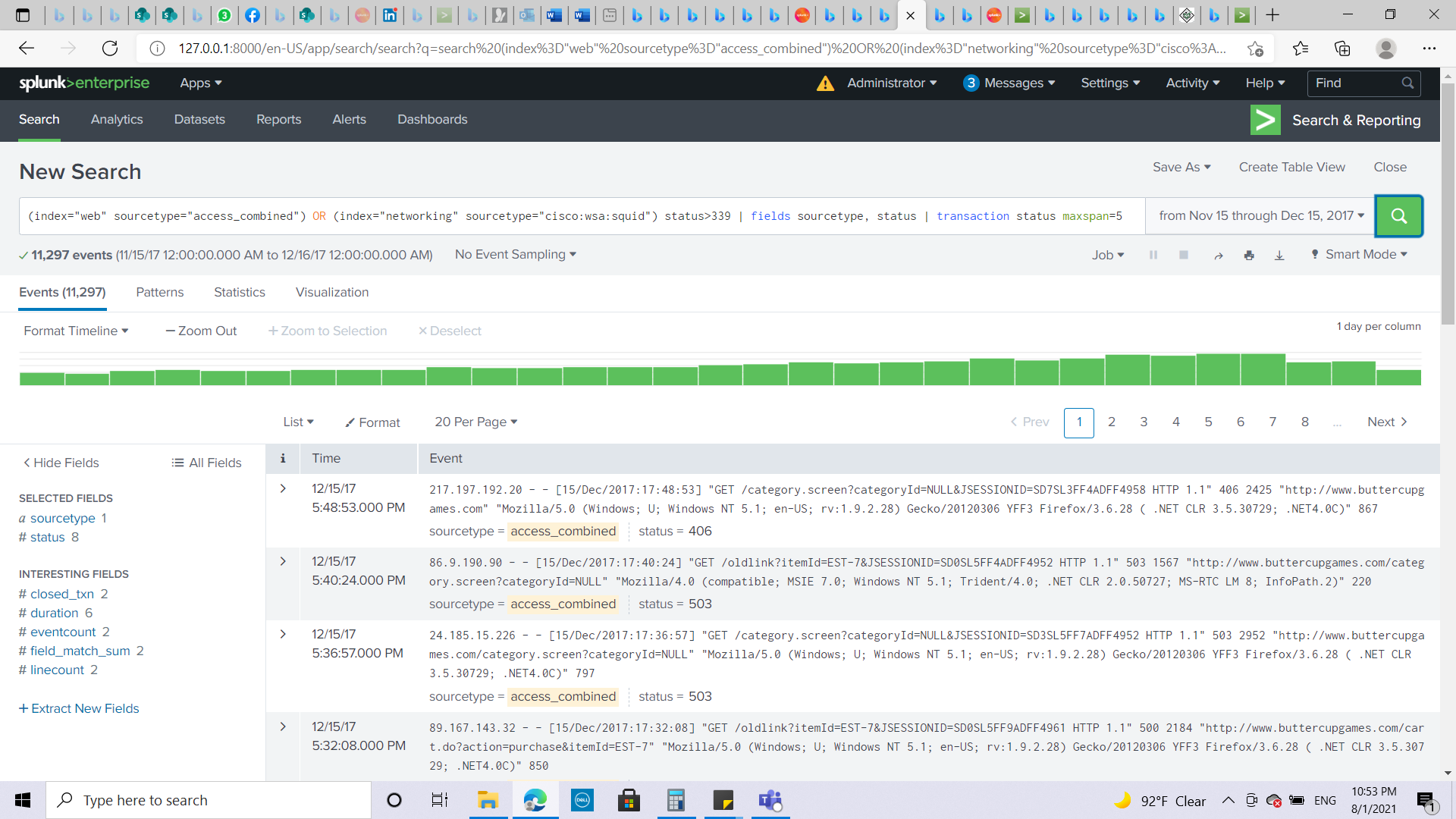
**Hint:**

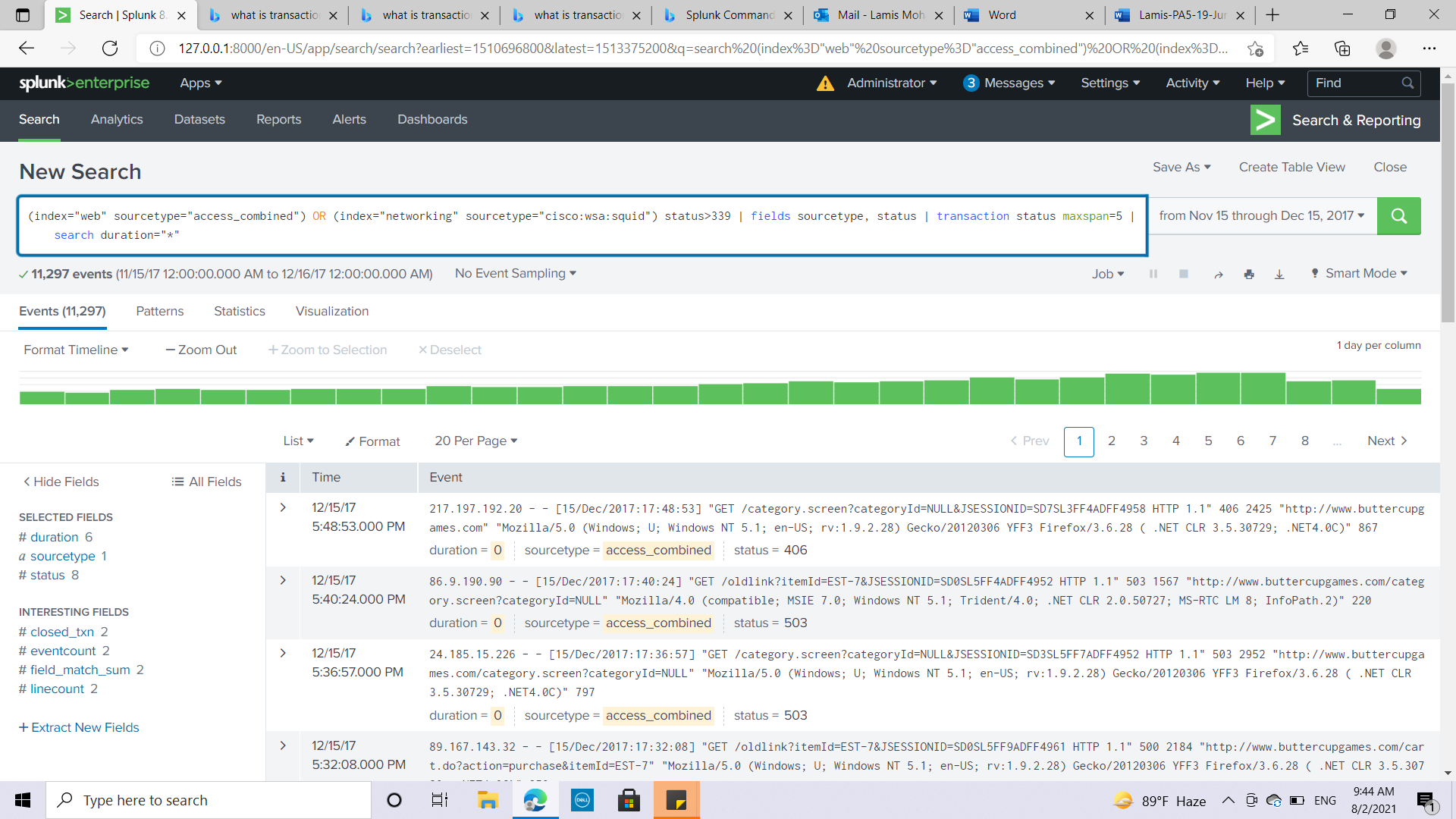
**(index=network sourcetype=cisco\_wsa\_squid) OR**

**(index=web sourcetype=access\_combined) status>399| fields sourcetype, status**

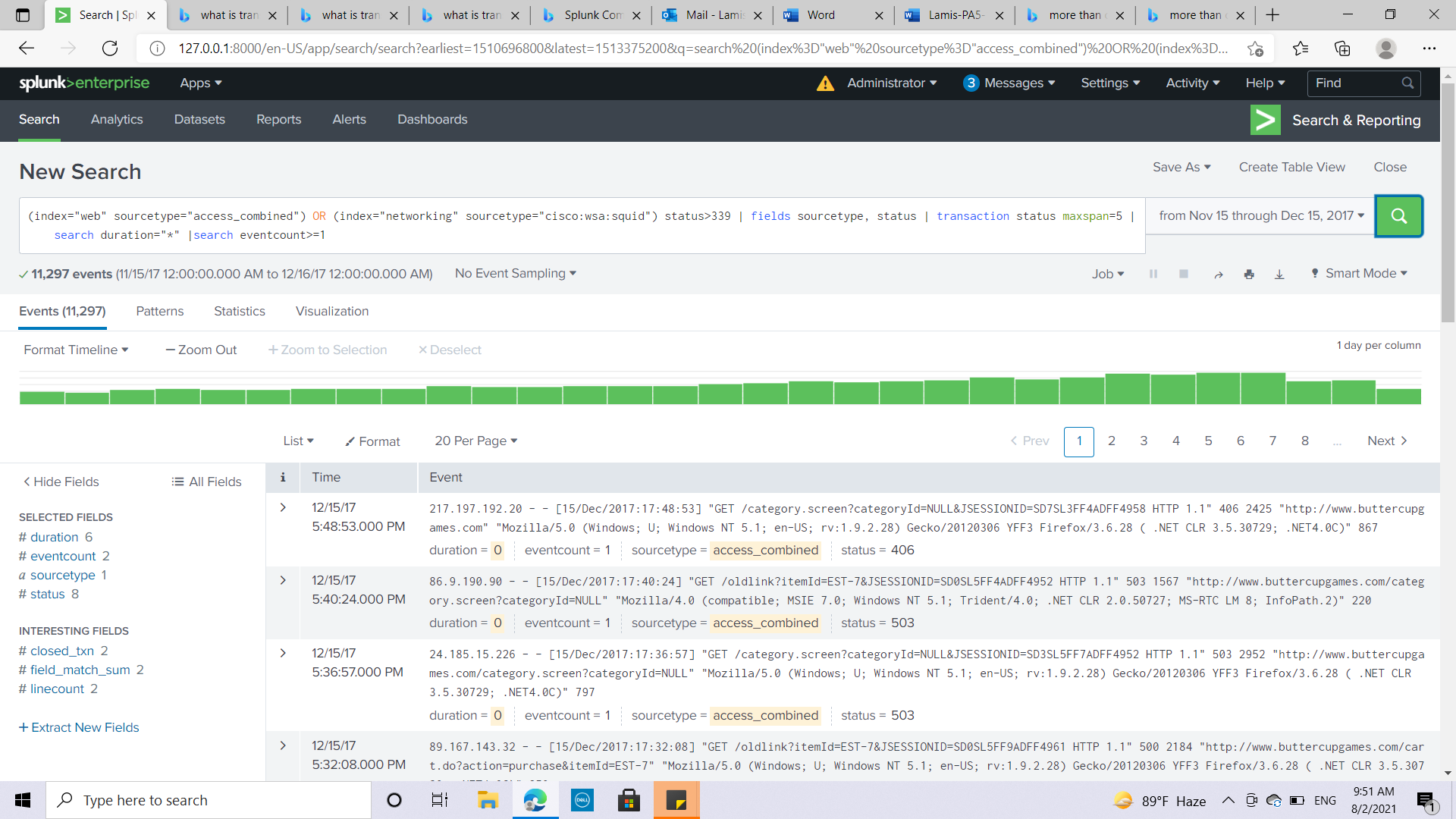


1. Create transactions based on status field values and limit the span to 5 minutes.

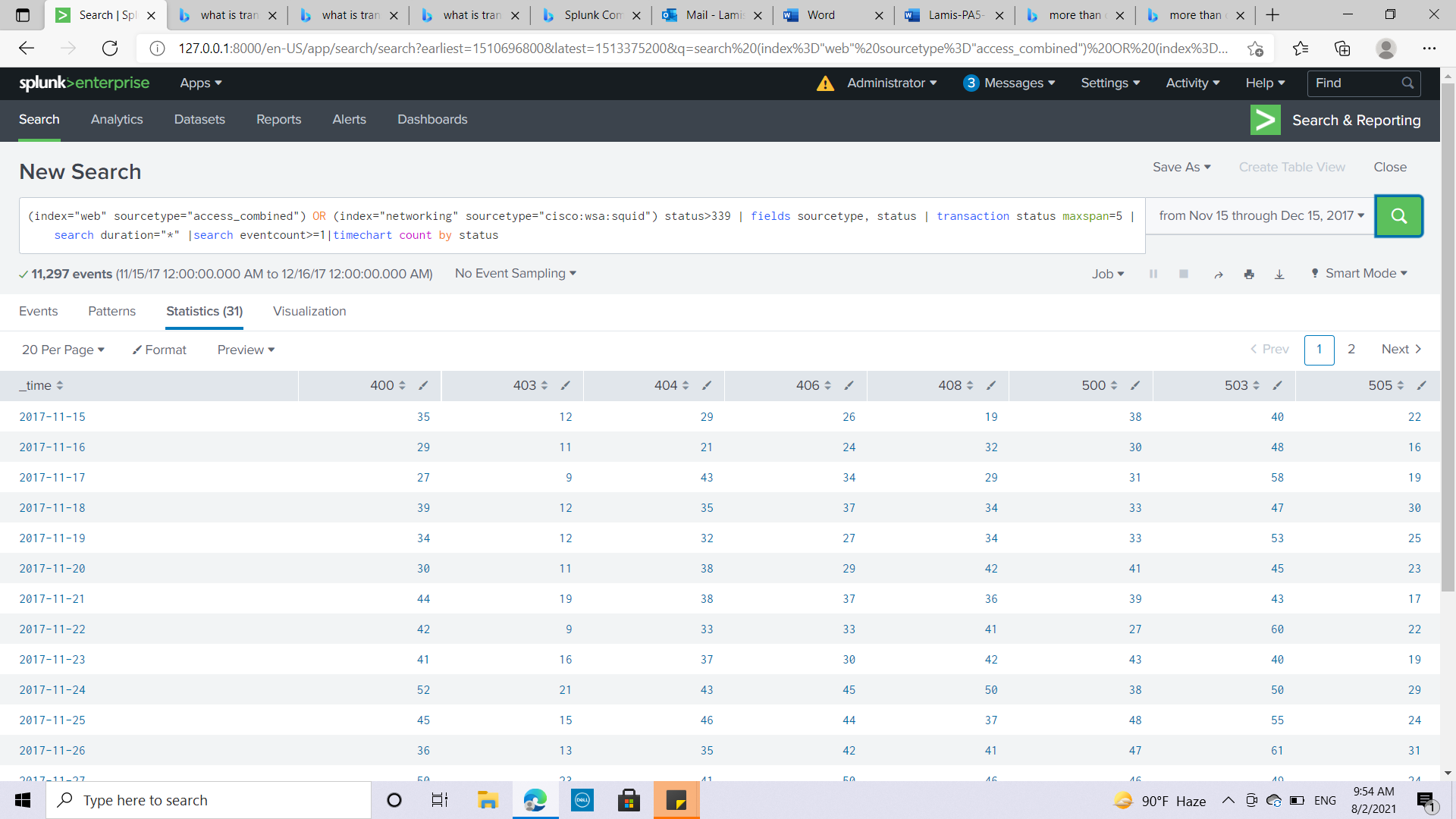


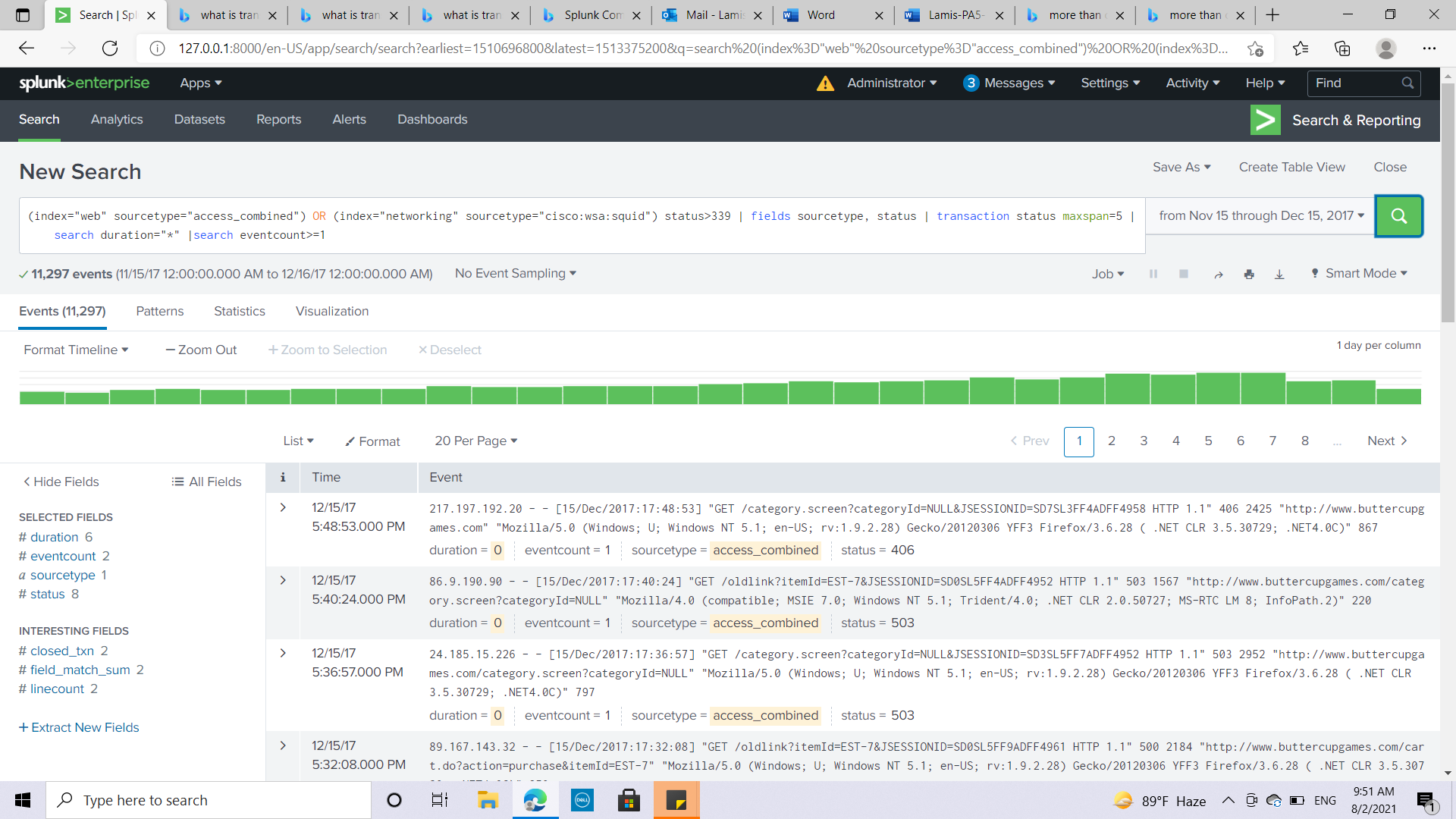


1. Limit the results to only transactions that contain at least one event from each sourcetype.



1. Use timechart to count events by status.

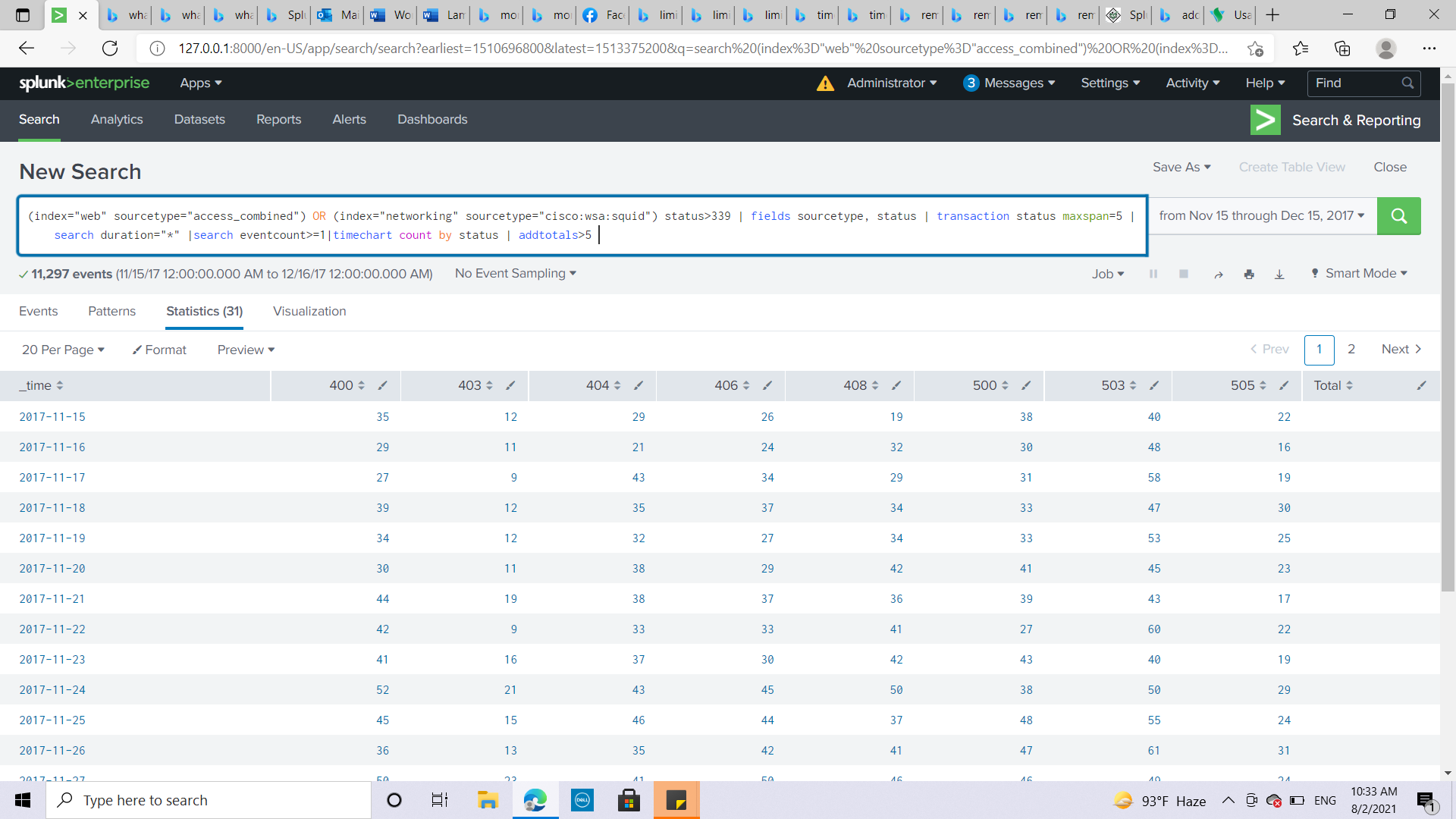




1. Discard rows that have fewer than 5 errors for all status values.

**Hint: Use addtotals.**

**| addtotals**



1. You will have a Total column, Remove the Total column and display the data as a Line chart and screen shot your work process.

