Sally oketch.

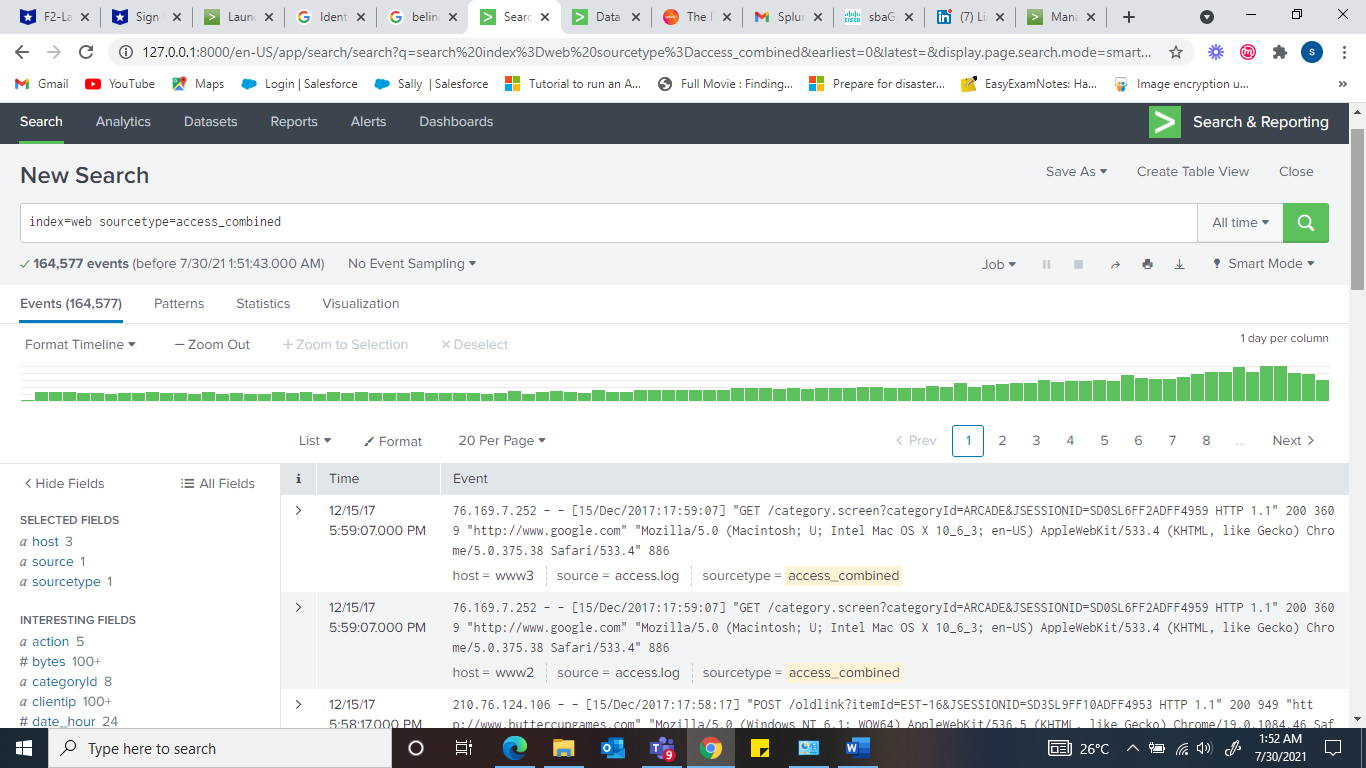
Sally.oketch@womentechsters.org

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

1. Search online sales [access\_combined] and answer with the

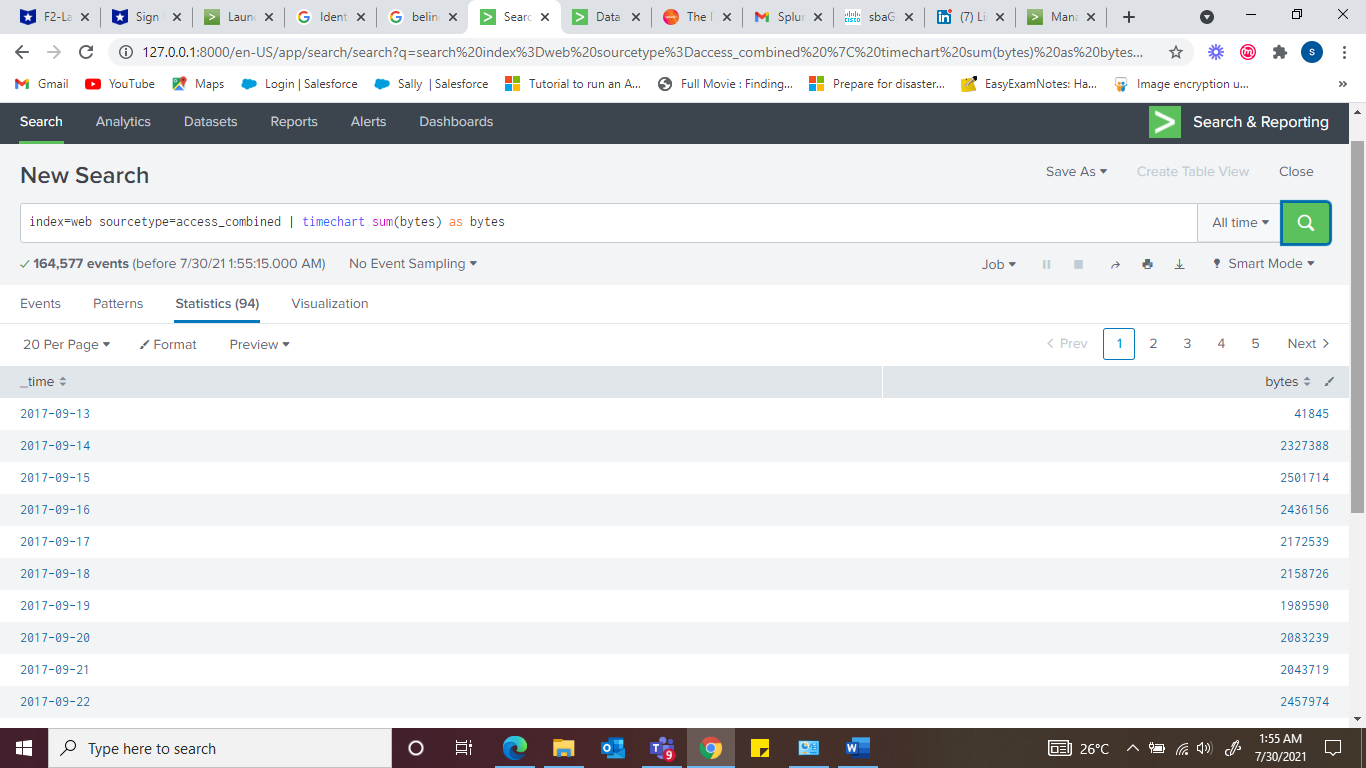
query you have  used.

**index=web sourcetype=access\_combined**



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

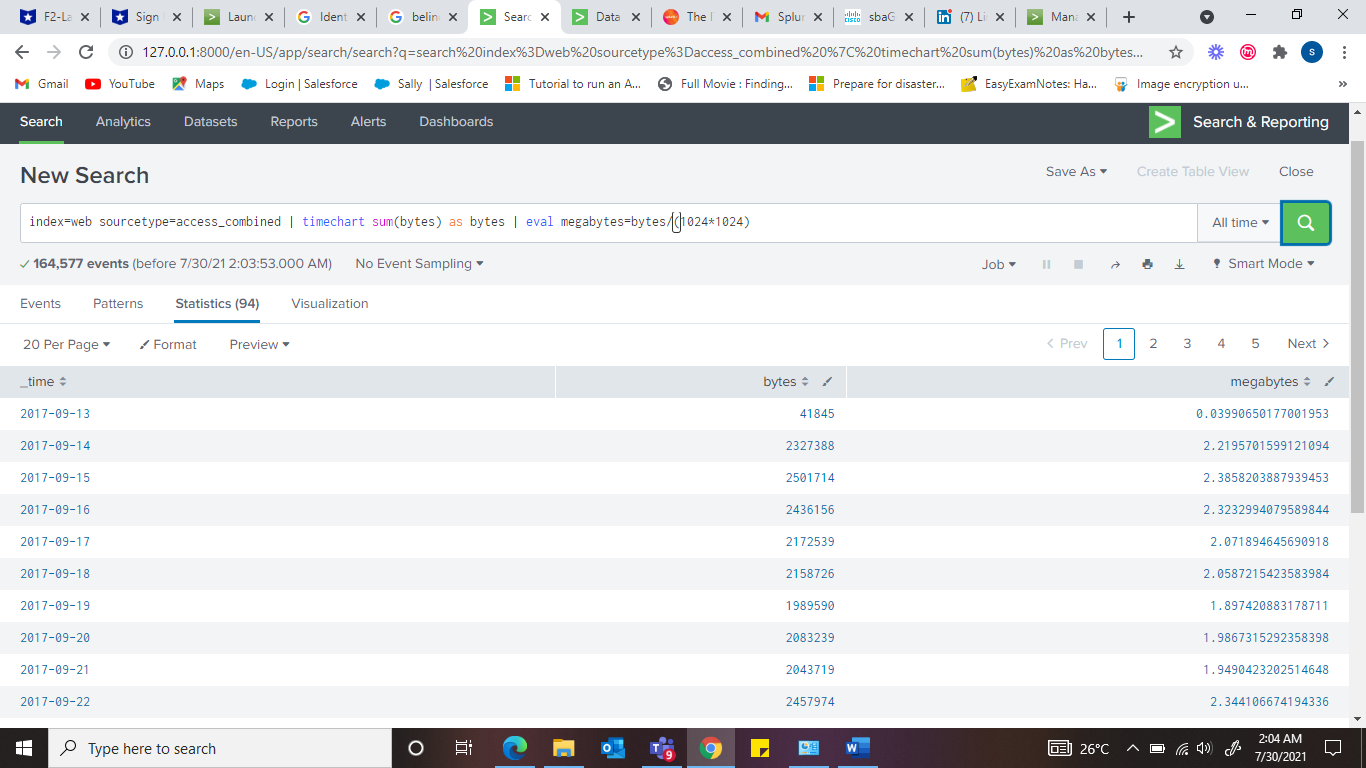
**index=web sourcetype=access\_combined | timechart sum(bytes) as bytes**



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

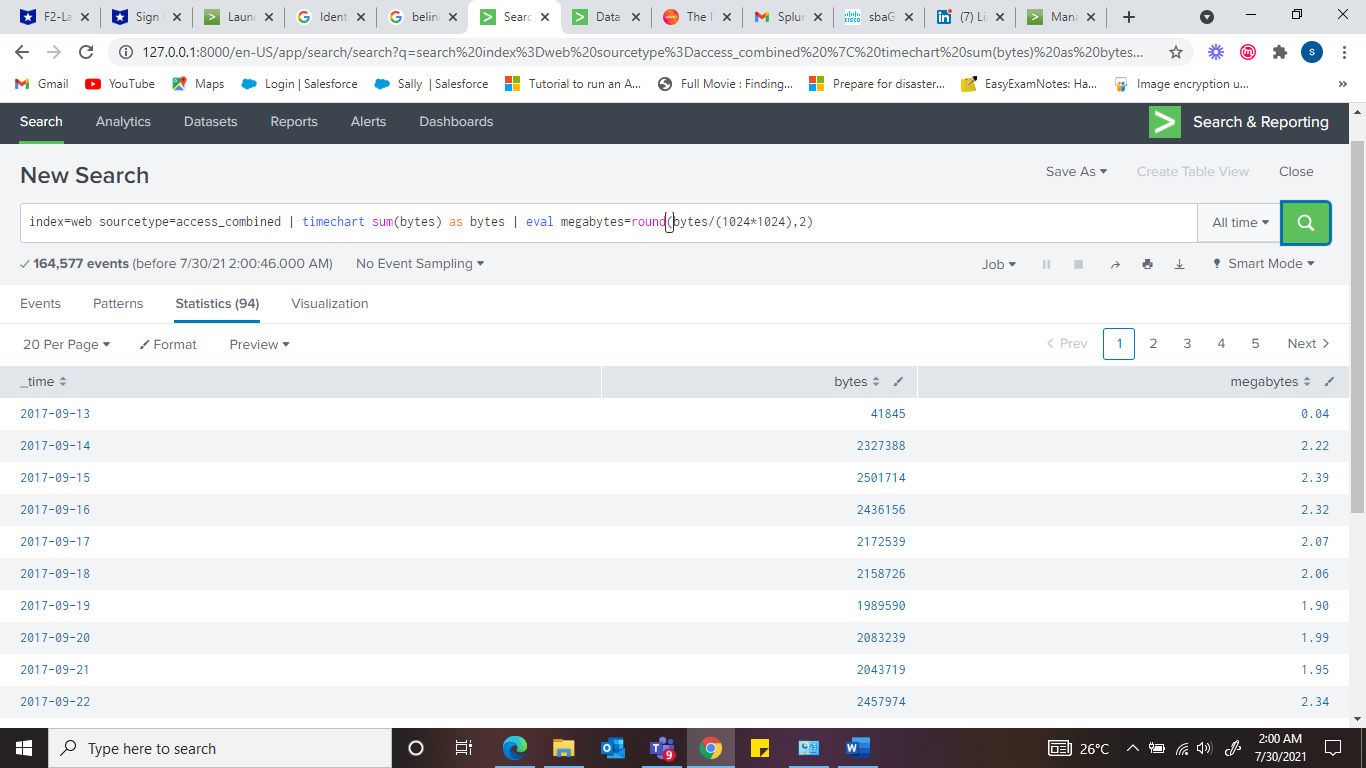
Hint: megabytes=bytes/(1024\*1024)

**index=web sourcetype=access\_combined | timechart sum(bytes) as bytes | eval megabytes=bytes/(1024\*1024)**

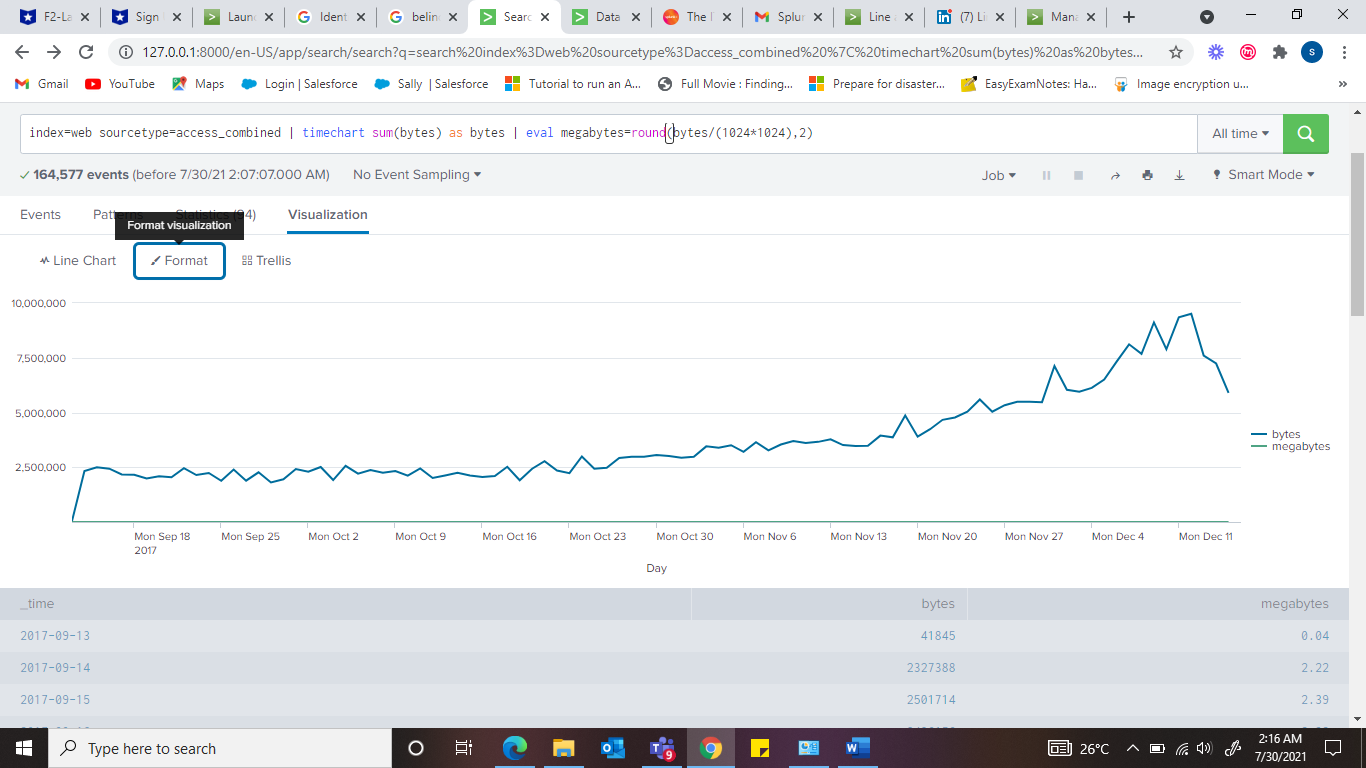


1. Use the round function to round the megabytes field values to two decimal places.

**index=web sourcetype=access\_combined | timechart sum(bytes) as bytes | eval megabytes=round(bytes/(1024\*1024),2)**

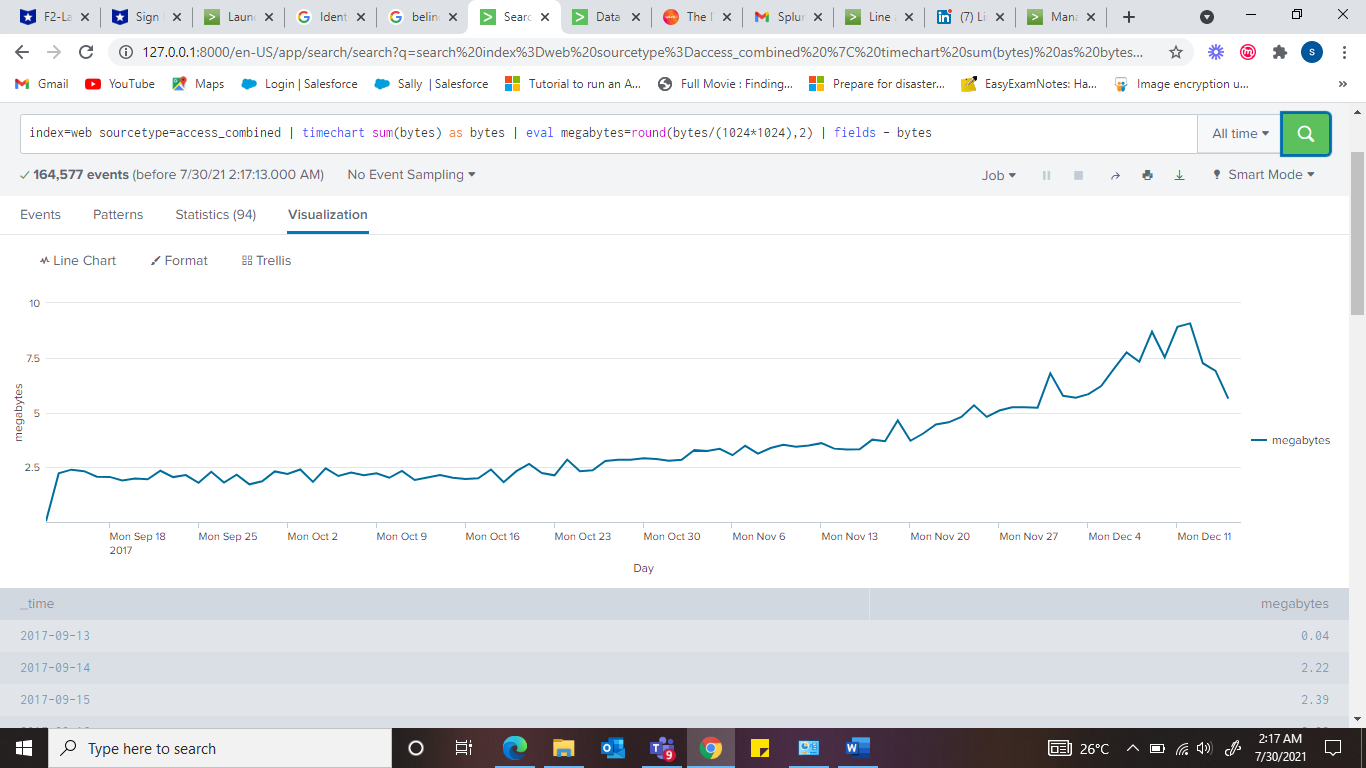


1. Switch to the Visualization tab and display the data as a Line Chart. Set the X-axis label to Day. Notice that the bytes field still displays.



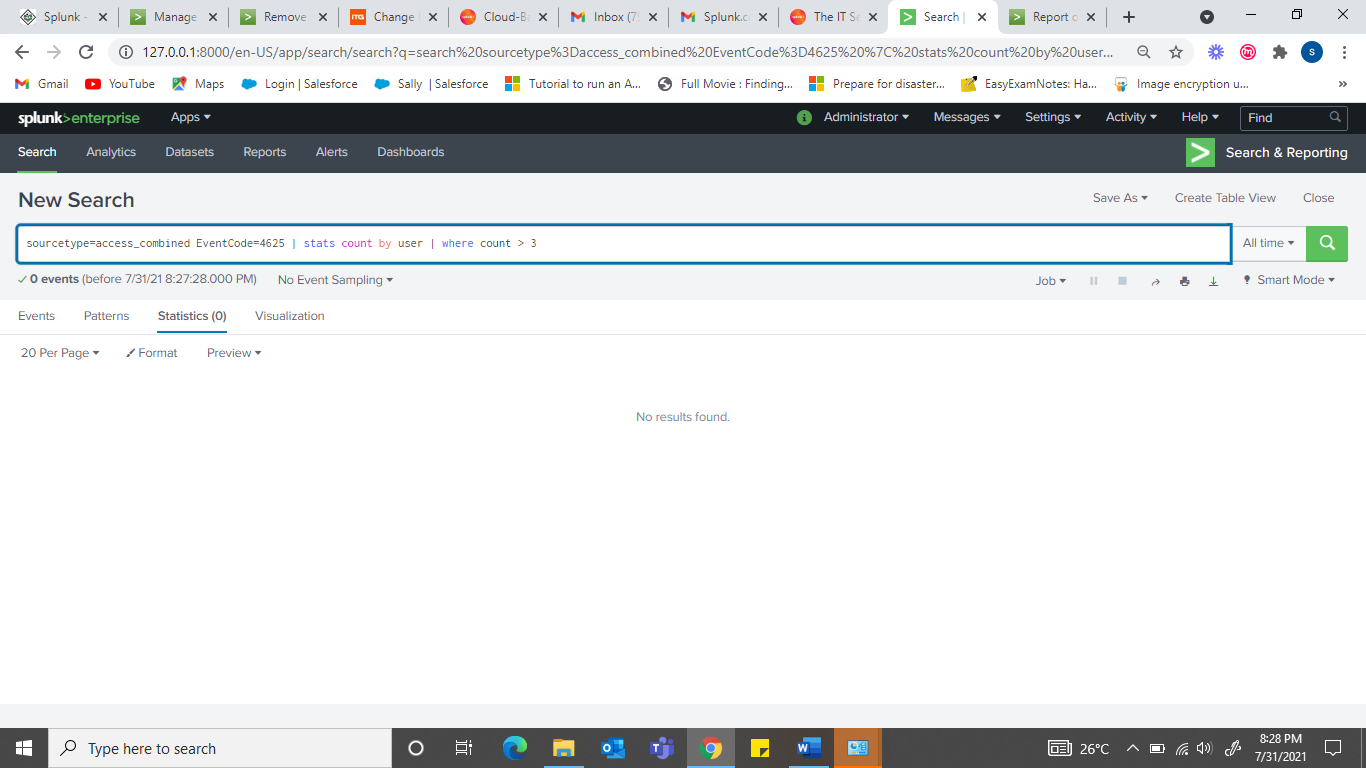
1. Use the fields command to remove the bytes field.

**index=web sourcetype=access\_combined | timechart sum(bytes) as bytes | eval megabytes=round(bytes/(1024\*1024),2) | fields - bytes**



**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.

**sourcetype=access\_combined EventCode=4625 | stats count by user | where count > 3**

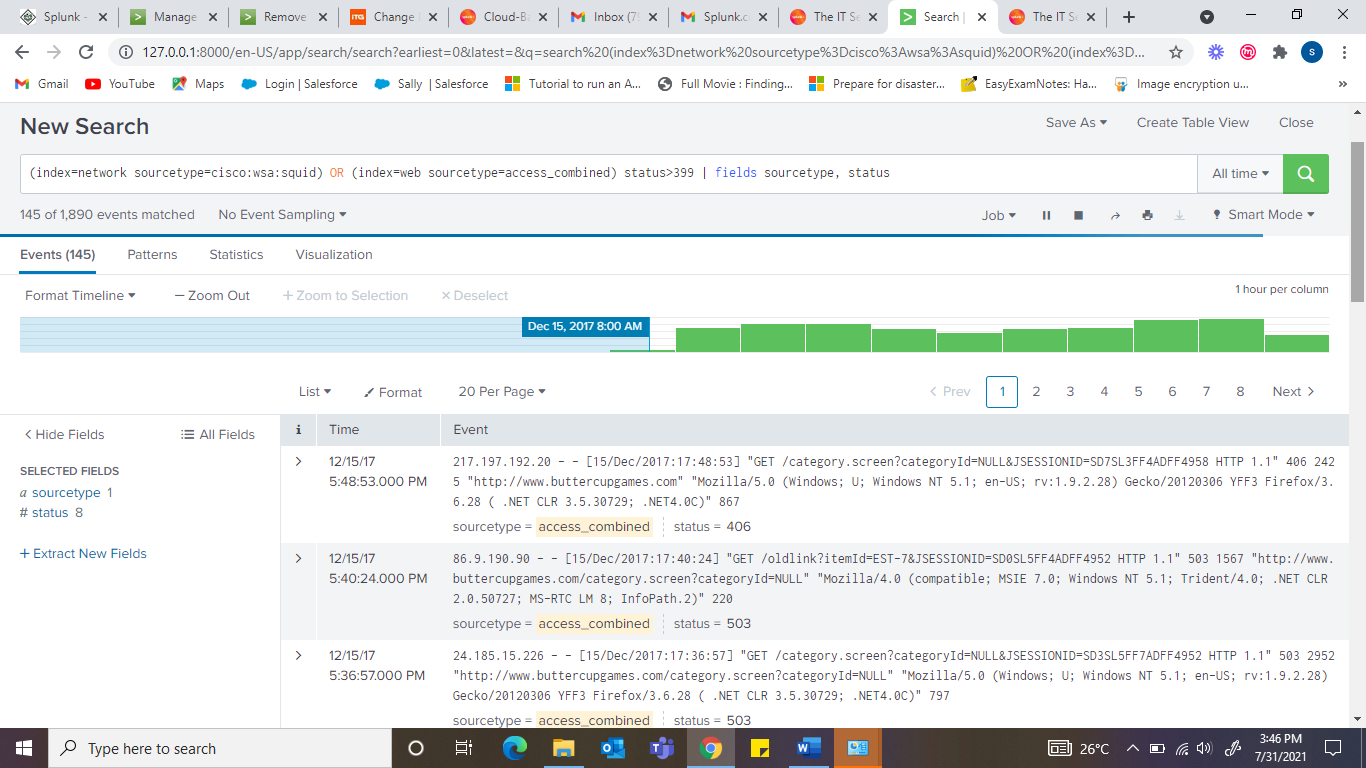


**Task 3: Report common HTTP status errors that occurred during that month in 2017 on the** online sales web servers and the internal web appliance within a proximity of 5 minutes or less. Only include days with more than 5 common errors.

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.

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

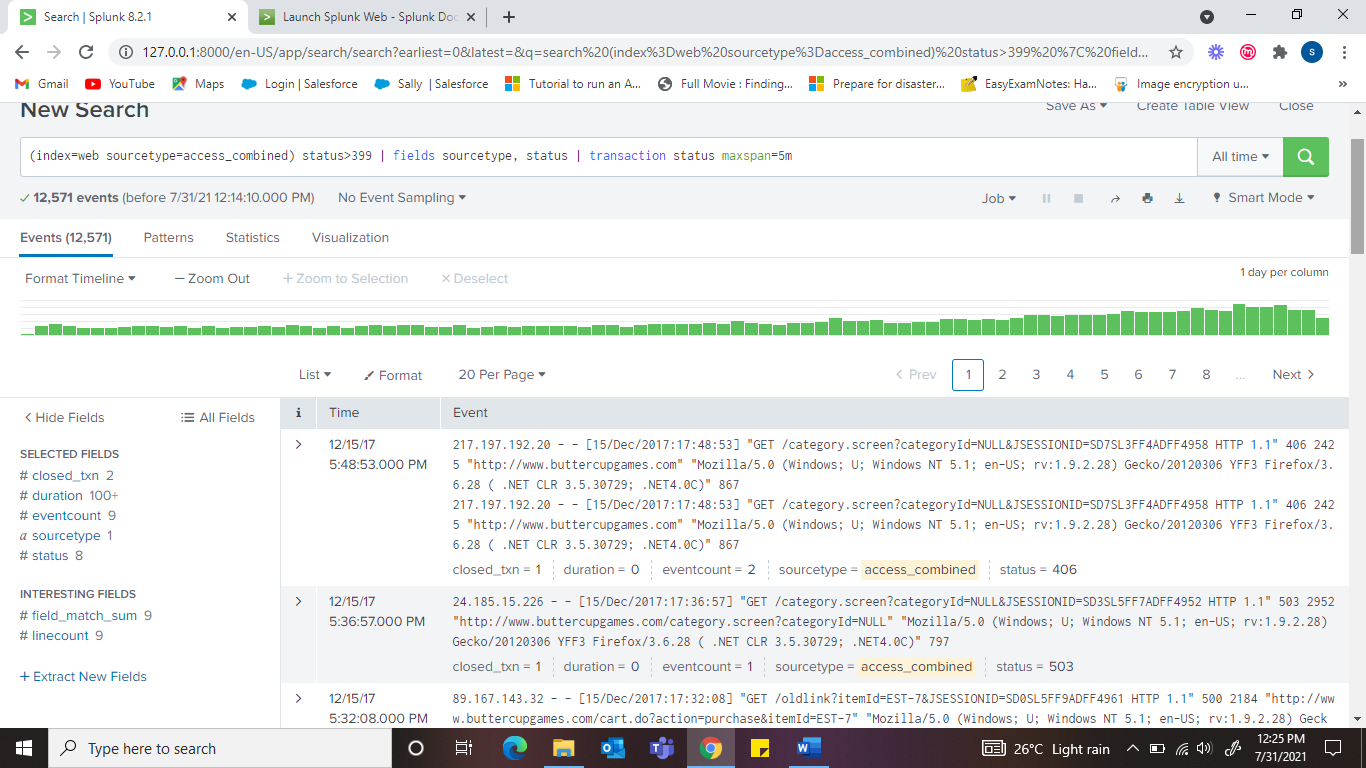
**(index=web sourcetype=access\_combined) status>399| fields sourcetype, status**



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

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

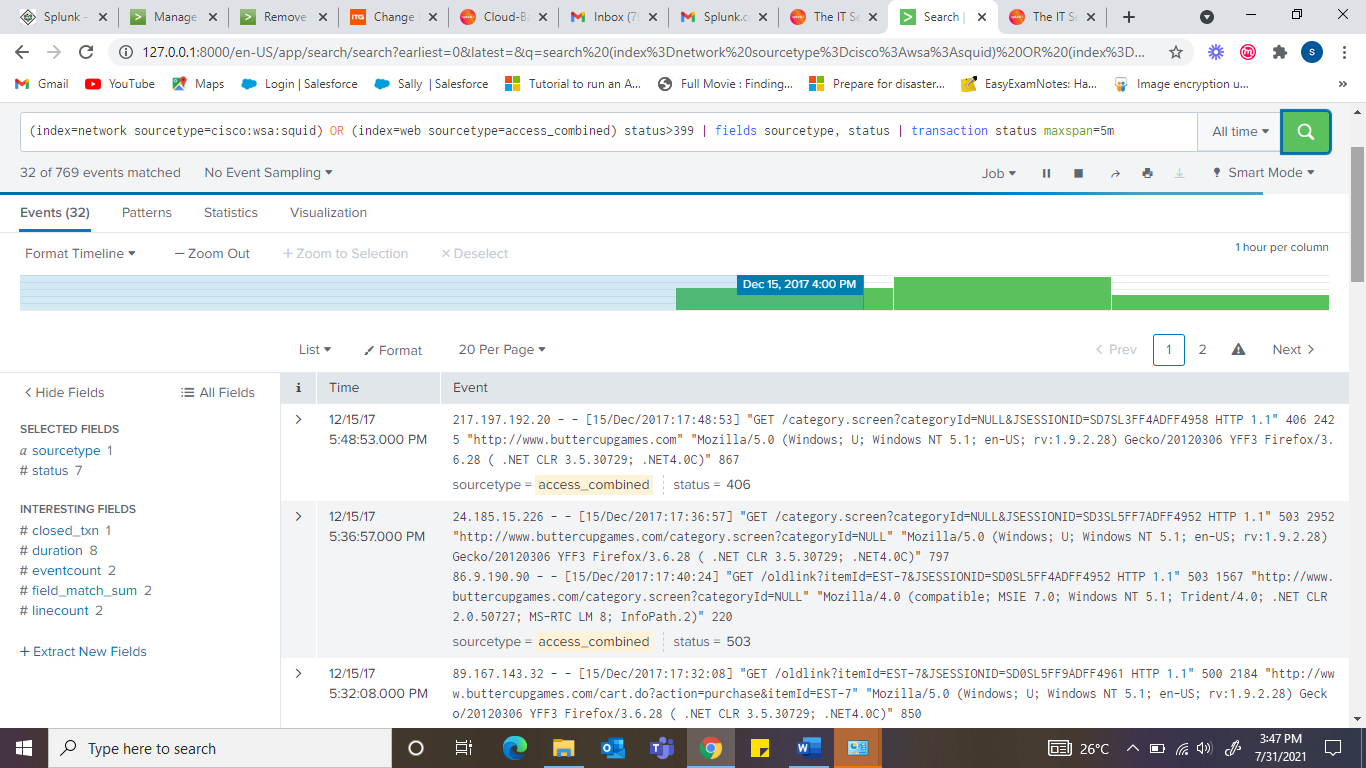
**| transaction status maxspan=5m**



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

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

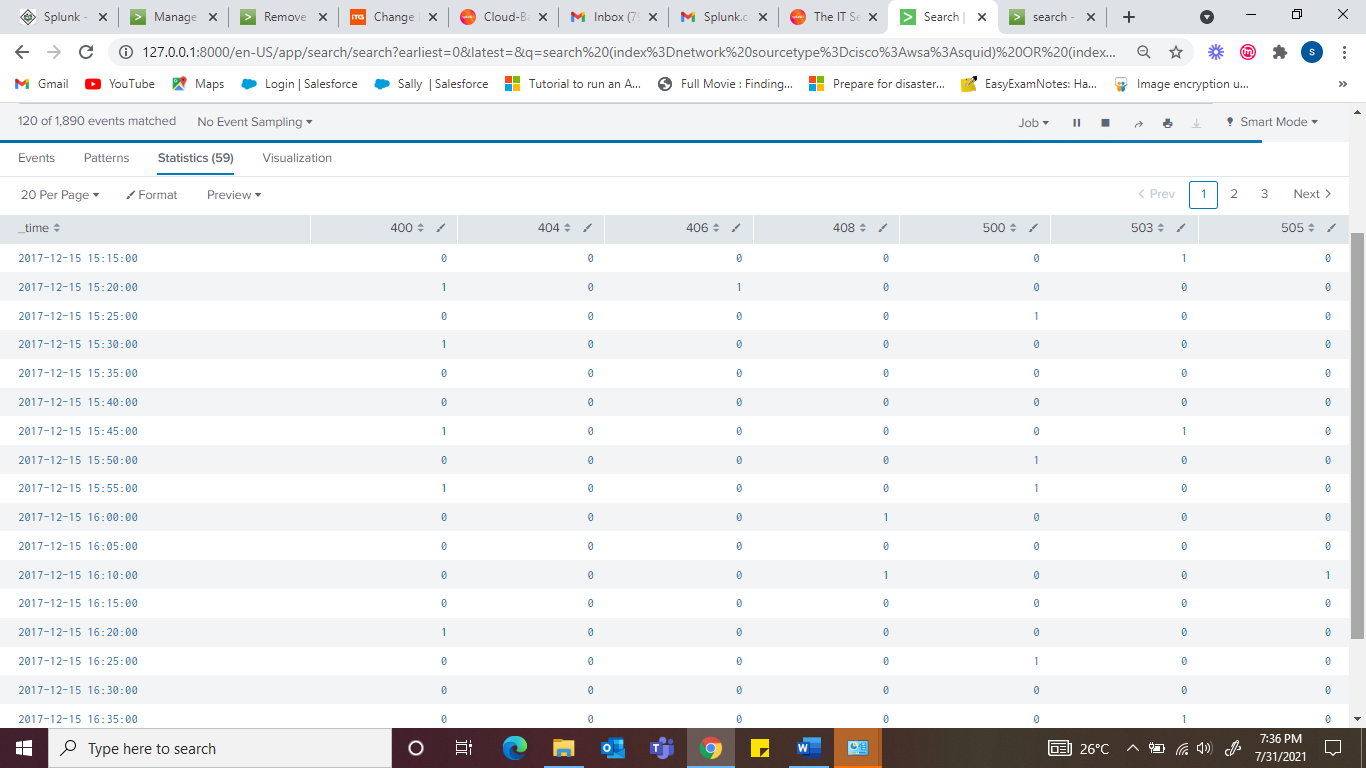
**| transaction status maxspan=5m | transaction status maxspan=5m**



1. Use timechart to count events by status.

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

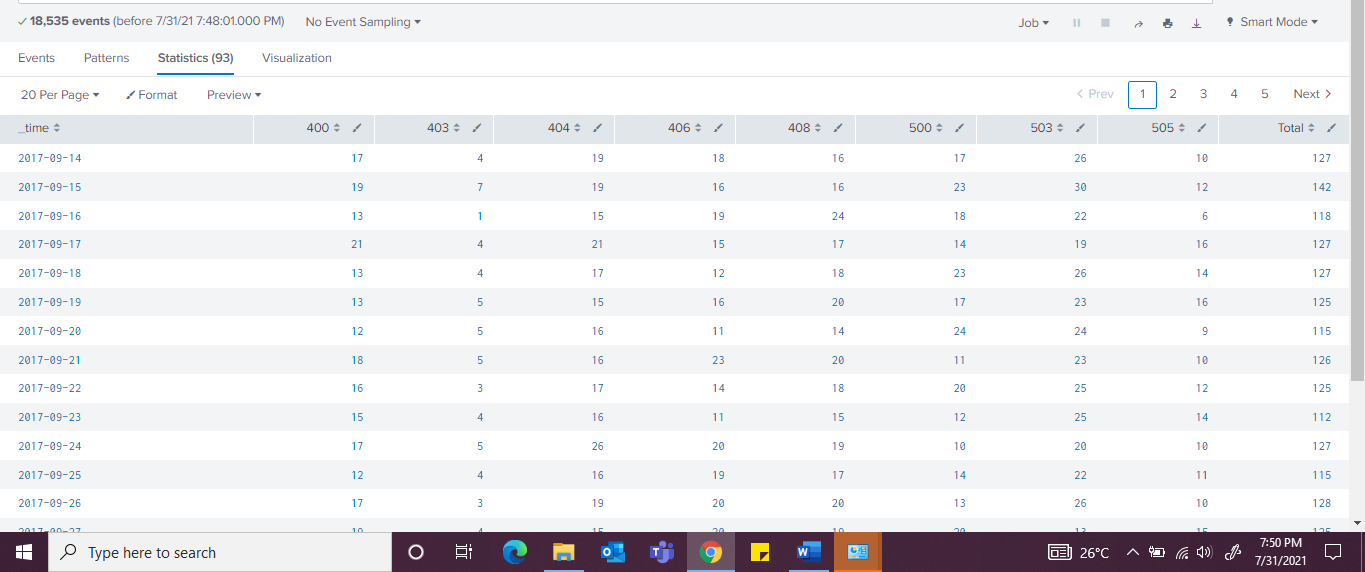
**| transaction status maxspan=5m | transaction status maxspan=5m | search sourcetype=access\_combined AND sourcetype=cisco:wsa:squid**



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

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

**| transaction status maxspan=5m | transaction status maxspan=5m | search sourcetype=access\_combined AND sourcetype=cisco:wsa:squid | 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.

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

**| transaction status maxspan=5m | transaction status maxspan=5m | search sourcetype=access\_combined AND sourcetype=cisco:wsa:squid | addtotals**

