LEARNING SPLUNK

Article by-DEEPALI GUPTA

SPLUNK :

Splunk is a software platform used for monitoring, searching, analyzing and visualizing machine-generated data in real time. It captures, indexes, and correlates real-time data in a searchable container and produces graphs, alerts, dashboards, and visualizations. Splunk is used to monitor and troubleshoot problems with applications, servers, and networks. Developers use Splunk to analyze and search data, create data models, and visualize results for monitoring and examining large amounts of machine-generated data.

MODULE 1: INSTALL SPLUNK ENTERPRISE

INSTALLATION OF SPLUNK :

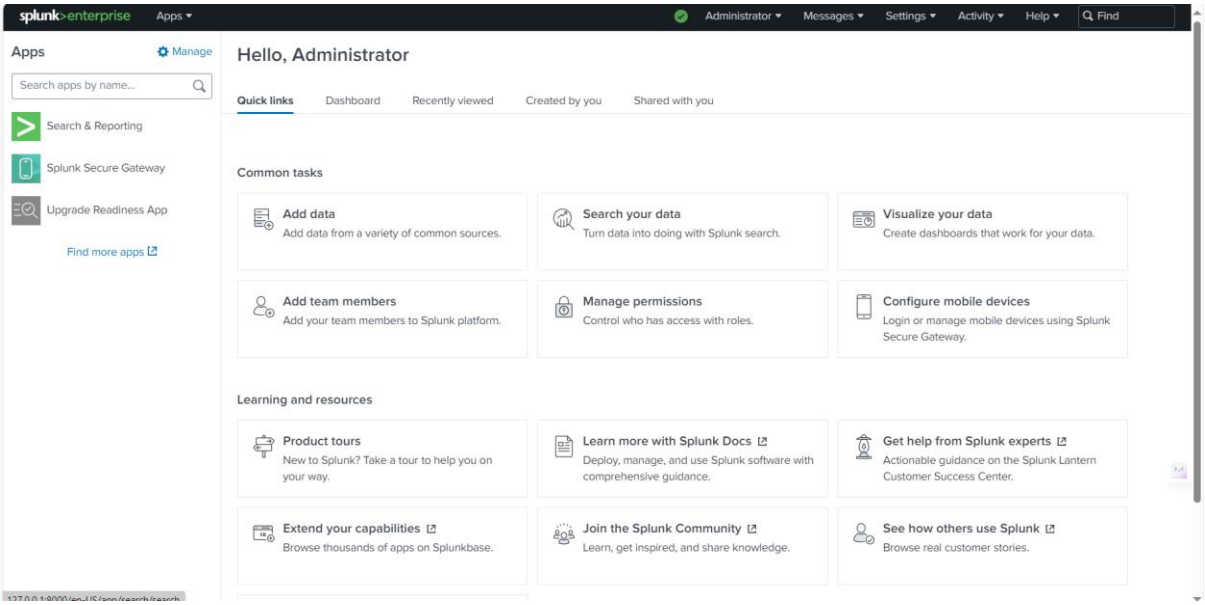
STEP 1: Go to the website of splunk- splunk.com.

STEP 2: Do the registration.

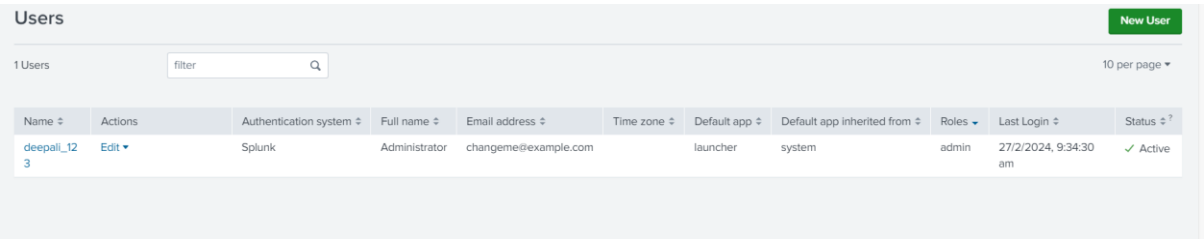
STEP 3: Go to products and download splunk enterprize.

STEP 4: Download will start and now you can run that msi file to install it on your system.

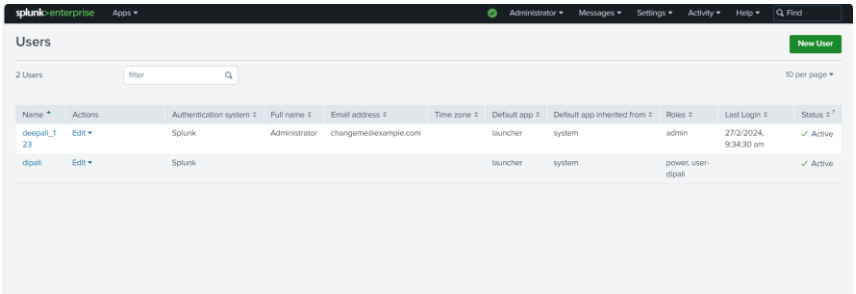
STEP 5: After installing , we can start with it.



Creating new user with administrator rights.

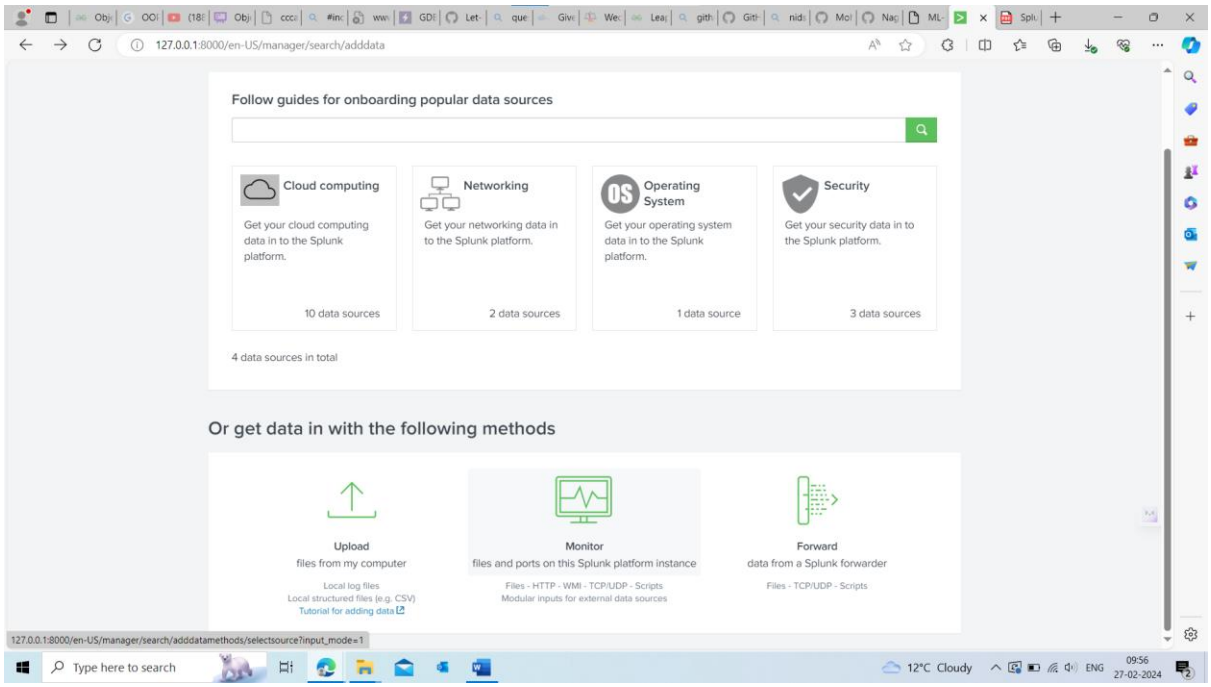


We can add users by:settings -> users-> new user. So ,here I created a new user with name – Dipali.

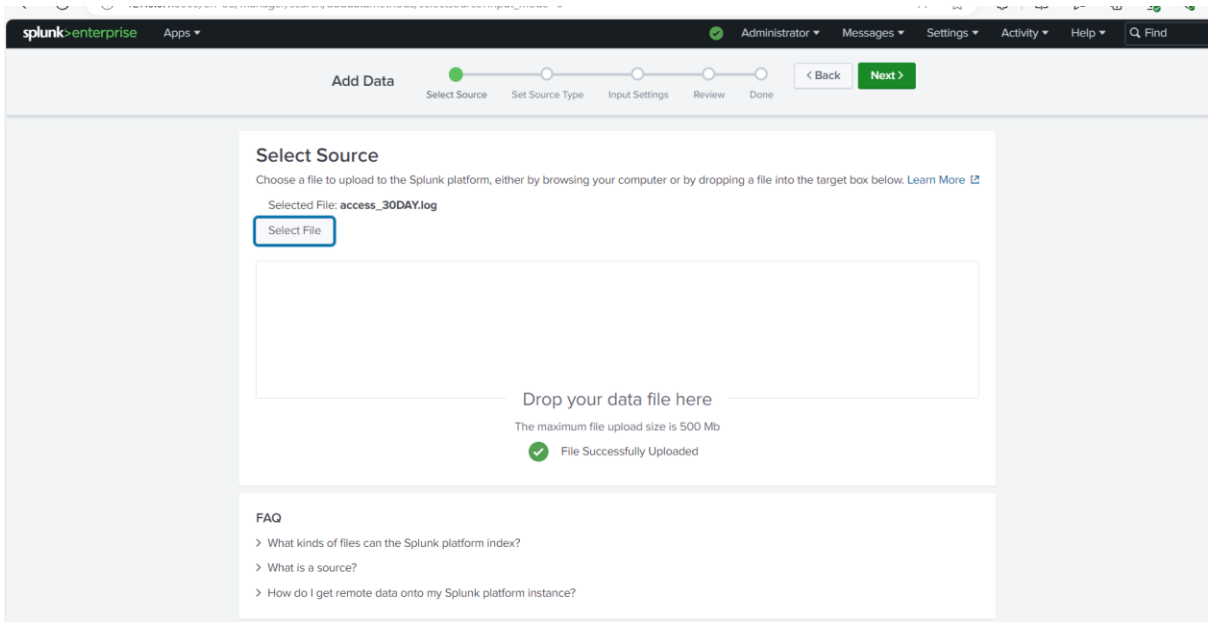


MODULE 2: INGESTING DATA

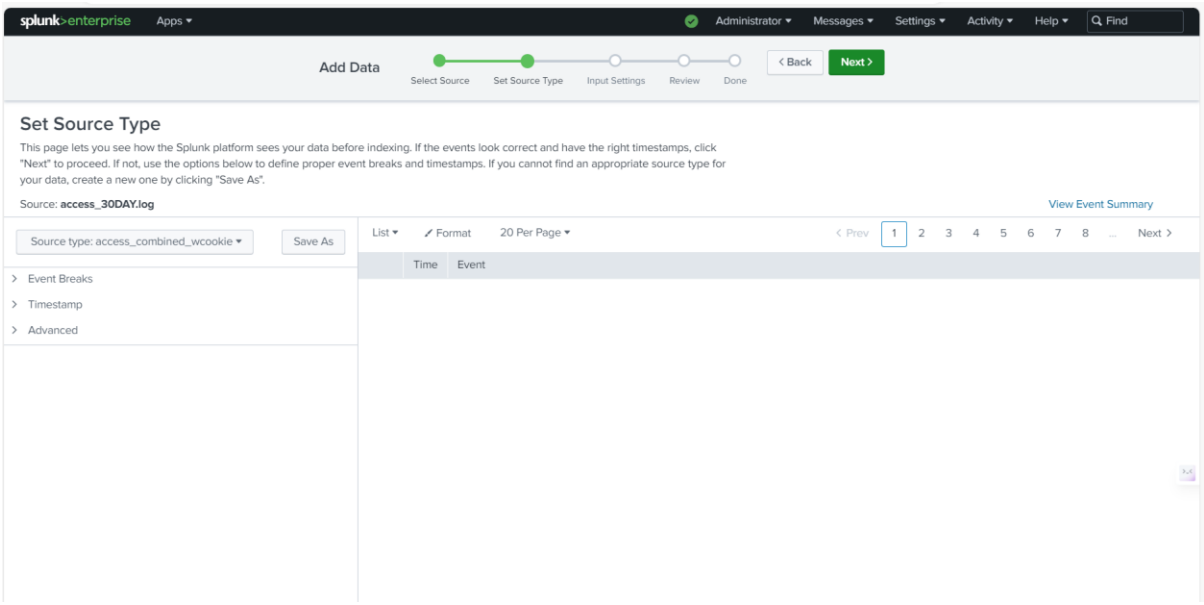
In this we will upload the file to analyse.



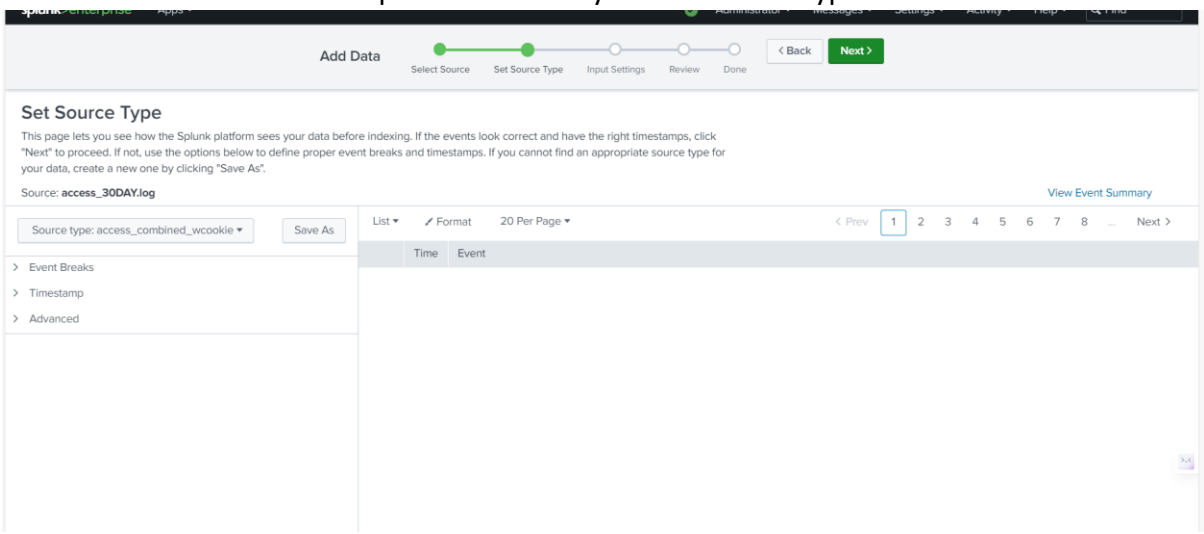
clicking on upload button, we will upload the file .



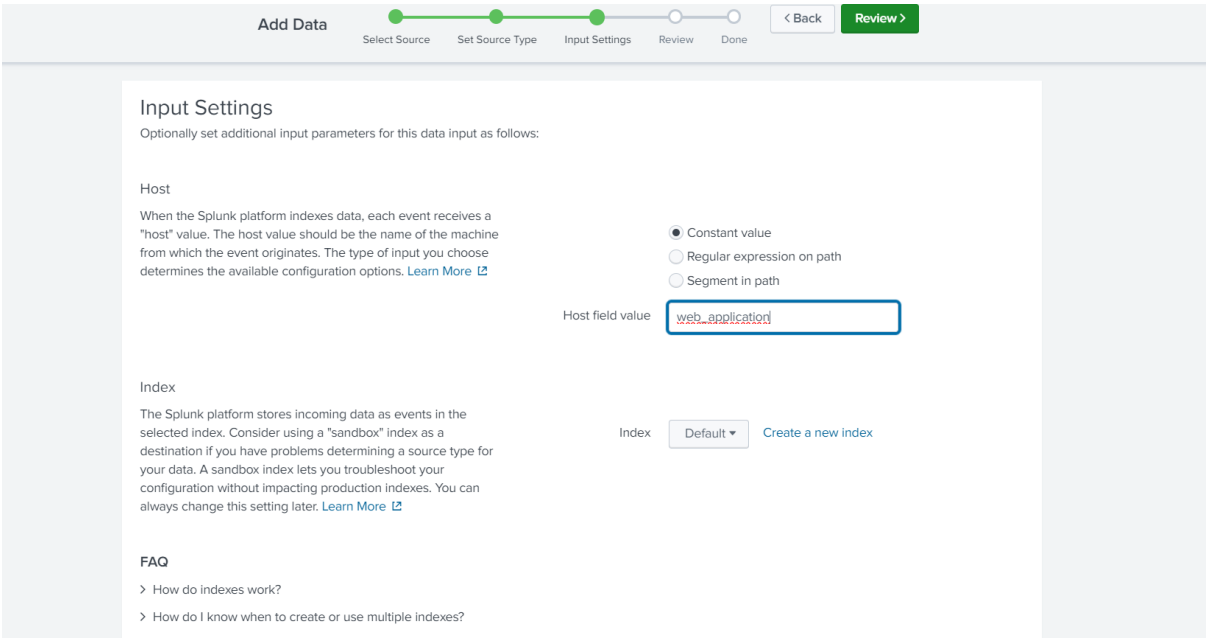
Now on clicking on next button, This screen will appear.



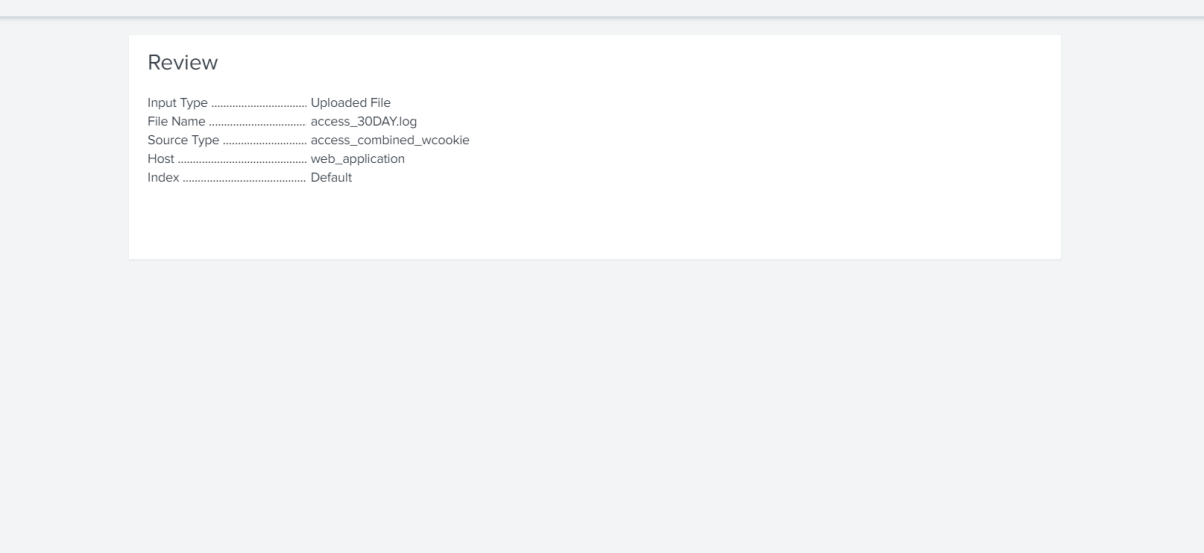
Now we can see in this that splunk has already set the source type.



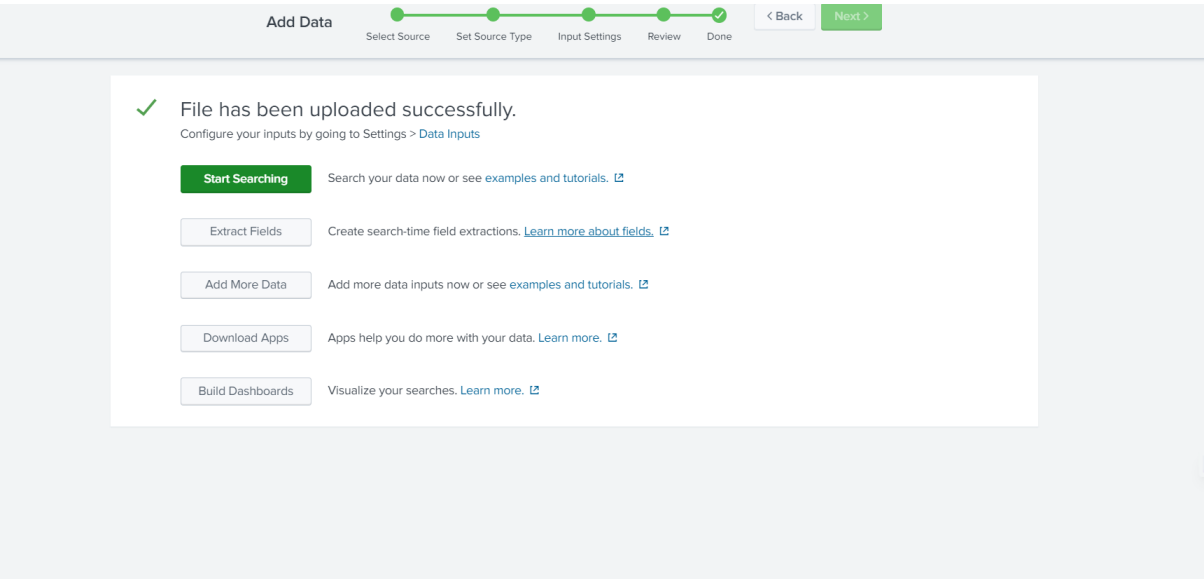
Now we have set the host field value as – web_application .



Clicking on Review button. We will get the page telling about our file details.

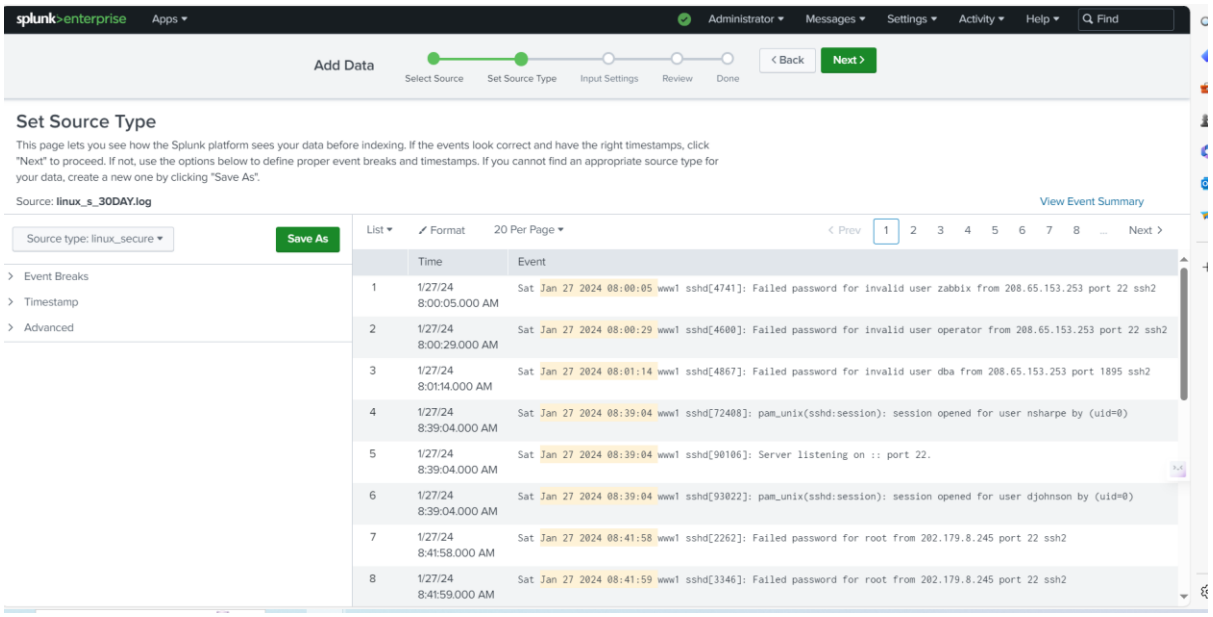


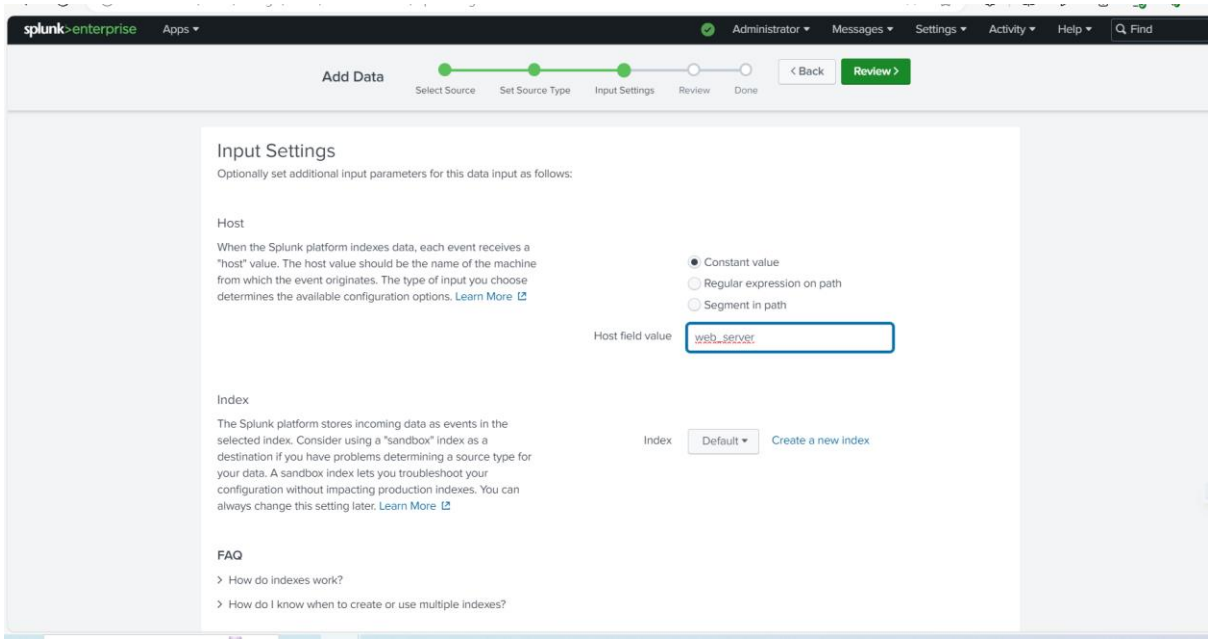
Clicking on submit button , our file will be submitted and we will now go to the task 3.

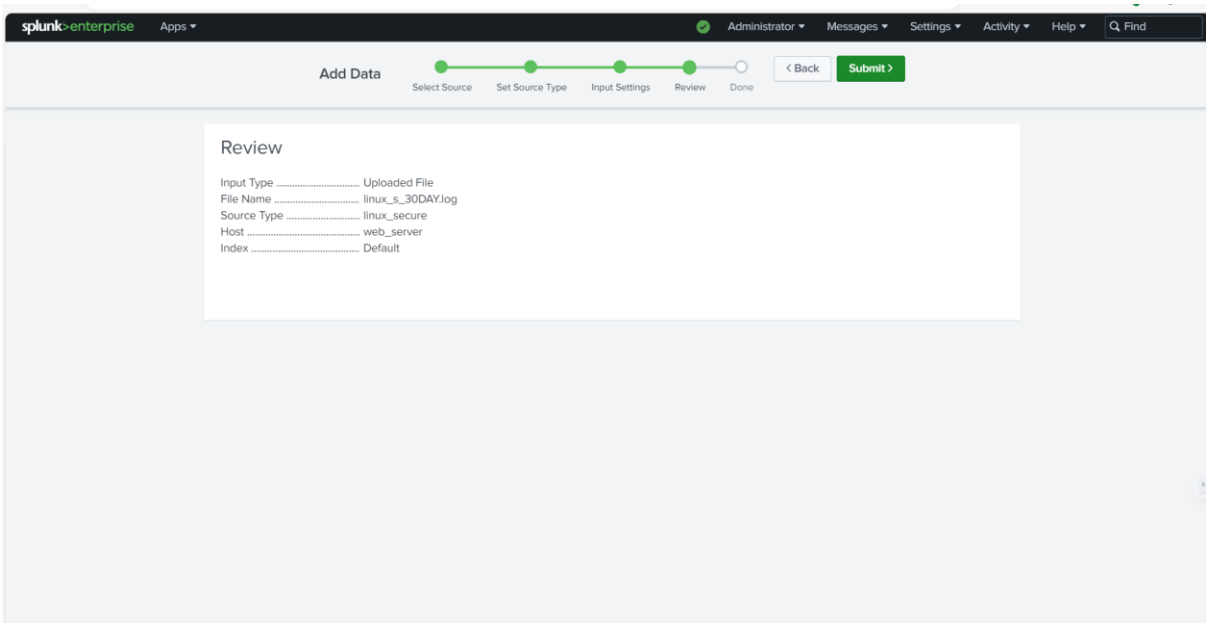


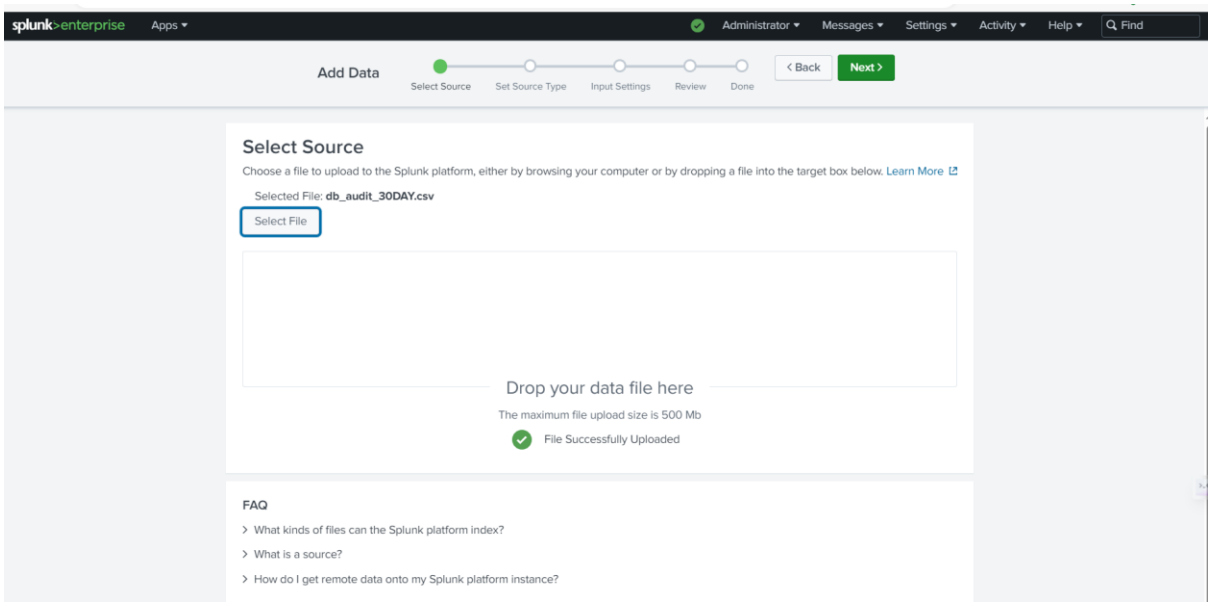
No we will upload the linux 30 day file by clicking on Add more button -> upload -> linux30day file.

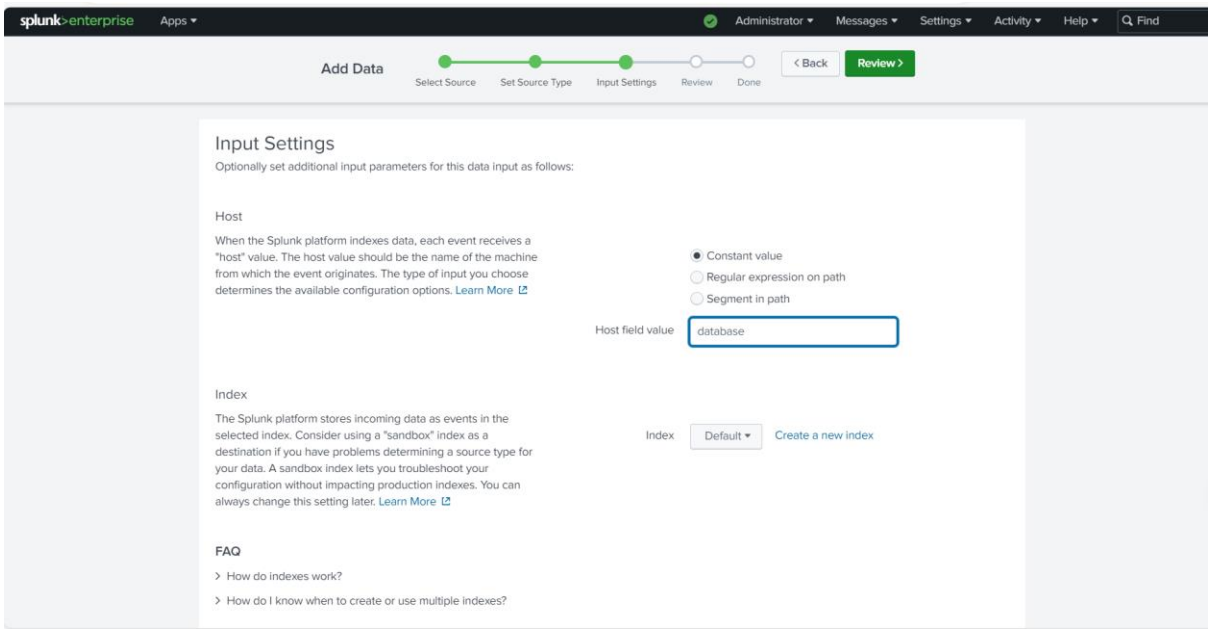
, now source type is to be set which is already set by the splunk.

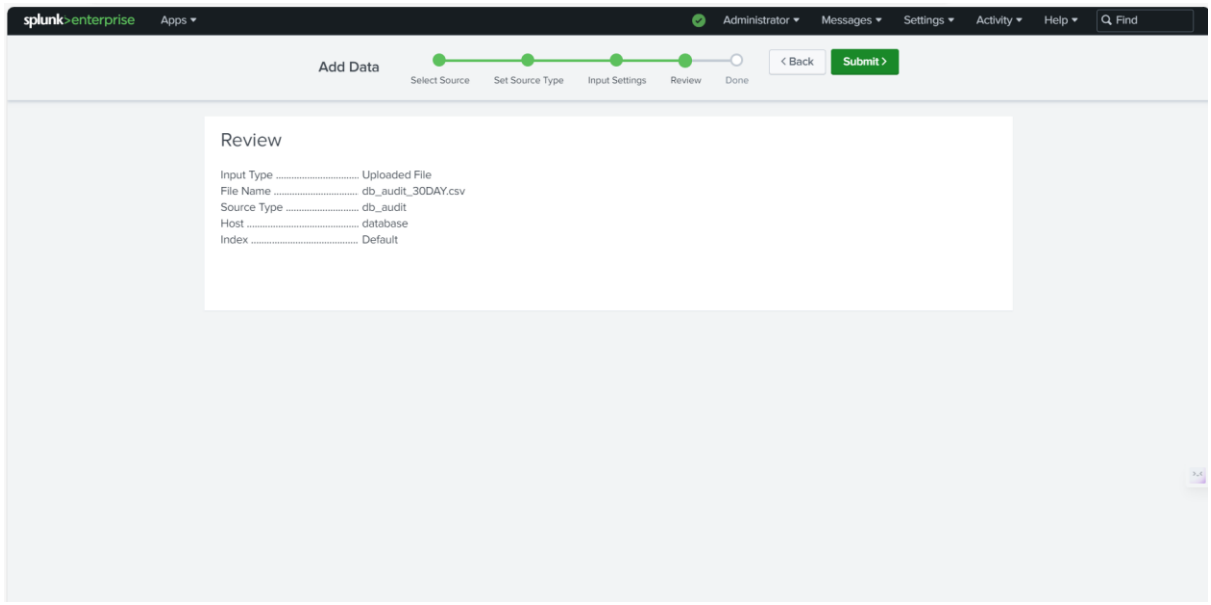

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: linux_s_30DAY.log
View Event Summary
Source type: linux_secure
Save As
Event Breaks
Timestamp
Advanced
List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8
Next
Time
Event
1 1/27/24 8:00:05.000 AM Sat Jan 27 2024 08:00:05 www1 sshd[4741]: Failed password for invalid user zabbix from 208.65.153.253 port 22 ssh2
2 1/27/24 8:00:29.000 AM Sat Jan 27 2024 08:00:29 www1 sshd[4600]: Failed password for invalid user operator from 208.65.153.253 port 22 ssh2
3 1/27/24 8:01:14.000 AM Sat Jan 27 2024 08:01:14 www1 sshd[4867]: Failed password for invalid user dba from 208.65.153.253 port 1895 ssh2
4 1/27/24 8:39:04.000 AM Sat Jan 27 2024 08:39:04 www1 sshd[72408]: pam_unix(sshd:session): session opened for user nsharpe by (uid=0)
5 1/27/24 8:39:04.000 AM Sat Jan 27 2024 08:39:04 www1 sshd[90106]: Server listening on :: port 22.
6 1/27/24 8:39:04.000 AM Sat Jan 27 2024 08:39:04 www1 sshd[93022]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
7 1/27/24 8:41:58.000 AM Sat Jan 27 2024 08:41:58 www1 sshd[2262]: Failed password for root from 202.179.8.245 port 22 ssh2
8 1/27/24 8:41:59.000 AM Sat Jan 27 2024 08:41:59 www1 sshd[3346]: Failed password for root from 202.179.8.245 port 22 ssh2


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Review
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
web_server
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
Default
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... Uploaded File
File Name ..... linux_s_30DAY.log
Source Type ..... linux_secure
Host ..... web_server
Index ..... Default


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Select Source
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More
Selected File: db_audit_30DAY.csv
Select File
Drop your data file here
The maximum file upload size is 500 Mb
File Successfully Uploaded
FAQ
What kinds of files can the Splunk platform index?
What is a source?
How do I get remote data onto my Splunk platform instance?

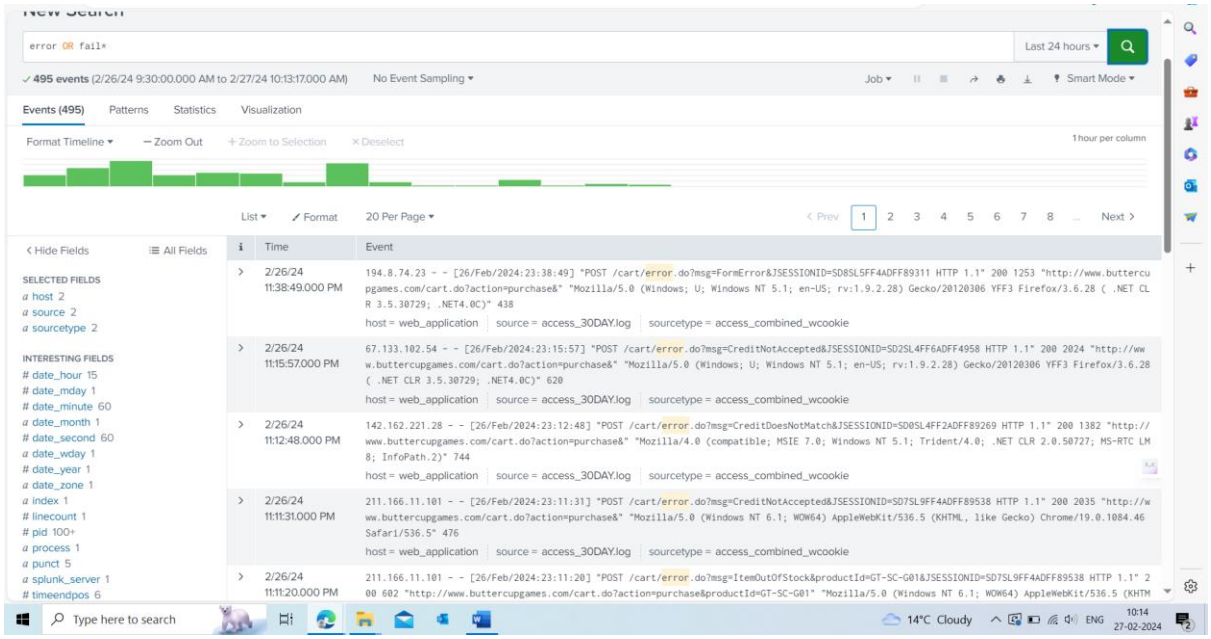

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
database
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
Default
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... Uploaded File
File Name ..... db_audit_30DAY.csv
Source Type ..... db_audit
Host ..... database
Index ..... Default

MODULE 3: SEARCHING

TASK 1: PERFORM A BASIC SEARCH

1. Performing Search with command : error OR fail*

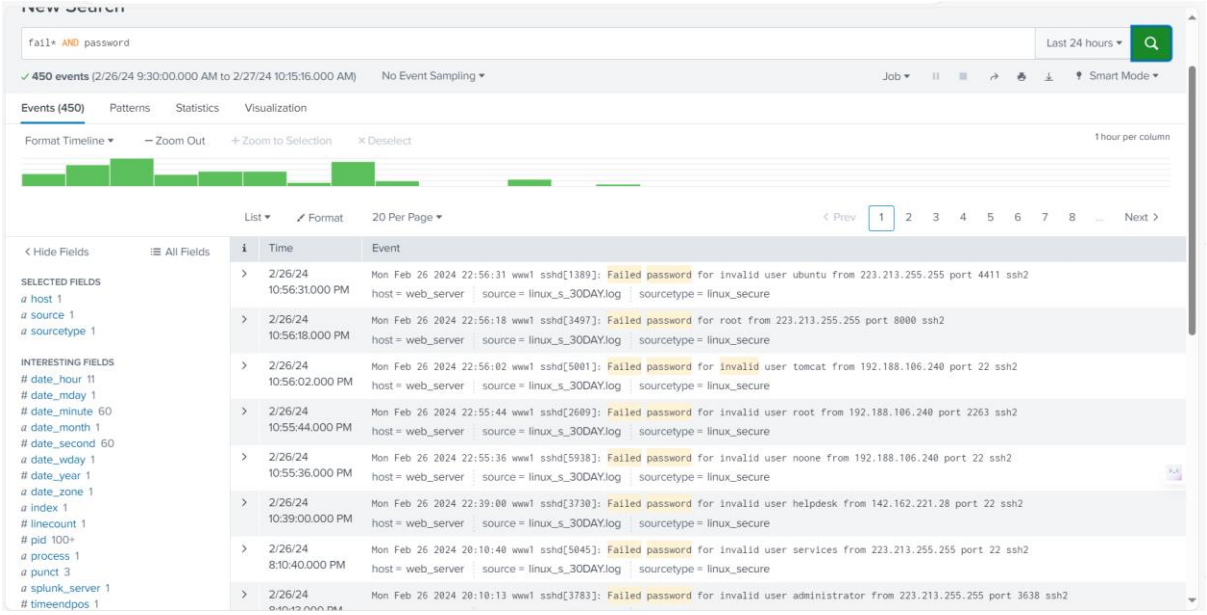


	11:06:48.000 PM			
>	2/26/24 11:06:40.000 PM	web_application	access_30DAY.log	access_combined_wcookie
>	2/26/24 10:56:31.000 PM	web_server	linux_s_30DAY.log	linux_secure
>	2/26/24 10:56:18.000 PM	web_server	linux_s_30DAY.log	linux_secure
>	2/26/24 10:56:02.000 PM	web_server	linux_s_30DAY.log	linux_secure

In this , we can observe , we are getting results for both web application and web server.

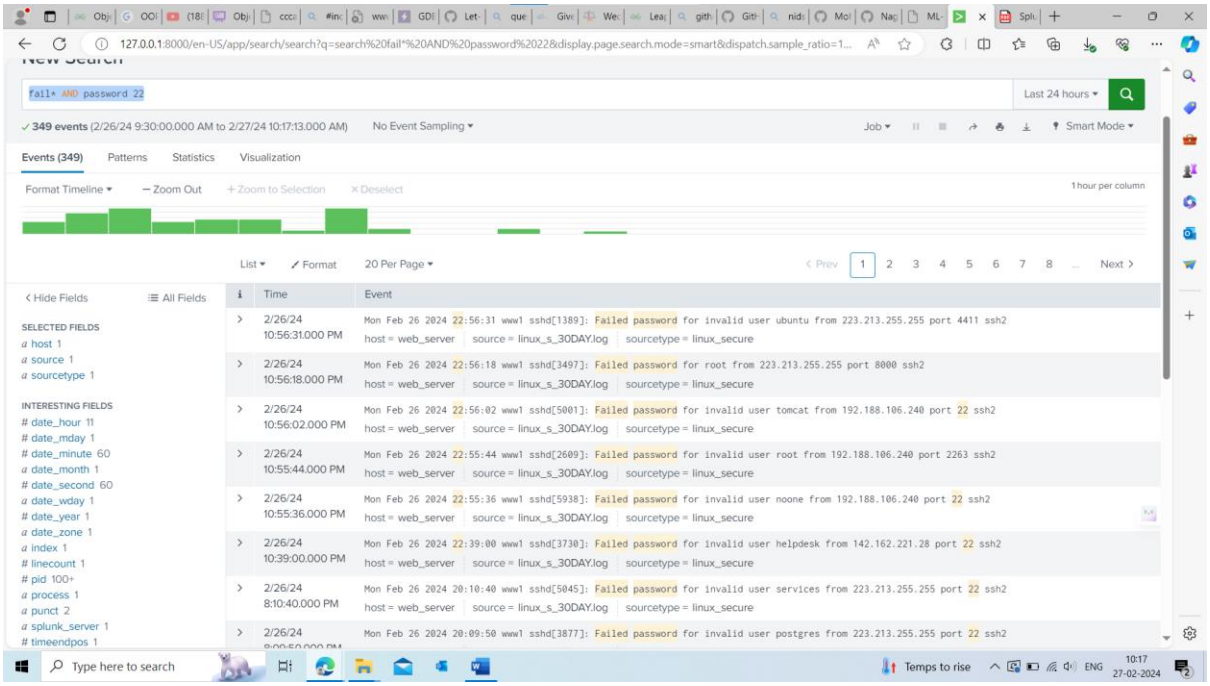
TASK 2: START A NEW SEARCH. NARROW YOUR RESULTS

2. Performing search with command : fail* AND password



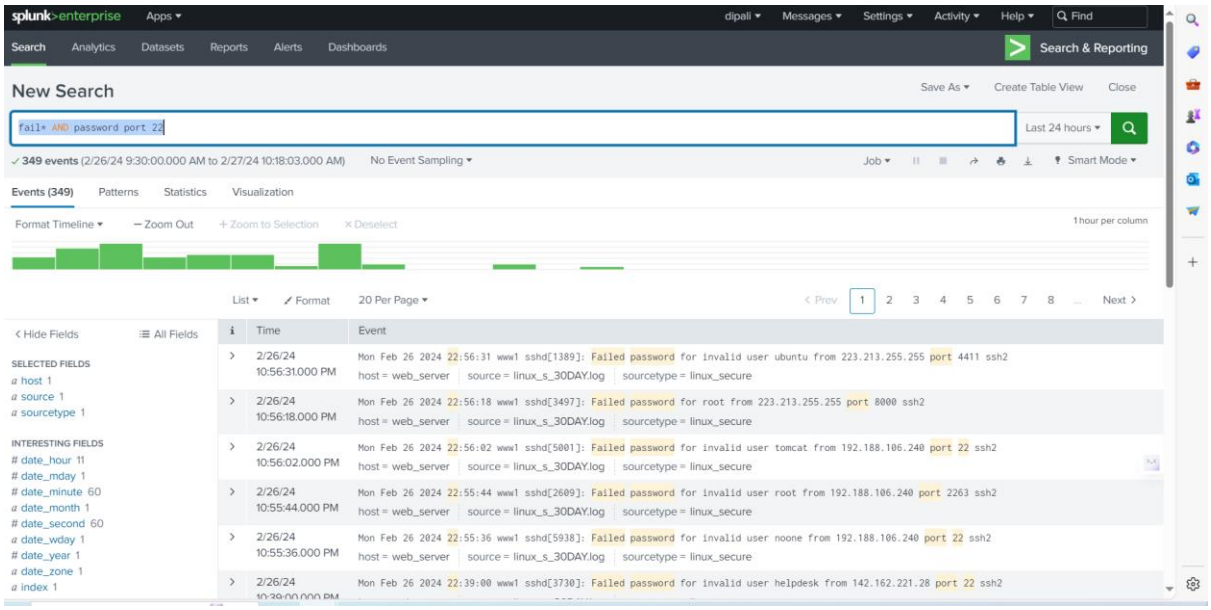
Review the results and notice the port values for a few of the events. You want to see users trying to log into the SSH port we have open, port 22.

3. Performing search with cmd : fail* AND password 22



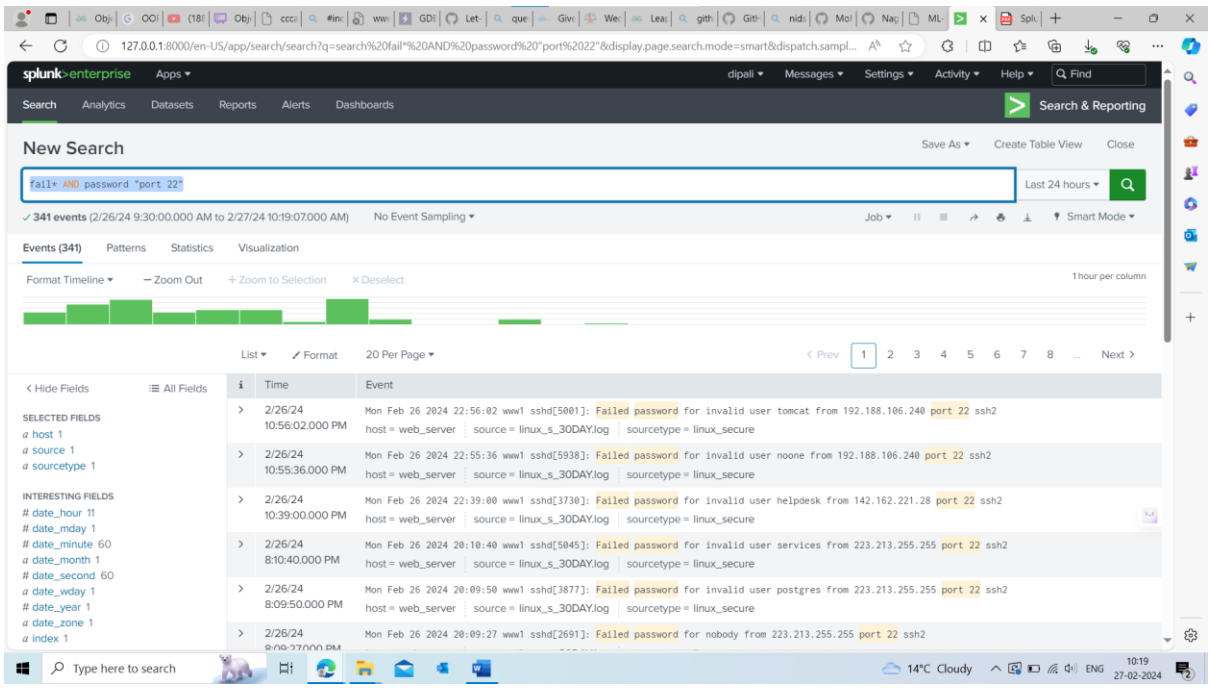
Notice that not only events with port 22 are selected, but any events with the number 22 in them.

4. Performing search with cmd : fail* AND password port 22



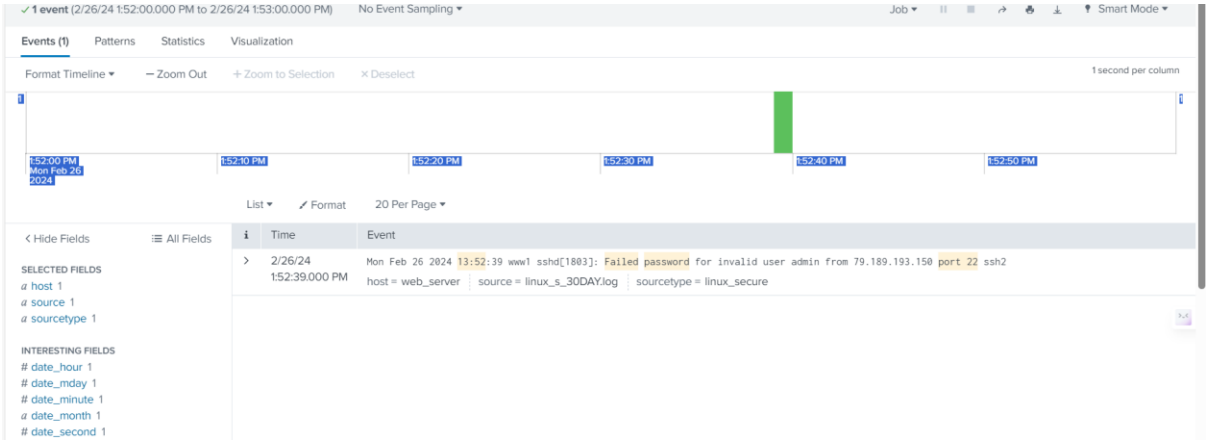
Notice that you are now only seeing events the entire phase.

5. Performing search with cmd : fail* AND password "port 22"



TASK 3: USE THE TIMELINE TO LOOK FOR TRENDS IN RESULTS.

6. Timeline :

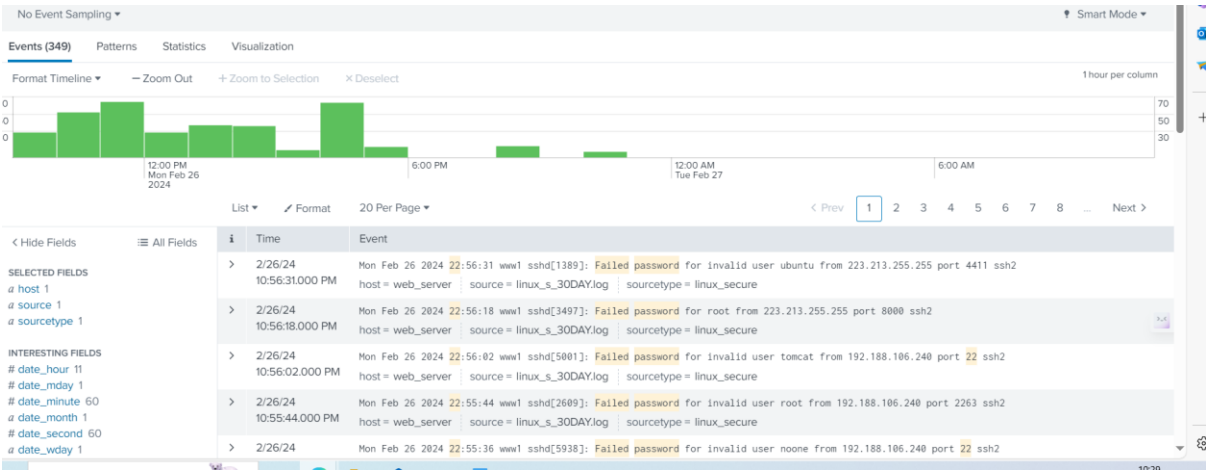


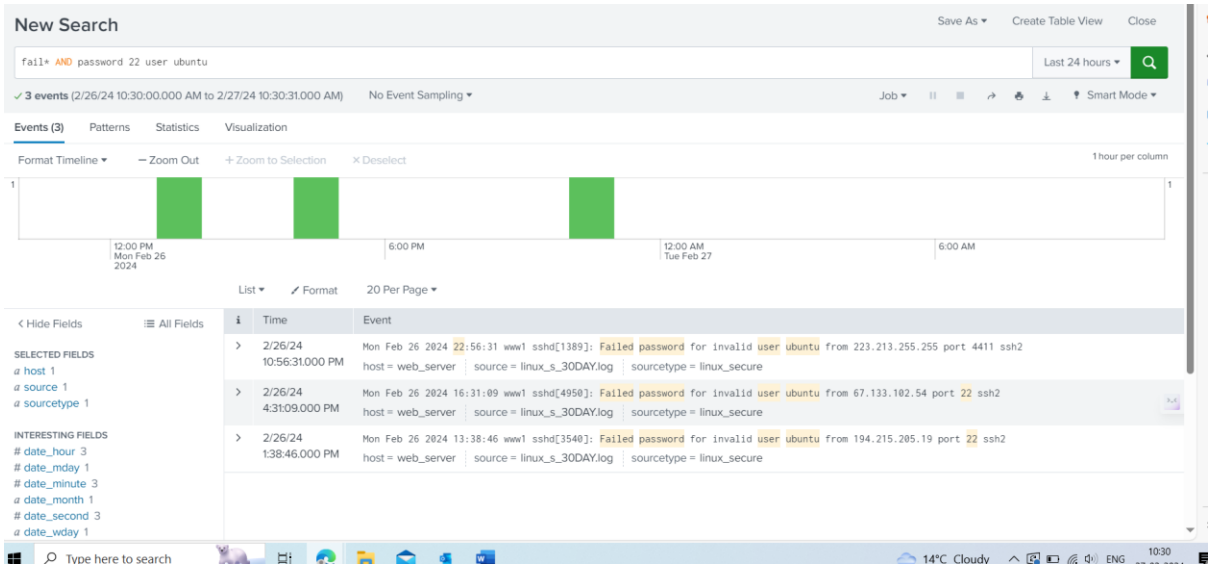
Single click another column. Look at these events. If there are spikes in events that look similar in time, your system may be the target of an attack. If there are no spikes, it has been a good month. Optionally, look at some of the events that were returned and see if you can spot any similarities in IP addresses or ports used.

TASK 4: USE THE OUTPUT OF YOUR SEARCH TO REFINE THE RESULTS.

Click one of the user names in the search results. Note that when you click a user name, a menu of options appears:

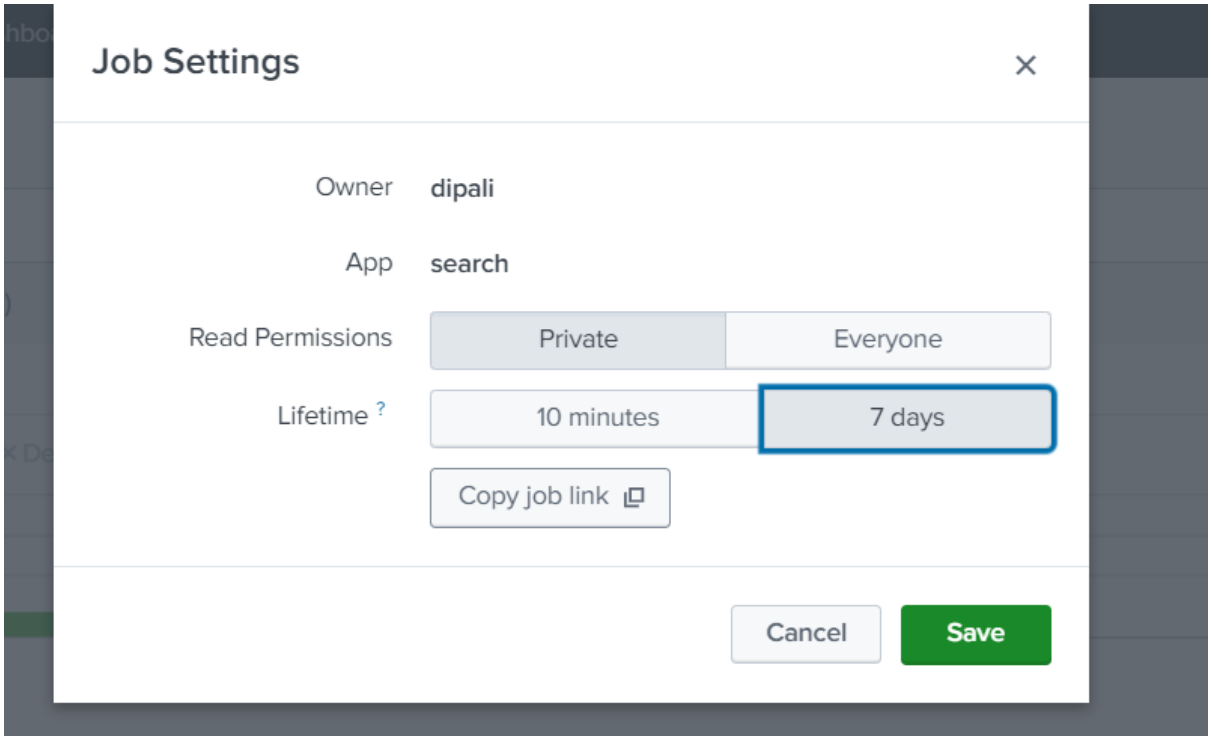
User – ubuntu



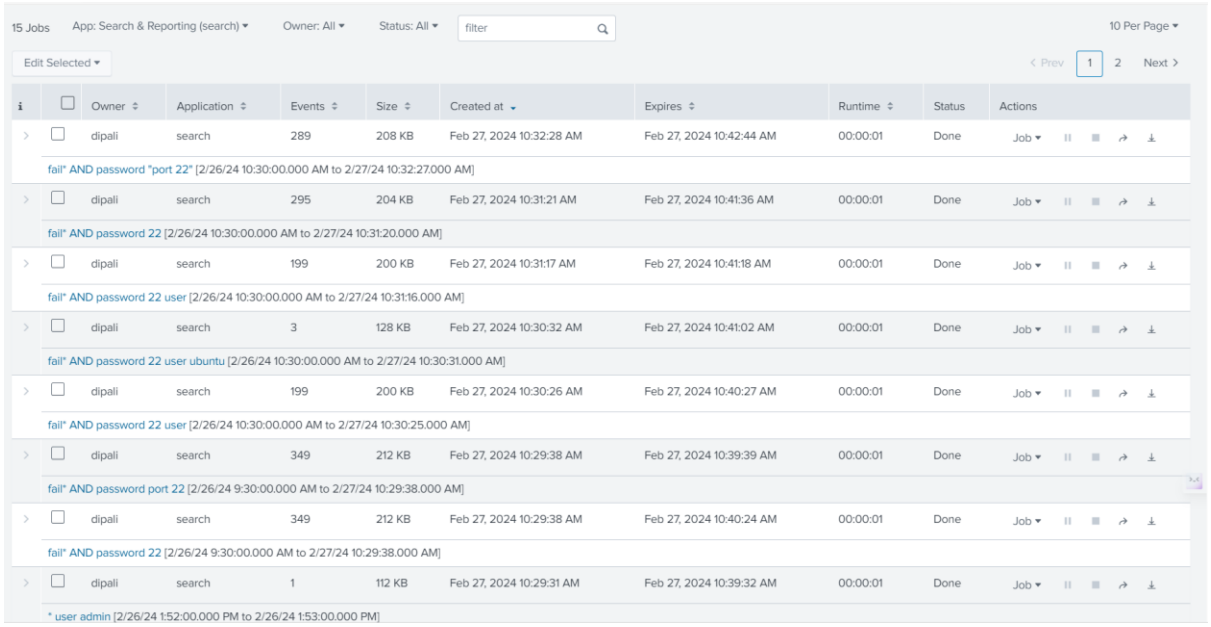


TASK 5: SAVE AND SHARE RESULTS. (EXTEND THE DEFAULT SAVE TIME. EXPAND DEFAULT VIEWING PERMISSIONS TO ALL.)

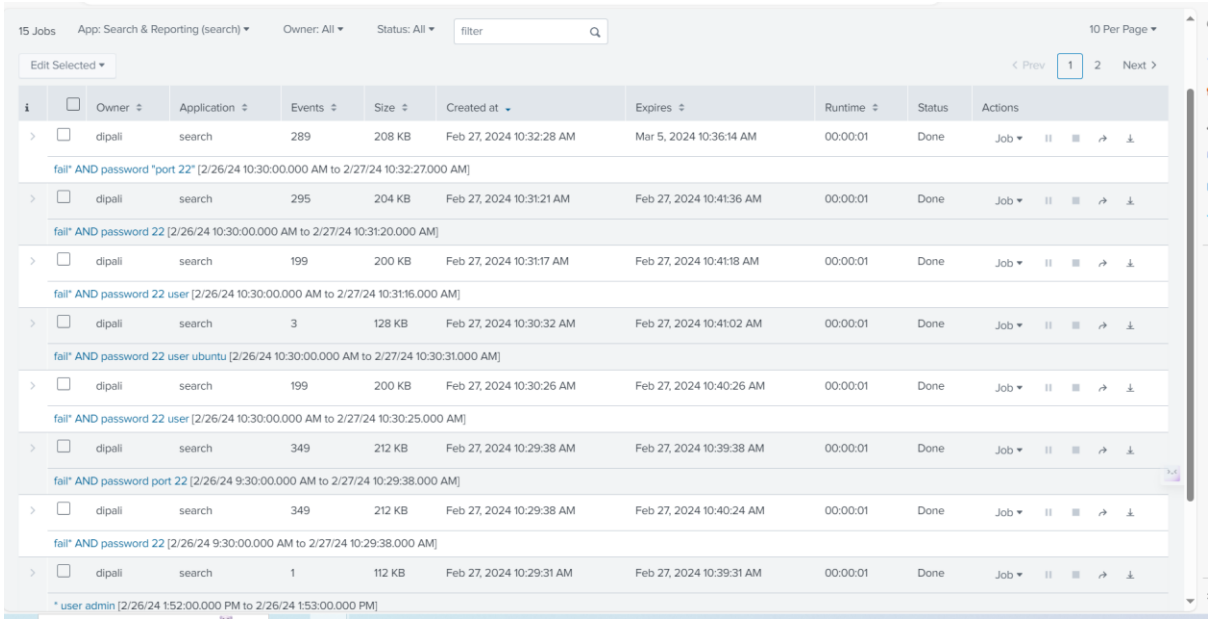
JOBS :



28: View your list of job histories from the Activity > Jobs menu (on the right side of the Splunk bar, which is the black bar at the top of the browser window).



29. Take a moment to review Owner, Events, Expires, Status, and Actions of the jobs. (Note that if a job is running, you can use the button – located under Actions - to stop it. This also sets the job status to Finalized.)

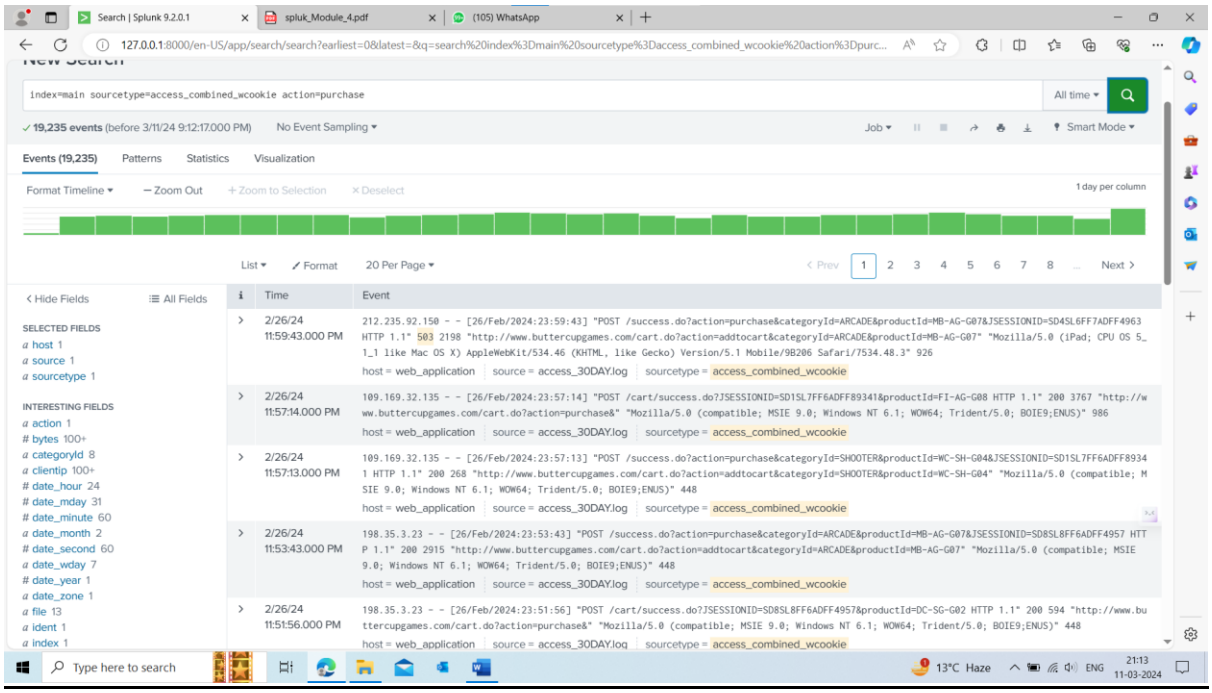


MODULE 4: USING FIELDS IN SEARCHES

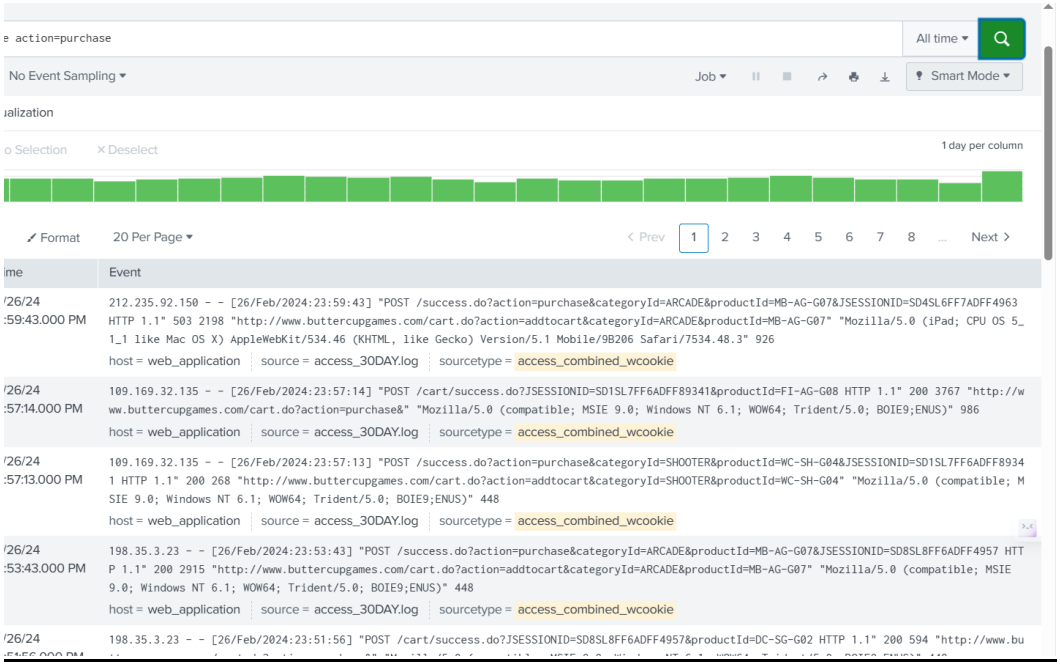
Task 1: Use the Fields sidebar to examine search results.

1. In the app navigation bar (i.e., the bar towards the top of the browser window,) click Search. If you do not see Search in the application bar – or to clear the previous search - click the App: Search & Reporting in the Splunk bar at the top of the browser window.
2. Search for index=main sourcetype=access_combined_wcookie action=purchase for All time.

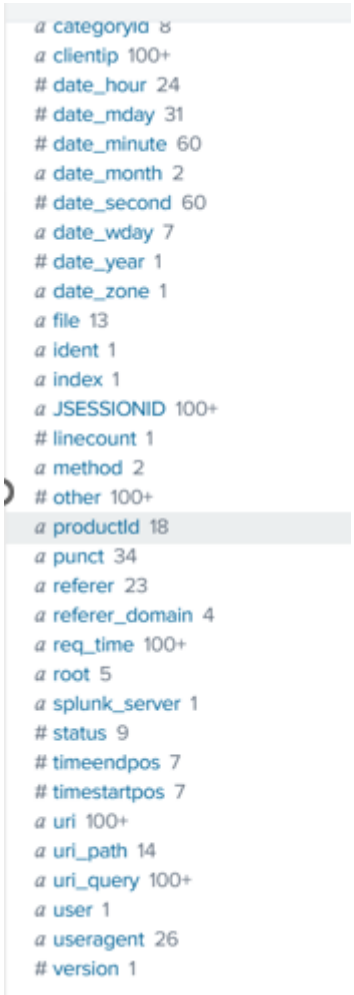
Solu: This returns all events where a purchase action was taken.



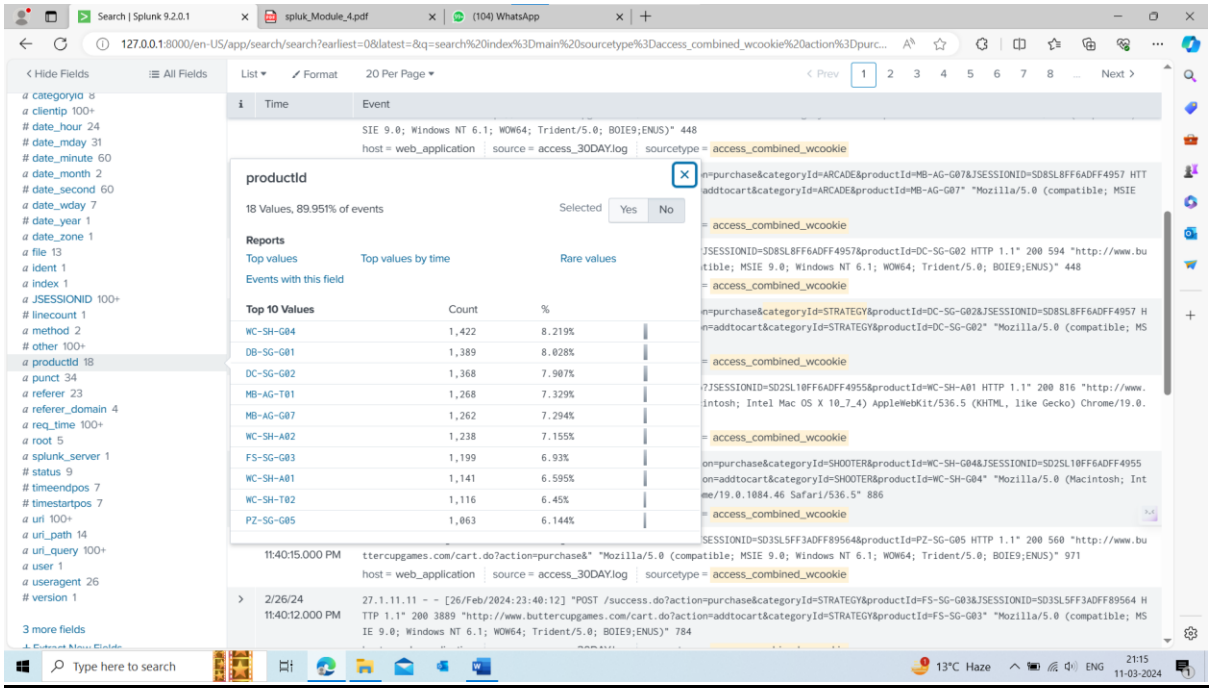
2. Verifying search executed in smart mode.



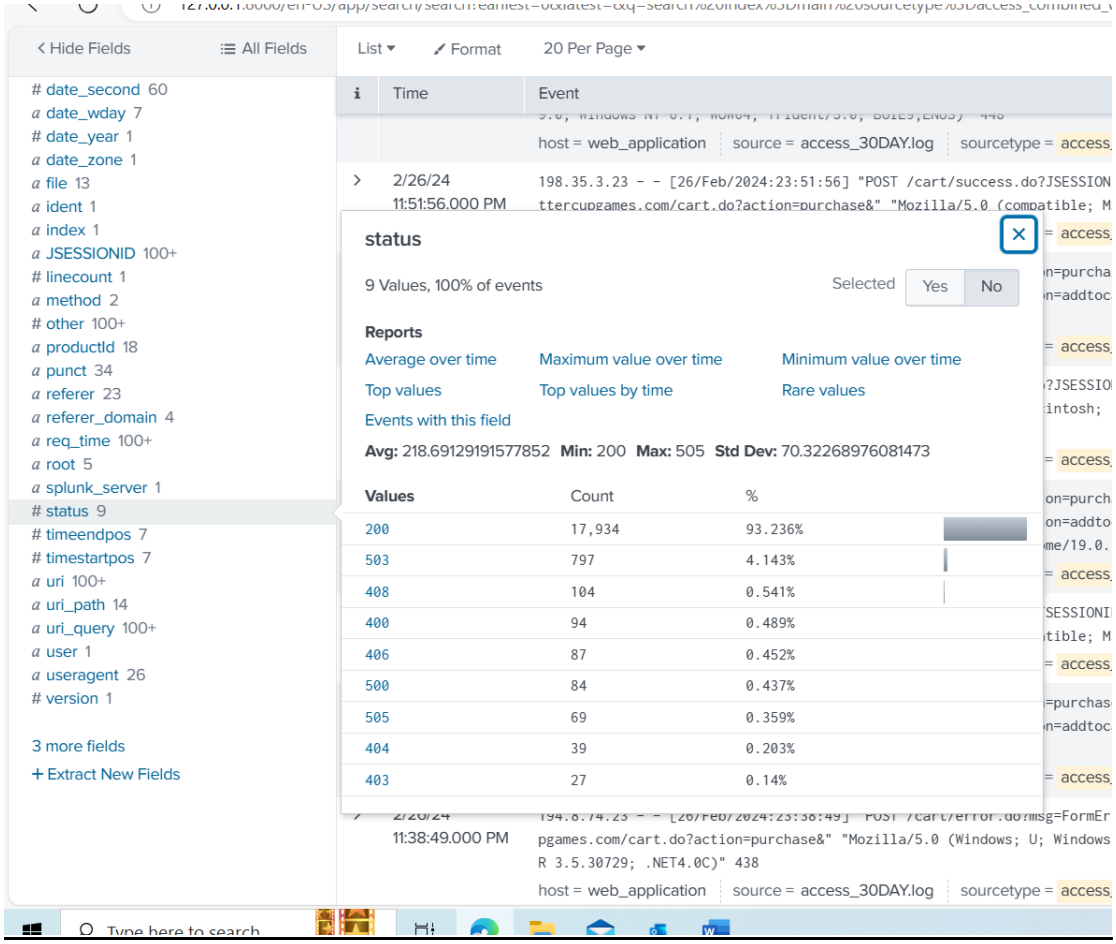
3. Sidebar's Interesting Fields list. ProductId is one of the fields extracted by Splunk.



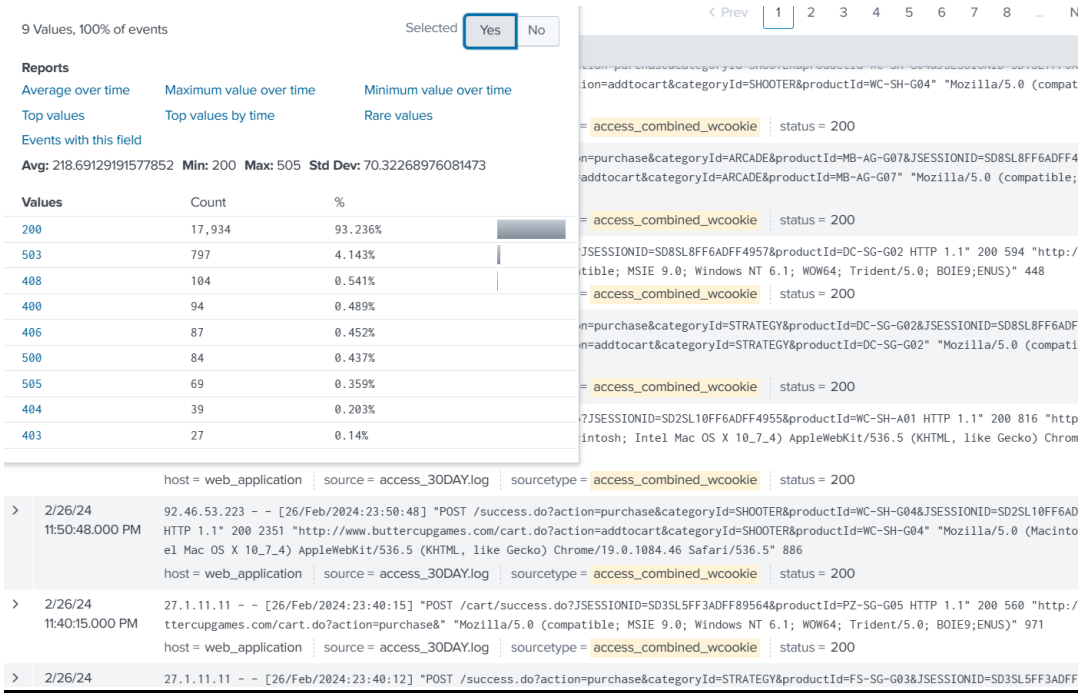
4. Product ids of ten purchased products



5. Click Status : This field contains the status of the web request. Anything greater than 200 means that the customer interaction ended in an error, and the purchase was not made



6. We can select the status by clicking on it, it will show all the status for each entry.

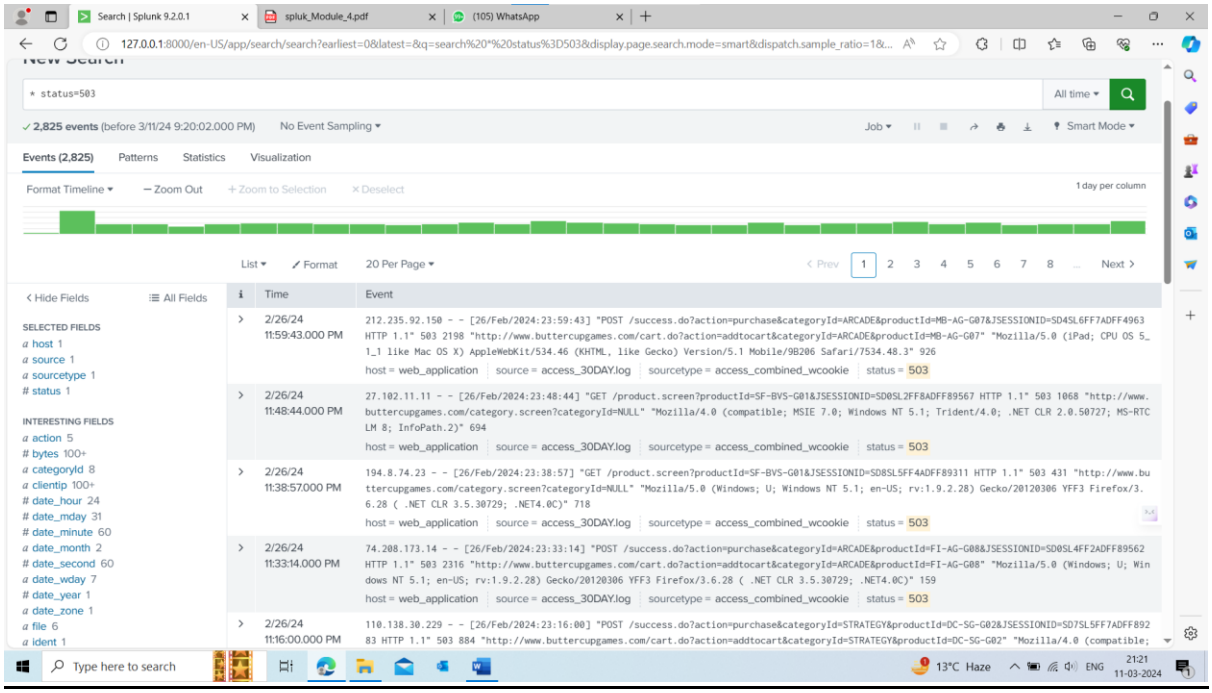


7. We can status for each entry.

Time	Event
2/26/24 11:59:43.000 PM	212.235.92.150 - - [26/Feb/2024:23:59:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 503 2198 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 926 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
2/26/24 11:57:14.000 PM	109.169.32.135 - - [26/Feb/2024:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
2/26/24 11:57:13.000 PM	109.169.32.135 - - [26/Feb/2024:23:57:13] "POST /success.do?action=purchase&categoryId=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
2/26/24 11:53:43.000 PM	198.35.3.23 - - [26/Feb/2024:23:53:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 2915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
2/26/24 11:51:56.000 PM	198.35.3.23 - - [26/Feb/2024:23:51:56] "POST /cart/success.do?JSESSIONID=SD8SL8FF6ADFF4957&productId=DC-SG-G02 HTTP 1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200

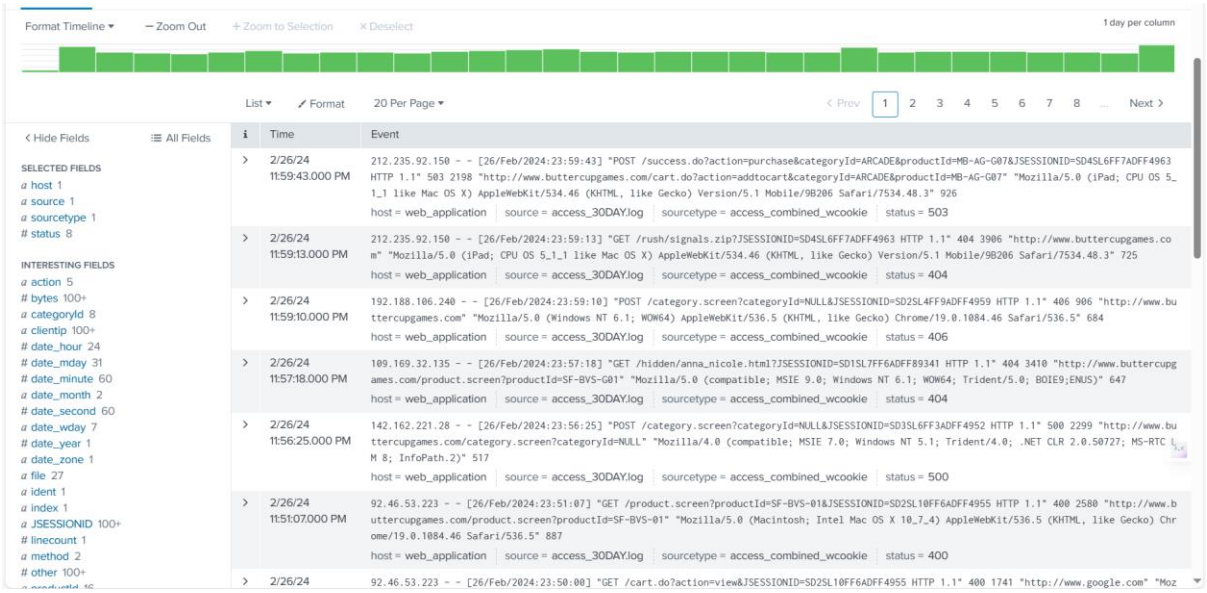
8.For adding a new search, add and select a status and add to new search , the results displayed are:

In the Fields sidebar, under Selected Fields, click the status field. From the field window, click the value with the highest number (listed at the top). Notice the field and value have been added to the search criteria in the search bar. Also, this selection causes a new search to be executed using the new search criteria.

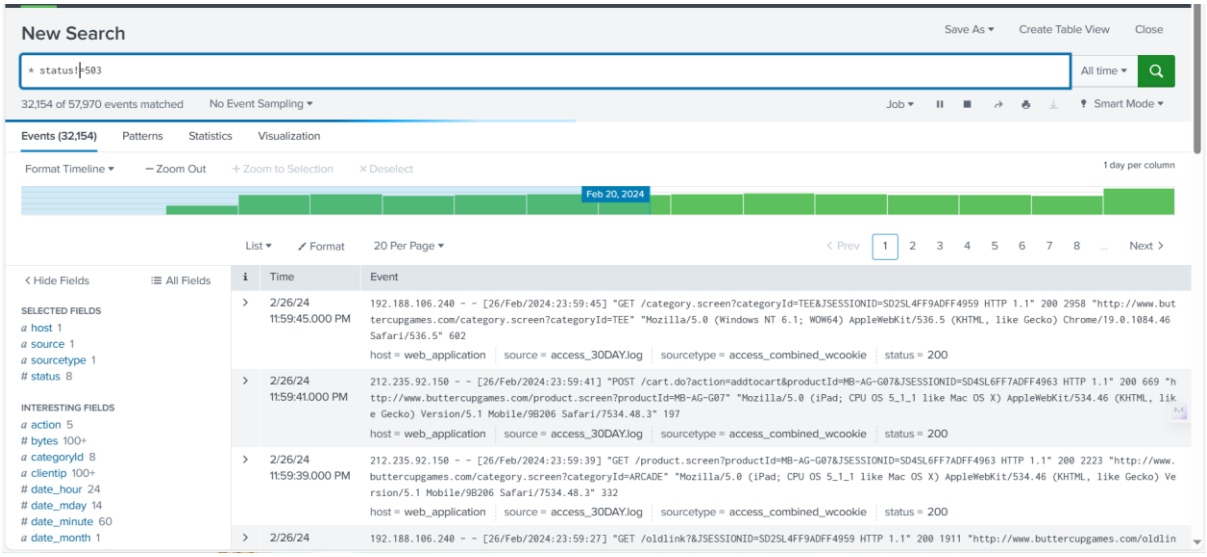


9. Since the value that shows up in the most results is 200, you are not seeing the server errors. Changing the comparison operator will correct this.

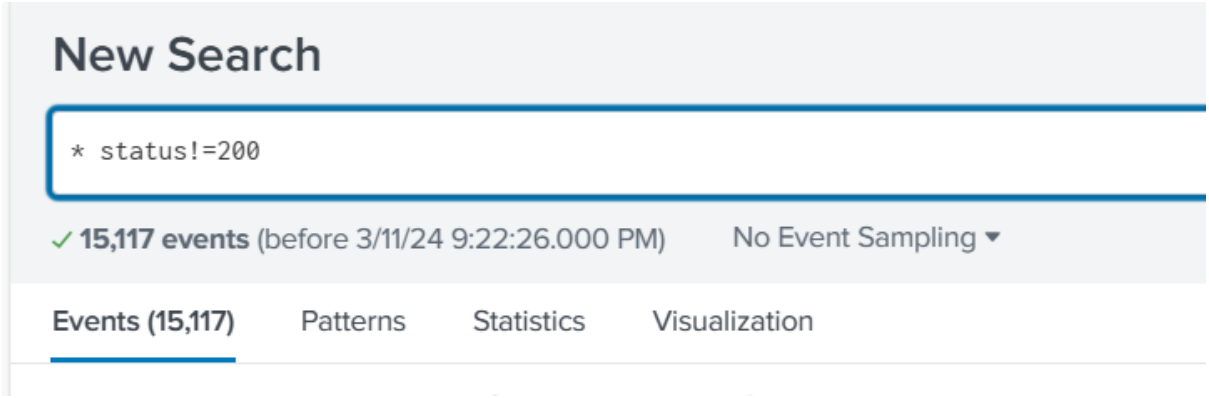
10. For searching status !=200;



11.After searching for status not equal to 503.



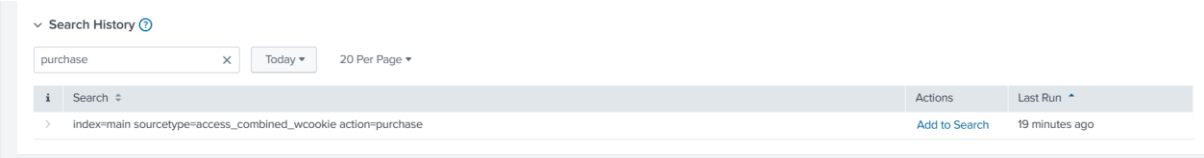
12. No of searches which ended in errors are:



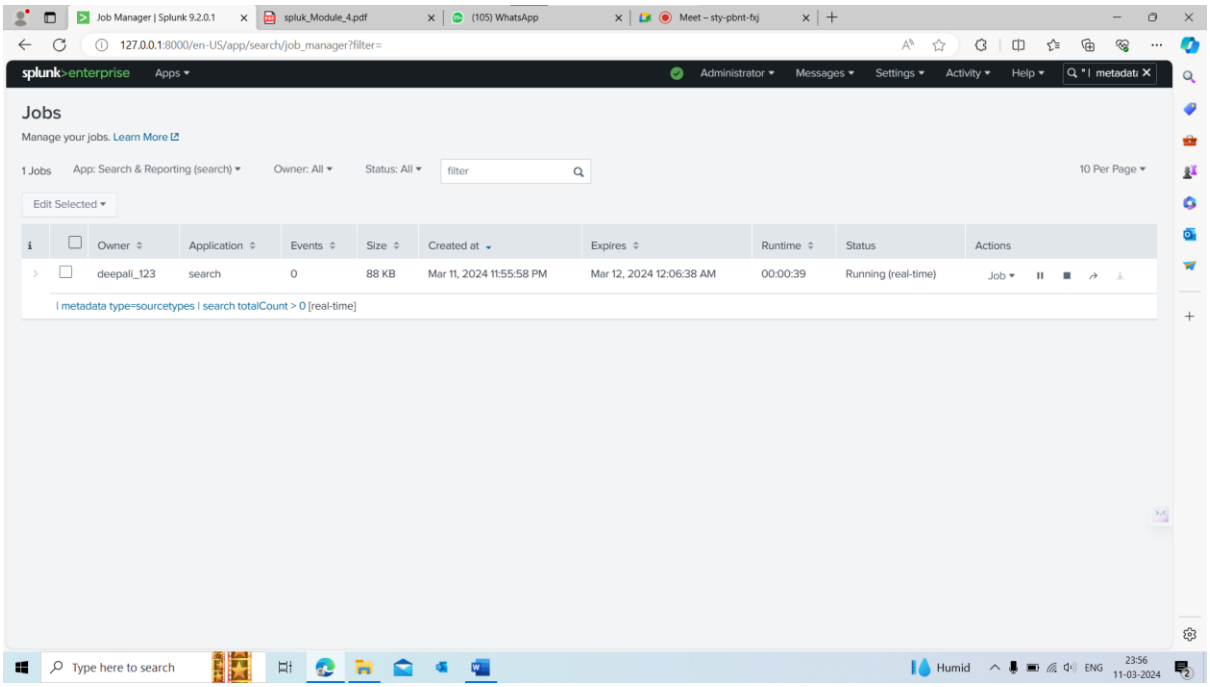
13. In the Fields sidebar, click status again and select No in the upper right corner next to Selected. This will remove it from the Selected Fields list. Click the x in the upper right corner to close the field window. Click the search link in the Splunk Bar to clear the search results.

Task 2: Use Search History to browse previously run searches.

14. Search history:



15. Click inside the Search History filter box, and type purchase. Notice the search list is shortened. Only the searches that contain the word purchase remain.

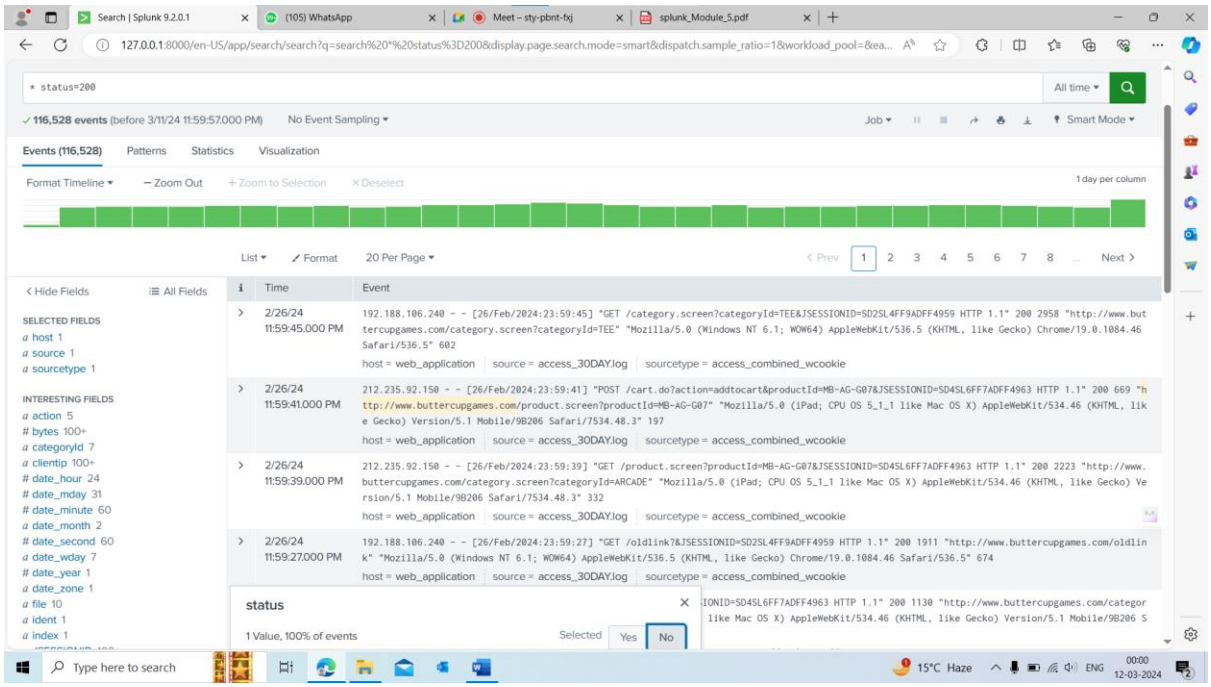


MODULE 5: BASIC COMMANDS

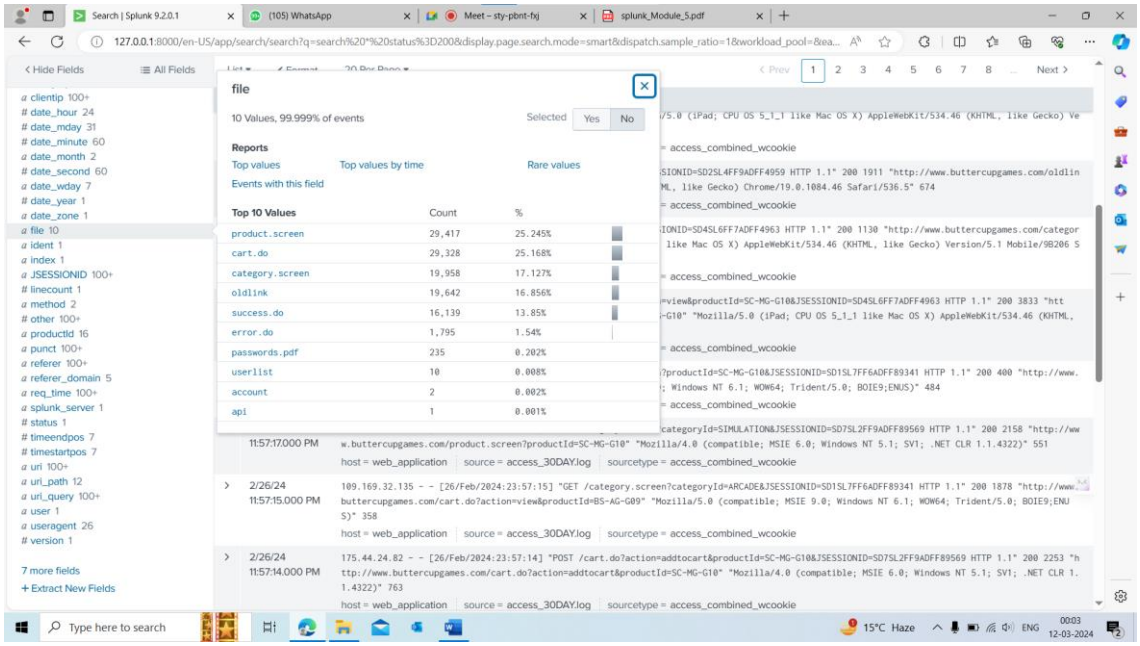
Task 1: Search for the requested data.

1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)
2. Enter a search that returns all web application events that include a purchase action with a web status of 200.

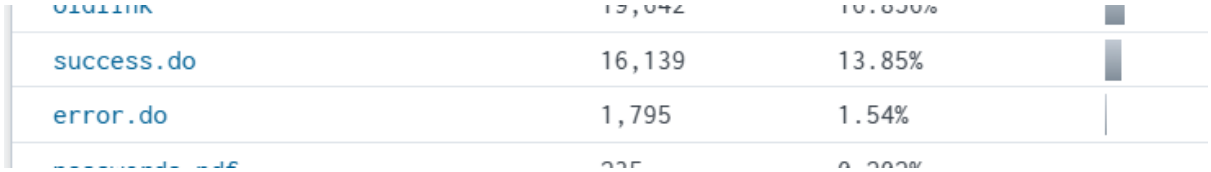
Command : index=main sourcetype=access_combined_wcookie action=purchase status=200



3. Select the file field in the Interesting Fields list.



4. Two files :error.do and success.do, Notice that there are two different files that were returned from the web server. They are: error.do and success.do. Our web development team informs us that the success.do is served when the order is processed and error.do is served when there is an error with the information being processed.



5. The team is only looking for successful purchases, so change your search to only return those.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do)

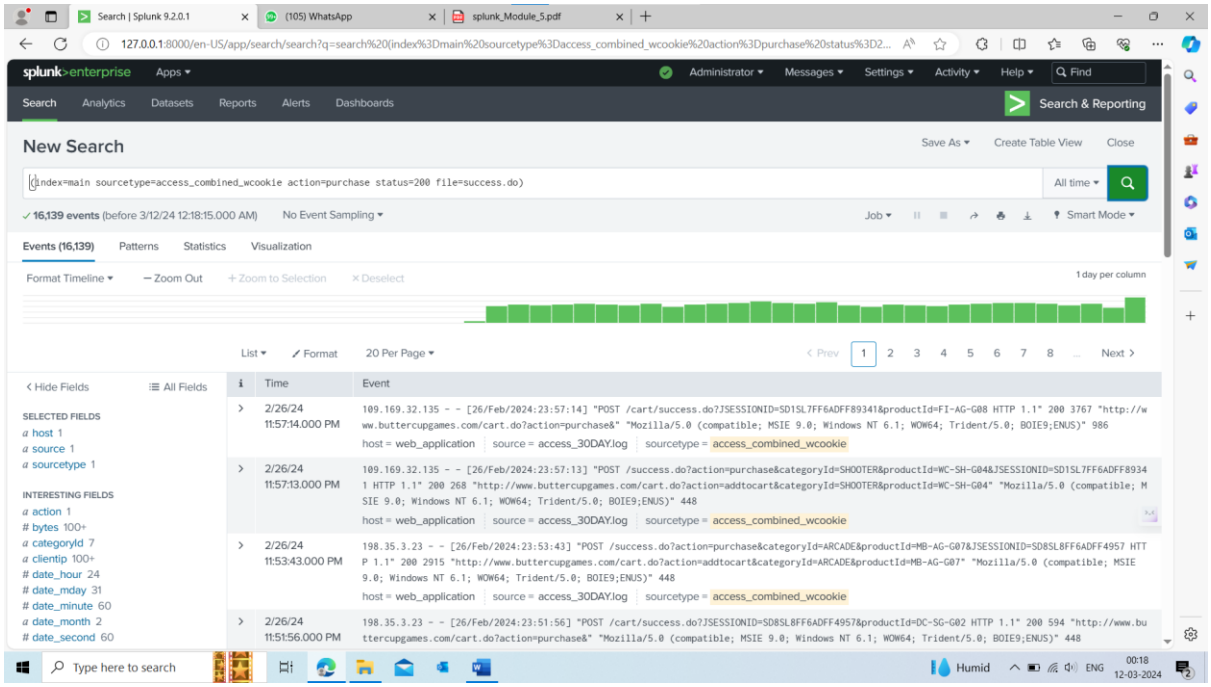
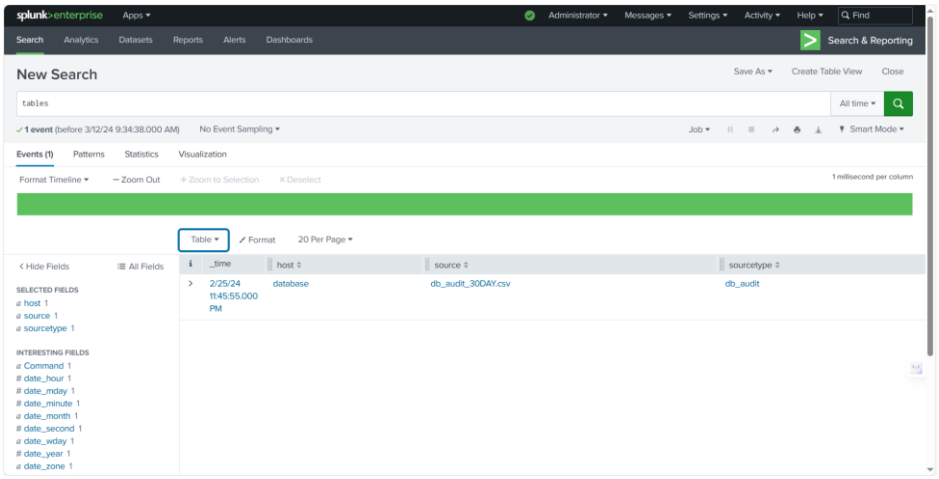
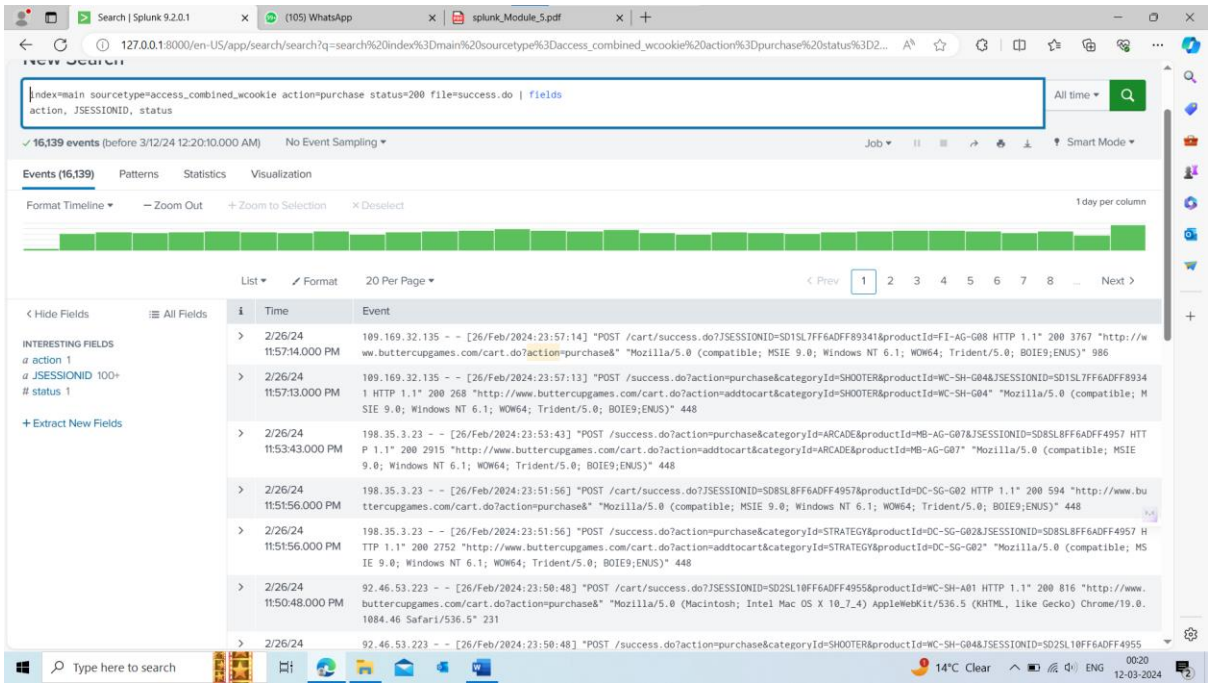


TABLE :



6. You will see fields that do not matter to the team. Use the fields command to only return the action, JSESSIONID and status fields. Does your search run faster using the command?
Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields action, JSESSIONID, status)



7. The fields list looks cleaner, but seeing the events like this might still be confusing for the team.

Task 2: Put the data into an easy to read table.

8. Replace the fields command with the table command to display the data as a table.

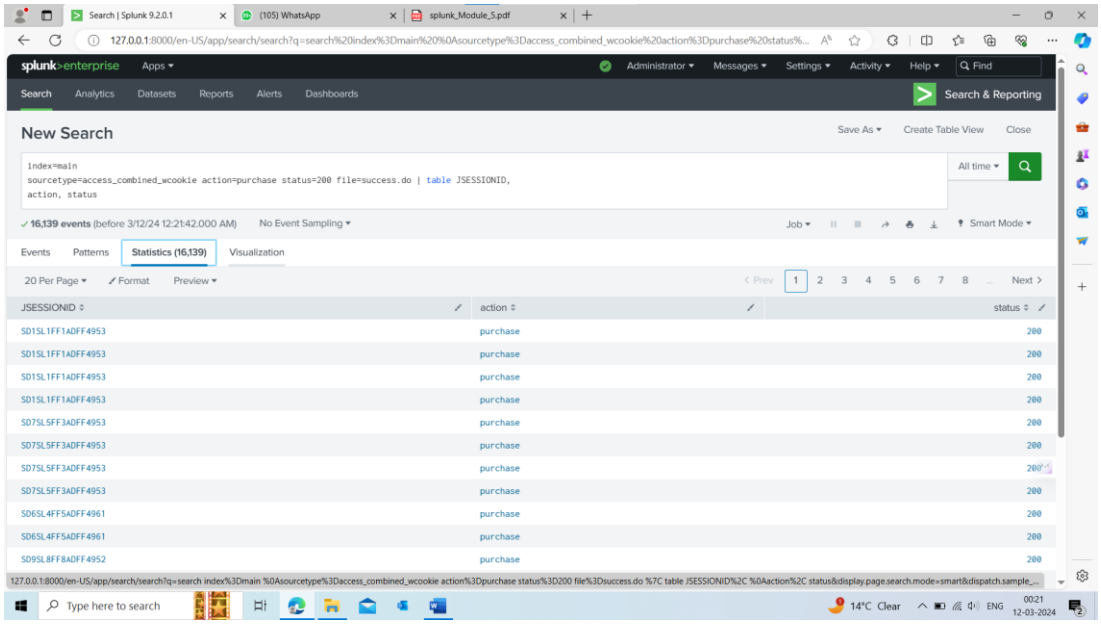
Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table action, JSESSIONID, status).

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

action	JSESSIONID	status
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200

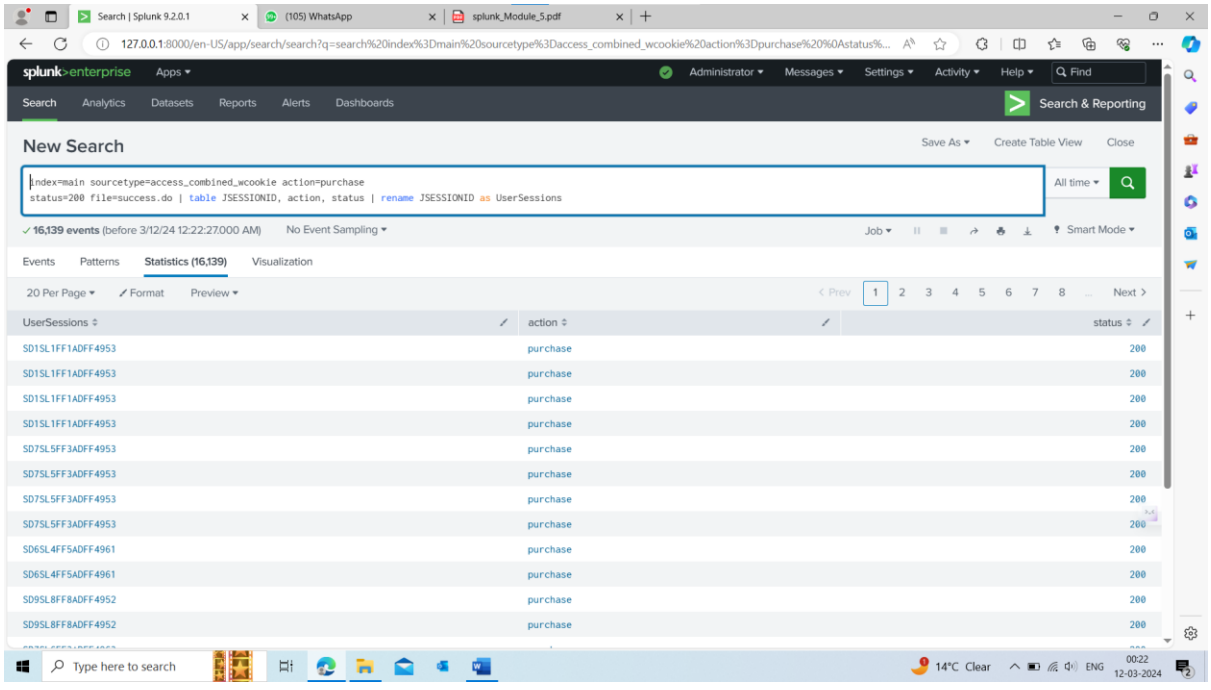
9. Change the order of the fields so that JSESSIONID is the first column.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status)



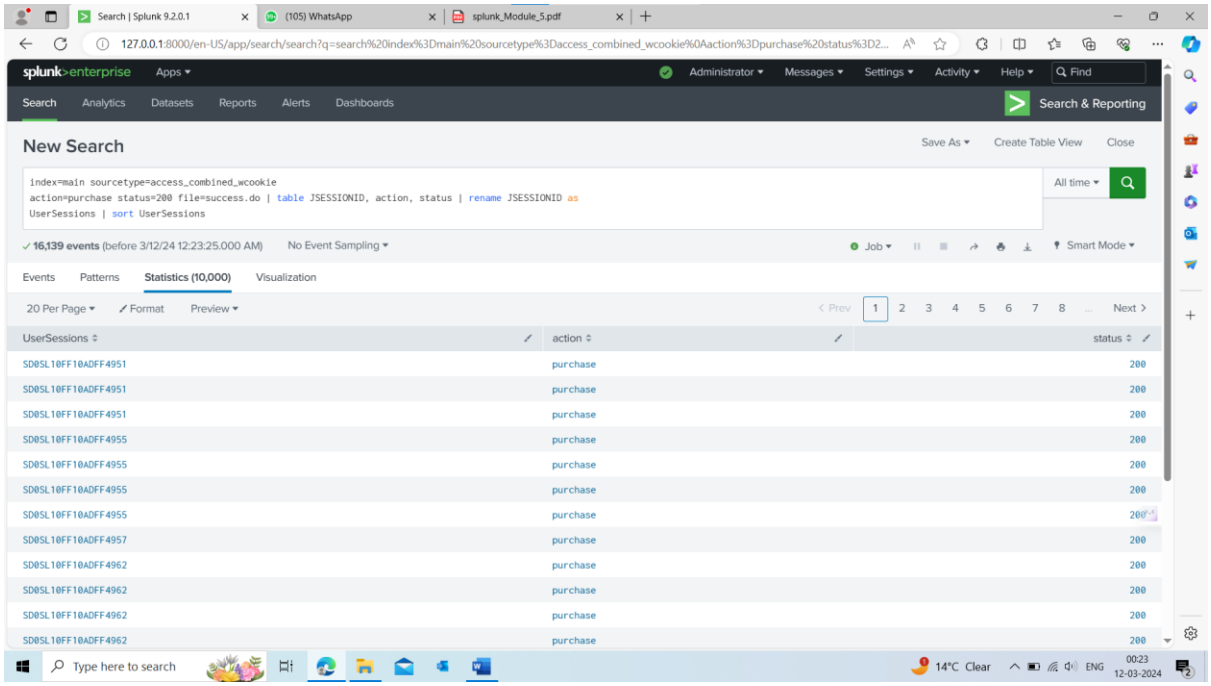
10. Session IDs are called "UserSessions" in the marketing data. Rename JSESSIONID so that your report matches the marketing data.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions)



11. Sort UserSessions using the sort command.

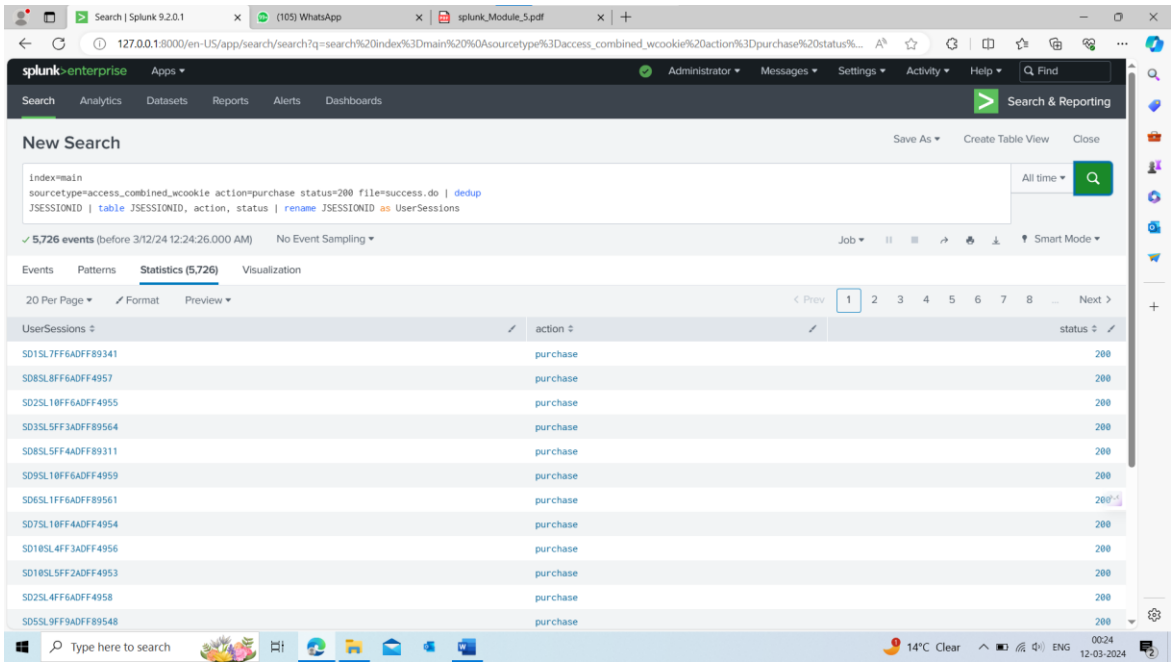
Command: (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions | sort UserSessions)



12. Notice that some UserSessions values show up multiple times. Also notice the number of events returned on the Statistics tab.

13. Remove the sort command and use dedup to remove any identical session values.

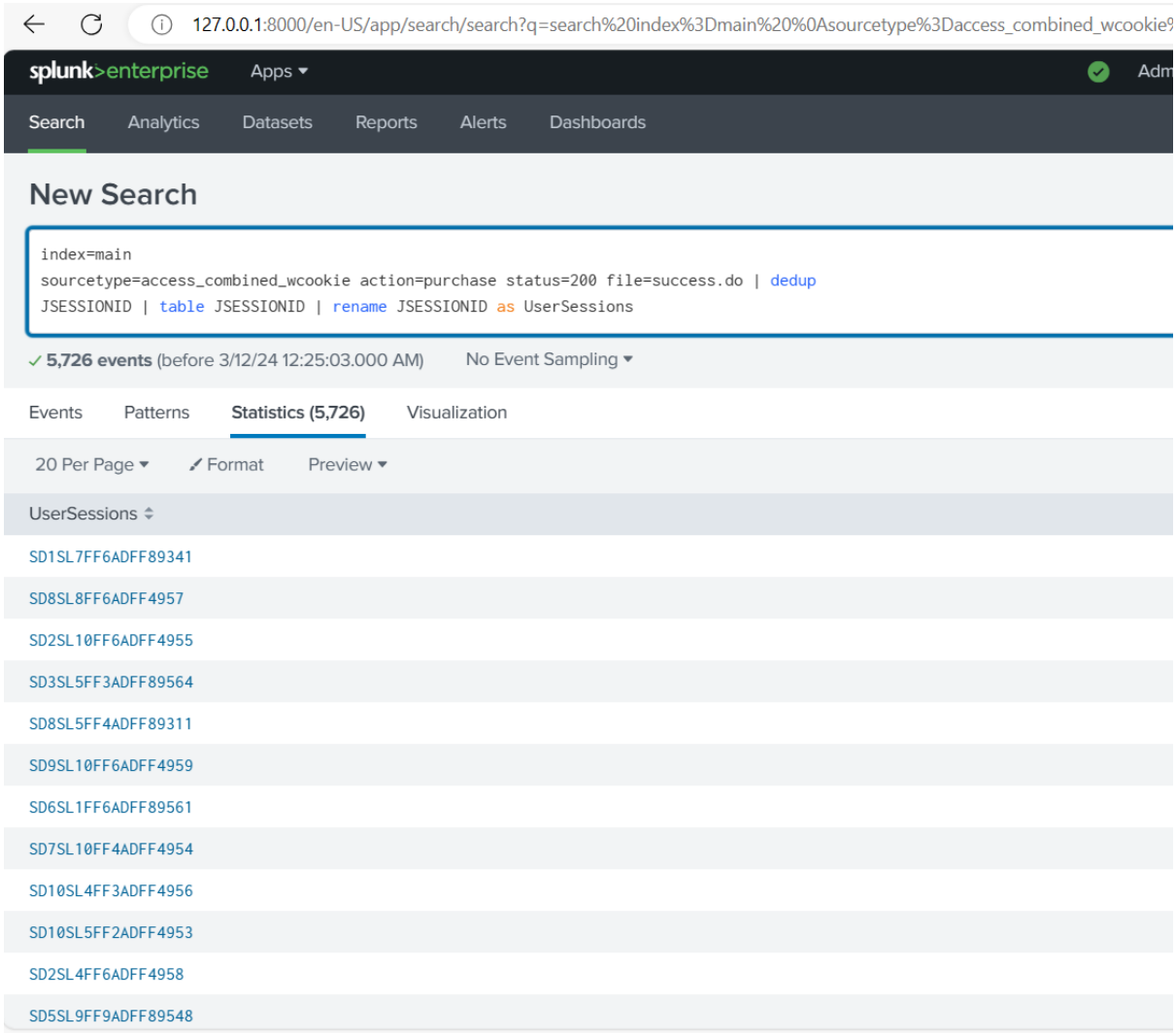
Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID, action, status | rename JSESSIONID as UserSessions)



14. How many events are now listed on the Statistics tab?
Ans : 5726

15. While having action and status fields displayed was nice for a sanity check of the data, the marketing team will not need to have these displayed. Remove them from your table display.

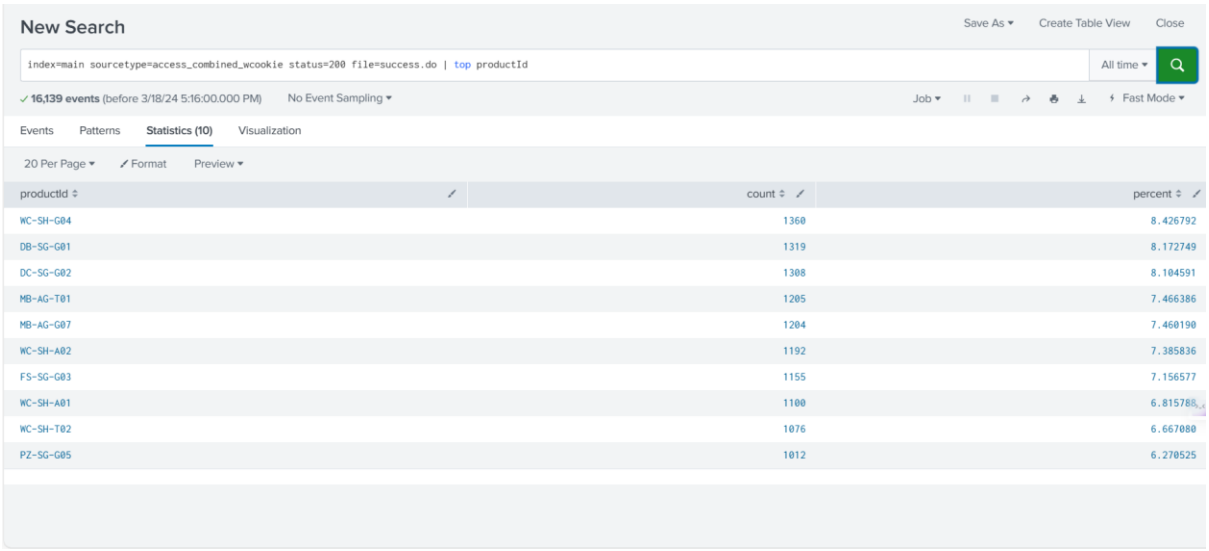
Command :(index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID | rename JSESSIONID as UserSessions)



MODULE 6 : TRANSFORMING COMMANDS

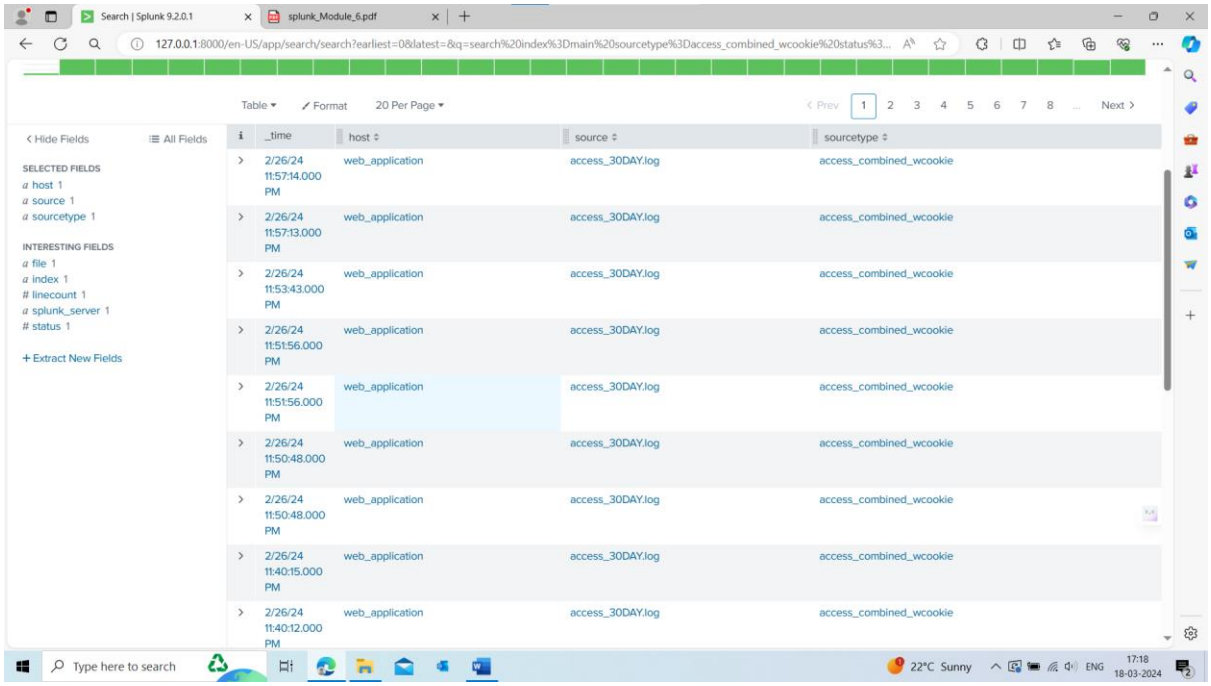
Task 1: Use the top command to get a list of the best-selling products.

1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.



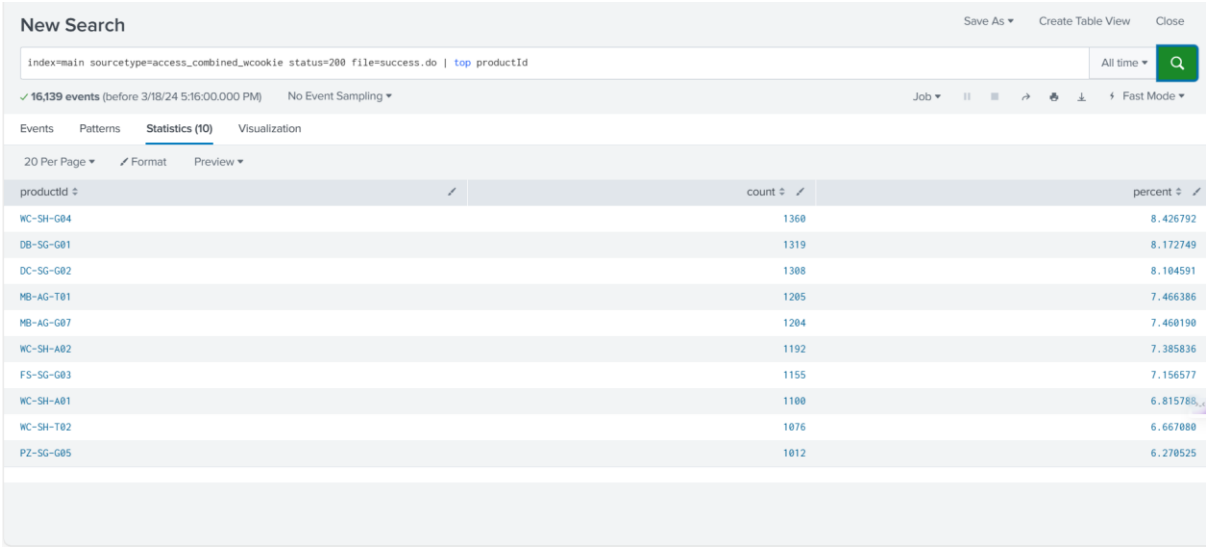
2. Enter a search that returns all web application events where an item was successfully purchased. Remember that if the success.do file is successfully returned to a user, a purchase was made.

Command : index=main sourcetype=access_combined_wcookie status=200 file=success.do



3. Use the top command to find the best-selling productIds for all time

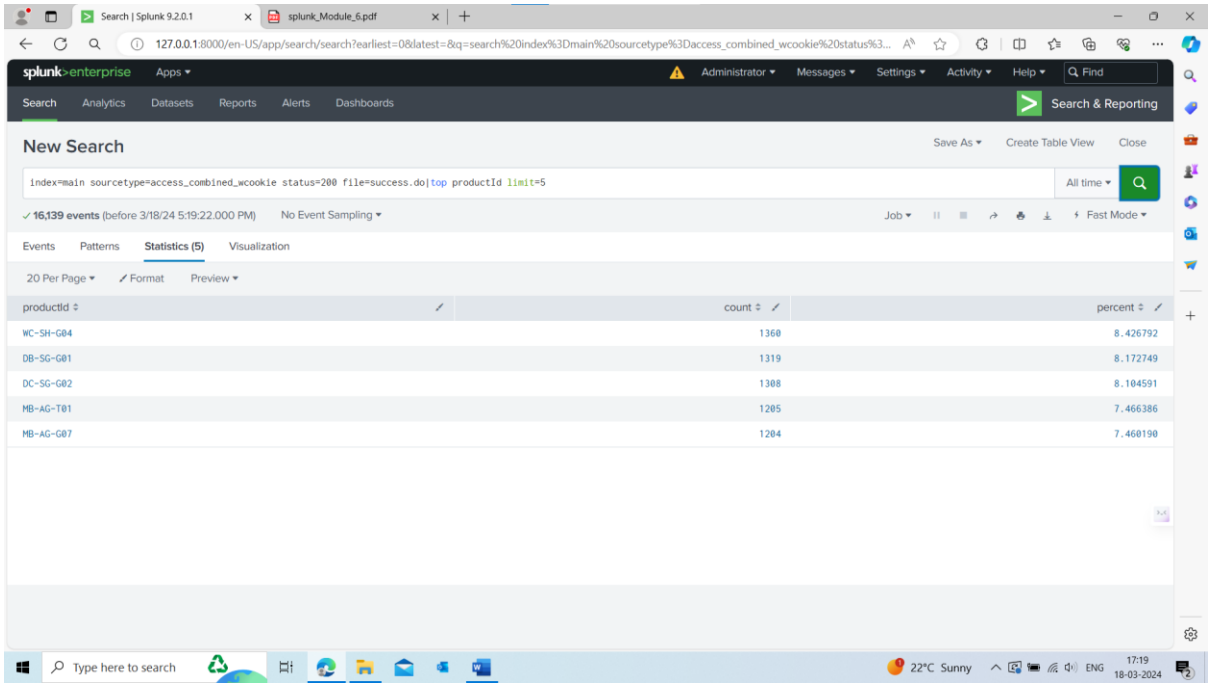
Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId



4. Notice that ten rows were returned. You were asked to only return the top 5.

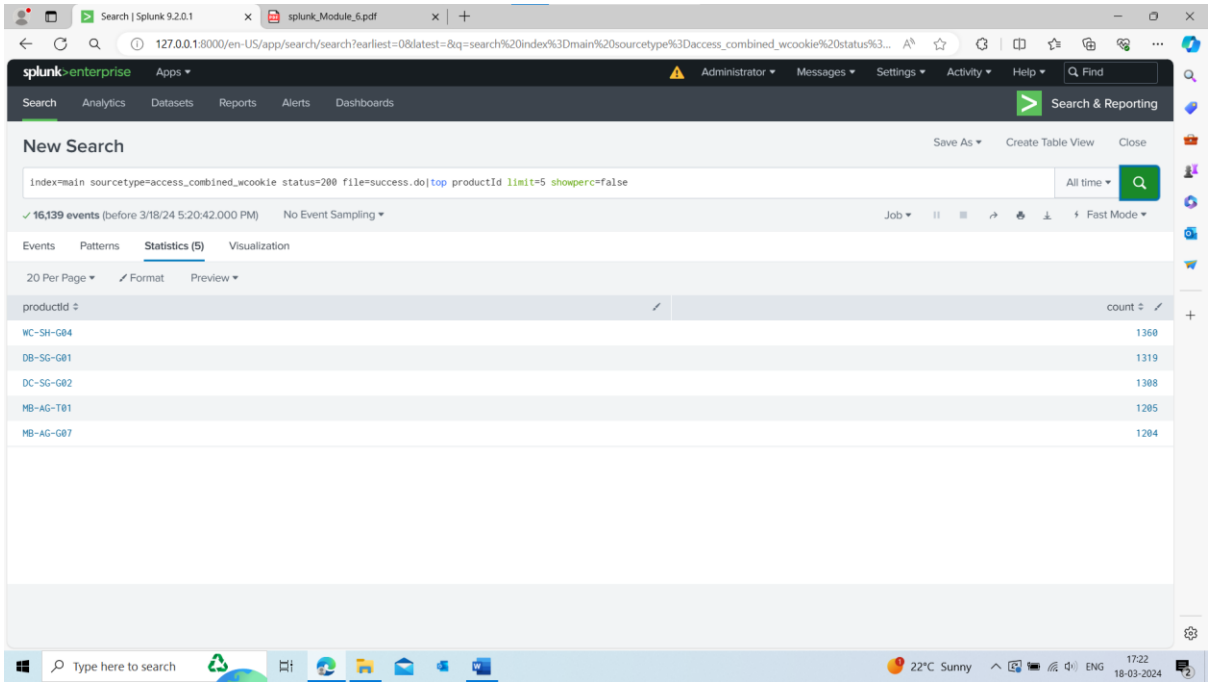
5. Use the limit argument to only return the number of rows requested.

Command: index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId limit=5

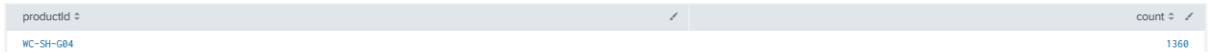


6. Use the showperc option of top to remove percent from the display.

Command : index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId limit=5 showperc=false



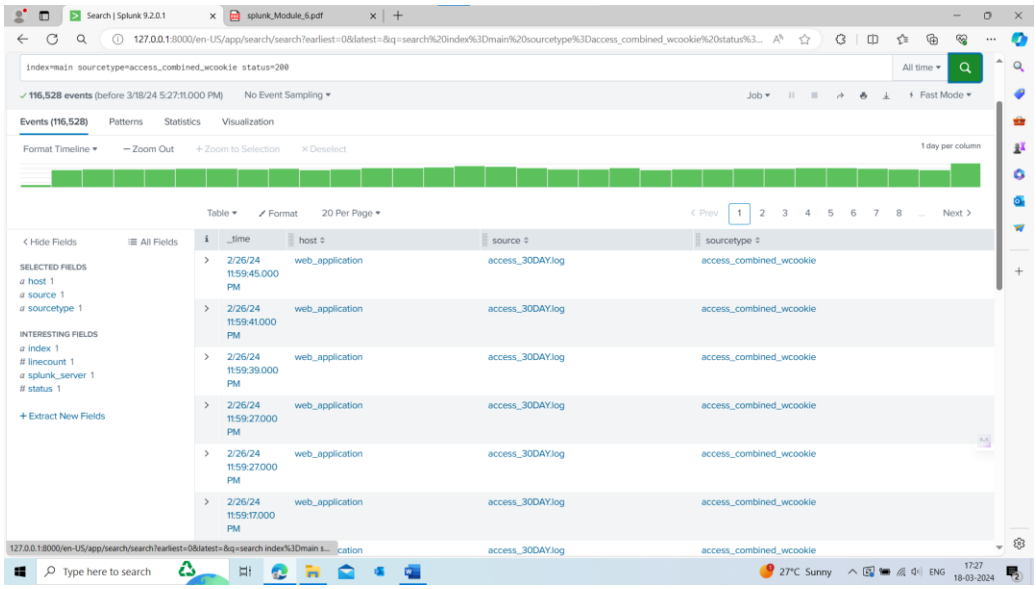
7. what is the productId of the best-selling product? Please take note as it might be in the quiz. (WC-SHG04)



<u>Task 2: Use the rare command to see what files get accessed the least amount in our web application</u>

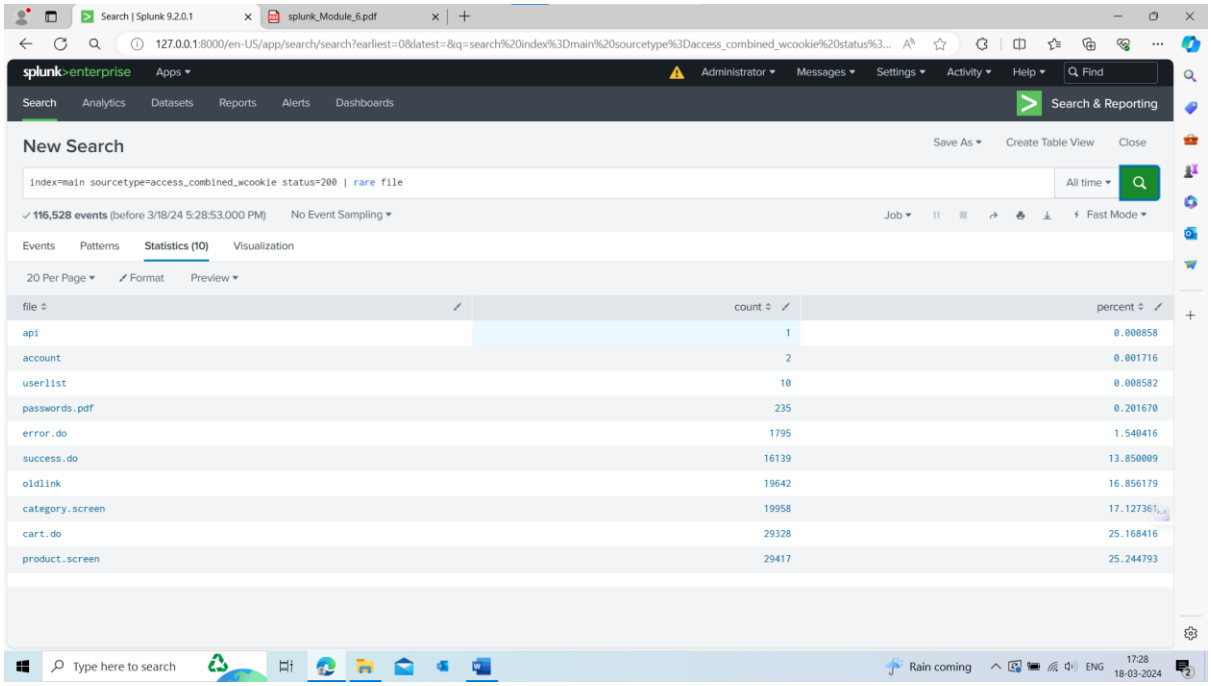
8. Enter a search that returns all web application events where a file was successfully served to the user.

Command : (index=main sourcetype=access_combined_wcookie status=200)



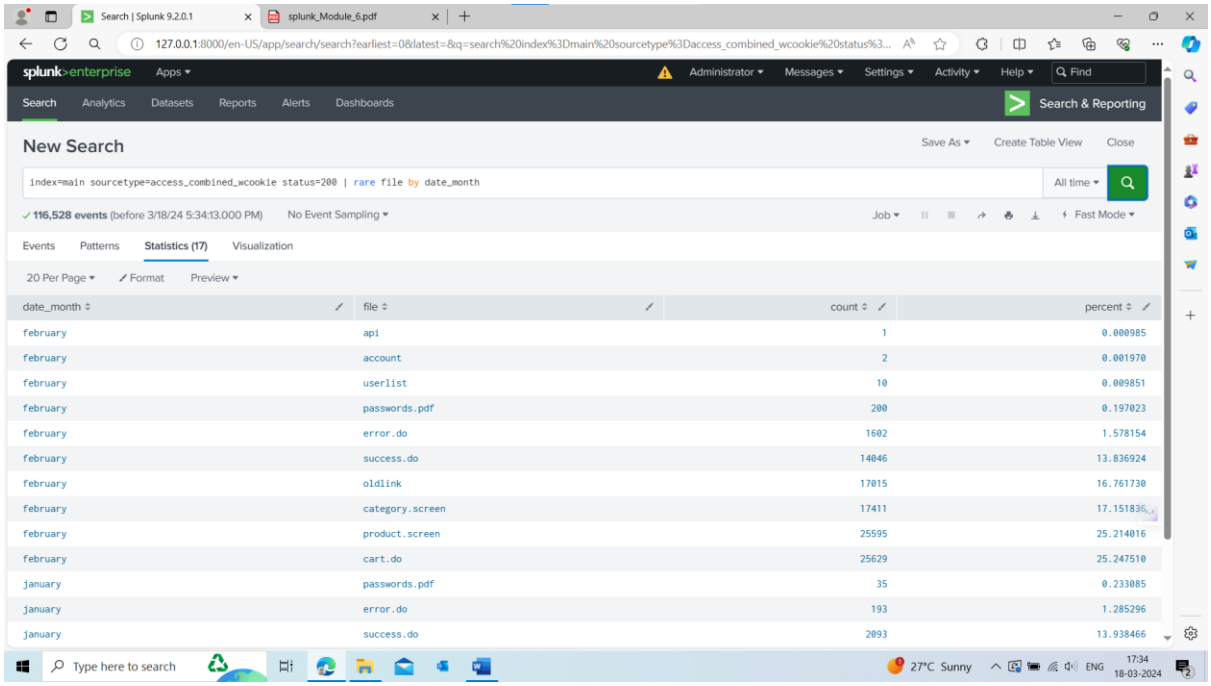
9. Use the rare command to find the files that show up the least amount of times in our events.

Commands : (index=main sourcetype=access_combined_wcookie status=200 | rare file)



10. Do you see anything that might be of a concern for the security team? Make the report even more granular using the by clause to split the rare events by the month in which they happened (date_month).

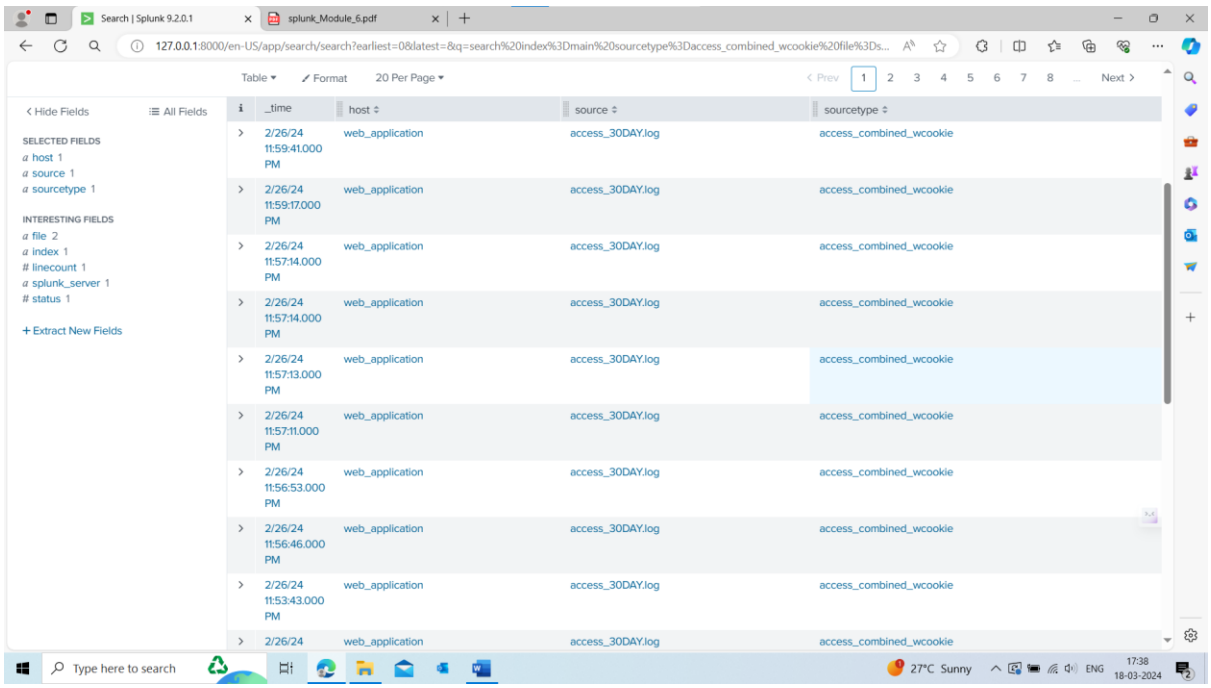
Command - index=main sourcetype=access_combined_wcookie status=200 | rare file by date_month



Task 3: Use the count function of the stats command to find out how many items were added to a cart versus being purchased

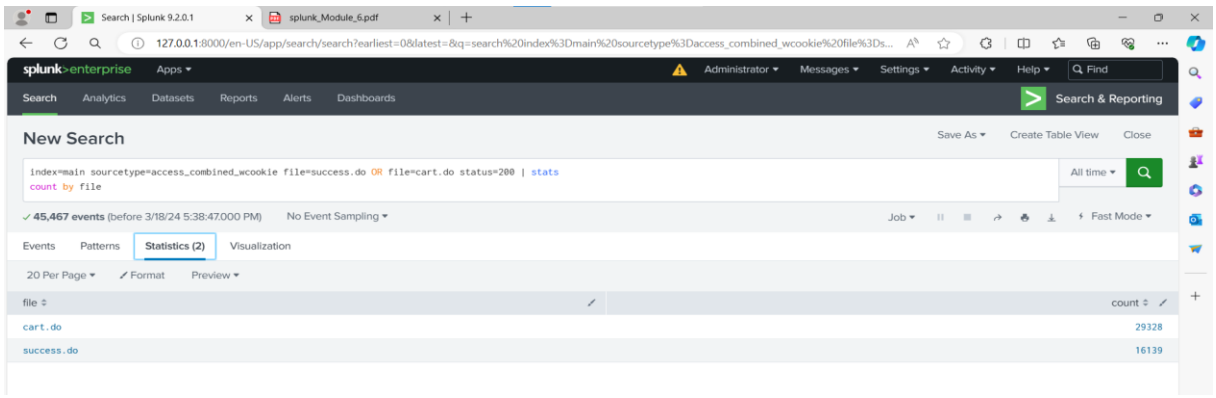
11. Enter a search that returns all web application events where an item was successfully added to a cart, or purchased. Remember, when an item is added to the cart the cart.do file is served; the success.do is served when the item is purchased.

Command - index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200



12. Use the stats count function with a by clause to count events by the file that was served.

Command : index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count by file



13. Notice that the count column is labeled count by default. Use an as clause to rename the column to Transactions.

Command : index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count as Transactions by file

file	Transactions
cart.do	29328
success.do	16139

14. Using the rename command, change the name of the file field to Function.

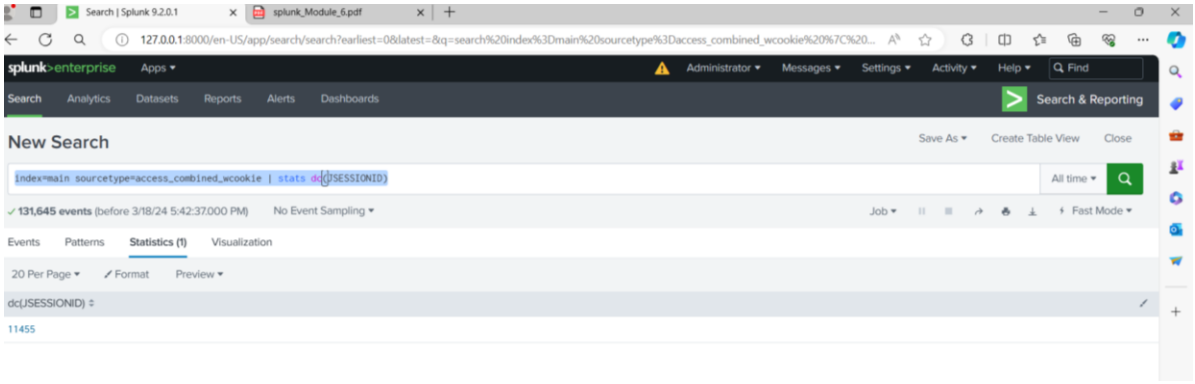
Command : (index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count as Transactions by file | rename file as Function)

Function	Transactions
cart.do	29328
success.do	16139

<u>Task 4: Use the distinct count stats function to count how many times sessions were created for users on the system.</u>

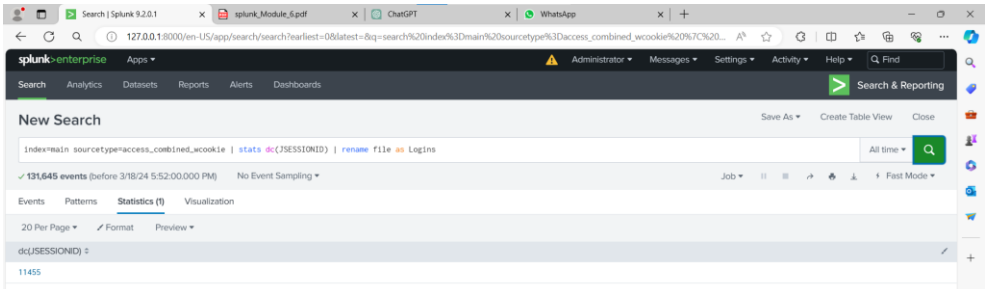
15. Use search terms with the stats dc function to count all sessions (JSESSIONID)that have been used in our web application data.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID)



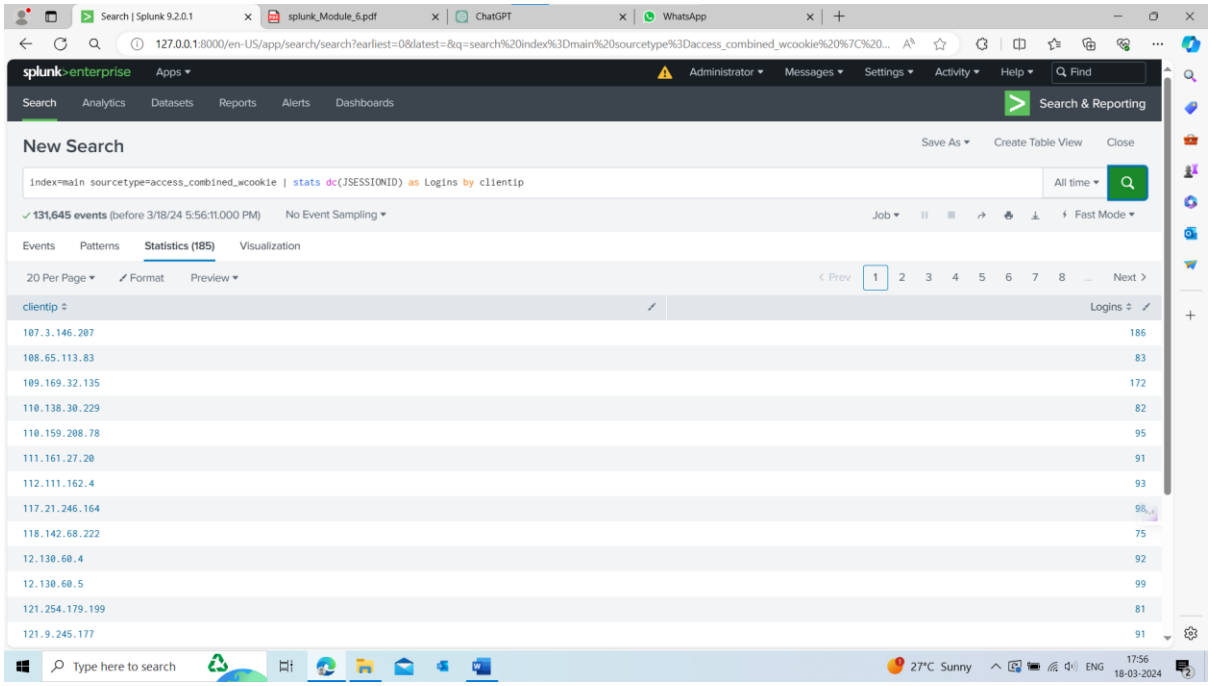
16. Use the as clause to rename the sessions as Logins.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) | rename file as Logins



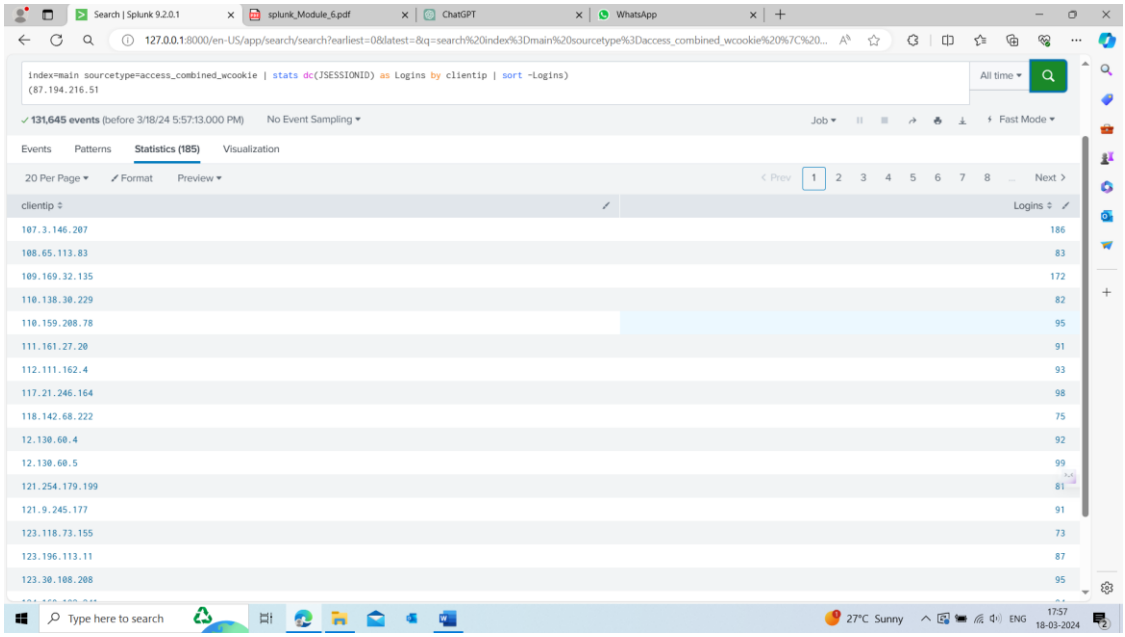
17. Using the by clause, split the Logins by clientip.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) as Logins by clientip



18. Use the sort command to sort Logins so that the clientip with the most Logins is displayed at the top of the list. Make a note of the top clientip you might be asked about it in the quiz.

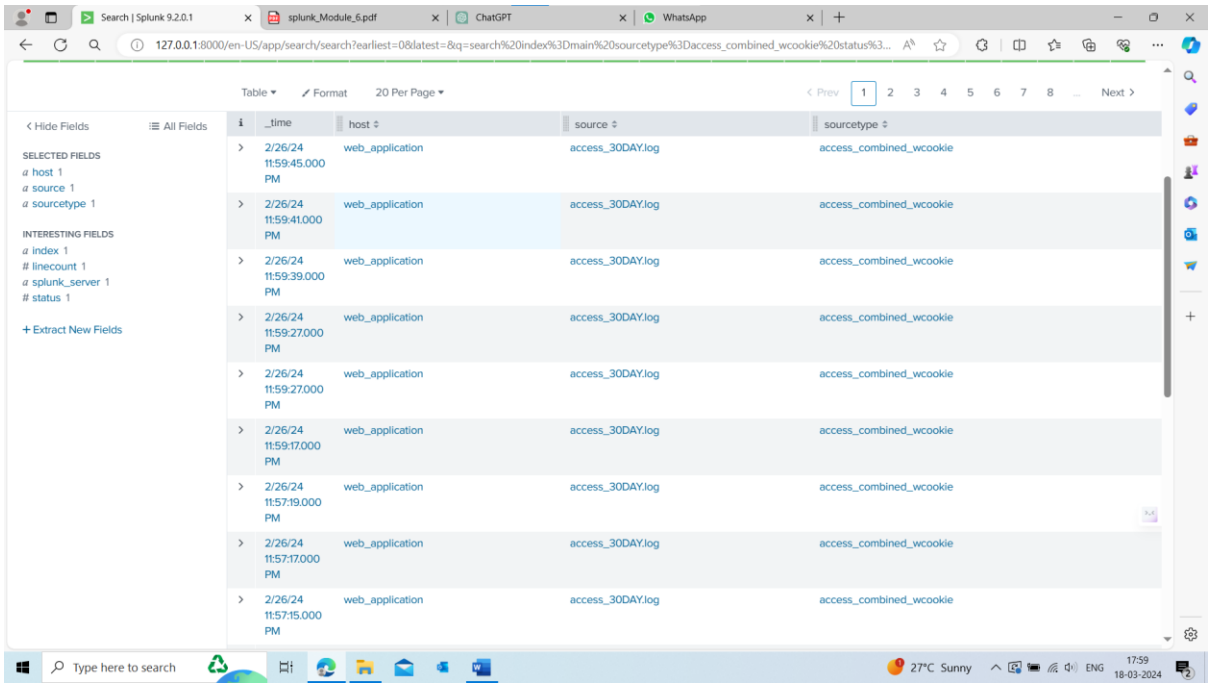
Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) as Logins by clientip | sort -Logins) (87.194.216.51)



Task 5: Use the stats sum function to find the total bytes used for the web application

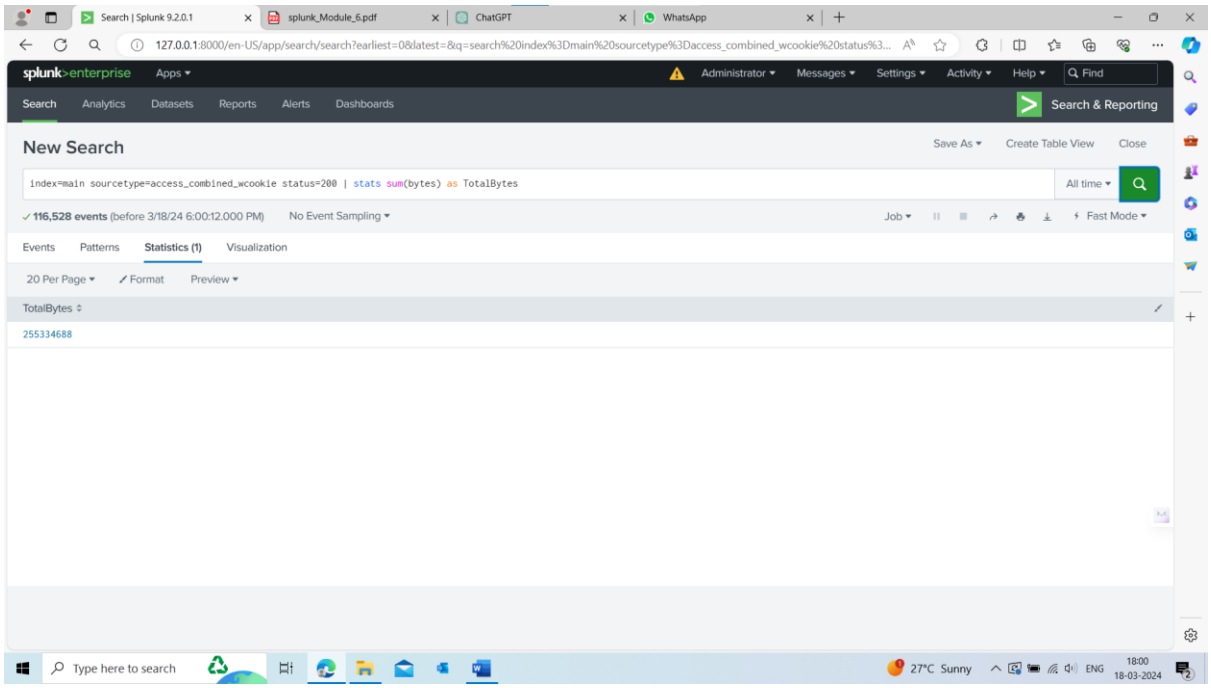
19. Craft search terms that return all events where a file was successfully served to a user.

Command : index=main sourcetype=access_combined_wcookie status=200



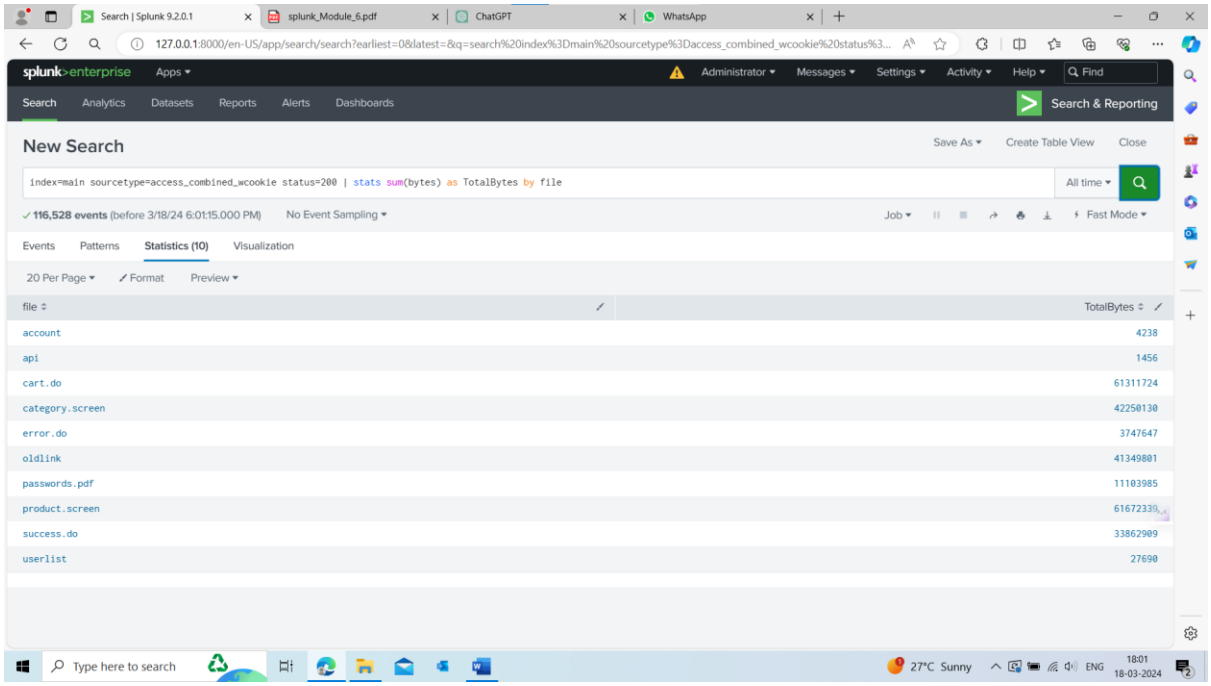
20. Create a field named TotalBytes by using the sum function of the stats command.

Command : index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes



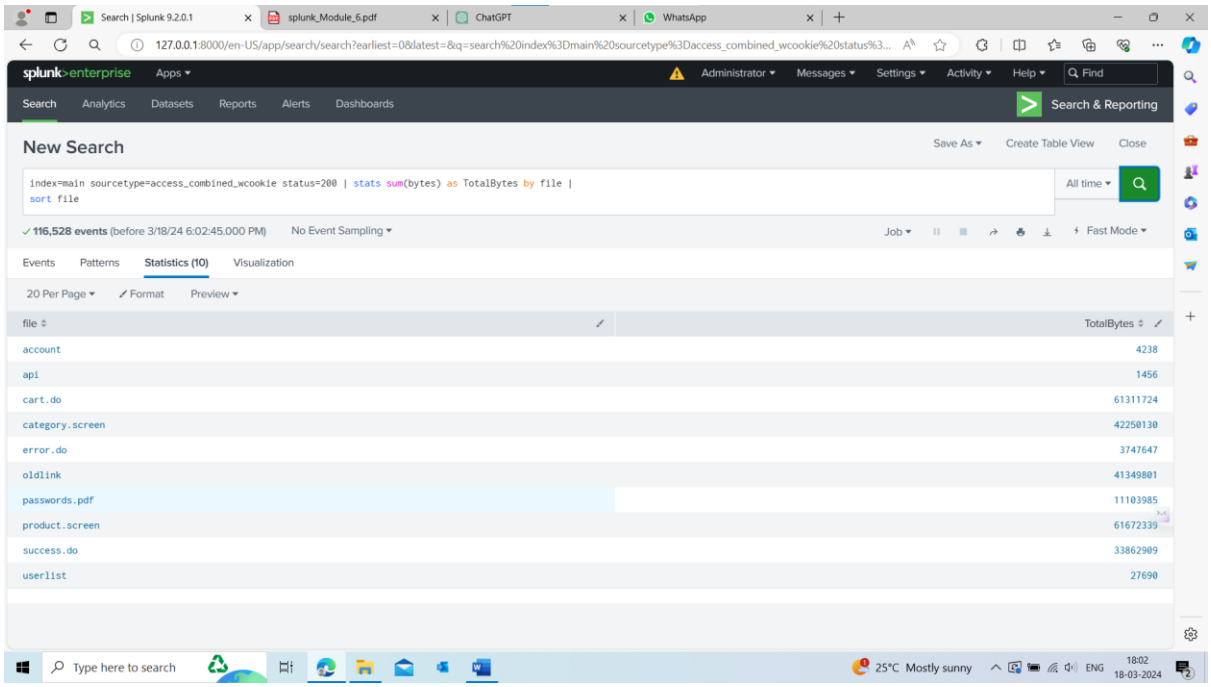
21. Split the results by the file field using the by clause.

Command : index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes by file



22. Use the sort command to sort the file names into alphabetical order.

Command : index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes by file | sort file



23. What is the name of the file that used the least amount of bandwidth? You might be asked about it in the quiz.

Command :

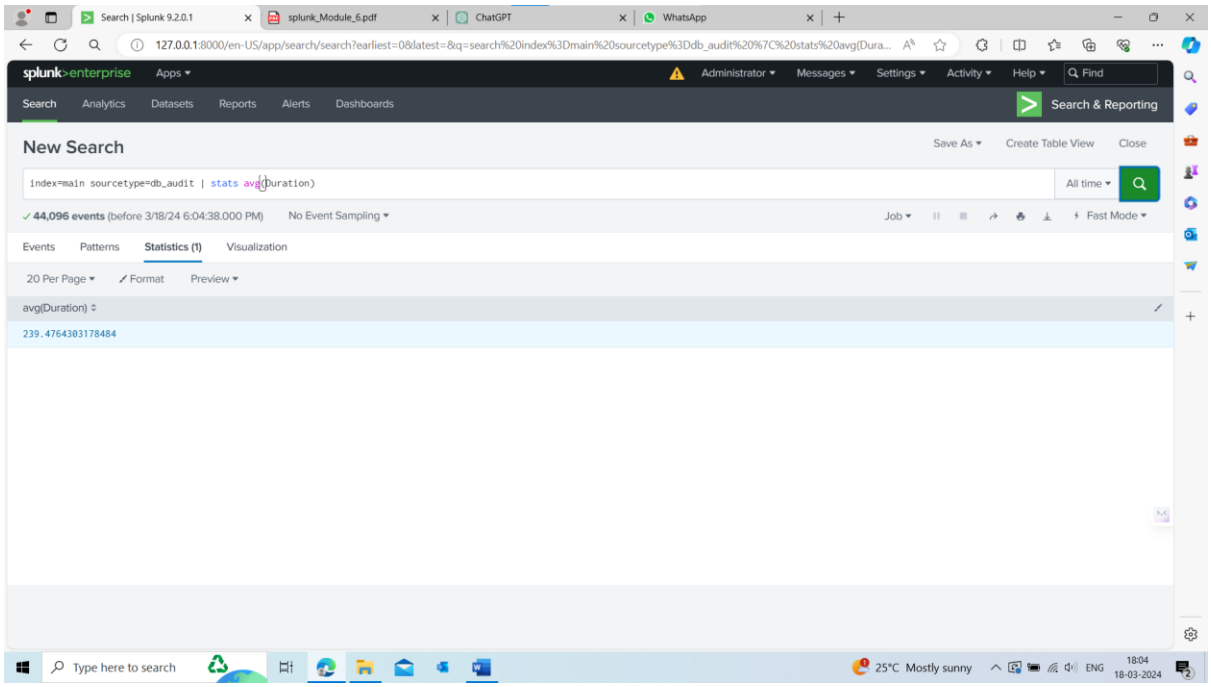
```
account
```

```
api
```

Task 6: Use the stats command's average function to find the average time for each database query being run

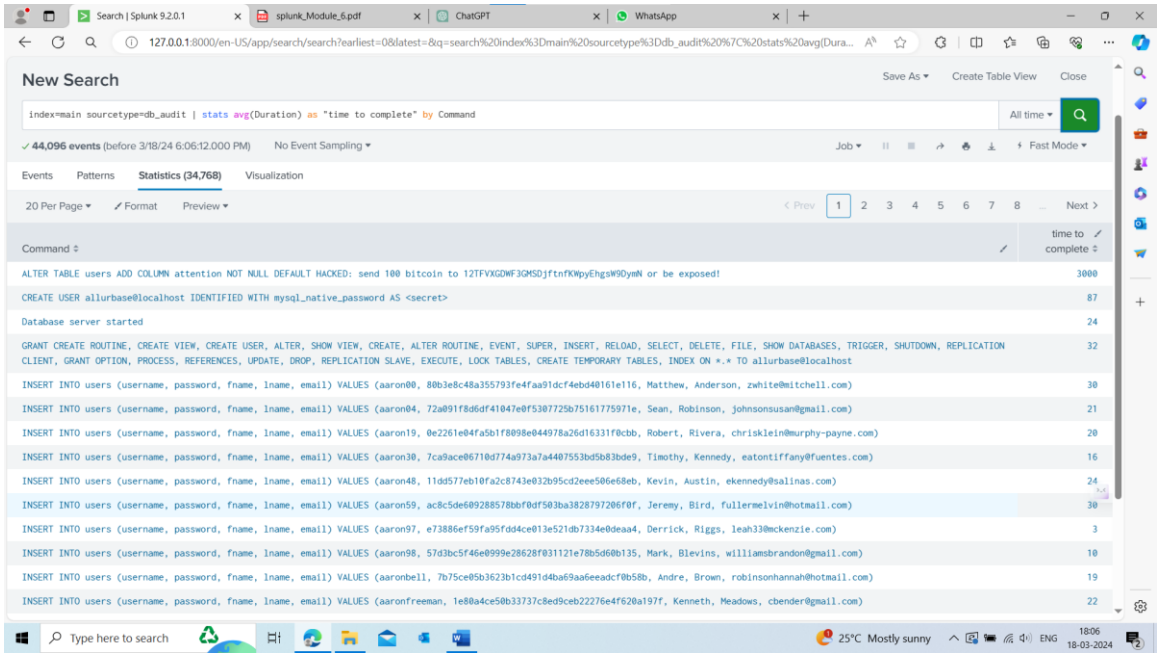
24. Search all database events and use the average (avg) function of the stats command to get an average Duration of all queries.

Command : index=main sourcetype=db_audit | stats avg(Duration)



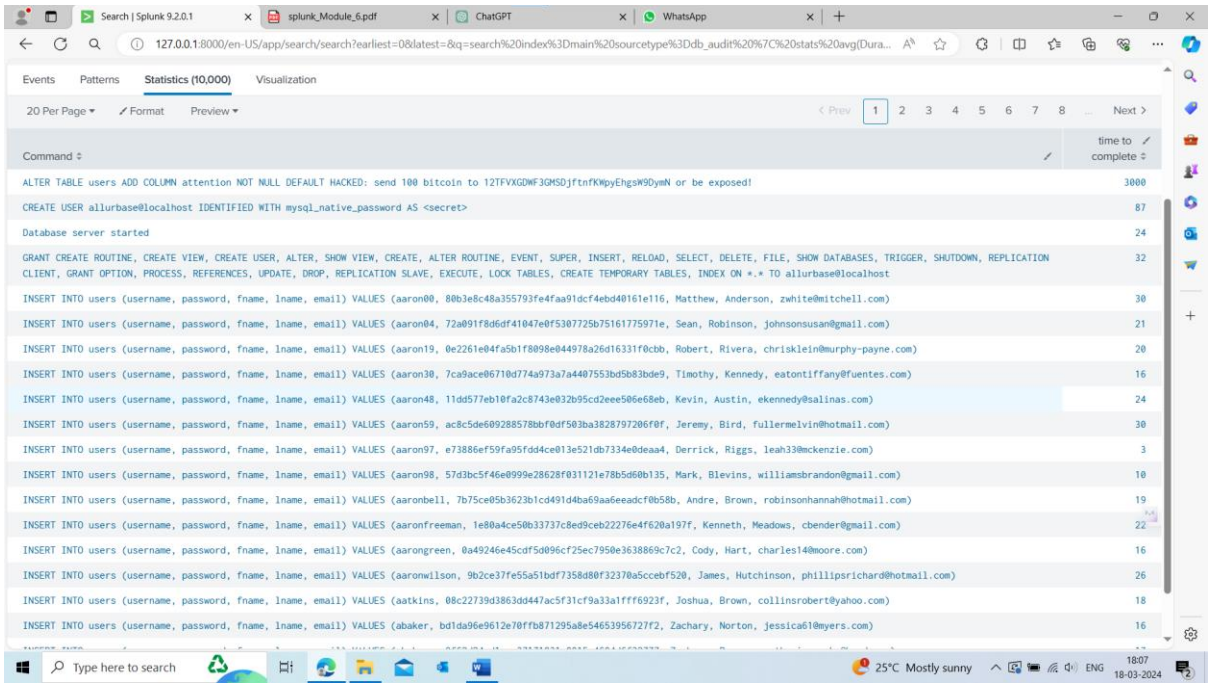
25. Use as and by clauses to rename the average field to time to complete and split by the Command.

Command : index=main sourcetype=db_audit | stats avg(Duration) as "time to complete" by Command.



26. Sort the time to complete so that Command values that take the longest are shown first.

Command : index=main sourcetype=db_audit | stats avg(Duration) as "time to complete" by Command | sort - "time to complete"

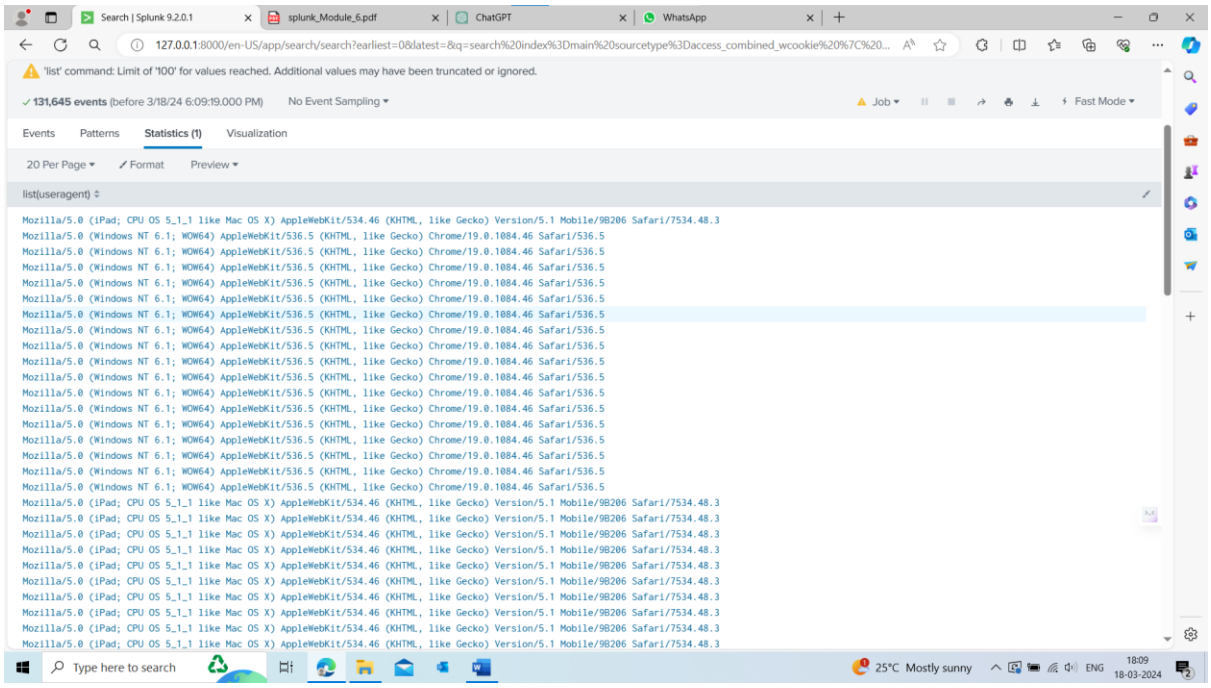


Notice anything about the Command values that are taking the longest to complete?

Task 7: Use the lists and values functions of the stats command to run a report of the browsers users are using to access the web application from.

28. Use the stats list function to generate a list of all useragent values that have accessed the web application.

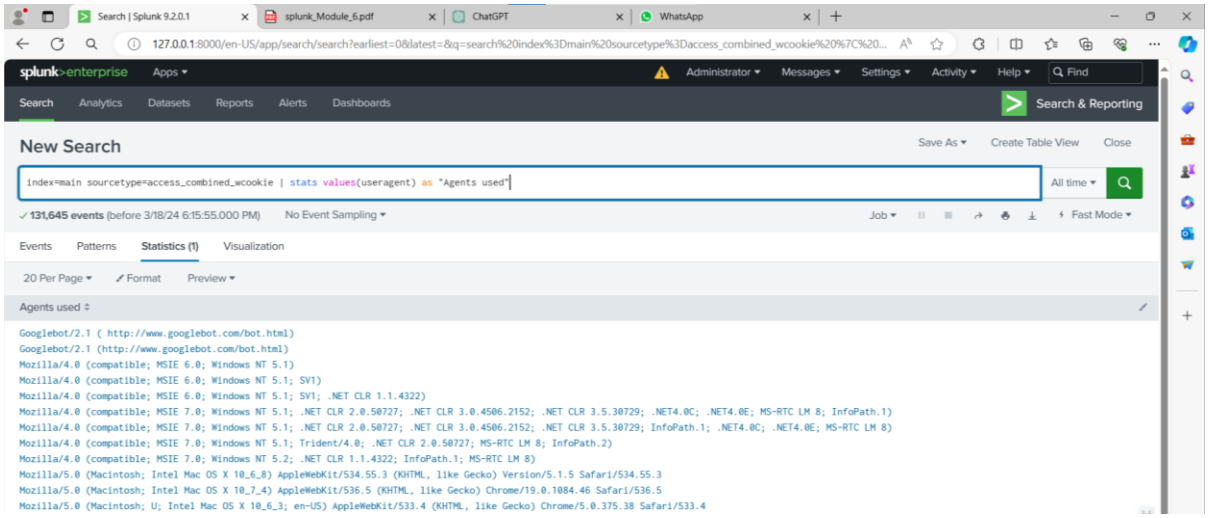
Command : index=main sourcetype=access_combined_wcookie | stats list(useragent)



29. Notice that most of the useragent values show up multiple times in the results.

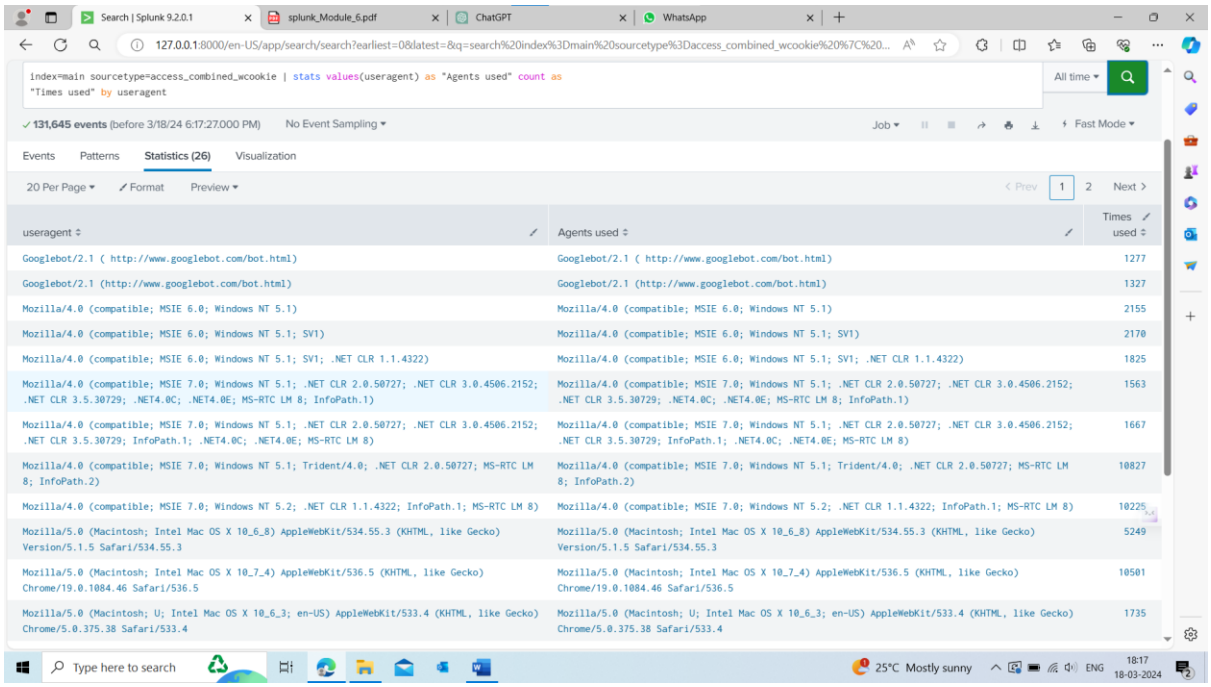
30. Use the stats values function to only return one instance of each useragent. Add an as clause to name the result as Agents used.

Command : index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used"



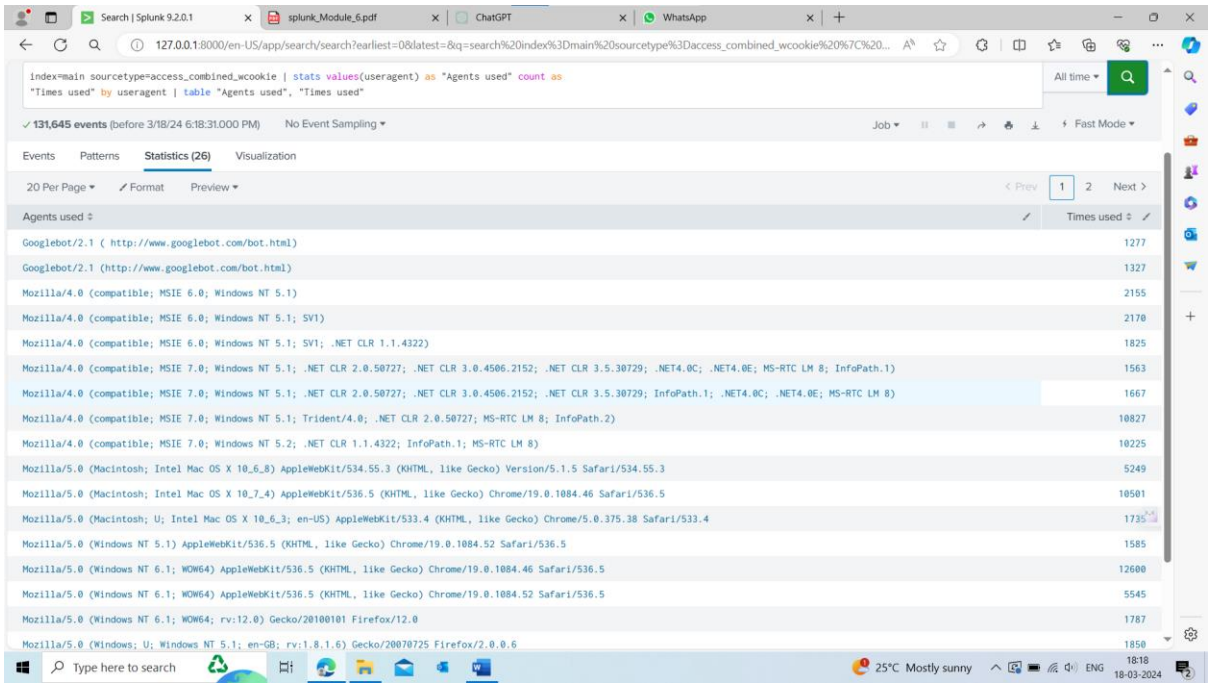
31. This report would be much more useful if we knew the number of times each useragent was used. Add a count function to the stats command that counts the events by useragent as Times used.

Command : index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used" count as "Times used" by useragent



32. Put the results of Agents used and Times used into a table.

Command : index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used" count as "Times used" by useragent | table "Agents used", "Times used"



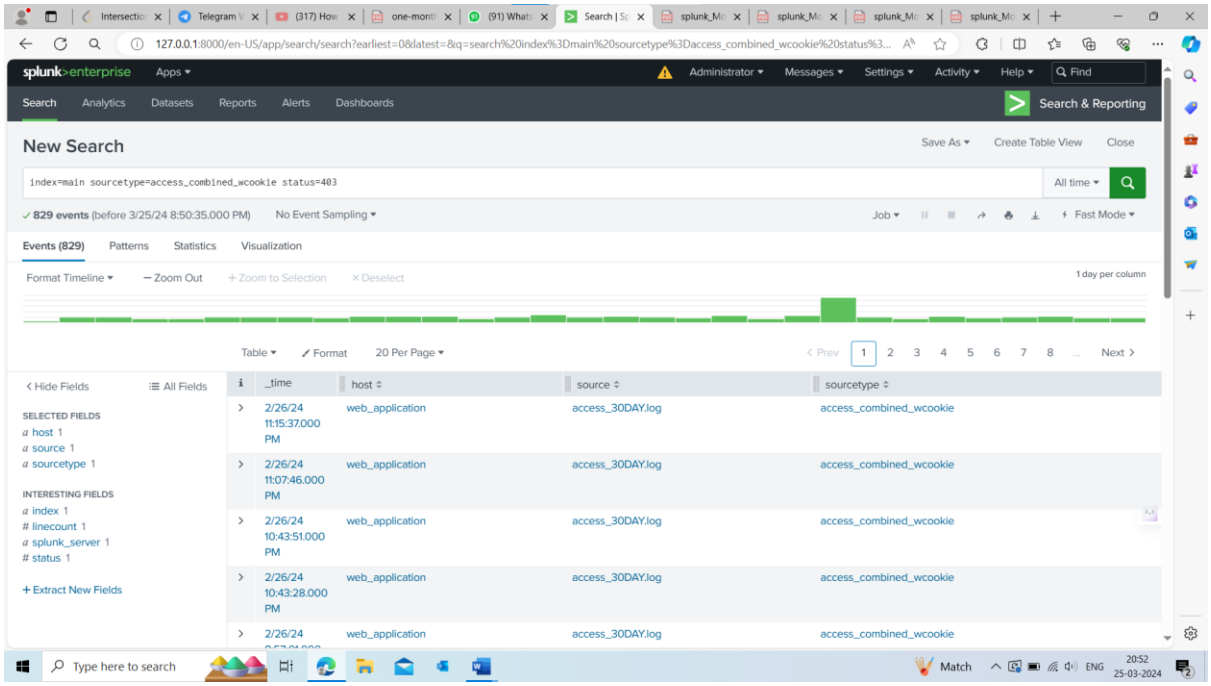
MODULE 7: – Creating Reports and Dashboards

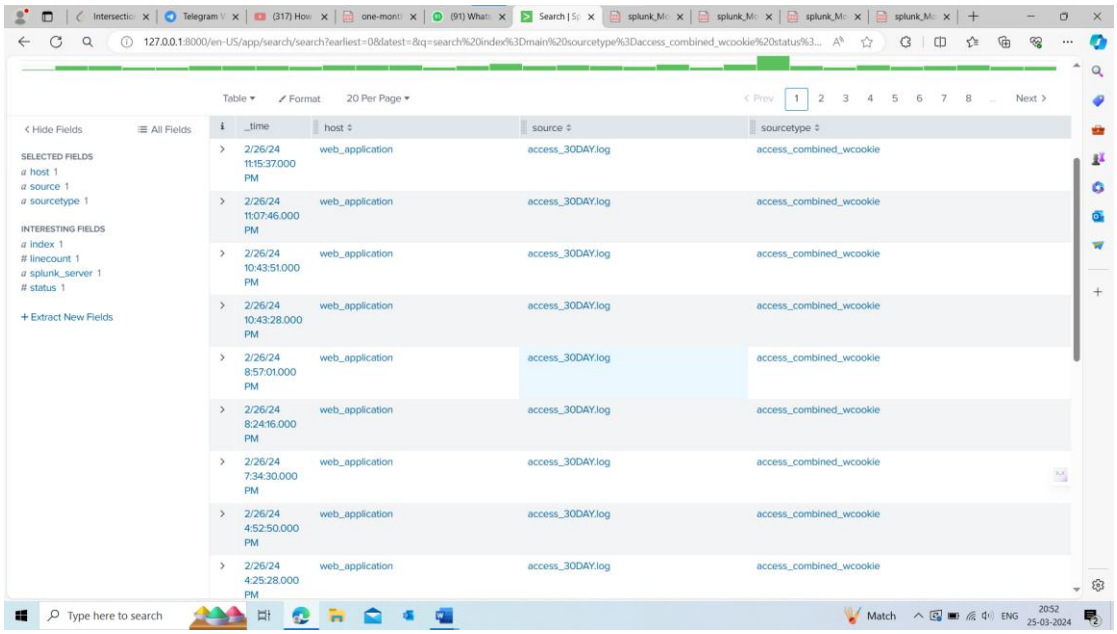
Task 1: Use the stats count function to get a report of users trying to access forbidden pages in the Buttercup Games web application.

1.Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)

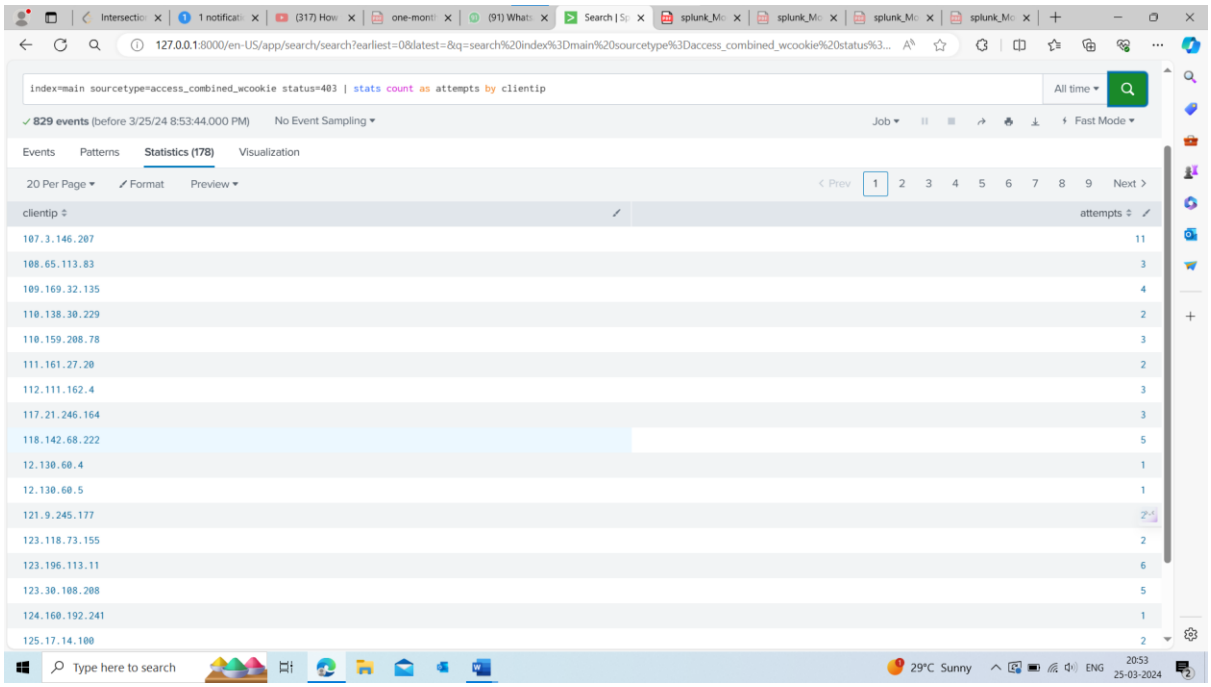
2.Enter a search that returns all web application events with a forbidden status (403).

Command: (index=main sourcetype=access_combined_wcookie status=403)

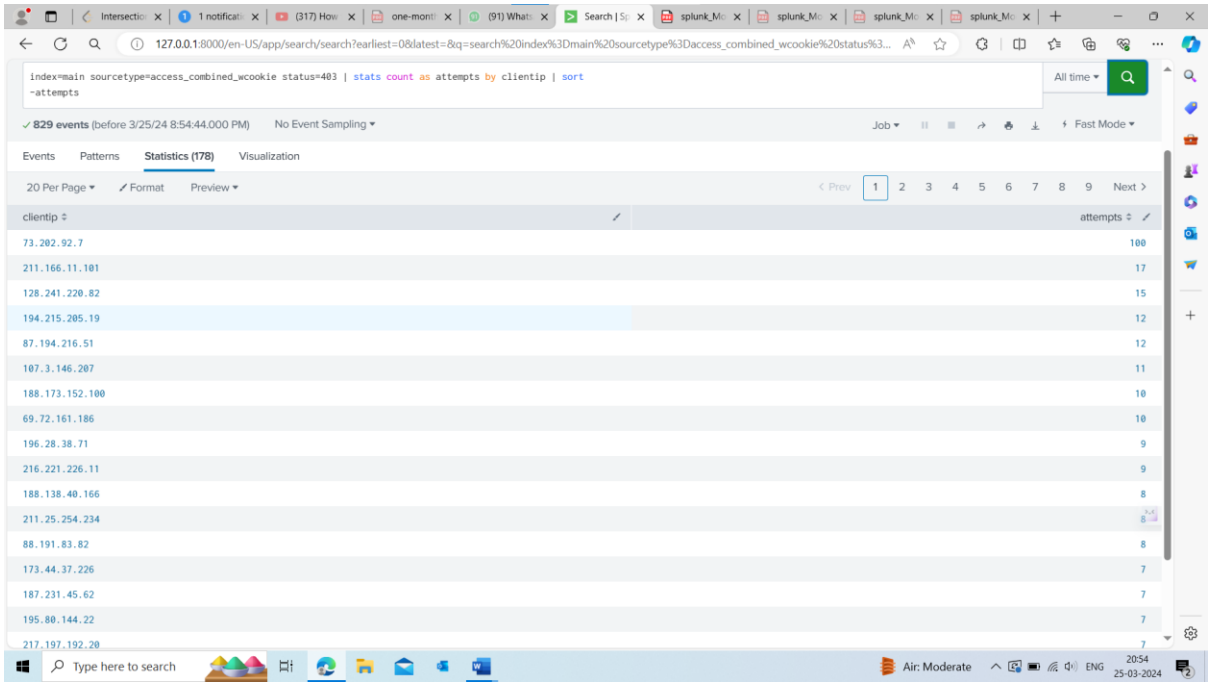




3. Use the stats count function to count the events by clientip and rename the count to attempts.
Command : (index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip)



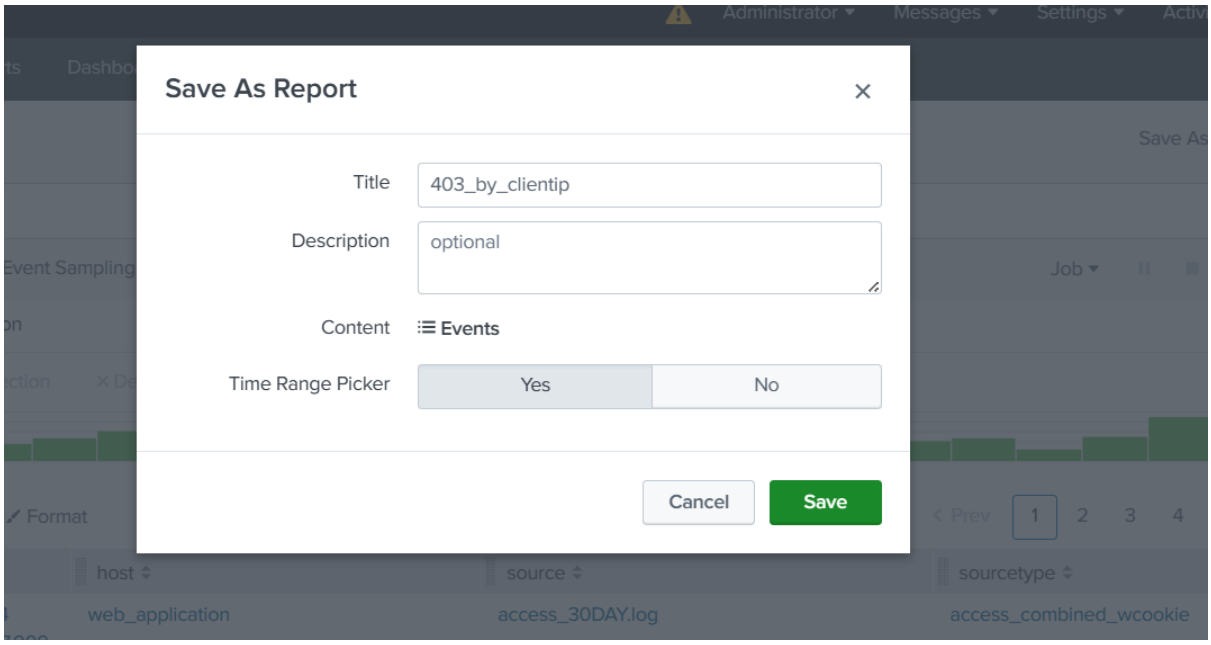
4. Use the sort command to display the results so that the clientip with the highest attempts appears first.
Command : index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip | sort -attempts



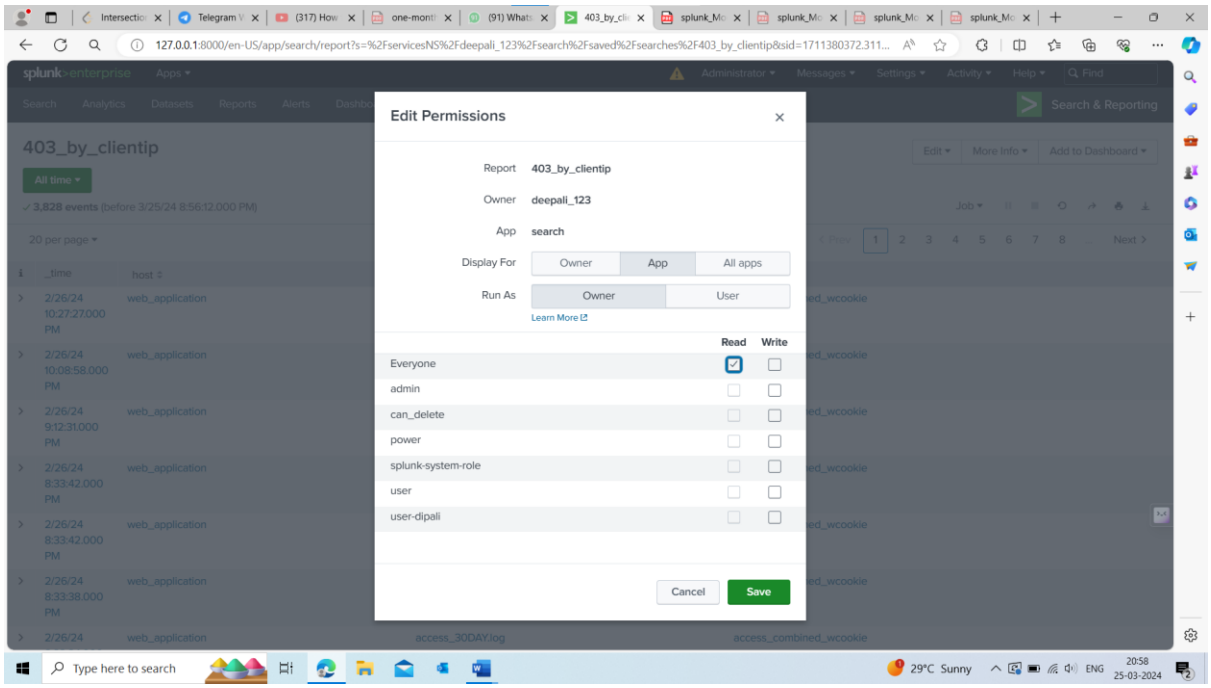
5. For the clientip with the most attempts, what was the total number of attempts? This might show up during the quiz module.

Ans: 100

6. Use the Save As menu (above the time range picker) to select Report.
7. Enter a Title of 403_by_clientip for the report and click Save.

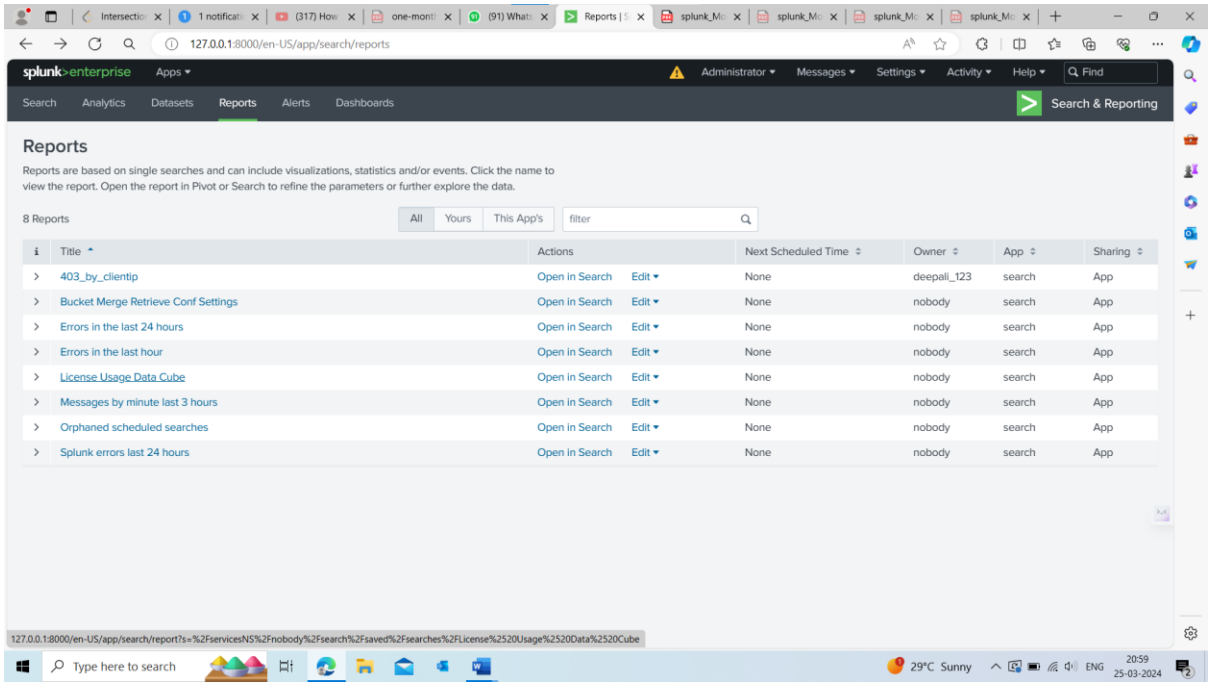


8. Use the Permissions link to make the report display for the App, run as Owner, and be readable by Everyone. Click Save.

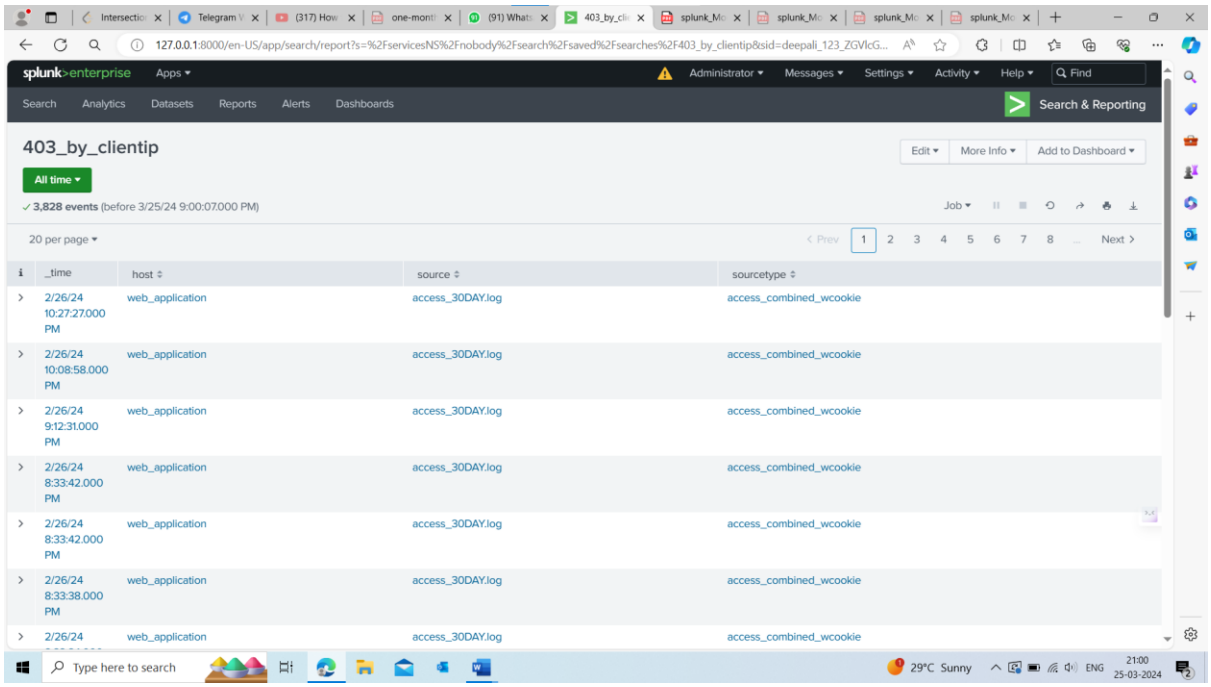


9. Access a list of the reports available to you using the Reports menu option on the bar at the top of the screen.

10.



10. Notice that the 403_by_clientip report is in the list. Click on the report title to run the report.

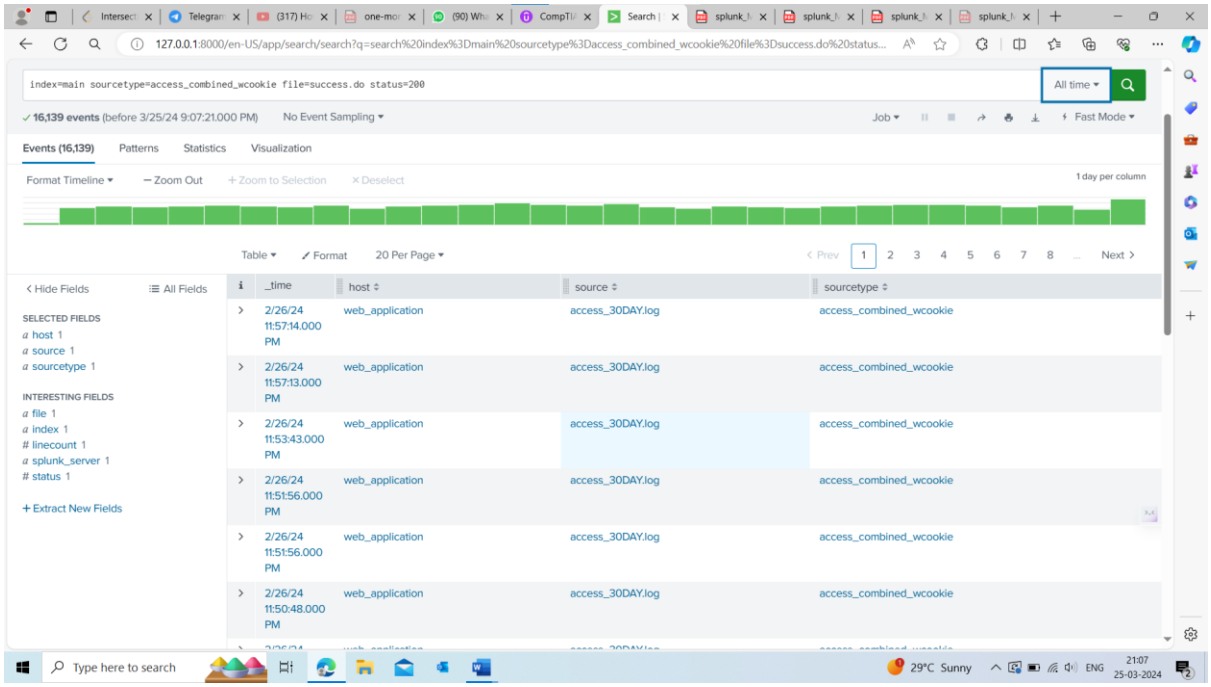


Task 2: Use stats functions to create visualizations of products sold, and add them to a dashboard.

11. Navigate to a new Search view. (Access the Search view by clicking the Search menu option on the bar at the top of the screen.)

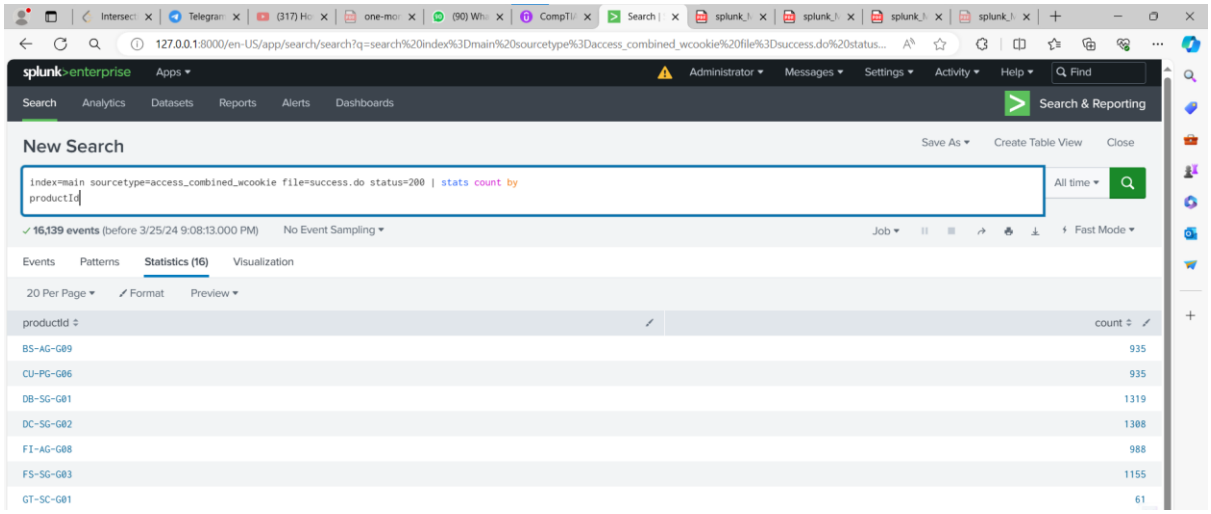
12. Enter a search that returns all web application events for all time where an item was successfully purchased. Remember, when an item is successfully purchased a success.do file is served and a 200 status is returned.

command : (index=main sourcetype=access_combined_wcookie file=success.do status=200)

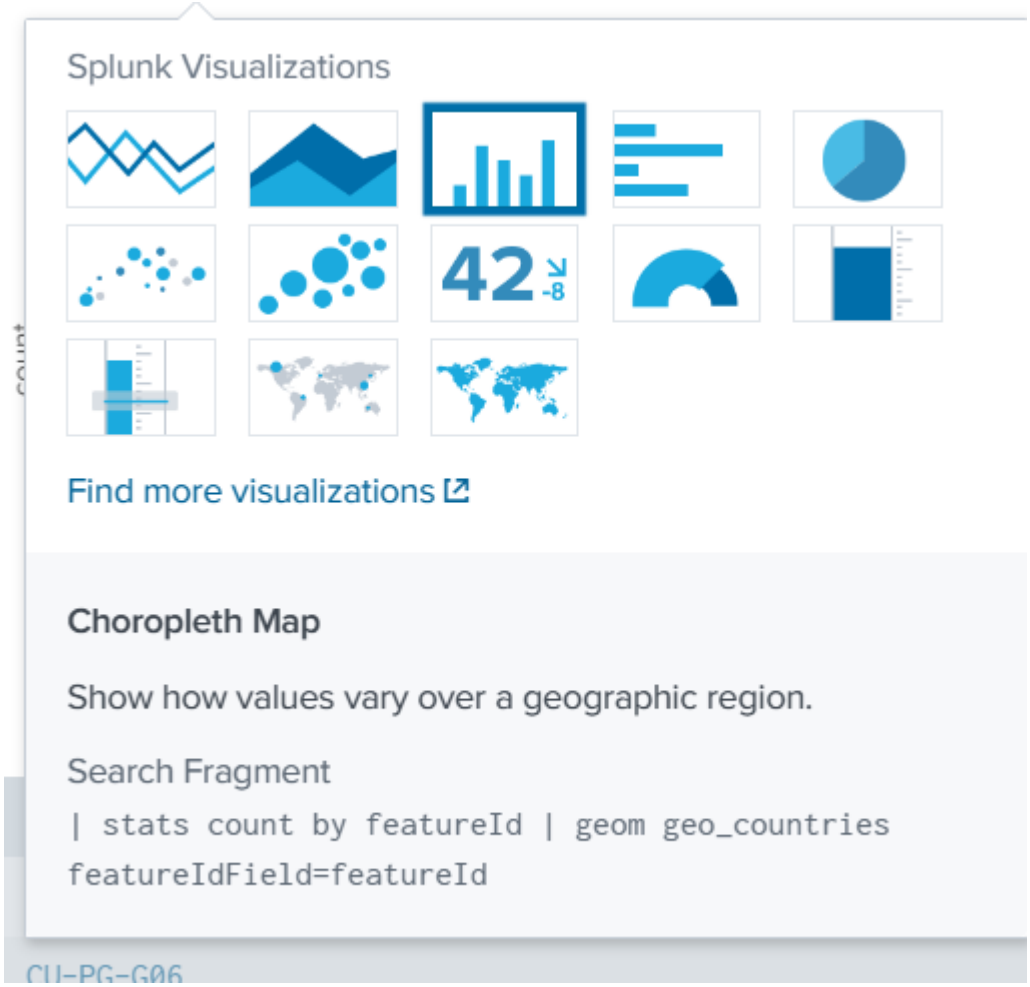


13. Use the stats count function with a by clause to count events by the productid.

Command : index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count by productid



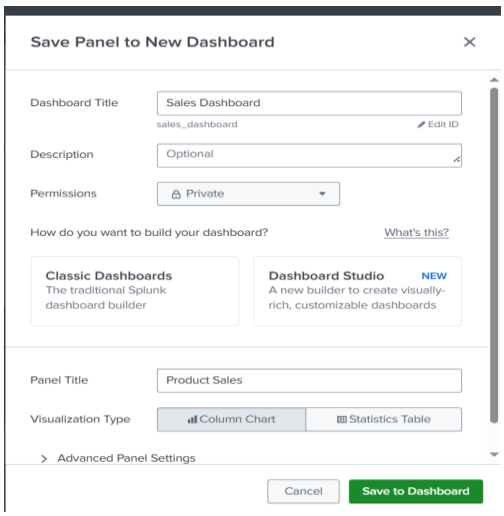
14. Select the Visualization tab and choose the Column Chart from the visualization selections.



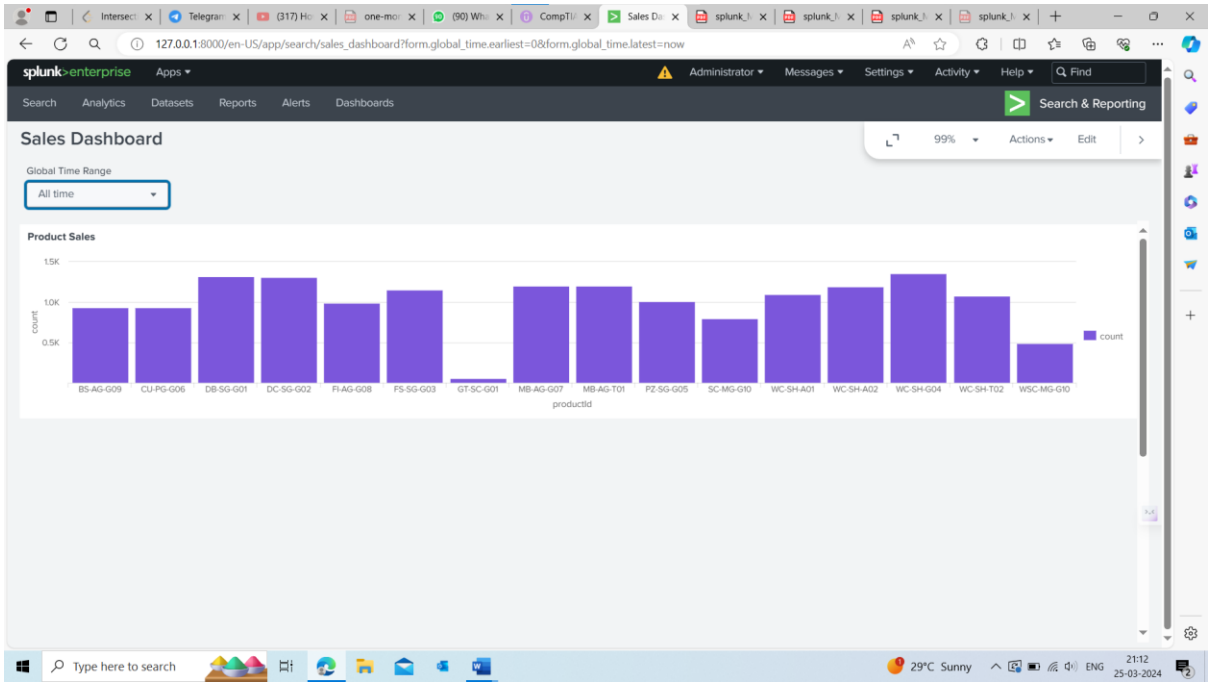
15. Use the Save As menu to select Dashboard Panel.

16. Save the dashboard with these values:

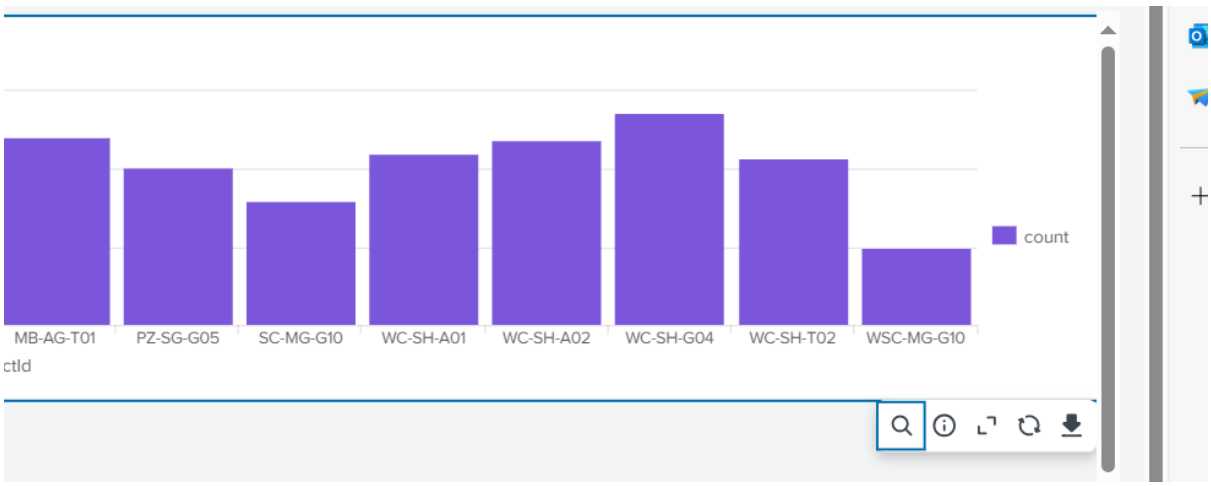
- Dashboard: New
- Dashboard Title: Sales Dashboard
- Panel Title: Product Sales



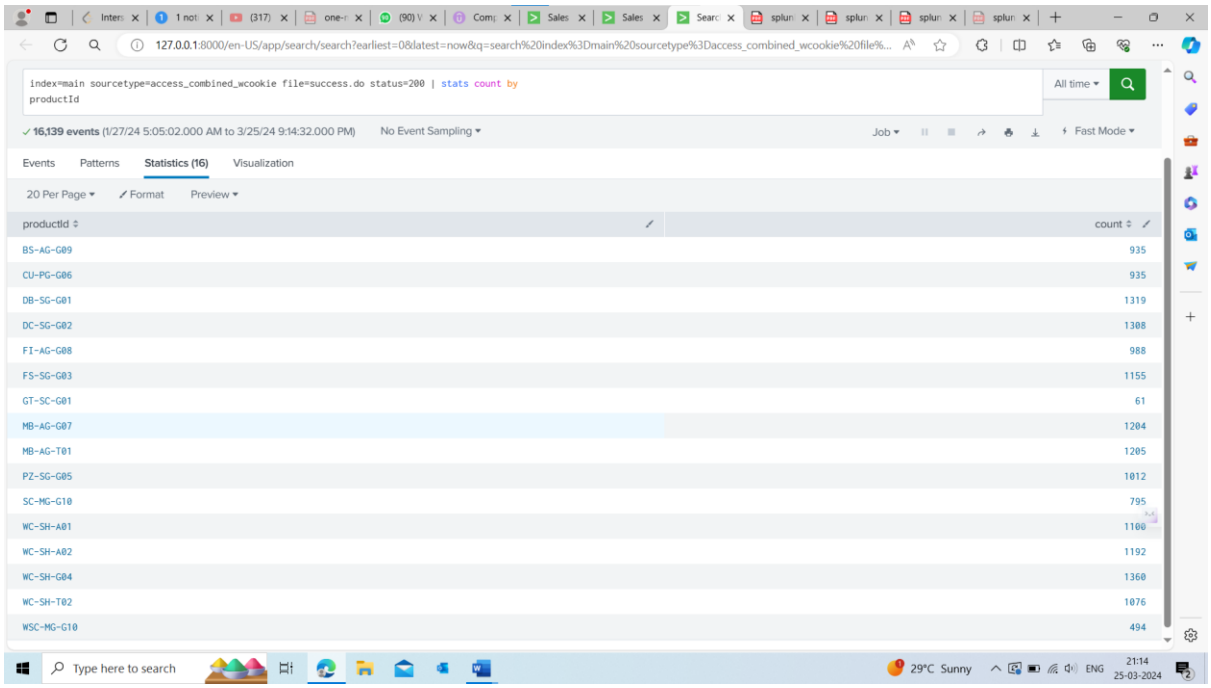
17. Once saved, click View Dashboard

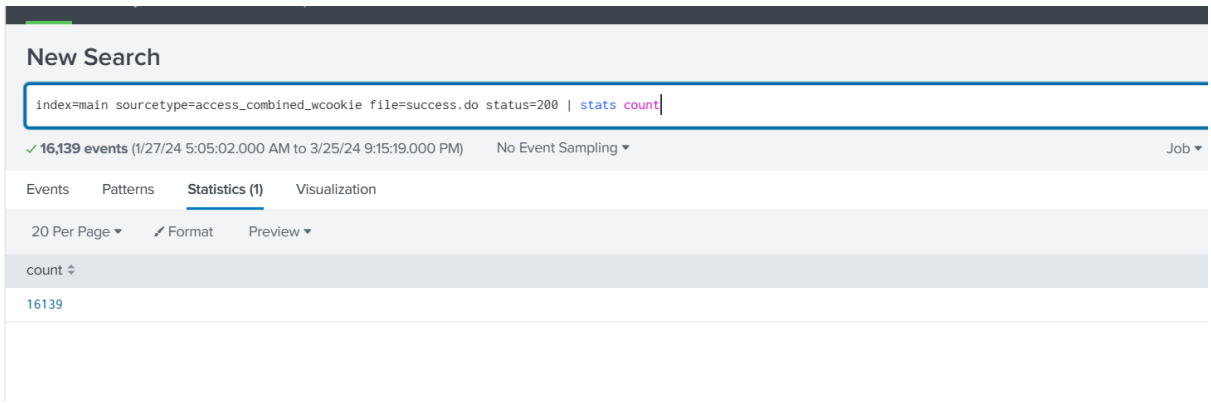


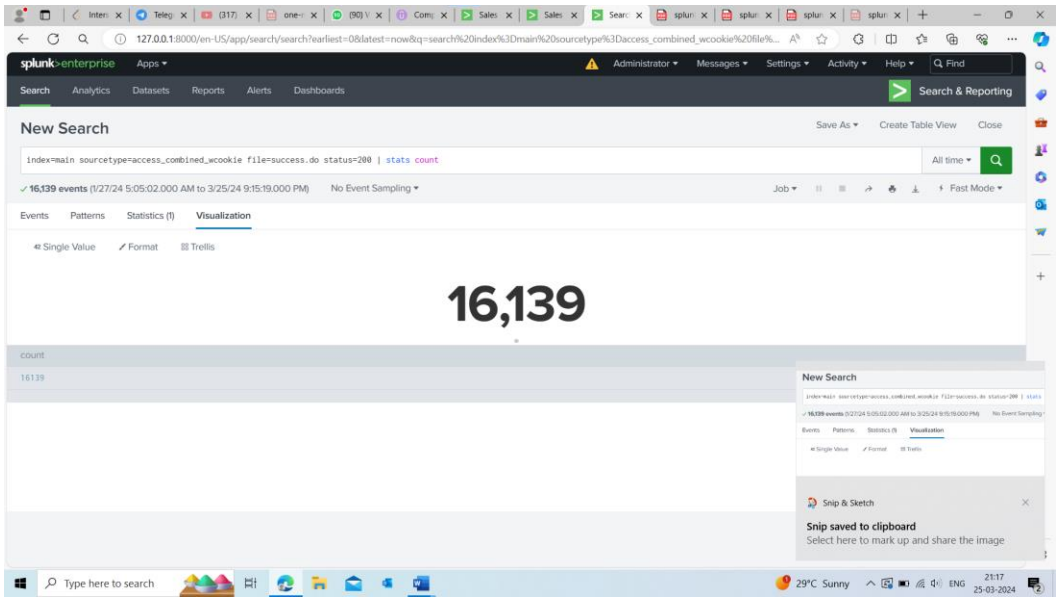
18. Roll over the columns in the chart to see the interaction, and notice the tools at the bottom of the panel.
19. Use the Open in Search icon at the bottom of the panel, to open the search view and run the search.



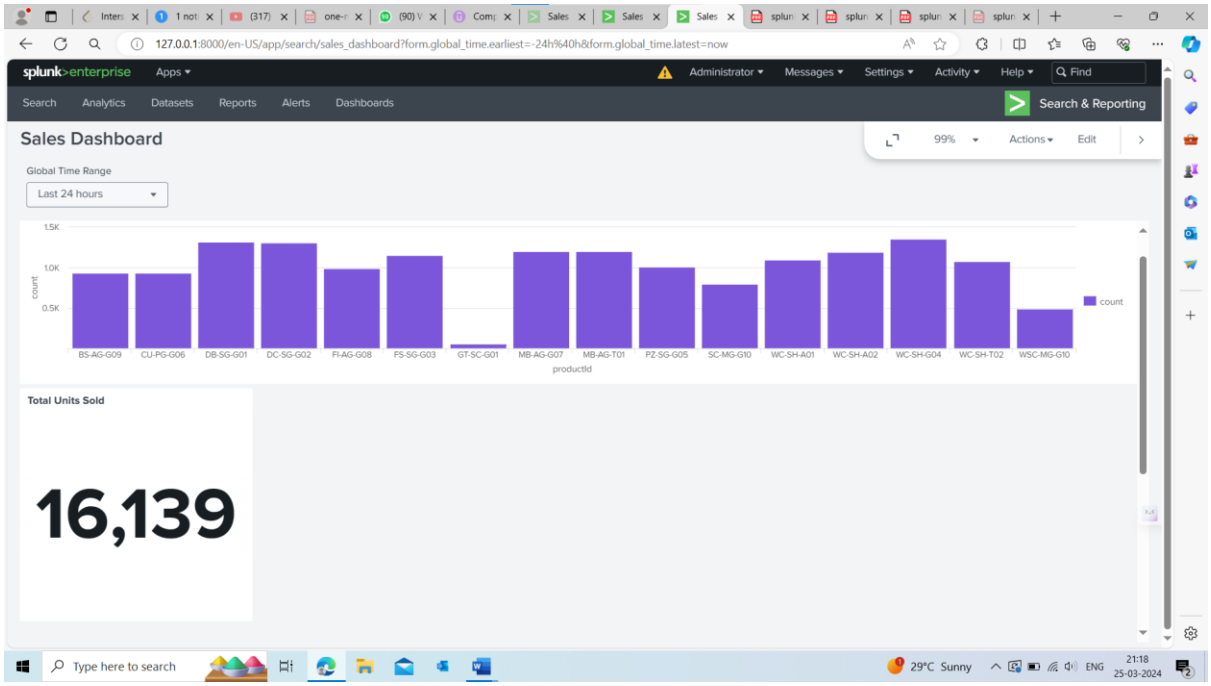
20. Remove the by clause from the search to return the total count of products sold.
Command : (index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count)



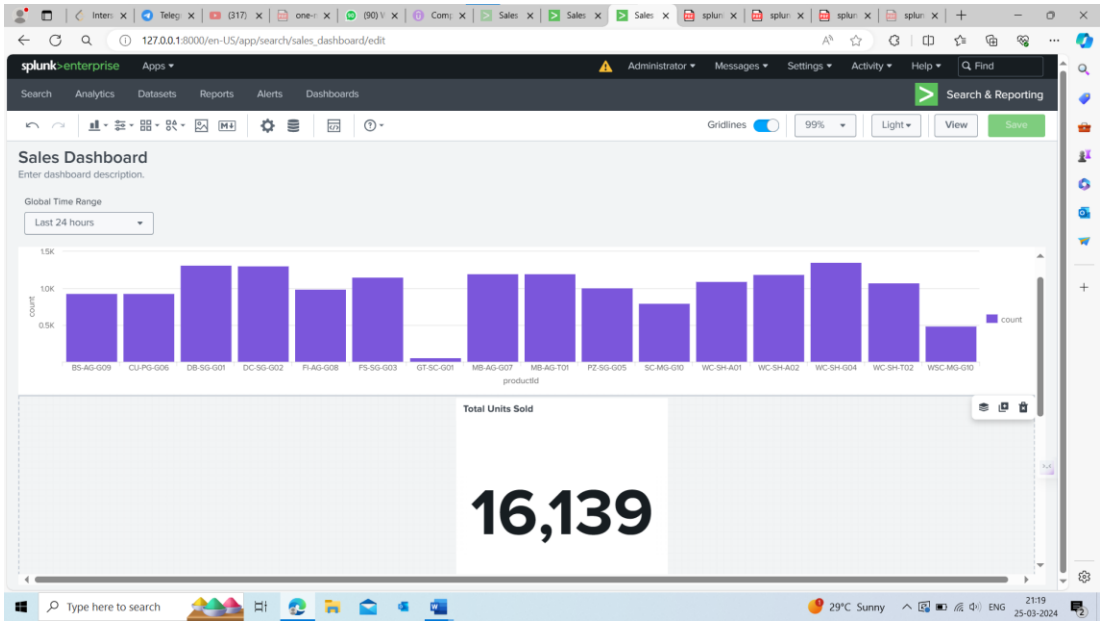




21. Select the Visualization tab and choose the Single Value visualization from the Splunk Visualizations menu.
22. Use the Save As menu to select Dashboard Panel.
23. Save the dashboard with these values:
• Dashboard: Existing
• Dashboard Title: Sales Dashboard
• Panel Title: Total Units Sold
24. Once saved, click View Dashboard.



25.The Total Units Sold panel is probably the first item our CFO will want to see. Click the Edit button at the top of the dashboard.



26.Click and hold the bar at the top of the Total Units Sold panel and drag the panel to the top of the dashboard. Once in place, drop and click Save.

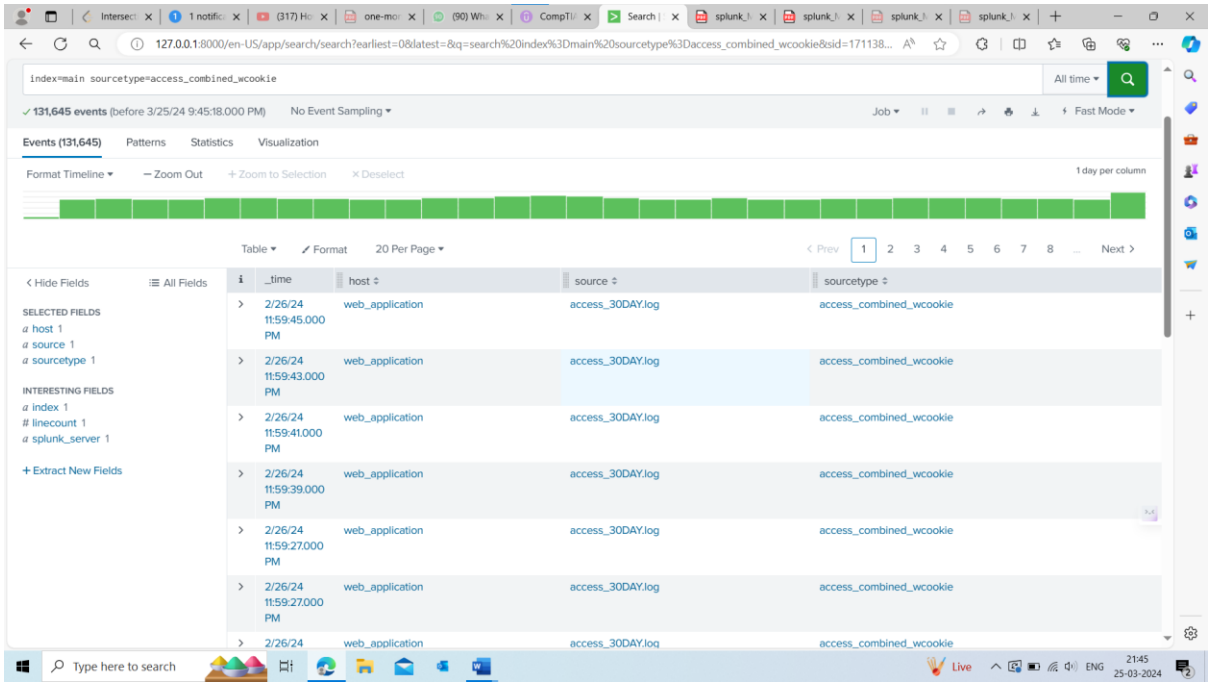
MODULE 8: USING PIVOT

Task 1: Use a non-transforming command with instant Pivot.

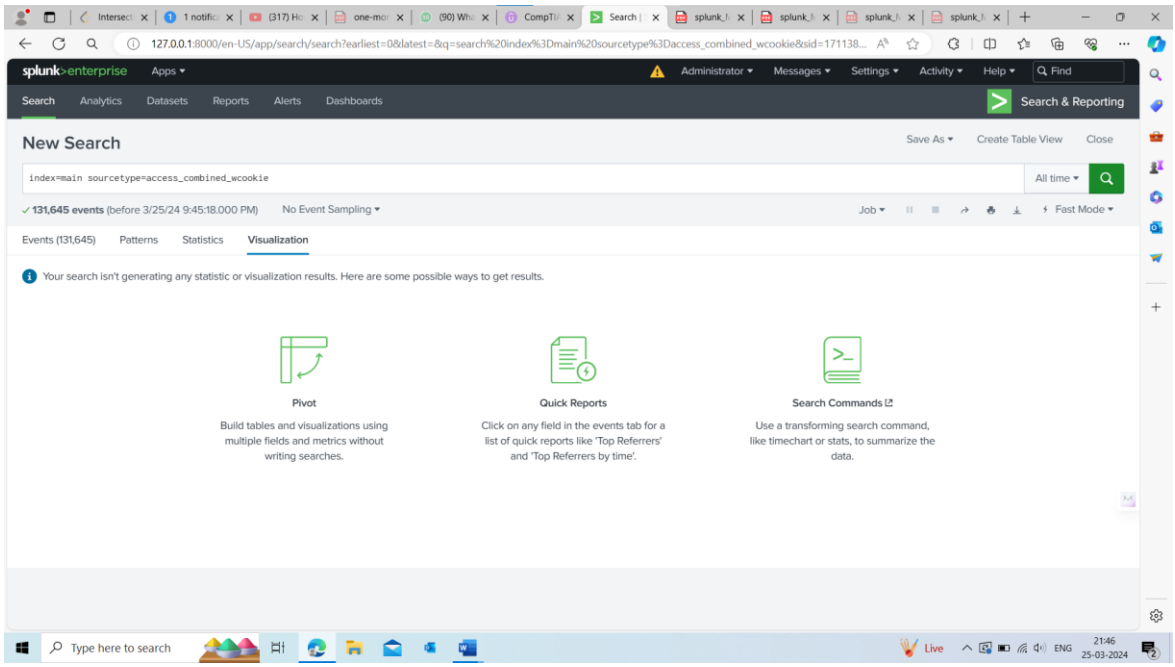
1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the green bar at the top of the screen.)

2. Enter in a search that returns all web application events for all time.

Command : index=main sourcetype=access_combined_wcookie



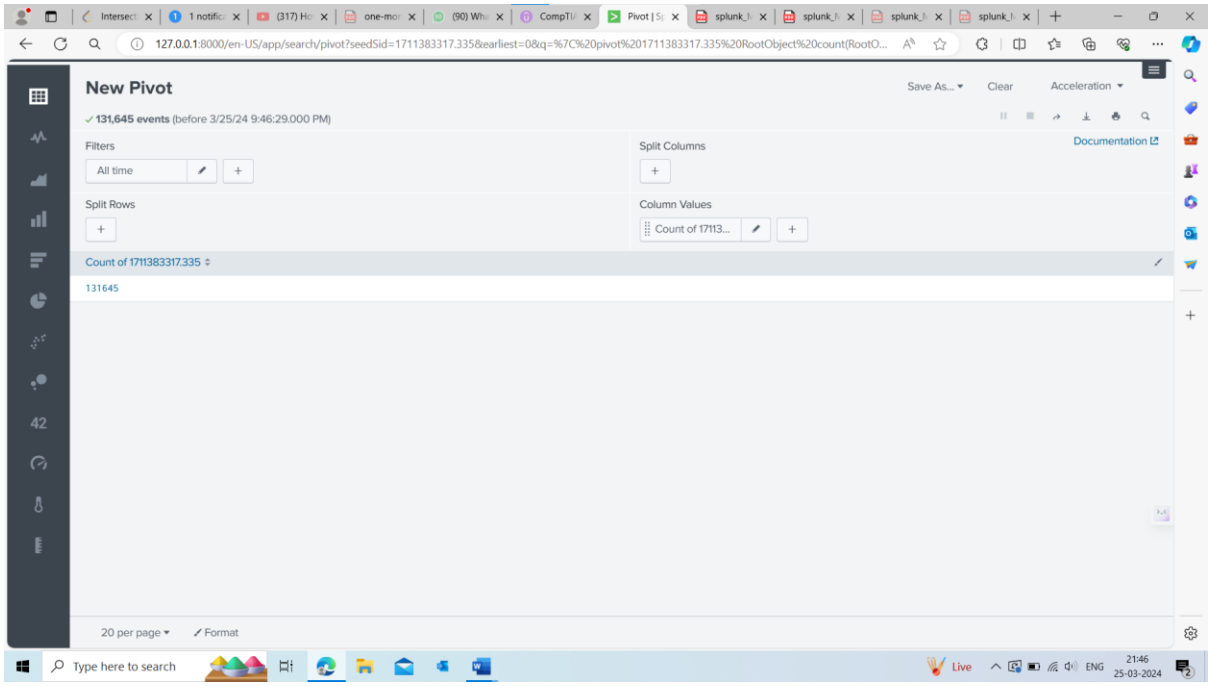
3. Click on the Visualization tab to see three icons: Pivot, Quick Reports, and Search Command.

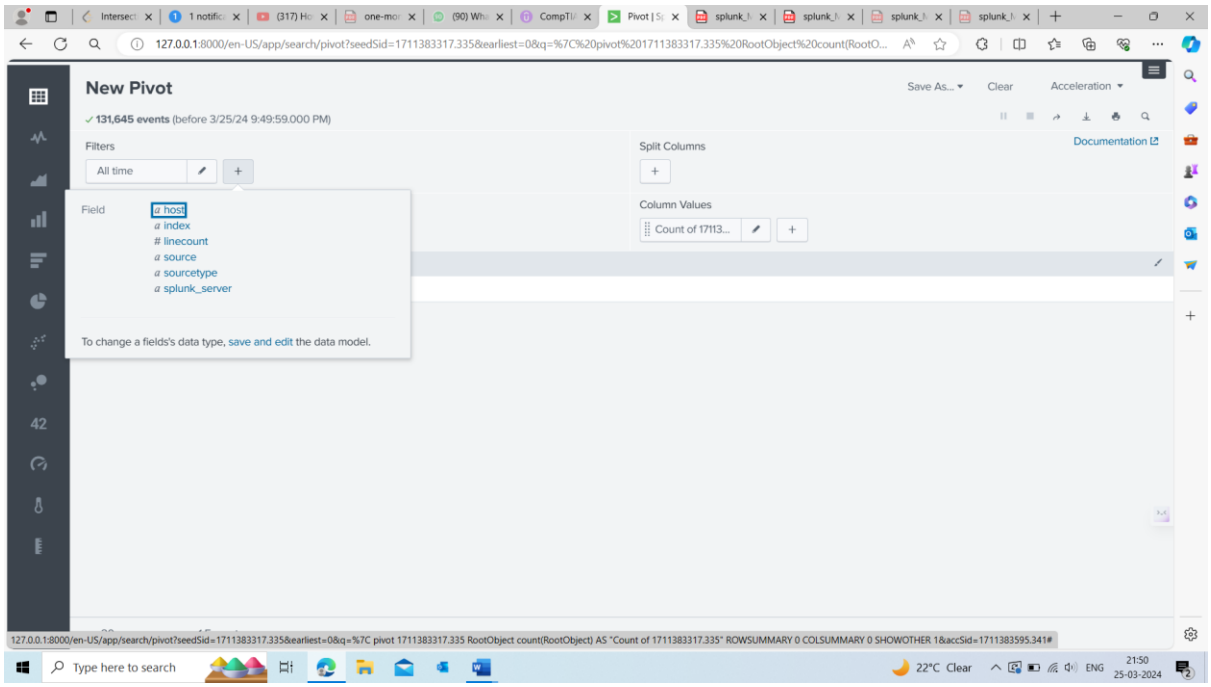


4. Click on the Pivot icon.
5. In the modal window, select to show All Fields and click OK.

Task 2: Build a report using the Pivot interface.

6. Under Filters, click , to open the filter selector, and select file from the Fields list.





MODULE 9 : CREATING LOOKUPS

Task 1: Download and examine the lookup file.

1.Open a new browser window and direct it to http://splk.it/productdata .

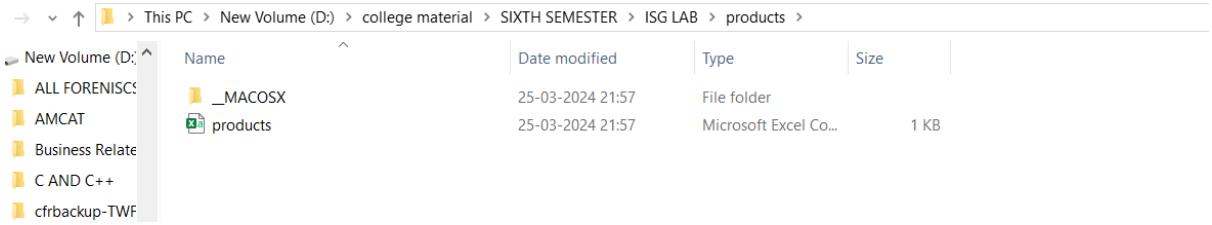
2.The file products.zip will be downloaded to your system.

3.Use an archive tool to unarchive the file.

4.Once unarchived, you will see a file named products.csv.

5.Return to the browser window for your instance of Splunk Web or open a new one.

6.Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)



Task 2: Add a lookup file and create a lookup definition.

7. Navigate to: Settings > Lookups > Lookup table files.

8.Click New Lookup Table File.

9. Save the lookup table file with these values:
- Destination app: search
- File: products.csv file
- Destination filename: products.csv

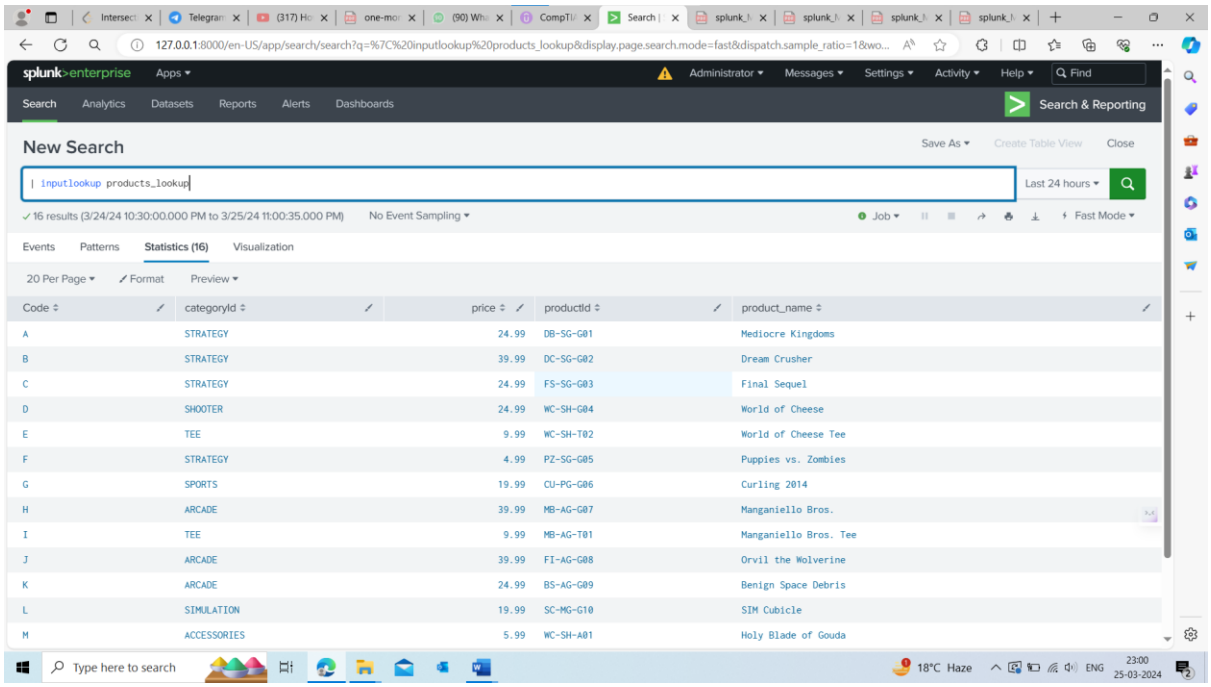
10. Navigate to Settings > Lookups > Lookup definitions.

11. Make sure Search & Reporting is selected for App context and Click New Lookup Definition

12. Save the lookup table file with these values:
- Destination app: search
- Name: products_lookup
- Type: File-based
- Lookup file: products.csv

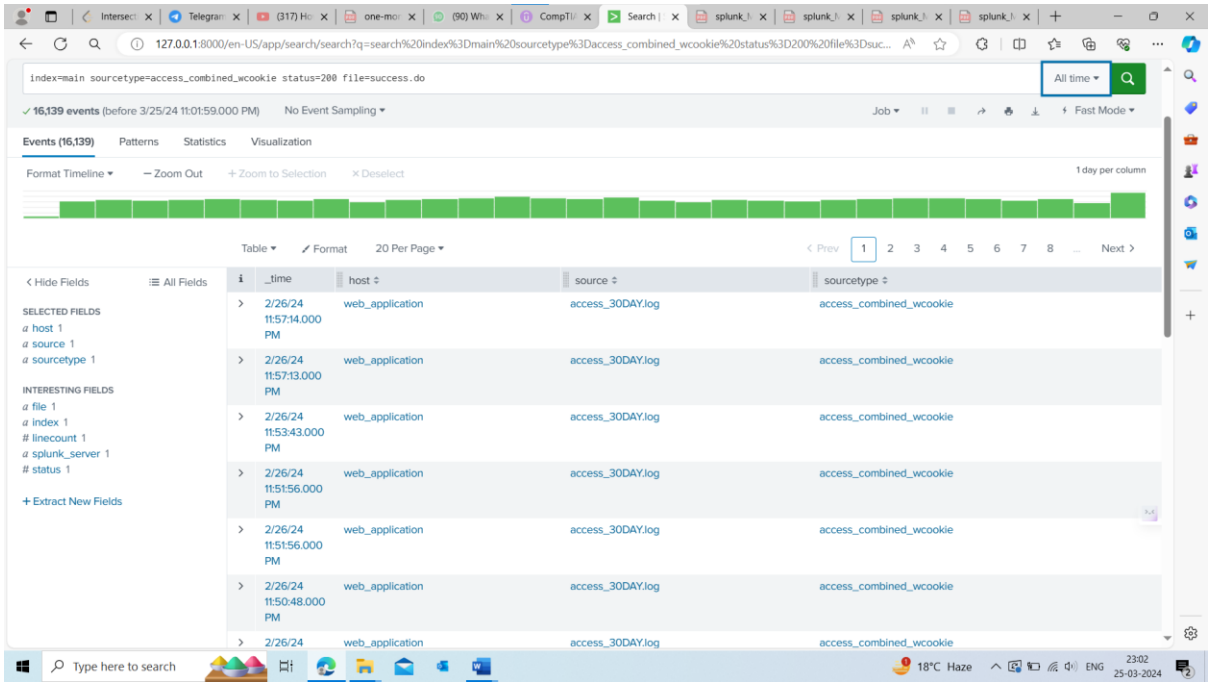
13. Return to the Search view.

14. Use inputlookup command to verify the lookup definition was created correctly.
Command : | inputlookup products_lookup



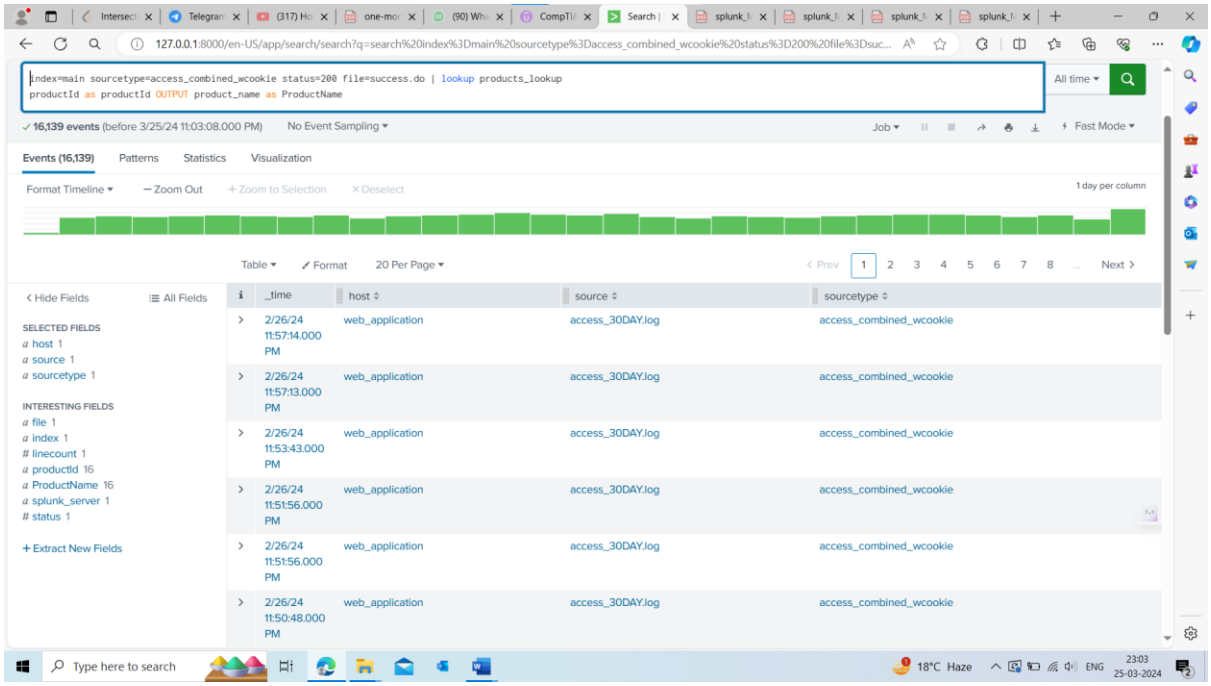
Task 3: Use the lookup in a search.

15. Search the web application data for all events where a user purchased a product successfully.
Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do)

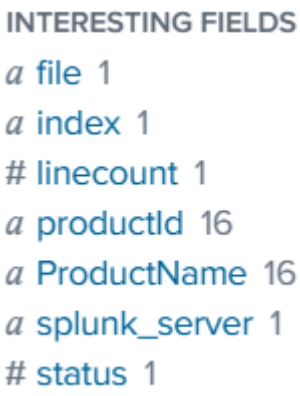


16. Use the lookup command and reference the lookup table you just created. Match the productId in lookup table to the productId field in the event data. Use the OUTPUT function to output the product_name lookup table data to a ProductName field.

Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do | lookup products_lookup productId as productId OUTPUT product_name as ProductName)

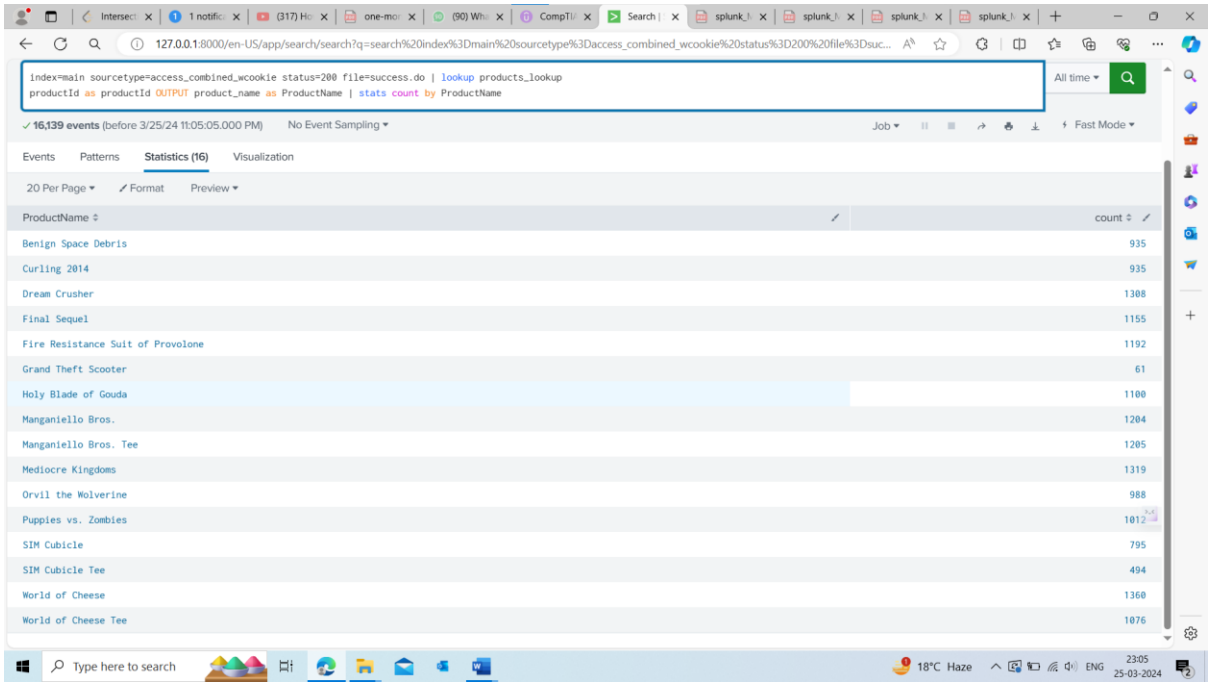


17. Notice that there is now a ProductName field in the fields list



18. Change the search to use a stats count function to count events by ProductName.

Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do | lookup products_lookup productId as productId OUTPUT product_name as ProductName | stats count by ProductName)



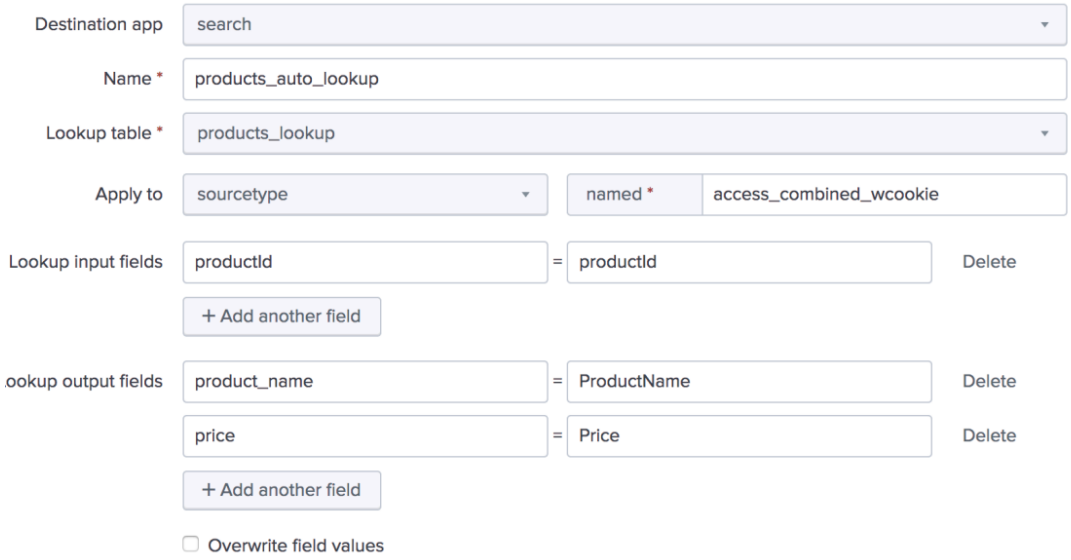
Task 4: Create an automatic lookup definition.

19. Navigate to Settings > Lookups > Automatic lookups

20. Save the automatic lookup with these values:

- Destination app: search
- Name: products_auto_lookup
- Lookup table: products_lookup
- Apply to: sourcetype
- named: access_combined_wcookie
- Lookup input fields: productId = productId
- Lookup output fields: product_name = ProductName

price = Price



Task 5: Verify your automatic lookup is working.

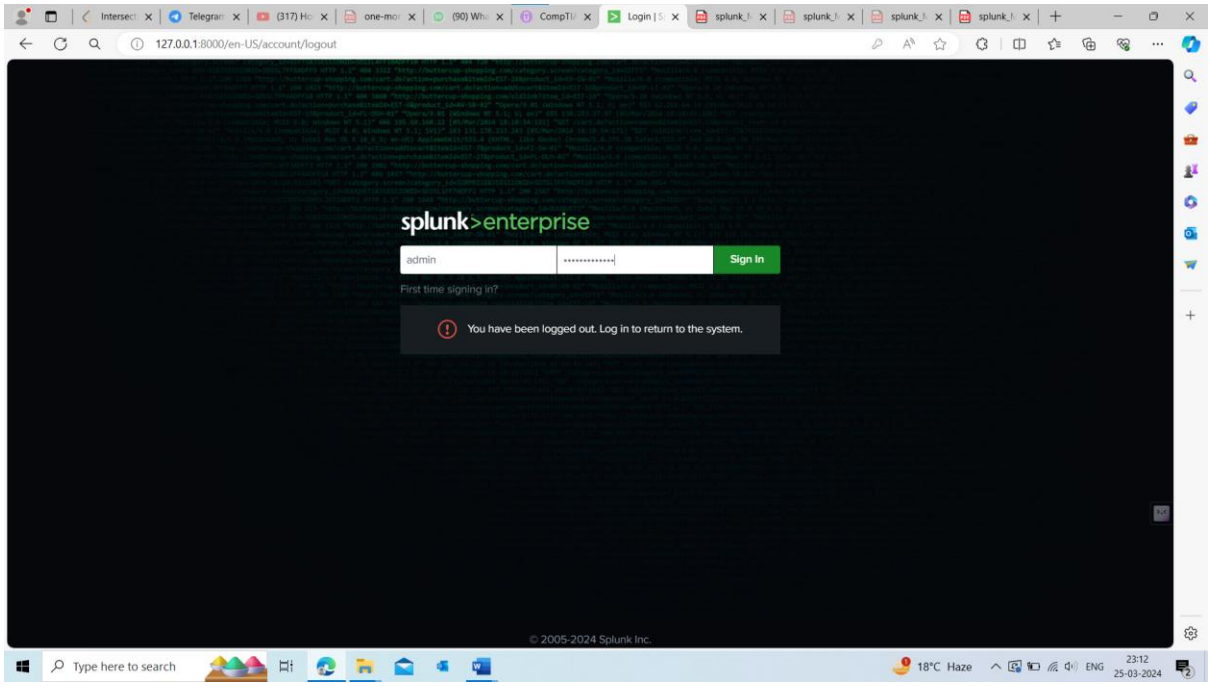
21. Return to the Search view.

22. Search the web application data for all events where a user purchased a product successfully. Use the stats sum function to sum the Price field by ProductName. Name the resulting field Revenue.
Command : index=main sourcetype="access_combined_wcookie" file=success.do status=200 | stats sum(Price) as Revenue by ProductName

MODULE 10: CREATING ALERTS

Task 1: Change user account and run a sample search.

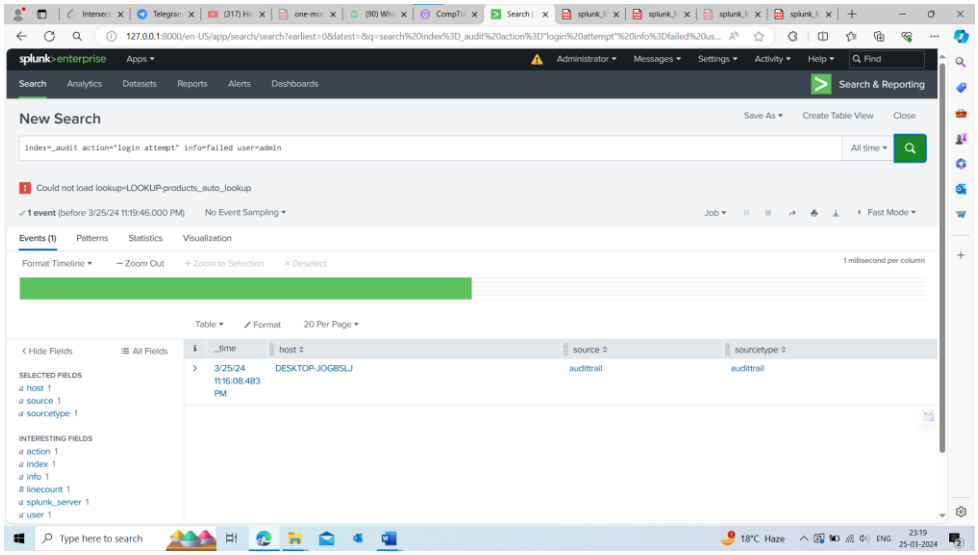
1. Log out of Splunk Enterprise using the uname > Logout menu
2. Enter admin for user name and the password of WrongPassword.



3. Now, enter admin for user name and the password you selected in Module

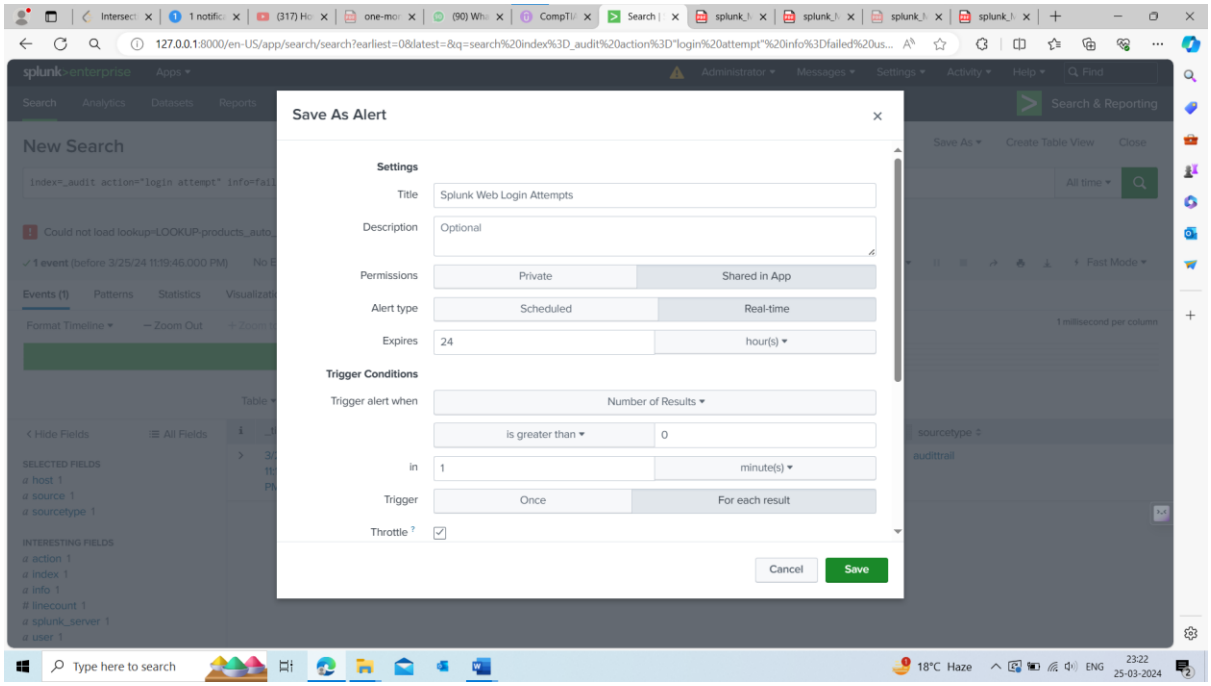
4.Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)

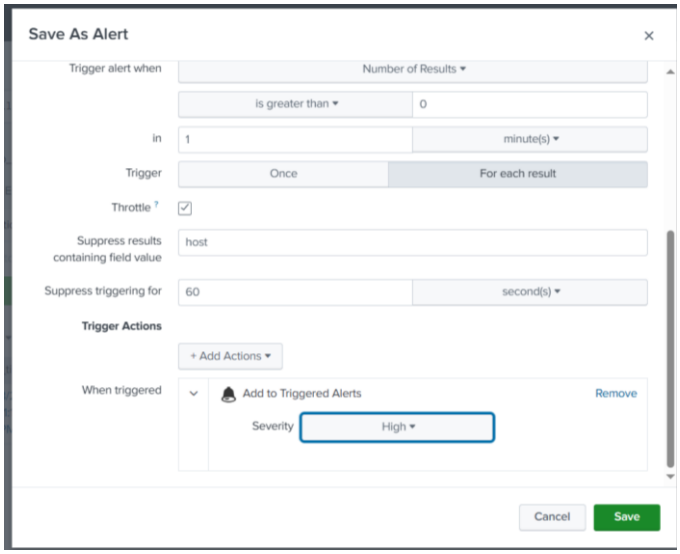
5. Search the _audit index for events where the action of "login attempt" returned a "failed" info value for the username of admin over the Last 15 Minutes.
Command : index=_audit action="login attempt" info=failed user=admin



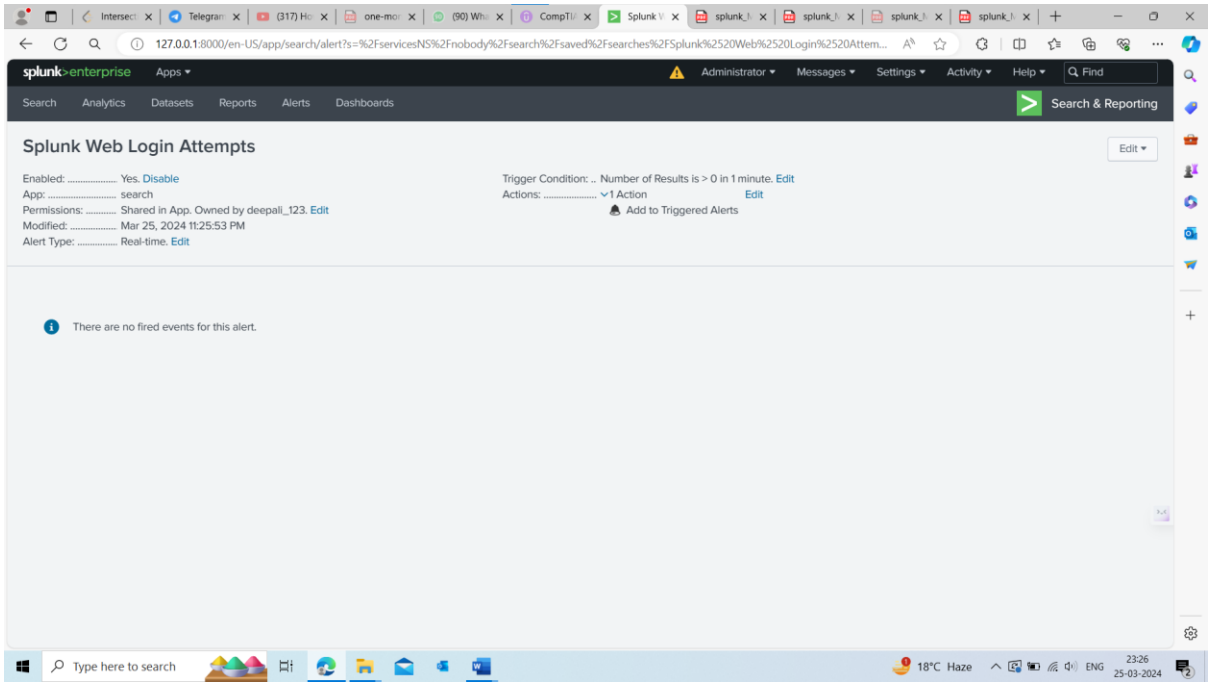
Task 2: Create an alert.

6. From the Save As menu, select Alert.
7. Title the alert: Splunk Web Login Attempts
8. For Permissions, select Shared in App.
9. For Alert type, select Real-time
10. For Trigger alert when, select Number of Results.
11. Set the number of results to: is greater than 0.
12. The in field should be set to 1 minute
13. For Trigger, select For each result.
14. Check the Throttle checkbox
15. For Suppress results containing field value, type: host
16. Make sure Suppress triggering for is set to 60 seconds.
17. Click Add Actions and select Add to Triggered Alerts.
18. Set the Severity to High.

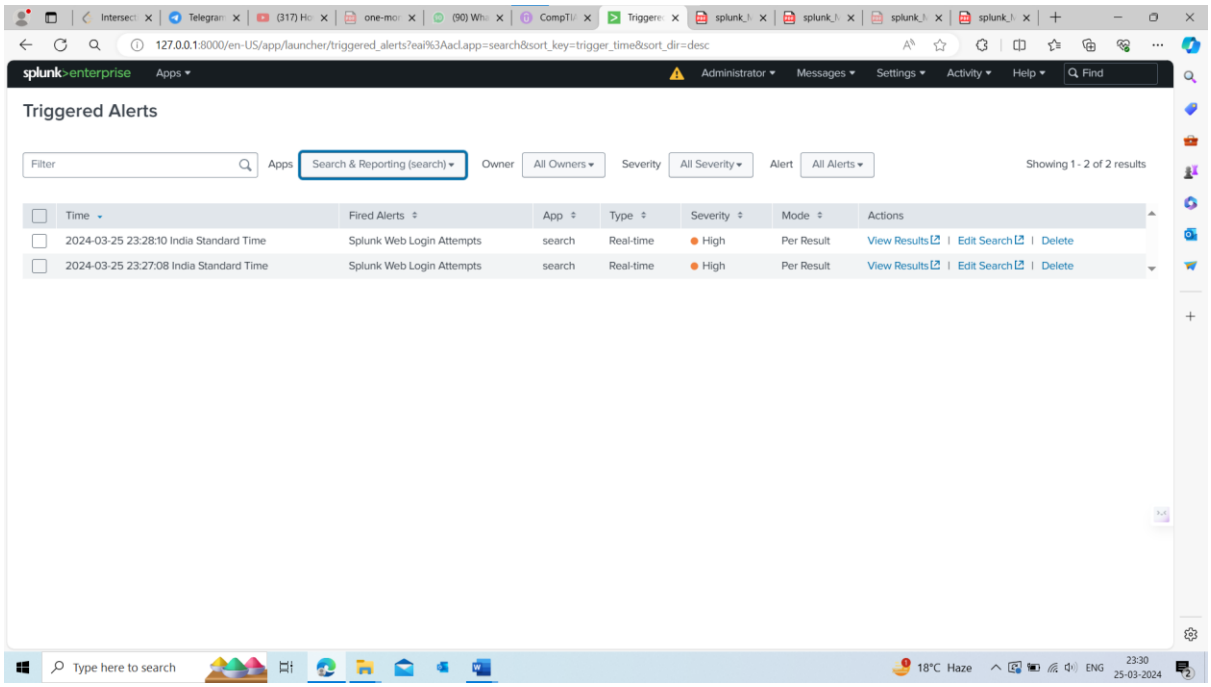




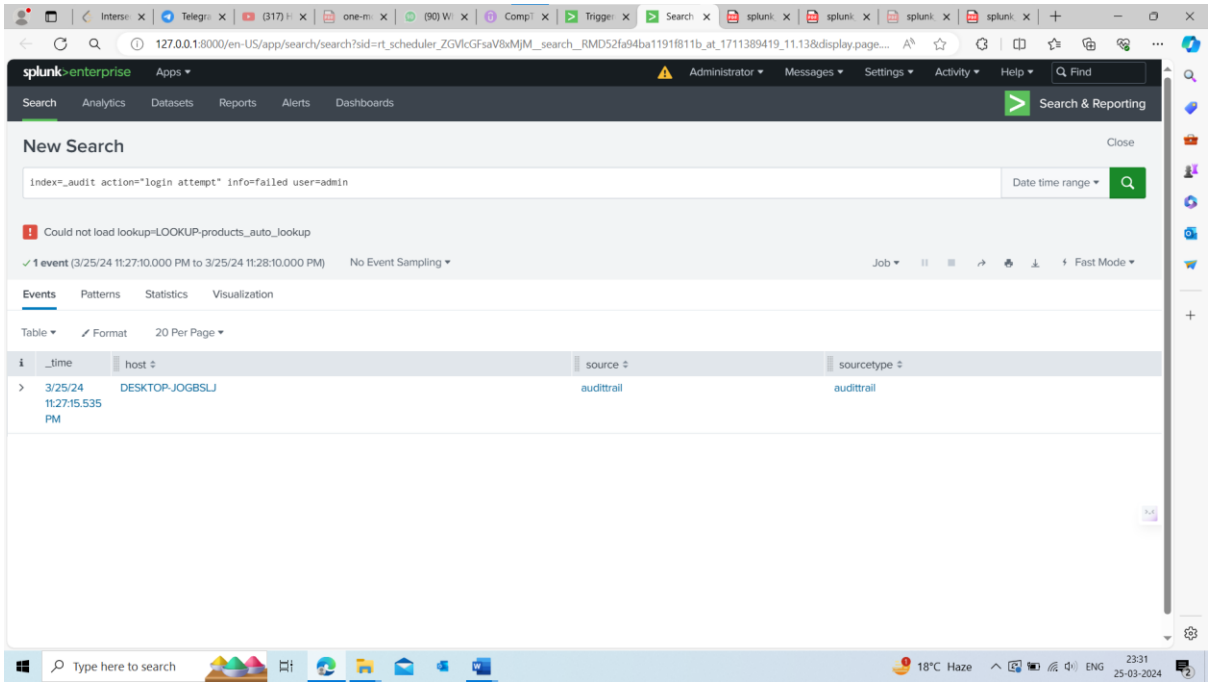
19. Click Save and Click View Alert.



20. Log out of Splunk Enterprise using the Administrator > Logout menu
21. Enter admin for user name and the password of WrongPassword three times in a row.
22. Now, enter admin for user name and the correct password.
23. From the Splunk bar, click Activity > Triggered Alerts.
24. Make sure Search & Reporting is selected for App.



25. Click the View results link on a triggered alert to see the event(s) that caused the alert.



Ques: Difference between fast mode , smart mode and verbose mode in splunk.

Ans : The **Fast mode turns off field discovery for event searches. The field and event data is turned off for searches with the stats command. The Smart mode turns on field discovery for event searches. The Smart mode is the default setting. The Verbose mode returns all field and event data**.