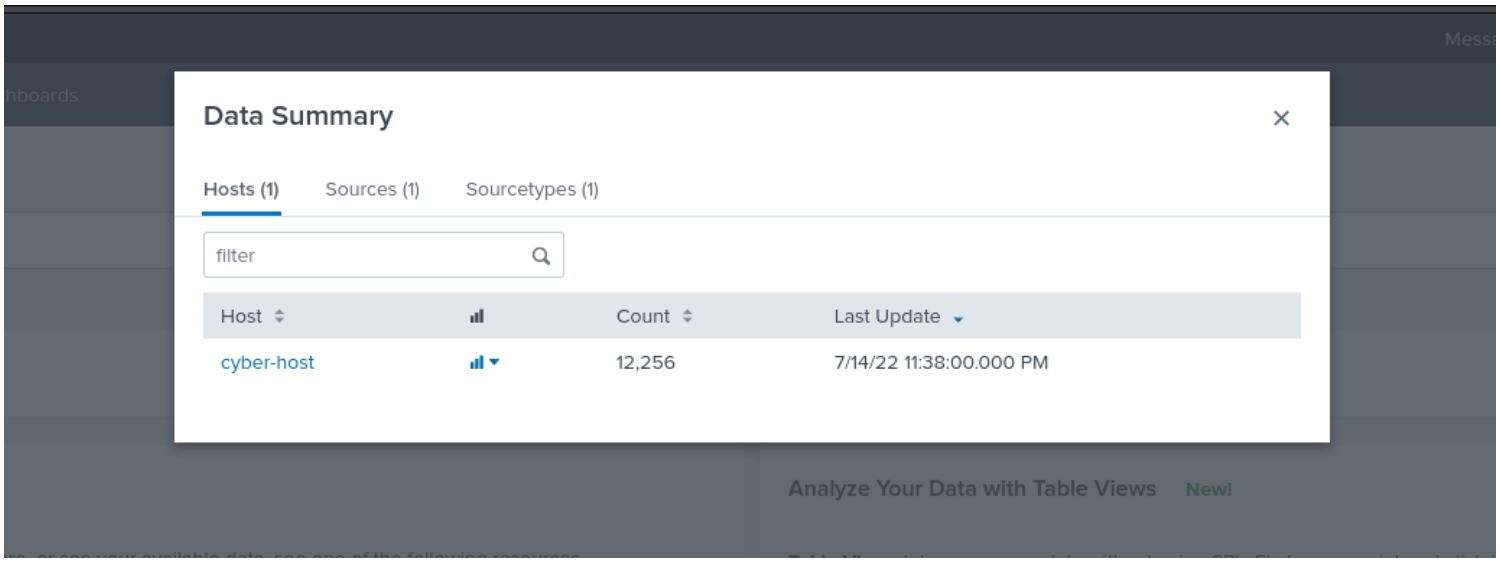
Splunk: Exploring SPL

INTRODUCTION
Splunk is a powerful SIEM solution that provides the ability to search and explore machine data. **Search Processing Language (SPL)** is used to make the search more effective. It comprises various functions and commands used together to form complex yet effective search queries to get optimized results.
This room will dives into some key fundamentals of searching capability, like chaining SPL queries to construct simple to complex queries.

What is the name of the host in the Data Summary tab?

cyber-host ✓ Correct

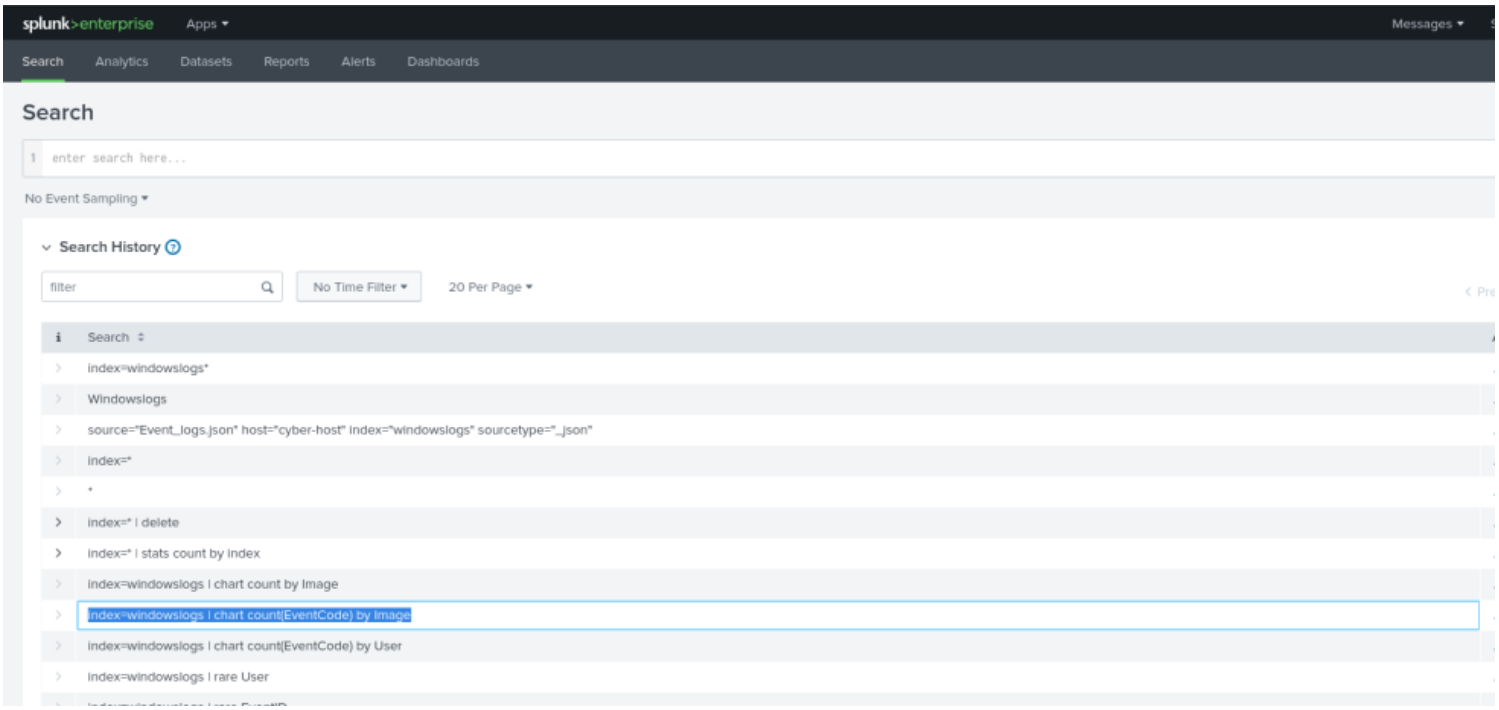
The filter " index=windowslogs *" is used to filter data from the "windowslogs" index, showing all events represented by the asterisk ().
Time filter set to all, to get all the existing logs. By this I was able to retreive the host name from the data summary tab.



In the search History, what is the 7th search query in the list? `(excluding your searches from today)`

index=windowslogs | chart count(EventCode) by Image ✓ Correct

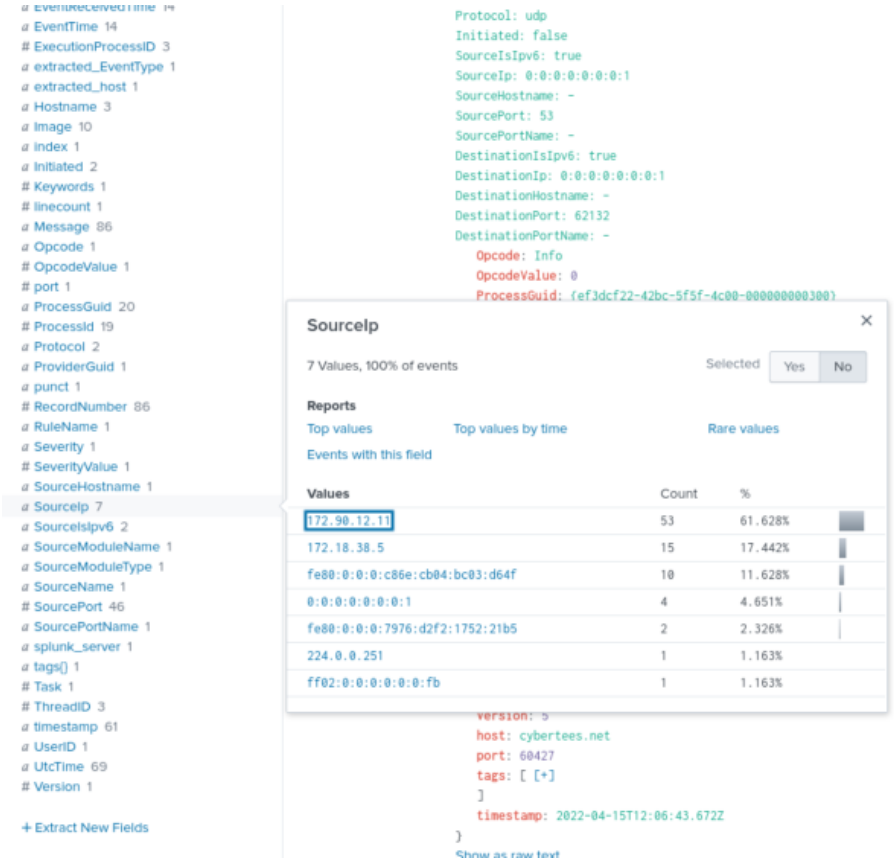
Setting no time filter to get all possible logs with the time duration set to week to date.
I also ignored all the logs for today and obtained the answer at the 7th place from the first search that did not occur today just as seen below.



In the left field panel, which Source IP has recorded max events?

172.90.12.11 ✓ Correct

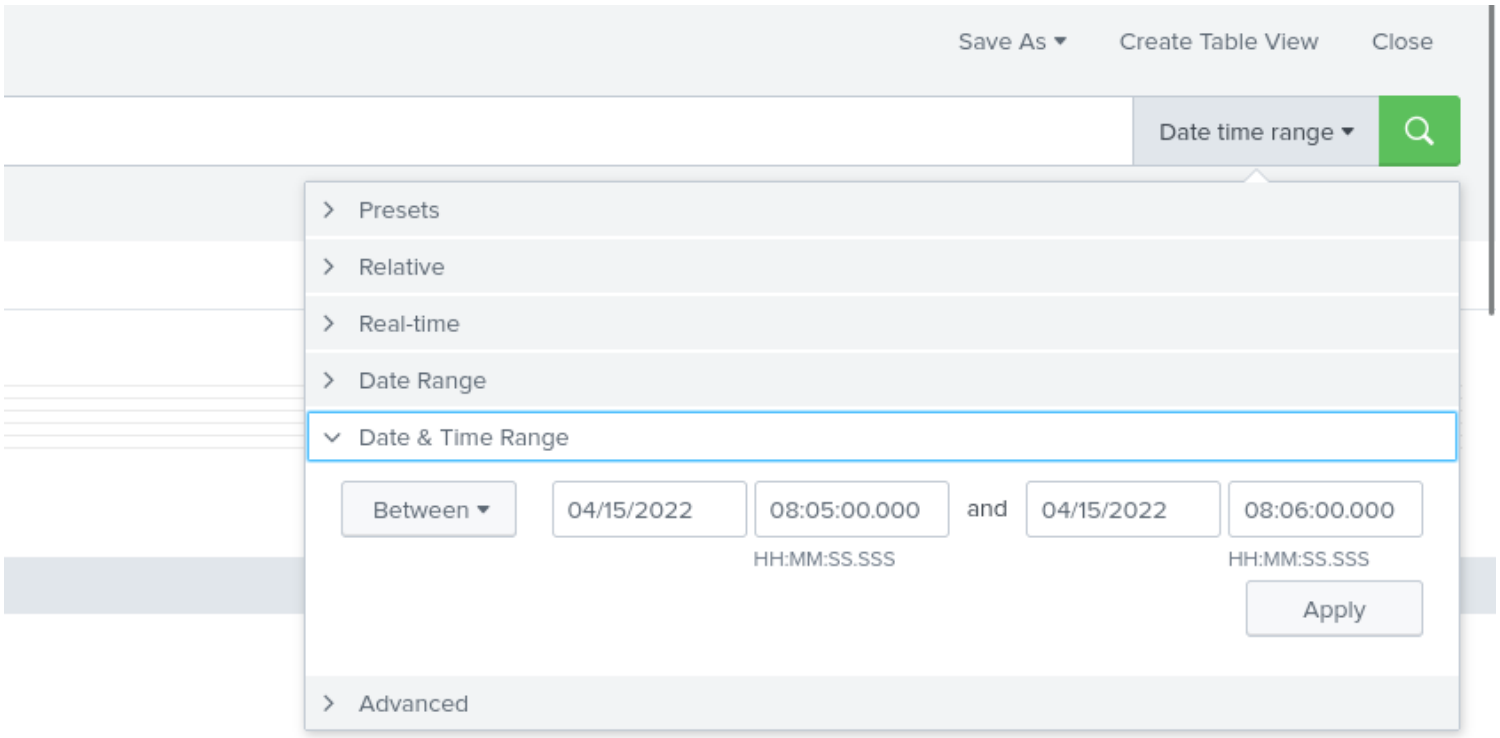
I used the new search query to search for source ip. host="cyber-host" sourceip as shown in the image below.

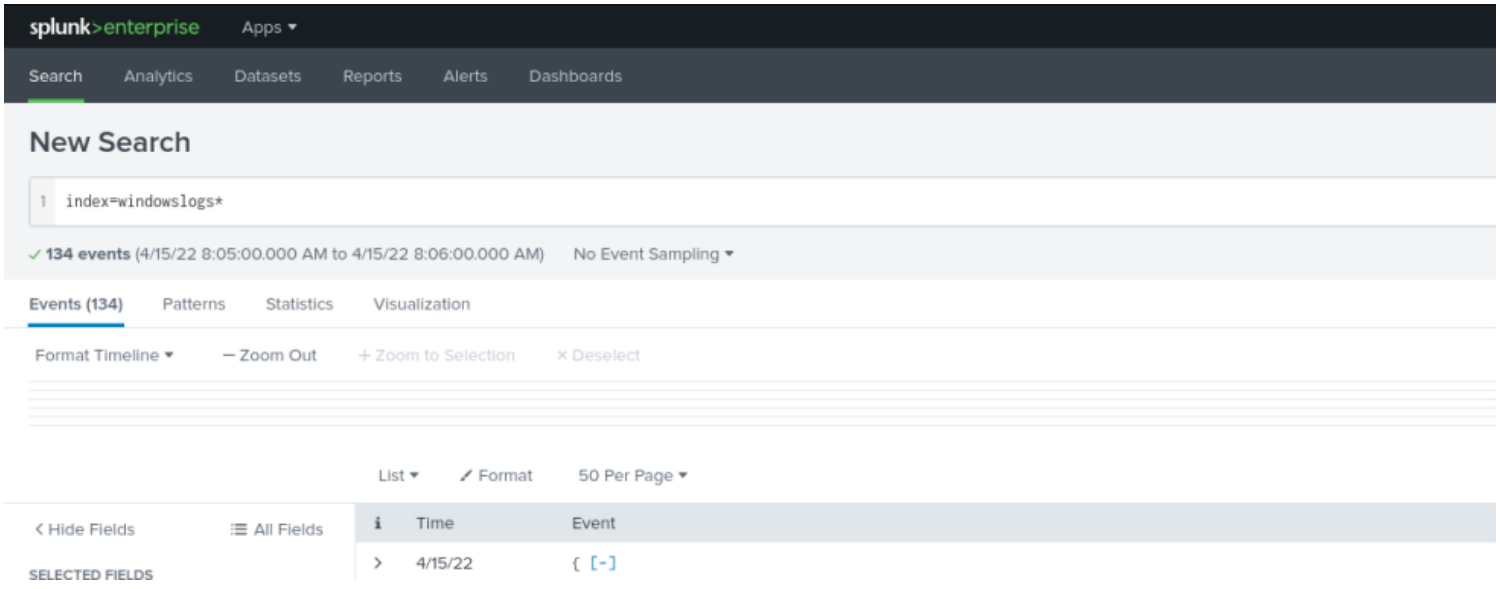


How many events are returned when we apply the time filter to display events on 04/15/2022 and Time from 08:05 AM to 08:06 AM?

134 ✓ Correct

I first applied the filters from the question in the splunk web interface as seen below, and then proceeded to search for the results as shown from the second image below.

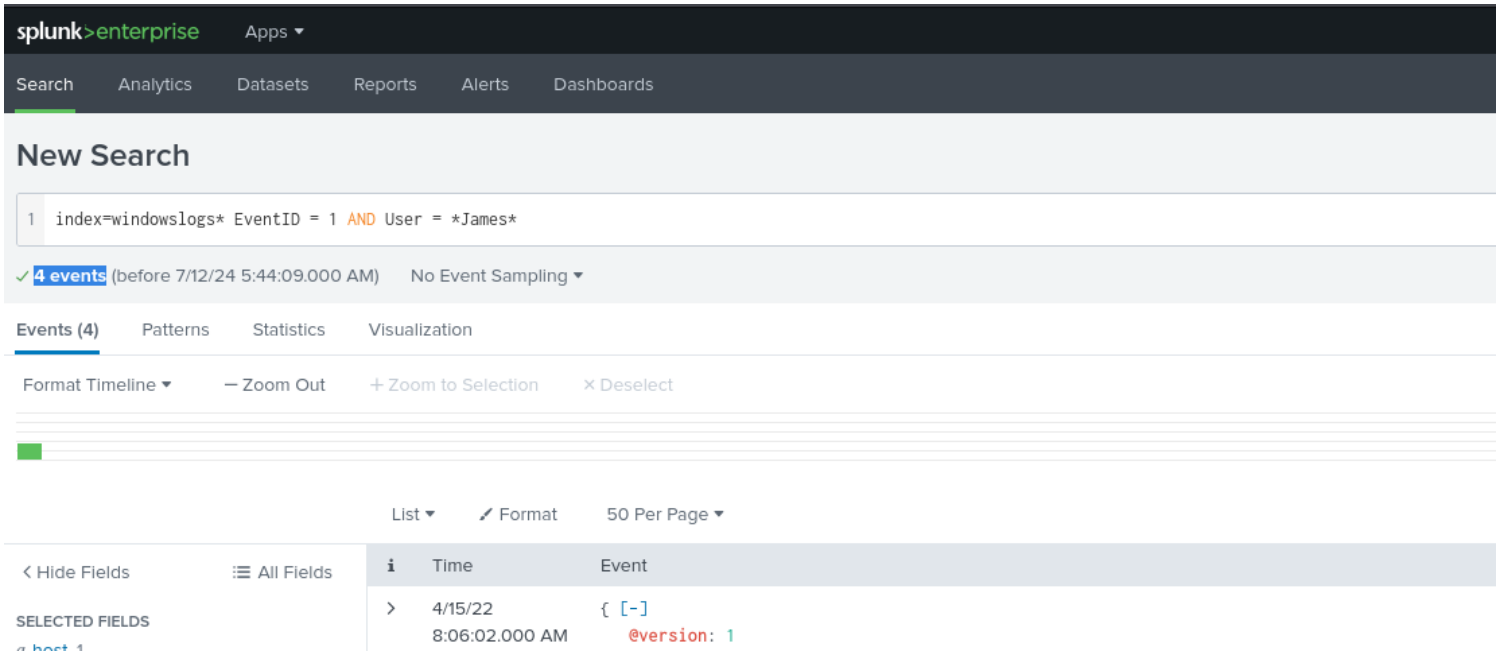




How many Events are returned when searching for Event ID 1 **AND** User as *James*?

4 ✓ Correct

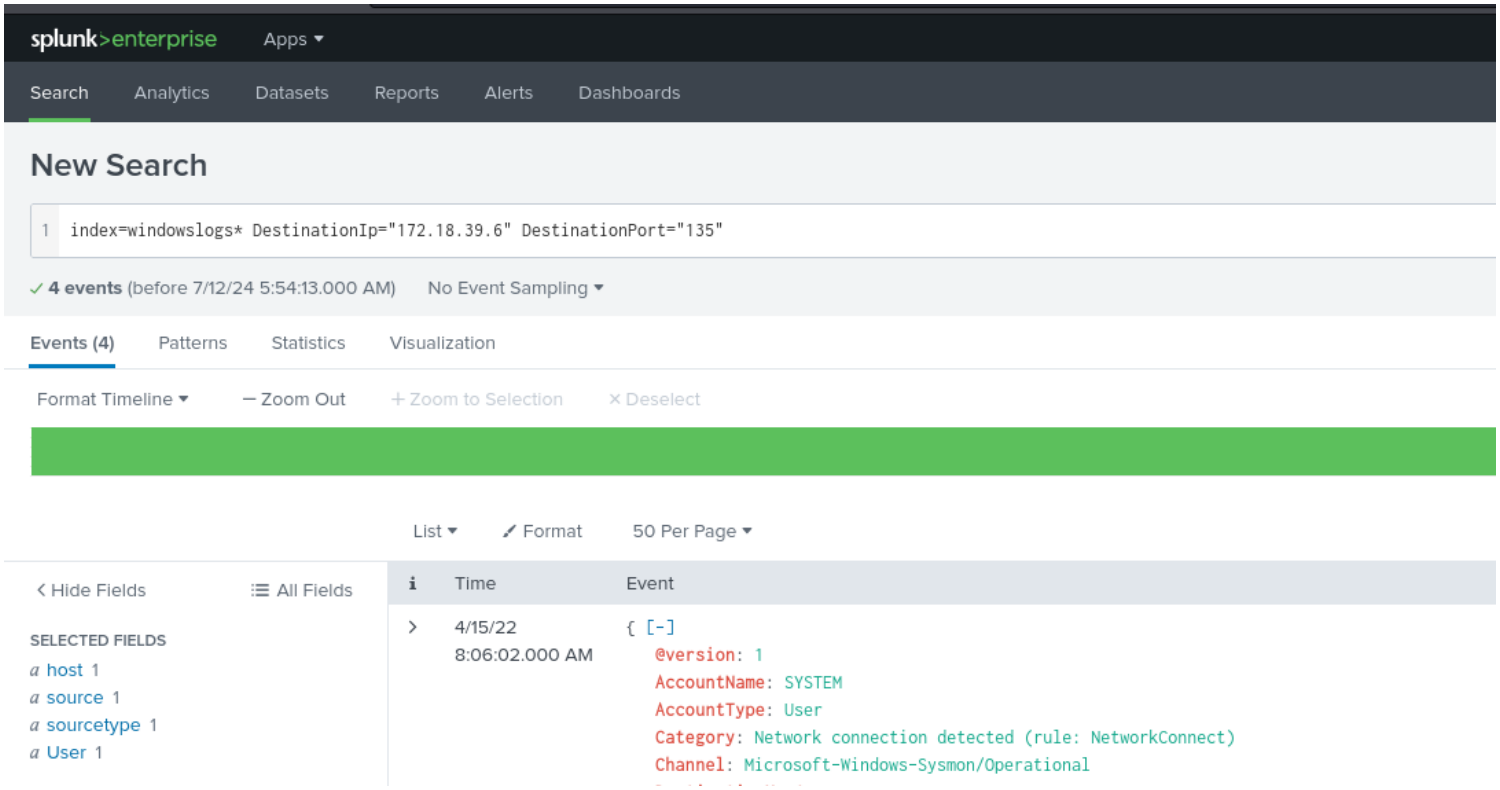
Four events are returned as seen from the image below. This is after applying the boolen operator “AND” in my SPL.



How many events are observed with Destination IP 172.18.39.6 AND destination Port 135?

4 ✓ Correct

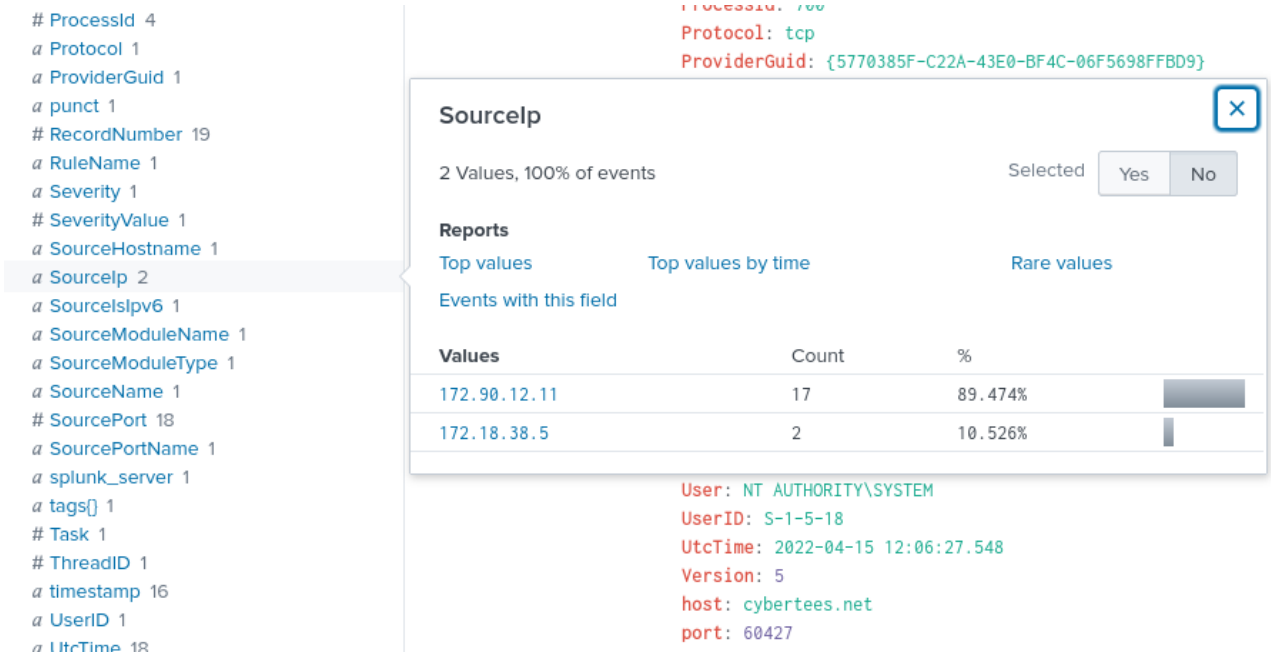
Four events are observed after filtering the results by setting dest ip and dest port as shown in the image below.



What is the Source IP with highest count returned with this Search query?
Search Query: index=windowslogs Hostname="Salena.Adam" DestinationIp="172.18.38.5"

172.90.12.11 ✓ Correct

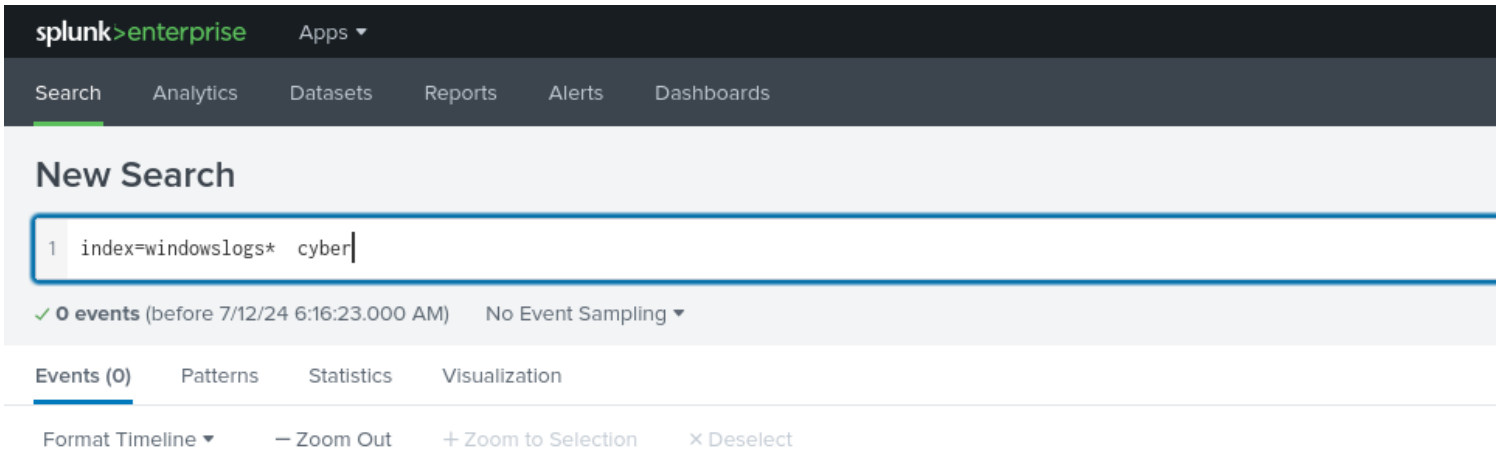
Given the **Search Query: index=windowslogs * Hostname="Salena.Adam" DestinationIp="172.18.38.5"**, From the results returned, I checked the ip from the sourceip column as seen below.



In the index windowslogs, search for all the events that contain the term **cyber** how many events returned?

0 ✓ Correct

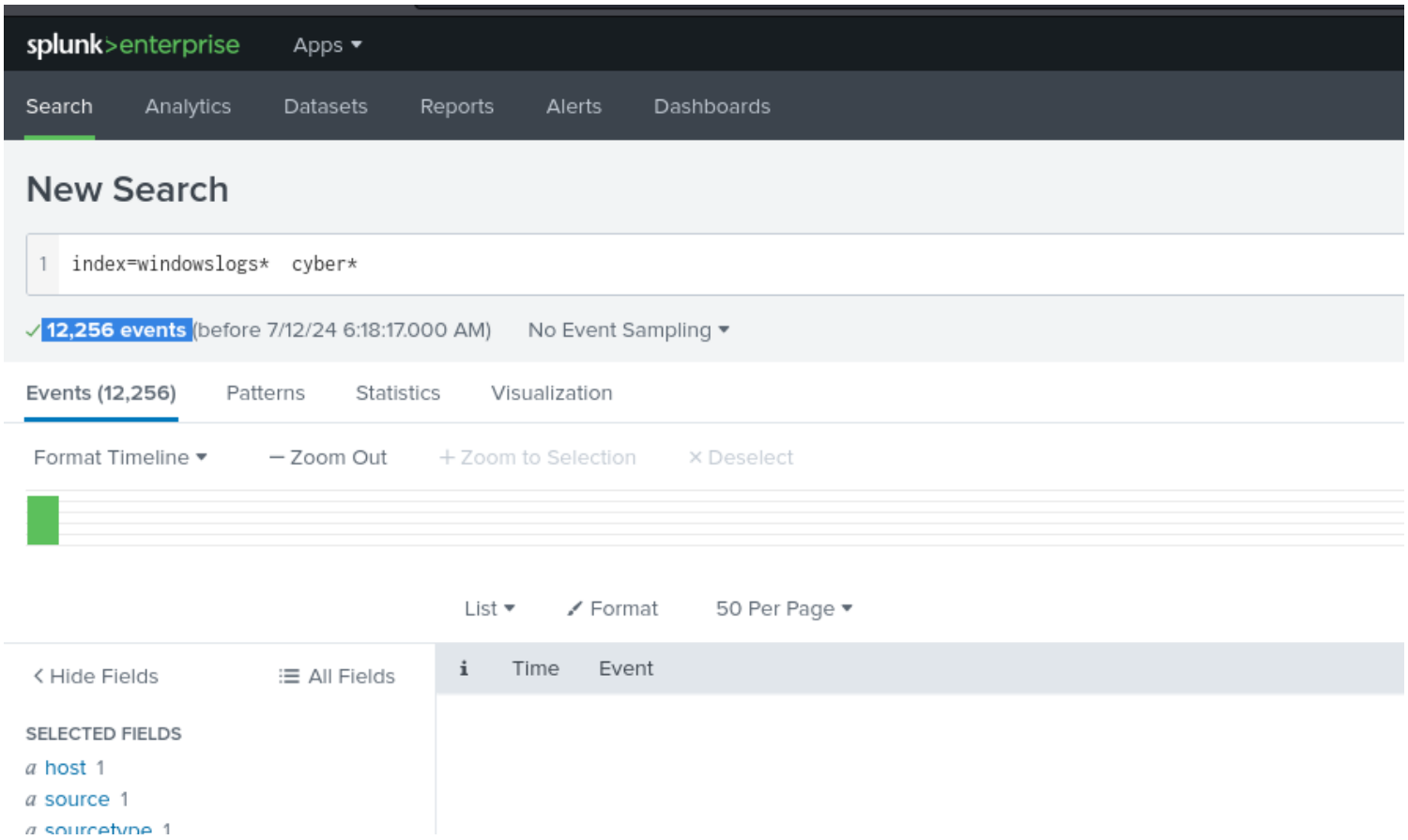
Using this SPL "index=windowslogs* cyber" events that contain the cyber term is zero.



Now search for the term **cyber***, how many events are returned?

12256 ✓ Correct

Though by adding * as per the instructions from the quiz above, the result returns 12256 events recorded.

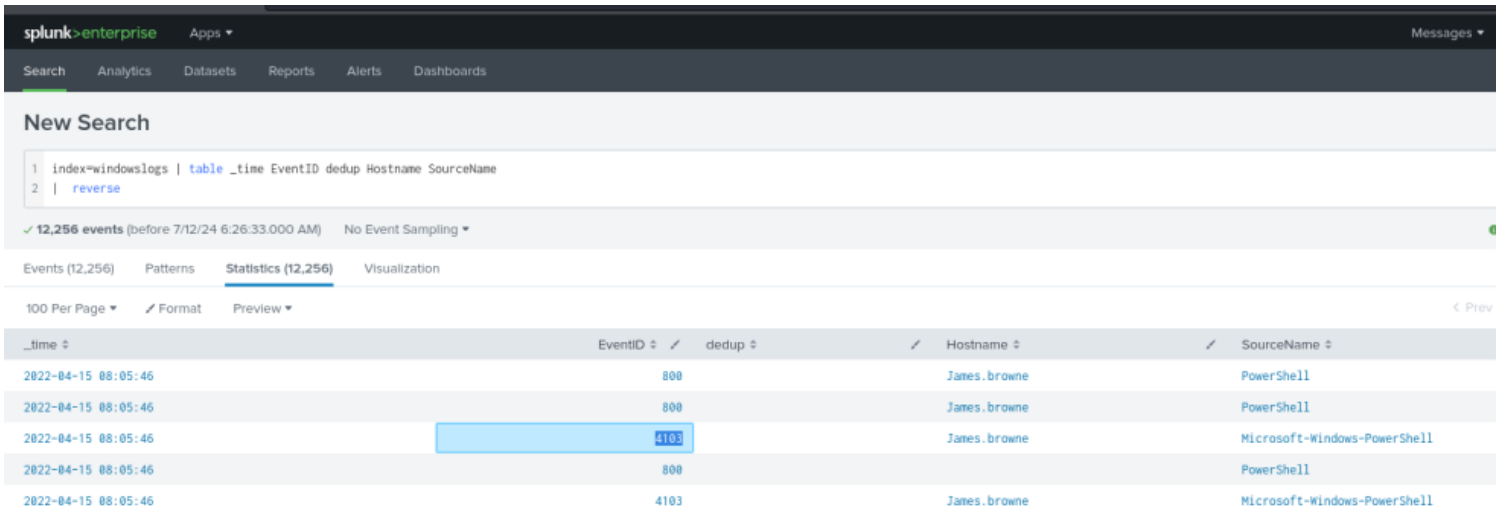


What is the third EventID returned against this search query?

Search Query: `index=windowslogs | table _time EventID Hostname SourceName | reverse`

4103 ✓ Correct

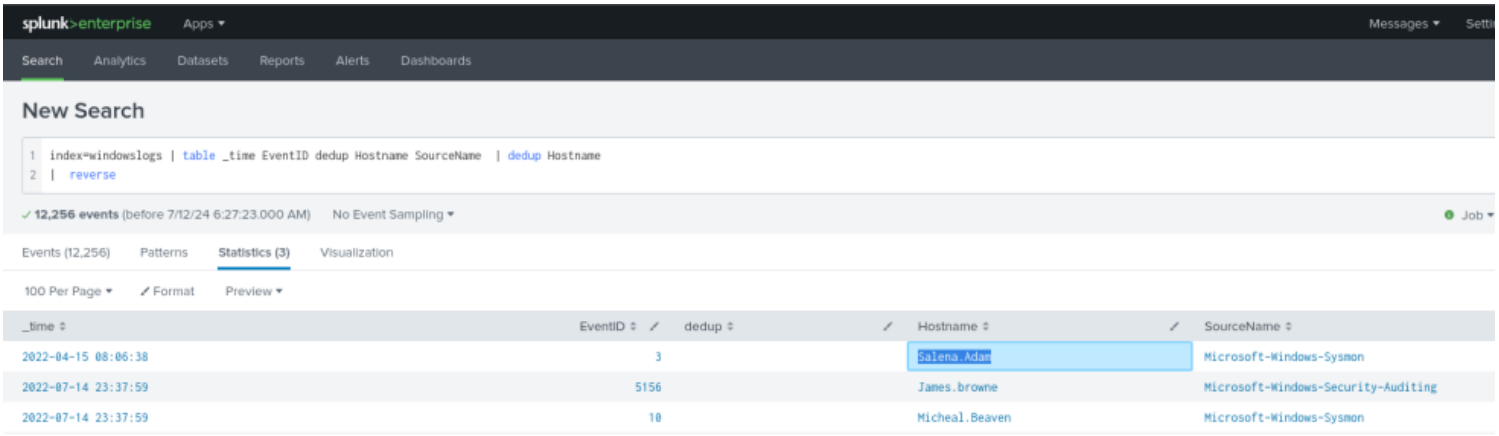
Using this **Search Query:**
index=windowslogs | table _time EventID Hostname SourceName | reverse, I was able to retrieve the results as shown below.



Use the dedup command against the Hostname field before the reverse command in the query mentioned in Question 1. What is the first username returned in the H

Salena.Adam ✓ Correct

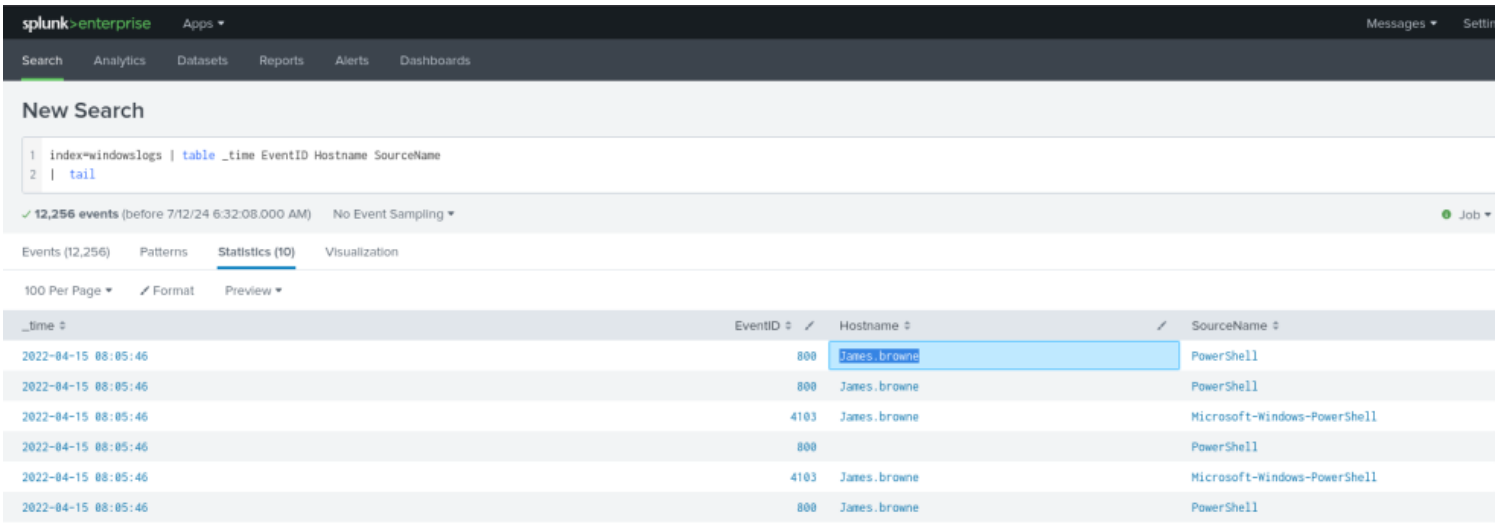
dedup cmd in SPL is used to remove duplicate values. By applying it in the Hostname field, I was able to retreive the first username as shown in the image below.



Using the Reverse command with the search query `index=windowslogs | table _time EventID Hostname SourceName` - what is the HostName that comes on t

James.browne ✓ Correct A

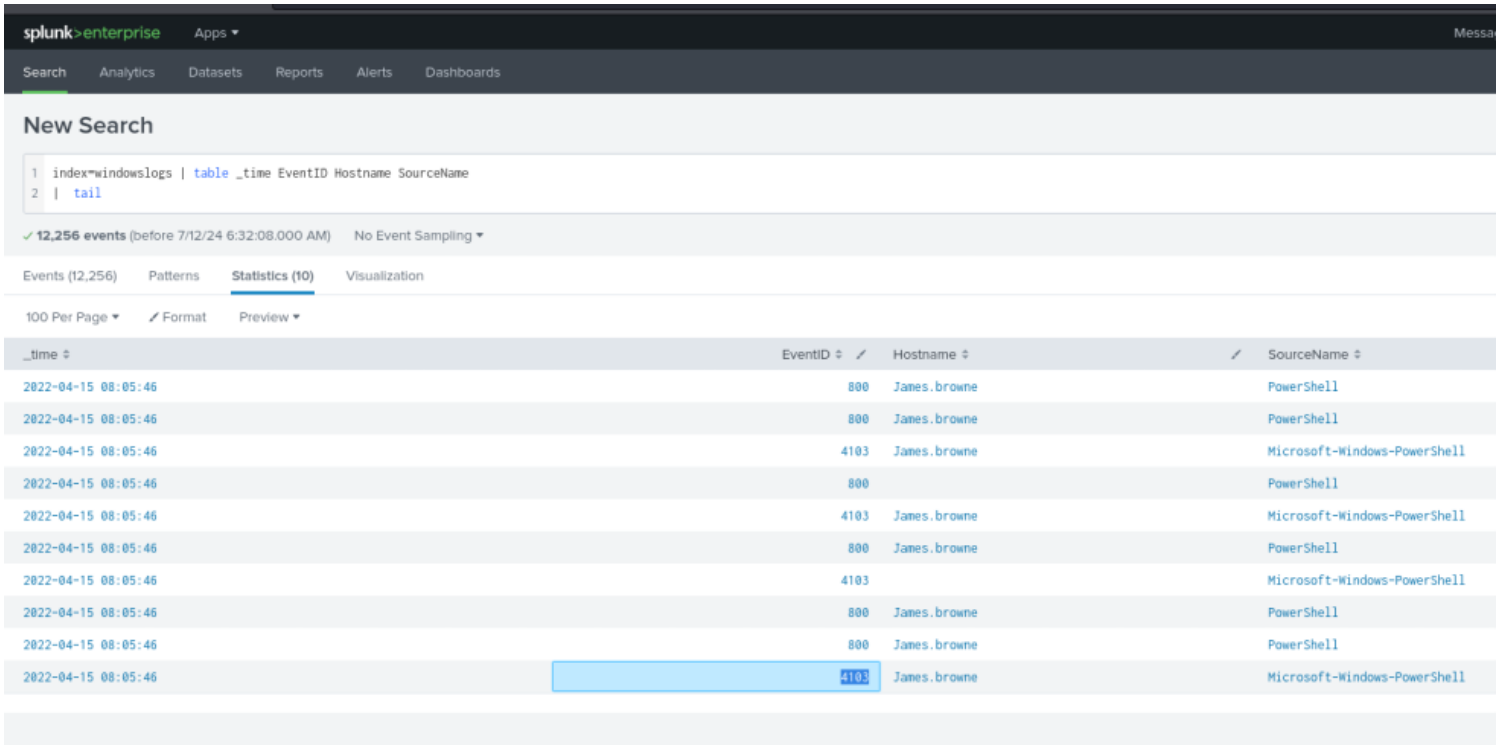
Structuring the results using the "tail" cmd alongside with the SPL query given in the question above, I was able to retreive the Hostname that appeared at the top.



What is the last EventID returned when the query in question 1 is updated with the **tail** command?

4103 ✓ Correct

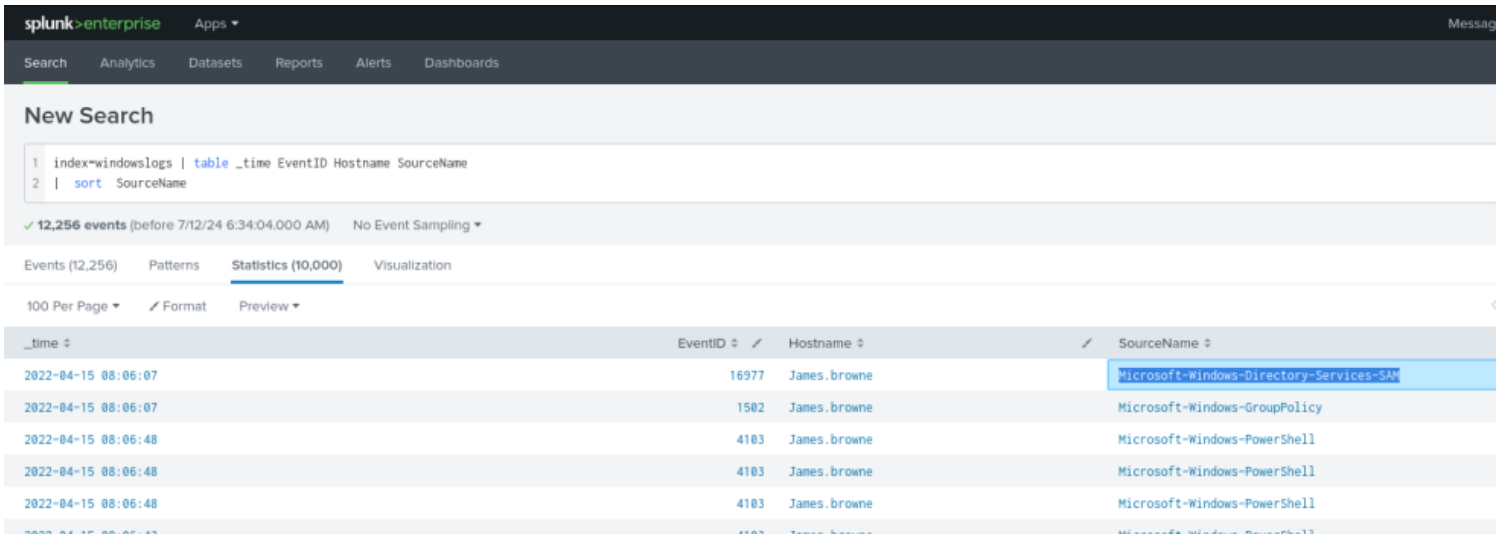
Updating the query in the previous question, I Structuring the results using the "tail" cmd alongside with the SPL query given in the question above, I was able to retreive the EventID that appeared at the bottom.



Sort the above query against the SourceName. What is the top SourceName returned?

Microsoft-Windows-Directory-Services-SAM ✓ Correct

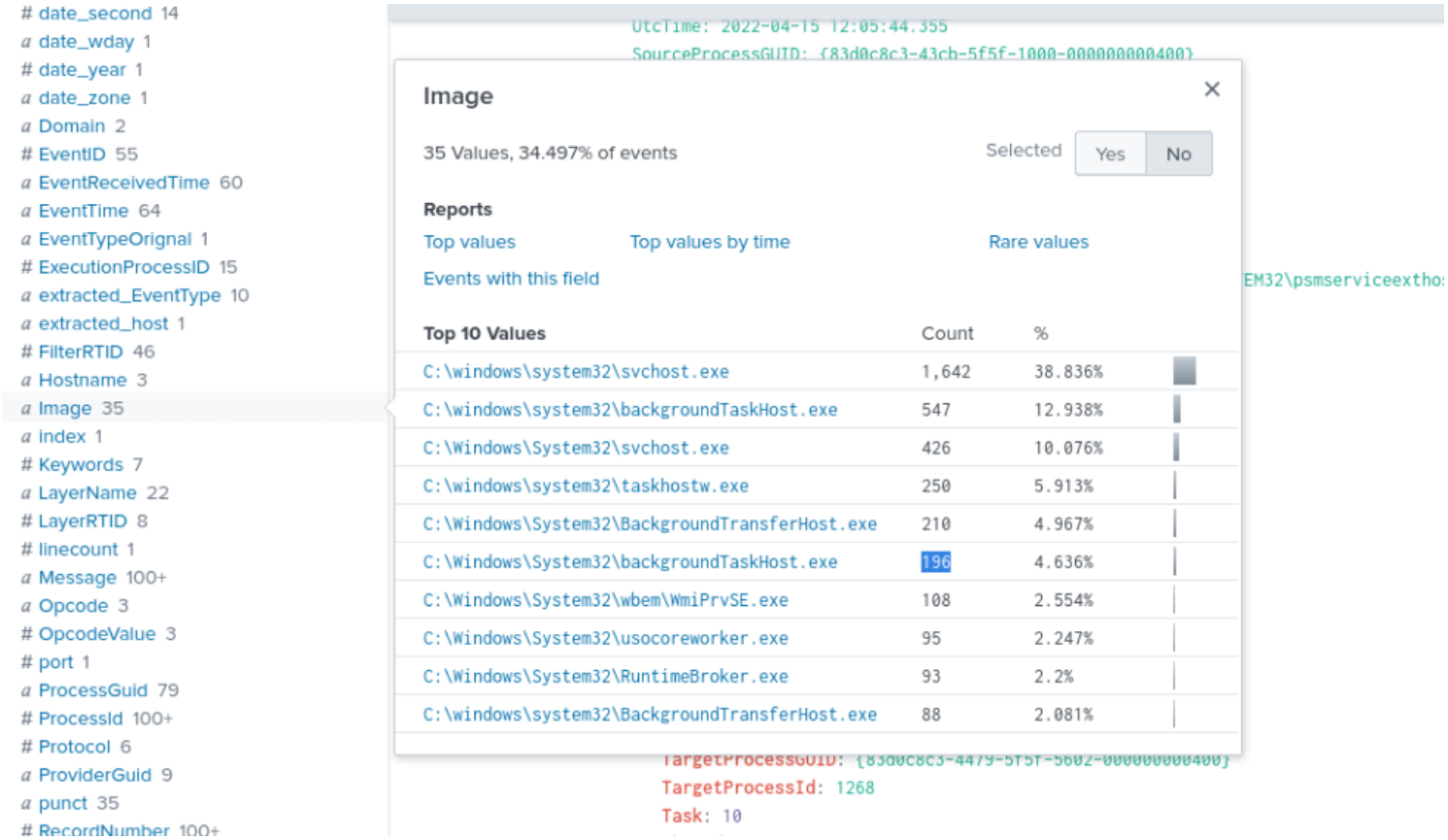
Using the sort keyword, I added it to my SPL query against the SourceName, and successfully retrieved the top sourcename as in the image below.



List the top 8 Image processes using the top command - what is the total count of the 6th Image?

196 ✓ Correct

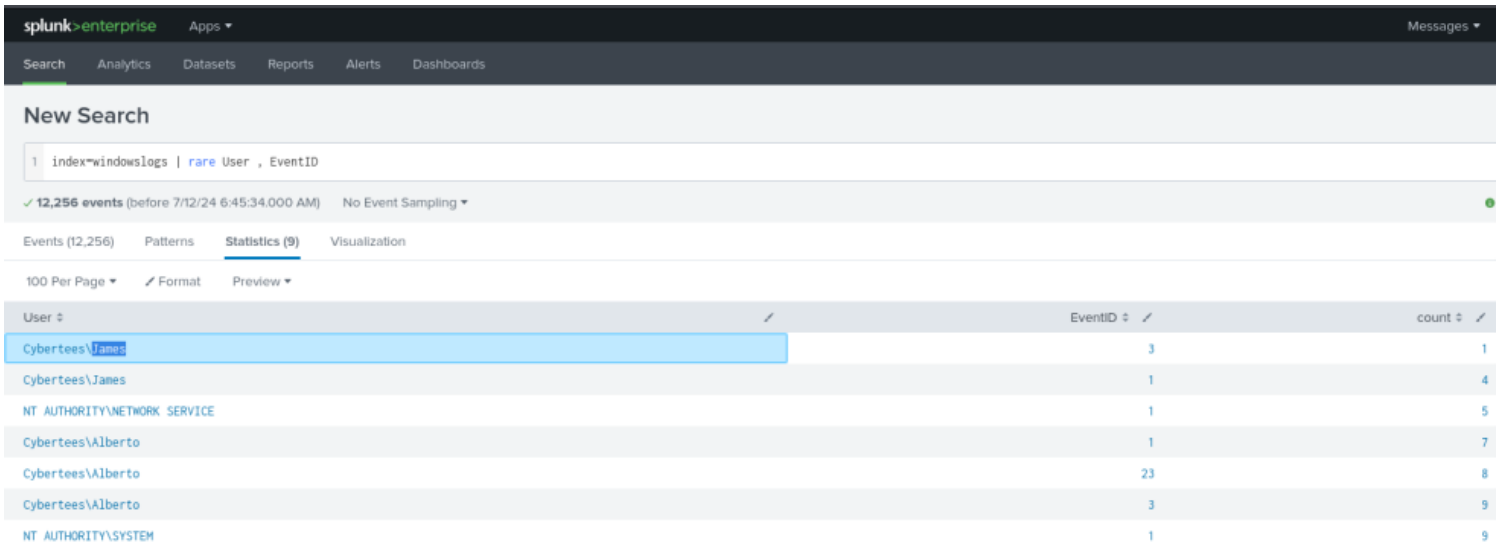
I used the transformational SPL "`top limit=`8 image" to filter the results and checked out the results in the "image" field as shown from the image below.



Using the rare command, identify the user with the least number of activities captured?

James ✓ Correct

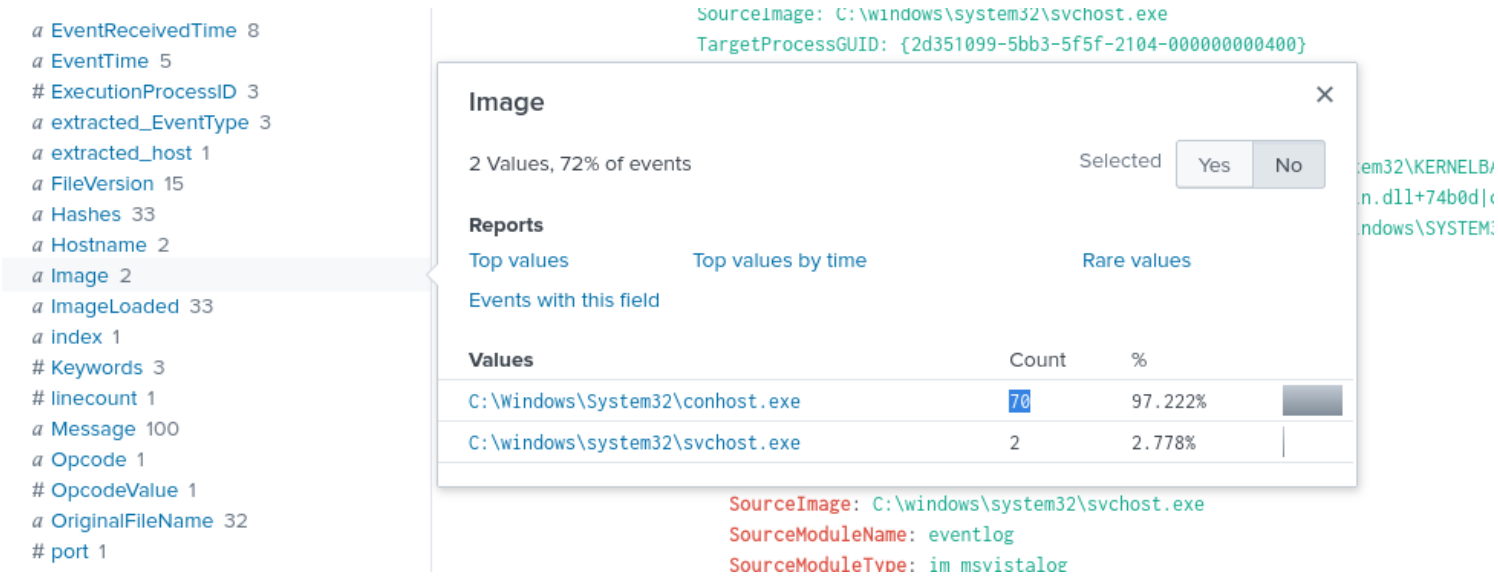
Using the rare cmd as per the instruction from the above task with the User, and Event ID fields, I was able to retrieve the user with the least number of activities. This can be seen from the image below under the statistics tab.



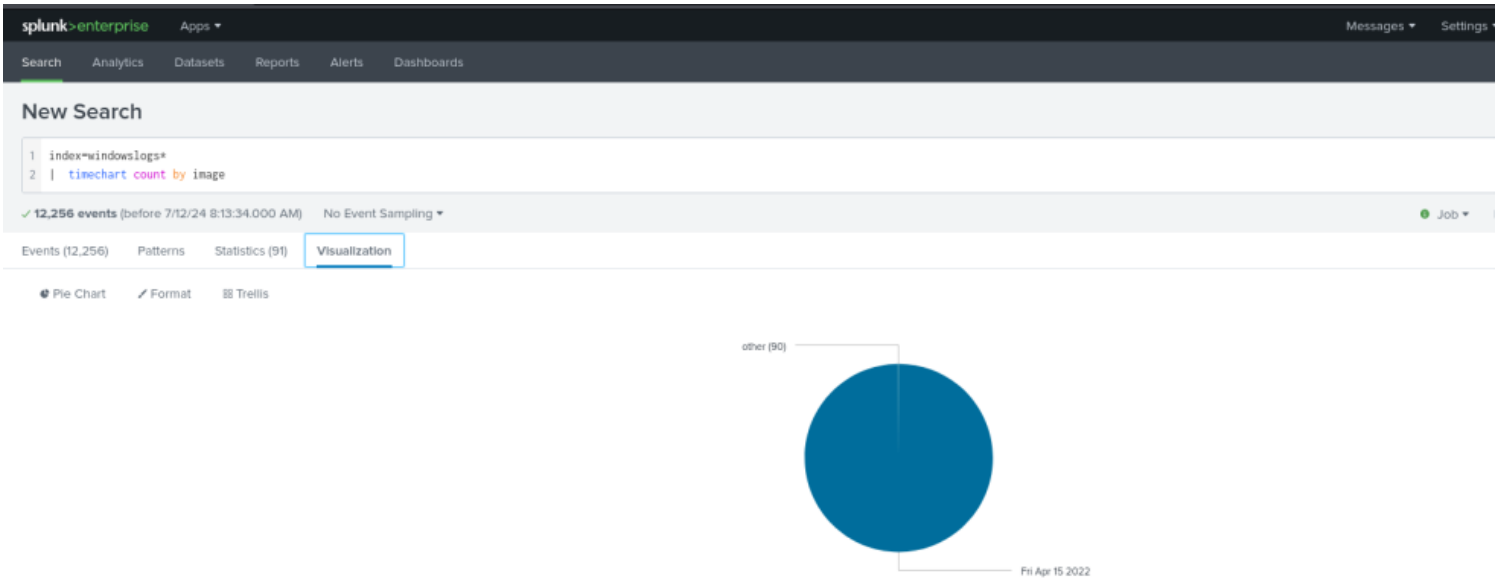
Create a pie-chart using the chart command - what is the count for the conhost.exe process?

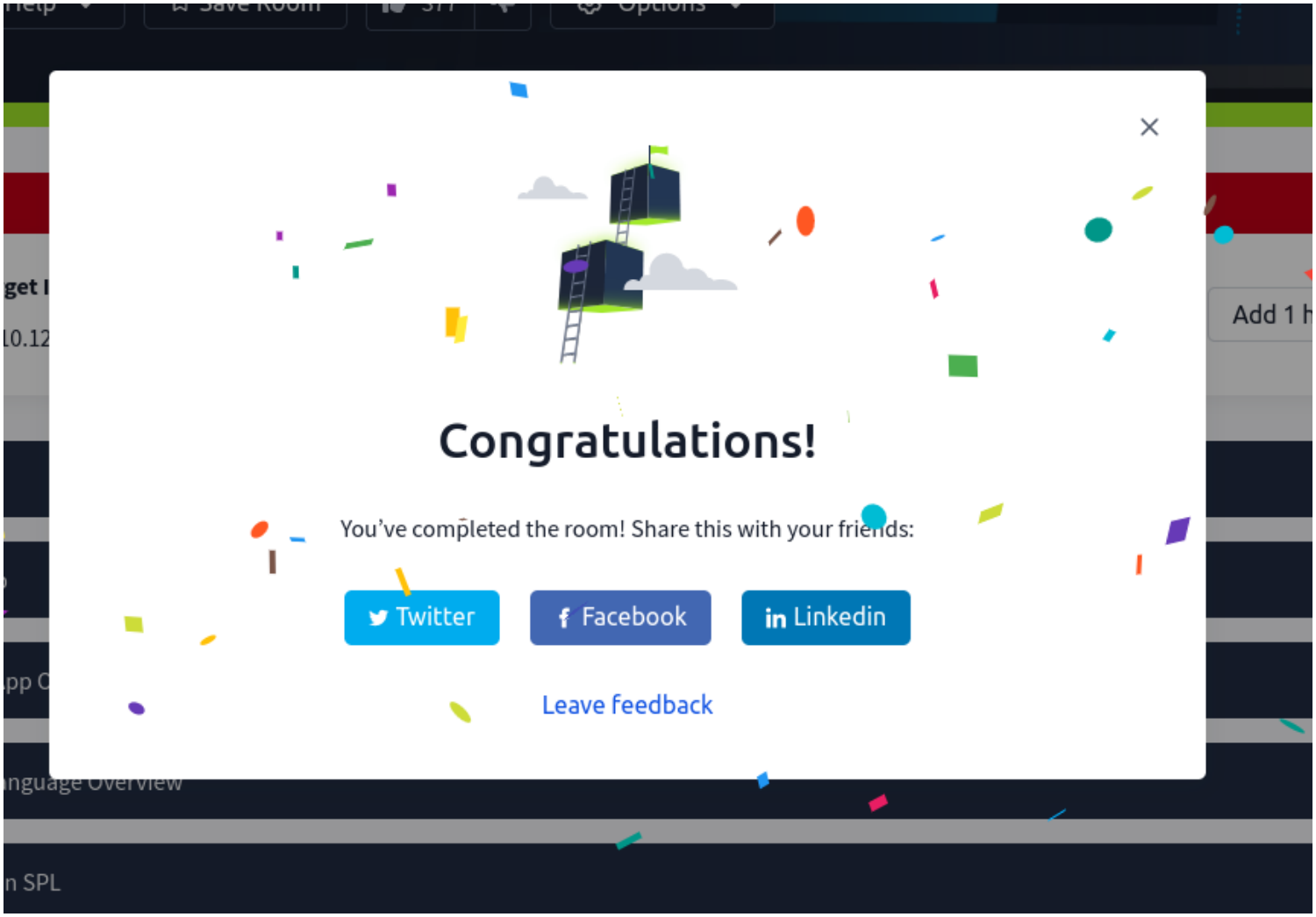
70 ✓ Correct

First, I searched for the conhost.exe process in the search bar and the results were as below.



Using the `timechart count by Image` cmd, the query displayed the Image chart based on the time as seen below.





https://tryhackme.com/r/room/splunkexploringspl

CONCLUSION
n this session, we explored the fundamental aspects of Splunk's powerful search and analysis features, particularly focusing on the Search Processing Language (SPL). As a newcomer to Splunk, it is evident that the tool offers immense potential for analyzing machine-generated data, making it a valuable asset for any organization aiming to leverage its data for actionable insights.

Key Learnings:
1. **Understanding Search Processing Language (SPL)**
2. **Applying Filters to Narrow Down Results**
3. **Using Transformational Commands**
4. **Changing the Order of the Results**

As a new user exploring Splunk for the first time, I find it to be an incredibly powerful and intuitive tool. The ability to search and explore machine data using SPL opens up numerous possibilities for data analysis and operational efficiency. The structured approach to learning SPL, from understanding basic queries to applying filters and using transformational commands, provides a clear pathway to mastering this tool. Indeed, the first interaction with Splunk has been super great, and it is exciting to see the potential it holds for future data-driven endeavors.
In conclusion, this introductory session on Splunk and SPL has been enlightening and promising. The robust functionality and flexibility of Splunk make it an indispensable tool for anyone looking to harness the power of their machine data.