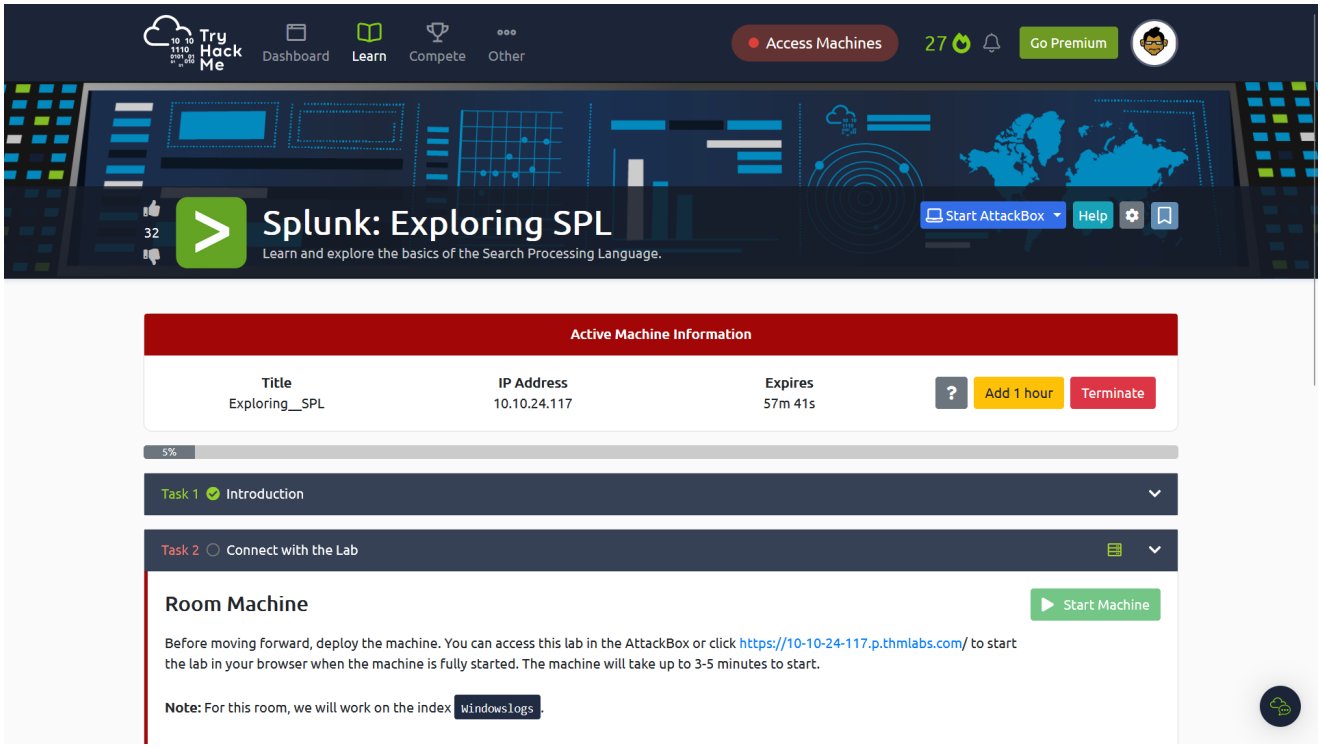
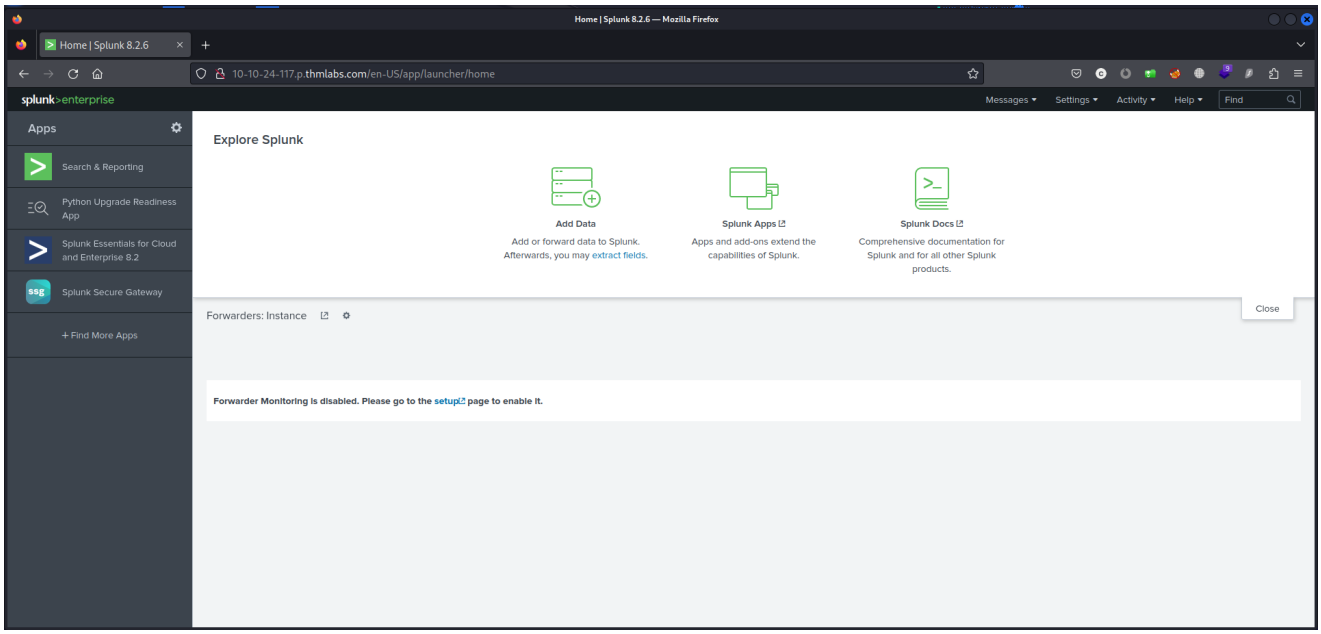
Splunk - Exploring SPL

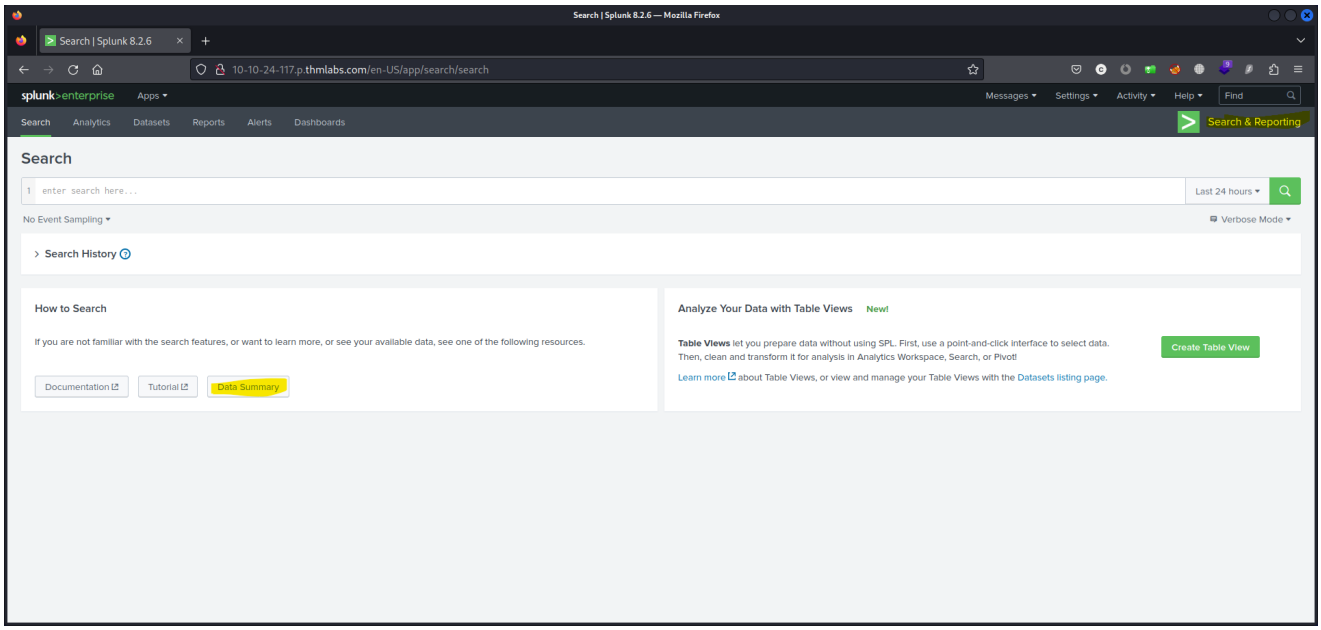
27072023Thu

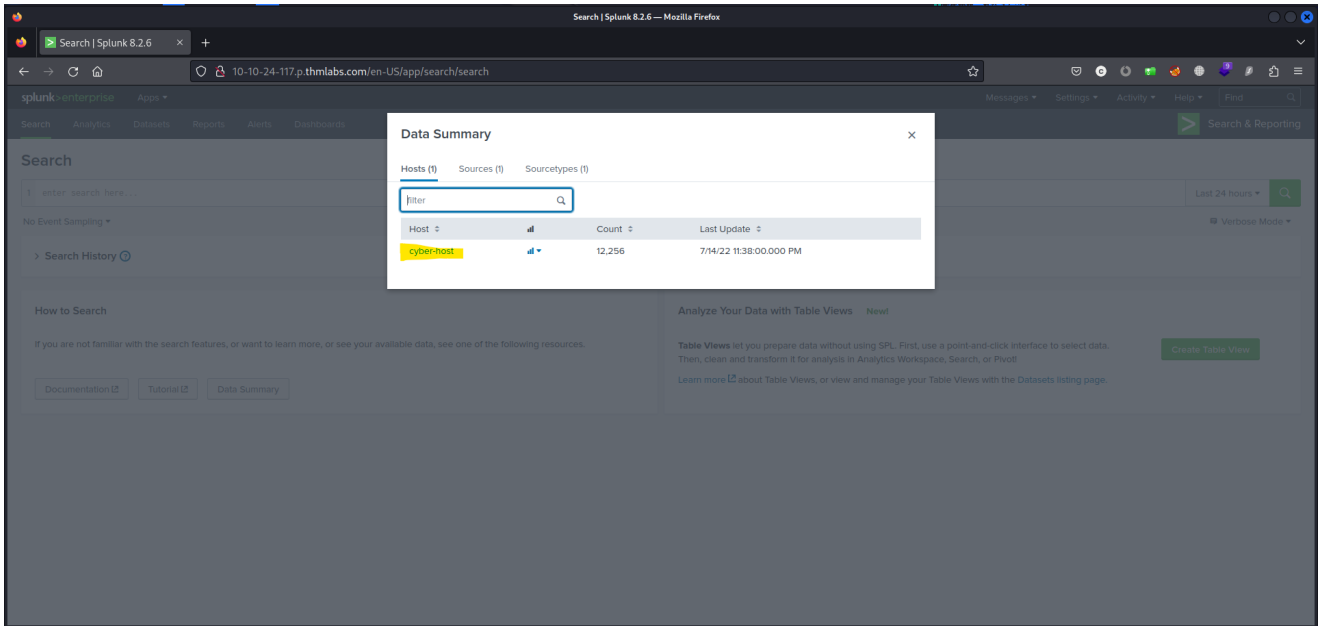
[TryHackMe | Splunk: Exploring SPL]

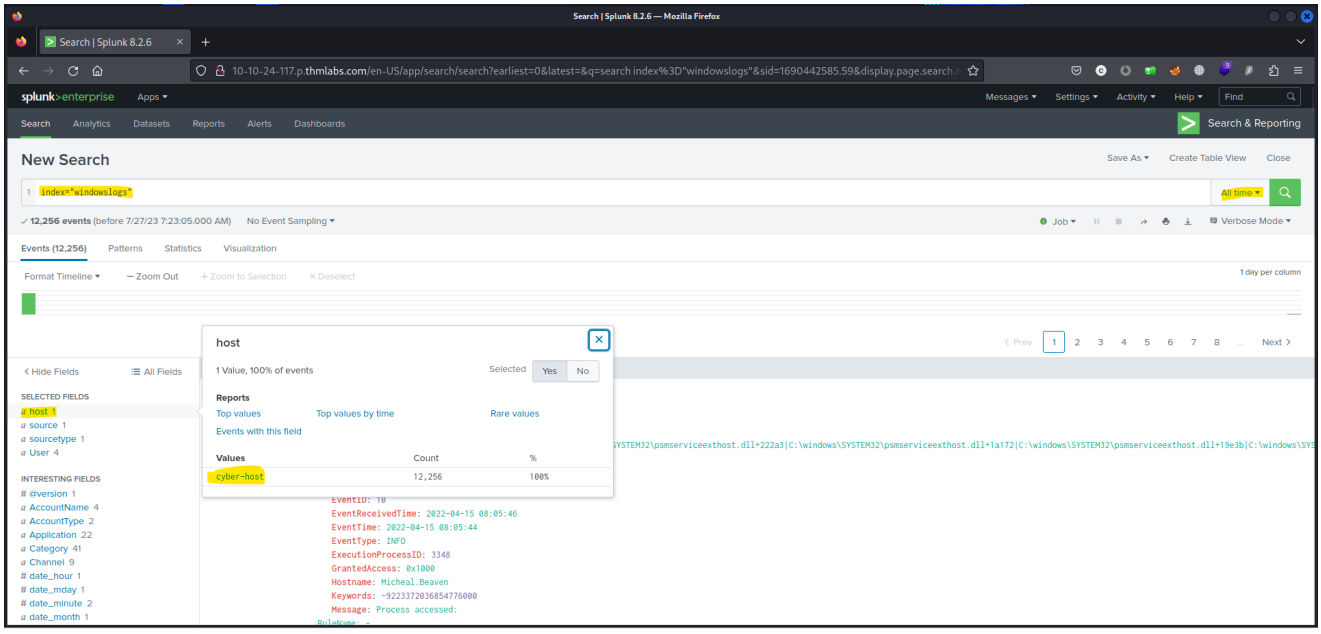
```
Learn and explore the basics of the Search Processing Language.
```







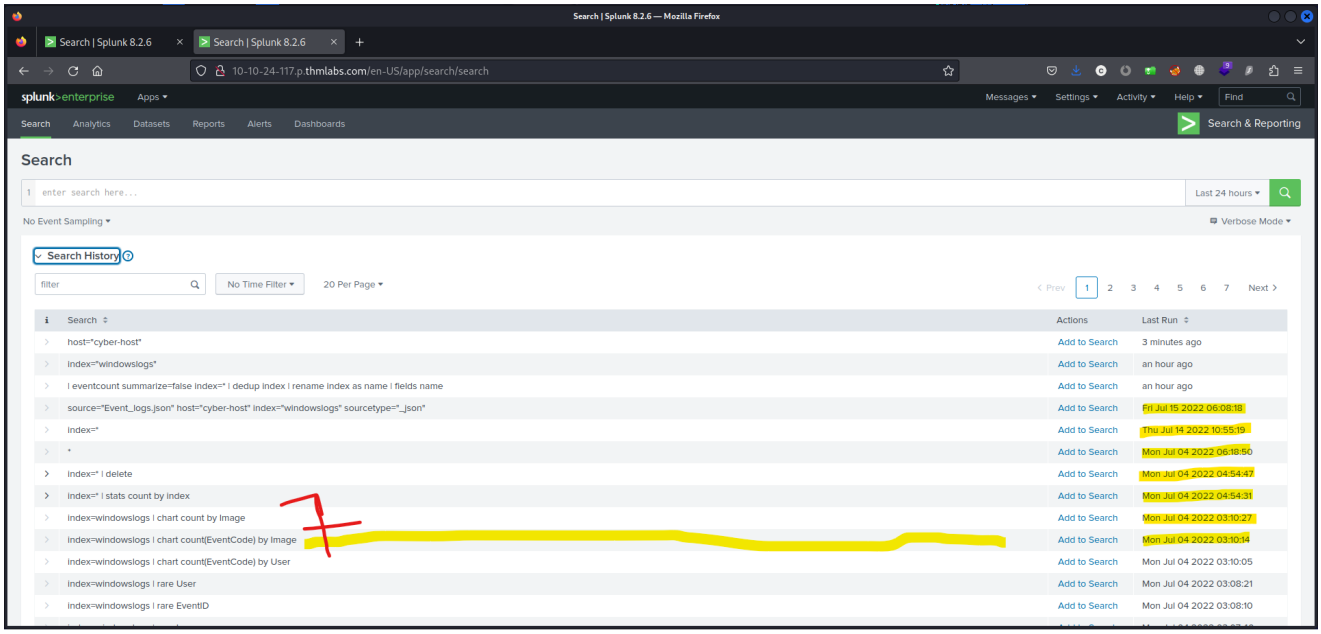




Task 2 Connect with the Lab

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

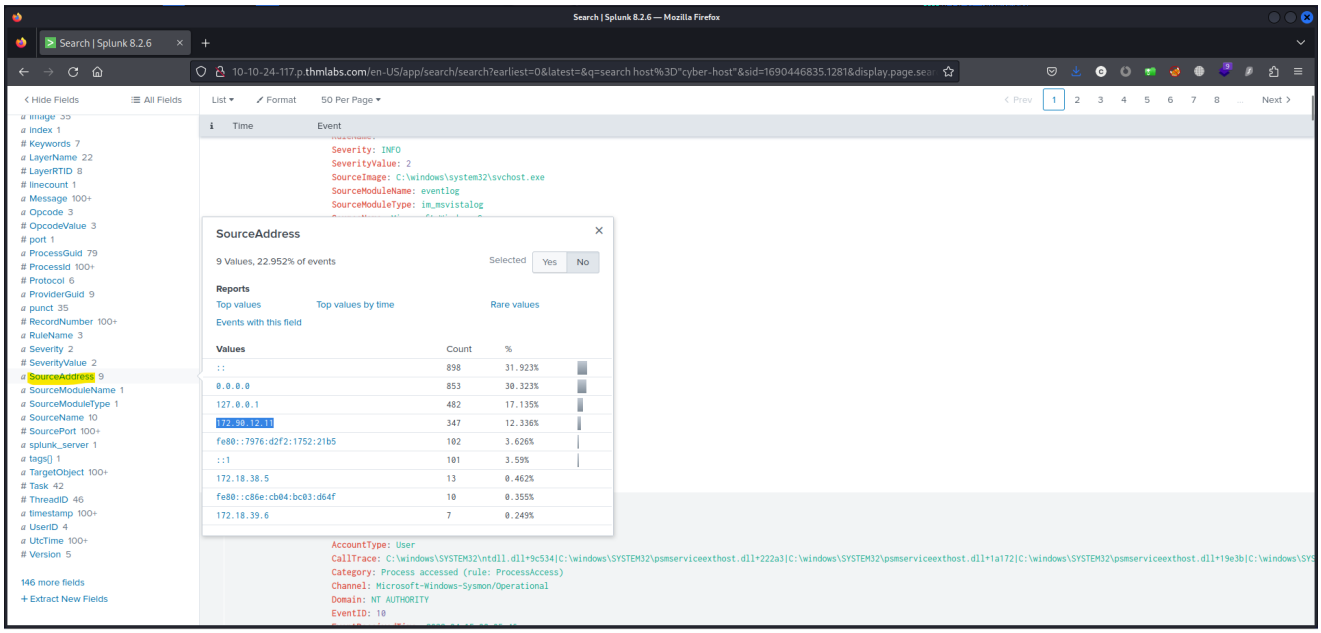
```
cyber-host
```



Task 3 Search & Reporting App Overview

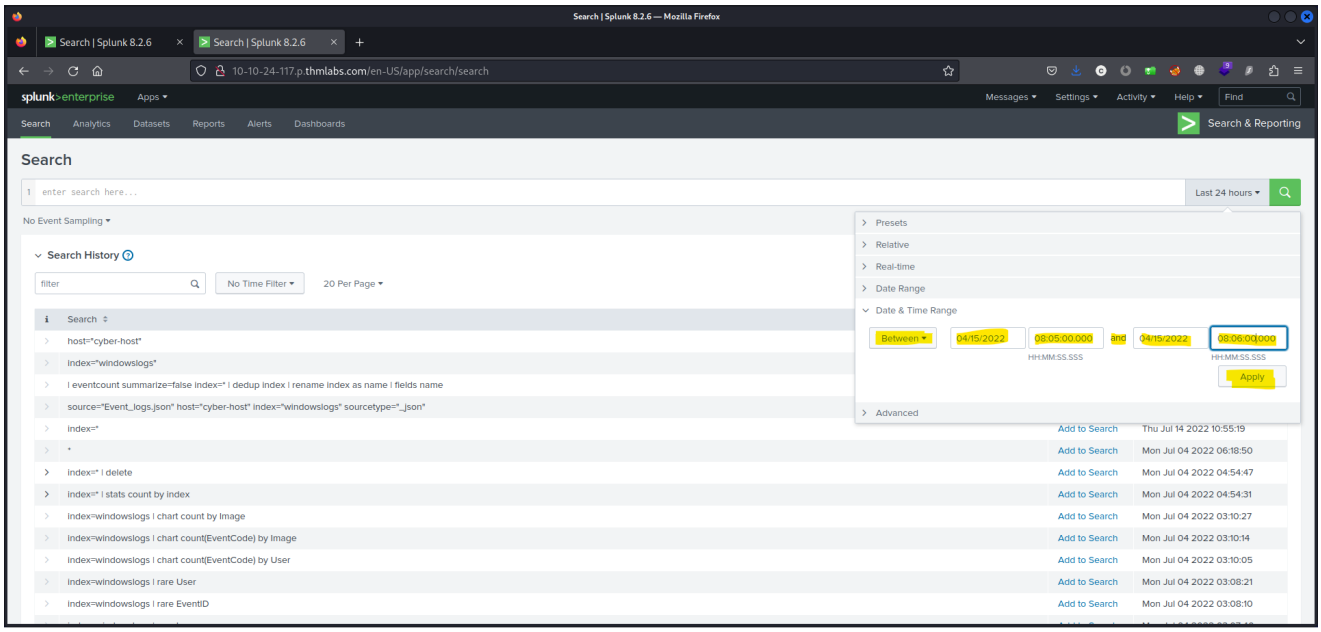
In the search History, what is the 7th search query in the list? (excluding your searches from today)

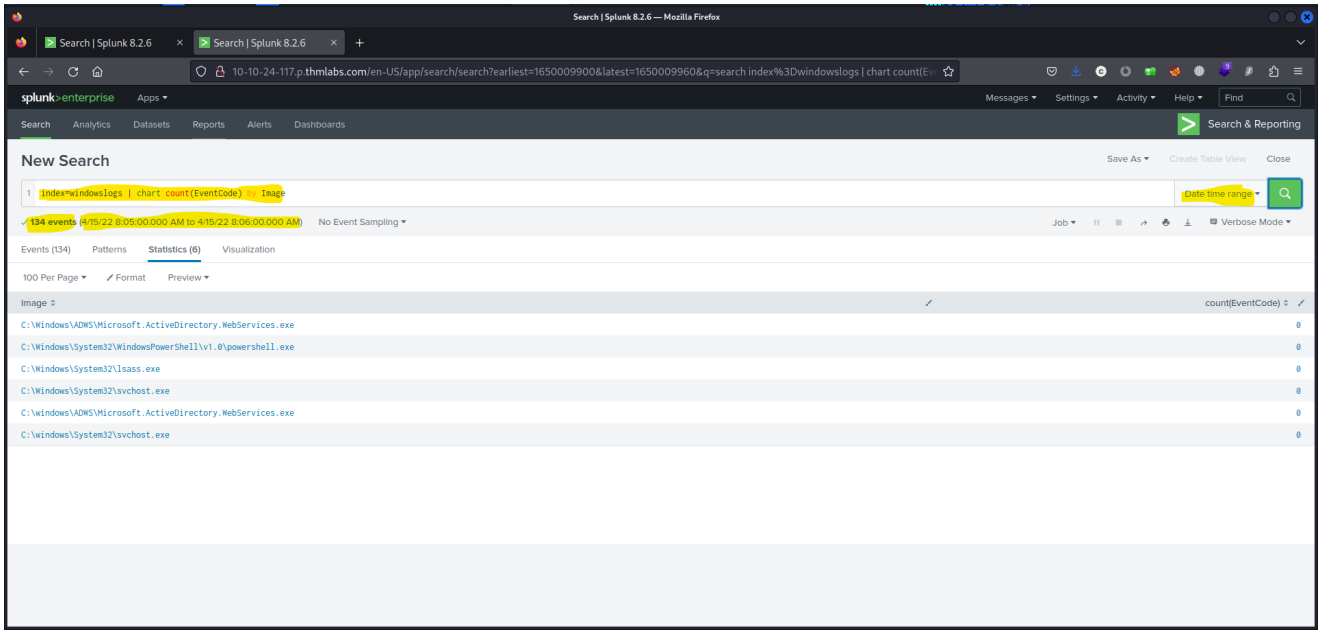
```
index=windowslogs | chart count(EventCode) by Image
```



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

```
172.90.12.11
```



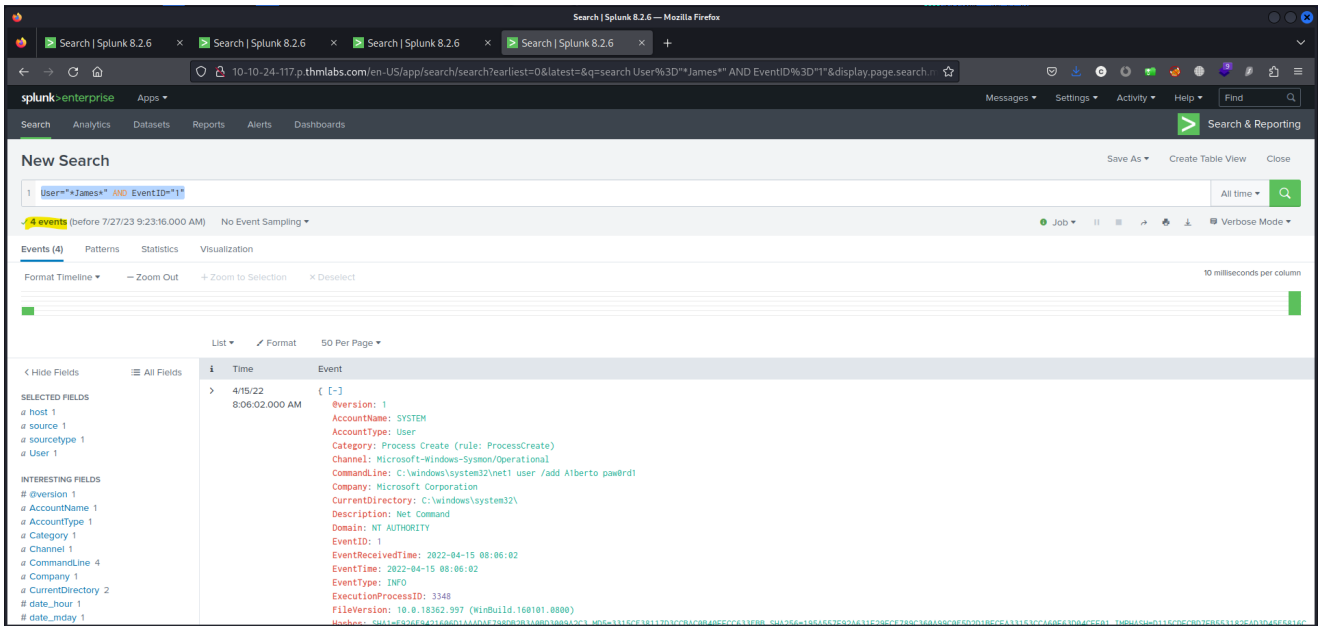


How many events are returned when we apply the time filter to display events on 04/15/2022 and Time from 08:05 AM to 08:06 AM?

```
134
```

Task 4 Splunk Processing Language Overview

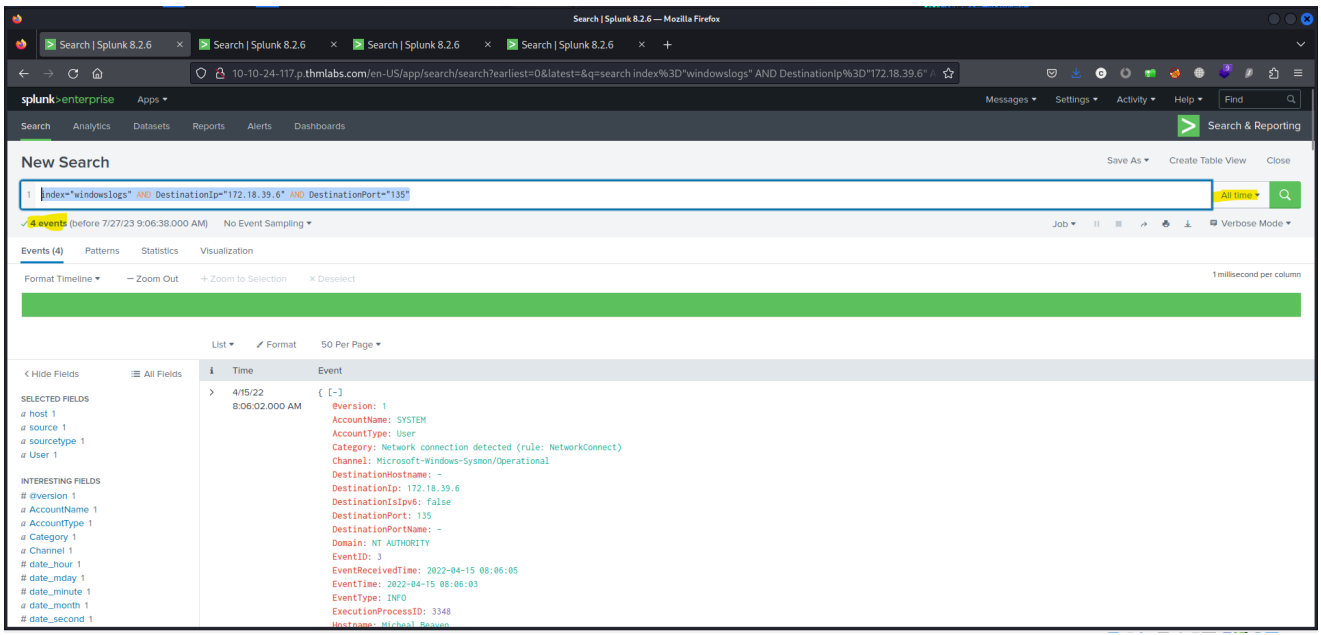
```
User="*James*" AND EventID="1"
```



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

4

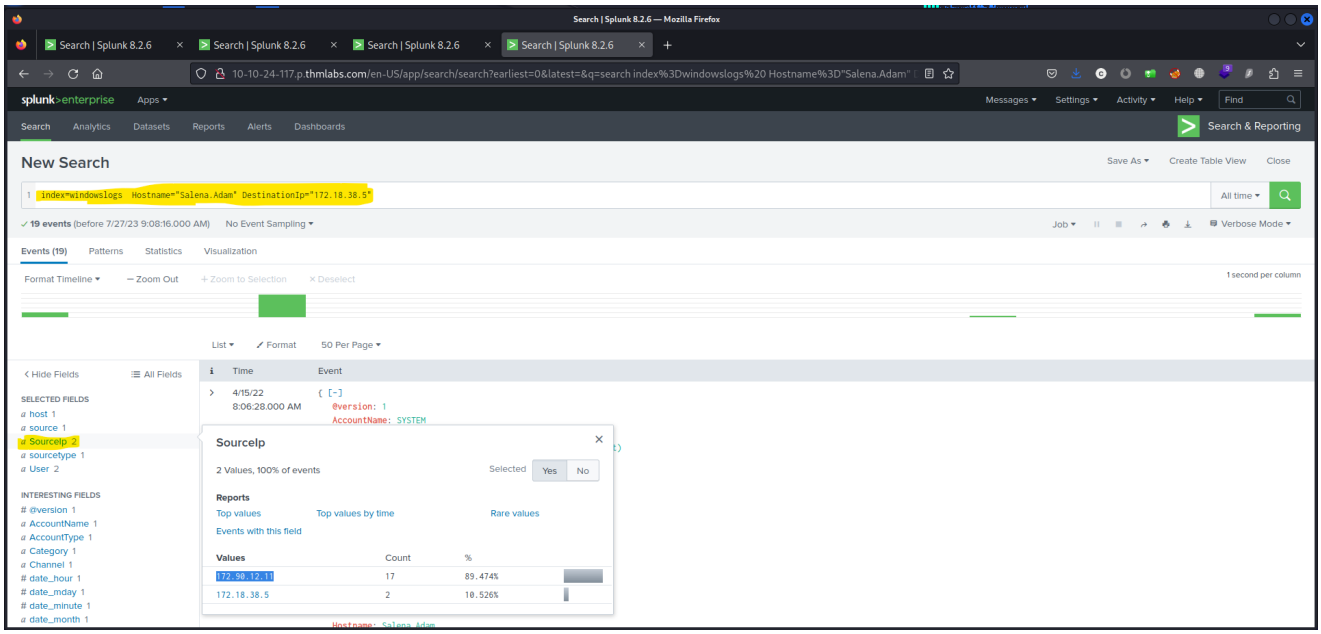
```
index="windowslogs" AND DestinationIp="172.18.39.6" AND DestinationPort="135"
```



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

4

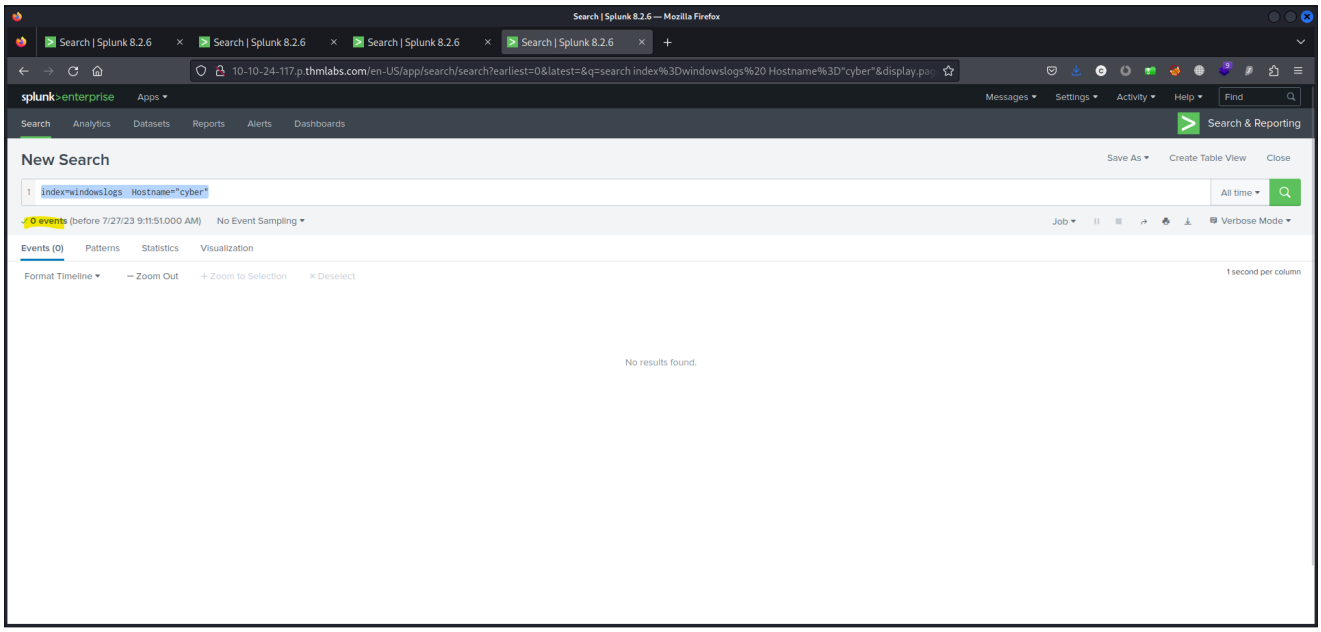
```
index=windowslogs  Hostname="Salena.Adam" DestinationIp="172.18.38.5"
```



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
```

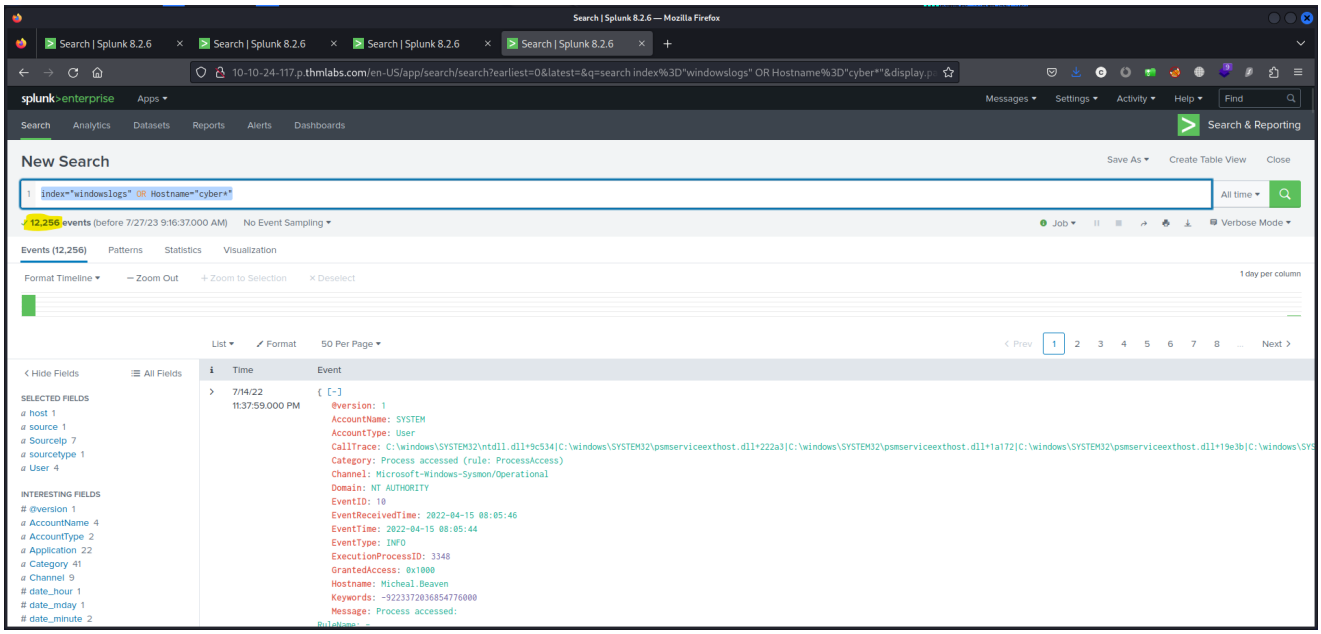
```
index=windowslogs  Hostname="cyber"
```



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

```
0
```

```
index="windowslogs" OR Hostname="cyber*"
```

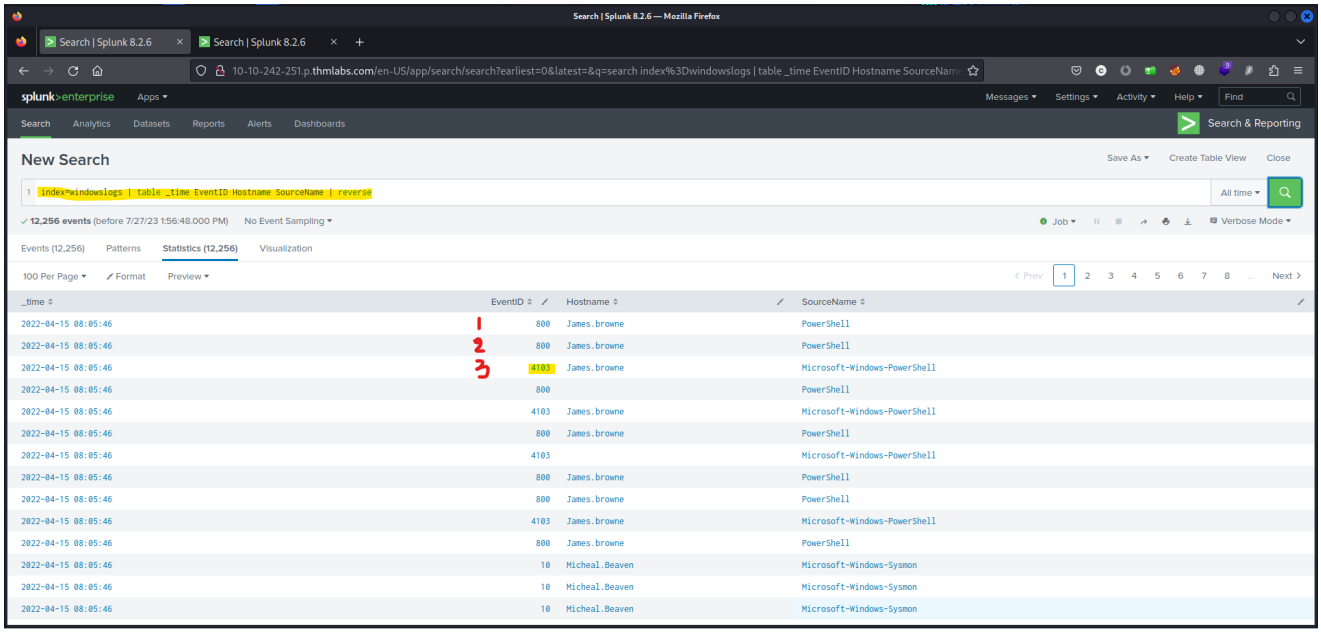


Now search for the term cyber , how many events are returned?*

```
12256
```

Task 5 Filtering the Results in SPL

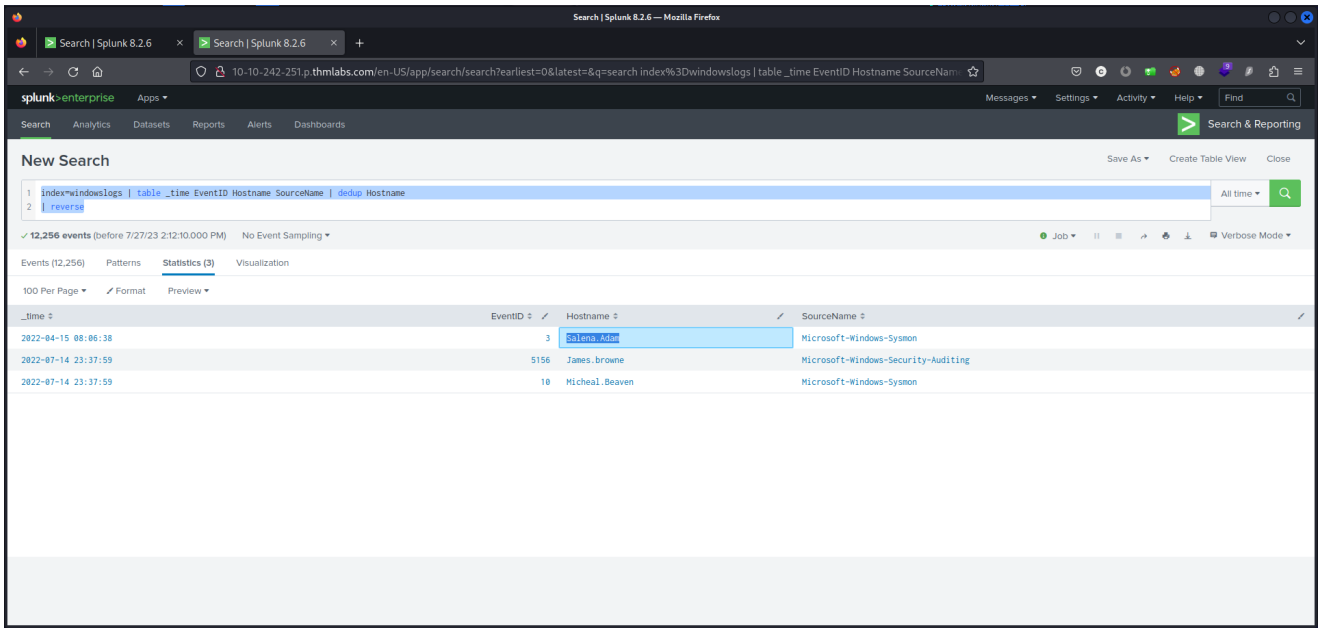
```
index=windowslogs | table _time EventID Hostname SourceName | reverse
```



What is the third EventID returned against this search query?

```
4103
```

```
index=windowslogs | table _time EventID Hostname SourceName | dedup Hostname |
reverse
```

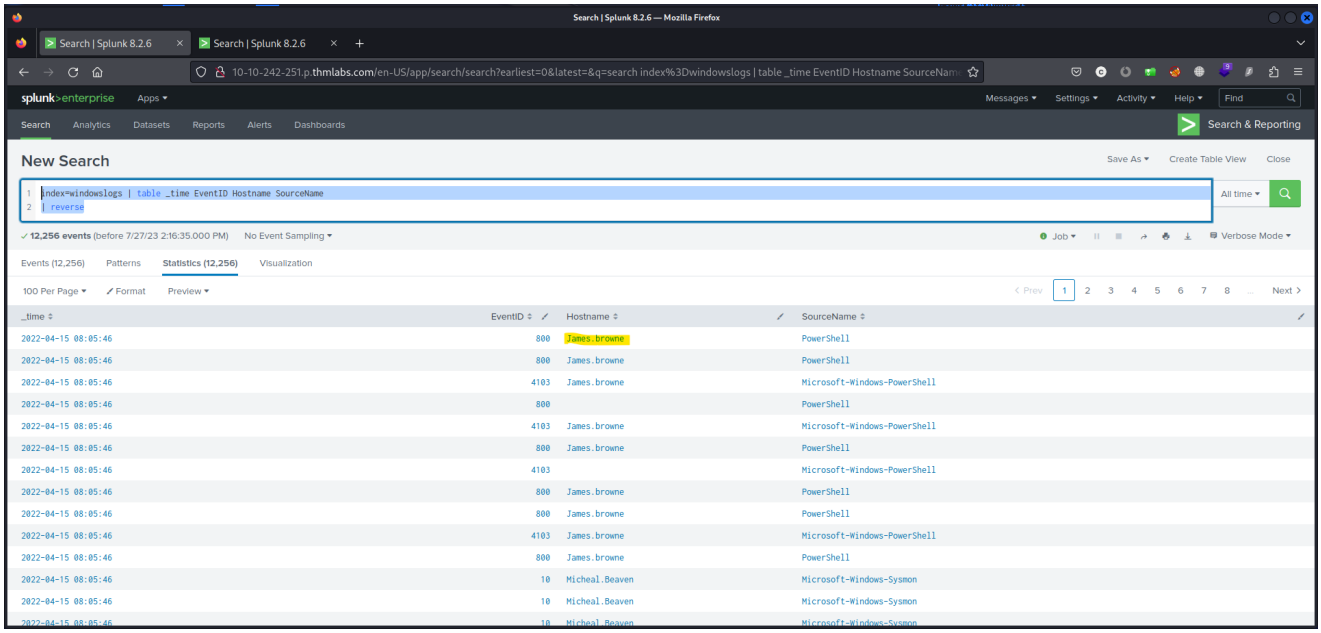


Use the dedup command against the Hostname field before the reverse command in the query mentioned in Question 1. What is the first username returned in the Hostname field?

```
Salena.Adam
```

Task 6 SPL - Structuring the Search Results

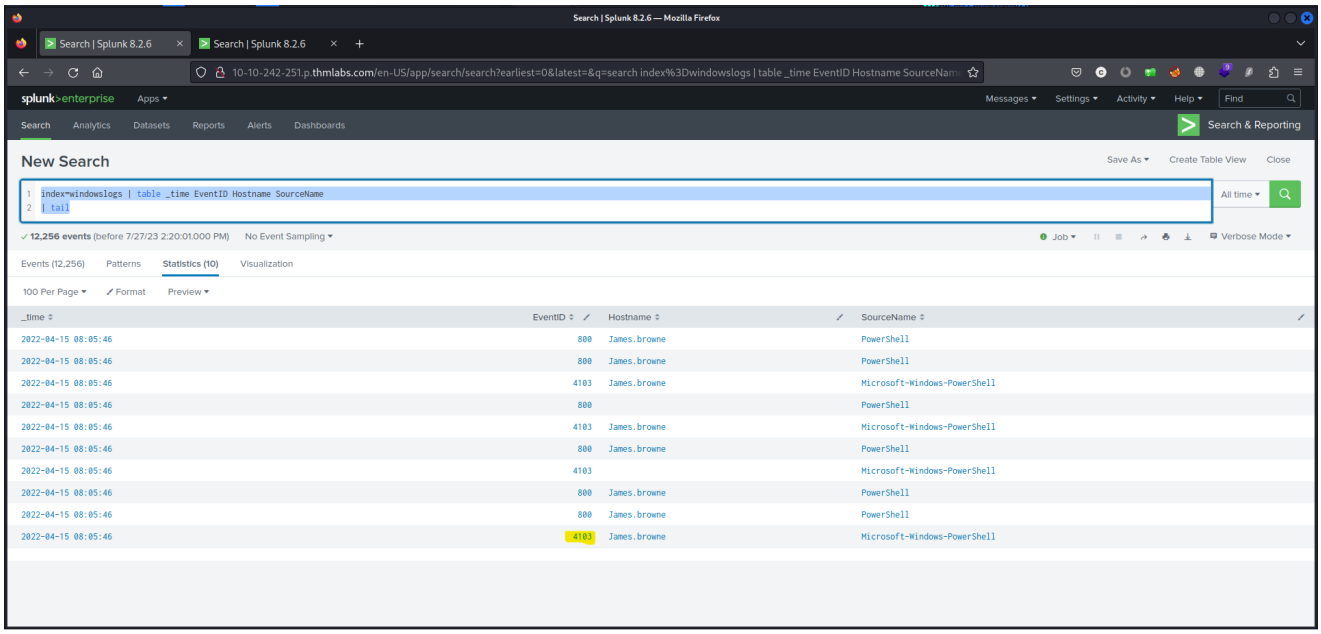
```
index=windowslogs | table _time EventID Hostname SourceName
| reverse
```



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

```
James.browne
```

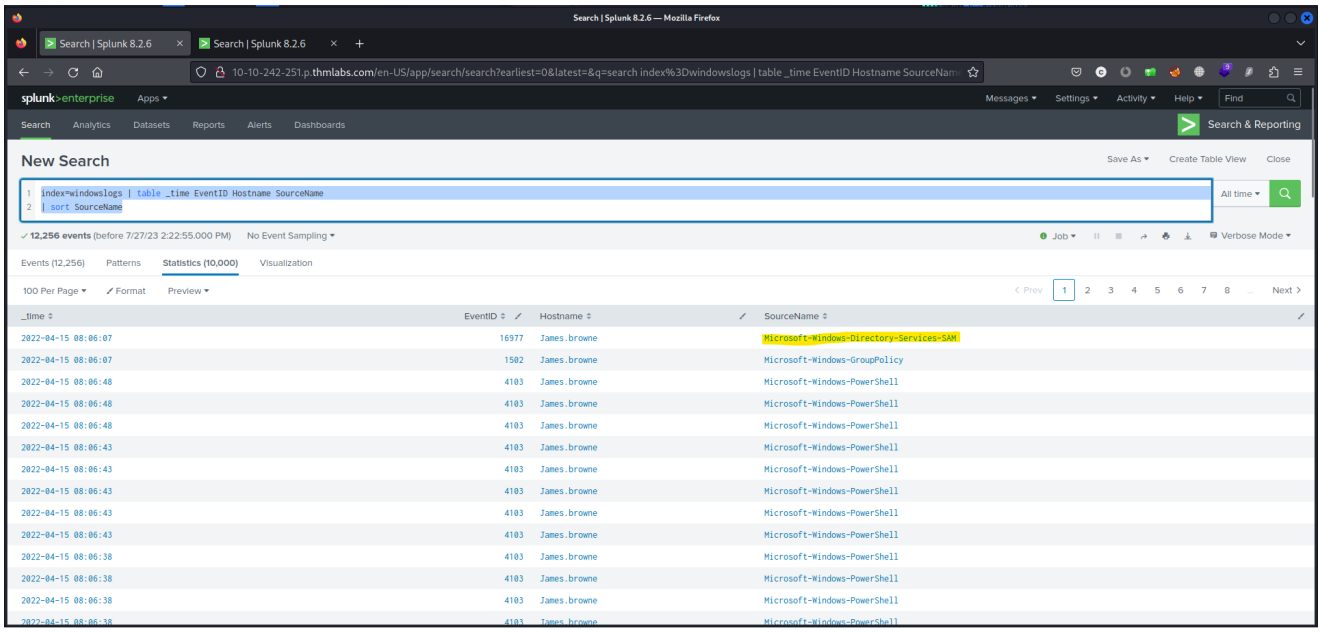
```
index=windowslogs | table _time EventID Hostname SourceName | tail
```



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

```
4103
```

```
index=windowslogs | table _time EventID Hostname SourceName | sort SourceName
```

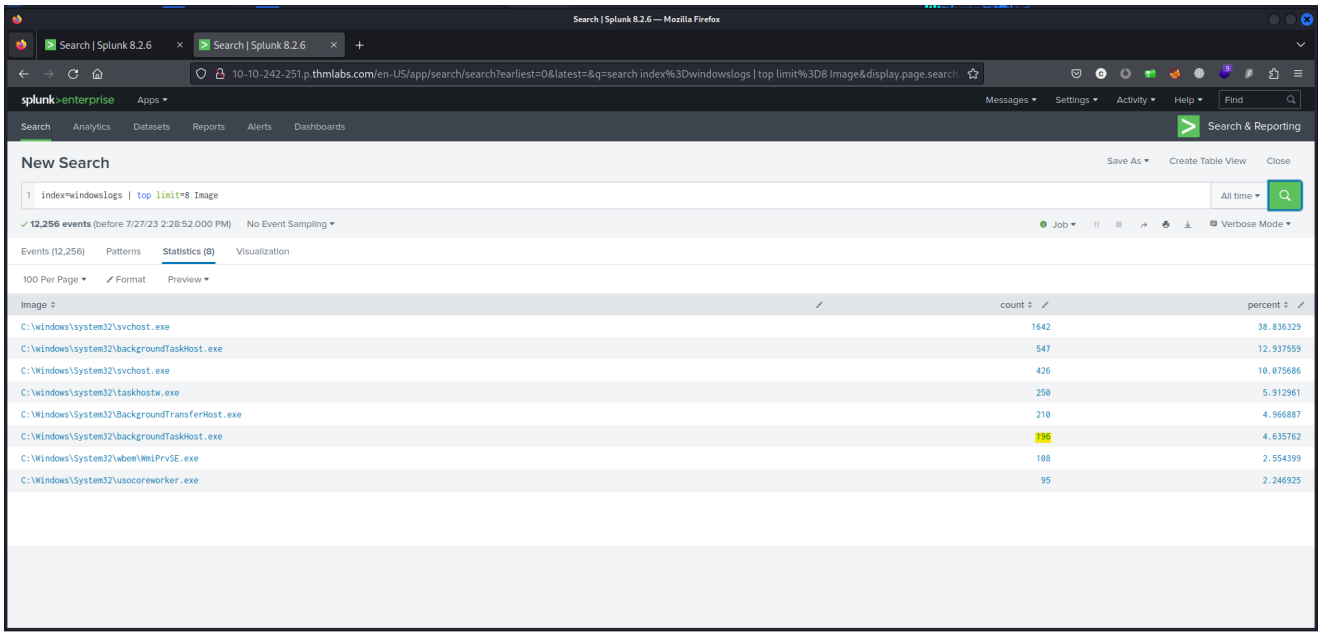


Sort the above query against the SourceName. What is the top SourceName returned?

```
Microsoft-Windows-Directory-Services-SAM
```

Task 7 Transformational Commands in SPL

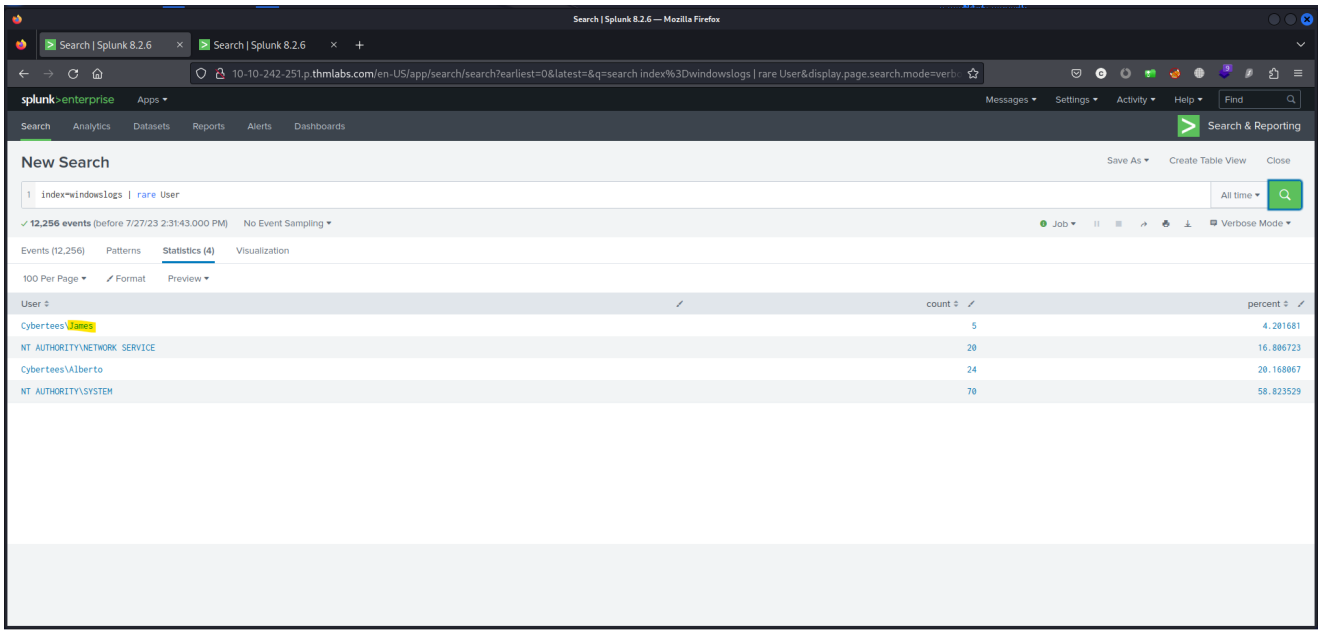
```
index=windowslogs | top limit=8 Image
```



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

```
196
```

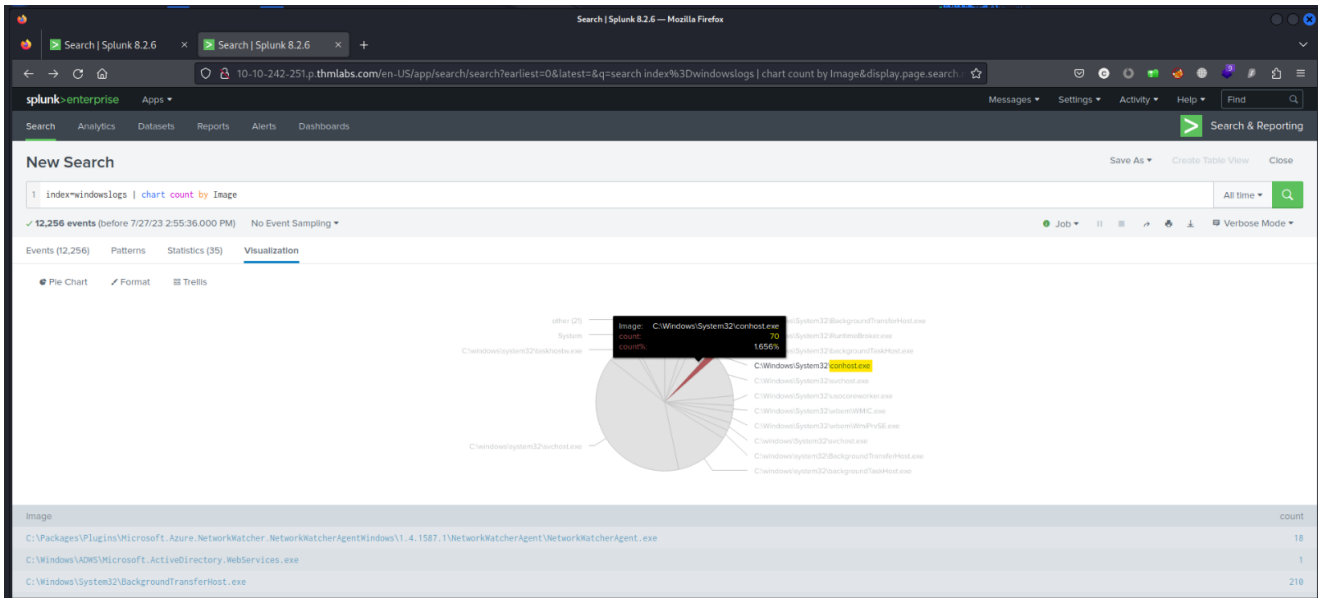
```
index=windowslogs | rare User
```



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

```
James
```

```
index=windowslogs | chart count by Image
```



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

```
70
```