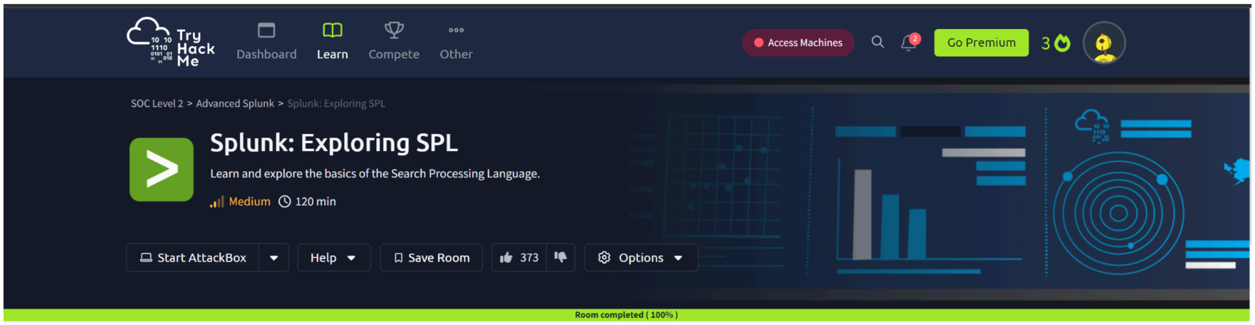
SPLUNK: EXPLORING SPL

ASSIGNMENT REPORT



SOC Level 2 > Advanced Splunk > Splunk: Exploring SPL

Splunk: Exploring SPL

Learn and explore the basics of the Search Processing Language.

Medium 120 min

Room completed (100%)

Peter Kinyumu,
cs-sa07-24067,
July 10th, 2024.

1. INTRODUCTION

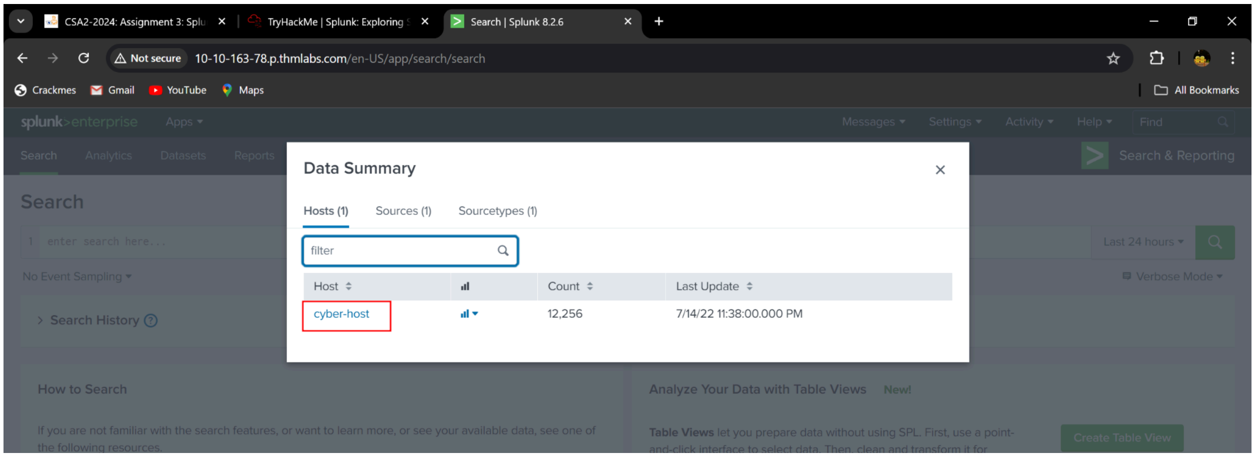
This room explores the basics of Splunk's Search Processing Language, a set of commands with a specific syntax that are used for searching, filtering, manipulation and visualization of log data ingested in the Splunk SIEM.

2. ANSWERS TO QUESTIONS

Connect With the Lab

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

- `cyber-host`



If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for

Data Summary

Hosts (1) Sources (1) Sourcetypes (1)

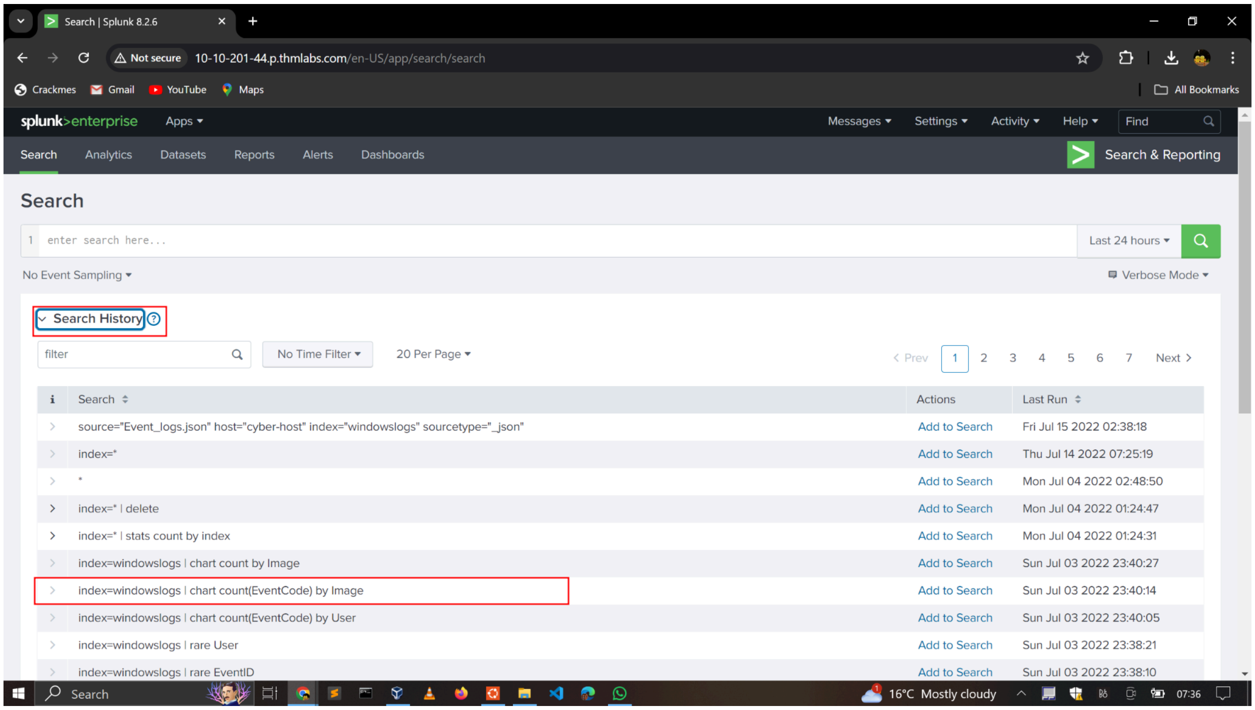
filter

Host		Count	Last Update
cyber-host		12,256	7/14/22 11:38:00.000 PM

Search & Reporting App Overview

a. 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`



Search

No Event Sampling ▾ Verbose Mode ▾

Search History

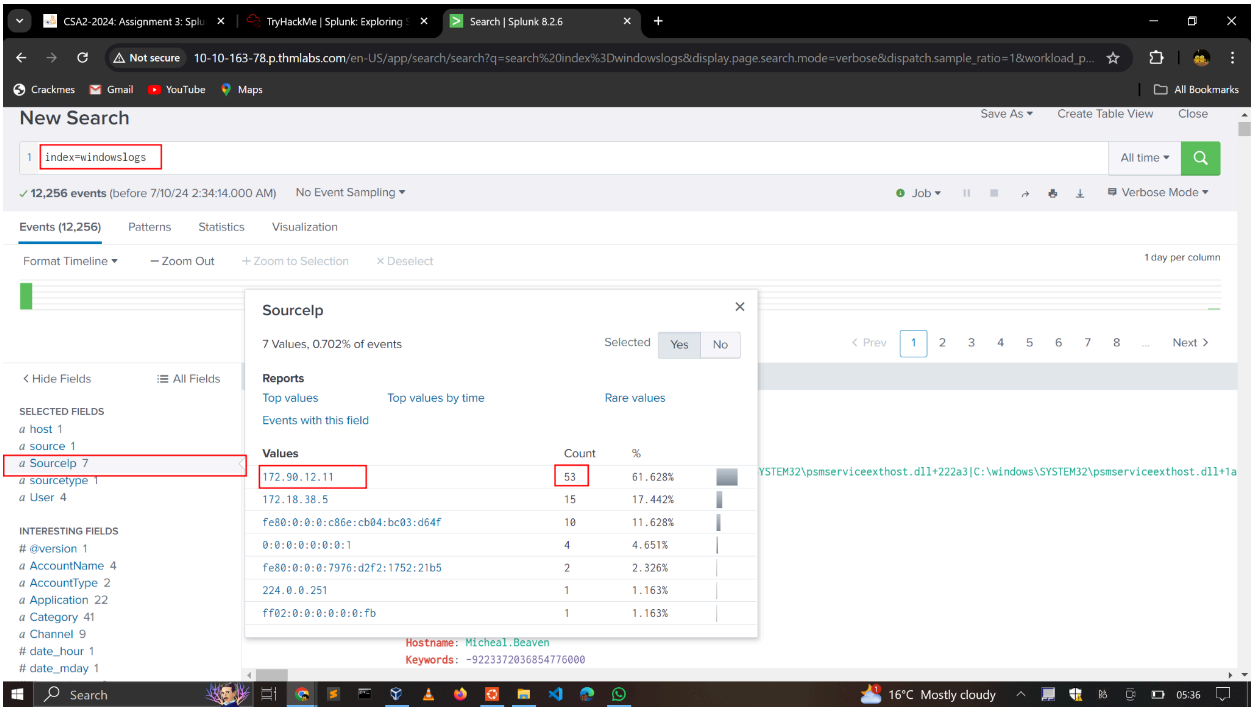
filter · No Time Filter ▾ · 20 Per Page ▾

i	Search	Actions	Last Run
›	source="Event_logs.json" host="cyber-host" index="windowslogs" sourcetype="_json"	Add to Search	Fri Jul 15 2022 02:38:18
›	index=*	Add to Search	Thu Jul 14 2022 07:25:19
›	*	Add to Search	Mon Jul 04 2022 02:48:50
›	index=* | delete	Add to Search	Mon Jul 04 2022 01:24:47
›	index=* | stats count by index	Add to Search	Mon Jul 04 2022 01:24:31
›	index=windowslogs | chart count by Image	Add to Search	Sun Jul 03 2022 23:40:27
›	index=windowslogs | chart count(EventCode) by Image	Add to Search	Sun Jul 03 2022 23:40:14
›	index=windowslogs | chart count(EventCode) by User	Add to Search	Sun Jul 03 2022 23:40:05
›	index=windowslogs | rare User	Add to Search	Sun Jul 03 2022 23:38:21
›	index=windowslogs | rare EventID	Add to Search	Sun Jul 03 2022 23:38:10

Search | Splunk 8.2.6
Not secure 10-10-201-44.p.thmlabs.com/en-US/app/search/search
Crackmes Gmail YouTube Maps All Bookmarks
splunk>enterprise Apps ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
Search Analytics Datasets Reports Alerts Dashboards Search & Reporting
enter search here... Last 24 hours ▾
‹ Prev 1 2 3 4 5 6 7 Next ›
Search 16°C Mostly cloudy 07:36

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

- 172.90.12.11



New Search

index=windowslogs

✓ 12,256 events (before 7/10/24 2:34:14.000 AM) No Event Sampling ▾

Events (12,256) Patterns Statistics Visualization

SELECTED FIELDS
a host 1
a source 1
a SourceIp 7
a sourcetype 1
a User 4

INTERESTING FIELDS
@version 1
a AccountName 4
a AccountType 2
a Application 22
a Category 41
a Channel 9
# date_hour 1
# date_mday 1

SourceIp

7 Values, 0.702% of events

Reports
Top values · Top values by time · Rare values
Events with this field

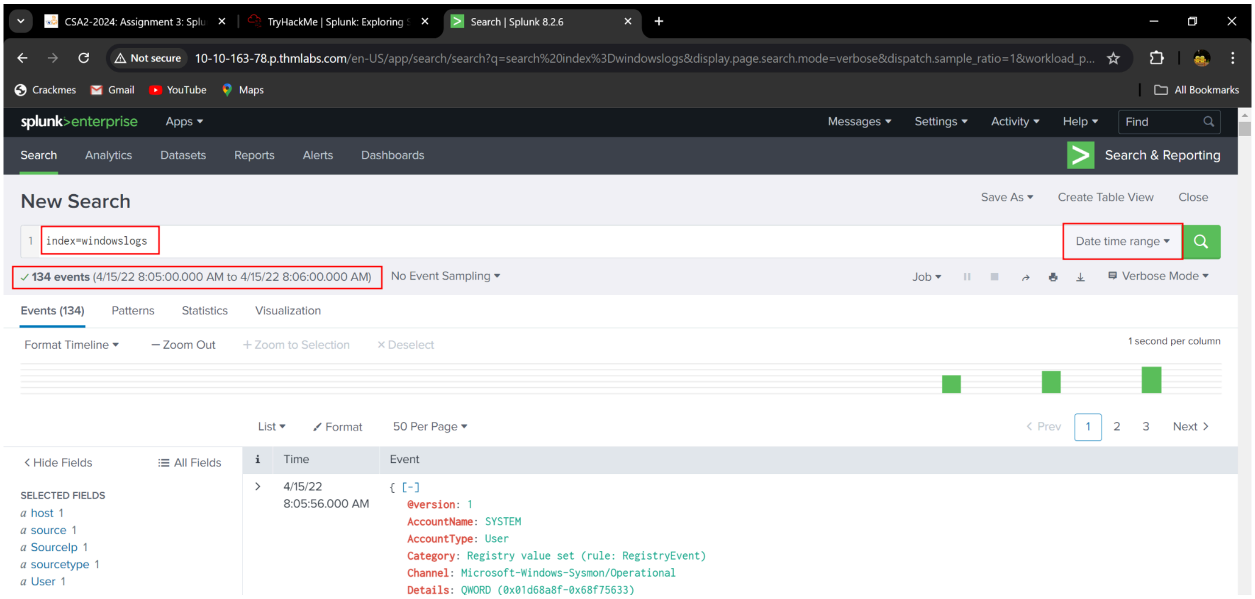
Values	Count	%
172.90.12.11	53	61.628%
172.18.38.5	15	17.442%
fe80:0:0:0:c86e:cb04:bc03:d64f	10	11.628%
0:0:0:0:0:0:0:1	4	4.651%
fe80:0:0:0:7976:d2f2:1752:21b5	2	2.326%
224.0.0.251	1	1.163%
ff02:0:0:0:0:0:0:fb	1	1.163%

```
YSTEM32\psmserviceexthost.dll+222a3|C:\windows\SYSTEM32\psmserviceexthost.dll+1a
Hostname: Micheal.Beaven
Keywords: -9223372036854776000
```

CSA2-2024: Assignment 3: Splu
TryHackMe | Splunk: Exploring
Search | Splunk 8.2.6
Not secure 10-10-163-78.p.thmlabs.com/en-US/app/search/search?q=search%20index%3Dwindowslogs&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_p...
Crackmes Gmail YouTube Maps All Bookmarks
Save As ▾ Create Table View Close
All time ▾
Job ▾ Verbose Mode ▾
Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 day per column
Selected Yes No
‹ Prev 1 2 3 4 5 6 7 8 ... Next ›
‹ Hide Fields ☰ All Fields
Search 16°C Mostly cloudy 05:36

c. 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



```
index=windowslogs
```

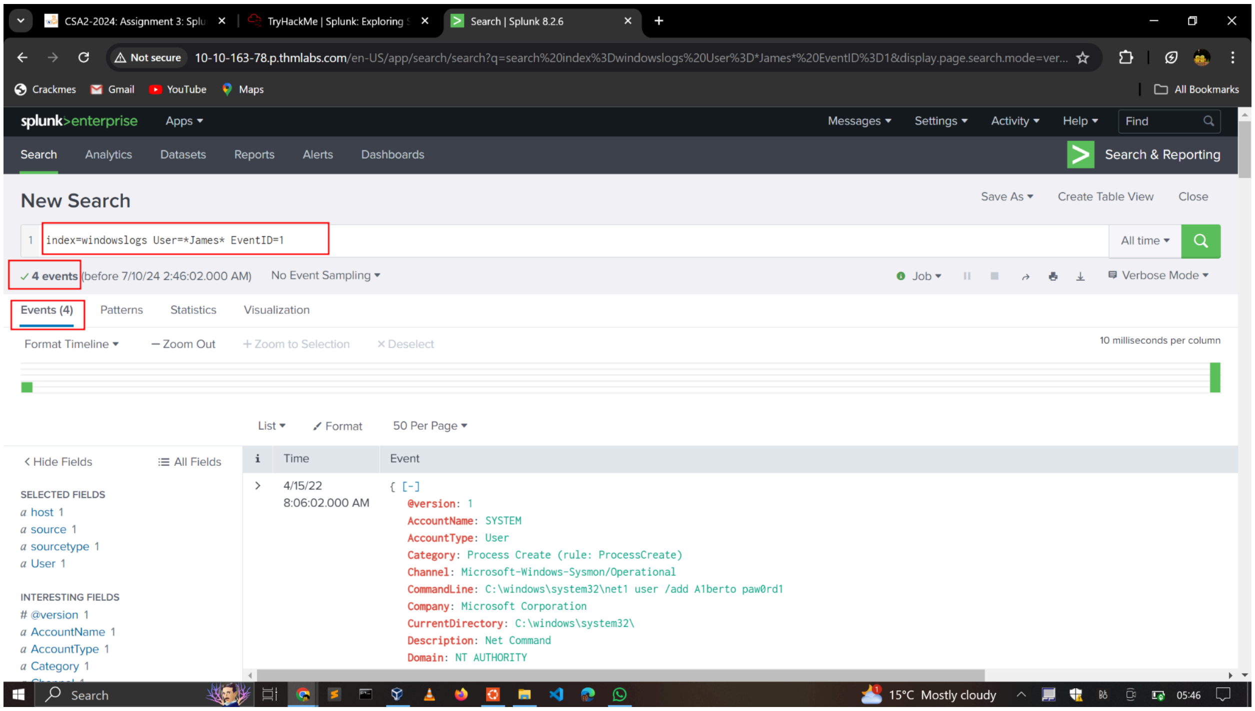
✓ 134 events (4/15/22 8:05:00.000 AM to 4/15/22 8:06:00.000 AM)

i	Time	Event
>	4/15/22 8:05:56.000 AM	{ [-] @version: 1 AccountName: SYSTEM AccountType: User Category: Registry value set (rule: RegistryEvent) Channel: Microsoft-Windows-Sysmon/Operational Details: QWORD (0x01d68a8f-0x68f75633)

Splunk Processing Language Overview

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

- 4



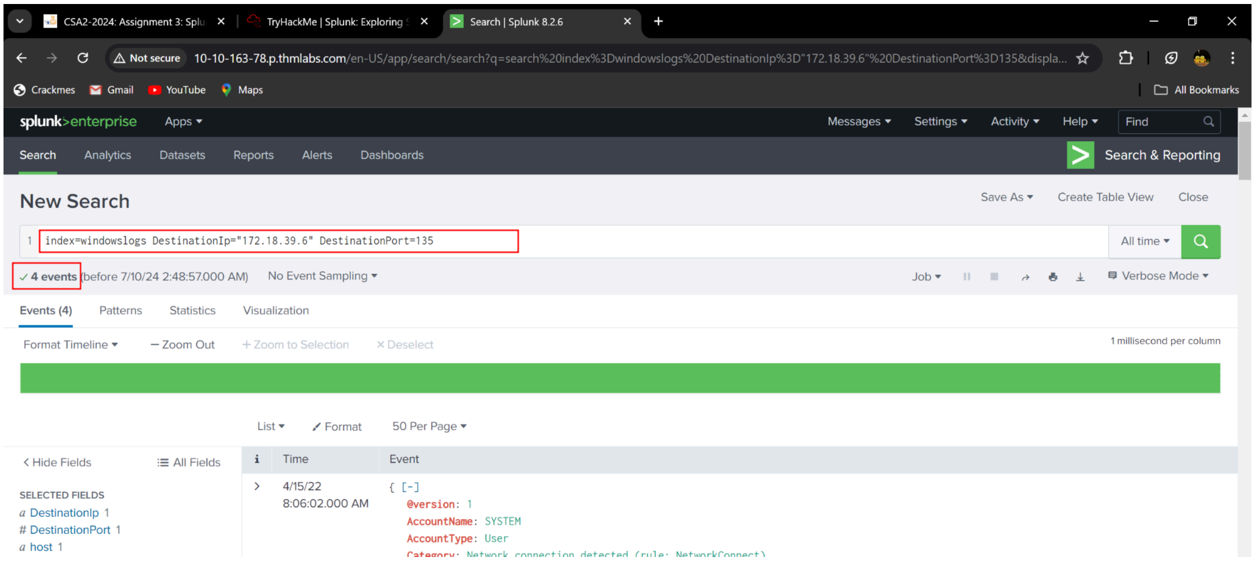
```
index=windowslogs User=*James* EventID=1
```

✓ 4 events (before 7/10/24 2:46:02.000 AM)

i	Time	Event
>	4/15/22 8:06:02.000 AM	{ [-] @version: 1 AccountName: SYSTEM AccountType: User Category: Process Create (rule: ProcessCreate) Channel: Microsoft-Windows-Sysmon/Operational CommandLine: C:\windows\system32\net1 user /add A1berto paw0rd1 Company: Microsoft Corporation CurrentDirectory: C:\windows\system32\ Description: Net Command Domain: NT AUTHORITY

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

- 4



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

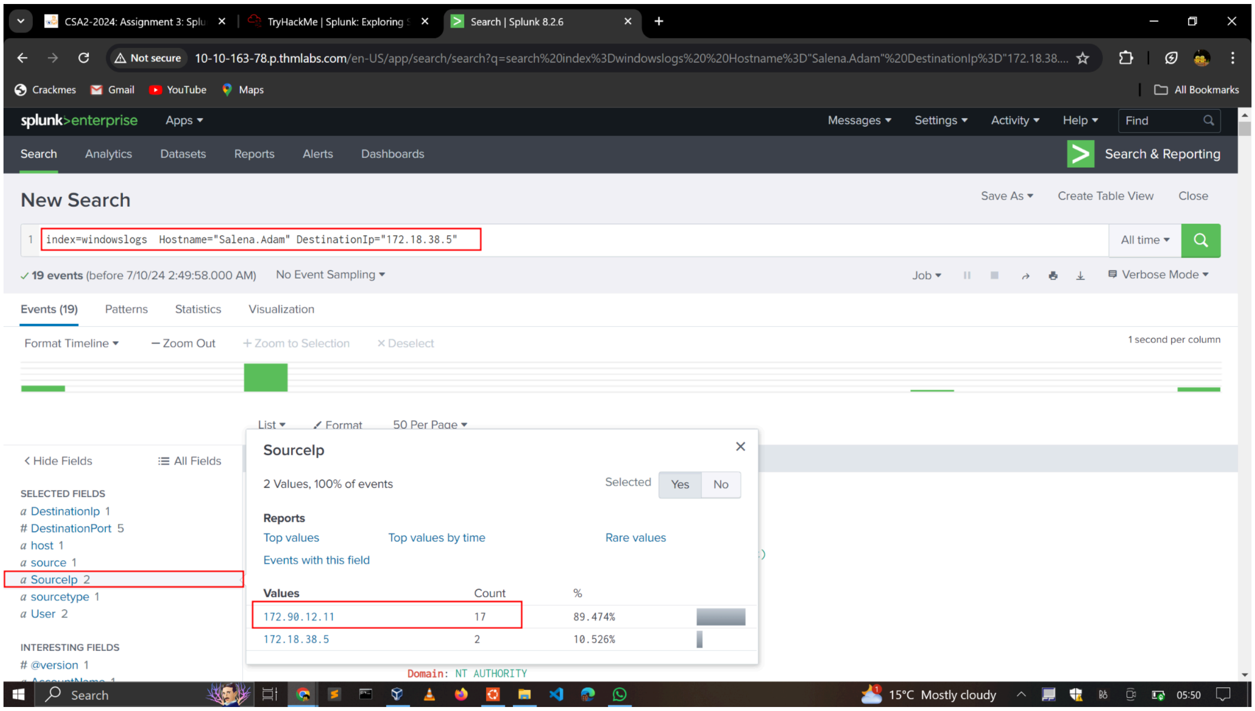
✓ 4 events (before 7/10/24 2:48:57.000 AM) No Event Sampling

SELECTED FIELDS
a DestinationIp 1
DestinationPort 1
a host 1

i	Time	Event
>	4/15/22 8:06:02.000 AM	{ [-] @version: 1 AccountName: SYSTEM AccountType: User Category: Network connection detected (rule: NetworkConnect)

c. **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="Salena.Adam" DestinationIp="172.18.38.5"
```

✓ 19 events (before 7/10/24 2:49:58.000 AM) No Event Sampling

SELECTED FIELDS
a DestinationIp 1
DestinationPort 5
a host 1
a source 1
a SourceIp 2
a sourcetype 1
a User 2

INTERESTING FIELDS
@version 1

SourceIp

2 Values, 100% of events

Selected Yes No

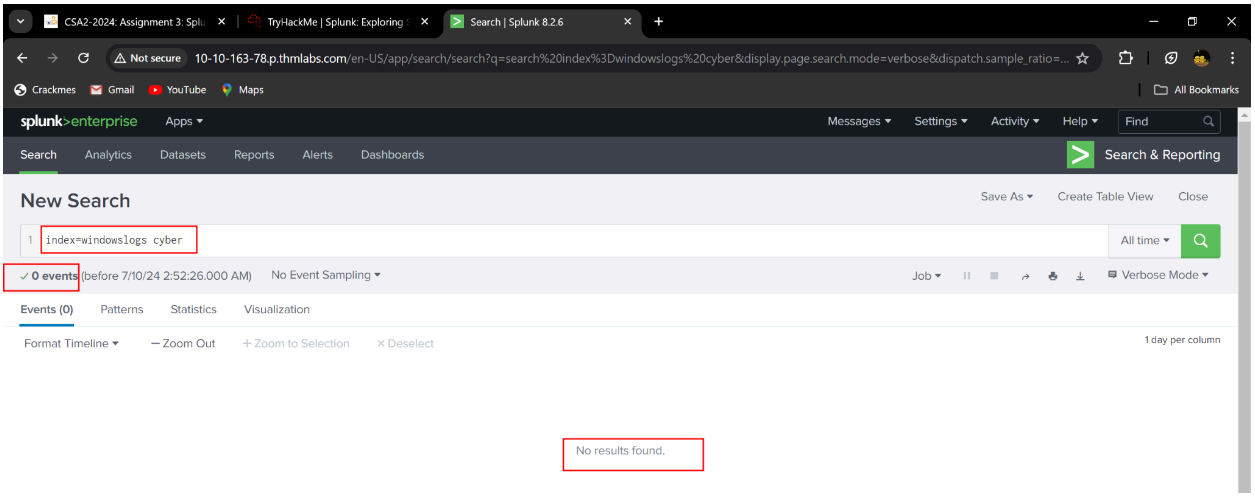
Reports
Top values Top values by time Rare values
Events with this field

Values	Count	%
172.90.12.11	17	89.474%
172.18.38.5	2	10.526%

Domain: NT AUTHORITY

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

- 0



10-10-163-78.p.thmlabs.com/en-US/app/search/search?q=search%20index%3Dwindowslogs%20cyber&display.page.search.mode=verbose&dispatch.sample_ratio=...

New Search

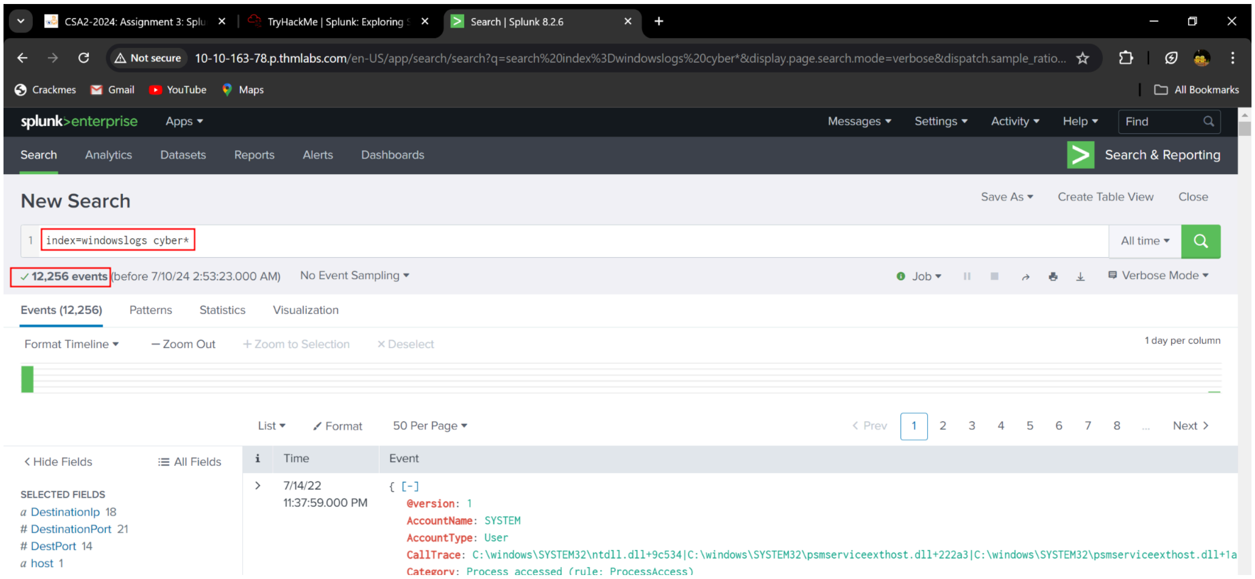
```
index=windowslogs cyber
```

✓ 0 events (before 7/10/24 2:52:26.000 AM) No Event Sampling

No results found.

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

- 12256



10-10-163-78.p.thmlabs.com/en-US/app/search/search?q=search%20index%3Dwindowslogs%20cyber*&display.page.search.mode=verbose&dispatch.sample_ratio...

New Search

```
index=windowslogs cyber*
```

✓ 12,256 events (before 7/10/24 2:53:23.000 AM) No Event Sampling

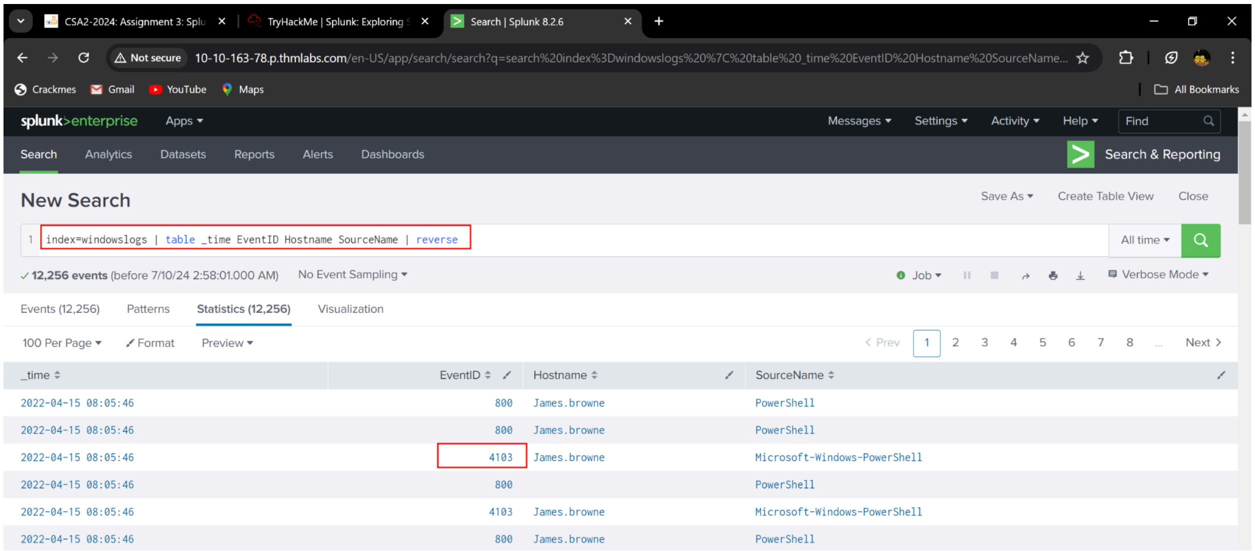
SELECTED FIELDS
a DestinationIp 18
DestinationPort 21
DestPort 14
a host 1

i	Time	Event
>	7/14/22 11:37:59.000 PM	{ [-] @version: 1 AccountName: SYSTEM AccountType: User CallTrace: C:\windows\SYSTEM32\ntdll.dll+9c534|C:\windows\SYSTEM32\psmserviceexthost.dll+222a3|C:\windows\SYSTEM32\psmserviceexthost.dll+1a Category: Process accessed (rule: ProcessAccess)

Filtering results in SPL

a. **What is the third EventID returned against this search query? Search Query: index=windowslogs | table _time EventID Hostname SourceName | reverse**

- 4103



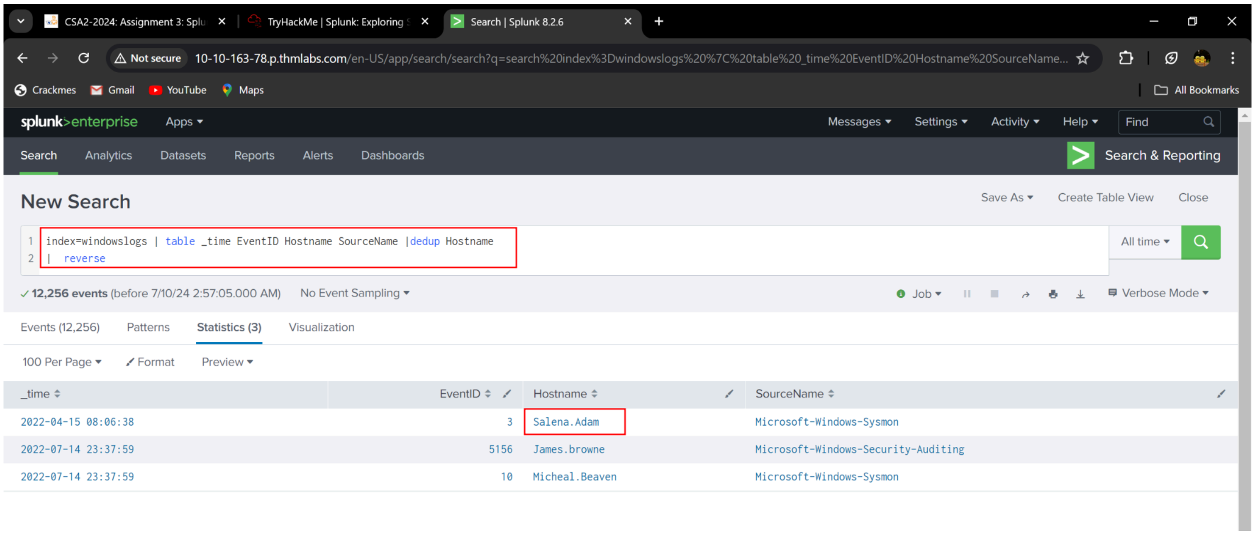
```
index=windowslogs | table _time EventID Hostname SourceName | reverse
```

✓ 12,256 events (before 7/10/24 2:58:01.000 AM)

_time	EventID	Hostname	SourceName
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800		PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell

b. **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



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

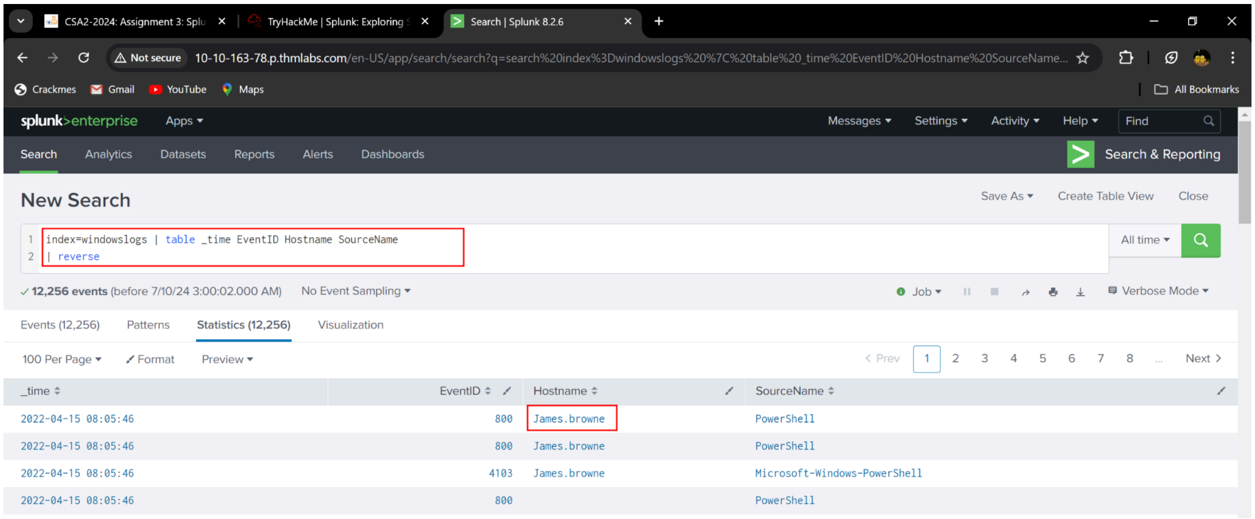
✓ 12,256 events (before 7/10/24 2:57:05.000 AM)

_time	EventID	Hostname	SourceName
2022-04-15 08:06:38	3	Salena.Adam	Microsoft-Windows-Sysmon
2022-07-14 23:37:59	5156	James.browne	Microsoft-Windows-Security-Auditing
2022-07-14 23:37:59	10	Micheal.Beaven	Microsoft-Windows-Sysmon

SPL - Structuring the search results

a. **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



New Search

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

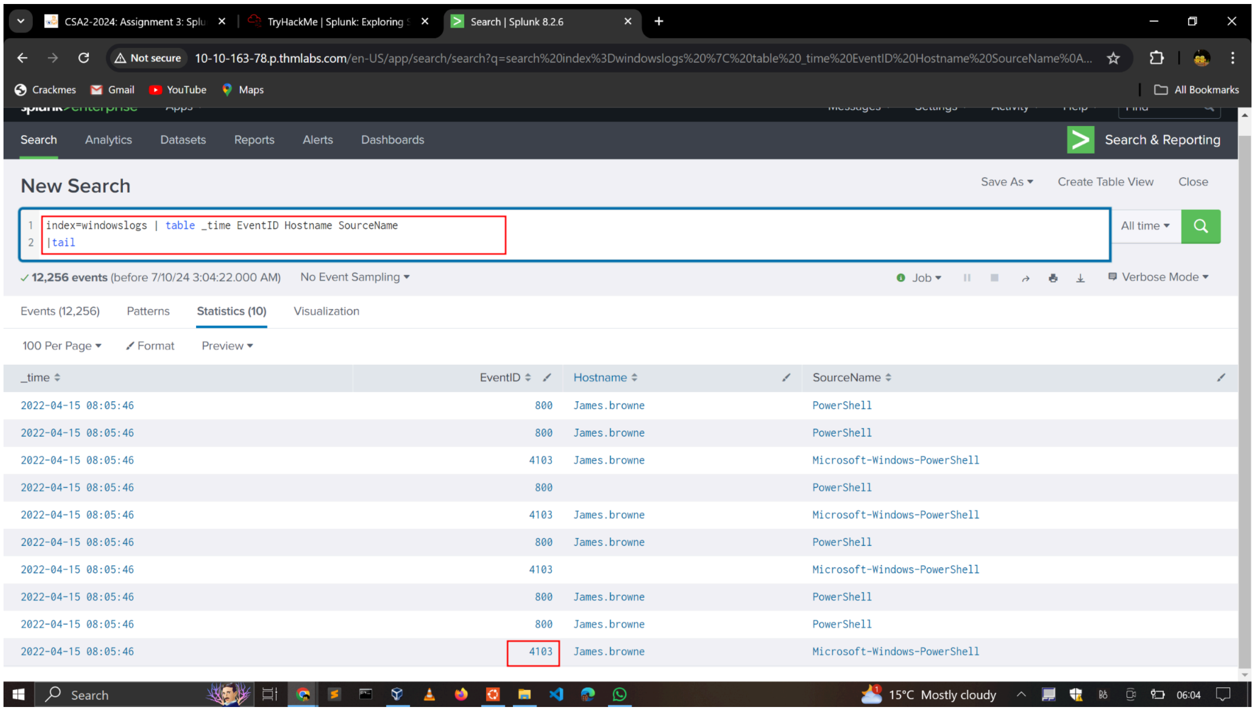
✓ 12,256 events (before 7/10/24 3:00:02.000 AM) No Event Sampling

Events (12,256) Patterns Statistics (12,256) Visualization

_time	EventID	Hostname	SourceName
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800		PowerShell

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

- 4103



New Search

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

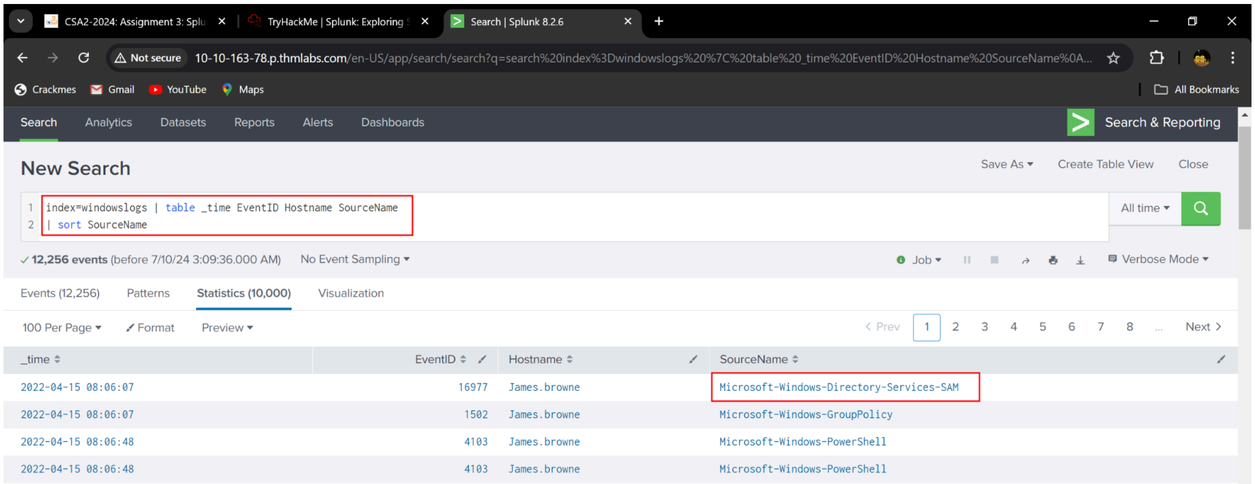
✓ 12,256 events (before 7/10/24 3:04:22.000 AM) No Event Sampling

Events (12,256) Patterns Statistics (10) Visualization

_time	EventID	Hostname	SourceName
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800		PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103		Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell

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

- Microsoft-Windows-Directory-Services-SAM



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

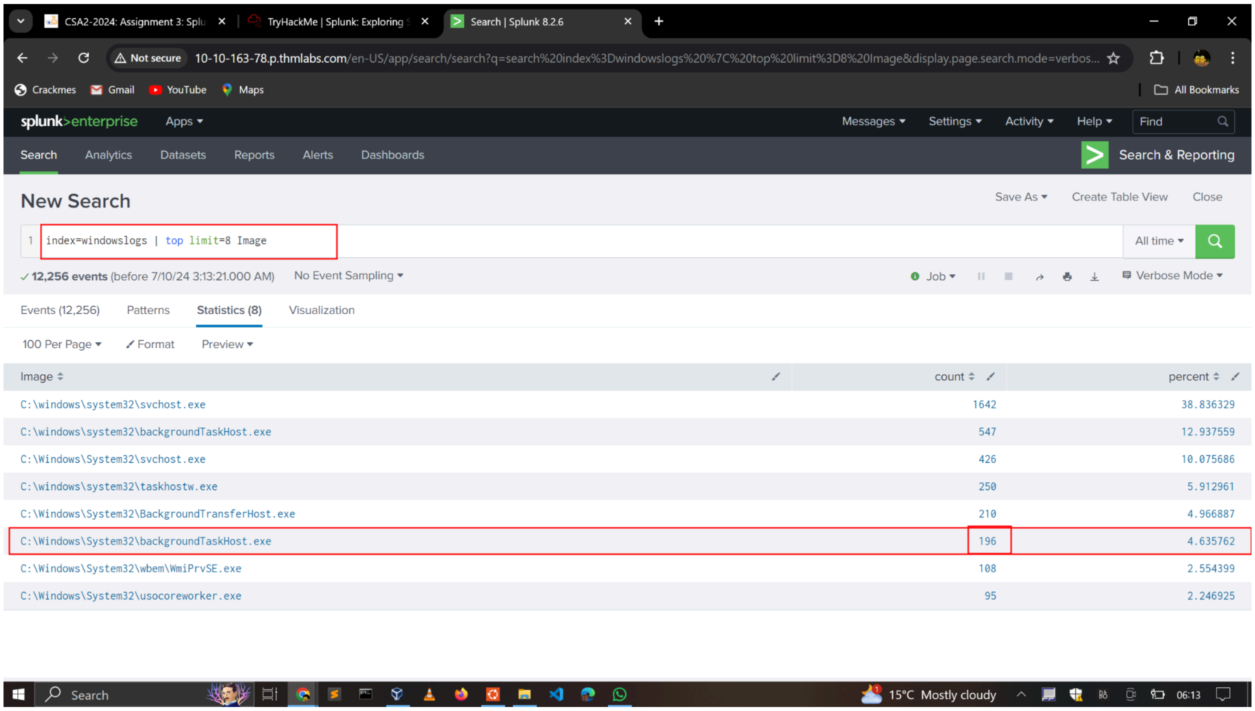
✓ 12,256 events (before 7/10/24 3:09:36.000 AM) No Event Sampling

_time	EventID	Hostname	SourceName
2022-04-15 08:06:07	16977	James.browne	Microsoft-Windows-Directory-Services-SAM
2022-04-15 08:06:07	1502	James.browne	Microsoft-Windows-GroupPolicy
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell

SPL - Structuring the search results

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

- 196



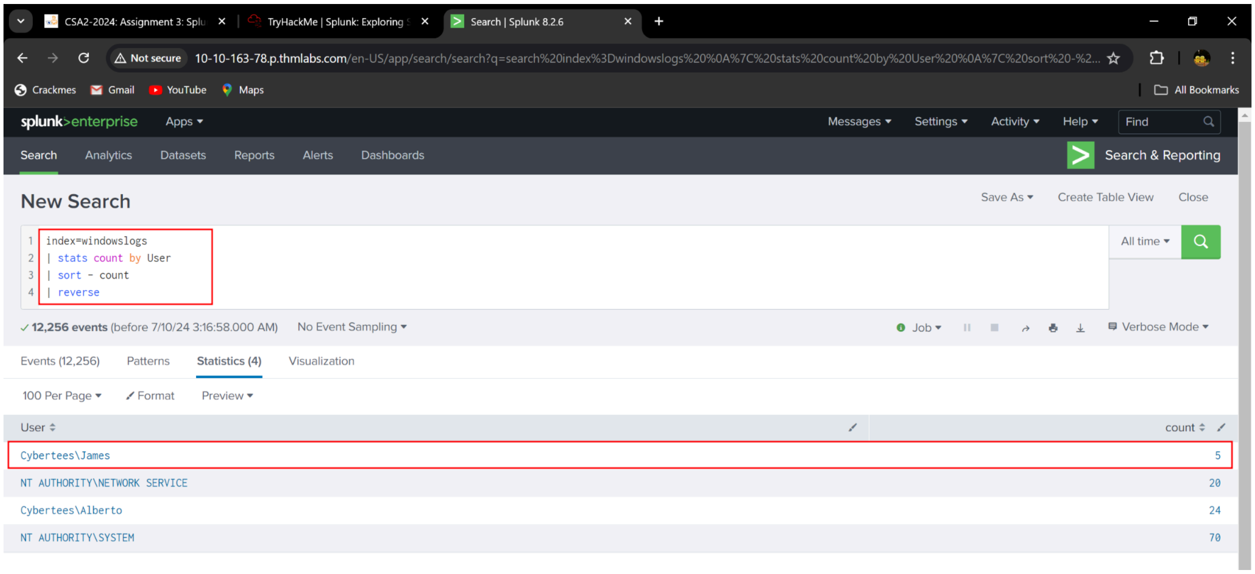
```
index=windowslogs | top limit=8 Image
```

✓ 12,256 events (before 7/10/24 3:13:21.000 AM) No Event Sampling

Image	count	percent
C:\windows\system32\svchost.exe	1642	38.836329
C:\windows\system32\backgroundTaskHost.exe	547	12.937559
C:\Windows\System32\svchost.exe	426	10.075686
C:\windows\system32\taskhostw.exe	250	5.912961
C:\Windows\System32\BackgroundTransferHost.exe	210	4.966887
C:\Windows\System32\backgroundTaskHost.exe	196	4.635762
C:\Windows\System32\wbem\WmiPrvSE.exe	108	2.554399
C:\Windows\System32\usocoreworker.exe	95	2.246925

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

- James



New Search

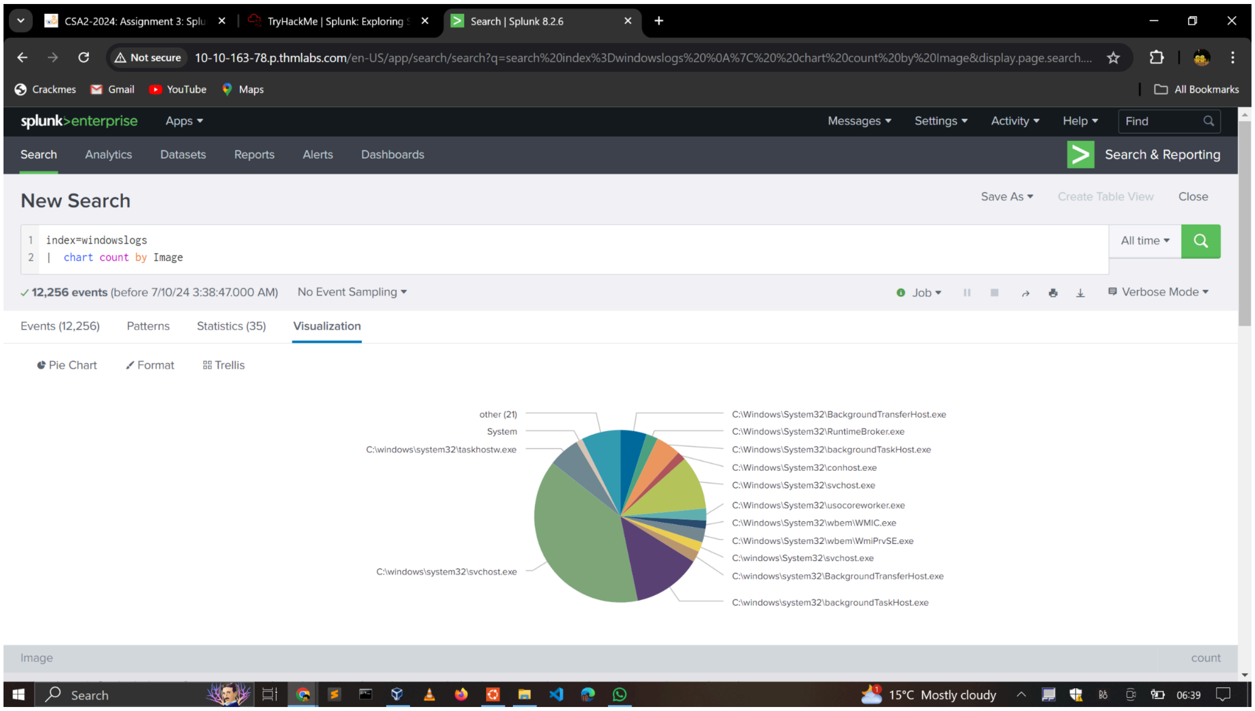
```
index=windowslogs
| stats count by User
| sort - count
| reverse
```

✓ 12,256 events (before 7/10/24 3:16:58.000 AM) No Event Sampling

User	count
Cybertees\James	5
NT AUTHORITY\NETWORK SERVICE	20
Cybertees\Alberto	24
NT AUTHORITY\SYSTEM	70

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

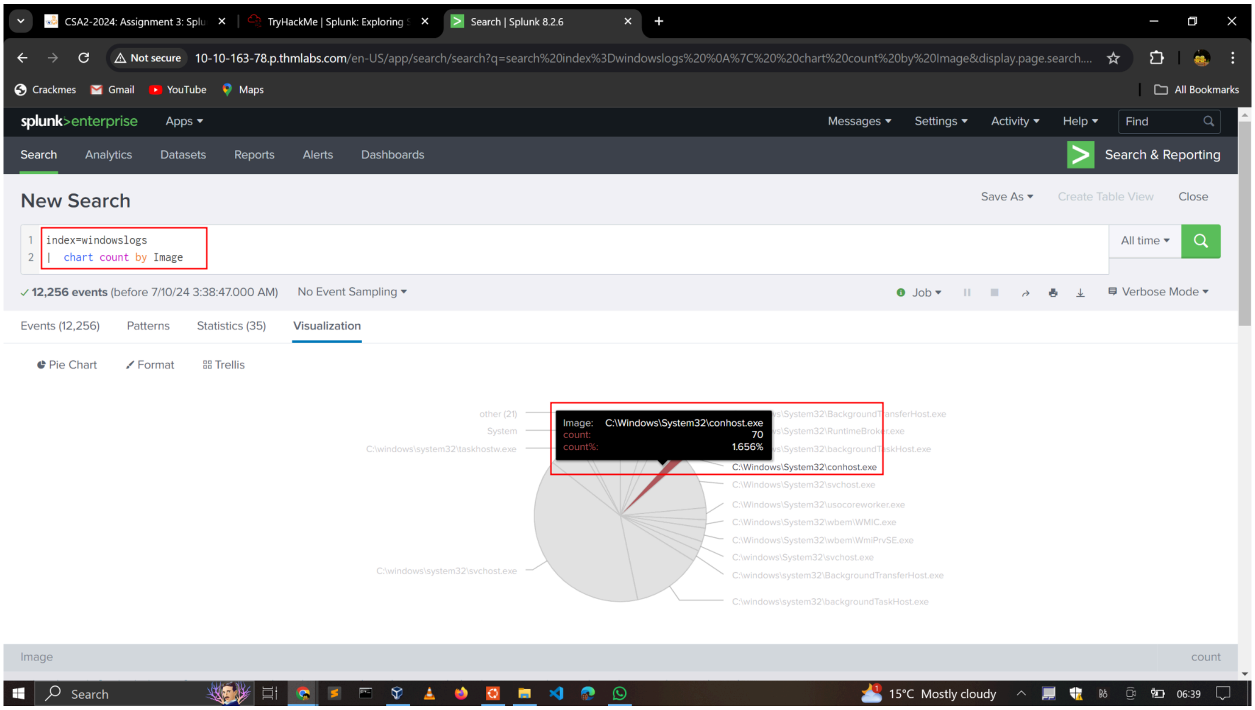
- 70


CSA2-2024: Assignment 3: Splu
TryHackMe | Splunk: Exploring
Search | Splunk 8.2.6
Not secure
10-10-163-78.p.thmlabs.com/en-US/app/search/search?q=search%20index%3Dwindowslogs%20%0A%7C%20%20chart%20count%20by%20Image&display.page.search....
Crackmes
Gmail
YouTube
Maps
All Bookmarks
splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Save As
Create Table View
Close
All time
Job
Verbose Mode
Events (12,256)
Patterns
Statistics (35)
Visualization
Pie Chart
Format
Trellis
other (21)
System
C:\windows\system32\taskhostw.exe
C:\windows\system32\svchost.exe
C:\Windows\System32\BackgroundTransferHost.exe
C:\Windows\System32\RuntimeBroker.exe
C:\Windows\System32\backgroundTaskHost.exe
C:\Windows\System32\conhost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\usocoreworker.exe
C:\Windows\System32\wbem\WMIC.exe
C:\Windows\System32\wbem\WmiPrvSE.exe
C:\windows\System32\svchost.exe
C:\windows\system32\BackgroundTransferHost.exe
C:\windows\system32\backgroundTaskHost.exe
Image
count
Search
15°C Mostly cloudy
06:39

New Search

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

✓ 12,256 events (before 7/10/24 3:38:47.000 AM) No Event Sampling



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

✓ 12,256 events (before 7/10/24 3:38:47.000 AM)   No Event Sampling

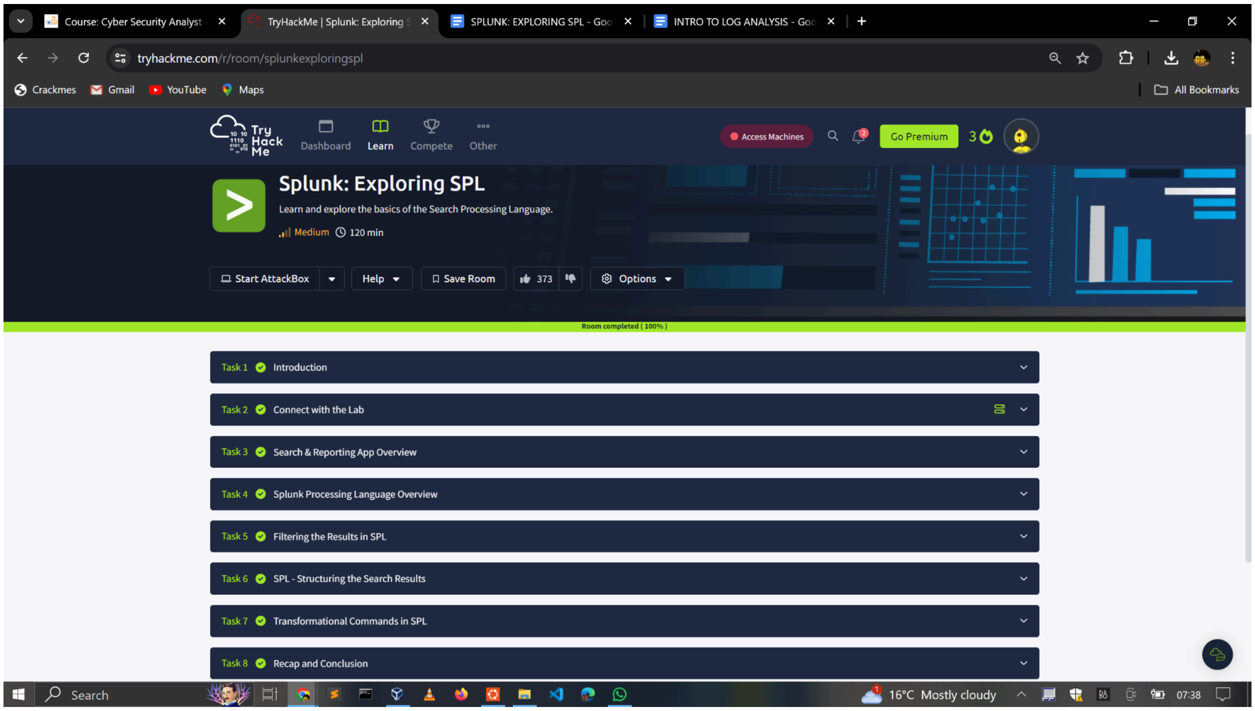
Events (12,256)   Patterns   Statistics (35)   Visualization

```
Image:  C:\Windows\System32\conhost.exe
count:  70
count%: 1.656%
```

New Search
Pie Chart
Format
Trellis
other (21)
System
C:\windows\system32\taskhostw.exe
C:\windows\system32\svchost.exe
C:\Windows\System32\BackgroundTransferHost.exe
C:\Windows\System32\RuntimeBroker.exe
C:\Windows\System32\backgroundTaskHost.exe
C:\Windows\System32\conhost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\usocoreworker.exe
C:\Windows\System32\wbem\WMIC.exe
C:\Windows\System32\wbem\WmiPrvSE.exe
C:\windows\System32\svchost.exe
C:\windows\system32\BackgroundTransferHost.exe
C:\windows\system32\backgroundTaskHost.exe
Image
count

3. MODULE COMPLETION

https://tryhackme.com/p/c1ph3rbnuk



Splunk: Exploring SPL

Learn and explore the basics of the Search Processing Language.

Medium   120 min

Room completed (100%)

- Task 1 ✓ Introduction
- Task 2 ✓ Connect with the Lab
- Task 3 ✓ Search & Reporting App Overview
- Task 4 ✓ Splunk Processing Language Overview
- Task 5 ✓ Filtering the Results in SPL
- Task 6 ✓ SPL - Structuring the Search Results
- Task 7 ✓ Transformational Commands in SPL
- Task 8 ✓ Recap and Conclusion

4. CONCLUSION

This assignment gave me a glimpse of working with Splunk for event log analysis. I have learned how to write SPL commands to retrieve, filter, transform, search and visualize data in Splunk. This knowledge will help me as a security analyst to sift through a mountain of logs generated daily in a work environment and identify anomalies and or track evidence of a security incident.