

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.

We go to the Search and data summary. We can see it's cyber host.

The screenshot shows the Splunk Search interface. A modal window titled "Data Summary" is open, displaying a table with the following data:

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

The modal also includes tabs for "Hosts (1)", "Sources (1)", and "Sourcetypes (1)", and a "filter" input field. The background interface shows the "Search" page with a search bar, "Search History", and "How to Search" section.

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

cyber-host

✓ Correct Answer

🔍 Hint

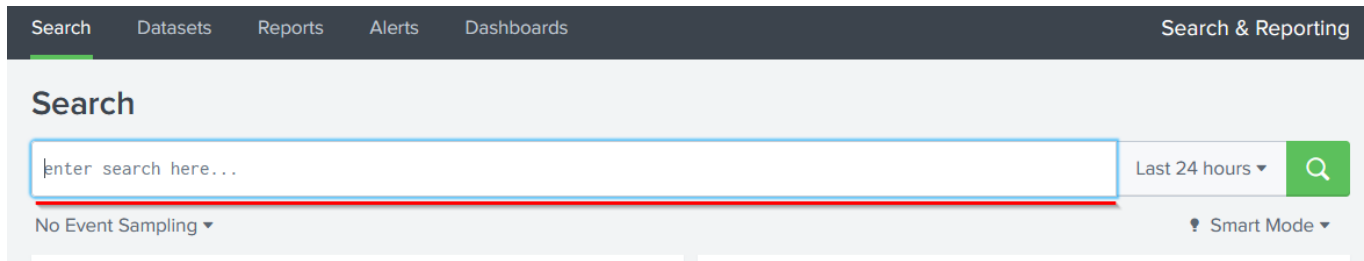
**Search & Reporting App** is the default interface used to search and analyze the data on the Splunk Home page. It has various functionalities that assist analysts in improving the search experience.

The screenshot shows the Splunk Search & Reporting App interface. The top navigation bar includes "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". The "Search" page is active, showing a search bar, "Search History", and "How to Search" section. The "How to Search" section includes links to "Documentation", "Tutorial", and "Data Summary". The "Search & Reporting" section is also visible, featuring a "Create Table View" button and a "Learn more" link.

Some important functionalities present in the search App are explained below:

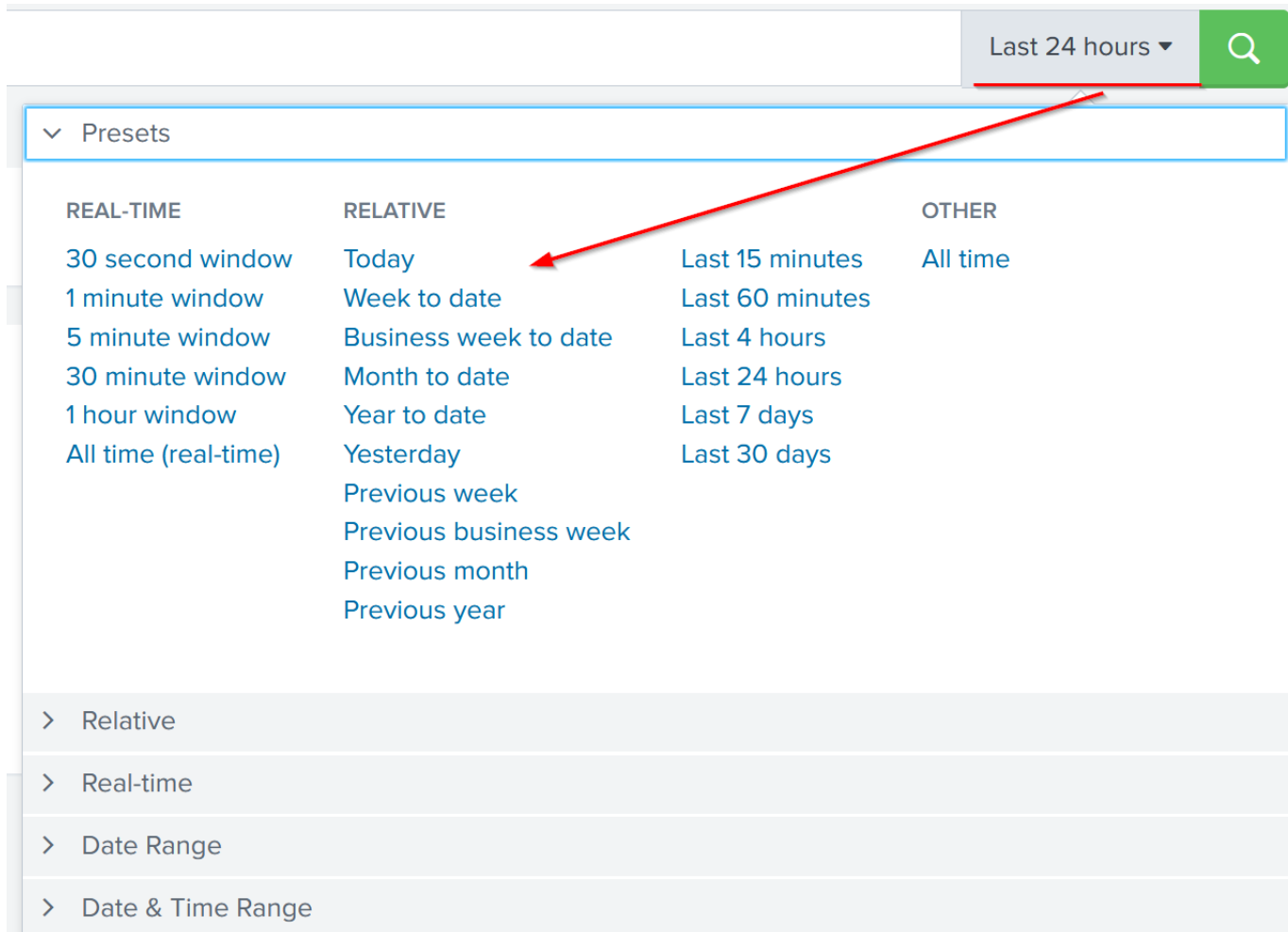
### 1) Search Head:

Search Head is where we use search processing language queries to look for the data.



### 2) Time Duration:

This tab option provides multiple options to select the time duration for the search. **All-time** will display the events in real-time. Similarly, the **last 60 minutes** will display all the events captured in the last hour.



### 3) Search History:

This tab saves the search queries that the user has run in the past along with the time when it was run. It lets the user click on the past searches and look at the result. The filter option is used to search for the particular query based on the term.

Search History

filter  No Time Filter 50 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

i	Search	Actions	Last Run
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>name"passwd=batman"*   stats count by _time, c_ip, form_data</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>name=admin&amp;"*   stats count by _time, c_ip, form_data</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>passwd"   rex field=form_data "passwd=(?&lt;p&gt;\w+)"   stats count</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>passwd"   rex field=form_data "passwd=(?&lt;p&gt;\w+)"   stats count</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>http_method="POST" form_data="username"passwd"   rex field=form_data "passwd=(?&lt;p&gt;\w+)"   stats count</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>form_data="username"passwd"   stats count by src_ip, dest_ip</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>form_data="username"passwd"   stats count by src_ip</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>form_data="username"passwd"   stats count by c_ip</div> <div>Add to Search</div> </div>	14 minutes ago
>	<div> <div>No Time Filter</div> <div> <div>Ran:</div> <div>Today</div> </div> <div> <div>Ran in:</div> <div>Last 7 Days</div> </div> <div> <div>Ran in:</div> <div>Last 30 Days</div> </div> </div>	<div> <div>form_data="username"passwd=batman"</div> <div>Add to Search</div> </div>	14 minutes ago

#### 4) Data Summary:

This tab provides a summary of the data type, the data source, and the hosts that generated the events as shown below. This tab is very important feature used to get a brief idea about the network visibility.

Search

Datasets

Reports

Alerts

Dashboards

Search & Reporting

Search

1 enter search here...

Last 24 hours

Q

No Event Sampling

Verbose Mode

How to Search

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

Documentation

Tutorial

What to Search

956,046 Events

6 years ago

4 hours ago

INDEXED

EARLIEST EVENT

LATEST EVENT

Data Summary

> Search History

#### 5) Field Sidebar:

The Field Sidebar can be found on the left panel of Splunk search. This sidebar has two sections showing selected fields and interesting fields. It also provides quick results, such as top values and raw values against each field.

List

Format

50 Per Page

< Hide Fields

All Fields

1

SELECTED FIELDS

3

a DestinationIp 18

a host 1

a source 1

a SourceIp 7

a sourcetype 1

a User 4

2

INTERESTING FIELDS

# @version 1

a AccountName 4

a AccountType 2

a Application 22

a Category 41

a Channel 9

4

# date\_hour 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:\w

Category: Process accessed (rule: ProcessAccess)

Channel: Microsoft-Windows-Sysmon/Operational

Domain: NT AUTHORITY

EventID: 10

EventReceivedTime: 2022-04-15 08:05:46

EventTime: 2022-04-15 08:05:44

EventType: INFO

ExecutionProcessID: 3348

GrantedAccess: 0x1000

Hostname: Micheal.Beaven

Keywords: -9223372036854776000

..

Some important points to understand about the sidebar are explained below:

<b>1- Selected Fields</b>	Splunk extracts the default fields like source, sourcetype, and host, which appear in each event, and places them under the selected fields column. We can select other fields that seem essential and add them to the list.
<b>2- Interesting Fields</b>	Pulls all the interesting fields it finds and displays them in the left panel to further explore.
<b>3- Alpha-numeric fields 'α'</b>	This alpha symbol shows that the field contains text values.
<b>4- Numeric fields '#'</b>	This symbol shows that this field contains numerical values.
<b>5- Count</b>	The number against each field shows the number of events captured in that timeframe.

Answer the questions below

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 Answer

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

We can find the answer here:

The screenshot shows the Splunk Search interface. At the top, there's a navigation bar with 'splunk enterprise' and various menu items like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. Below this, a search bar contains the text '1 enter search here...'. To the right of the search bar, there's a 'Last 24 hours' filter and a search icon. Below the search bar, there's a 'No Event Sampling' dropdown and a 'Verbose Mode' checkbox. The main section is titled 'Search History' and contains a table with search queries and their execution details.

i	Search	Actions	Last Run
>	source="Event_logs.json" host="cyber-host" index="windowslogs" sourcetype="json"	<a href="#">Add to Search</a>	Fri Jul 15 2022 01:38:18
>	index="	<a href="#">Add to Search</a>	Thu Jul 14 2022 06:25:19
>	*	<a href="#">Add to Search</a>	Mon Jul 04 2022 01:48:50
>	index="   delete	<a href="#">Add to Search</a>	Mon Jul 04 2022 00:24:47
>	index="   stats count by index	<a href="#">Add to Search</a>	Mon Jul 04 2022 00:24:31
>	index=windowslogs   chart count by Image	<a href="#">Add to Search</a>	Sun Jul 03 2022 22:40:27
>	index=windowslogs   chart count(EventCode) by Image	<a href="#">Add to Search</a>	Sun Jul 03 2022 22:40:14
>	index=windowslogs   chart count(EventCode) by User	<a href="#">Add to Search</a>	Sun Jul 03 2022 22:40:05
>	index=windowslogs   rare User	<a href="#">Add to Search</a>	Sun Jul 03 2022 22:38:21
>	index=windowslogs   rare EventID	<a href="#">Add to Search</a>	Sun Jul 03 2022 22:38:10

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

172.90.12.11

✓ Correct Answer

🔍 Hint

The screenshot shows the Splunk Search interface with a field panel open. The field panel is titled 'SourceIP' and shows 7 values, 0.702% of events. It has a 'Selected' dropdown set to 'Yes' and a 'No' button. Below the dropdown, there's a 'Reports' section with 'Top values', 'Top values by time', and 'Rare values'. The 'Top values' report is selected, showing a table of values, counts, and percentages.

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%
0:0:0:0:0:0:1	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:fb	1	1.163%

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 Answer

Splunk Search Processing Language comprises of multiple functions, operators and commands that are used together to form a simple to complex search and get the desired results from the ingested logs. Main components of SPL are explained below:

## Search Field Operators

Splunk field operators are the building blocks used to construct any search query. These field operators are used to filter, remove, and narrow down the search result based on the given criteria. Common field operators are Comparison operators, wildcards, and boolean operators.

## Comparison Operators

These operators are used to compare the values against the fields. Some common comparisons operators are mentioned below:

Field Name	Operator	Example	Explanation
Equal	=	UserName=Mark	This operator is used to match values against the field. In this example, it will look for all the events, where the value of the field UserName is equal to Mark.
Not Equal to	!=	UserName!=Mark	This operator returns all the events where the UserName value does not match Mark.
Less than	<	Age < 10	Showing all the events with the value of Age less than 10.
Less than or Equal to	<=	Age <= 10	Showing all the events with the value of Age less than or equal to 10.
Greater than	>	Outbound_traffic > 50 MB	This will return all the events where the Outbound traffic value is over 50 MB.
Greater Than or Equal to	>=	Outbound_traffic >= 50 MB	This will return all the events where the Outbound traffic value is greater or equal to 50 MB.

Lets use the comparison operator to display all the event logs from the index "windowslogs", where AccountName is not Equal to "System"

**Search Query:** `index=windowslogs AccountName !=SYSTEM`

1 index=windowslogs AccountName !=SYSTEM

✓ 84 events (before 9/30/22 8:42:34.000 AM) No Event Sampling ▼

Events (84) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 50 Per Page ▼

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # @version 1
- a AccountName 3
- a AccountType 2
- a ActivityID 80
- a Category 1
- a Channel 4
- a ContextInfo 79
- # date\_hour 1
- # date\_mday 1

**AccountName**

3 Values, 100% of events Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Values	Count	%
James	79	94.048%
NETWORK SERVICE	4	4.762%
LOCAL SERVICE	1	1.19%

## Boolean Operators

Splunk supports the following Boolean operators, which can be very handy in searching/filtering and narrowing down results.

Operator	Syntax	Explanation
<b>NOT</b>	field_A <b>NOT</b> value	Ignore the events from the result where field_A contain the specified value.
<b>OR</b>	field_A=value1 <b>OR</b> field_A=value2	Return all the events in which field_A contains either value1 or value2.
<b>AND</b>	field_A=value1 <b>AND</b> field_B=value2	Return all the events in which field_A contains value1 and field_B contains value2.

To understand how boolean operator works in SPL, lets add the condition to show the events from the James account.

**Search Query:** index=windowslogs AccountName !=SYSTEM **\*\*AND\*\*** AccountName=James

## New Search

Save As ▾ Create Table View Close

**1** index=windowslogs AccountName !=SYSTEM AND AccountName=James

All time ▾ 🔍

✓ 79 events (before 9/23/22 1:08:40.000 AM) No Event Sampling ▾

🟢 Job ▾ || 📊 ↺ 🖨️ ⬇️ 🗨️ Verbose Mode ▾

Events (79) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 second per column

List ▾ ✎ Format 50 Per Page ▾ < Prev **1** 2 Next >

< Hide Fields	⚙ All Fields	i Time	Event
SELECTED FIELDS		> 4/15/22	{ [-]
a host 1		8:06:48.000 AM	@version: 1
a source 1			AccountName: James
a sourcetype 1			AccountType: User

## Wild Card

Splunk supports wildcards to match the characters in the strings.

Wildcard symbol	Example	Explanation
*	status=fail*	It will return all the results with values like  status=failed  status=failure

In the events, there are multiple DestinationIPs reported. Let's use the wildcard only to show the **DestinationIP** starting from 172.\*

**Search Query:** index=windowslogs DestinationIp=172.\*



1 index=windowslogs DestinationIp=172.\*

✓ 53 events (before 9/23/22 1:44:35.000 AM) No Event Sampling ▾

Events (53) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields ⋮ All Fields

SELECTED FIELDS

- a DestinationIp 3
- a host 1
- a source 1
- a sourcetype 1
- a User 3

INTERESTING FIELDS

- # @version 1

**DestinationIp**

3 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
172.18.38.5	37	69.811%
172.90.12.11	10	18.868%
172.18.39.6	6	11.321%

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

4

✓ Correct Answer

So first in the search we type this

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

New Search

1 index=windowslogs EventID="1" User=\*JAMES\*

Save As ▾ Create Table View Close

All time

✓ 4 events (before 7/9/24 9:50:31.000 AM) No Event Sampling ▾

Job ▾

from this we get number of events like shown in the next photo:

New Search

Save As ▾ Create Table View Close

1 index=windowslogs EventID="1" User=\*JAMES\*

All time

✓ 4 events (before 7/9/24 9:50:31.000 AM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

10 milliseconds per column

List ▾ Format 50 Per Page ▾

< Hide Fields ⋮ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1
- a User 1

INTERESTING FIELDS

- # @version 1
- a AccountName 1
- a AccountType 1
- a Category 1
- a Channel 1
- a CommandLine 1

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\net user /add Alberto paw0rd1 Company: Microsoft Corporation CurrentDirectory: C:\windows\system32\ Description: Net Command Domain: NT AUTHORITY EventID: 1

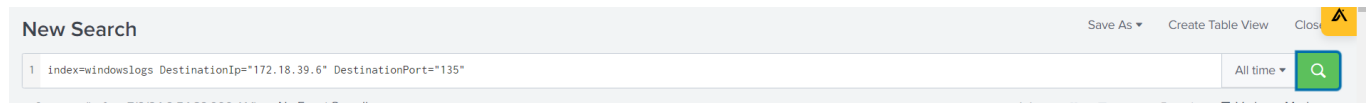
How many events are observed with Destination IP 172.18.39.6 AND destination Port 135?

4

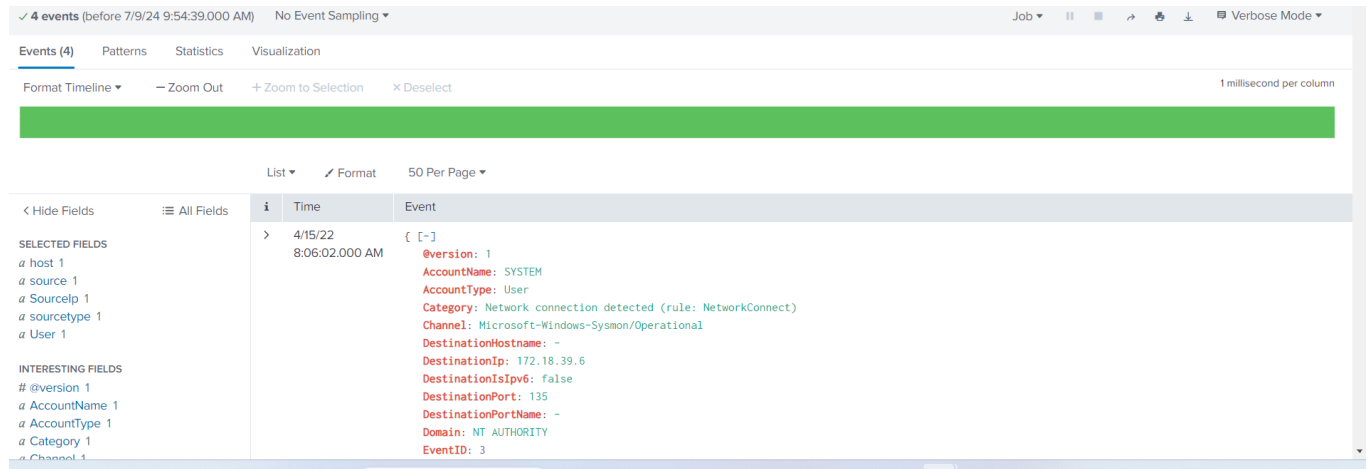
✓ Correct Answer

🔍 Hint

For this answer in search we typed in this



and we got 4 events



so that's why the answer is 4

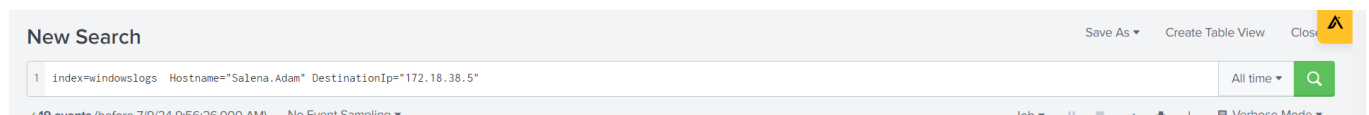
What is the Source IP with highest count returned with this Search query?

Search Query: index=windowslogs Hostname="Salena.Adam" DestinationIp="172.18.38.5"

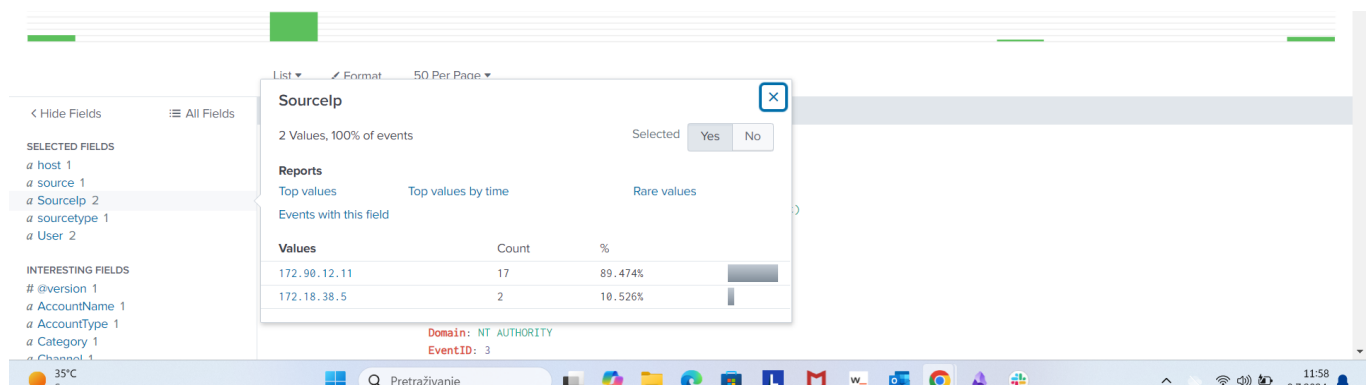
172.90.12.11

✓ Correct Answer

For this question in the search bar we had to type in this:



Then here we can see answer to our question



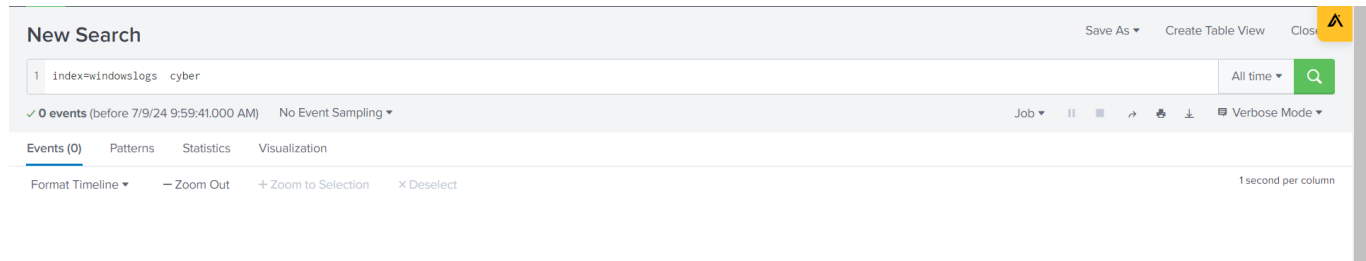
In the index windowslogs, search for all the events that contain the term **cyber** how many events returned?

0

✓ Correct Answer

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

In the search bar we type in this



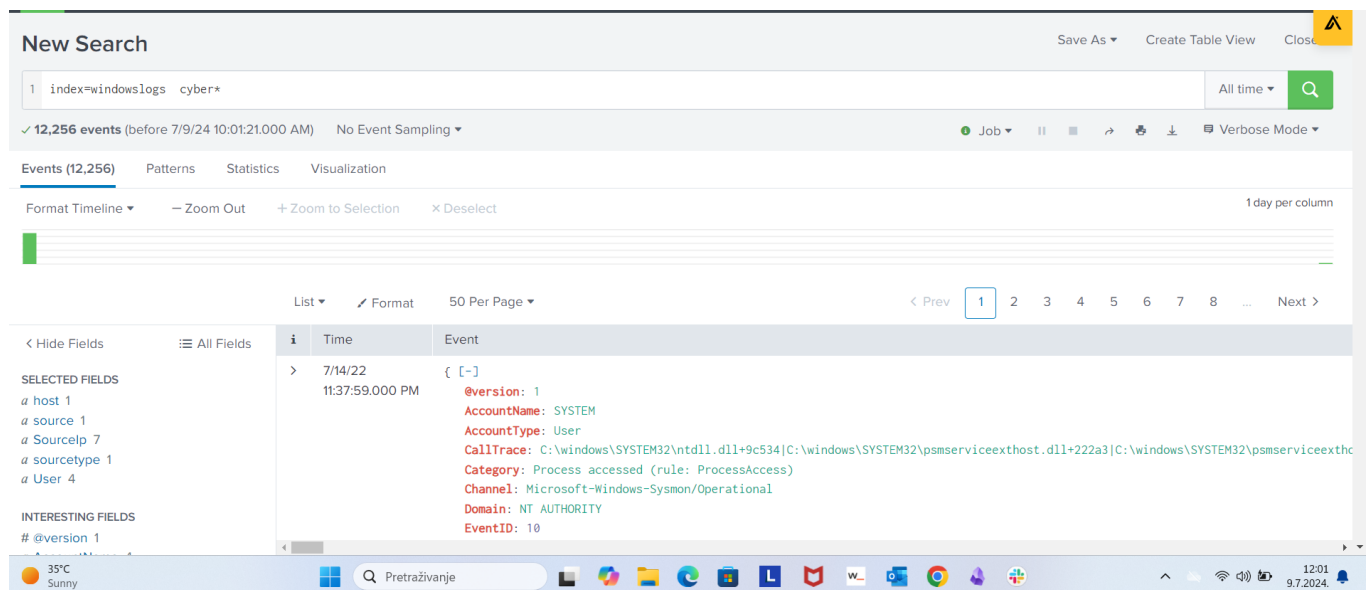
and we can see that the output is 0

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

12256

✓ Correct Answer

In the search bar we type this



and we can see there are 12256 generated events so that is the answer to our question.

Our network generates thousands of logs each minute, all ingesting into our SIEM solution. It becomes a daunting task to search for any anomaly without using filters. SPL allows us to use **Filters** to narrow down the result and only show the important events that we are interested in. We can add or remove certain data from the result using filters. The following commands are useful in applying filters to the search results.

## Fields

<b>Command</b>	<b>fields</b>
<b>Explanation</b>	Fields command is used to add or remove mentioned fields from the search results. To remove the field, minus sign ( - ) is used before the fieldname and plus ( + ) is used before the fields which we want to display.
<b>Syntax</b>	fields <field_name1> <field_name2>
<b>Example</b>	fields + HostName - EventID

Let's use the fields command to only display host, User, and SourceIP fields using the following syntax.

**Search Query:** `index=windowslogs | fields + host + User + SourceIp`

**New Search**

1 `index=windowslogs | fields + host + User + SourceIp`

✓ 12,256 events (before 9/23/22 3:41:06.000 AM) No Event Sampling ▼

Events (12,256) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ / Format 50 Per Page ▼

< Hide Fields All Fields

**SELECTED FIELDS**

- a host 1
- a SourceIp 7
- a User 4

**Event**

i	Time	Event
>	7/14/22 11:37:59.000 PM	{ [-] @version: 1 AccountName: SYSTEM AccountType: User CallTrace: C:\windows\% Category: Process acces

**Note:** Click on the **More field** to display the fields if some fields are not visible.

< Hide Fields

☰ All Fields

## SELECTED FIELDS

*a* host 1

*a* User 4

1 more field

+ Extract New Fields

## Search

<b>Command</b>	<b>search</b>
<b>Explanation</b>	This command is used to search for the raw text while using the chaining command <code>\ </code>
<b>Syntax</b>	<code>  search &lt;search_keyword&gt;</code>
<b>Example</b>	<code>  search "Powershell"</code>

Use the search command to show all the events containing the term Powershell. This will return all the events that contain the term "**Powershell**".

**Search Query:** `index=windowslogs | search Powershell`

New SearchSave AsCreate Table

1 index=windowslogs | search Powershell

✓ 198 events (before 10/26/22 8:25:41.000 PM)

No Event Sampling

Job

Events (198)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

List

Format

50 Per Page

Prev

1

2

3

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

a User 1

INTERESTING FIELDS

# @version 1

a AccountName 2

a AccountType 1

a ActivityID 79

a Category 9

i

Time

Event

>

4/15/22

8:06:48.000 AM

{ [-]

@version: 1

Category: Pipeline Execution Details

Channel: Windows PowerShell

EventID: 800

EventReceivedTime: 2022-04-15 08:06:49

EventTime: 2022-04-15 08:06:48

EventType: INFO

ExecutionProcessID: 0

Hostname: James.browne

Keywords: 36028797018963970

Message: Pipeline execution details for command line:

## Dedup

<b>Command</b>	<b>dedup</b>
<b>Explanation</b>	Dedup is the command used to remove duplicate fields from the search results. We often get the results with various fields getting the same results. These commands remove the duplicates to show the unique values.
<b>Syntax</b>	dedup
<b>Example</b>	dedup EventID

We can use the dedup command to show the list of unique **EventIDs** from a particular hostname.

**Search Query:** index=windowslogs | table EventID User Image Hostname | dedup EventID

New Search

Save As

Create Table View

Close

1 index=windowslogs | table EventID User Image Hostname | dedup EventID

All time

12,256 events (before 10/26/22 8:38:50.000 PM)

No Event Sampling

Job

Verbose Mode

Events (12,256)

Patterns

Statistics (55)

Visualization

100 Per Page

Format

Preview

EventID	User	Image	Hostname
18		C:\Windows\System32\RuntimeBroker.exe	James.browne
12		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	James.browne
3	NT AUTHORITY\SYSTEM	C:\Windows\System32\dns.exe	Salena.Adam
22		C:\Windows\System32\svchost.exe	James.browne
7		C:\Windows\System32\svchost.exe	James.browne
1	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	James.browne

## Rename

Command	rename
Explanation	It allows us to change the name of the field in the search results. It is useful in a scenario when the field name is generic or log, or it needs to be updated in the output.
Syntax	rename
Example	rename User as Employees

Let's rename the User field to Employees using the following search query.

**Search Query:** index=windowslogs | fields + host + User + SourceIp | rename User as Employees

## New Search

1 index=windowslogs | fields + host + User + SourceIp | rename User as Employees

✓ 12,256 events (before 9/23/22 3:45:00.000 AM) No Event Sampling

Events (12,256) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect



List ▾ / Format 50 Per Page ▾

< Hide Fields

≡ All Fields

SELECTED FIELDS

a Employees 4

a host 1

a SourceIp 7

+ Extract New Fields

i	Time	Event
>	7/14/22 11:37:59.000 PM	{ [-] @version: 1 AccountName: SYSTEM AccountType: User CallTrace: C:\windows Category: Process acc Channel: Microsoft-Wi Domain: NT AUTHORITY

Answer the questions below

What is the third EventID returned against this search query?

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

4103

✓ Correct Answer

We first type in this to the search query

New Search

Save As ▾ Create Table View Close

1 index=windowslogs | table \_time EventID Hostname SourceName | reverse

All time ▾



and we can see answer from the output



## New Search

1

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

All time

🔍

✓ 12,256 events (before 7/9/24 10:06:47.000 AM) No Event Sampling

🟢 Job

⏸

■

↶

🖨

⬇

🗨 Verbose Mode

Events (12,256)

Patterns

Statistics (12,256)

Visualization

100 Per Page

✍ Format

Preview

< Prev

1

2

3

4

5

6

7

8

...

Next >

_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 08:05:46.000 to 2022-04-15 08:05:46.001	800	James.browne	PowerShell
View events	4103	James.browne	Microsoft-Windows-PowerShell
Narrow to this time range	800	James.browne	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	800	James.browne	PowerShell

We type in this to the search bar

and we get the output like this

So first generated username is Selena.Adam

## Table

<b>Example</b>	table
	head 20 # will return the top 20 events from the result list.

This search query will create a table with three columns selected and ignore all the remaining columns from the display.

**Search Query:** index=windowslogs | table EventID Hostname SourceName

### New Search

1 index=windowslogs | table EventID Hostname SourceName

✓ 12,256 events (before 10/26/22 9:07:01.000 PM) No Event Sampling ▼

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

100 Per Page ▼
Format
Preview ▼
< Prev

EventID ↕	Hostname ↕	SourceName ↕
10	Micheal.Beaven	Microsoft-Windows-Sysmon
10	Micheal.Beaven	Microsoft-Windows-Sysmon
10	Micheal.Beaven	Microsoft-Windows-Sysmon
10	Micheal.Beaven	Microsoft-Windows-Sysmon
5156	James.browne	Microsoft-Windows-Security-Auditing
5158	James.browne	Microsoft-Windows-Security-Auditing
800	James.browne	PowerShell
4103	James.browne	Microsoft-Windows-PowerShell
800	James.browne	PowerShell

## Head

<b>Explanation</b>	The <b>head</b> command returns the first 10 events if no number is specified.
<b>Syntax</b>	head
<b>Example</b>	head # will return the top 10 events from the result list   head 20 # will return the top 20 events from the result list

The following search query will show the table containing the mentioned fields and display only the top 5 entries.

**Search Query:** index=windowslogs | table \_time EventID Hostname SourceName  
| \*\*head 5\*\*

1

index=windowslogs | table \_time EventID Hostname SourceName | head 5

All time

✓ 12,256 events (before 9/25/22 12:38:38.000 AM) No Event Sampling ▾

Job ▾

▮

↗

🖨

⬇

🗨 Verbose

Events (12,256)

Patterns

Statistics (5) ▾

Visualization

100 Per Page ▾

✎ Format

Preview ▾

_time ▾	EventID ▾ ✎	Hostname ▾ ✎	SourceName ▾
2022-07-14 23:37:59	10	Micheal.Beaven	Microsoft-Windows-Sysmon
2022-07-14 23:37:59	10	Micheal.Beaven	Microsoft-Windows-Sysmon
2022-07-14 23:37:59	10	Micheal.Beaven	Microsoft-Windows-Sysmon
2022-07-14 23:37:59	10	Micheal.Beaven	Microsoft-Windows-Sysmon
2022-07-14 23:37:59	5156	James.browne	Microsoft-Windows-Security-Auditing

## Tail

Explanation	The <b>Tail</b> command returns the last 10 events if no number is specified.
Syntax	tail
Example	tail # will return the last 10 events from the result list    tail 20 # will return the last 20 events from the result list

The following search query will show the table containing the mentioned fields and display only 5 entries from the bottom of the list.

**Search Query:** index=windowslogs | table \_time EventID Hostname SourceName | tail 5

1 index=windowslogs | table \_time EventID Hostname SourceName | tail 5

✓ 12,256 events (before 9/25/22 1:14:18.000 AM) No Event Sampling ▾

Job ▾ || ▣ ↗ 🖨 ⬇ 🗨 V

Events (12,256) Patterns **Statistics (5)** Visualization

100 Per Page ▾ ✎ Format Preview ▾

_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

## sort

<b>Explanation</b>	The <b>Sort</b> command allows us to order the fields in ascending or descending order.
<b>Syntax</b>	sort <field_name>
<b>Example</b>	sort Hostname # This will sort the result in Ascending order.

The following search query will sort the results based on the Hostname field.

**Search Query:** index=windowslogs | table \_time EventID Hostname SourceName | sort Hostname

1 index=windowslogs   table _time EventID Hostname SourceName   sort Hostname					All
✓ 12,256 events (before 9/25/22 1:17:18.000 AM) No Event Sampling ▾					Job ▾    ■ → 🖨️ ⬇️ 🗨️ Ve
Events (12,256)	Patterns	Statistics (10,000)	Visualization		
100 Per Page ▾	Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8		
_time ▾	EventID ▾	Hostname ▾	SourceName ▾		
2022-07-14 23:37:59	5156	James.browne	Microsoft-Windows-Security-Auditing		
2022-07-14 23:37:59	5158	James.browne	Microsoft-Windows-Security-Auditing		
2022-04-15 08:06:48	800	James.browne	PowerShell		
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell		
2022-04-15 08:06:48	800	James.browne	PowerShell		
2022-04-15 08:06:48	800	James.browne	PowerShell		
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell		
2022-04-15 08:06:48	800	James.browne	PowerShell		
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell		
2022-04-15 08:06:48	800	James.browne	PowerShell		

## Reverse

<b>Explanation</b>	The reverse command simply reverses the order of the events.
<b>Syntax</b>	reverse
<b>Example</b>	<Search Query> \   reverse

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

# New Search

Save As Create

1 index=windowslogs | table \_time EventID Hostname SourceName | reverse

✓ 12,256 events (before 10/26/22 9:28:24.000 PM) No Event Sampling
Job

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

100 Per Page Format Preview
< Prev 1 2 3 4 5 6

_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

Answer the questions below

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

✓ Correct Answer

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

We can see the answer is James.browne

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

4103

✓ Correct Answer

When we type this into the search bar we can see what was the last EventID

# New Search

1 index=windowslogs | table \_time EventID Hostname SourceName  
2 | tail

All time

✓ 12,256 events (before 7/9/24 10:21:33.000 AM) No Event Sampling
Job
Verbose Mode

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

100 Per Page Format Preview

_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

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

Microsoft-Windows-Directory-Services-SAM

✓ Correct Answer

We can see the answer is this

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below this is a 'Search & Reporting' section with a 'New Search' button. The search query is entered in a text box: `1 index=windowslogs | table _time EventID Hostname SourceName`  
`2`  
`3 | sort SourceName`  
The results show 12,256 events. The 'Statistics (10,000)' tab is selected, displaying a table with columns: \_time, EventID, Hostname, and SourceName. The table shows several rows of data, with the top SourceName being 'Microsoft-Windows-Directory-Services-SAM'. The interface also includes a 'Save As' button, 'Create Table View', and 'Close' options. The bottom of the screen shows a Windows taskbar with various application icons and a system clock.

Transformational commands are those commands that change the result into a data structure from the field-value pairs. These commands simply transform specific values for each event into numerical values which can easily be utilized for statistical purposes or turn the results into visualizations. Searches that use these transforming commands are called transforming searches. Some of the most used transforming commands are explained below.

## General Transformational Commands

### Top

Command	<b>top</b>
Explanation	This command returns frequent values for the top 10 events.
Syntax	<code>  top &lt;field_name&gt;</code>  <code>  top limit=6 &lt;field_name&gt;</code>
Example	<code>top limit=3 EventID</code>

The following command will display the top 7 Image ( representing Processes) captured.

**Search Query:** `index=windowslogs | top limit=7 Image`

1 index=windowslogs   top limit=7 Image			All time	
✓ 12,256 events (before 6/28/22 11:29:39.000 PM) No Event Sampling			Job	
Events (12,256)	Patterns	Statistics (7)	Visualization	
100 Per Page	Format	Preview		
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	

## Rare

<b>Command</b>	<b>rare</b>
<b>Explanation</b>	This command does the opposite of top command as it returns the least frequent values or bottom 10 results.
<b>Syntax</b>	rare <field_name>    rare limit=6 <field_name>
<b>Example</b>	rare limit=3 EventID

The following command will display the rare 7 Image (Processes) captured.

**Search Query:** index=windowslogs | rare limit=7 Image

1 index=windowslogs   rare limit=7 Image			All time	
✓ 12,256 events (before 6/28/22 11:32:48.000 PM) No Event Sampling			Job	
Events (12,256)	Patterns	Statistics (7)	Visualization	
100 Per Page	Format	Preview		
Image		count	percent	
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe		1	0.023652	
C:\windows\system32\SecurityHealthService.exe		1	0.023652	
C:\windows\system32\net1.exe		1	0.023652	
C:\windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe		2	0.047304	
C:\Windows\System32\dfsrs.exe		3	0.070956	
C:\windows\Explorer.EXE		3	0.070956	
C:\windows\system32\services.exe		5	0.118259	

## Highlight

<b>Command</b>	<b>highlight</b>
----------------	------------------

<b>Explanation</b>	The highlight command shows the results in raw events mode with fields highlighted.
<b>Syntax</b>	highlight <field_name1> <field_name2>
<b>Example</b>	highlight User, host, EventID, Image

The following command will highlight the three mentioned fields in the raw logs

**Search Query:** index=windowslogs | highlight User, host, EventID, Image

1 index=windowslogs All time

✓ 12,256 events (before 6/28/22 11:42:24.000 PM) No Event Sampling

Events (12,256) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 50 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- 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

Time Event

> 6/23/22 8:23:26.000 PM { [-]

```

@version: 1
AccountName: SYSTEM
AccountType: User
CallTrace: C:\windows\SYSTEM32\ntdll.dll+9c534|C:\windows\SYSTEM32\psmserviceexhost.dll+222a3|C:\windows\SYSTEM32\psmser
Category: Process accessed (rule: ProcessAccess)
Channel: Microsoft-Windows-Sysmon/Operational
Domain: NT AUTHORITY
EventID: 10
EventReceivedTime: 2022-02-14 08:05:46
EventTime: 2022-02-14 08:05:44
EventType: INFO
ExecutionProcessID: 3348

```

## STATS Commands

SPL supports various stats commands that help in calculating statistics on the values. Some common stat commands are:

Command	Explanation	Syntax	Example
<b>Average</b>	This command is used to calculate the average of the given field.	stats avg(field_name)	stats avg(product_price)
<b>Max</b>	It will return the maximum value from the specific field.	stats max(field_name)	stats max(user_age)
<b>Min</b>	It will return the minimum value from the specific field.	stats min(field_name)	stats min(product_price)
<b>Sum</b>	It will return the sum of the fields in a specific value.	stats sum(field_name)	stats sum(product_cost)
<b>Count</b>	The count command returns the number of data occurrences.	stats count(function) AS new_NAME	stats count(source_IP)



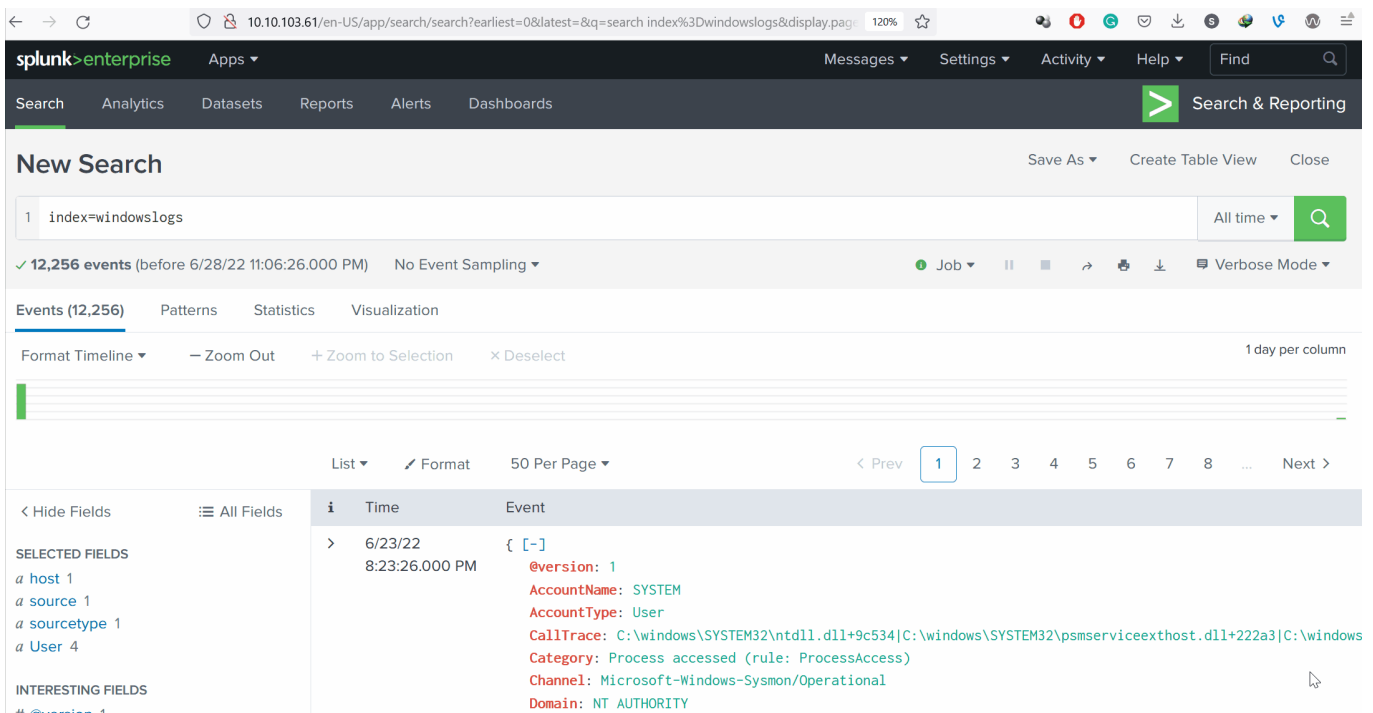
## Splunk Chart Commands

These are very important types of transforming commands that are used to present the data in table or visualization form. Most of the chart commands utilize various stat commands.

### Chart

<b>Command</b>	<b>chart</b>
<b>Explanation</b>	The chart command is used to transform the data into tables or visualizations.
<b>Syntax</b>	chart
<b>Example</b>	chart count by User

**Search Query:** `index=windowslogs | chart count by User`



### Timechart

<b>Command</b>	<b>timechart</b>
<b>Explanation</b>	The timechart command returns the time series chart covering the field following the function mentioned. Often combined with STATS commands.
<b>Syntax</b>	timechart function <field_name>
<b>Example</b>	timechart count by Image

The following query will display the Image chart based on the time.

Search Query: `index=windowslogs | timechart count by Image`

Answer the questions below

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

196

✓ Correct Answer

We can see from the output that the total count of the 6th image is this

New Search

Save As Create Table View Close

1 index=windowslogs | top limit=7 Image

All time

✓ 12,256 events (before 7/9/24 10:29:39.000 AM) No Event Sampling

Job

Events (12,256) Patterns Statistics (7) Visualization

100 Per Page Format Preview

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\WmiPrivSE.exe	108	2.554399

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

James

✓ Correct Answer

When we type this into search we can see the user is James

New Search

Close

1 index=windowslogs | rare limit=7 User

All time

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

70

✓ Correct Answer