

Learn the following:

- SPL (Search Processing Language)
- Applying filters
- Transformational commands
- Changing order of results



Splunk: Exploring SPL

Learn and explore the basic of the SPL (Search Processing Language)

Task 1 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 dive deep into some key fundamentals of searching capability, like chaining SPL queries to construct simple to complex queries.

Learning Objectives

This room will teach the following topics:

- What is Search Processing Language?
- How to apply filters to narrow down results.
- Using transformational commands.
- Changing the order of the results.

Room Prerequisites

- This room is based on the SIEM concepts covered in Intro to SIEM and Splunk: Basics rooms. Complete these rooms and continue to the next task.

Answer the questions below

No answer needed

Task 2 Connect with the Lab

Room Machine

Before moving forward, deploy the machine. You can access this lab in the AttackBox or click <https://10-64-186-165.reverse-proxy.cell-prod-us-east-1a.vm.tryhackme.com/> to start the lab in your browser when the machine is fully started. The machine will take up to 3-5 minutes to start.

Note: For this room, we will work on the index **Windowslogs**.

Answer the questions below

1. Connect with Lab.

Launch **AttackBox** Machine

Launch **Firefox browser**: Enter given URL in browser to start the Splunk lab

On **Splunk GUI**:

1. Enter: `index=windows.logs*` (use windows log file for investigation)
2. In Time Frame: Select **All time**

The screenshot shows the Splunk interface with a search bar containing 'index=windows.logs*'. To the right of the search bar, a dropdown menu for 'Time' is open, showing various time ranges like 'REAL-TIME', 'RELATIVE', and 'ALL TIME'. The 'All time' option is highlighted. Below the search bar, there is a table of search results with columns for 'EventID', 'EventTime', 'EventType', 'ExecutionProcessID', 'File', 'Host', and 'Keywords'. One row in the table is highlighted, showing details for an event with EventID 302-84-15_08-05-46, EventTime 2022-04-15_08-05-46, EventType INFO, ExecutionProcessID 3348, File C:\Windows\System32\user32.dll, Hostname Michael.Beauchene, and Keywords -122317201884776908.

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

Answer: `cyber-host`

Click: `host`

The screenshot shows the Splunk interface with a search bar containing 'host cyber-host'. To the right of the search bar, a dropdown menu for 'Time' is open, showing various time ranges like 'REAL-TIME', 'RELATIVE', and 'ALL TIME'. The 'All time' option is highlighted. Below the search bar, there is a table of search results with columns for 'Value', 'Count', and '%'. The value 'cyber-host' has a count of 12,296 and a percentage of 100%. The table also includes columns for 'EventID', 'EventTime', 'EventType', 'ExecutionProcessID', 'File', 'Host', and 'Keywords'. One row in the table is highlighted, showing details for an event with EventID 302-84-15_08-05-46, EventTime 2022-04-15_08-05-44, EventType INFO, ExecutionProcessID 3348, File C:\Windows\System32\user32.dll, Hostname Michael.Beauchene, and Keywords -122317201884776908.

Task 3 Search & Reporting App Overview

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. At the top, there's a navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The main area is titled "Search" and contains a search bar with placeholder text "enter search here...". Below the search bar are buttons for "Last 24 hours" and a magnifying glass icon. A "No Event Sampling" message is displayed. To the right, there's a section titled "Analyze Your Data with Table Views" with a "Create Table View" button. On the left, there's a "How to Search" section with links to "Documentation", "Tutorial", and "Data Summary".

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.

The screenshot shows the Search Head interface. It features a search bar with "enter search here..." placeholder text and a "Last 24 hours" dropdown. Below the search bar is a "No Event Sampling" message. On the right side, there's a "Smart Mode" dropdown.

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.

The screenshot shows the "Time Duration" selection interface. It includes a "Presets" dropdown and three columns of time range options. A red arrow points from the "Last 24 hours" button at the top right towards the "Relative" column. The columns are labeled: REAL-TIME, RELATIVE, and OTHER. The REAL-TIME column lists "30 second window", "1 minute window", "5 minute window", "30 minute window", "1 hour window", and "All time (real-time)". The RELATIVE column lists "Today", "Week to date", "Business week to date", "Month to date", "Year to date", "Yesterday", "Previous week", "Previous business week", "Previous month", and "Previous year". The OTHER column lists "Last 15 minutes", "Last 60 minutes", "Last 4 hours", "Last 24 hours", "Last 7 days", and "Last 30 days". Below the columns, there are sections for "Relative", "Real-time", "Date Range", and "Date & Time Range".

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	Q	No Time Filter	50 Per Page ▾	< Prev	1	2	3	4	5	6	7	8	...	Next >
i	Search											Actions	Last Run			
	sourceType:stream/http	✓ No Time Filter	Ron:	Today	sme"passwd="batman"" i stats count by _time, c_ip, form_data	Add to Search	14 minutes ago									
>	sourceType:stream/http		Ron in:		ime\admin;" i stats count by _time, c_ip, form_data	Add to Search	14 minutes ago									
>	sourceType:stream/http		Last 7 Days		passwd" i rex field=form_data "passwd"(?>p>w)" i stats count	Add to Search	14 minutes ago									
>	sourceType:stream/http		Ron in:		passwd" i rex field=form_data "passwd"(?>p>w)" i stats count	Add to Search	14 minutes ago									
>	sourceType:stream/http		Last 30 Days		passwd" i rex field=form_data "passwd"(?>p>w)" i stats count	Add to Search	14 minutes ago									
>	sourceType:stream/http _method="POST" form_data="username"passwd"				src_ip, dest_ip	Add to Search	14 minutes ago									
>	sourceType:stream/http "imreallynotbatman.com" form_data="username"passwd"					Add to Search	14 minutes ago									
>	sourceType:stream/http "imreallynotbatman.com" form_data="username"passwd"					Add to Search	14 minutes ago									
>	sourceType:stream/http "imreallynotbatman.com" form_data="username"passwd="batman"					Add to Search	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.

The screenshot shows the Splunk search interface. At the top, there are navigation links: Search, Datasets, Reports, Alerts, and Dashboards. On the far right, there's a green arrow icon followed by the text "Search & Reporting". Below the header, the word "Search" is highlighted in bold. A search bar contains the placeholder "enter search here...". To the right of the search bar are two buttons: "Last 24 hours" with a dropdown arrow and a magnifying glass icon. Further right is a "Verbosity Mode" button with a gear icon. Below the search bar, a message says "No Event Sampling" with a dropdown arrow. The main content area is divided into two sections: "How to Search" (with links to Documentation and Tutorial) and "What to Search" (showing statistics for indexed events). At the bottom left, there's a link to "Search History".

Search

1 enter search here... Last 24 hours ▾ 🔍

No Event Sampling ▾ Verbosity 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 ③ SELECTED FIELDS <i>a DestinationIp 18</i> <i>a host 1</i> <i>a source 1</i> <i>a Sourcelp 7</i> <i>a sourcetype 1</i> <i>a User 4</i> ④ INTERESTING FIELDS <i># @version 1</i> <i>a AccountName 4</i> <i>a AccountType 2</i> <i>a Application 22</i> <i>a Category 41</i> <i>a Channel 9 ⑤</i> <i>⑥ # date_hour 1</i>	☰ All Fields	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.Bea... Keywords: -9223372036854776000 ...

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

1- Selected Fields

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.

2- Interesting Fields

Pulls all the interesting fields it finds and displays them in the left panel to further explore.

3- Alpha-numeric fields 'a'

This alpha symbol shows that the field contains text values.

4- Numeric fields '#'

This symbol shows that this field contains numerical values.

5- Count

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)

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

Click: **Search tab**

Click: **Search History**

The screenshot shows the Splunk interface with the 'Search History' page open. The top navigation bar includes 'Search', 'Analytics', 'Databases', 'Reports', 'Alerts', 'Dashboards', and 'Search & Reporting'. The 'Search' tab is active. Below the navigation is a search bar with placeholder 'Enter search here...' and a 'Last 24 hours' dropdown. A 'Search History' button is highlighted with an orange arrow. The main area displays a list of search queries with their details. One specific query is highlighted with a red box: 'index=windowslogs | chart count(EventCode) by Image'. This query has a timestamp of 'Sun Jul 03 2022 21:40:14' and an 'Actions' column showing 'Add to Search' and 'Edit' options.

Time	Action
Sun Jul 03 2022 00:35:18	Add to Search
Sun Jul 03 2022 00:48:50	Add to Search
Sun Jul 03 2022 23:24:47	Add to Search
Sun Jul 03 2022 21:02:27	Add to Search
Sun Jul 03 2022 21:40:14	Add to Search
Sun Jul 03 2022 21:40:05	Add to Search
Sun Jul 03 2022 21:38:21	Add to Search
Sun Jul 03 2022 21:38:10	Add to Search
Sun Jul 03 2022 21:37:40	Add to Search

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

Answer: 172.90.12.11

Click: **SourceAddress**

This alpha symbol shows that the field contains test values.

4-Numeric fields "A" This symbol shows that this field contains numerical values.

5-Count The number against each field shows the number of events captured at 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(EventCode) by Image` > Correct Answer

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

`172.30.12.11` > Correct Answer

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?

Check

Task 4 Splunk Search Processing Language Overview

Task 5 Filtering the Results in SPL

Task 6 SPL - Structuring the Search Results

Transformations and Commands in SPL

The screenshot displays the Splunk interface with several panels. On the left, a sidebar lists tasks: Task 4 (Splunk Search Processing Language Overview), Task 5 (Filtering the Results in SPL), Task 6 (SPL - Structuring the Search Results), and Transformations and Commands in SPL. The main area shows search results for 'index=windowslogs | chart(EventCode) by Image'. A specific event is highlighted with a bounding box, showing details like EventID: 20, Image: 'C:\Windows\system32\svchost.exe', and SourceFile: 'eventlog'. Below this, a table shows event counts for different source addresses. Orange arrows point from the question text to the highlighted event and the table. The bottom right corner shows a snippet of SPL code related to event filtering.

3. 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?

Answer: 134

In Time Frame:

Select Date & Time Range

Enter required data

Click: Apply

4-Numeric fields #* This symbol shows that this field contains numerical values.

S-Count 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)

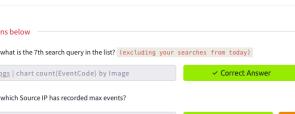
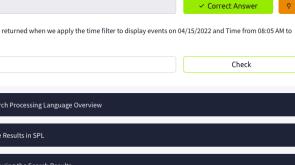
`index=_windowslogs | count[EventCode] by Image` Correct Answer

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

`172.16.0.121` Correct Answer

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?

Check

New Search

Source: `_source=WindowsEventLog`

Presets: `12,256 events (before 27/01/2026 12:26:03.000)`

Events (12,256) Patterns Statistics View

Format Timeline ▾ Date Range: 2, fill in required data

Between `04/15/2022 08:05:00.000` and `04/15/2022 08:06:00.000` Relative

Advanced 3 Apply

Task 4: Splunk Search 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: Review and Conclusion

- The screenshot shows a browser window with several tabs open. The main tab displays a Splunk search results page for the query "index=windowslogs | chart count(EventCode) by Image". The results show 134 events, with the top event being "EventCode: 134". A green box highlights the "Correct Answer" next to the event count. Below the results, a message asks if the user wants to "Copy to clipboard".

The sidebar on the left lists tasks:

 - Task 4: Splunk Search 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

Task 4 Splunk Search Processing Language Overview

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

A screenshot of the Splunk interface showing search results for the query "index=windowslogs AccountName !=SYSTEM". The search bar at the top contains the query. Below it, a histogram shows the distribution of AccountName values. A red arrow points from the search bar down to the histogram. On the left side, there is a sidebar with "SELECTED FIELDS" and "INTERESTING FIELDS" sections. A modal window titled "AccountName" is open, showing a table of values, count, and percentage. The table is highlighted with a red border.

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
NOT	field_A NOT value	Ignore the events from the result where field_A contain the specified value.
OR	field_A=value1 OR field_A=value2	Return all the events in which field_A contains either value1 or value2.
AND	field_A=value1 AND 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

A screenshot of the Splunk interface showing search results for the query "index=windowslogs AccountName !=SYSTEM AND AccountName=James". The search bar at the top contains the query. Below it, a histogram shows the distribution of AccountName values. A red arrow points from the search bar down to the histogram. On the left side, there is a sidebar with "SELECTED FIELDS" and "INTERESTING FIELDS" sections. A modal window titled "AccountName" is open, showing a table of values, count, and percentage. The table is highlighted with a red border.

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

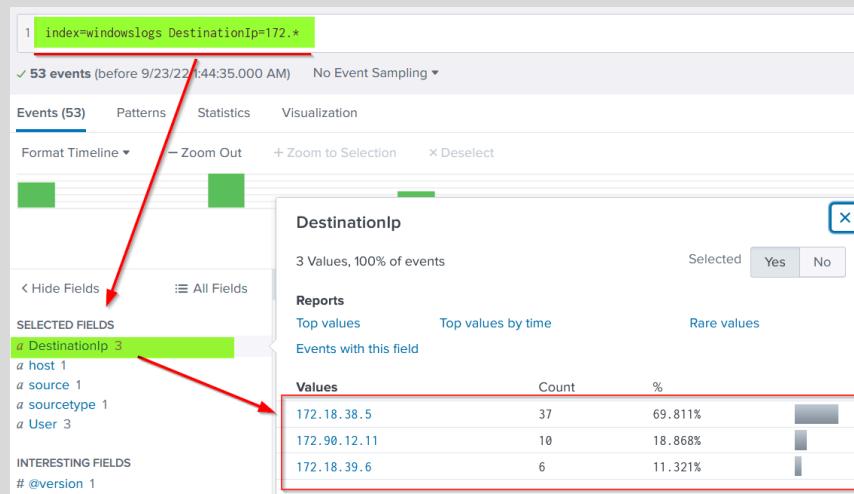
Wild Card

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.*



Answer the questions below

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

Answer: 4

In Time Frame: Select All times

In Search Box: Enter EventID="1" AND User="James"

The screenshot shows two windows side-by-side:

- Challenge Window:**
 - Shows a table of DestinationIp values (172.18.38.5, 172.90.12.11, 172.18.39.6) with counts (37, 10, 6) and percentages (69.811%, 18.868%, 11.321%).
 - A question asks: "How many Events are returned when searching for Event ID 1 AND User as *James*?" with a "Correct Answer" button.
 - Another question asks: "How many events are observed with Destination IP 172.18.39.6 AND destination Port 135?" with a "Check" button.
 - Other questions include: "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"', and "Now search for the term cyber*, how many events are returned?" with "Check" buttons.
- Splunk Search Results:**
 - Search Bar: EventID="1" AND User="James"
 - Results Summary: 4 events (before 2/7/2020 13:50:44.000) No Event Sampling
 - Event List: Shows four events with timestamp, source, and details.
 - Selected Fields: host, source, sourcetype, User.
 - Interesting Fields: @version.

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

Answer: 4

In Search Box: Enter **DestinationIP:172.18.39.6 AND DesitinationPort="135"**

Time	Event
08:06:23.000	Category: SYSTEM AccountType: user Category: Network connection detected (rule: NetworkConnect) Channel: Microsoft-Windows-SysmonOperational DestinationIp: 172.18.39.6 DestinationIsLocal: false DestinationPort: - DestinationPortName: - Domain: NT AUTHORITY EventCode: 401 EventReceiveTime: 2022-04-15 08:05:05 EventTime: 2022-04-15 08:05:03 EventType: INFO

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

Search Query: **index=windowslogs Hostname="Salena.Adam"**

DestinationIp="172.18.38.5"

Answer: 172.90.12.11

1. In Search Box: Enter **index=windowslogs Hostname="Salena.Adam"**
DestinationIp="172.18.38.5"

Time	Event
08:06:28.000	Category: SYSTEM AccountType: user Category: Network connection detected (rule: NetworkConnect) Channel: Microsoft-Windows-SysmonOperational DestinationIp: 172.18.38.5 DestinationIsLocal: false DestinationPort: 383 DestinationPortName: - Domain: NT AUTHORITY EventCode: 401 EventReceiveTime: 2022-04-15 08:05:29 EventTime: 2022-04-15 08:05:29 EventType: INFO

2. Click: SourceIP

Values	Count	%
172.90.12.11	17	41.4%
172.18.38.5	2	18.5%

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

Answer: 0

In Search Box: Enter **Index=windows.logs* cyber**

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

Answer: 12256

In Search Box: Enter **Index=windows.logs* cyber***

Task 5 Filtering the Results in SPL

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

Command	fields
Explanation	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.
Syntax	fields <field_name1> <field_name2>

Example

```
| 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

The screenshot shows the Splunk interface for a 'New Search'. The search bar contains the query: 'index=windowslogs | fields + host + User + SourceIp'. Below the search bar, it says '12,256 events (before 9/23/22 3:41:06.000 AM) No Event Sampling'. The 'Events (12,256)' tab is selected. A red arrow points from the 'Selected Fields' panel to the event table. The 'Selected Fields' panel lists: 'host 1', 'SourceIp 7', and 'User 4'. The event table shows a single event with the following details:

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

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



Search

Command	<code>search</code>
Explanation	This command is used to search for the raw text while using the chaining command <code> </code>
Syntax	<code> search <search_keyword></code>
Example	<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

Dedup

Command	<code>dedup</code>
Explanation	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.
Syntax	<code> dedup <fieldname></code>
Example	<code> dedup EventID</code>

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

Rename

Command	<code>rename</code>
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 <fieldname>
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 ▾

Selected Fields

- a Employees 4
- a host 1
- a Sourcelp 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\SYSTEM

Answer the questions below

1. What is the third EventID returned against this search query?

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

Answer: 4103

In Search Box: Enter

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

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

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

Check

Task 6: SPL - Structuring the Search Results

Task 7: Transformational Commands in SPL

Task 8: Recap and Conclusion

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now

Applications Places System Tue Jul 27 10:13 AttackBox IP:10.64.72.248

Search Analytics Databases Reports Alerts Dashboards Search & Reporting

New Search

index=windowslogs | table _time EventID Hostname SourceName | reverse

✓ 12,256 events (before 27/07/2025 19:05:00) No Event Sampling

Events (12,256) Patterns Statistics Visualization

i	EventID	Hostname	SourceName
2022-04-12 08:05:46	800	James.brown	PowerShell
2022-04-12 08:05:46	800	James.brown	PowerShell
2022-04-12 08:05:46	4103	James.brown	Microsoft-Windows-PowerShell
2022-04-12 08:05:46	800	James.brown	PowerShell
2022-04-12 08:05:46	4103	James.brown	Microsoft-Windows-PowerShell
2022-04-12 08:05:46	800	James.brown	PowerShell
2022-04-12 08:05:46	4103	James.brown	Microsoft-Windows-PowerShell
2022-04-12 08:05:46	800	James.brown	PowerShell
2022-04-12 08:05:46	10	Michael.Beaureve	Microsoft-Windows-System
2022-04-12 08:05:46	10	Michael.Beaureve	Microsoft-Windows-System
2022-04-12 08:05:46	10	Michael.Beaureve	Microsoft-Windows-System

2. 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?

Answer: Salena.Adam

In Search Box: Enter

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

The screenshot shows a search interface with the following details:

- Search Query:** index=windowslogs | table _time EventID Hostname SourceName | dedup Hostname | reverse
- Results:** A table view showing three events. The first event has "Salena.Adam" highlighted in yellow.

EventID	Hostname	SourceName
4103	Salena.Adam	Microsoft-Windows-Security-Auditing
5105	JAMES.BROWNE	Microsoft-Windows-Security-Auditing
10	Michael.Beauchamp	Microsoft-Windows-Security-Auditing

Task 6 Structuring the Search Results

SPL provides various commands to bring structure or order to the search results. These sorting commands like **head**, **tail**, and **sort** can be very useful during logs investigation. These ordering commands are explained below:

Table

Explanation	Each event has multiple fields, and not every field is important to display. The Table command allows us to create a table with selective fields as columns.
Syntax	table <field_name1> <fieldname_2>
Example	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

EventID	Hostname	SourceName
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
...

Head

Explanation

The **head** command returns the first 10 events if no number is specified.

Syntax

```
| head <number>
```

```
| head # will return the top 10 events from the result list
```

Example

```
| 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

_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 **Tail** command returns the last 10 events if no number is specified.

Syntax

```
| tail <number>
```

```
| tail # will return the last 10 events from the result list
```

Example

```
| 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`

_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

Explanation

The `Sort` command allows us to order the fields in ascending or descending order.

Syntax

```
| sort <field_name>
```

Example

```
| 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`

_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

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

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

The screenshot shows a Splunk search interface with the following search bar content:
`1 index=windowslogs | table _time EventID Hostname SourceName | reverse`

Below the search bar, it says "12,256 events (before 10/26/22 9:28:24.000 PM) No Event Sampling".

The results table has columns: _time, EventID, Hostname, and SourceName. The data is as follows:

_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	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	4103	James.browne	Microsoft-Windows-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	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell

Answer the questions below

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

Answer: James.browne

In Search Box: Enter

`index=windowslogs | table _time EventID Hostname SourceName`

The screenshot shows a Splunk search interface with the following search bar content:
`1 index=windowslogs | table _time EventID Hostname SourceName`

Below the search bar, it says "12,256 events (before 23/09/2016 15:46:000000) No Event Sampling".

The results table has columns: _time, EventID, Hostname, and SourceName. The data is as follows:

_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	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	4103	James.browne	Microsoft-Windows-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	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell

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

Answer: 4103

In Search Box: Enter

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

EventID	Hostname	SourceName
4097	James.brown	PowerShell
4098	James.brown	Microsoft-Windows-PowerShell
4099	James.brown	PowerShell
4100	James.brown	PowerShell
4101	James.brown	Microsoft-Windows-PowerShell
4102	James.brown	PowerShell
4103	James.brown	PowerShell
4104	James.brown	Microsoft-Windows-PowerShell
4105	James.brown	PowerShell
4106	James.brown	PowerShell
4107	James.brown	PowerShell
4108	James.brown	PowerShell
4109	James.brown	PowerShell

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

Answer: Microsoft-Windows-Directory-Services-SAM

In Search Box: Enter

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

EventID	Hostname	SourceName
4097	James.brown	PowerShell
4098	James.brown	Microsoft-Windows-PowerShell
4099	James.brown	PowerShell
4100	James.brown	PowerShell
4101	James.brown	Microsoft-Windows-PowerShell
4102	James.brown	PowerShell
4103	James.brown	PowerShell
4104	James.brown	PowerShell
4105	James.brown	PowerShell
4106	James.brown	PowerShell
4107	James.brown	PowerShell
4108	James.brown	PowerShell
4109	James.brown	Microsoft-Windows-Directory-Services-SAM

Task 7 Transformational Commands in SPL

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.

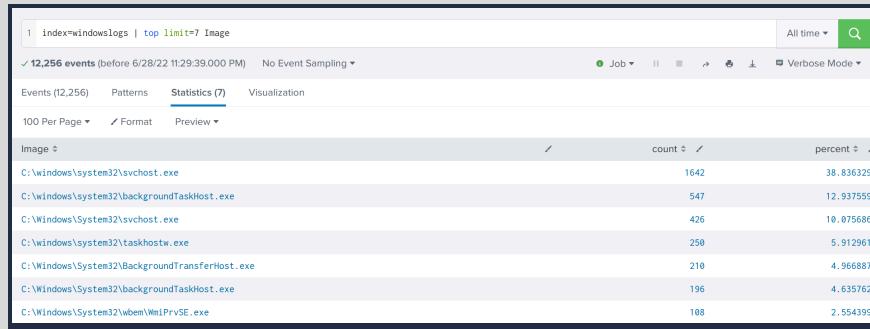
General Transformational Commands

Top

Command	<code>top</code>
Explanation	This command returns frequent values for the top 10 events.
Syntax	<code> top <field_name></code> <code> top limit=6 <field_name></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`

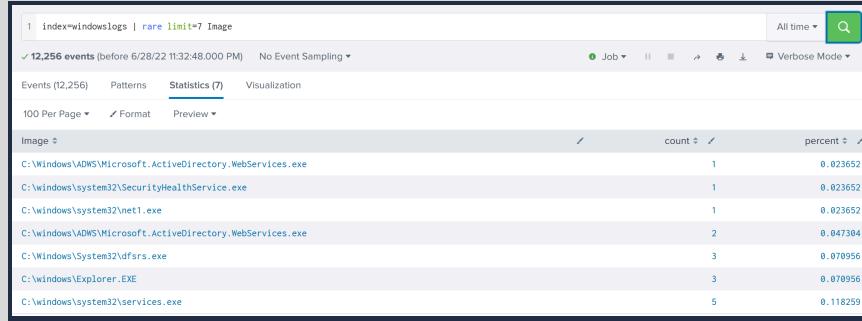


Rare

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

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

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



Highlight

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

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

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



STATS Commands

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

Command	Explanation	Syntax	Example
Average	This command is used to calculate the average of the given field.	stats avg(field_name)	stats avg(product_price)
Max	It will return the maximum value from the specific field.	stats max(field_name)	stats max(user_age)
Min	It will return the minimum value from the specific field.	stats min(field_name)	stats min(product_price)
Sum	It will return the sum of the fields in a specific value.	stats sum(field_name)	stats sum(product_cost)
Count	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

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

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



Timechart

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

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

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



Answer the questions below

1. List the top 8 Image processes using the `top` command - what is the total count of the 6th Image?
Answer: 196

In Search Box: `index="windows.logs" | top limit=8 Image`

Image	Count	Percent
C:\Windows\System32\svchost.exe	1642	38.83029
C:\Windows\System32\backgroundTaskHost.exe	547	12.33709
C:\Windows\System32\lsmHost.exe	426	10.47566
C:\Windows\System32\backgroundTaskHost.exe	258	5.31291
C:\Windows\System32\backgroundTaskHost.exe	218	4.36687
C:\Windows\System32\lsmHost.exe	188	4.03982
C:\Windows\System32\lsmHost.exe	148	2.55499
C:\Windows\System32\userworker.exe	95	2.24692

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

Answer: James

In Search Box: `index="windows.logs" | rare limit=8 User`

User	Count	Percent
James	5	4.39181
NT AUTHORITY\SYSTEM	20	16.98872
CyberTeekAlberto	24	20.14481
NT AUTHORITY\SYSTEM	30	58.42352

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

Answer: 70

1. In Search Box: `index="windows.logs" | chat count by Image`
2. Click: **Visualization**
3. Click: **C:\Windows\System32\conhost.exe**

Image	Count
conhost.exe	70
other 2%	2

The left window displays a challenge interface with several questions:

- List the top 8 image processes using the top command - what is the total count of the 6th image? (Answer: 196)
- Using the rare command, identify the user with the least number of activities (Answer: James)
- Create a pie-chart using the chart command - what is the count for the cohosh.exe process? (Answer: 70)

The right window shows a Splunk search results page for the query `index="windowslog" | top 70 events | sort -Time`. The results table includes columns for Time, Event, and other fields like EventID, SourceName, and Category. One visible row from the table is:

Time	Event
15/04/2022 08:08:52,000	EventID: 5 EventTime: 2022-04-15 08:08:51 EventType: 1 Hostname: James-braine Image: C:\Windows\System32\cmd.exe ProcessName: cmd.exe User: James Version: 1 AccountName: SYSTEM AccountType: User Category: Process terminated (rule: Processterminated) DisplayName: cmd.exe EventID: 5 EventTime: 2022-04-15 08:08:51 EventType: 1 Hostname: James-braine Image: C:\Windows\System32\cmd.exe ProcessName: cmd.exe User: James Version: 1 AccountName: SYSTEM AccountType: User Category: Process terminated (rule: Processterminated) DisplayName: cmd.exe

Task 8 Recap & Conclusion

This wraps up the [Splunk SPL room](#).

We have covered various functions and commands used together to form search queries to look for the data more effectively. To practice more, look at the following [Splunk rooms](#) and challenges.

- [Incident handling with Splunk](#)
- [Investigating with Splunk](#)
- [Benign](#)
- [PS Eclipse](#)

Answer the questions below

No answer needed