SPLUNK COMMANDS

abstract

Description: **Modify field values using a pattern or replacement.**

Example Input Query:

```
your_search_here
| abstract fieldname | table fieldname
```

Example Output:

```
| fieldname |
|---------------|
| value1    |
| value2    |
| value3    |
```

accum

Description: **Accumulate values over time or events.**

Example Input Query:

```
your_search_here | accum fieldname | table fieldname
```

Example Output:

```
| fieldname                |
|---------------------------|
| value1                   |
| value1, value2           |
| value1, value2, value3 |
```

addcoltotals

Description: **Add column-wise totals to search results.**

Example Input Query:

```
your_search_here | addcoltotals
```

Example Output:

```
| field1 | field2 | field3 |
|---------|---------|---------|
| value1 | value2 | value3 |
| value4 | value5 | value6 |
| Total  | Total  | Total  |
```

addinfo

Description: Append search information to each event.

Example Input Query:

```
your_search_here | addinfo | table _time, info
```

Example Output:

```
| _time              | info                     |
|--------------------|--------------------------|
| 2023-06-01 10:00:00 | search_id=ABC, user=john |
| 2023-06-01 11:00:00 | search_id=XYZ, user=mary |
```

addtotals

Description: Add total values for specific fields in search results.

Example Input Query:

```
your_search_here | addtotals field1 field2
```

Example Output:

```
| field1 | field2 |
|--------|--------|
| value1 | value2 |
| value3 | value4 |
| Total  | Total  |
```

appendcols

Description: Append fields from a subsearch to the main search results as new columns.

Example Input Query:

```
your_main_search_here | appendcols [your_subsearch_here]
```

Example Output:

```
| field1 | field2 | subfield1 | subfield2 |
|--------|--------|-----------|-----------|
| value1 | value2 | subvalue1 | subvalue2 |
| value3 | value4 | subvalue3 | subvalue4 |
```

appendpipe

Description: Append events from a subsearch to the main search results as new events.

Example Input Query:

```
your_main_search_here | appendpipe [your_subsearch_here]
```

Example Output:

```
| field1 | field2 |
|--------|--------|
| value1 | value2 |
| value3 | value4 |
| subvalue1 | subvalue2 |
| subvalue3 | subvalue4 |
```

arules

Description: Perform association rule analysis on your search results.

Example Input Query:

```
your_search_here
| arules [field1, field2] support=0.2 confidence=0.8
```

Example Output:

```
| antecedent     | consequent | support | confidence |
|----------------|------------|---------|------------|
| {value1}       | {value2}   | 0.5     | 0.9        |
| {value3}       | {value4}   | 0.3     | 0.7        |
```

associate

Description: Perform association analysis on your search results.

Example Input Query:

```
your_search_here | associate [field1, field2] support=0.2 confidence=0.8
```

Example Output:

```
| itemset        | support | confidence |
|----------------|---------|------------|
| {value1}       | 0.5     | 0.9        |
| {value2}       | 0.3     | 0.7        |
```

audit

Description: Generate an audit trail of search activities.

Example Input Query:

```
your_search_here | audit action="search" info="Performed search activity."
```

Example Output:

```
Audit log entry created.
```

autoregress

Description: Create a time-series prediction using autoregressive modeling.

Example Input Query:

```
your_search_here | autoregress fieldname lag=3 predict=5
```

Example Output:

```
| _time               | fieldname | predicted_fieldname |
|---------------------|-----------|---------------------|
| 2023-06-01 10:00:00 | value1    | prediction1         |
| 2023-06-01 11:00:00 | value2    | prediction2         |
```

bin (bucket)

Description: Group numerical values into specified ranges or buckets.

Example Input Query:

```
your_search_here
| bin fieldname span=10
```

Example Output:

```
| fieldname |
|-----------|
| 0-9       |
| 10-19     |
| 20-29     |
```

bucketdir

Description: Manage the Splunk bucket directory.

Example Input Query:

```
bucketdir [-sub] [options]
```

Example Output:

```
Bucket directory management results.
```

chart

Description: Create visualizations such as line charts, bar charts, and pie charts.

Example Input Query:

```
your_search_here
| chart count by fieldname
```

Example Output:

```
| fieldname | count |
|-----------|-------|
| value1    | 10    |
| value2    | 20    |
| value3    | 15    |
```

cluster

Description: Group events based on common attributes using machine learning clustering algorithms.

Example Input Query:

```
your_search_here
| cluster fieldname
```

Example Output:

```
| fieldname | cluster |
|-----------|---------|
| value1    | 1       |
| value2    | 2       |
| value3    | 1       |
```

cofilter

Description: Combine search results using boolean logic.

Example Input Query:

```
your_search_here
| cofilter condition1 [AND|OR] condition2
```

Example Output:

Combined search results.

collect

Description: **Accumulate events into a single event with multivalue fields.**

Example Input Query:

```
your_search_here
| collect fieldname
```

Example Output:

```
| fieldname |
|-----------|
| value1    |
| value2    |
| value3    |
```

concurrency

Description: **Limit the number of concurrent searches.**

Example Input Query:

```
your_search_here
| concurrency max=5
```

Example Output:

```
Search results limited to maximum concurrency.
```

contingency

Description: **Compute a contingency table to analyze associations between fields.**

Example Input Query:

```
your_search_here
| contingency field1 field2
```

Example Output:

```
|           | field2_1 | field2_2 |
|-----------|----------|----------|
| field1_1  | 10       | 5        |
| field1_2  | 3        | 8        |
```

convert

Description: Convert fields into different formats or data types.

Example Input Query:

```
your_search_here
| convert fieldname=strftime(_time, "%Y-%m-%d")
```

Example Output:

```
| fieldname    |
|--------------|
| 2023-06-01   |
| 2023-06-02   |
| 2023-06-03   |
```

correlate

Description: Correlate events in one search with events in another search.

Example Input Query:

```
your_search1_here
| correlate your_search2_here
```

Example Output:

Correlated search results.

datamodel

Description: Access and work with data models in Splunk.

Example Input Query:

```
datamodel your_datamodel_name [your_search_here]
```

Example Output:

Data model search results.

dbinspect

Description: Inspect a database connection to retrieve table and column information.

Example Input Query:

```
| dbinspect your_database_connection_name
```

Example Output:

```
| table_name | column_name |
|------------|-------------|
| table1     | column1     |
| table1     | column2     |
| table2     | column1     |
```

dedup

Description: **Remove duplicate events based on specified fields.**

Example Input Query:

```
your_search_here
| dedup fieldname
```

Example Output:

Deduplicated search results.

delete

Description: **Delete events from the index.**

Example Input Query:

```
delete [your_search_here]
```

Example Output:

Events deleted.

delta

Description: **Compute the difference between consecutive numeric field values.**

Example Input Query:

```
your_search_here
| delta fieldname as difference
```

Example Output:

```
| fieldname | difference |
|-----------|------------|
| 10        |            |
| 15        | 5          |
| 20        | 5          |
```

diff

Description: **Compare two search results and return the differences.**

Example Input Query:

```
your_search1_here
| diff your_search2_here
```

Example Output:

Differences between search results.

erex

Description: **Extract fields using regular expressions.**

Example Input Query:

```
your_search_here
| erex fieldname=regex
```

Example Output:

```
| fieldname |
|-----------|
| value1    |
| value2    |
| value3    |
```

eval

Description: **Create new calculated fields or modify existing fields.**

Example Input Query:

```
your_search_here
| eval new_fieldname = expression
```

Example Output:

```
| new_fieldname |
|---------------|
| value1        |
| value2        |
| value3        |
```

eventcount

Description: **Count the number of events in the search results.**

Example Input Query:

```
your_search_here
| eventcount
```

Example Output:

```
| count |
|-------|
| 100   |
```

eventstats

Description: **Calculate statistics on numeric fields in the search results.**

Example Input Query:

```
your_search_here
| eventstats sum(fieldname) as total
```

Example Output:

```
| total |
|-------|
| 500   |
```

extract (kv)

Description: **Extract key-value pairs from events using regular expressions.**

Example Input Query:

```
your_search_here
| extract kvdelim="=" fieldname
```

Example Output:

```
| fieldname1 | fieldname2 |
|------------|------------|
| value1     | value2     |
| value3     | value4     |
```

fieldformat

Description: **Modify the format of fields.**

Example Input Query:

```
your_search_here
| fieldformat fieldname1=lower(fieldname1)
```

Example Output:

Modified search results.

fields

Description: **Restrict the search to specific fields.**

Example Input Query:

```
your_search_here | fields fieldname1, fieldname2
```

Example Output:

```
| fieldname1 | fieldname2 |
|------------|------------|
| value1     | value2     |
| value3     | value4     |
```

fieldsummary

Description: **Summarize field values and calculate statistics.**

Example Input Query:

```
your_search_here
| fieldsummary fieldname
```

Example Output:

```
| fieldname | count | distinct_count | min   | max   | avg   |
|-----------|-------|----------------|-------|-------|-------|
| value1    | 100   | 10             | 1     | 50    | 25.5  |
| value2    | 100   | 5              | A     | E     | -     |
```

filldown

Description: **Fill empty field values with the previous non-empty value.**

Example Input Query:

```
your_search_here
| filldown fieldname
```

Example Output:

Filled search results.

fillnull

Description: **Replace null or empty field values with specified values.**

Example Input Query:

```
your_search_here
| fillnull value="N/A" fieldname
```

Example Output:

```
| fieldname |
|-----------|
| value1    |
| N/A       |
| value2    |
```

findtypes

Description: Identify the data types of fields in the search results.

Example Input Query:

```
your_search_here
| findtypes
```

Example Output:

```
| fieldname1 | type    |
|------------|---------|
| value1     | number  |
| value2     | string  |
```

folderize

Description: Organize search results into hierarchical structures.

Example Input Query:

```
your_search_here
| folderize fieldname1, fieldname2
```

Example Output:

Folderized search results.

foreach

Description: Apply a subsearch to each value of a field.

Example Input Query:

```
your_search_here
| foreach fieldname [your_subsearch_here]
```

Example Output:

Modified search results.

format

Description: Apply formatting to field values.

Example Input Query:

```
your_search_here
| format fieldname "%Y-%m-%d"
```

Example Output:

Formatted search results.

from

Description: **Specify the data source or index to search.**

Example Input Query:

```
from your_data_source_or_index
| your_search_here
```

Example Output:

Search results from the specified data source or index.

gauge

Description: **Create a gauge visualization.**

Example Input Query:

```
your_search_here
| stats count by fieldname
| gauge fieldname
```

Example Output:

Gauge visualization.

gentimes

Description: **Generate a series of events with specific timestamps.**

Example Input Query:

```
gentimes start=-1d/d end=now() increment=1h
```

Example Output:

Generated events with timestamps.

geom

Description: **Create geospatial visualizations.**

Example Input Query:

```
your_search_here
| geom fieldname
```

Example Output:

Geospatial visualization.

geomfilter

Description: Apply filters to geospatial data.

Example Input Query:

```
your_search_here
| geom fieldname
| geomfilter condition
```

Example Output:

Filtered geospatial visualization.

eventcount

Description: Count the number of events in the search results.

Example Input Query:

```
your_search_here
| eventcount
```

Example Output:

```
| count |
|-------|
| 100   |
```

eventstats

Description: Calculate statistics on numeric fields in the search results.

Example Input Query:

```
your_search_here
| eventstats sum(fieldname) as total
```

Example Output:

```
| total |
|-------|
| 500   |
```

extract (kv)

Description: Extract key-value pairs from events using regular expressions.

Example Input Query:

```
your_search_here | extract kvdelim="=" fieldname
```

Example Output:

```
| fieldname1 | fieldname2 |
|------------|------------|
| value1     | value2     |
| value3     | value4     |
```

fieldformat

Description: Modify the format of fields.

Example Input Query:

```
your_search_here
| fieldformat fieldname1=lower(fieldname1)
```

Example Output:

```
Modified search results.
```

fields

Description: Restrict the search to specific fields.

Example Input Query:

```
your_search_here
| fields fieldname1, fieldname2
```

Example Output:

```
| fieldname1 | fieldname2 |
|------------|------------|
| value1     | value2     |
| value3     | value4     |
```

fieldsummary

Description: Summarize field values and calculate statistics.

Example Input Query:

```
your_search_here
| fieldsummary fieldname
```

Example Output:

```
| fieldname | count | distinct_count | min   | max   | avg   |
|-----------|-------|----------------|-------|-------|-------|
| value1    | 100   | 10             | 1     | 50    | 25.5  |
| value2    | 100   | 5              | A     | E     | -     |
```

filldown

Description: **Fill empty field values with the previous non-empty value.**

Example Input Query:

```
your_search_here
| filldown fieldname
```

Example Output:

Filled search results.

fillnull

Description: **Replace null or empty field values with specified values.**

Example Input Query:

```
your_search_here
| fillnull value="N/A" fieldname
```

Example Output:

```
| fieldname |
|-----------|
| value1    |
| N/A       |
| value2    |
```

findtypes

Description: **Identify the data types of fields in the search results.**

Example Input Query:

```
your_search_here
| findtypes
```

Example Output:

```
| fieldname1 | type    |
|------------|---------|
| value1     | number  |
| value2     | string  |
```

folderize

Description: **Organize search results into hierarchical structures.**

Example Input Query:

```
your_search_here
| folderize fieldname1, fieldname2
```

Example Output:

Folderized search results.

foreach

Description: **Apply a subsearch to each value of a field.**

Example Input Query:

```
your_search_here
| foreach fieldname [your_subsearch_here]
```

Example Output:

Modified search results.

format

Description: **Apply formatting to field values.**

Example Input Query:

```
your_search_here
| format fieldname1 "%Y-%m-%d"
```

Example Output:

Formatted search results.

from

Description: **Specify the data source or index to search.**

Example Input Query:

```
from your_data_source_or_index | your_search_here
```

Example Output:

Search results from the specified data source or index.

gauge

Description: **Create a gauge visualization.**

Example Input Query:

```
your_search_here
| stats count by fieldname
| gauge fieldname
```

Example Output:

Gauge visualization.

gentimes

Description: Generate a series of events with specific timestamps.

Example Input Query:

```
gentimes start=-1d/d end=now() increment=1h
```

Example Output:

Generated events with timestamps.

geom

Description: Create geospatial visualizations.

Example Input Query:

```
your_search_here
| geom fieldname
```

Example Output:

Geospatial visualization.

geomfilter

Description: Apply filters to geospatial data.

Example Input Query:

```
your_search_here
| geom fieldname
| geomfilter condition
```

Example Output:

Filtered geospatial visualization.

geostats

Description: Generate geospatial statistics and visualizations.

Example Input Query:

```
your_search_here
| geostats latfield=latitude longfield=longitude count by fieldname
```

Example Output:

Geospatial statistics and visualization.

head

Description: Display the first few events from the search results.

Example Input Query:

```
your_search_here
| head 10
```

Example Output:

First 10 events from the search results.

highlight

Description: Apply syntax highlighting to search results.

Example Input Query:

```
your_search_here
| highlight fieldname
```

Example Output:

Highlighted search results.

history

Description: Display the search history for the current user.

Example Input Query:

```
| history
```

Example Output:

Search history for the current user.

iconify

Description: Create icon-based visualizations.

Example Input Query:

```
your_search_here
| iconify fieldname
```

Example Output:

Icon-based visualization.

inputcsv

Description: Read and process CSV files.

Example Input Query:

```
| inputcsv your_csv_file.csv
```

Example Output:

Processed CSV file data.

inputlookup

Description: Perform lookups on external lookup tables.

Example Input Query:

```
your_search_here
| inputlookup your_lookup_table
```

Example Output:

Looked up values from the external lookup table.

iplocation

Description: Perform IP geolocation lookup.

Example Input Query:

```
your_search_here
| iplocation fieldname
```

Example Output:

IP geolocation information.

join

Description: Combine results from multiple searches based on common fields.

Example Input Query:

```
search 1
| join common_field [search 2]
```

Example Output:

Combined results based on the common field.

kmeans

Description: Perform k-means clustering analysis on numeric fields.

Example Input Query:

```
your_search_here
| kmeans fieldname1 fieldname2 k=3
```

Example Output:

K-means clustering analysis results.

kvform

Description: Transform key-value pairs into a tabular format.

Example Input Query:

```
your_search_here
| kvform input=fieldname
```

Example Output:

Tabular format of key-value pairs.

loadjob

Description: Load search results from a saved search or a job.

Example Input Query:

```
| loadjob savedsearch_or_job_id
```

Example Output:

Loaded search results from the saved search or job.

localize

Description: Localize field values using translation files.

Example Input Query:

```
your_search_here
| localize fieldname
```

Example Output:

Localized field values.

localop

Description: Perform arithmetic or logical operations on fields.

Example Input Query:

```
your_search_here
| localop fieldname1 + fieldname2 as sum
```

Example Output:

Search results with the local operation applied.

lookup

Description: Perform lookups on external lookup tables.

Example Input Query:

```
your_search_here
| lookup lookup_table_name field_to_match OUTPUT new_field
```

Example Output:

Looked up values from the external lookup table.

makecontinuous

Description: Convert discrete time series data into continuous time series data.

Example Input Query:

```
your_search_here
| makecontinuous fieldname span=1d
```

Example Output:

Continuous time series data.

makemv

Description: Convert field values into multi-value fields.

Example Input Query:

```
your_search_here
| makemv fieldname1 fieldname2
```

Example Output:

Search results with multi-value fields.

makeresults

Description: Generate synthetic search results.

Example Input Query:

```
| makeresults count=10
```

Example Output:

Generated synthetic search results.

map

Description: Apply a subsearch to each value of a field.

Example Input Query:

```
your_search_here
| map [your_subsearch_here]
```

Example Output:

Modified search results.

mcollect

Description: Collect events from remote indexers.

Example Input Query:

```
|mcollect index=your_index
```

Example Output:

Collected events from remote indexers.

metadata

Description: Retrieve metadata information about fields and event types.

Example Input Query:

```
your_search_here
| metadata fieldname
```

Example Output:

Metadata information about the specified field.

metasearch

Description: Perform a parallel search across multiple indexes or hosts.

Example Input Query:

```
metasearch index=your_index search="your_search_query"
```

Example Output:

Search results from multiple indexes or hosts.

meventcollect

Description: Collect events from remote peers.

Example Input Query:

```
| meventcollect index=your_index
```

Example Output:

Collected events from remote peers.

mpreview

Description: Preview search results from multiple searches.

Example Input Query:

```
| multisearch [your_search1] [your_search2]
| mpreview
```

Example Output:

Preview of search results from multiple searches.

msearch

Description: Perform multiple searches concurrently.

Example Input Query:

```
| msearch [your_search1] [your_search2]
```

Example Output:

Search results from multiple concurrent searches.

mstats

Description: Perform statistical operations on multiple fields.

Example Input Query:

```
your_search_here
| mstats sum(fieldname1) as total1, avg(fieldname2) as average2 by fieldname3
```

Example Output:

Statistical operations on multiple fields.

multikv

Description: **Extract key-value pairs from events with multiple fields.**

Example Input Query:

```
your_search_here
| multikv fields fieldname1, fieldname2
```

Example Output:

Extracted key-value pairs from events with multiple fields.

multisearch

Description: **Perform multiple searches and combine the results.**

Example Input Query:

```
| multisearch [your_search1] [your_search2]
```

Example Output:

Combined search results from multiple searches.

mvcombine

Description: **Combine multi-value fields into a single field.**

Example Input Query:

```
your_search_here
| mvcombine fieldname1 fieldname2 separator=","
```

Example Output:

Combined multi-value fields into a single field.

mvexpand

Description: **Expand multi-value fields into separate events.**

Example Input Query:

```
your_search_here
| mvexpand fieldname
```

Example Output:

Expanded multi-value fields into separate events.

nomv

Description: Convert multi-value fields into separate fields.

Example Input Query:

```
your_search_here
| nomv fieldname
```

Example Output:

Search results with multi-value fields converted into separate fields.

outlier

Description: Identify outliers in statistical data.

Example Input Query:

```
your_search_here
| outlier fieldname
```

Example Output:

Identified outliers in the statistical data.

outputcsv

Description: Save search results to a CSV file.

Example Input Query:

```
your_search_here
| outputcsv output_file.csv
```

Example Output:

Search results saved to a CSV file.

outputlookup

Description: Save search results to an external lookup table.

Example Input Query:

```
your_search_here
| outputlookup lookup_table_name
```

Example Output:

Search results saved to the external lookup table.

outputtext

Description: Save search results to a text file.

Example Input Query:

```
your_search_here
| outputtext output_file.txt
```

Example Output:

Search results saved to a text file.

overlap

Description: Identify overlapping events based on timestamp fields.

Example Input Query:

```
your_search_here
| overlap fieldname
```

Example Output:

Identified overlapping events based on the specified timestamp field.

pivot

Description: Generate pivot tables to summarize and visualize data.

Example Input Query:

```
your_search_here
| pivot your_pivot_configuration
```

Example Output:

Pivot table summarizing and visualizing the data.

predict

Description: Perform predictive modeling and forecasting.

Example Input Query:

```
your_search_here
| predict fieldname
```

Example Output:

Predictive modeling and forecasting results.

rangemap

Description: Map numeric ranges to labels or categories.

Example Input Query:

```
your_search_here
| rangemap fieldname range1=category1 range2=category2
```

Example Output:

Mapped numeric ranges to labels or categories.

rare

Description: Identify rare or infrequent events.

Example Input Query:

```
your_search_here
| rare fieldname
```

Example Output:

Identified rare or infrequent events based on the specified field.

redistribute

Description: Redistribute events across indexers for load balancing.

Example Input Query:

```
your_search_here
| redistribute
```

Example Output:

Redistributed events across indexers for load balancing.

regex

Description: Perform regular expression matching and extraction.

Example Input Query:

```
your_search_here
| regex fieldname "regular_expression"
```

Example Output:

Results of regular expression matching and extraction.

reltime

Description: Convert relative time expressions into absolute time values.

Example Input Query:

your_search_here
| reltime fieldname

Example Output:

Converted relative time expressions into absolute time values.

rename

Description: Rename fields in the search results.

Example Input Query:

your_search_here
| rename old_fieldname as new_fieldname

Example Output:

Search results with renamed fields.

replace

Description: Replace field values with specified values.

Example Input Query:

your_search_here
| replace fieldname value_to_replace_with

Example Output:

Field values replaced with the specified values.

require

Description: Specify search requirements for the following s.

Example Input Query:

your_search_here
| require fieldname1=value1 fieldname2=value2

Example Output:

Search results that meet the specified requirements.

rest

Description: **Interact with Splunk's REST API.**

Example Input Query:

```
| rest /endpoint_name
```

Example Output:

Results retrieved from the specified REST API endpoint.

return

Description: **Terminate a subsearch and return the results.**

Example Input Query:

```
your_search_here
| return fieldname
```

Example Output:

Results returned from the terminated subsearch.

reverse

Description: **Reverse the order of events.**

Example Input Query:

```
your_search_here
| reverse
```

Example Output:

Search results with the order of events

rex

Description: **Extract fields using regular expressions.**

Example Input Query:

```
your_search_here
| rex field=fieldname "regular_expression"
```

Example Output:

Extracted fields using regular expressions.

rtorder

Description: Reorder events based on specified fields.

Example Input Query:

```
your_search_here
| rtorder fieldname1 fieldname2
```

Example Output:

Reordered events based on the specified fields.

savedsearch

Description: Run a saved search within a search pipeline.

Example Input Query:

```
| savedsearch "your_saved_search_name"
```

Example Output:

Results from running the saved search within the pipeline.

script (run)

Description: Execute an external script or .

Example Input Query:

```
your_search_here
| script "your_script.sh"
```

Example Output:

Results generated by executing the external script or .

scrub

Description: Remove sensitive data from search results.

Example Input Query:

```
your_search_here
| scrub fieldname
```

Example Output:

Search results with sensitive data removed from the specified field.

search

Description: Perform a new search within the current search.

Example Input Query:

```
your_search_here
| search "your_subsearch_query"
```

Example Output:

Results from the new search performed within the current search.

searchtxn

Description: Group events into transactions based on specified criteria.

Example Input Query:

```
your_search_here
| searchtxn startswith="criteria1" endswith="criteria2"
```

Example Output:

Events grouped into transactions based on the specified criteria.

selfjoin

Description: Join events based on common fields within the same search.

Example Input Query:

```
your_search_here
| selfjoin fieldname
```

Example Output:

Joined events based on the common field within the same search.

sendemail

Description: Send search results via email.

Example Input Query:

```
your_search_here
| sendemail to="recipient@example.com" subject="Your Subject" message="Your Message"
```

Example Output:

Search results sent via email.

set

Description: Set field values or create new fields.

Example Input Query:

```
your_search_here
| set fieldname1=value1 fieldname2=value2
```

Example Output:

Field values set or new fields created.

setfields

Description: Set field values or create new fields.

Example Input Query:

```
your_search_here
| setfields fieldname1=value1 fieldname2=value2
```

Example Output:

Field values set or new fields created.

sichart

Description: Generate statistical charts and visualizations.

Example Input Query:

```
your_search_here
| sichart chart_type fieldname
```

Example Output:

Statistical chart or visualization based on the specified field.

sirare

Description: Identify rare or infrequent events within a specified time range.

Example Input Query:

```
your_search_here
| sirare fieldname time_range
```

Example Output:

Identified rare or infrequent events within the specified time range.

sistats

Description: **Generate statistical summaries and calculations.**

Example Input Query:

```
your_search_here
| sistats count(fieldname) as total, avg(fieldname) as average by fieldname2
```

Example Output:

Statistical summaries and calculations based on the specified fields.

sitimechart

Description: **Generate time-based statistical charts and visualizations.**

Example Input Query:

```
your_search_here
| sitimechart chart_type fieldname
```

Example Output:

Time-based statistical chart or visualization based on the specified field.

sitop

Description: **Generate a ranked list of values for a specified field.**

Example Input Query:

```
your_search_here
| sitop fieldname
```

Example Output:

Ranked list of values for the specified field.

sort

Description: **Sort search results based on specified fields.**

Example Input Query:

```
your_search_here
| sort fieldname1 fieldname2
```

Example Output:

Search results sorted based on the specified fields.

spath

Description: Extract fields using the Splunk-specific path syntax.

Example Input Query:

```
your_search_here
| spath input=fieldname output=new_fieldname path_expression
```

Example Output:

Extracted fields using the Splunk-specific path syntax.

stats

Description: Perform statistical calculations and aggregations.

Example Input Query:

```
your_search_here
| stats count(fieldname) as total, avg(fieldname) as average by fieldname2
```

Example Output:

Statistical calculations and aggregations based on the specified fields.

strcat

Description: Concatenate multiple fields into a single field.

Example Input Query:

```
your_search_here
| strcat fieldname1 fieldname2 as new_fieldname
```

Example Output:

Concatenated multiple fields into a single field.

streamstats

Description: Perform rolling calculations and statistics on search results.

Example Input Query:

```
your_search_here
| streamstats sum(fieldname1) as total1, avg(fieldname2) as average2 by fieldname3
```

Example Output:

Rolling calculations and statistics based on the specified fields.

table

Description: Display search results in tabular format.

Example Input Query:

```
your_search_here
| table fieldname1, fieldname2
```

Example Output:

Search results displayed in tabular format with the specified fields.

tags

Description: Add tags to events based on specified criteria.

Example Input Query:

```
your_search_here
| tags fieldname criteria
```

Example Output:

Events tagged based on the specified criteria.

tail

Description: Display the most recent events in search results.

Example Input Query:

```
your_search_here
| tail 10
```

Example Output:

The 10 most recent events in the search results.

timechart

Description: Generate time-based charts and visualizations.

Example Input Query:

```
your_search_here
| timechart chart_type(fieldname)
```

Example Output:

Time-based chart or visualization based on the specified field.

timewrap

Description: Wrap time series data into specified time intervals.

Example Input Query:

```
your_search_here
| timewrap time_interval
```

Example Output:

Time series data wrapped into the specified time intervals.

tojson

Description: Convert search results to JSON format.

Example Input Query:

```
your_search_here
| tojson
```

Example Output:

Search results converted to JSON format.

top

Description: Generate a ranked list of values for a specified field.

Example Input Query:

```
your_search_here
| top fieldname
```

Example Output:

Ranked list of values for the specified field.

transaction

Description: Group events into transactions based on specified criteria.

Example Input Query:

```
your_search_here
| transaction startswith="criteria1" endswith="criteria2"
```

Example Output:

Events grouped into transactions based on the specified criteria.

transpose

Description: **Transpose rows and columns in search results.**

Example Input Query:

```
your_search_here
| transpose
```

Example Output:

Transposed rows and columns in the search results.

trendline

Description: **Add trendlines to time-based charts and visualizations.**

Example Input Query:

```
your_search_here
| trendline fieldname
```

Example Output:

Time-based chart or visualization with trendlines based on the specified field.

tscollect

Description: **Collect and analyze time series data.**

Example Input Query:

```
your_search_here
| tscollect fieldname1 fieldname2 by fieldname3
```

Example Output:

Collected and analyzed time series data based on the specified fields.

tstats

Description: **Perform statistical calculations and aggregations on time series data.**

Example Input Query:

```
your_search_here
| tstats count(fieldname) as total, avg(fieldname) as average by fieldname2
```

Example Output:

Statistical calculations and aggregations on time series data based on the specified fields.

typeahead

Description: Provide typeahead suggestions for field values.

Example Input Query:

```
your_search_here
| typeahead fieldname
```

Example Output:

Typeahead suggestions for field values based on the specified field.

typelearner

Description: Learn and predict field types in search results.

Example Input Query:

```
your_search_here
| typelearner fieldname
```

Example Output:

Learned and predicted field types in the search results.

typer

Description: Explicitly specify field types in search results.

Example Input Query:

```
your_search_here
| typer fieldname as type
```

Example Output:

Explicitly specified field types in the search results.

union

Description: Combine multiple search result sets into a single result set.

Example Input Query:

```
your_search_here
| union [ your_search1_here | table fieldname1 ], [ your_search2_here | table fieldname2 ]
```

Example Output:

Combined search result sets into a single result set.

uniq

Description: Remove duplicate events from search results.

Example Input Query:

```
your_search_here
| uniq fieldname
```

Example Output:

Search results with duplicate events removed based on the specified field.

untable

Description: Convert multivalue fields into separate events.

Example Input Query:

```
your_search_here
| untable fieldname
```

Example Output:

Multivalue fields converted into separate events based on the specified field.

walklex

Description: Extract lexicons from search results.

Example Input Query:

```
your_search_here
| walklex fieldname
```

Example Output:

Extracted lexicons from the search results.

where

Description: Filter events based on specified criteria.

Example Input Query:

```
your_search_here
| where condition
```

Example Output:

Filtered events based on the specified criteria.

x11

Description: Apply seasonal decomposition using the X-11 method to time series data.

Example Input Query:

your_search_here
| x11 fieldname

Example Output:

Time series data decomposed using the X-11 method.

xmlkv

Description: Extract key-value pairs from XML data.

Example Input Query:

your_search_here
| xmlkv fieldname

Example Output:

Key-value pairs extracted from the XML data.

xmlunescape

Description: Unescape XML-encoded values.

Example Input Query:

your_search_here
| xmlunescape fieldname

Example Output:

Unescaped XML-encoded values in the specified field.

xpath

Description: Extract data using XPath expressions from XML data.

Example Input Query:

your_search_here
| xpath fieldname xpath_expression

Example Output:

Data extracted from XML using the specified XPath expression.

xyseries

Description: Create a time series from x and y values.

Example Input Query:

```
your_search_here
| xyseries xfield=yfield
```

Example Output:

Time series created from the specified x and y values.