PER SCHOLAS

Lesson 200.3 Using Fields in Searches

Learning Objectives

At the end of this lesson, learners will be able to:

- Explain fields.
- Use the fields sidebar.
- Use fields in searches.
    - Preview the Table command.

PER SCHOLAS

Introduction

Fields are searchable **name/value** pairings in event data. All fields have names and can be searched using those names.

Searches with field expressions are more **precise** (and therefore more **efficient**) than searches using only keywords and quoted phrases.

In this lesson, we will take a **deeper look** at Splunk fields, and how to use them.

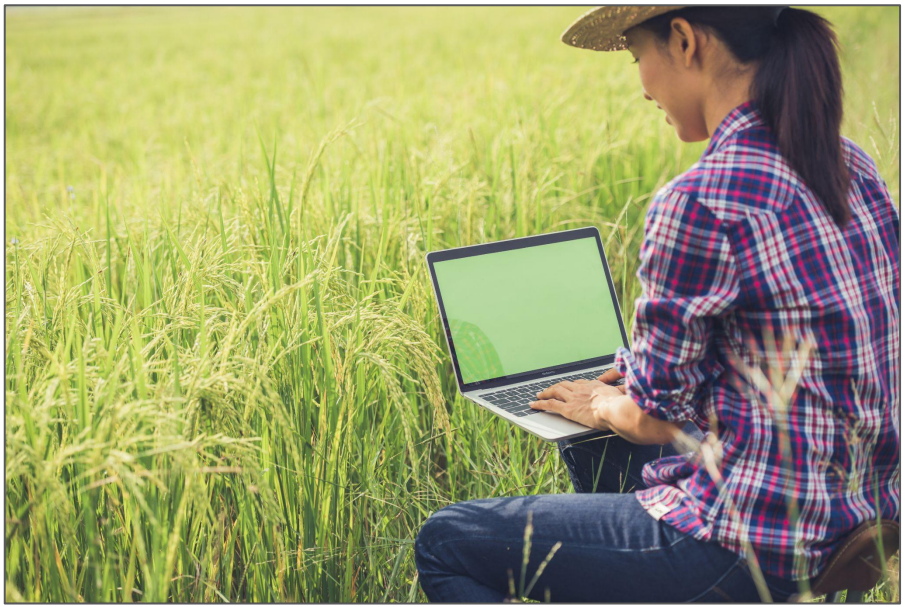


image: Freepik.com

PER SCHOLAS

3.1 Explain Fields

- **Fields** are knowledge objects that represent **searchable key/value pairs** in the event data. e.g. **host=www2 and status=200**
- Fields can be **extracted** at various times by Splunk based on the data source and its format, or they can be created and defined by the **user**.
- **Event fields** are extracted from the **raw data**, while **internal fields** are added by Splunk to track **metadata** and statistical information about the event, such as the **source**, **sourcetype**, **host**, and **timestamp**.

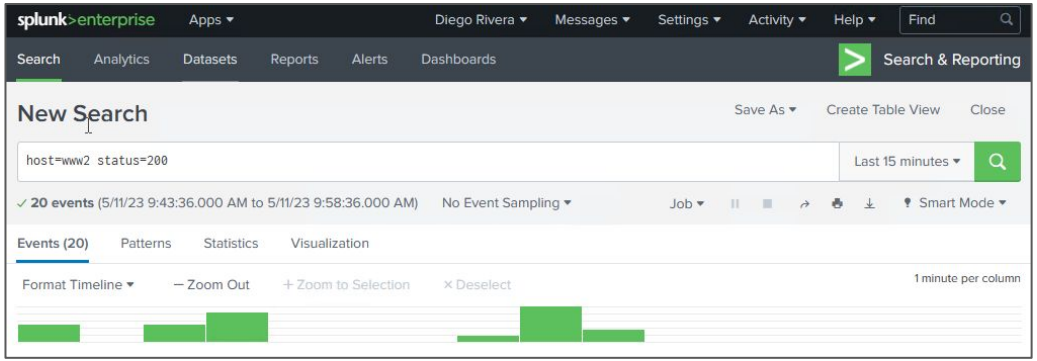
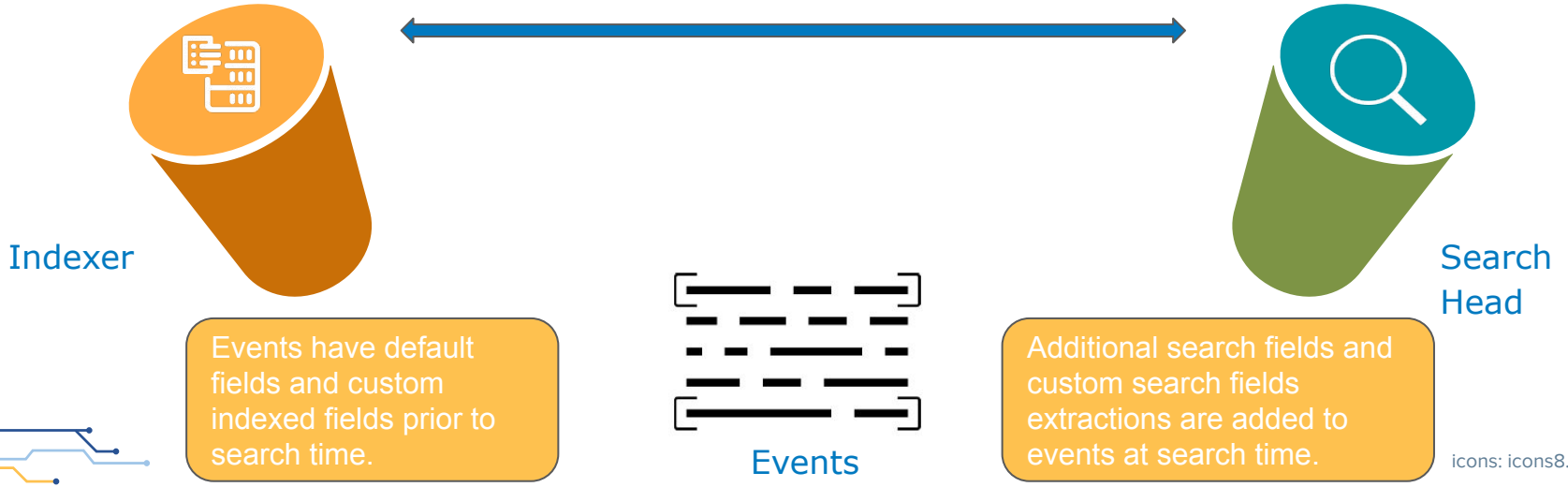


image: screenshot, splunk Search & Reporting app

3.1 Explain Fields (continued)

- Fields can be categorized into two main types: **indexed** fields and **search-time** fields.
- **Indexed fields** are **extracted at index time** and stored in Splunk's index, while **search-time fields** are extracted at **search time** using search commands and regular expressions.



3.1 Explain Fields (continued)

Index time

At index time, Splunk automatically creates several **default fields** for each event. Some of these fields are:

- **host**: Indicates the hostname or IP address of the machine where the event originated.
- **source**: Specifies the input source or file from which the event was read.
- **sourcetype**: Identifies the type or format of the data source, such as a log file or network data.
- **index**: Represents the index in which the event is stored.

Other **basic default fields** are: linecount, punct,splunk_server, and timestamp.

Users can define **custom indexed fields** by configuring field extractions in Splunk.

Indexer

3.1 Explain Fields (continued)

Search time

- At search time, Splunk automatically looks for **key=value** patterns and **extracts** them into **field-value** pairs for events associated with a specific **host**, **source**, or **sourcetype**.
- Data-specific fields come from **specific attributes** of your data.
  - Sometimes this is indicated by obvious **key=value** pairs (**action=purchase**). Other times, it is based on a sequence of characters that are recognized by the **sourcetype** (e.g., **access_combined** interprets **203.45.206.135** as **clientip=203.45.206.135)**

Search Head

image: screenshot, splunk Search & Reporting app

icons: icons8.com

3.1 Explain Fields (continued)

Search time

The **search mode** determines the **fields returned** at search time. Splunk user interface provides **three** (3) search modes.

Search modes determine how much **field data is returned** as search results, and affects how **fast** the search compleates.

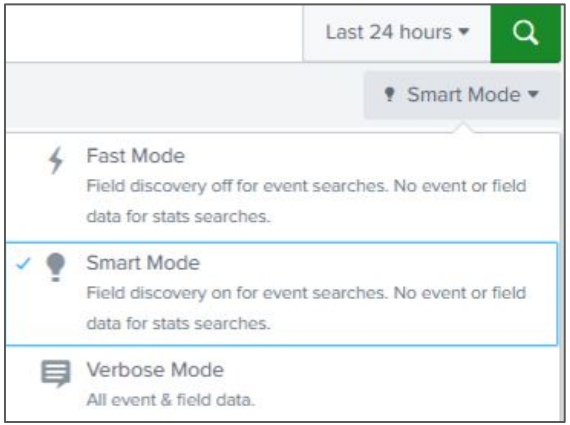


image: screenshot, splunk Search & Reporting app

Search Head

PER SCHOLAS

3.1 Explain Fields (continued)

Fast Mode

- Places a higher priority on **speed** over **completeness**.
- **Disables Field Discovery**:
  - Returns **default fields** and **indexed field extractions**
  - Extracts and provides **specific fields** that are **explicitly** mentioned in the **basic search**.
- If a **transforming command** is added to the search, the **results** display on the **Statistics** or **Visualizations** tabs only.

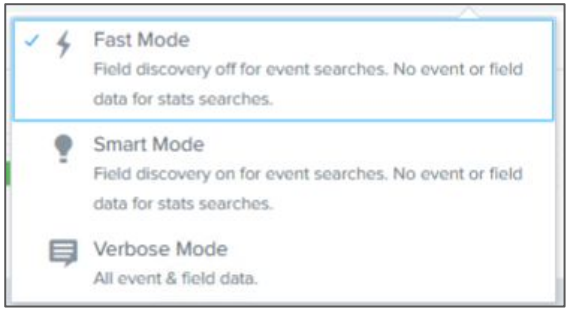


image: screenshot, splunk Search & Reporting app

Transforming commands such as stats, chart, and table, are commands that reshape, or aggregate data during the search, resulting in statistical and visual tables and charts.

PER SCHOLAS

3.1 Explain Fields (continued)

Verbose Mode

- Places a higher priority on **completeness** over **speed**.
- **Returns all extracted fields**.
- Returns full event list and event timeline for every search.
- **Slowest** search mode due to increased size of search payload.
- If a **transforming command** is added to the search, the **results** display on the **Statistics** or **Visualizations** tabs, but events are still listed under the **Events** tab.

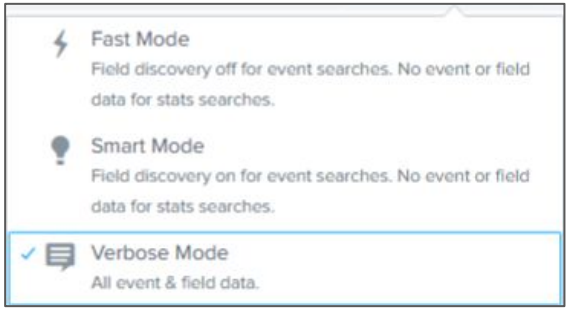


image: screenshot, splunk Search & Reporting app

Transforming commands such as stats, chart, and table, are commands that reshape, or aggregate data during the search, resulting in statistical and visual tables and charts.

3.1 Explain Fields (continued)

Smart Mode

- Smart mode is the **default** search mode.
- It balances **completeness** and **speed**.
- When running a **transforming search**, the user is presented with a report **result table** or a **visualisation**.
  - No **event list** or **timeline** is generated.
  - Performs like **Fast Mode**.
- When running a **non-transforming** search an **event list** and **timeline** are generated.
  - Performs like **Verbose Mode**.

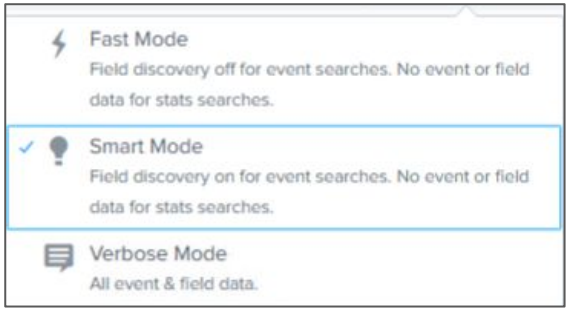


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.1 Explain fields - Summary

- Fields are searchable **name/value** pairings in event data.
- Searches with field expressions are **more efficient**.
- Some **basic fields** such as host, source, and sourcetype are extracted during i**ndex time**.
- Other fields are extracted during **search time.** Sourcetype definitions for specific data logs help **Splunk interpret** the data and add the field name when it is not specified.
- The **search mode** affects how Splunk **retrieves data** and extracts fields.

PER SCHOLAS

3.2 Use the Fields Sidebar

The Fields Sidebar

- The **fields sidebar** is a navigation panel or menu that appears in the search interface, typically located on the **left side of the screen**.
- It provides a **list of fields that are available in the search results**, allowing users to easily explore and interact with the data.
- The fields sidebar displays both **indexed** and **extracted** fields from the events in the search results.
- **Indexed** fields are the **default fields** that Splunk extracts automatically during indexing, such as timestamp, source, and host.
- **Extracted** fields are **user-defined or automatically extracted** fields that provide additional context and information about the events.

PER SCHOLAS

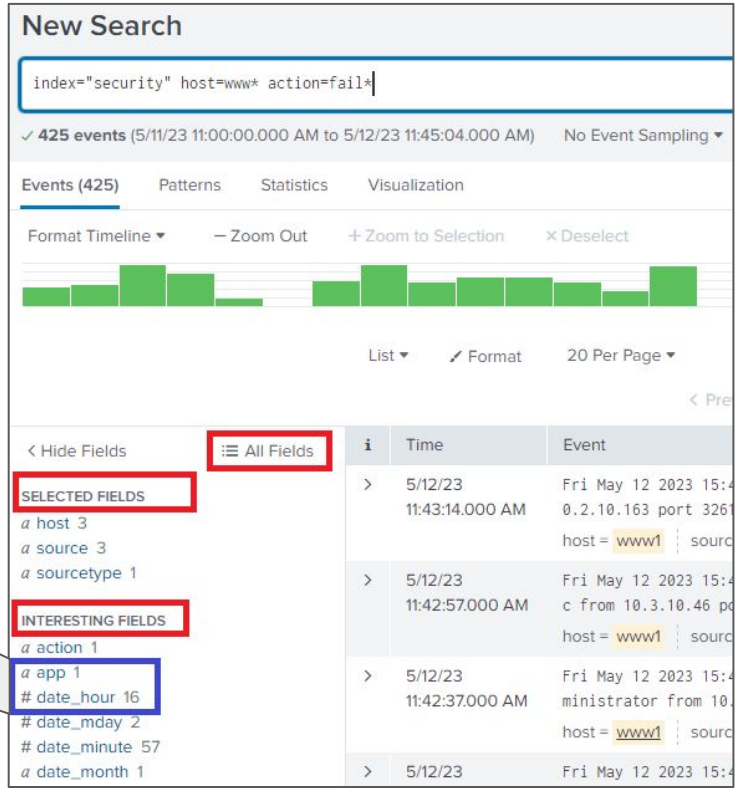
3.2 Use the Fields Sidebar (continued)

image: screenshot, splunk Search & Reporting app

The Fields Sidebar

The main sections of the **fields sidebar** are:

- **Selected Fields**: a set of fields displayed for each event.
- **Interesting Fields**: fields that occur in at least **20 percent** of the resulting events.
- **All Fields**: will open a window displaying all fields (including non-interesting fields).



The symbol to the left of the field indicates if the field values are alphanumeric (α) or numerical (#).

The number to the right of each field indicates how many unique values exist for the field.

PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Fields Sidebar - Selected Fields

- There are three **default** Selected Fields: **host**, **source**, and **sourcetype**.

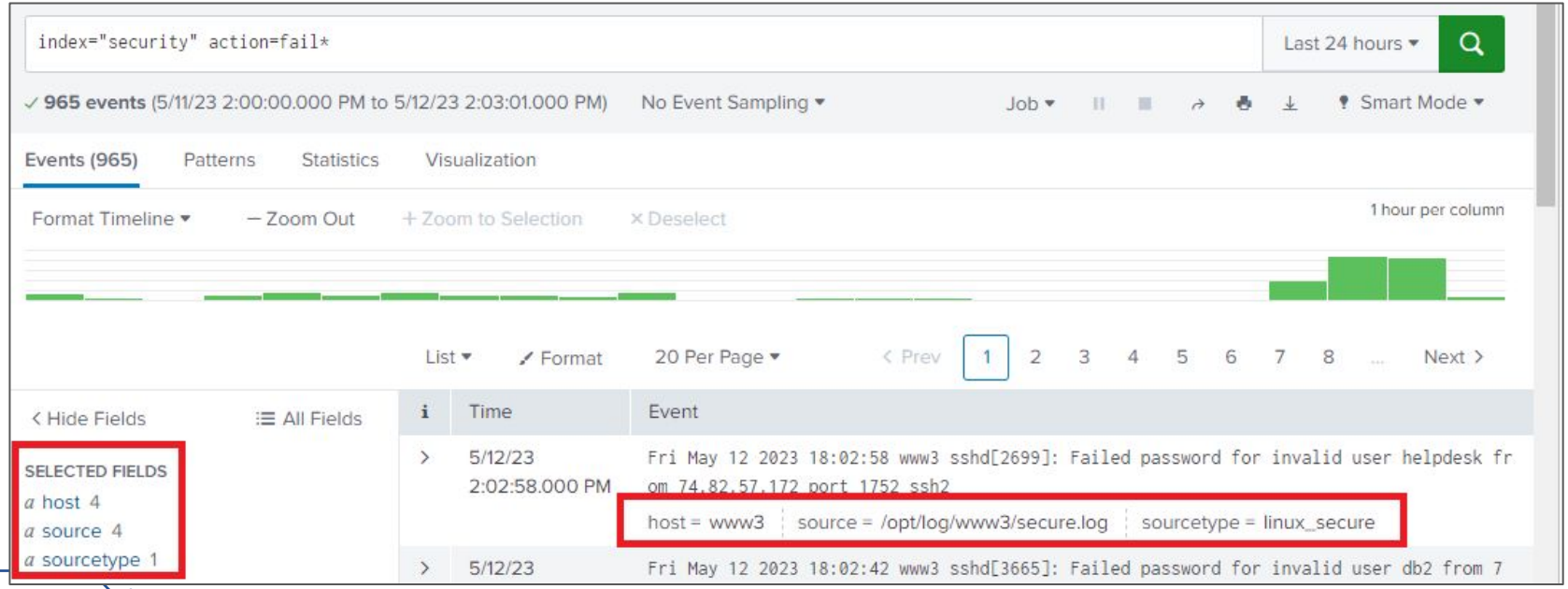


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Fields Sidebar - Selected Fields

- **Interesting Fields** can be selected and moved to the **Selected Fields** section.

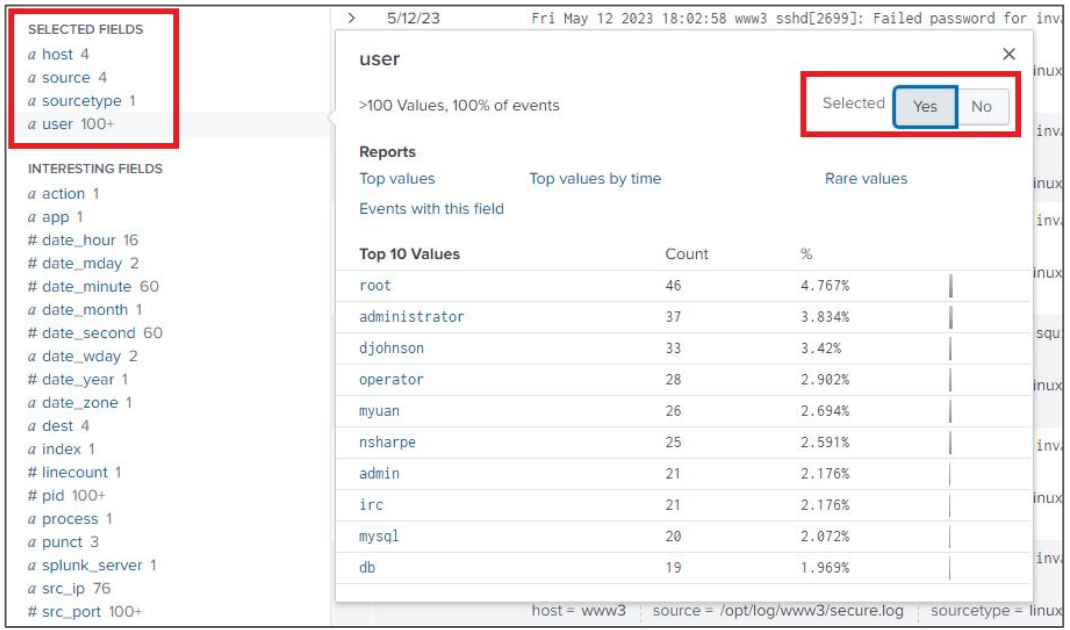


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Fields Sidebar - Selected Fields

Clicking the **All Fields** link will open a **window** allowing you to **select** or **deselect** fields, and provide insight into **statistics** and **characteristics** regarding the field, such as the **number of values** and the **field type**.

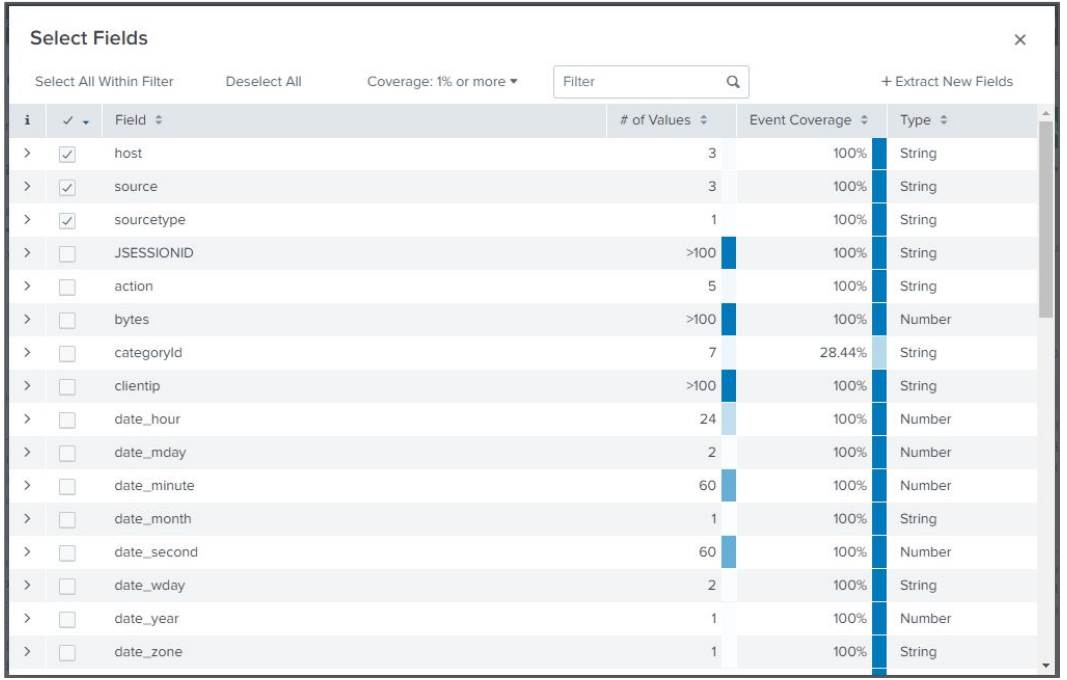


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Field Window

Clicking on a **field name** on the Fields Sidebar opens the **Field Window:**

- You can create statistical reports (add transforming command to the search).
- Narrow down the search results by adding the field name to the search
- Click a value to add the field-value pair to your search.

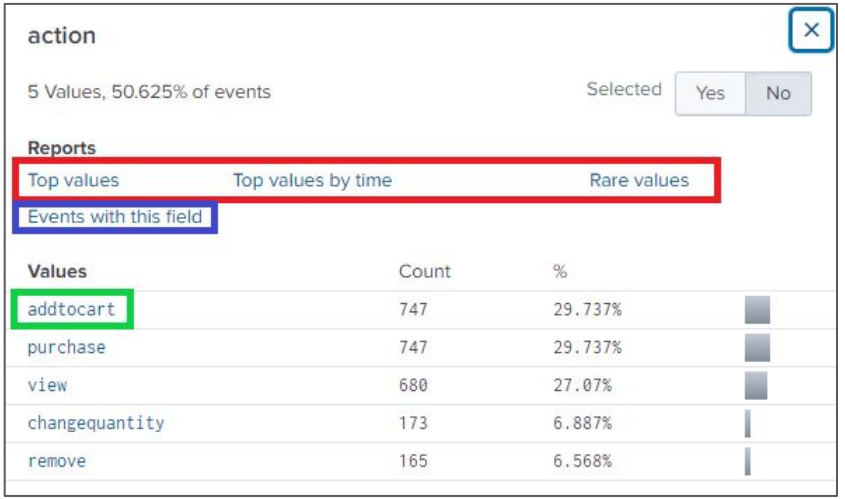


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Field Window - reports

The **options** available to you will **differ** depending on whether the field values are **alphanumeric** or **numeric**.

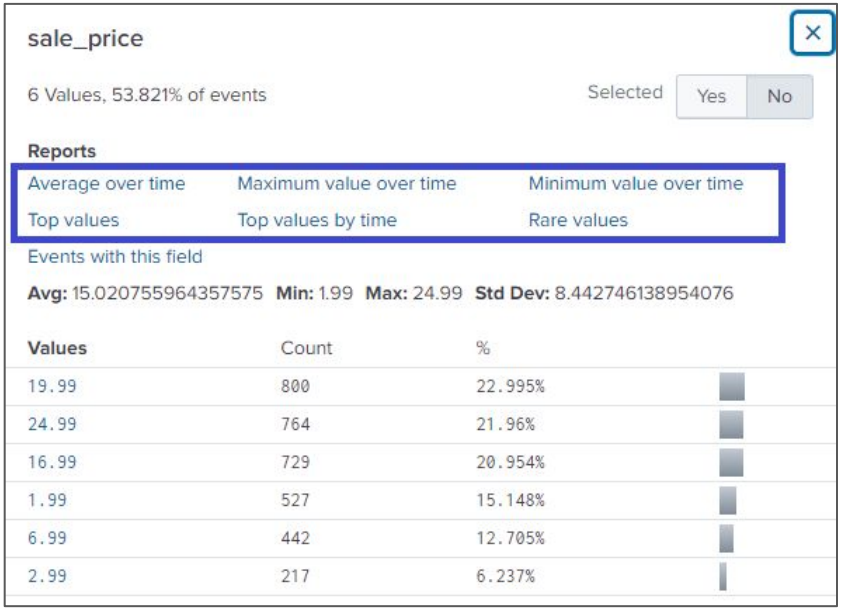


image: screenshot, splunk Search & Reporting app

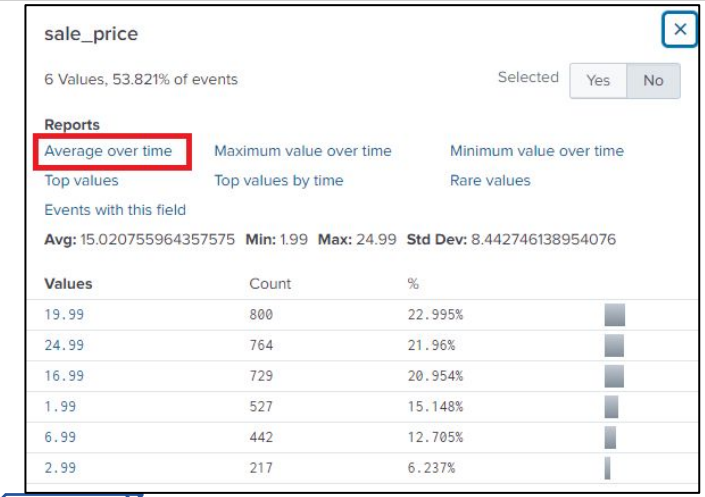
PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Field Window - reports (numeric values)

- When you use the **Reports** within the Fields Window, **transforming** commands are **added** automatically to your **search**.

```
index=web sourcetype=access_combined status=200 action=purchase
```



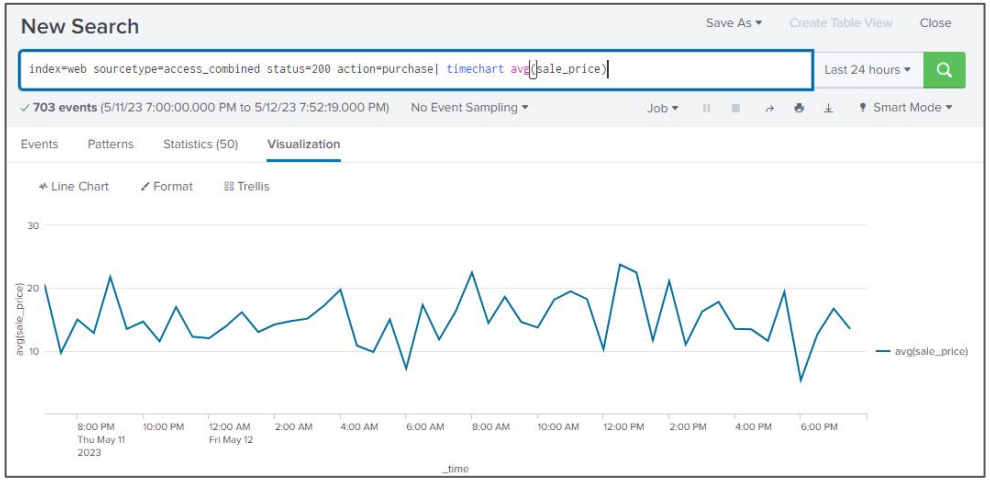


image: screenshot, splunk Search & Reporting app

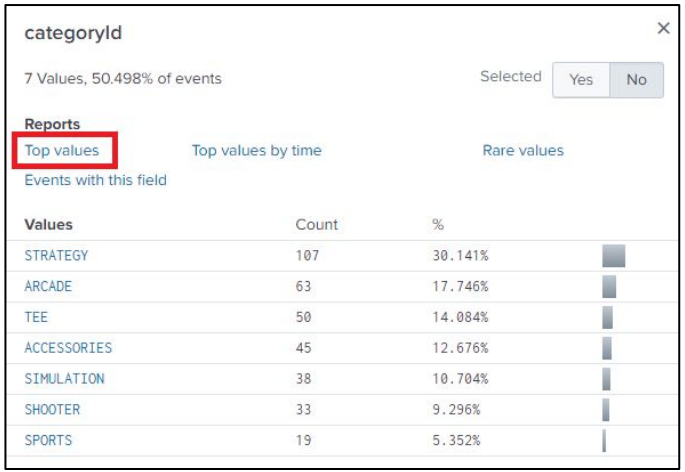
PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Field Window - reports (alphanumeric values)

- When you use the **Reports** within the Fields Window, **transforming** commands are **added** automatically to your **search**.

```
index=web sourcetype=access_combined status=200 action=purchase
```



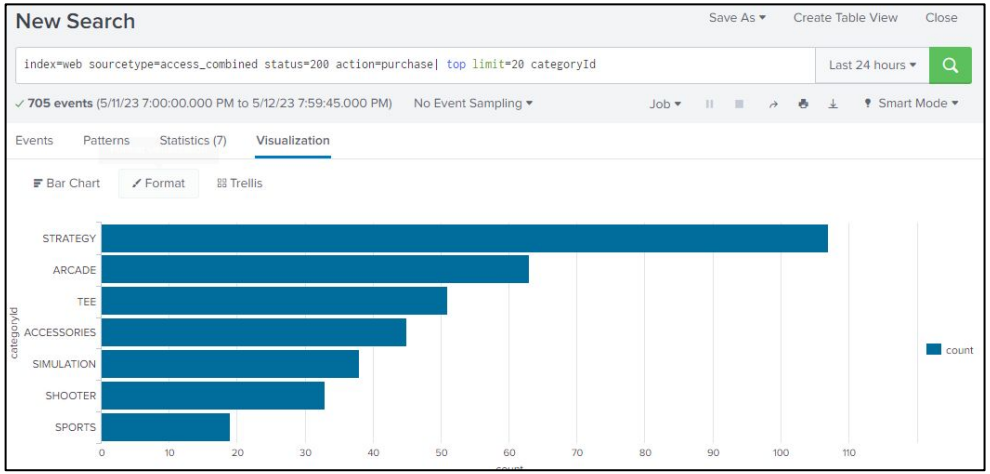


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.2 Use the Fields Sidebar (continued)

The Fields Sidebar - the index field

- **index** always appears as a field in the search results.
- If **no index is specified in the search**, data is returned from all indexes **accessible** to the **role of the user** executing the search*.
- A best practice is to **always specify indexes** when searching

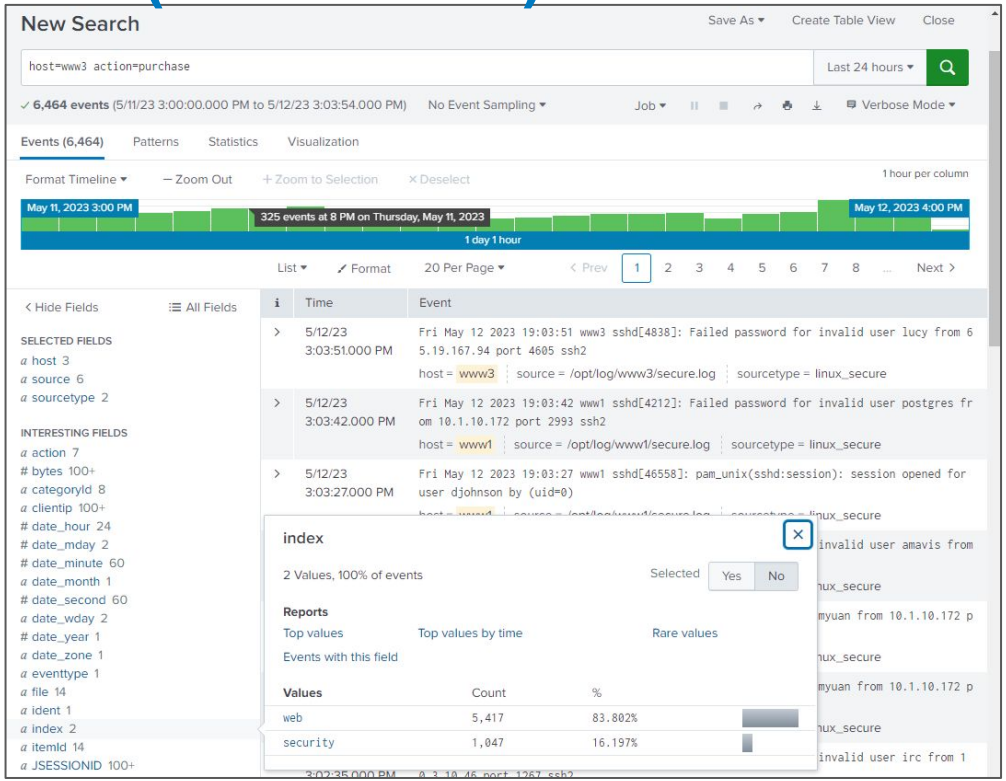


image: screenshot, splunk Search & Reporting app

3.2 Use the Fields Sidebar - Summary

The fields sidebar in Splunk is a user interface element that provides a comprehensive view of the fields present in your search results.

It displays a list of fields, along with their corresponding values, allowing you to explore and analyze the data more effectively.

Using the Fields Sidebar is helpful for quick access to relevant data that results from a search.

The Selected Fields section is a set of fields displayed for each event.

Interesting Fields on the sidebar occur in at least 20 percent of the resulting events.

Transforming options are different for alphanumeric and numeric fields.

PER SCHOLAS

3.3 Use Fields in Searches

Fields as Filters

- Including **fields** in the **basic search** allows for **effective** event **filtering** and **refining** of search **results**.
- By specifying fields in the **search query**, users can **focus** their search on **specific** data attributes and **narrow** down the results to the **desired** subset of events.

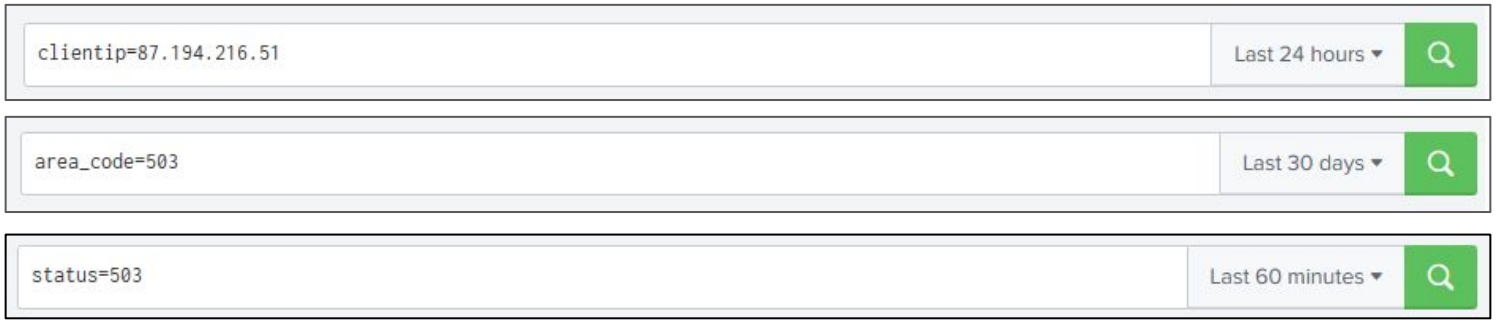


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searchesn (continued)

Fields as Filters

- When searching for field **values** without **specifying** the field **name**, results for **different fields** containing **similar** values will be returned.
- For example: searching for the value **503** may return events that fit the key/value pair **status=503** and **area_code=503.**

The first line in the search bar defines a basic search; it is a best practice to make the basic search as specific as possible.

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Fields as Filters

Remember: Field names are case sensitive; Field values are not!

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Fields as Filters

- When a search term is **enclosed in quotation marks**, Splunk will only return **results** that contain that **exact** phrase.
- For example, a search for **product_name="Dream Crusher"** (with quotes) will only return results that contain **those two words** next to each other in that order. Without the quotes, Splunk would return **any result** that contains both **"Dream"** and **"Crusher"**, even if they are not part of the same phrase.
- Quotation marks can also be used to search for values that contain **special characters**.

image: screenshot, splunk Search & Reporting app

3.3 Use Fields in Searches (continued)

Wildcards

- A **wildcard** is a character or symbol that can be used to **represent** one or more **characters** in a string.
- It is often used as a **placeholder** or a search pattern to match multiple strings that share a common pattern.
- In Splunk the **asterisk** (*) character is the wildcard used to match an **unlimited** number of characters in a string.
- For example, **status="fail*"** will match **any value of the status field** that starts with **fail** such as **failed**, **failure**, **fails**, **faille**, and so on.
- Searching for a **specific** word or phrase is more **efficient** than a search that uses a **wildcard**.
- For example, searching for "**access denied**" is always better than searching for "**access*.**"

3.3 Use Fields in Searches (continued)

Wildcards

Best practices for using wildcards.

- The **best** way to use a **wildcard** is at the **end** of a term.
- Specify a **field-value pair** whenever possible to **avoid** searching the raw field, which is the entire event.

Avoid using wildcards in the middle of a string.

- This may return **inconsistent** results because of the way in which data that contains punctuation is indexed and searched.

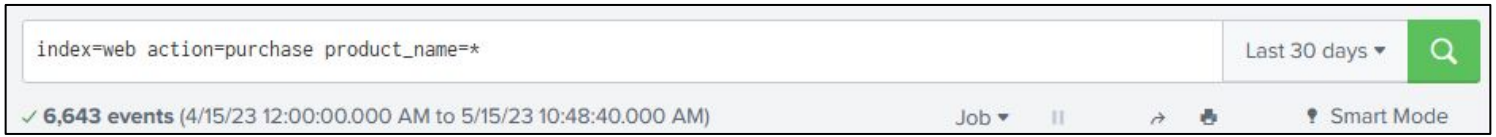


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Avoid using wildcards to match punctuation.

- **Punctuation** are characters that **are not numbers or letters**.
- If you want to match a string that includes punctuation, specify the **entire string** with the punctuation that you are searching for.
- Instead of **uri_path="/cart*"** to match paths under **/cart** specify the punctuation **directly** in your search criteria:

...uri_path="/cart.do" OR uri_path="/cart/error.do" OR uri_path="/cart/success.do"

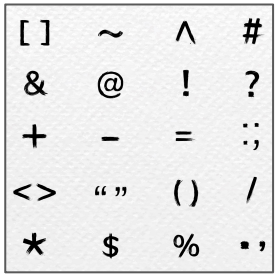


image: Freepik.com

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Avoid using wildcards as prefixes.

- When you use a wildcard character at the **beginning of a string**, the search must look at **every string** to determine if the end of the string matches what you specify after the asterisk. **Using a prefix wildcard is almost like using a wildcard by itself.**
- Prefix wildcards might cause **performance issues**. **Avoid** using wildcards at the **beginning** of search terms.

Certification question example:

According to Splunk best practices, which placement of the wildcard results in the most efficient search?

A. f*il
B. *fail
C. fail*
D. *fail*

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Boolean Operators: AND, OR, and NOT

Boolean Operators are simple words (AND, OR, NOT or AND NOT) used as conjunctions to combine or exclude keywords in a search.

- The **AND, OR, and NOT** operators are **always uppercase**.
- The **AND operator** is **implied** between search terms unless **otherwise** specified.

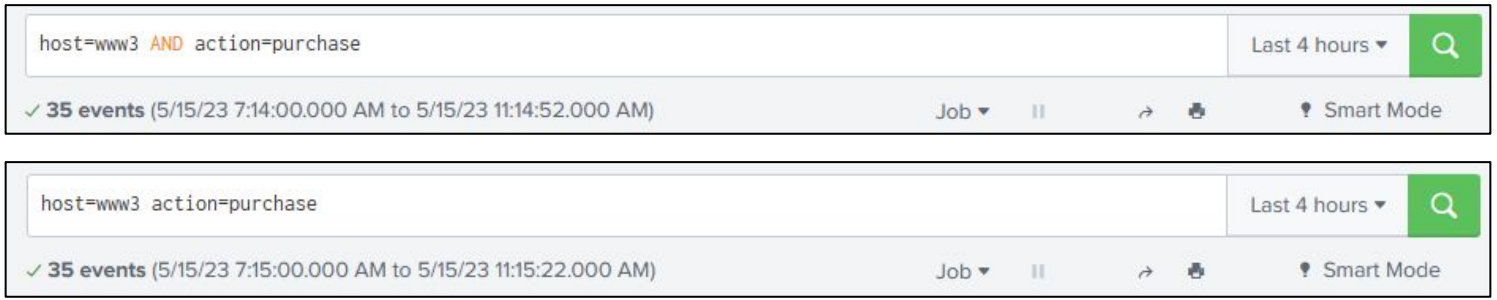


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Operators: AND, OR, and NOT

- The **OR operator** is used to search for results that match **at least one** of the conditions or key-value pairs.

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Operators: AND, OR, and NOT

- The **NOT** operator is used to **exclude results** that match a certain condition or key-value pair.

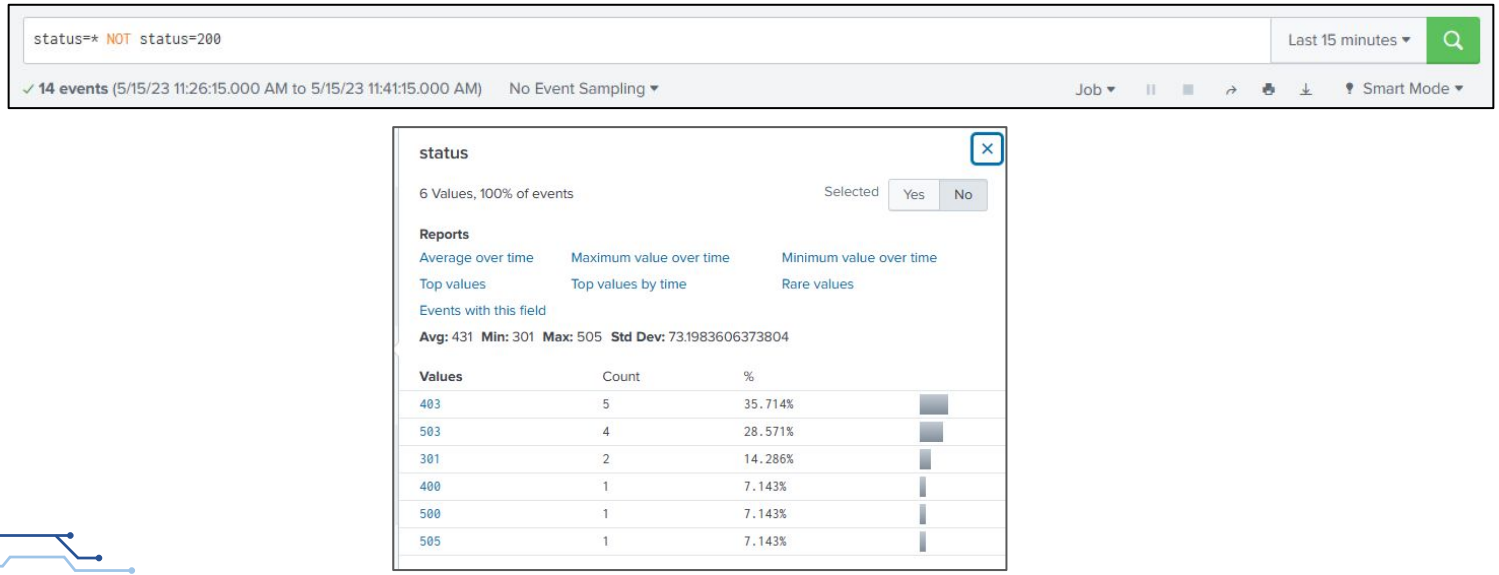


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Use comparison operators to match field values

You can use **comparison operators** to match a specific **value** or a **range** of field values.

Operator	Example	Result
=	field=foo	Multivalued field values that exactly match "foo".
!=	field!=foo	Multivalued field values that don't exactly match "foo".
<	field<x	Numerical field values that are less than x.
>	field>x	Numerical field values that are greater than x.
<=	field<=x	Numerical field values that are less than and equal to x.
>=	field>=x	Numerical field values that are greater than and equal to x.

image: https://docs.splunk.com/Documentation/Splunk/9.0.4/Search/Fieldexpressions

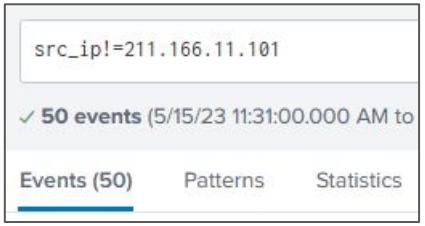
image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

Difference between != and NOT

When you want to **exclude** results from your search you can use the **NOT** operator or the **!=** field expression. However, there is a **significant difference** in the results that are returned from these two methods.



Searching with !=

If you search with the **!= expression**, every event that **has a value** in the field, where that value **does not match** the value you specify, **is returned**.

Events that **do not have a value** in the field **are not included** in the results.

> For example, if you search for **src_ip!="211.166.11.101"**, **events** that **do not have 211.166.11.101** as the src_ip **are returned**.

Events that do **not** have a **src_ip value** are **not included** in the results.

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches (continued)

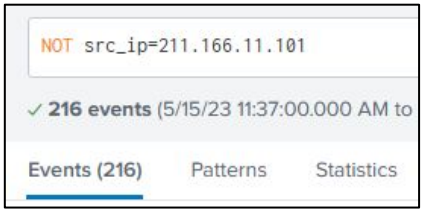
Difference between != and NOT

Searching with NOT

If you search with the **NOT** operator, **every event is returned** except the events that contain the value you specify.

This includes events that **do not have a value** in the field.

> For example, if you search using **NOT src_ip="211.166.11.101”**, every event is returned except the events that contain the value "**211.166.11.101**". This **includes** events that **do not have** a **src_ip** value.



Searching with != or NOT is not efficient

Using the **!=** expression or **NOT** operator to **exclude events** from your search results is **not an efficient method of filtering events**. **Inclusion** is better than **exclusion**.

image: screenshot, splunk Search & Reporting app

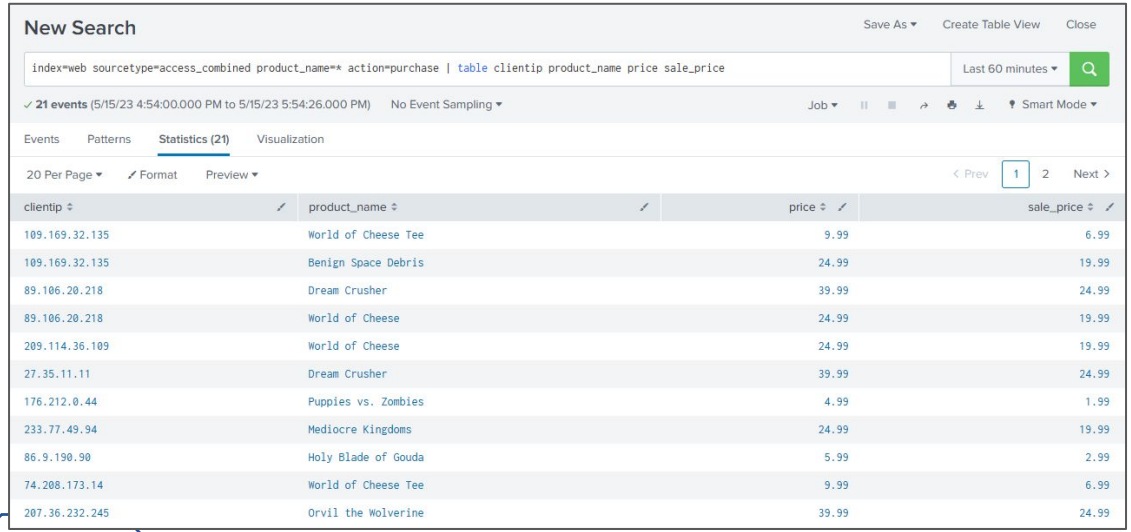
PER SCHOLAS

3.3 Use Fields in Searches (continued)

Display fields in a table using the table command.

When you search for several fields, it is **convenient** to display the **fields** in **tabular** format.

Consider the following scenario: "Display a list of **purchased products** with the **client's IP** address, the product **price,** and the **sale price.**"



clientip	product_name	price	sale_price
109.169.32.135	World of Cheese Tee	9.99	6.99
109.169.32.135	Benign Space Debris	24.99	19.99
89.106.20.218	Dream Crusher	39.99	24.99
89.106.20.218	World of Cheese	24.99	19.99
209.114.36.109	World of Cheese	24.99	19.99
27.35.11.11	Dream Crusher	39.99	24.99
176.212.0.44	Puppies vs. Zombies	4.99	1.99
233.77.49.94	Mediocre Kingdoms	24.99	19.99
86.9.190.90	Holy Blade of Gouda	5.99	2.99
74.208.173.14	World of Cheese Tee	9.99	6.99
207.36.232.245	Orvil the Wolverine	39.99	24.99

NOTE: In Splunk, the vertical bar symbol (|) is known as the pipe operator.

It is used to chain or combine multiple commands in a search pipeline.

The pipe operator allows you to pass the output of one command as the input to the next command in the sequence.

image: screenshot, splunk Search & Reporting app

3.3 Use Fields in Searches (continued)

The rename command.

```
... | rename <field> AS <NewField>
```

- Use the **rename** command to **assign** fields with more **meaningful** and **user-friendly** names.
- Use **double straight quotes** to include **spaces** and **special characters** in field names.
- When a field is **renamed**, **no permanent** change is made to the **indexed** data. The change **only exists** for the **lifetime** of the **search**.

PER SCHOLAS

3.3 Use Fields in Searches (continued)

The rename command.

```
index=web sourcetype=access_combined product_name=* action=purchase
| table clientip product_name price sale_price
| rename clientip AS "Client IP Address", product_name AS "Game Name",
price AS "Listed Price", sale_price AS "Sold For"
```

Client IP Address	Game Name	Listed Price	Sold For
27.102.11.11	Fire Resistance Suit of Provolone	3.99	1.99
27.102.11.11	Puppies vs. Zombies	4.99	1.99
27.102.11.11	Orvil the Wolverine	39.99	24.99
222.41.213.238	Mediocre Kingdoms	24.99	19.99
64.66.0.20	Manganiello Bros.	39.99	24.99
64.66.0.20	Manganiello Bros.	39.99	24.99
198.35.3.23	Mediocre Kingdoms	24.99	19.99
198.35.3.23	Puppies vs. Zombies	4.99	1.99

NOTE: Once a field is renamed, the new field name must be used in the rest of the search string.

image: screenshot, splunk Search & Reporting app

PER SCHOLAS

Table formatting

Tables can be easily formatted to better display visual results.

- Use the **paintbrush** icon to access the **table formatting** options.
- You can change the **color** of the column based on the **values** it contains, and change the **number formatting** to fit your needs.

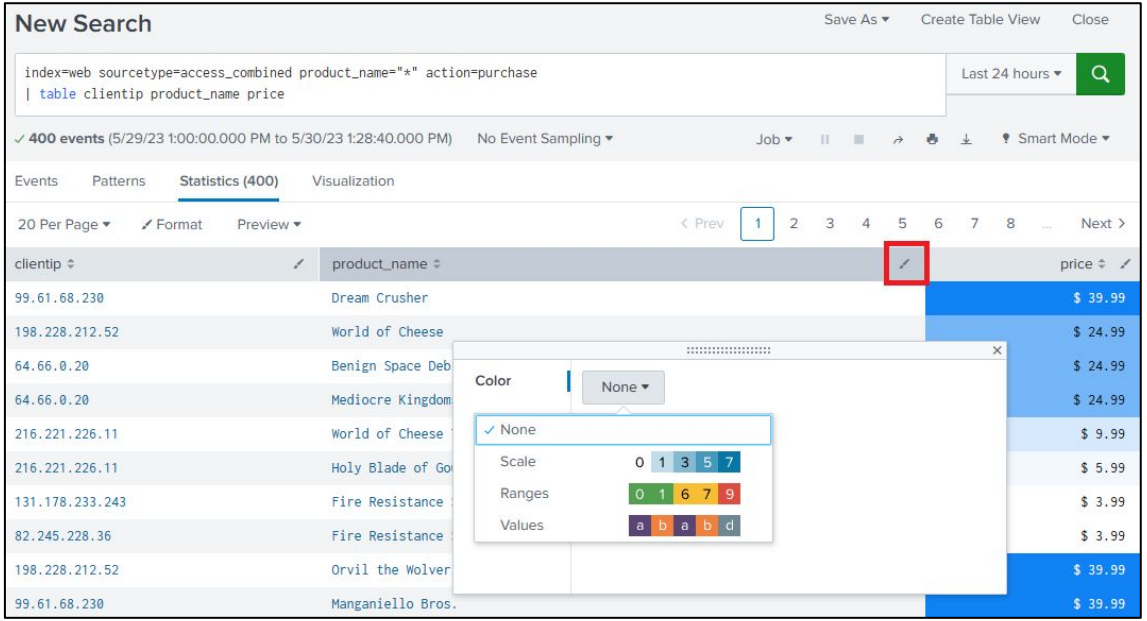


image: screenshot, splunk Search & Reporting app

PER SCHOLAS

3.3 Use Fields in Searches - Summary

- Using **fields** in Splunk allows you to **filter** events and refine search results based on **specific** data attributes.
- Field **names** are **case sensitive**; Field **values are not**!
- Use double **quotation marks** to search for values that contain **spaces** or **special** characters.
- The **(*)** wildcard can be used to **match characters** in **string** values, but using a wildcard is **less efficient**, and when using them they should be placed at the **end of the term**.
- The **boolean** operators **AND, OR, NOT** help specifying the field values we are searching for.
- Splunk also supports **comparison operators** to match field values.
- The **table** command is a simple way to display the content of fields in **tabular format**.
- The **rename** command is used to to rename fields **temporarily**, more **meaningful** and **user-friendly** names.

PER SCHOLAS

Knowledge Check

- What are fields in Splunk? Provide an example of a field.
- What is the difference between indexed fields and search-time fields?
- What are are the the three Splunk search modes, and how do they differ?
- What does the (α) symbol displayed to the left of a field name on the Field Sidebar indicate?
- What does the (#) symbol displayed to the left of a field name on the Field Sidebar indicate?
- On the Fields Sidebar, what are the three default Selected Fields?
- What is used by Splunk as a wildcard?
- What operator is implied between search terms, unless otherwise specified?
- After renaming a field, how long does the change exist?