

Basic Searching >

Basic search terms (building blocks)

- Keywords
 - `failed, error`
- Phrases
 - `“failed login”`
- Fields
 - Key value pairs
 - `user=user1.domain.com`
- Wildcards
 - `*ailed, fail*, user=*`
- Booleans
 - Case sensitive (upper)
 - `AND, OR, NOT`

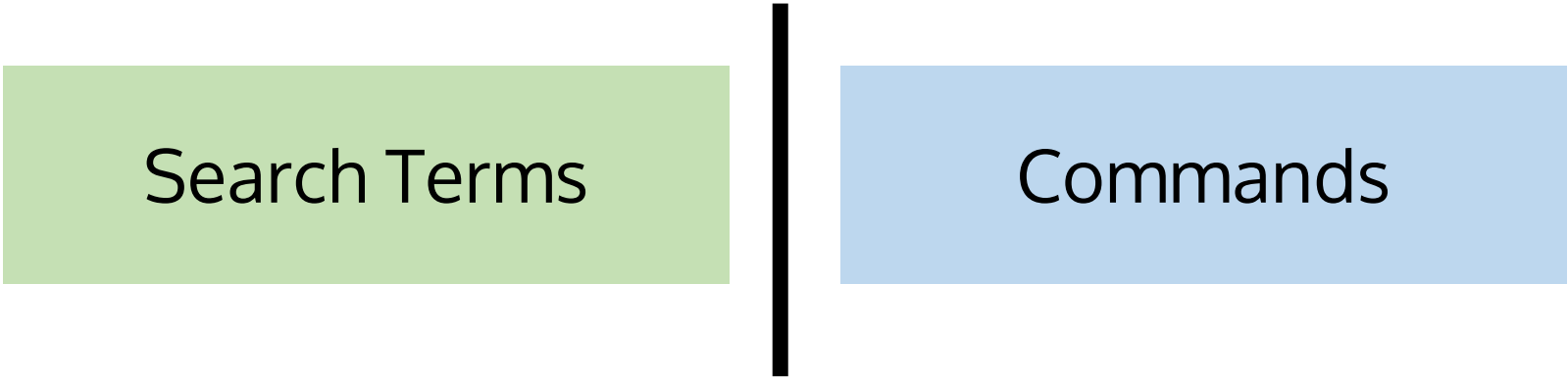
Basic Searching >

Basic search commands

- `chart / timechart`
 - Returns results in tabular output for charting
- `rename`
 - Renames a specific field
- `sort`
 - Sorts results by specified fields
- `stats`
 - Provides statistics
- `eval`
 - Calculates an expression
- `dedup`
 - Removes duplicates
- `table`
 - Builds a table with the specified fields

Basic Searching >

Constructing a basic search



Search Terms

Commands

```
host=myhost.lcl  source=hstlogs  user=*  message=fail*  OR  lock*  
| table _time user message  
| rename _time AS Time user AS User message AS Message  
| sort -Time
```

Basic Searching >

Time	User	Message
2017-03-28-7:10:07	user1.domain.com	failed log on
2017-03-28-7:17:00	user1.domain.com	failed log on
2017-03-28-7:17:00	user1.domain.com	locked

Thanks, Splunkers!

