Splunk

- eval command
- Event vs Statistics Tab
- Event data

eval command

The `eval` command can be used with either table data or event data.If used with event data the new field that is created won't be shown, because the event tab only shows the event data as a whole. Duh.

To show the new field that you have created then you will have to use the `table` command to include that new field.

Important note

If you use `eval` command with field names that include non-alphanumeric characters, other than '_', you must surround the field with **single quotation marks**. For example, if you are using 'server-1' field in your `eval` expression then you must do it like so

```
eval new=count+'server-1'
```

Inline eval

If you use inline `eval` with commands such as `stats / chart` then you can evaluate new fields using the existing ones, you just need to use the `AS` to assign it to a new column. As opposite from doing `variable=<expression>`

Event vs Statistics Tab

If you perform a normal search, the event tab list all the events that are matched with the search query that you have specified. The statistics tab will not display any reporting data since you did not used any reporting commands.

Reporting commands are commands that creates a table: Commands such as `stats count`, `table`, or `chart`.

Reporting (transforming) command

As long as you don't use any transforming commands your results will always be in the Event tab. If you use any transforming command then the data be transformed to numerical values and ordered the results into a data table, which is why your result will show up in the Statistics tab.

Transforming commands are required if you need visualization.

Event data

An event is just the data that is sent by the forwarder and parsed by the indexer. It is associated with a timestamp.

The event can be a simple log, stack trace, or even a JSON payload.