Day - 2

22 July 2025 10:05

1. Addcoltotal & Addtotal.

addtotal → Addition of rows.

4 . 5 7 8 → 24

|addtotal

addcoltotal → Addition column wise.

Syn. → |addcoltotal columnname labelfield=Sum|

label=total CTS

1
2
3
4
10

total → 10

2. Top / Rare:-

Top → top command will give you the top values.

Syn:- |top sourcetype → Top 10 values by default.

|top limit = 3 sourcetype
↳ limiting upto 3 values.

|top limit=0 sourcetype
↳ Display all the values.

Rare:- least 10 values.

Syn:- |rare sourcetype → least values.
↳ upto 10 values.

two fields
count & Percentage

|rare limit=0 sourcetype. give all the values.

|rare limit=3 sourcetype.

## (3) search & where Command:-

Both of these command is used for filter Activity.

| A | B |
|---|---|
| 5 | 4 |
| 10 | 18 |
| 7 | 2 |
| 25 | 35 |

search → | search A>10

| A | B |
|---|---|
| 25 | 35 |

where → When you compare two different field.

ex → | where A > B

| A | B |
|---|---|
| 5 | 4 |
| 7 | 2 |

09-09-09 09:09

%d-%m-%y

%m-%d-%y

%y-%m-%d

## (4) Eventcount :-

| eventcount index=main Summarize=false

tsidx → timestamp index file.

& summary

→ list → quick

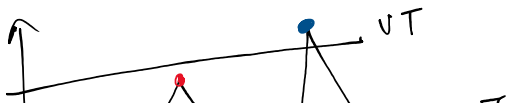
## (5) chart :-

| chart count by current_ticket_state.

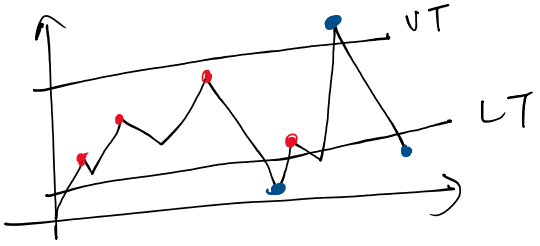
count → y-axis

current_ticket_state → X_axis.

Multiselects



Multiselect:-

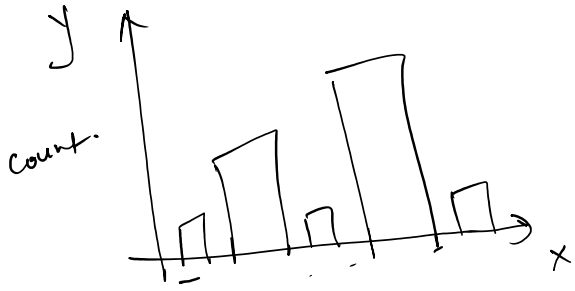



6. Single Value Visualization:-

Single numeric value, we show on the chart.

1. Radial Gauge
2. Filler Gauge.
3. Style Value
4. Marker Gauge.

7. timechart:-




Interval ⇒ span = 1 mon

|timechart count by CTS

_time, renewed by (_time)

s = sec
w = week.

y = year
mon = Month
H = Hour
M = Minute

8. Date & time functions:-

Strptime → That will convert the date & time function into format.

%-Y.%m|y %-H:%-M)

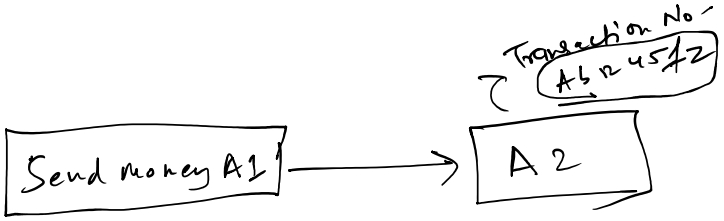
Strptime → That will con.
↓
Parse your datetime fun. system format.

eval epoc_time = Strptime(f1, "%.d-%.m-%.y %.H:%.M")

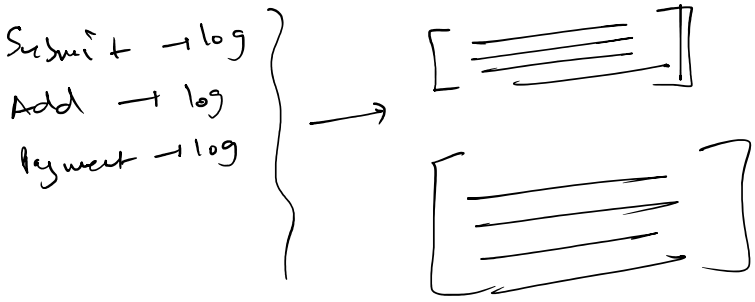
(9.) rex → Regular expression in splunk.
↓
Extract the field out of the raw.

|rex field="f1" "regular expression".

(10.) Transactions




Group the events on the basis of Transaction.




Syn:- |transaction f1, f2

T1
= [e1, e2, e3, e4, e5]
→ maxevent → 5
maxpause = (e2-e1), (e3-e2), (e4-e3)
maxspan = (e5-e1)

maxspan
maxpause
maxevent.

maxevent → 5 (total No. of event in the transaction will be b/w 1 to 5)

..cutive event

maxevents → 5 (...

↳ will be b/w 1 to 5)

maxpause → time diff. b/w two consecutive event in a single transaction.

maxspan = time diff. b/w first & last event in a transaction