Day - 2

20 August 2024 09:42

1. Top & Rare.
2. where & search.
3. chart.
4. Timechart
5. Date & Time fun~.
6. Single value Visualization
7. Geo Map.
8. Custom Visualization.
9. Append.
10. Join.

① Top & Rare:-

Top Command → Top Values — Count, percent.

① Default = 10

Top sourcetype.

Top limit = 3 sourcetype ② Top 3 values.

Top limit = 0 sourcetype. ③ Top values in Descending.

② Rare Command:- Least value, Ascending order.

③ Where & Search:-

Severity	Count
1	5
3	3
4	15
~	

Search severity = 1 → filter the events on the basis of Severity value 1.

where command is used to Compare Two fields.

Where Count > Threshold.

Count	Threshold.
	15
10	15
5	15
8	15
2	15
12	

④ chart:-

| chart count by Current_ticket_state

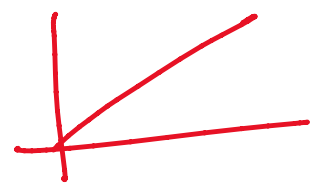
count → y-axis.

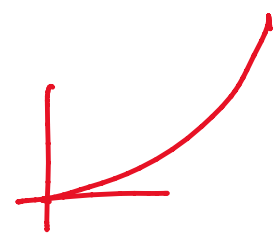
Current_ticket_state → X-axis

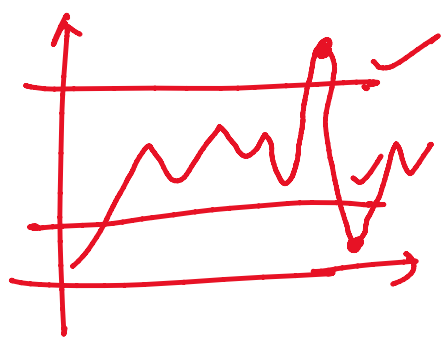
10, 20, 30, 40 - - - - -

log → 10^x

10, 100, 1000, 10000

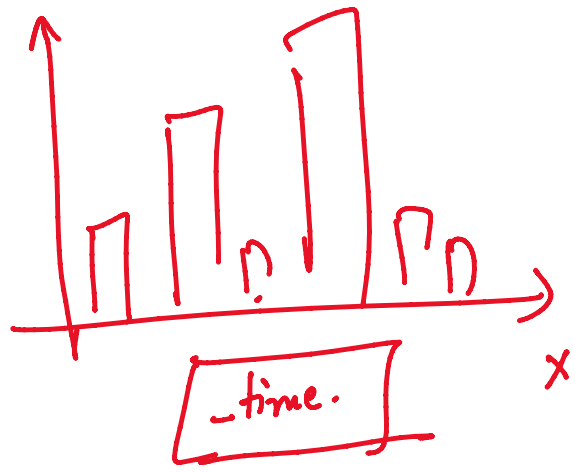






Single Value → Visualize the single value chart.

Timechart:-



GeoMap:- Coordinate. → Longitude, Latitude

Pinpoint on the cluster Map

Append:-

(1) Append

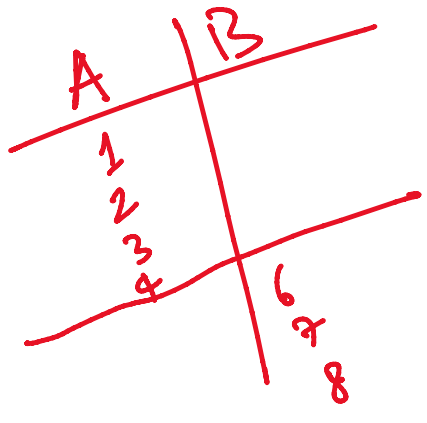
(2) Append Cols.

(3) Appendpipe.

Append:-

A | append[B]

Append | Combine Two diff. data set.



Appendpipe:-

(A) | appendpipe [Search B]

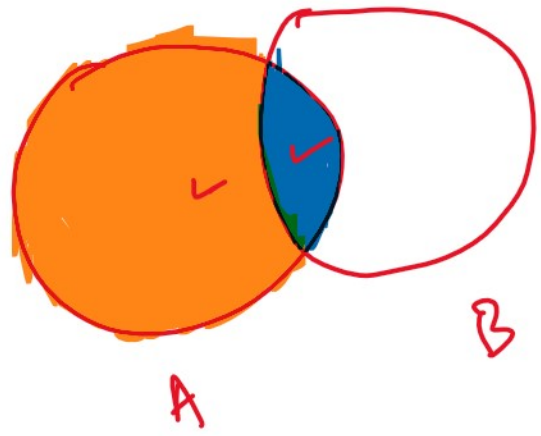
A o/p → I/p

join:-

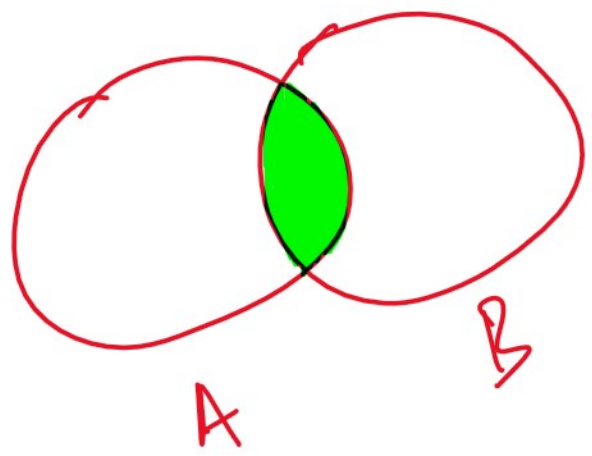
① Outer / left

② Inner join

① Left join:-



② Inner join:-



Tstab → Tsidx file

↓

Ts collect statistics

High performance

Transaction:-

↓

Grouping the events.

① Beneficiary Ac
② Amount
③ from which
④ Time
⑤ Mode
⑥ Phone/Laptop
⑦ Browse
⑧ Android/IPhone

(1) Maxspan - (event5 - event1)

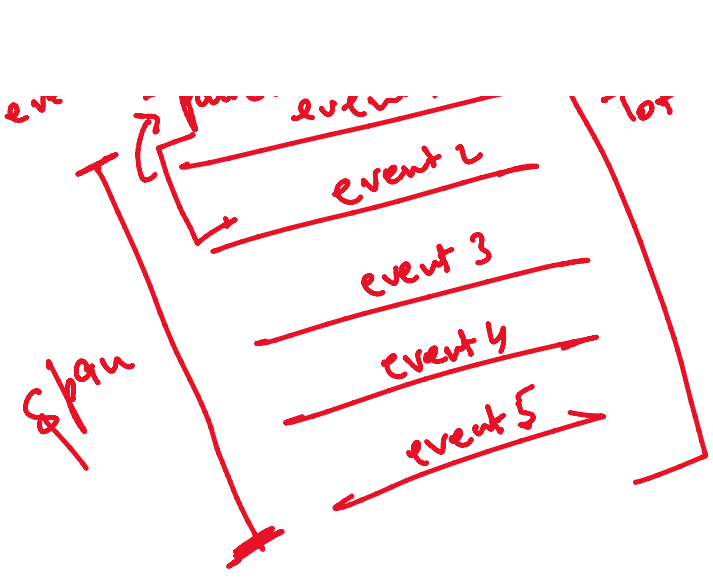
Consecutive event

T [1 pause. event1 / event2] Total event ≤ 5

① Maxspan - event

② Maxpause - Two Consecutive event Time diff.

③ Maxevents.



* Rex, Regex & erex:-

① Rex:-

1234-5678-9101-1213

xxxx-xxxx-xxxx-1213 → Mask

① Substitution - S | <string1> | <string2>

② Replacement - S | <regex> | <replacement>

→ Regular expression

Data Masking:-

erex → example

example → Auto. R.E → Implemented on your event.

Regex:- filter the events on the basis of the certain Key/Pattern.

Field Alias:- Creating New Name of the field.

↓

New Name | Nick Name.

Severity → Priority

ticket_number → incident_number.

ticket_num...

I1
emp_id
↓
emp_id.

I2
employee
↓
emp_id] → FA

I3
e_id
↓
emp_id] → FA

① emp_id → FA_name...

① It will effect the existig data set.

② Severity → Priority] → Both the field will be available (i.e. old field, new field created by FA).