SPL Query:-

---

① Table:-   Tabular output: → field name are case sensitive.

| table f1, f2, f3, f4

↳ Name the same seq. o/p will come.

---

② Rename:-   Rename the field

Search time rename.

| rename old-field AS New-field.

| rename CTS AS Ticket state
         └ Old Name   New Name.

---

③ Stats:-   Statistical output.

→ Count — | Stats count as total.
→ Avg- — | Stats avg (f1) as f1 ⎫
→ Sum- — | stats sum(f1) as f1 ⎬
→ list ⎫   → Categoris the data.
       ⎬   hist (current ticket had)
→ Values ⎭   ↓ duplicate
        ↓
     Unique

---

④ Eval:-   eval command used for evaluation purpose.

int ⎫
var ⎬ → initialize Variable   eval → initialize Variable.
str ⎭

                    eval a = b + c
                        ↖___↓___|

— → Convert the value from byte to Kb.

(i) Calculation:- Convert the value from "J" :

(ii) if else:-

```
if (a>b)
{
    Print(a);
}
else { print (b);
}
```

→

if (a>b, a, b)
 └→   └→ └→
   ↓   ↓   ↓
Condition. True False.

(iii) Case:-

Case (cond1, Value1, Cond2, Value2, Cond3, Value3, - - - , 1=1, Univesal)
                                                              ↓   Value
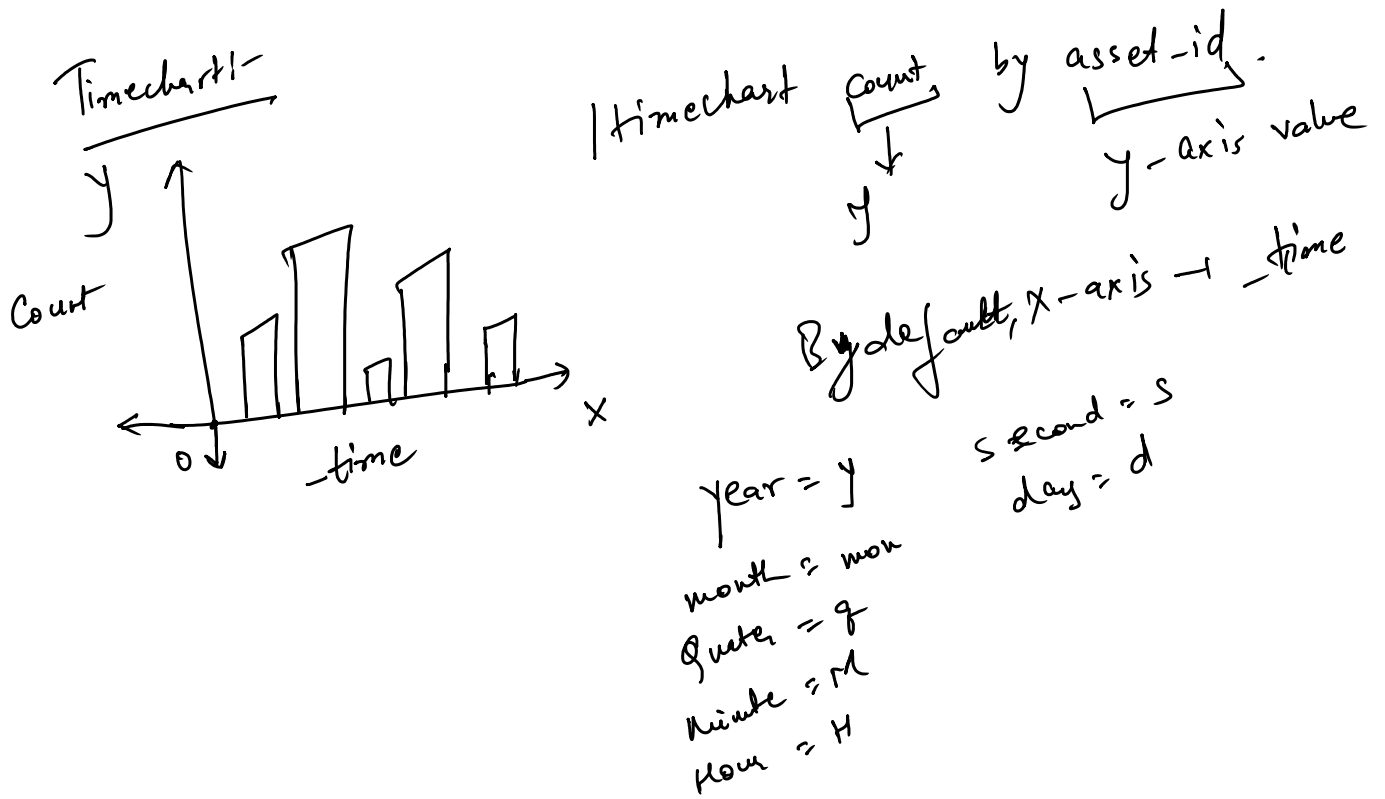→ execution works from left to right-
                                                          Universal
                                                          Value.

(3) Sort → Sorting purpose
         Sort - fieldname → Descending order
         Sort + fieldname → Ascending order ⎫
          ↓   ⎬ —
         Sort fieldname → Ascending order   ⎭

(4) chart & timechart:-

|chart count by Severity,
        └→   └→
      y-axis   x-axis

Timechart!-

| timechart count, by asset-id.

By default, X-axis → _time

year = y   second = s
                day = d
month = mon
Quater = q
Minute = M
Hour = H

Single Value Visualization

Single Numeric Data as an output.

Trend Analysis!-

timechart trend.

Geomap!-

Coordinate system

latitude & longitude

| Geostats latfield = ___ logfield = ___

count by state

Addcoltotal!-

Column wise addition.

Addtotal!-

Row wise Addition.

Addtotal:- Row wise Addition.

Fillnull:- Fillnull Command is used to handle the blank Values.

| fillnull
↓
Default blank spaces is filled with 0.

| fillnull Value = "NA"
↓
Blank spaces is filled with **NA**

Head:- First two values.

| head 2
↓
Default value is 10

Tail → Value from the bottom

| tail 3
↓
Bottom 3 values.
↓
Default value is 10

Top & Rare:-
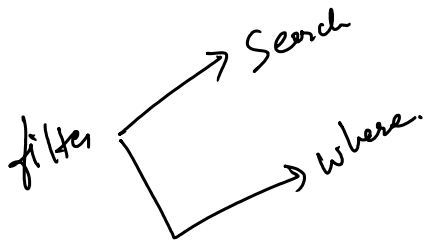
Top → Top 10 values.

| top Sourcetype

Sourcetype	Count	Percent

| rare limit = a sourcetype
→ ..3 values → 0 unlimited

Rare → least 10 Values

| rare | sourcetype | least 3 valu. |
| unlim... nah. |

Sourcetype	Count	Percent

filter → Search
       → where.

A → B (circled A)

A	B
10	15
20	25
15	35
5	4
7	2

In the same field itself | Search A > 10

A	B
20	25
15	35

where — Compare two fields.

| where A > B

A	B
5	4
7	2

VT1   VT2   VT3

index=vk_idx source=Sample_tickets.csv | stats count by current_ticket_state | eval threshold=15 | search count>10 |

where count > threshold

VT4
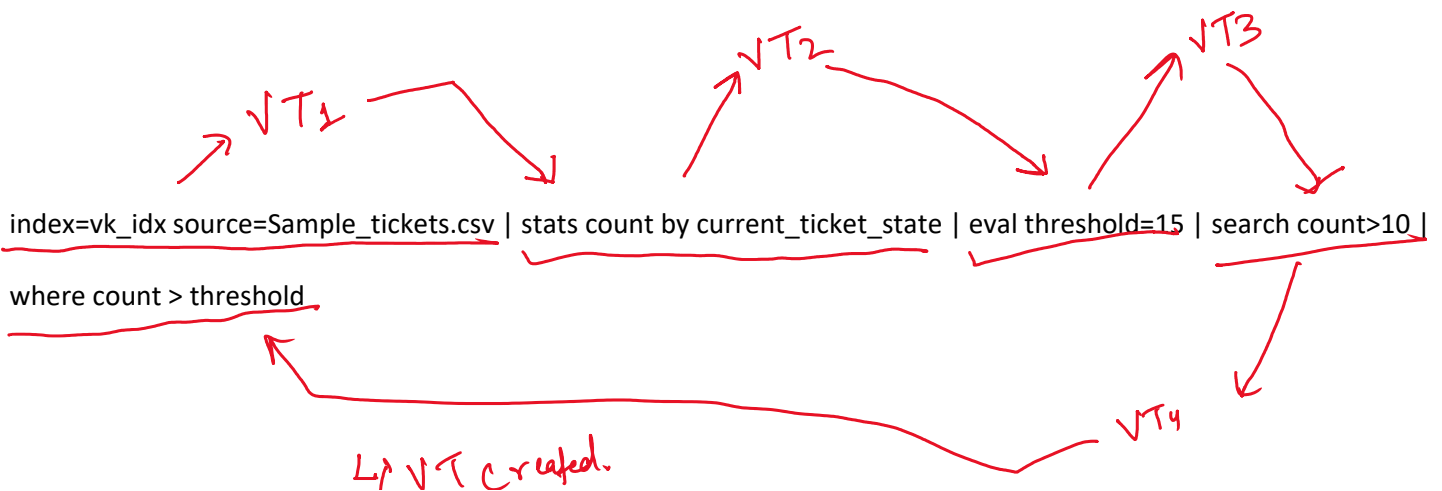
→ VT created.

ↄ VT created.   VTy

Assignment   Regular expression Writing.