Day - 2

22 April 2025 10:12

1. Eval:- Eval is used for evaluation purposes.

Var a
int a
Str a
} → Variable

Eval $\underbrace{\quad a \quad}$
↓
initialize the variable named a

1. Calculation
2. if-else
3. Case statement.

1. Calculation:

bytes → kb

(bytes/1024) → kb

```
index=_internal
| eval kb = bytes/1024
| table bytes, kb
| eval kb_round = round(kb,3)
| eval kb_concat = kb_round." KB"
```

```
index=_internal
| eval kb = round(bytes/1024,3)." KB"
| table bytes, kb
```

```
index=_internal | eval kb=bytes/1024 , kb_concat=kb." KB" , kb_round=round(kb,2)  | table kb
kb_round kb_concat bytes | sort - kb
```

2. if-else statement:-

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

$$\text{eval} \_ = \text{if}\ (\underbrace{a>b}_{\text{Condition}},\ \overset{\text{True}}{a},\ \underset{\text{False.}}{b})$$

```
    Print(a);
    }
else
    {
    Print(b);
    }
```

3. Case Statement :-

```
switch(a): ______
switch(b): ______
      (c): ______
      (d): ______
default(1=1): ⟶
```

Case(Severity=1, "Critical", Sev=2, "Normal", Sev=3, "Low", 1=1, "Info")

$\underbrace{1=1}_{\text{Universal condition.}}$

```
index=vk_idx  → 99        → 99
| eval priority = case(severity=1,"Critical", severity=2, "High", severity=3, "Low",1=1,"Info")
| table severity, priority  → 99
| dedup severity  → 4
| sort severity  → 4
```

```
index=vk_idx  → 99
| dedup severity  → 4        → 4
| eval priority = case(severity=1,"Critical", severity=2, "High", severity=3, "Low",1=1,"Info")
| table severity, priority  → 4
| sort severity  → 4
```

Top or Rare :-

top 10 values.

| top sourcetype

By default, it will give top 10 Values

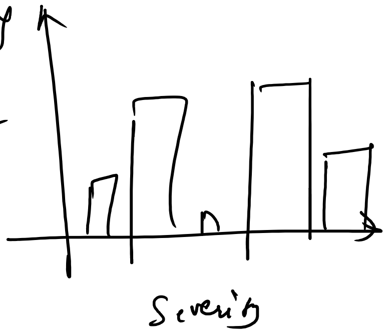
limit=3 → Top 3 values

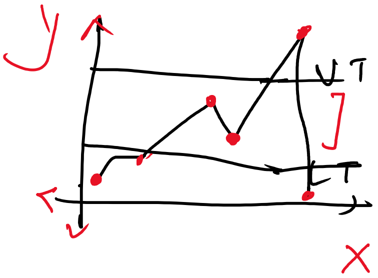
1. l=0 → Unlimited Values.

limit= 3

limit=0 → Unlimited Values.

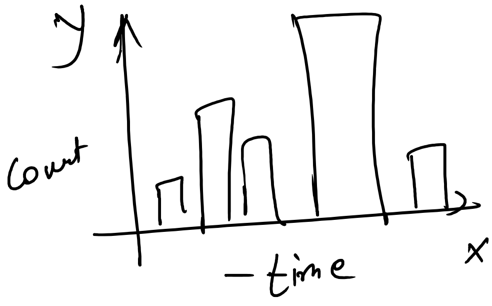
chart:- | chart $\underbrace{\text{count}}_{\text{y-axis}}$ by $\underbrace{\text{severity}}_{\text{x-axis}}$





Timechart x_axis → time

y_axis → numeric (count)



GeoMap:- Latitude

Longitude.

Single Value Visualization:-

1. Single Numeric Value on output.

2. Regular expression.

Rex:- Regular expression.

Field Extraction → Delimiter.

↓

Pattern.

Regular expression

Regular Exp.

Data Masking → y/<regex>/ <——> /flag.