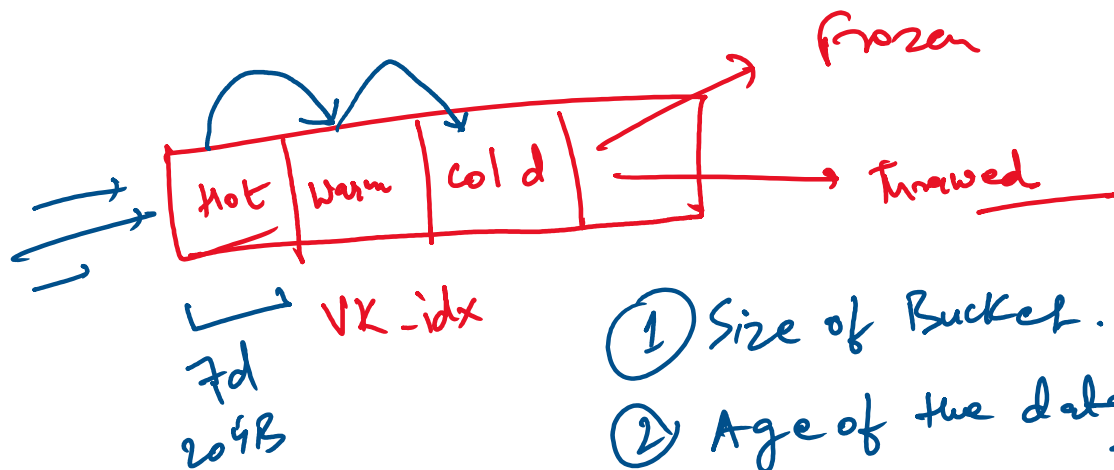


Indexer → Index.



SPL (Search Processing Language):

1. Table: Tabular format. Syn: table field1, field2, field3.
 2. Rename: Change to new name. Syn: rename old-name AS new-name
 3. Sort: Sort + | —, → Ascending, sort - fieldname → Descending.
 4. Dedup → dedup f1, f2 → Remove Duplicate values.
 5. Stats:
 - ① Count → Count on basis of certain condition.
 - ② avg → Avg. on the basis of certain condition.
 - ③ Sum → Sum of numeric field.
 - ④ list → Group the field with certain value.
 - ⑤ Values → Group the fields with unique values.
- ... purposes. eval a

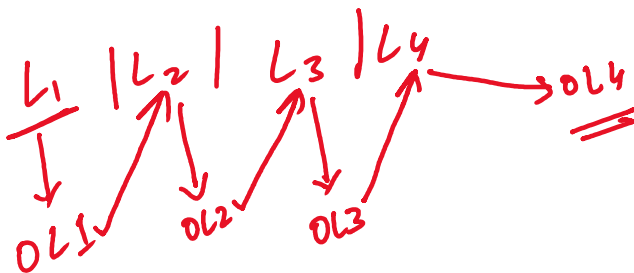
- (4) use \rightarrow Group the fields -
 (5) Values \rightarrow eval a
 6. eval (1) Calculation \rightarrow evaluation purpose.
 (2) if-else \rightarrow if condition
 (3) Case statement \rightarrow Switch condition.

7. Chart \rightarrow

8. Time chart

(1) Date & Time function

9. Single value visualization.
 10. GeoMapbox



fillnull value="NA" $\frac{b}{a}$

a	b	c
NA	NA	NA
NA	NA	NA
NA	NA	NA

11. a7b)

if (cond1, True, False)
 11. a7b. a, b)

if else ->

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

```
if (a > b, a, b)
```

Case Statement:-

```
switch (a):
    switch (b):
        default:
```

```
case (Cond1, "true", Cond2, "-",
      Cond3, "-", 1=1, "-")
```

Chart:-

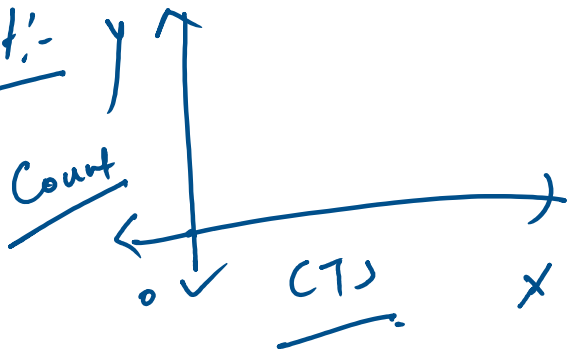
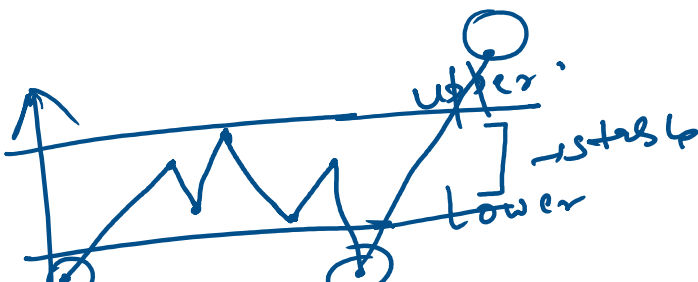
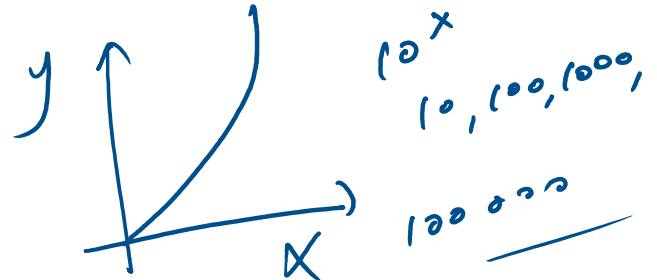
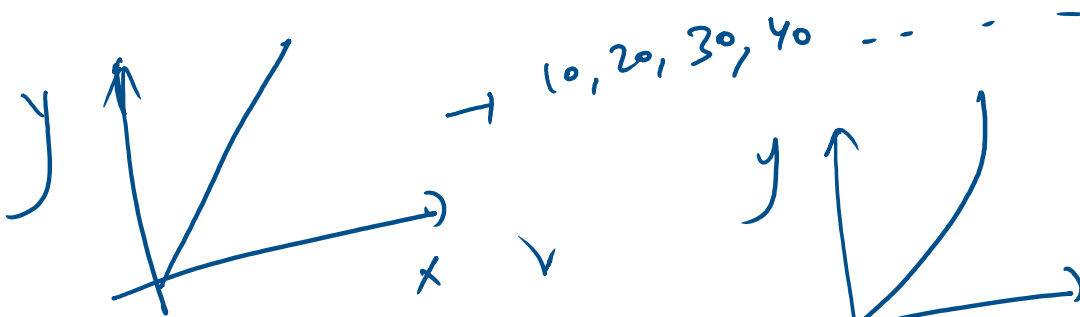
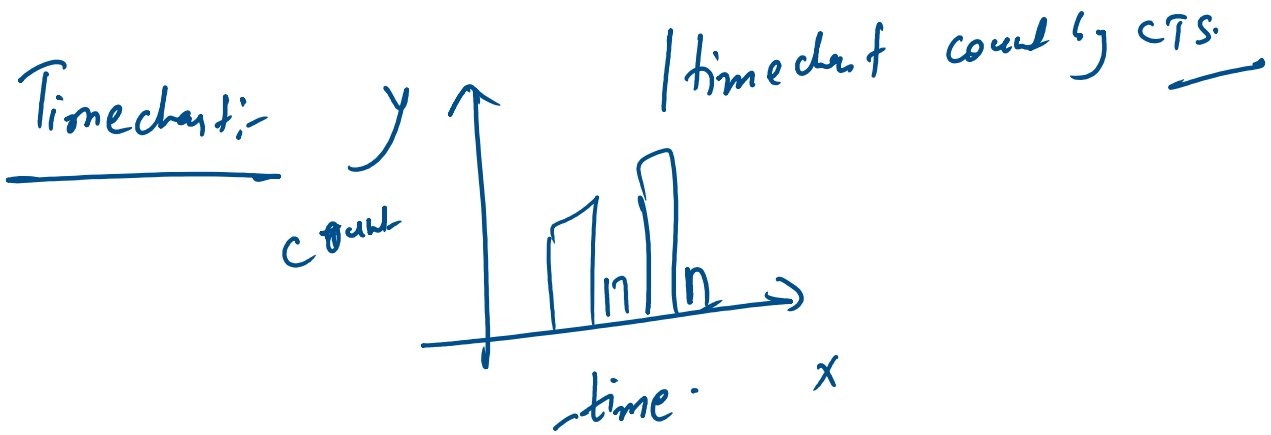


chart count by Current ticket state
 ↓ ↓
 y-axis x-axis





09-09-09 09:09:09

US - %m-%d-%y D₁ -
 EMEA - %y-%m-%d D₂ -
 AIX - %d-%m-%y (D₂ - D₁)

Strptime - function that will convert the
 date & time function to epoch format.

13-01-17 04:01 → Strptime, Strptime.
 ↓
13-Jan-2017 07:01 (Sunday)