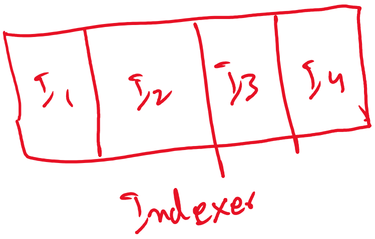
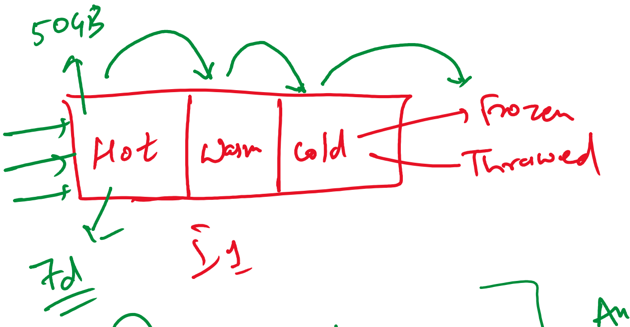
Day - 3

09 January 2025 10:17

Index:-





1. Age of Data.
2. Size of the Bucket.

→ Anyone cond^n is true.

1

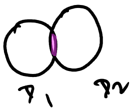
1. Append → Combine two dataset

2. Appendcols → Combine two dataset. In this both the Query will run parallely.

3. Appendpipe. → Output of the 1st dataset, will be the input for 2nd dataset.

```
index=_internal
| stats count by sourcetype, source
| appendpipe
   [| stats sum(count) as count by sourcetype
    | eval source="Total event in the respective source"]
| sort sourcetype
```

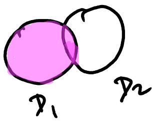
4. join → 1 Inner →



```
index=_internal
| stats count by sourcetype, source
| join type=inner sourcetype
   [search index=_internal
    | stats count by sourcetype, log_level]
```

2 left/outer.

E QO On--0



```
index=_internal
| stats count by sourcetype, source
| join type=left sourcetype
   [search index=_internal
    | stats count by sourcetype, log_level]
```

5. multikv → split the multiple field /multikv.

6. rex →

7. spath → XML & json dataset.

XML -

```
source="test_xml.txt" host="LAPTOP-CRDN7G9S"
index="main" sourcetype="vk_xml"
| spath output=yearpublished
path=purchases.book.title{@yearPublished}
```

Json -

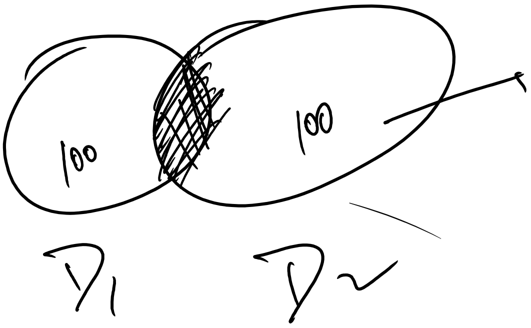
```
source="raw_nyc_phil_mod.json" host="LAPTOP-CRDN7G9S"
sourcetype="vn"
| spath path=programs{}.work{}.workTitle
```

8. tstats → Tsidx file → Timestamp file → Hit the tsidx file directly.

9. Addcoltotal. → Addition Column wise.

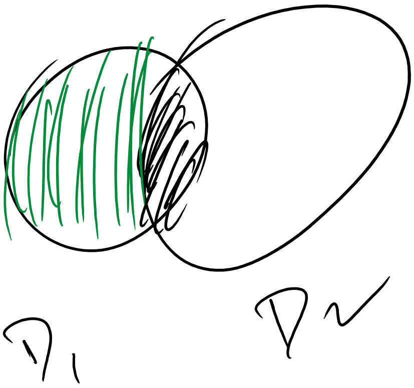
10. Addtotal. → Addition done row wise.

```
index=_internal
| chart count by sourcetype, source
| addcoltotals label=total labelfield=sourcetype
| addtotals fieldname=summmm
```



Sourcetype, | log level.

Sourcetype	Source	log level.



Common of D1

rex → Works on regular expression.