- (1) Field Summary.
- 2. Text function.
- (3) Conversion Junction.
- (4) Informational function.
- ( Statistical function!

- @ Multiku.
- (7) bin Command
  - (8) xyseries
  - 6 untable.
  - 6 foreach.

- (1) Patel hime fut (Shoftime ship time)
- (12) mv expand.
- (13) Coralense.
- (14) Studio (Input filter)
- (15) MLTK Toolkit.

- (1) Studio Pashsoard:
- (1) Basa Send
- D chain Sench
- 3 Savedsend
- 4) you Mat
- B) filter
- 5) Visuelization.
- (2.) Text functioni
  - 1) len length of the strip.
  - (2) Lower Strip to the lower case.
    - 3 upper 1 stig to tre upper Cone.
    - (4.) Etim 1 Frim the Certain Value four the stripfronte left certain Value with other (5) replace 4 Replace a certain Value with other
      - 1 Train fonte right side-

(6) < fring Trim for the nght.  (7) trim of Trim a certain value from the string.  (eplace - Lstr), Lreger, Creplacement?
2) Information function:  (is loot - True   false  (is double - Poulse Park Type  (is double - Value is integer  (is int - Value is their   Not  (is revalue is Number  (is sum - Value is strip   Nat  (is strip
4) Statistical Commandi
1) Stah
O steams Lab-
3 eventstats Commend.

Date & Time function—

1) Steptime - convert date & time value into epoch found

1) Steptime - Convert the epoc der into human realite

1) Steptime - Convert the epoc der into human realite

1) Steptime - Convert the epoc der into human realite

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoch found

1) Steptime - Convert the epoc der into epoc

US 7 7.m - 7.d - 7.7 EMEA 7 7.7-7.m - 7.9 MAC 7 7.d-7.m - 7.9 (D2-D1) X (D2-D1) X (P2-time-epoc)

index=main source="Sample\_tickets.csv"
| table time\_submitted , last\_resolved\_date
| eval last\_resolved\_epoc = strptime(last\_resolved\_date, "%d-%m-%y %H:%M")
| eval time\_submitted\_epoc = strptime(time\_submitted, "%d-%m-%y %H:%M")
| eval diff = last\_resolved\_epoc-time\_submitted\_epoc
| eval time\_submitted\_format = strftime(time\_submitted\_epoc, "%d-%B-%Y %A")
| eval diff\_format = strftime(diff, "%d")



index=main source="Sample\_tickets.csv" | stats count by severity, current\_ticket\_state | xyseries severity, current\_ticket\_state, count | fillnull

(7) Untable Command's

index=main source="Sample\_tickets.csv"
| stats count by severity, current\_ticket\_state
| xyseries severity, current\_ticket\_state, count
| untable severity, current\_ticket\_state, count

@Bin



index=main source="Sample\_tickets.csv"
| bin span=1mon \_time
| stats count by \_time, severity



| makeresults count=5 | streamstats count as counter | eval field1 = "col1", field2="col2" | mvcombine delim=";" counter | mvexpand counter

(10) Field Summary: - It will summarine the end tevery field in the filtered darket.

> index=main source="data.csv" | fieldsummary

A B C

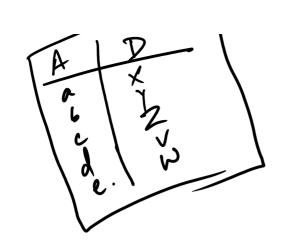
a s g

v

v

v

eval D = Coal esce (B1C)



eval P = Coal esce

Forend Commandi

Run the subsemed that will run in the iteration.

| makeresults

eval myfield1 = 5, myfield2 = 10

| foreach myfield\*

[ eval <<FIELD>> = '<<FIELD>>' + <<MATCHSTR>>]

3) Splunk MLTK Toolkiti-

Machine Learni 1-1 c orthur

1) liven Repersion.

2.) Multi liven Regnersion.

(1) Linea Repression: Cost of My House X Size of House ~ ~ (Veriable)

Cost of My House X 11 -- 8 Only one fretor is involed in Prediction. 1.) Mult linen Keg!

Cost of Home - Size of Proximity + Age + Ruild Quelly

Cost of Home - Size of Proximity + Age + Ruild Quelly Muriple fichers involved for ma Frediction. Cost of My la & lige of los - Siyle linen Regassion Cost of Con X Age, Kins, Diesel/Petrol/CNG, Auto/Monder ergine Multiple linear Repression. Python I Ml code Mgr. Predit 1 BJU Datasel Training Dats - Modelus kill is traited is

(701.)

Datasel
100 ever 7 cut date
(30'1.)

Fusher Frediction!