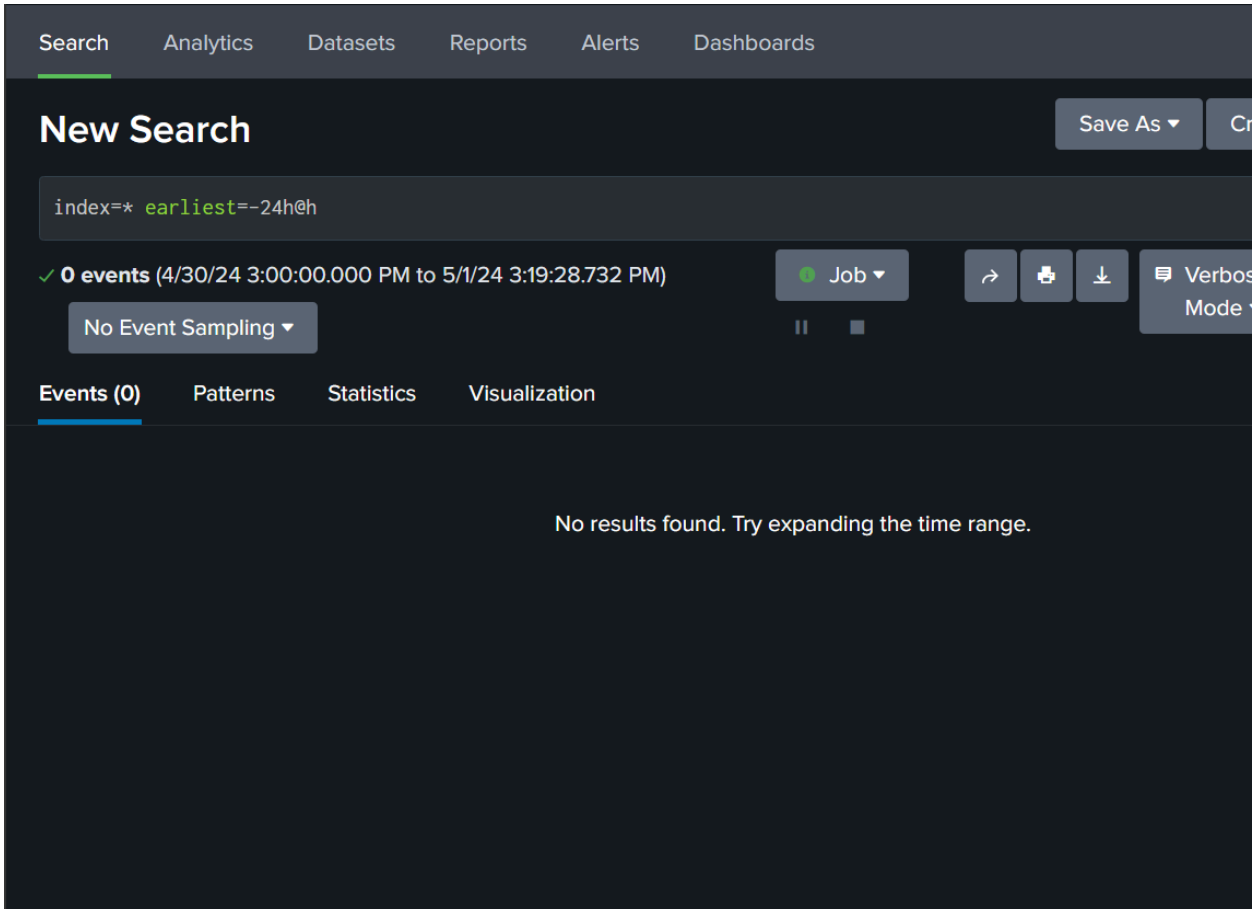
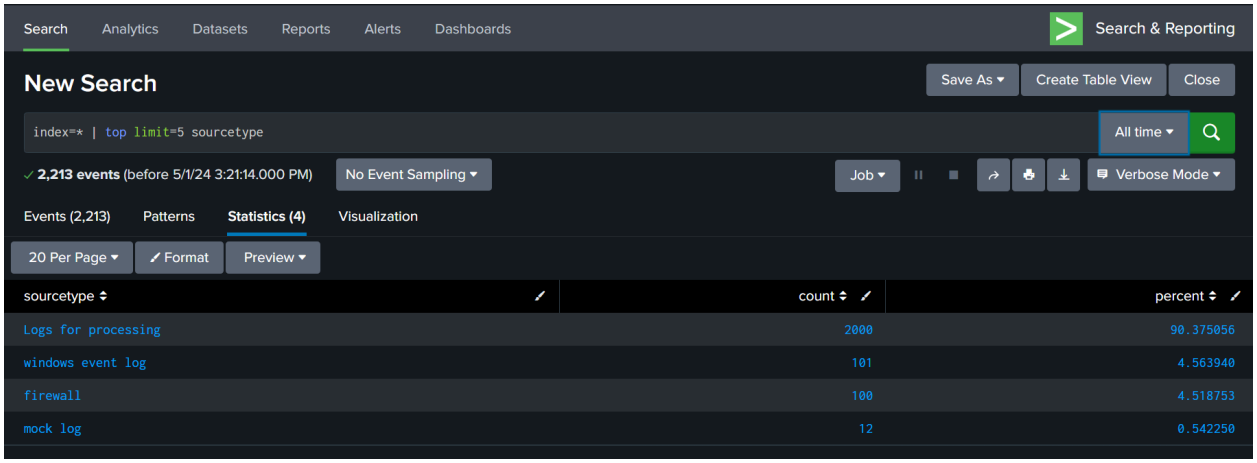
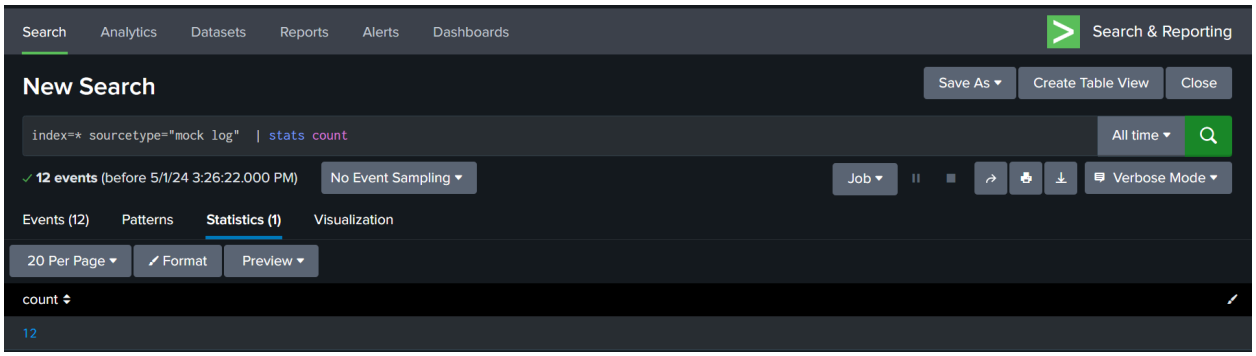
1.)


Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
index=* earliest=-24h@h
0 events (4/30/24 3:00:00.000 PM to 5/1/24 3:19:28.732 PM)
Job
No Event Sampling
Events (0)
Patterns
Statistics
Visualization
No results found. Try expanding the time range.

2.)

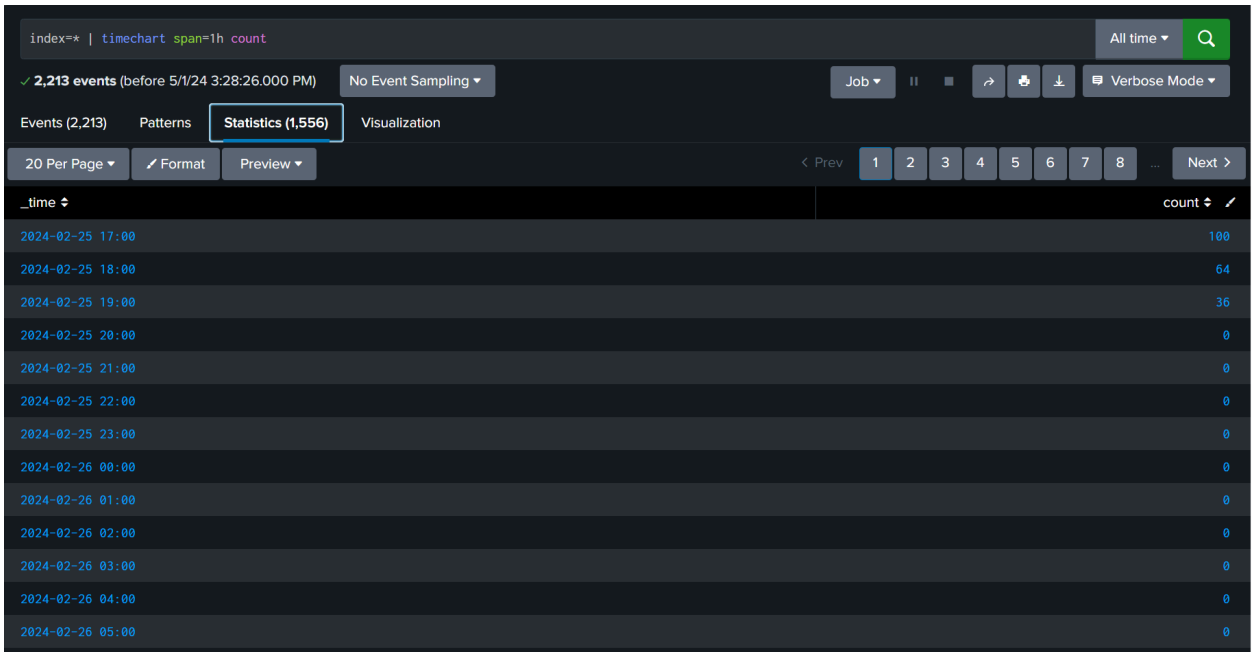

Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* | top limit=5 sourcetype
All time
2,213 events (before 5/1/24 3:21:14.000 PM)
No Event Sampling
Job
Verbose Mode
Events (2,213)
Patterns
Statistics (4)
Visualization
20 Per Page
Format
Preview
sourcetype
count
percent
Logs for processing 2000 90.375056
windows event log 101 4.563940
firewall 100 4.518753
mock log 12 0.542250

3.)

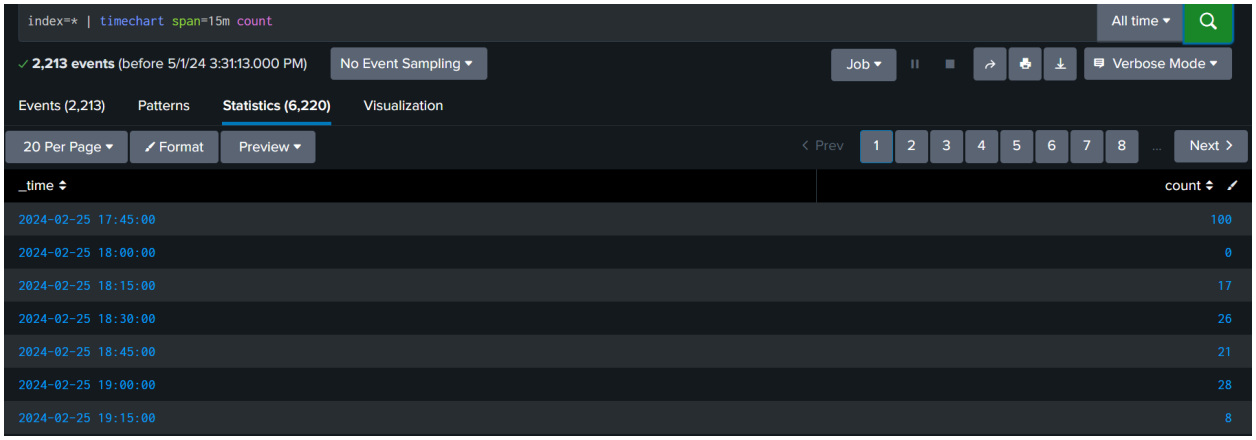

Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* sourcetype="mock log" | stats count
All time
12 events (before 5/1/24 3:26:22.000 PM)
No Event Sampling
Job
Verbose Mode
Events (12)
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
count
12

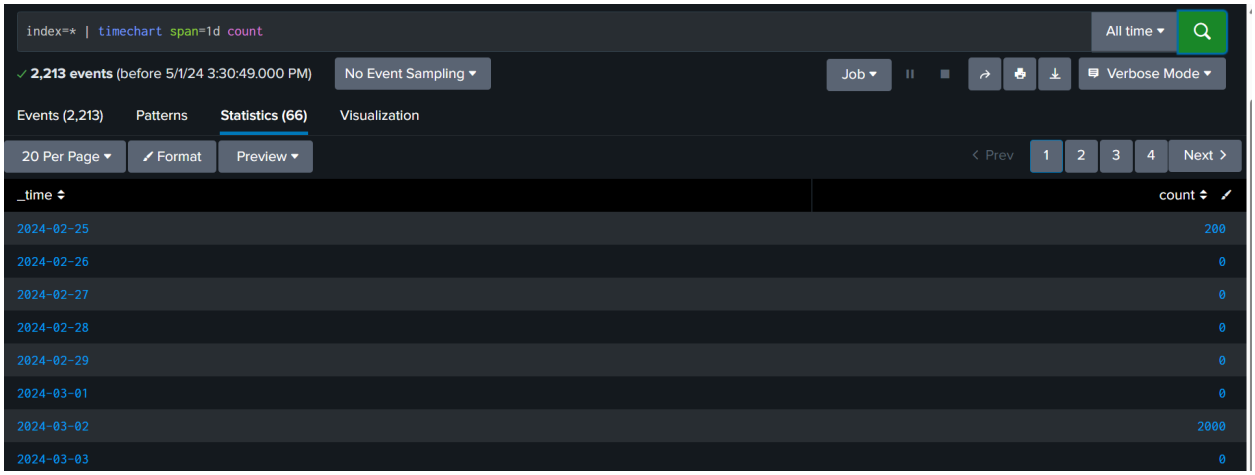
4.)

a.)

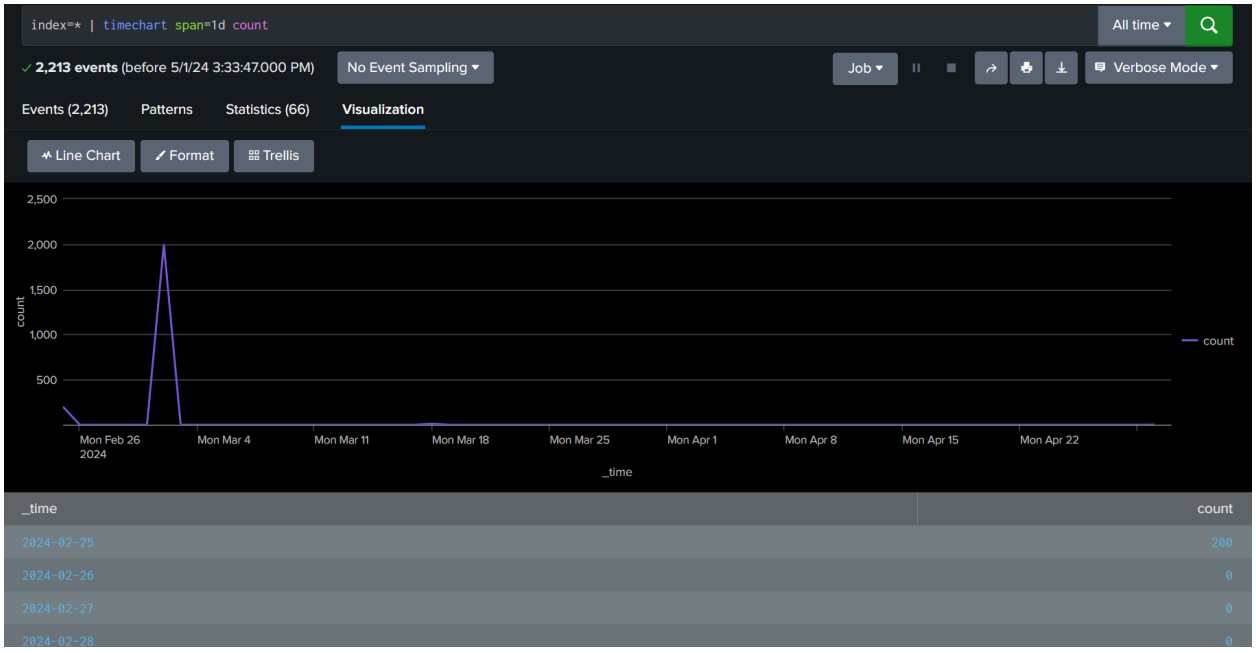

index=* | timechart span=1h count
All time
2,213 events (before 5/1/24 3:28:26.000 PM)
No Event Sampling
Job
Verbose Mode
Events (2,213)
Patterns
Statistics (1,556)
Visualization
20 Per Page
Format
Preview
Prev
1
2
3
4
5
6
7
8
Next
_time
count
2024-02-25 17:00 100
2024-02-25 18:00 64
2024-02-25 19:00 36
2024-02-25 20:00 0
2024-02-25 21:00 0
2024-02-25 22:00 0
2024-02-25 23:00 0
2024-02-26 00:00 0
2024-02-26 01:00 0
2024-02-26 02:00 0
2024-02-26 03:00 0
2024-02-26 04:00 0
2024-02-26 05:00 0

b.)


index=* | timechart span=15m count
All time
2,213 events (before 5/1/24 3:31:13.000 PM)
No Event Sampling
Job
Verbose Mode
Events (2,213)
Patterns
Statistics (6,220)
Visualization
20 Per Page
Format
Preview
Prev
1 2 3 4 5 6 7 8 ...
Next
_time
count
2024-02-25 17:45:00 100
2024-02-25 18:00:00 0
2024-02-25 18:15:00 17
2024-02-25 18:30:00 26
2024-02-25 18:45:00 21
2024-02-25 19:00:00 28
2024-02-25 19:15:00 8


index=* | timechart span=1d count
All time
2,213 events (before 5/1/24 3:30:49.000 PM)
No Event Sampling
Job
Verbose Mode
Events (2,213)
Patterns
Statistics (66)
Visualization
20 Per Page
Format
Preview
Prev
1 2 3 4
Next
_time
count
2024-02-25 200
2024-02-26 0
2024-02-27 0
2024-02-28 0
2024-02-29 0
2024-03-01 0
2024-03-02 2000
2024-03-03 0

c.)


index=* | timechart span=1d count
All time
2,213 events (before 5/1/24 3:33:47.000 PM)
No Event Sampling
Job
Verbose Mode
Events (2,213)
Patterns
Statistics (66)
Visualization
Line Chart
Format
Trellis
2,500
2,000
1,500
1,000
500
count
Mon Feb 26 2024
Mon Mar 4
Mon Mar 11
Mon Mar 18
Mon Mar 25
Mon Apr 1
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time
count
_time
count
2024-02-25 200
2024-02-26 0
2024-02-27 0
2024-02-28 0