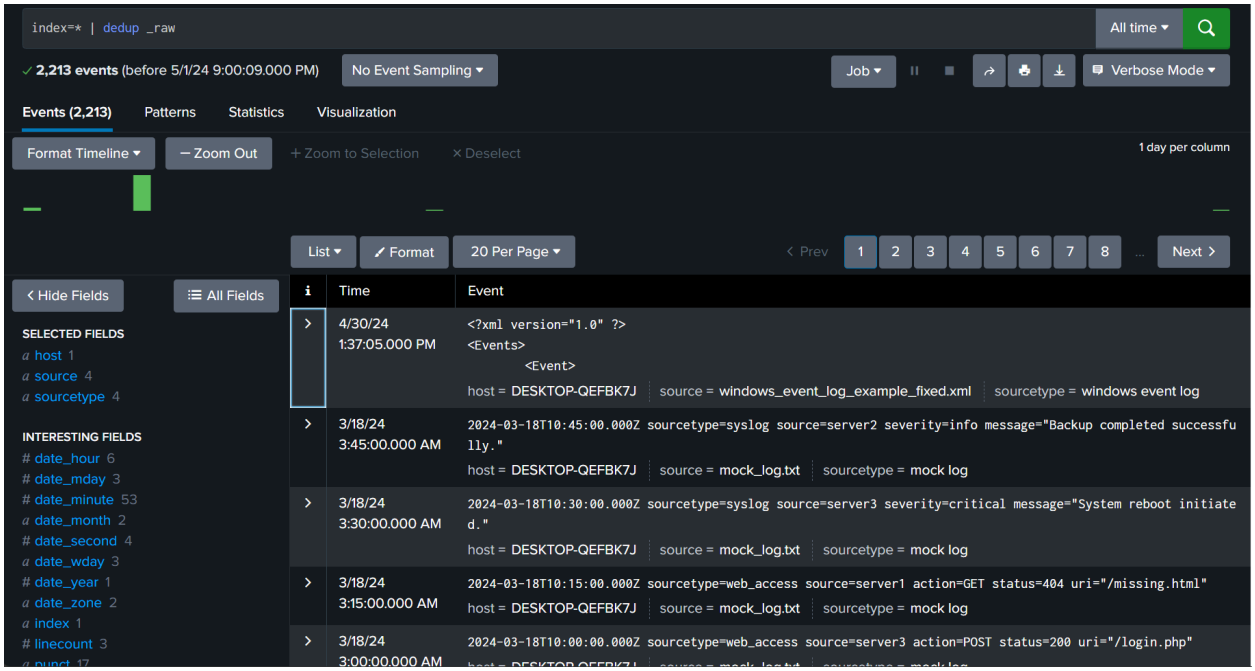
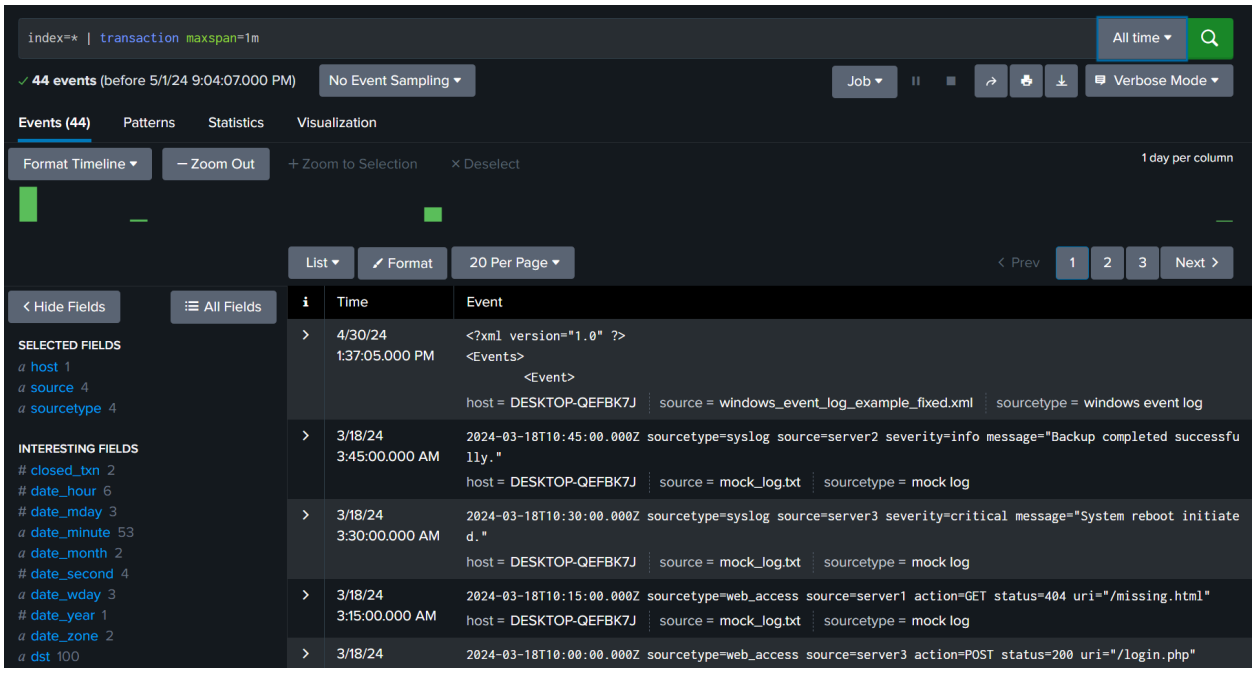
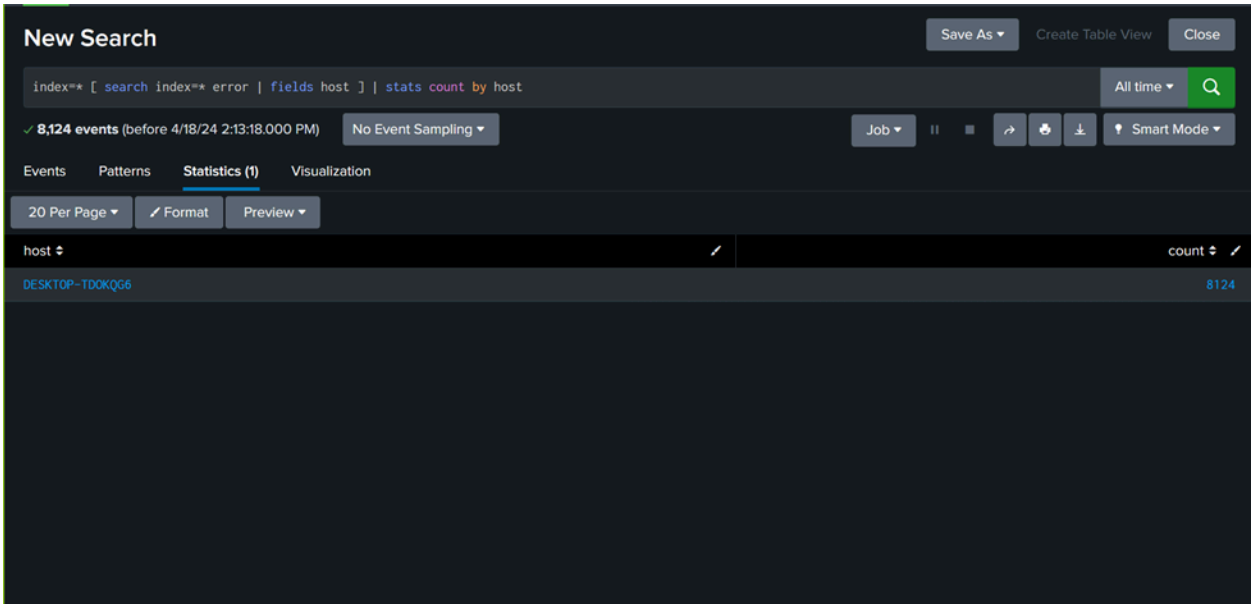
1.)


index=* | dedup _raw
All time
2,213 events (before 5/1/24 9:00:09.000 PM)
No Event Sampling
Job
Verbose Mode
Events (2,213)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 day per column
List
Format
20 Per Page
Prev 1 2 3 4 5 6 7 8 Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 4
a sourcetype 4
INTERESTING FIELDS
date_hour 6
date_mday 3
date_minute 53
a date_month 2
date_second 4
a date_wday 3
date_year 1
a date_zone 2
a index 1
linecount 3
Time
Event
4/30/24 1:37:05.000 PM
<?xml version="1.0" ?>
<Events>
<Event>
host = DESKTOP-QEFBK7J source = windows_event_log_example_fixed.xml sourcetype = windows event log
3/18/24 3:45:00.000 AM
2024-03-18T10:45:00.000Z sourcetype=syslog source=server2 severity=info message="Backup completed successfully."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 3:30:00.000 AM
2024-03-18T10:30:00.000Z sourcetype=syslog source=server3 severity=critical message="System reboot initiated."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 3:15:00.000 AM
2024-03-18T10:15:00.000Z sourcetype=web_access source=server1 action=GET status=404 uri="/missing.html"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 3:00:00.000 AM
2024-03-18T10:00:00.000Z sourcetype=web_access source=server3 action=POST status=200 uri="/login.php"

2.)


index=* | transaction maxspan=1m
All time
44 events (before 5/1/24 9:04:07.000 PM)
No Event Sampling
Job
Verbose Mode
Events (44)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 day per column
List
Format
20 Per Page
Prev 1 2 3 Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 4
a sourcetype 4
INTERESTING FIELDS
closed_txn 2
date_hour 6
date_mday 3
a date_minute 53
a date_month 2
date_second 4
a date_wday 3
date_year 1
a date_zone 2
a dst 100
Time
Event
4/30/24 1:37:05.000 PM
<?xml version="1.0" ?>
<Events>
<Event>
host = DESKTOP-QEFBK7J source = windows_event_log_example_fixed.xml sourcetype = windows event log
3/18/24 3:45:00.000 AM
2024-03-18T10:45:00.000Z sourcetype=syslog source=server2 severity=info message="Backup completed successfully."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 3:30:00.000 AM
2024-03-18T10:30:00.000Z sourcetype=syslog source=server3 severity=critical message="System reboot initiated."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 3:15:00.000 AM
2024-03-18T10:15:00.000Z sourcetype=web_access source=server1 action=GET status=404 uri="/missing.html"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24
2024-03-18T10:00:00.000Z sourcetype=web_access source=server3 action=POST status=200 uri="/login.php"

3.)


New Search
Save As
Create Table View
Close
index=* [search index=* error | fields host] | stats count by host
All time
8,124 events (before 4/18/24 2:13:18.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
host
count
DESKTOP-TDOKQG6
8124

4.)