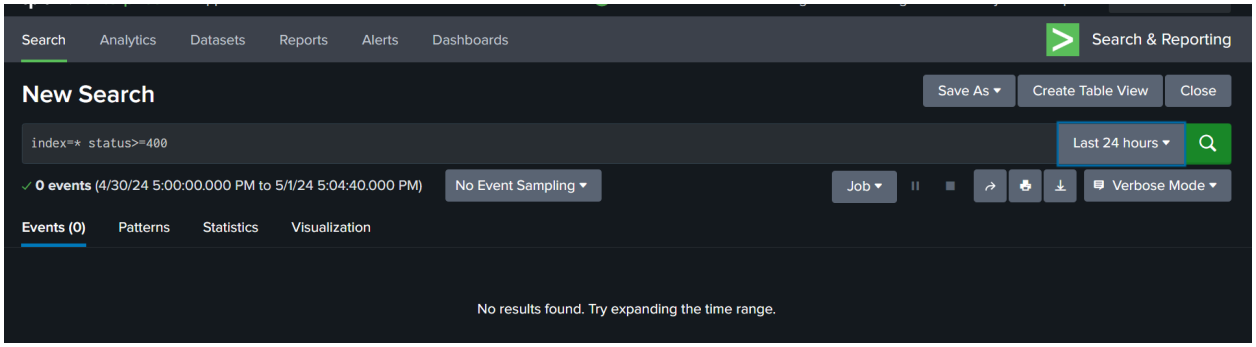
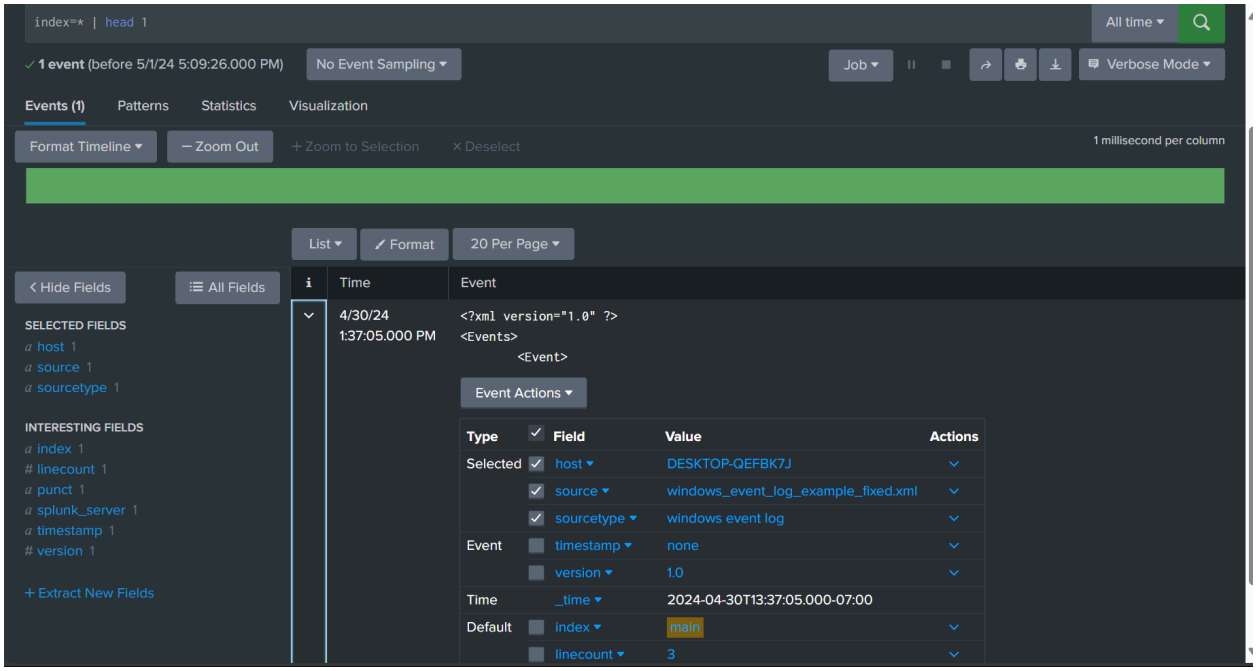
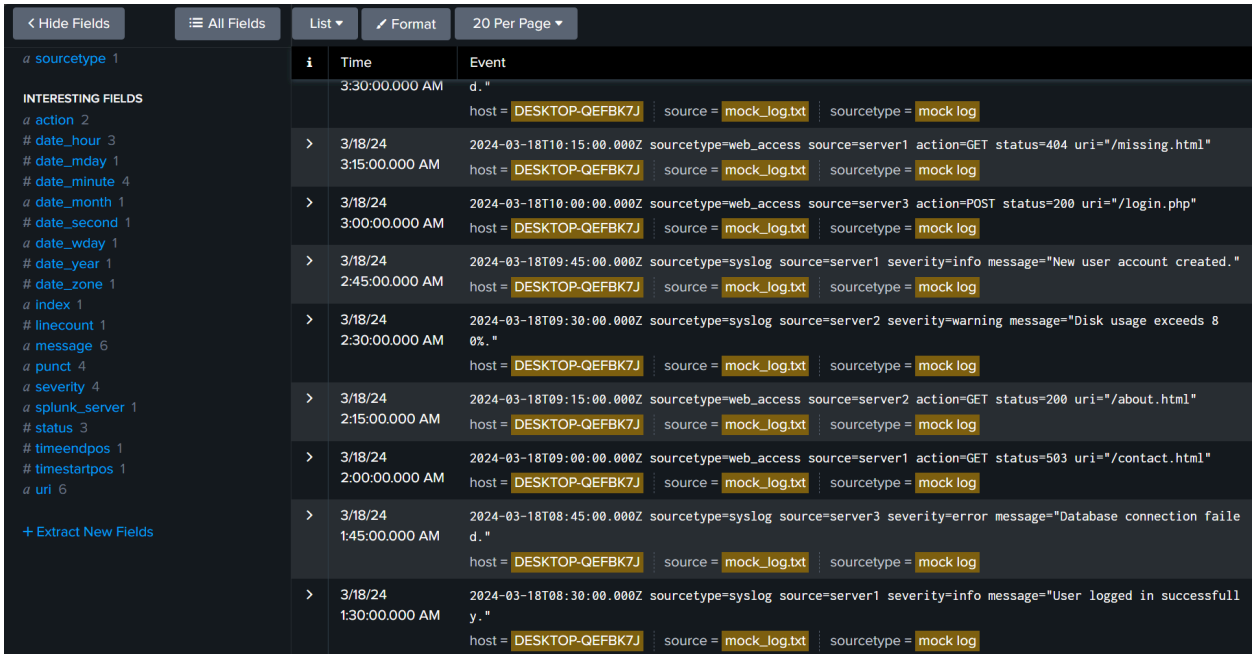
1.)

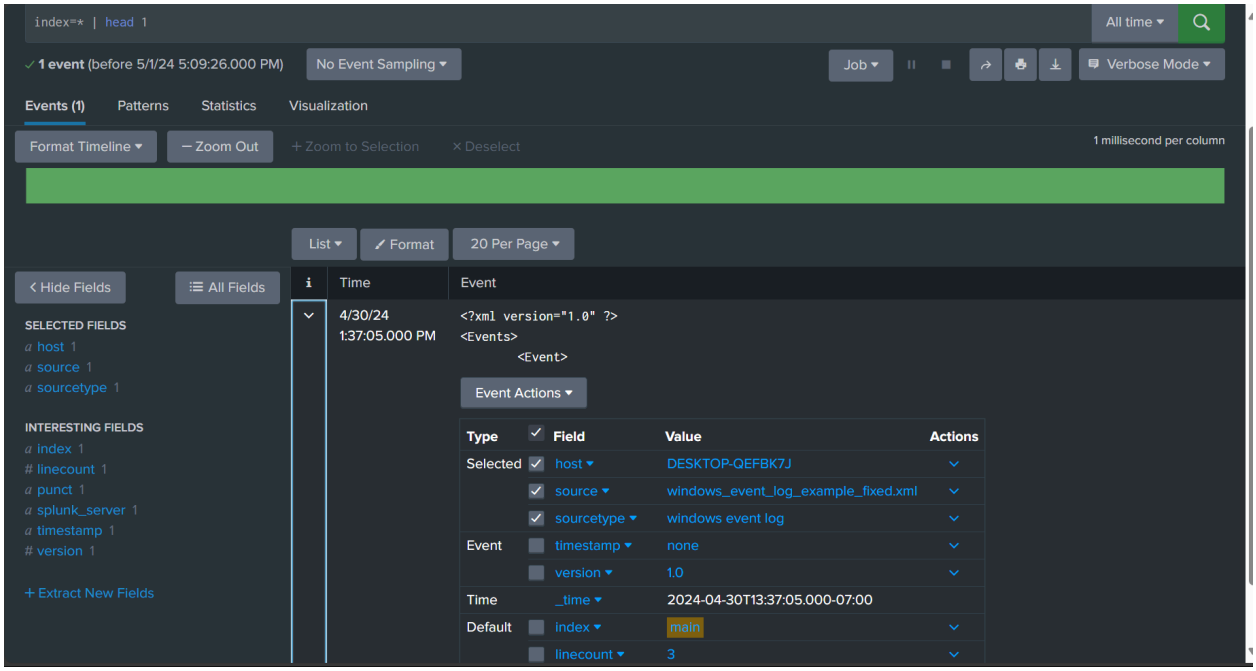

Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* status>=400
Last 24 hours
0 events (4/30/24 5:00:00.000 PM to 5/1/24 5:04:40.000 PM)
No Event Sampling
Job
Verbose Mode
Events (0)
Patterns
Statistics
Visualization
No results found. Try expanding the time range.

2.)


index=* | head 1
All time
1 event (before 5/1/24 5:09:26.000 PM)
No Event Sampling
Job
Verbose Mode
Events (1)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 millisecond per column
List
Format
20 Per Page
Hide Fields
All Fields
Time
Event
4/30/24
1:37:05.000 PM
<?xml version="1.0" ?>
<Events>
<Event>
Event Actions
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a index 1
# linecount 1
a punct 1
a splunk_server 1
a timestamp 1
# version 1
+ Extract New Fields
Type
Field
Value
Actions
Selected
host
DESKTOP-QEFBK7J
source
windows_event_log_example_fixed.xml
sourcetype
windows event log
Event
timestamp
none
version
1.0
Time
_time
2024-04-30T13:37:05.000-07:00
Default
index
main
linecount
3

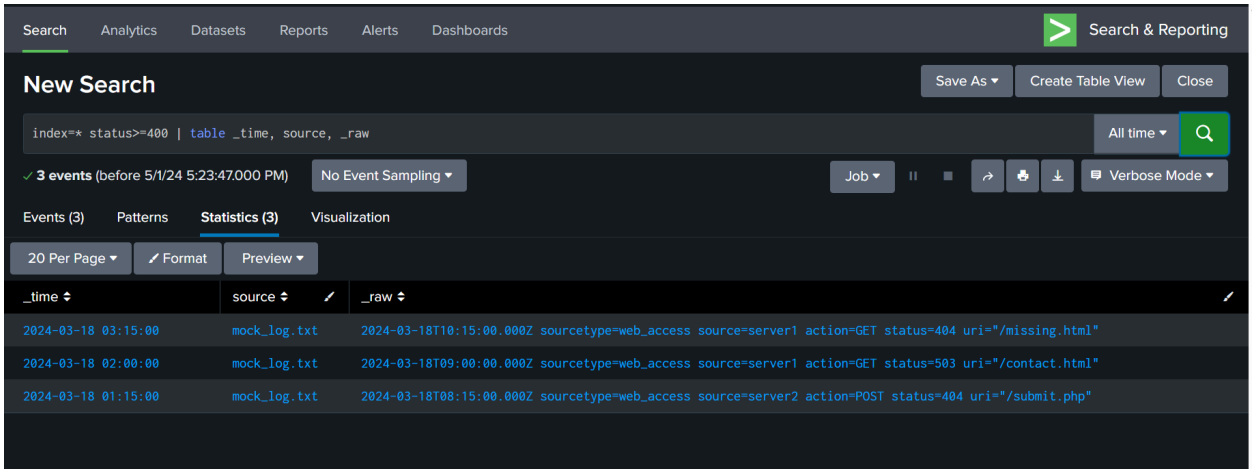
3.)


Hide Fields
All Fields
List
Format
20 Per Page
a sourcetype 1
INTERESTING FIELDS
a action 2
# date_hour 3
# date_mday 1
# date_minute 4
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
# date_zone 1
a index 1
# linecount 1
a message 6
a punct 4
a severity 4
a splunk_server 1
# status 3
# timeendpos 1
# timestartpos 1
a uri 6
+ Extract New Fields
Time
Event
3:30:00.000 AM
d."
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"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 2:45:00.000 AM
2024-03-18T09:45:00.000Z sourcetype=syslog source=server1 severity=info message="New user account created."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 2:30:00.000 AM
2024-03-18T09:30:00.000Z sourcetype=syslog source=server2 severity=warning message="Disk usage exceeds 8 0%."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 2:15:00.000 AM
2024-03-18T09:15:00.000Z sourcetype=web_access source=server2 action=GET status=200 uri="/about.html"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 2:00:00.000 AM
2024-03-18T09:00:00.000Z sourcetype=web_access source=server1 action=GET status=503 uri="/contact.html"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 1:45:00.000 AM
2024-03-18T08:45:00.000Z sourcetype=syslog source=server3 severity=error message="Database connection faile d."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 1:30:00.000 AM
2024-03-18T08:30:00.000Z sourcetype=syslog source=server1 severity=info message="User logged in successfull y."
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log

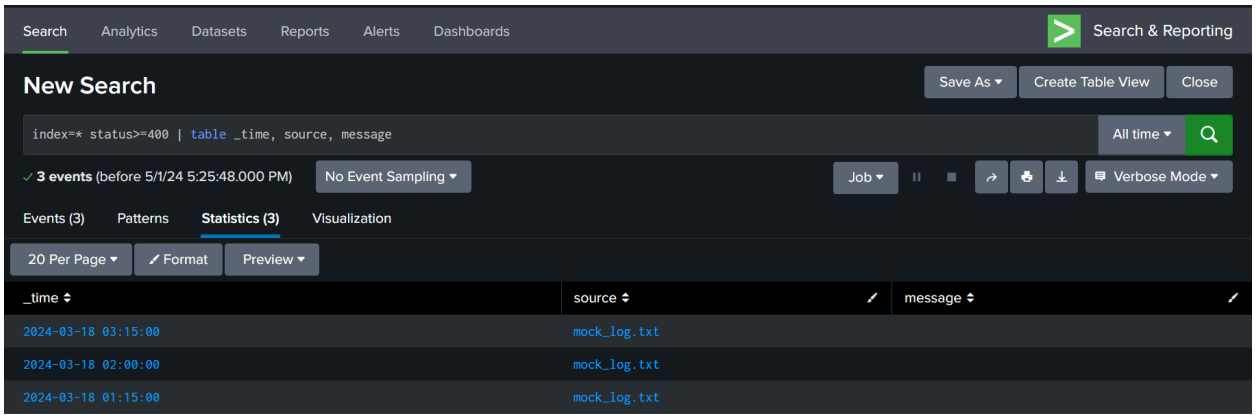

index=* | head 1
All time
1 event (before 5/1/24 5:09:26.000 PM)
No Event Sampling
Job
Verbose Mode
Events (1)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 millisecond per column
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a index 1
# linecount 1
a punct 1
a splunk_server 1
a timestamp 1
# version 1
+ Extract New Fields
Time
Event
4/30/24 1:37:05.000 PM
<?xml version="1.0" ?>
<Events>
<Event>
Event Actions
Type
Field
Value
Actions
Selected
host
DESKTOP-QEFBK7J
source
windows_event_log_example_fixed.xml
sourcetype
windows event log
Event
timestamp
none
version
1.0
Time
_time
2024-04-30T13:37:05.000-07:00
Default
index
main
linecount
3

3.)

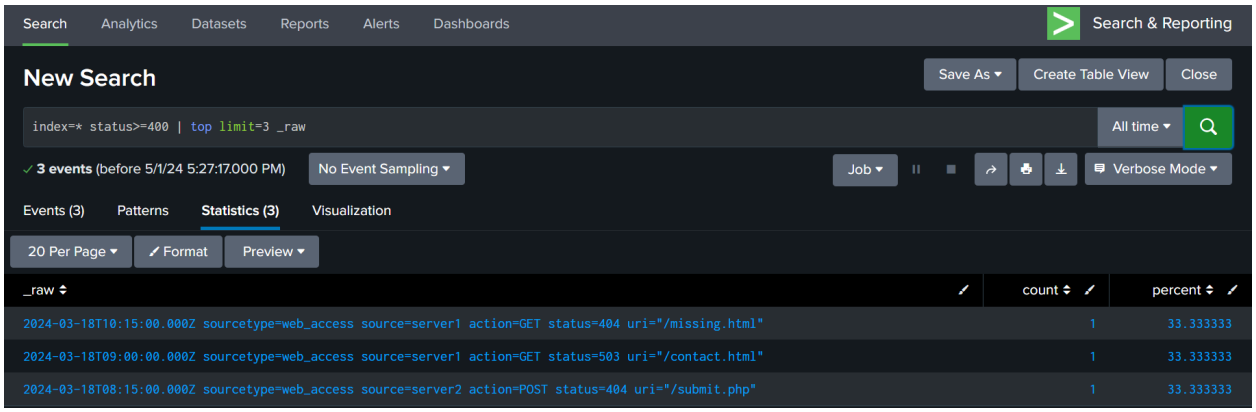
a.)


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* status>=400 | table _time, source, _raw
All time
3 events (before 5/1/24 5:23:47.000 PM)
No Event Sampling
Job
Verbose Mode
Events (3)
Patterns
Statistics (3)
Visualization
20 Per Page
Format
Preview
_time
source
_raw
2024-03-18 03:15:00
mock_log.txt
2024-03-18T10:15:00.000Z sourcetype=web_access source=server1 action=GET status=404 uri="/missing.html"
2024-03-18 02:00:00
mock_log.txt
2024-03-18T09:00:00.000Z sourcetype=web_access source=server1 action=GET status=503 uri="/contact.html"
2024-03-18 01:15:00
mock_log.txt
2024-03-18T08:15:00.000Z sourcetype=web_access source=server2 action=POST status=404 uri="/submit.php"

b.)


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* status>=400 | table _time, source, message
All time
3 events (before 5/1/24 5:25:48.000 PM)
No Event Sampling
Job
Verbose Mode
Events (3)
Patterns
Statistics (3)
Visualization
20 Per Page
Format
Preview
_time
source
message
2024-03-18 03:15:00
mock_log.txt
2024-03-18 02:00:00
mock_log.txt
2024-03-18 01:15:00
mock_log.txt

4.)


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* status>=400 | top limit=3 _raw
All time
3 events (before 5/1/24 5:27:17.000 PM)
No Event Sampling
Job
Verbose Mode
Events (3)
Patterns
Statistics (3)
Visualization
20 Per Page
Format
Preview
_raw
count
percent
2024-03-18T10:15:00.000Z sourcetype=web_access source=server1 action=GET status=404 uri="/missing.html"
1
33.333333
2024-03-18T09:00:00.000Z sourcetype=web_access source=server1 action=GET status=503 uri="/contact.html"
1
33.333333
2024-03-18T08:15:00.000Z sourcetype=web_access source=server2 action=POST status=404 uri="/submit.php"
1
33.333333