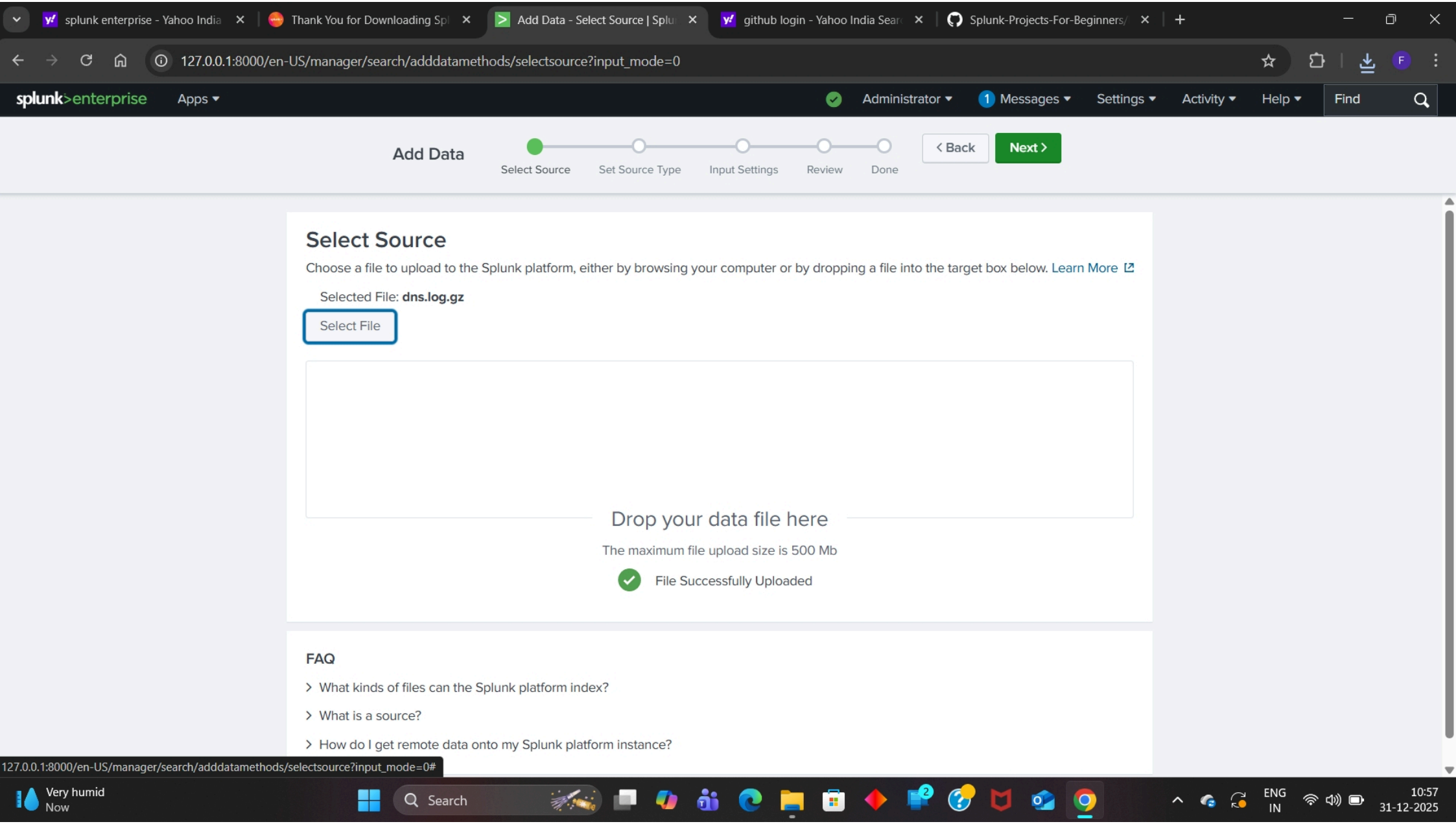
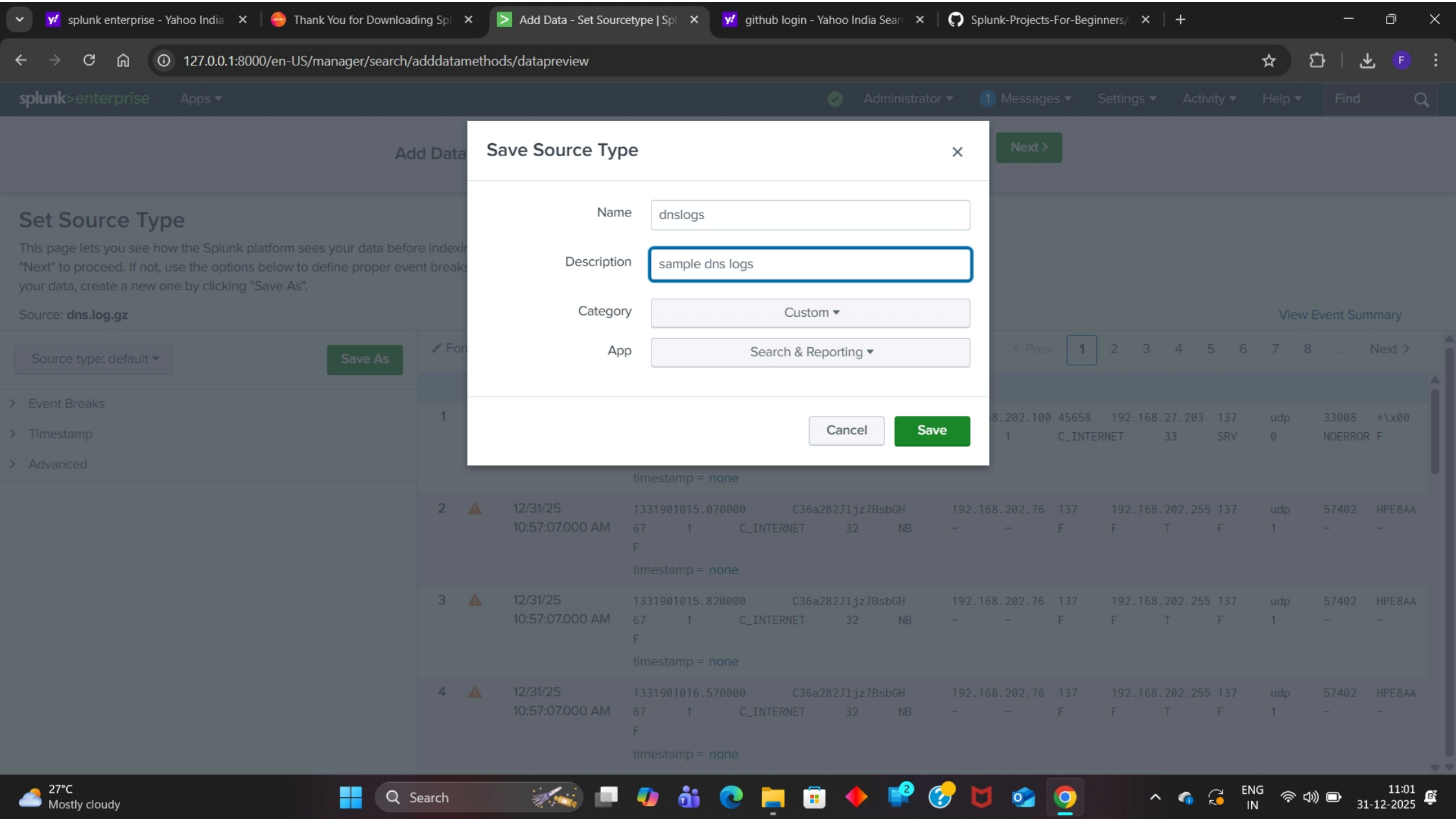
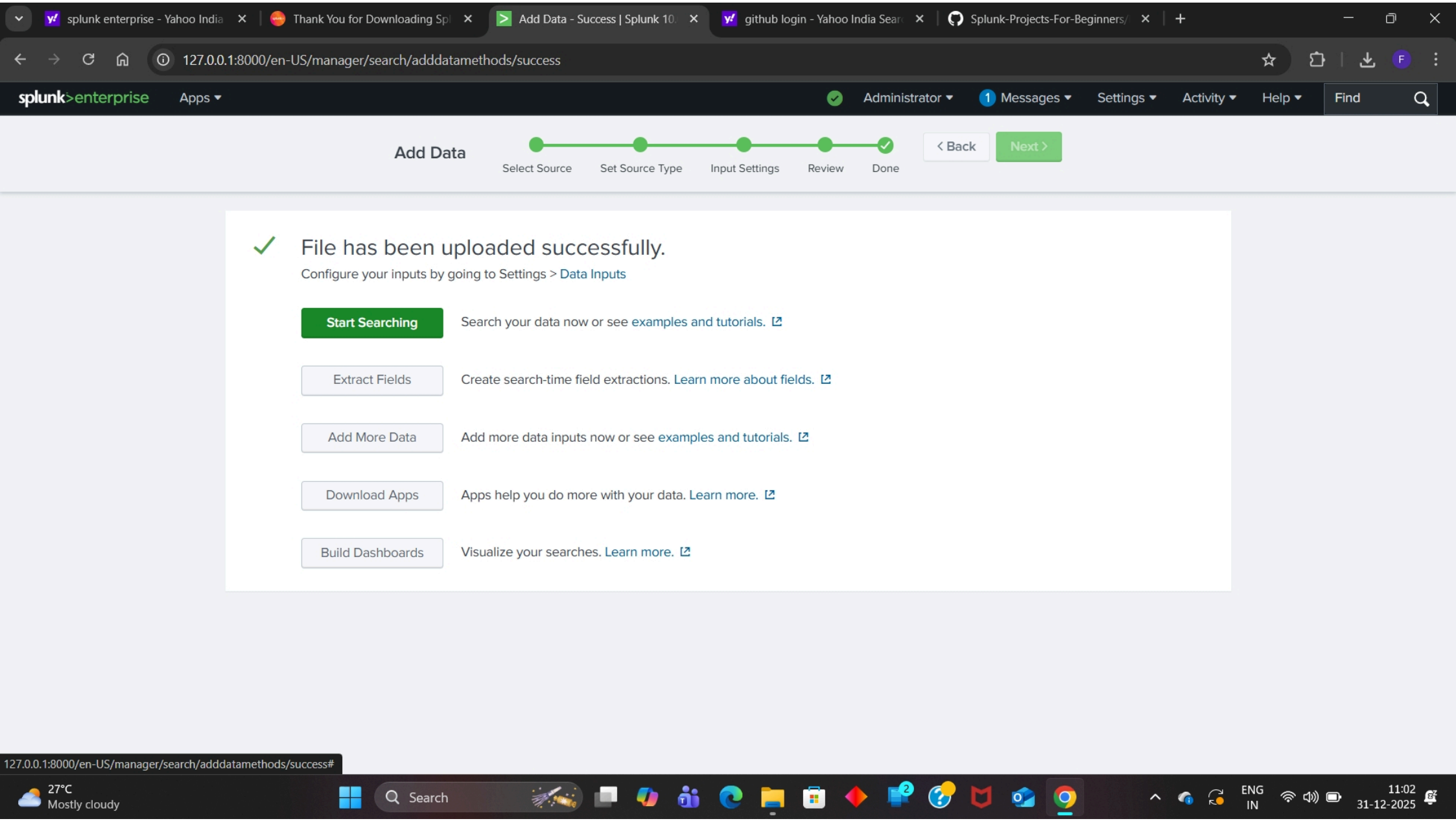
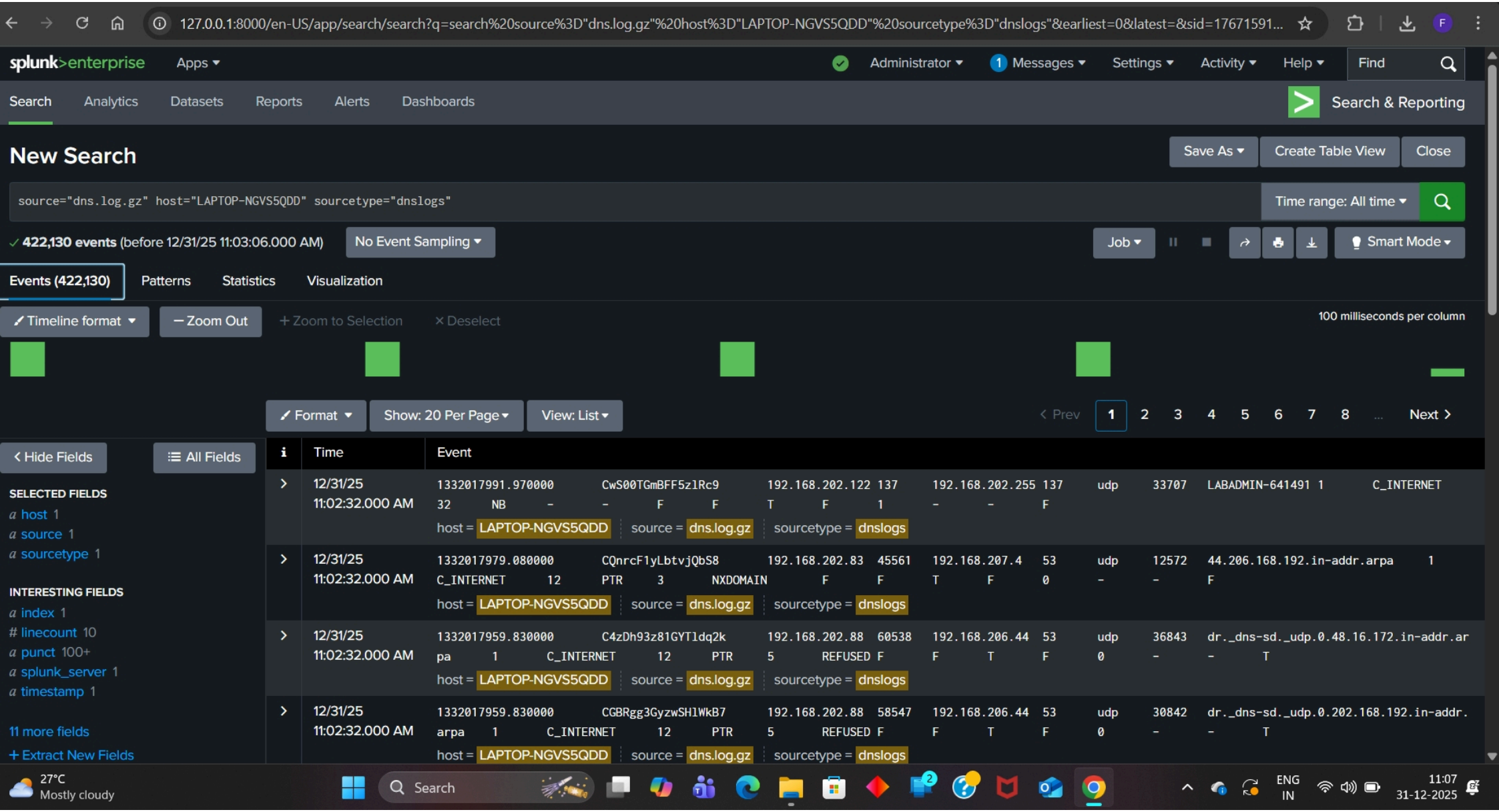
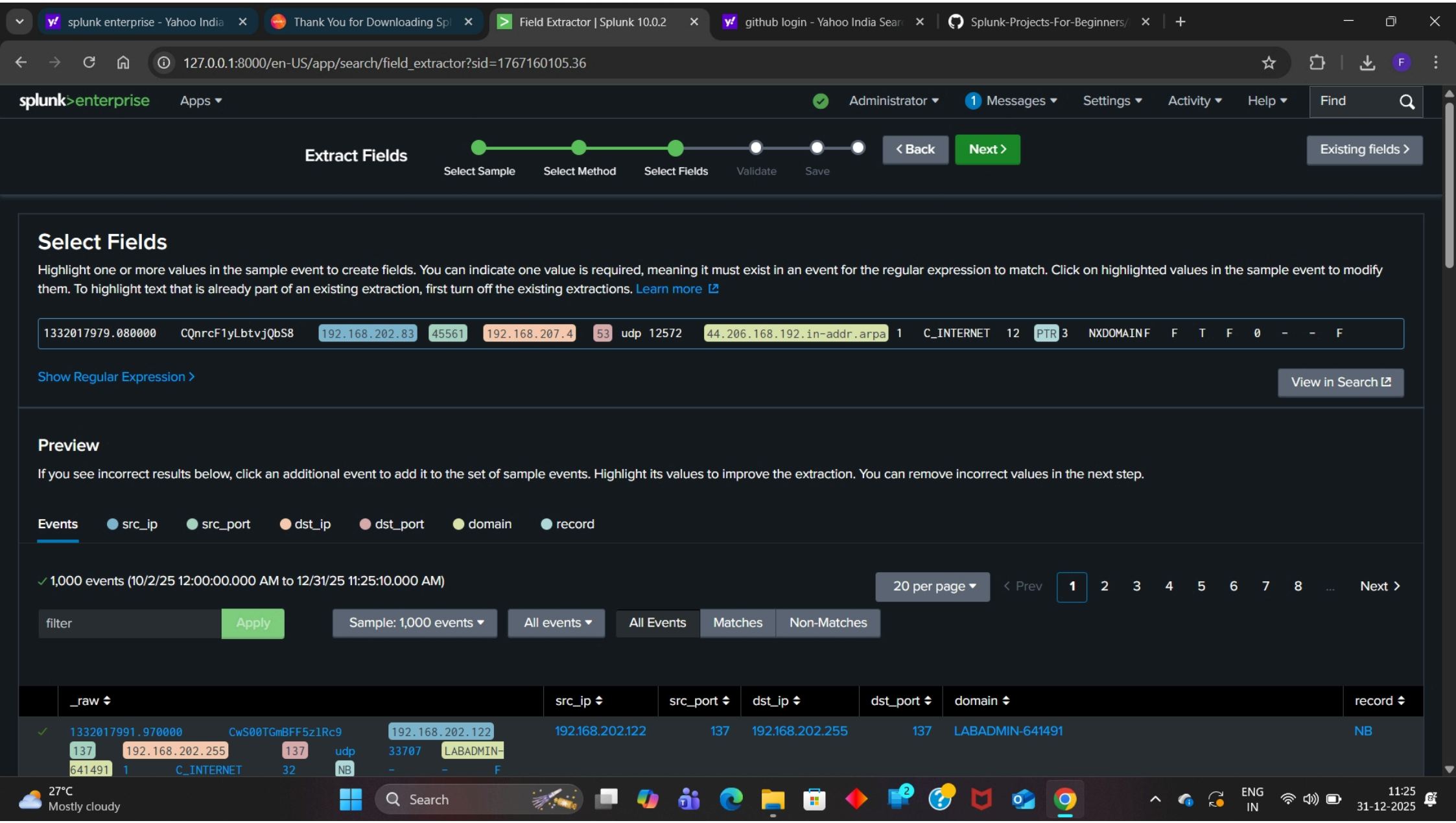
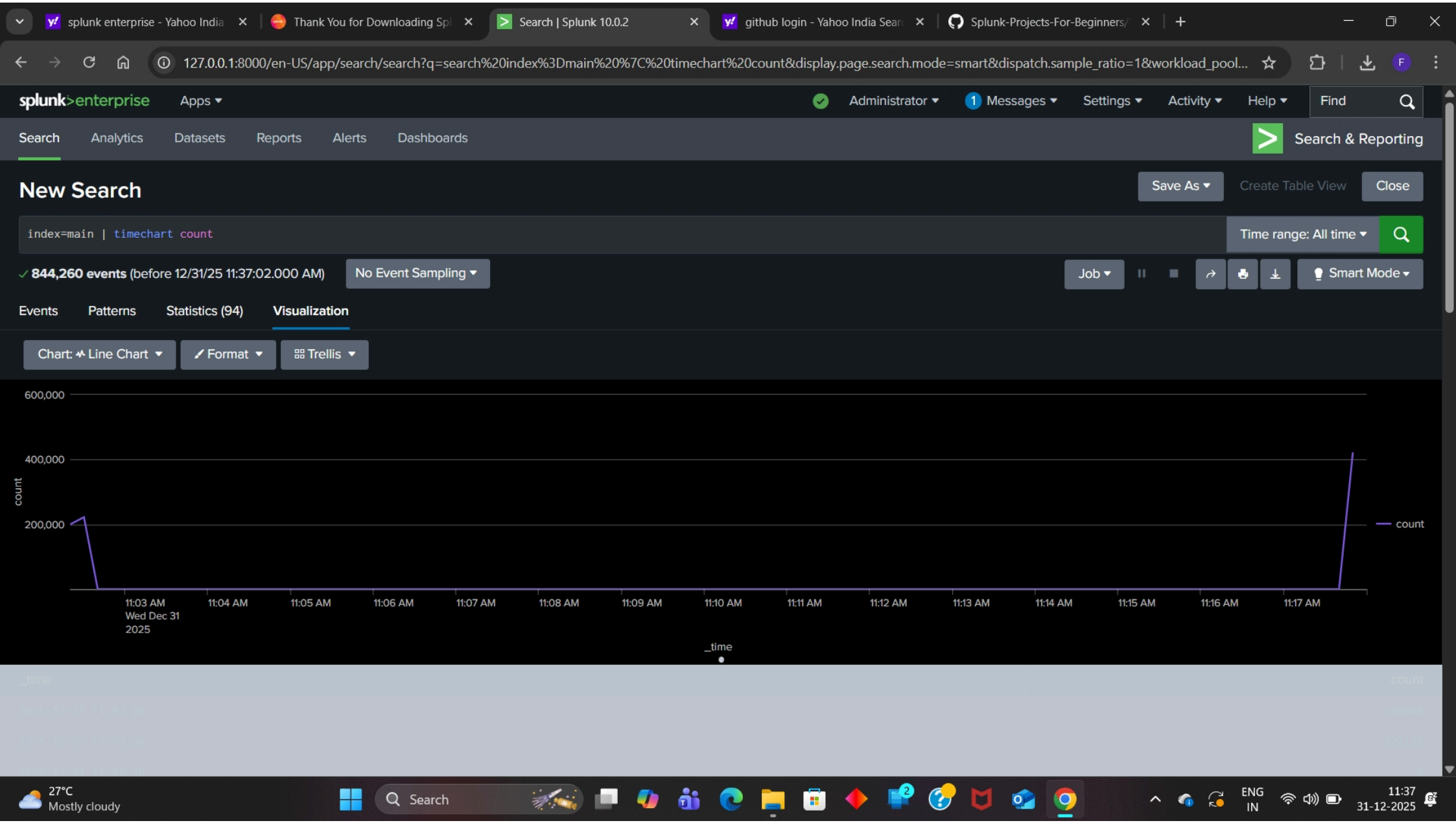

splunk enterprise - Yahoo India
Thank You for Downloading Spl
Add Data - Select Source | Splu
github login - Yahoo India Sear
Splunk-Projects-For-Beginners/
127.0.0.1:8000/en-US/manager/search/adddatamethods/selectsource?input_mode=0
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Select Source
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More
Selected File: dns.log.gz
Select File
Drop your data file here
The maximum file upload size is 500 Mb
File Successfully Uploaded
FAQ
What kinds of files can the Splunk platform index?
What is a source?
How do I get remote data onto my Splunk platform instance?
127.0.0.1:8000/en-US/manager/search/adddatamethods/selectsource?input_mode=0#
Very humid
Now
Search
ENG
IN
10:57
31-12-2025


splunk enterprise - Yahoo India
Thank You for Downloading Spl
Add Data - Set Sourcetype | Spl
github login - Yahoo India Sear
Splunk-Projects-For-Beginners/
127.0.0.1:8000/en-US/manager/search/adddatamethods/datapreview
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Next >
Set Source Type
This page lets you see how the Splunk platform sees your data before indexi
"Next" to proceed. If not, use the options below to define proper event breaks
your data, create a new one by clicking "Save As".
Source: dns.log.gz
View Event Summary
Source type: default
Save As
Event Breaks
Timestamp
Advanced
Prev 1 2 3 4 5 6 7 8 Next >
Save Source Type
Name
dnslogs
Description
sample dns logs
Category
Custom
App
Search & Reporting
Cancel
Save
timestamp = none
12/31/25 10:57:07.000 AM
1331901015.070000 C36a282J1jz7BsbGH 192.168.202.76 137 192.168.202.255 137 udp 57402 HPE8AA
1331901015.820000 C36a282J1jz7BsbGH 192.168.202.76 137 192.168.202.255 137 udp 57402 HPE8AA
1331901016.570000 C36a282J1jz7BsbGH 192.168.202.76 137 192.168.202.255 137 udp 57402 HPE8AA
27°C
Mostly cloudy
Search
ENG
IN
11:01
31-12-2025


splunk enterprise - Yahoo India
Thank You for Downloading Spl
Add Data - Success | Splunk 10.
github login - Yahoo India Sear
Splunk-Projects-For-Beginners/
127.0.0.1:8000/en-US/manager/search/adddatamethods/success
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Extract Fields
Create search-time field extractions. Learn more about fields.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.
127.0.0.1:8000/en-US/manager/search/adddatamethods/success#
27°C
Mostly cloudy
Search
ENG
IN
11:02
31-12-2025


127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D"dns.log.gz"%20host%3D"LAPTOP-NGVS5QDD"%20sourcetype%3D"dnslogs"&earliest=0&latest=&sid=17671591...
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="dns.log.gz" host="LAPTOP-NGVS5QDD" sourcetype="dnslogs"
Time range: All time
422,130 events (before 12/31/25 11:03:06.000 AM)
No Event Sampling
Job
Smart Mode
Events (422,130)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
Format
Show: 20 Per Page
View: List
Prev
1 2 3 4 5 6 7 8 ... Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a index 1
# linecount 10
a punct 100+
a splunk_server 1
a timestamp 1
11 more fields
Extract New Fields
Time
Event
12/31/25 11:02:32.000 AM
1332017991.970000 CwS00TGmBFF5zlRc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_INTERNET 32 NB - - F F T F 1 - - F
host = LAPTOP-NGVS5QDD source = dns.log.gz sourcetype = dnslogs
12/31/25 11:02:32.000 AM
1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NXDOMAIN F F T F 0 - - F
host = LAPTOP-NGVS5QDD source = dns.log.gz sourcetype = dnslogs
12/31/25 11:02:32.000 AM
1332017959.830000 C4zDh93z81GYTldq2k 192.168.202.88 60538 192.168.206.44 53 udp 36843 dr._dns-sd._udp.0.48.16.172.in-addr.ar pa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T
host = LAPTOP-NGVS5QDD source = dns.log.gz sourcetype = dnslogs
12/31/25 11:02:32.000 AM
1332017959.830000 CGBRgg3GyzwSH1WkB7 192.168.202.88 58547 192.168.206.44 53 udp 30842 dr._dns-sd._udp.0.202.168.192.in-addr. arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T
host = LAPTOP-NGVS5QDD source = dns.log.gz sourcetype = dnslogs
27°C Mostly cloudy
Search
ENG IN
11:07 31-12-2025


splunk enterprise - Yahoo India
Thank You for Downloading Spl
Field Extractor | Splunk 10.0.2
github login - Yahoo India Sear
Splunk-Projects-For-Beginners/
127.0.0.1:8000/en-US/app/search/field_extractor?sid=1767160105.36
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Extract Fields
Select Sample
Select Method
Select Fields
Validate
Save
Back
Next
Existing fields
Select Fields
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more
1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NXDOMAIN F T F 0 - - F
Show Regular Expression
View in Search
Preview
If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.
Events
src_ip
src_port
dst_ip
dst_port
domain
record
1,000 events (10/2/25 12:00:00.000 AM to 12/31/25 11:25:10.000 AM)
20 per page
Prev
1
2
3
4
5
6
7
8
Next
filter
Apply
Sample: 1,000 events
All events
All Events
Matches
Non-Matches
_raw
src_ip
src_port
dst_ip
dst_port
domain
record
1332017991.970000 CwS00TGmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_INTERNET 32 NB - - F
192.168.202.122 137 192.168.202.255 LABADMIN-641491 NB
27°C
Mostly cloudy
Search
ENG
IN
11:25
31-12-2025


splunk enterprise - Yahoo India
Thank You for Downloading Spl
Search | Splunk 10.0.2
github login - Yahoo India Sear
Splunk-Projects-For-Beginners/
127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dmain%20%7C%20timechart%20count&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool...
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=main | timechart count
Time range: All time
844,260 events (before 12/31/25 11:37:02.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (94)
Visualization
Chart: Line Chart
Format
Trellis
600,000
400,000
200,000
count
11:03 AM
Wed Dec 31
2025
11:04 AM
11:05 AM
11:06 AM
11:07 AM
11:08 AM
11:09 AM
11:10 AM
11:11 AM
11:12 AM
11:13 AM
11:14 AM
11:15 AM
11:16 AM
11:17 AM
_time
count
27°C
Mostly cloudy
Search
ENG
IN
11:37
31-12-2025

splunk enterprise - Yahoo India | Thank You for Downloading Spl | Search | Splunk 10.0.2

127.0.0.1:8000/en-US/app/search/search?sid=1767164213.196&s=Sourcetype&display.page.search.mode=fast&dispatch.sample_ratio=1&q=search%20index%3Dmain%20%7C%20stats...

splunk>enterprise Apps Administrator 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

# Sourcetype

Save Save As View Create Table View Close

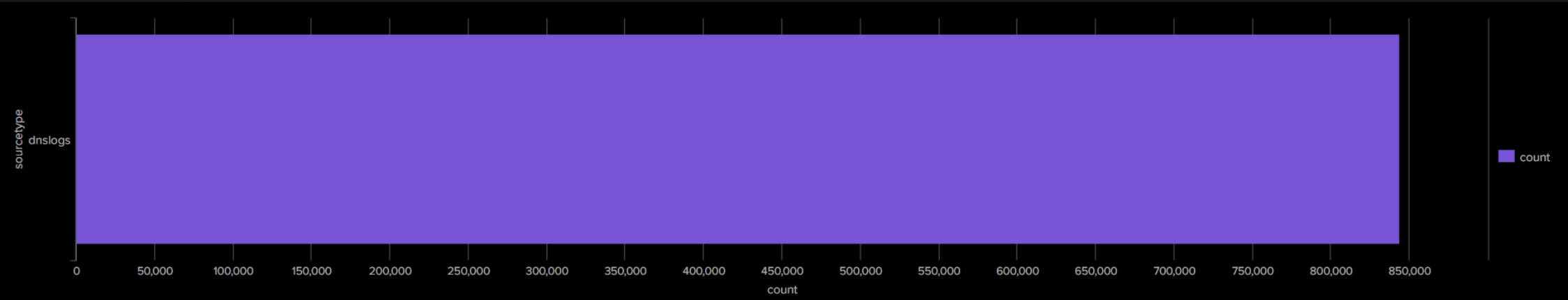
```
index=main | stats count by sourcetype
```

Time range: All time

✓ **844,260 events** (before 12/31/25 12:26:53.000 PM) No Event Sampling Job Fast Mode

Events Patterns Statistics (1) Visualization

Chart: Bar Chart Format Trellis




| sourcetype | count |
|---|---|
| dnslogs | 844260 |

Air: Satisfactory Tomorrow Search ENG IN 12:27 31-12-2025

splunk enterprise - Yahoo India | Thank You for Downloading Spl | Search | Splunk 10.0.2

127.0.0.1:8000/en-US/app/search/search?s=Sourcetype&display.page.search.mode=fast&dispatch.sample_ratio=1&q=search%20index%3Dmain%20%7C%20stats%20count%20by%20so...

splunk>enterprise Apps Administrator 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

# Sourcetype

Save Save As View Create Table View Close

```
index=main | stats count by source
```

Time range: All time

✓ **844,260 events** (before 12/31/25 12:27:21.000 PM) No Event Sampling Job Fast Mode

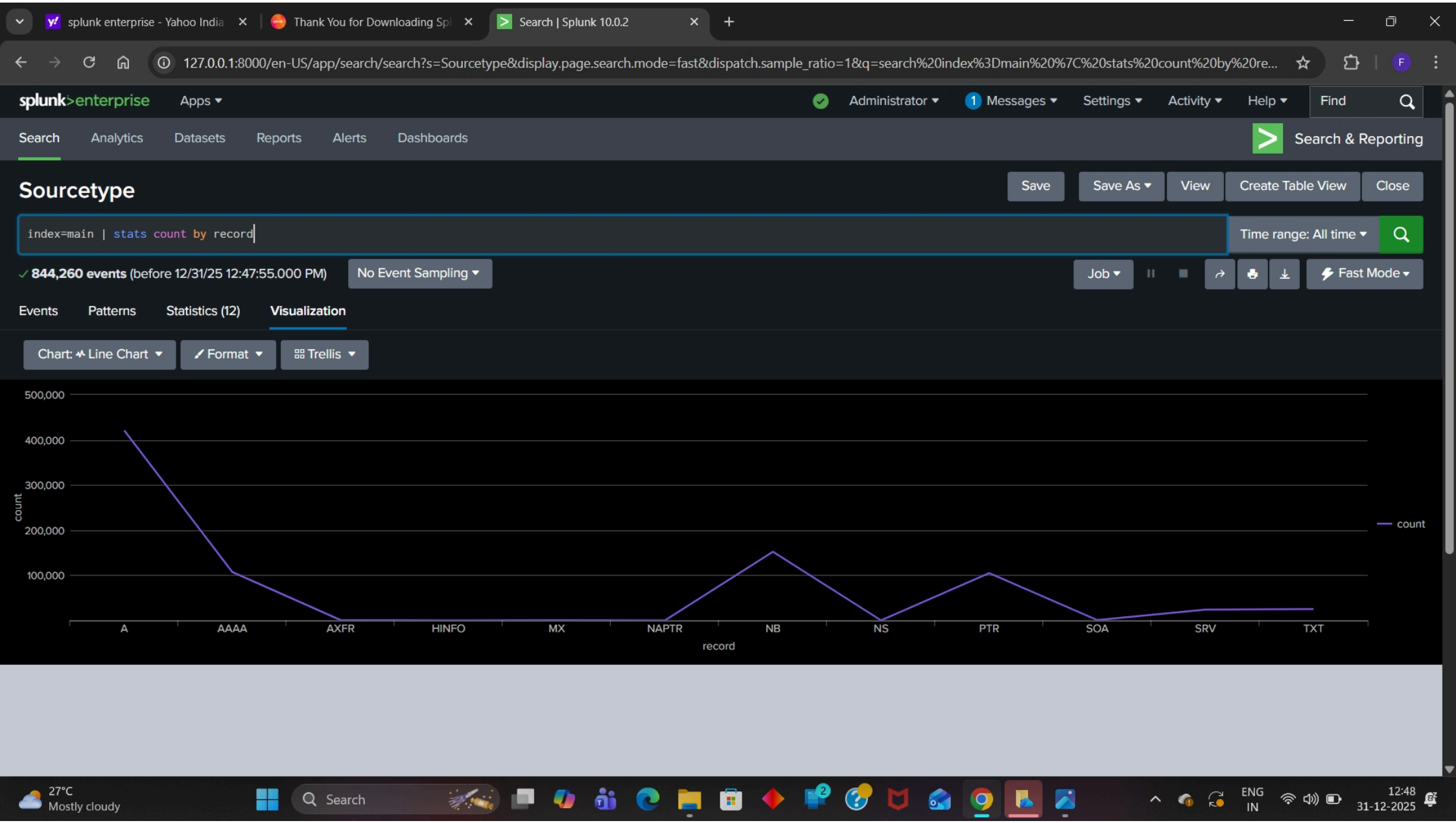
Events Patterns Statistics (1) Visualization

Chart: Column Chart Format Trellis


source count

dns.log.gz 844260

Rain coming In about 2.5 hours Search ENG IN 12:27 31-12-2025


splunk enterprise - Yahoo India
Thank You for Downloading Spl
Search | Splunk 10.0.2
127.0.0.1:8000/en-US/app/search/search?s=Sourcetype&display.page.search.mode=fast&dispatch.sample_ratio=1&q=search%20index%3Dmain%20%7C%20stats%20count%20by%20re...
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Sourcetype
Save
Save As
View
Create Table View
Close
index=main | stats count by record
Time range: All time
844,260 events (before 12/31/25 12:47:55.000 PM)
No Event Sampling
Job
Fast Mode
Events
Patterns
Statistics (12)
Visualization
Chart: Line Chart
Format
Trellis
500,000
400,000
300,000
200,000
100,000
count
A
AAAA
AXFR
HINFO
MX
NAPTR
NB
NS
PTR
SOA
SRV
TXT
record
count
27°C
Mostly cloudy
Search
ENG
IN
12:48
31-12-2025

splunk enterprise - Yahoo India | Thank You for Downloading Spl | Search | Splunk 10.0.2

127.0.0.1:8000/en-US/app/search/search?s=Sourcetype&display.page.search.mode=fast&dispatch.sample_ratio=1&q=search%20index%3Dmain%20%7C%20stats%20count%20by%20ds...

splunk>enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

# Sourcetype

Save Save As ▾ View Create Table View Close

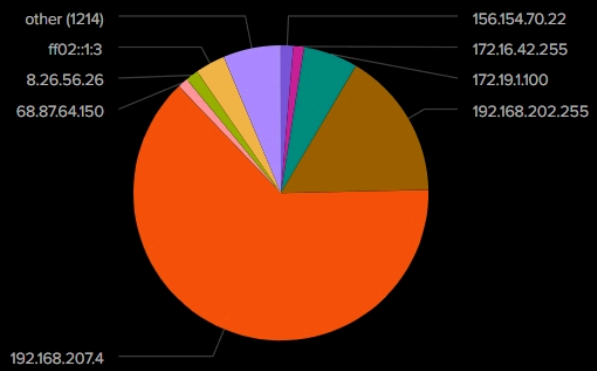
```
index=main | stats count by dst_ip
```

Time range: All time

✓ **844,260 events** (before 12/31/25 12:29:26.000 PM) No Event Sampling ▾ Job ▾ Fast Mode ▾

Events Patterns Statistics (1,222) Visualization

Chart: Pie Chart ▾ Format ▾ Trellis ▾




27°C Mostly cloudy Search ENG IN 12:30 31-12-2025

splunk enterprise - Yahoo India | Thank You for Downloading Spl | Search | Splunk 10.0.2

127.0.0.1:8000/en-US/app/search/search?s=Sourcetype&display.page.search.mode=fast&dispatch.sample_ratio=1&q=search%20index%3Dmain%20%7C%20stats%20count%20by%20ds...

splunk>enterprise Apps Administrator 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

# Sourcetype

Save Save As View Create Table View Close

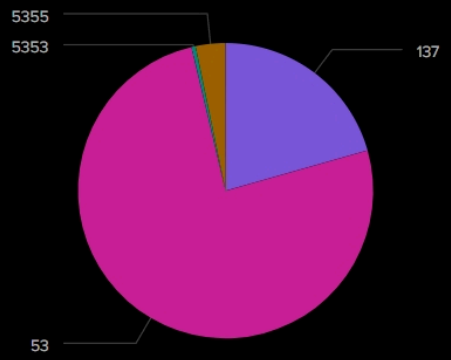
```
index=main | stats count by dst_port
```

Time range: All time

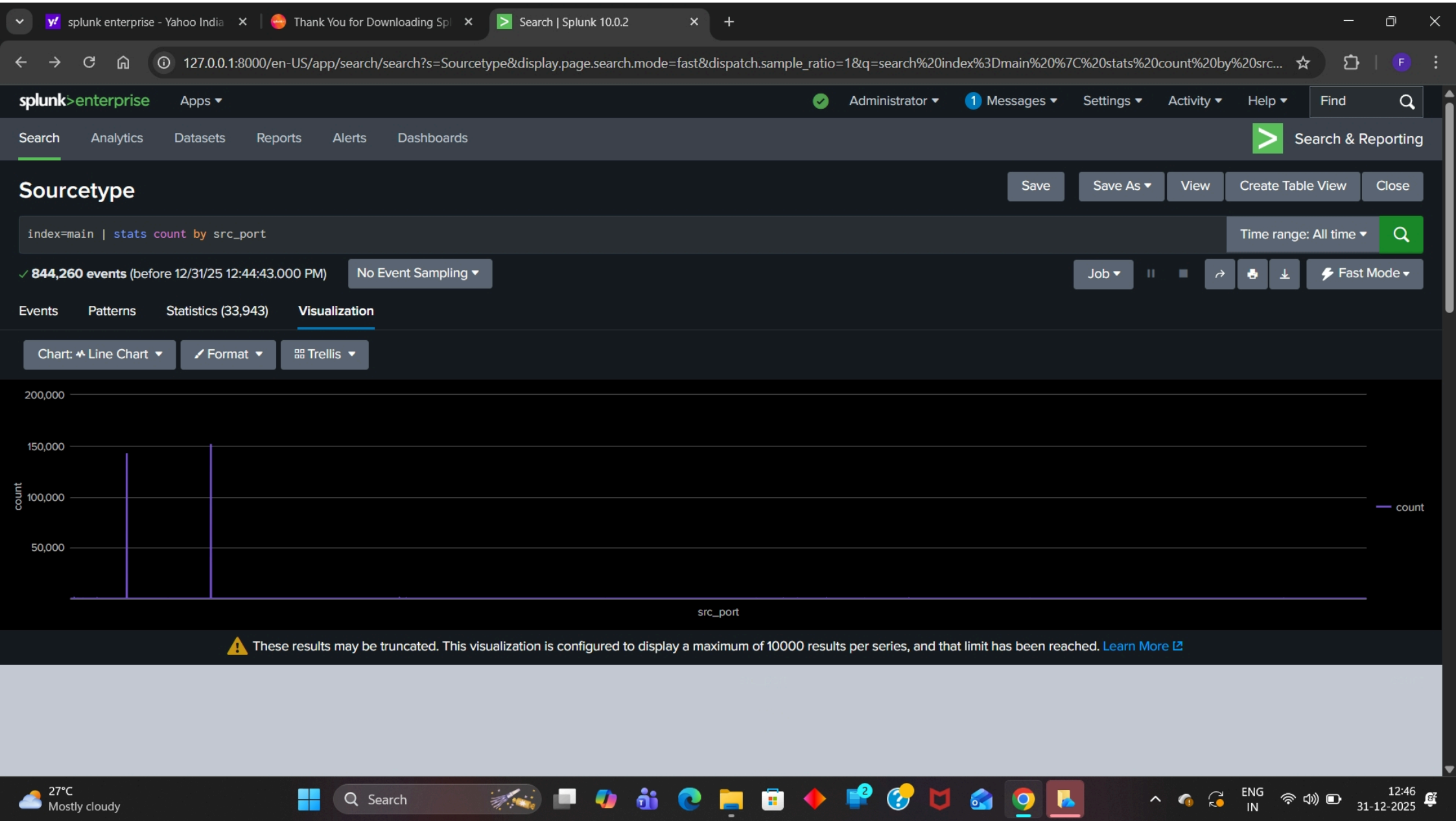
✓ **844,260 events** (before 12/31/25 12:30:49.000 PM) No Event Sampling Job Fast Mode

Events Patterns Statistics (4) Visualization

Chart: Pie Chart Format Trellis




27°C Mostly cloudy Search ENG IN 12:31 31-12-2025


splunk enterprise - Yahoo India
Thank You for Downloading Spl
Search | Splunk 10.0.2
127.0.0.1:8000/en-US/app/search/search?s=Sourcetype&display.page.search.mode=fast&dispatch.sample_ratio=1&q=search%20index%3Dmain%20%7C%20stats%20count%20by%20src...
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Sourcetype
Save
Save As
View
Create Table View
Close
index=main | stats count by src_port
Time range: All time
844,260 events (before 12/31/25 12:44:43.000 PM)
No Event Sampling
Job
Fast Mode
Events
Patterns
Statistics (33,943)
Visualization
Chart: Line Chart
Format
Trellis
200,000
150,000
100,000
50,000
count
src_port
count
These results may be truncated. This visualization is configured to display a maximum of 10000 results per series, and that limit has been reached. Learn More
27°C
Mostly cloudy
Search
ENG
IN
12:46
31-12-2025

127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dmain%20%7C%20stats%20count%20by%20src_ip&display.page.search.mode=smart&dispatch.sample_ratio=1&workloa...

splunk>enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

# Sourcetype

Save Save As ▾ View Create Table View Close

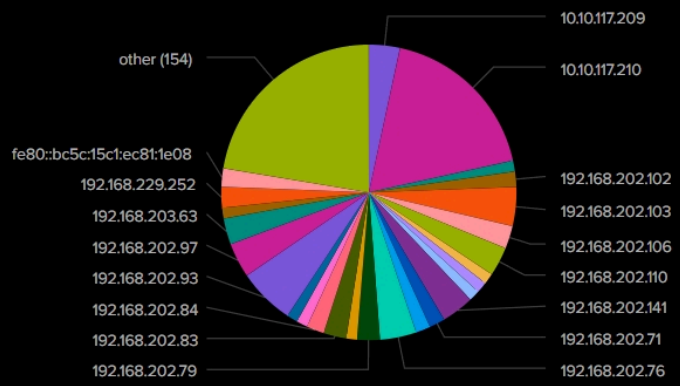
```
index=main | stats count by src_ip
```

Time range: All time ▾

✓ **844,260 events** (before 12/31/25 11:53:26.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (180) **Visualization**

Chart: Pie Chart ▾ Format ▾ Trellis ▾




| src_ip | count |
|---|---|
| 10.10.10.10 | 138 |
| 10.10.117.209 | 28444 |
| 10.10.117.210 | 151886 |

27°C Mostly cloudy Search ENG IN 12:06 31-12-2025