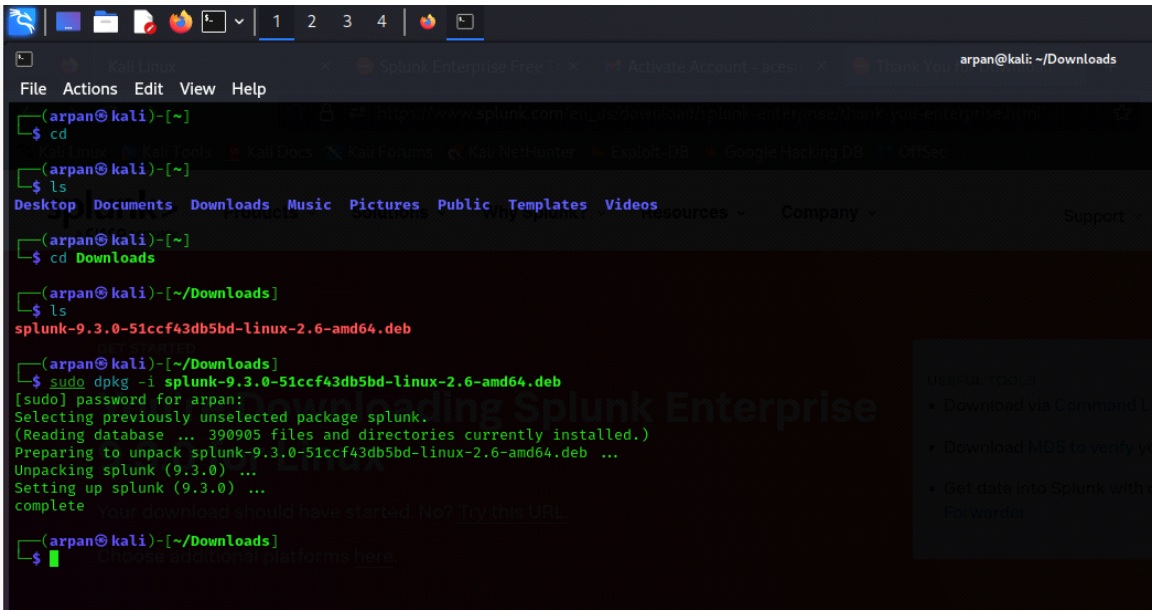
This project covers splunk enterprise installation and analysis of DNS log files

Installing splunk on kali :

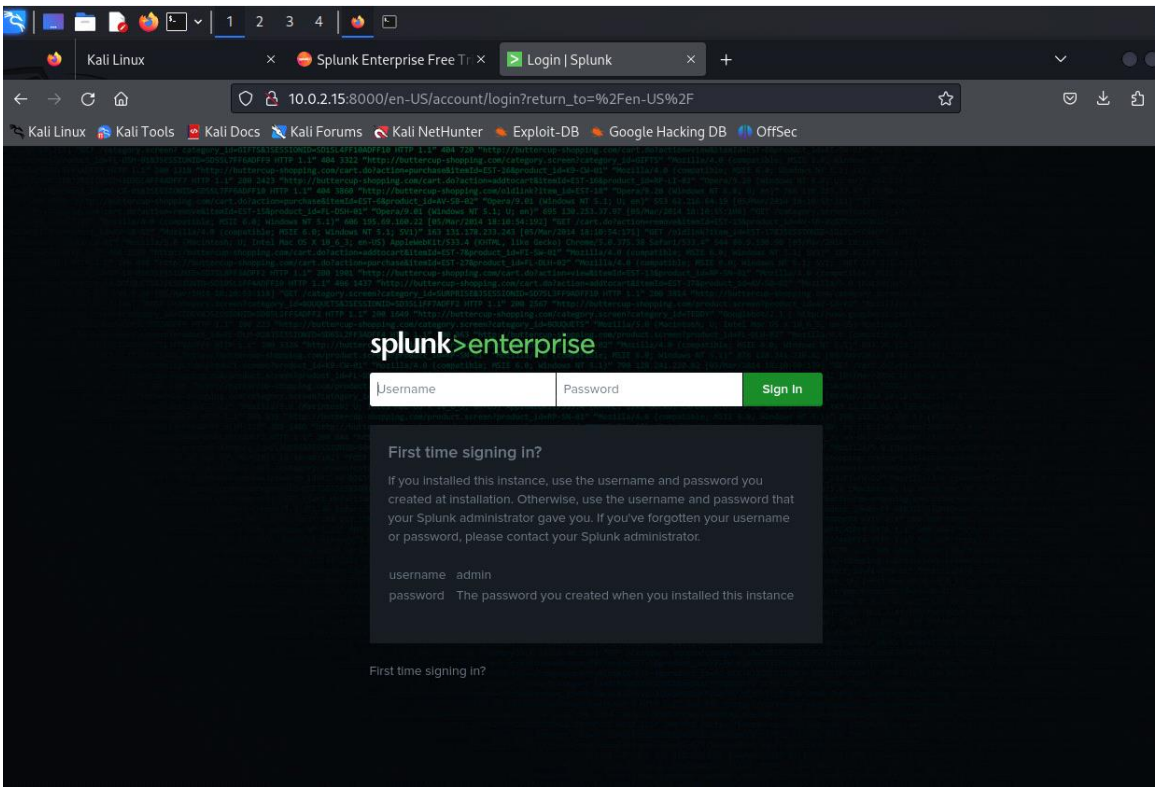


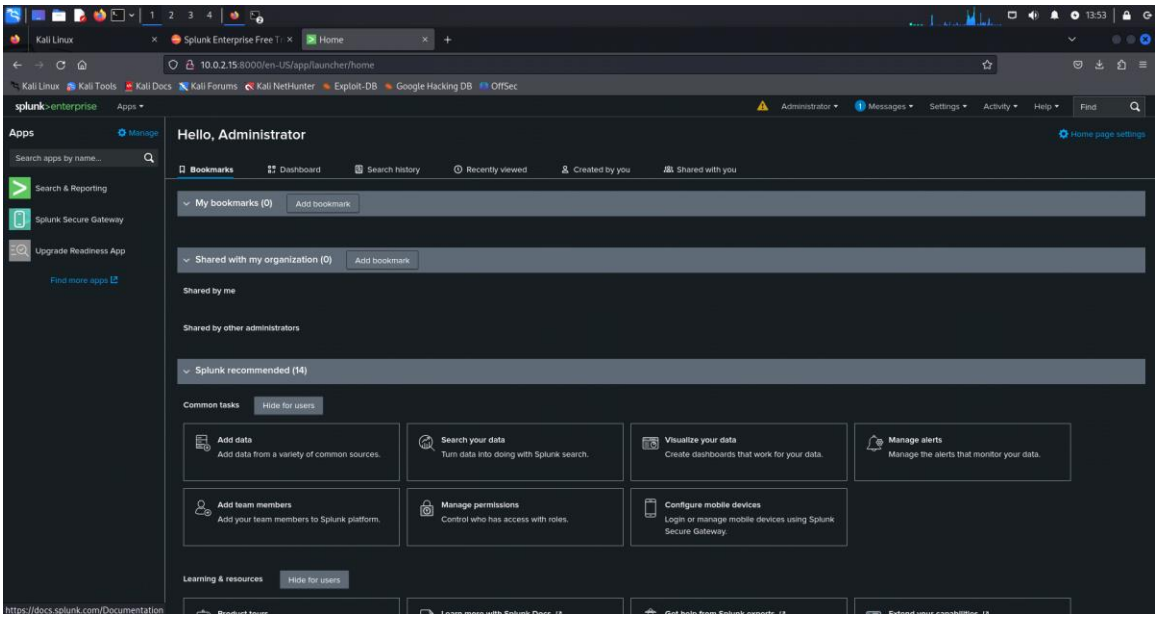
Use the following command to start splunk and accept the license agreement:

sudo /opt/splunk/bin/splunk start

```
File  Actions  Edit  View  Help
┌──(arpan㉿kali)-[~]
└─$ cd
┌──(arpan㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
┌──(arpan㉿kali)-[~]
└─$ cd Downloads

┌──(arpan㉿kali)-[~/Downloads]
└─$ ls
splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb

┌──(arpan㉿kali)-[~/Downloads]
└─$ sudo dpkg -i splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb
[sudo] password for arpan:
Selecting previously unselected package splunk.
(Reading database ... 390905 files and directories currently installed.)
Preparing to unpack splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.0) ...
Setting up splunk (9.3.0) ...
complete

┌──(arpan㉿kali)-[~/Downloads]
└─$

┌──(arpan㉿kali)-[~/Downloads]
└─$ ls /opt
microsoft  splunk

┌──(arpan㉿kali)-[~/Downloads]
└─$ ls
splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb

┌──(arpan㉿kali)-[~/Downloads]
└─$ sudo /opt/splunk/bin/splunk start
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware
corporation, with its principal place of business at 270 Brannan Street, San
Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you
("Customer" or "you" or "your") apply to the purchase of licenses and
subscriptions for Splunk's Offerings. By clicking on the appropriate button,
or by downloading, installing, accessing or using the Offerings, you agree to
these General Terms. If you are entering into these General Terms on behalf of
Customer, you represent that you have the authority to bind Customer. If you
do not agree to these General Terms, or if you are not authorized to accept
the General Terms on behalf of the Customer, do not download, install, access,
or use any of the Offerings.

See the General Terms Definitions Exhibit attached for definitions of
capitalized terms not defined herein.

1. License Rights
```

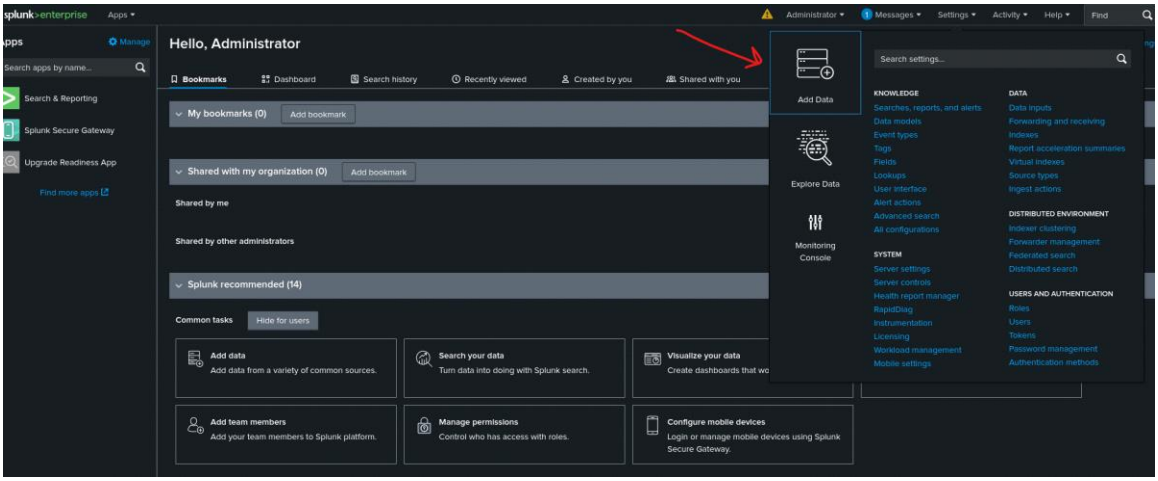
The web interface can be found locally on port **8000**. Login with the set credentials and access splunk ui.

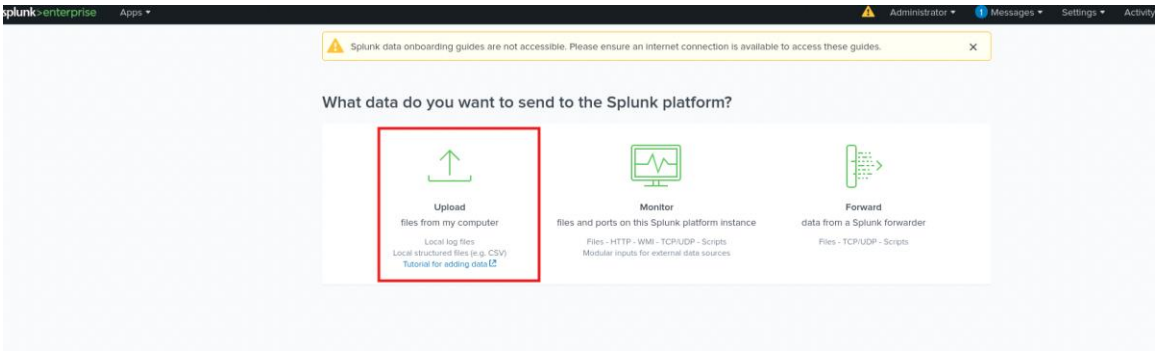




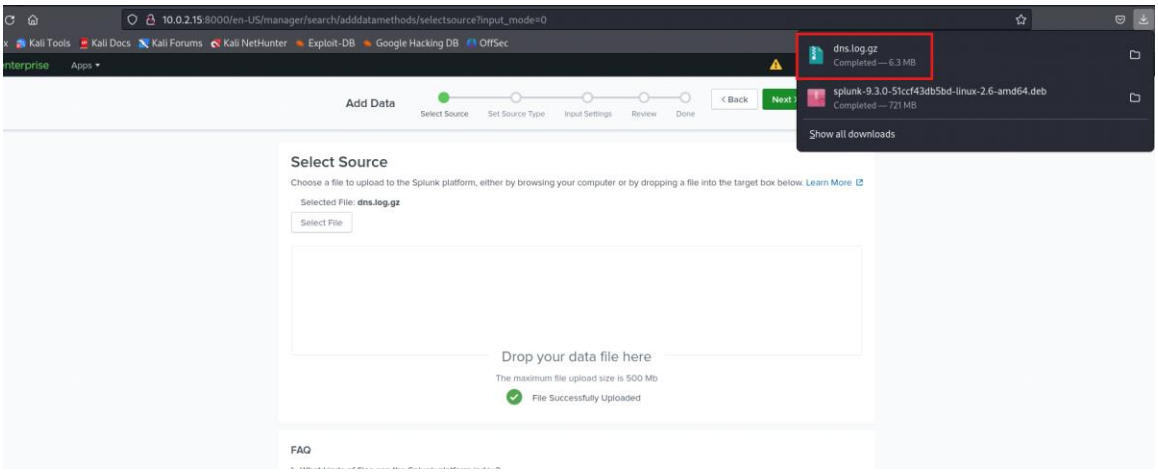
Analysing DNS logs

To add dns log file, click on **Settings >> Add Data >> Upload**

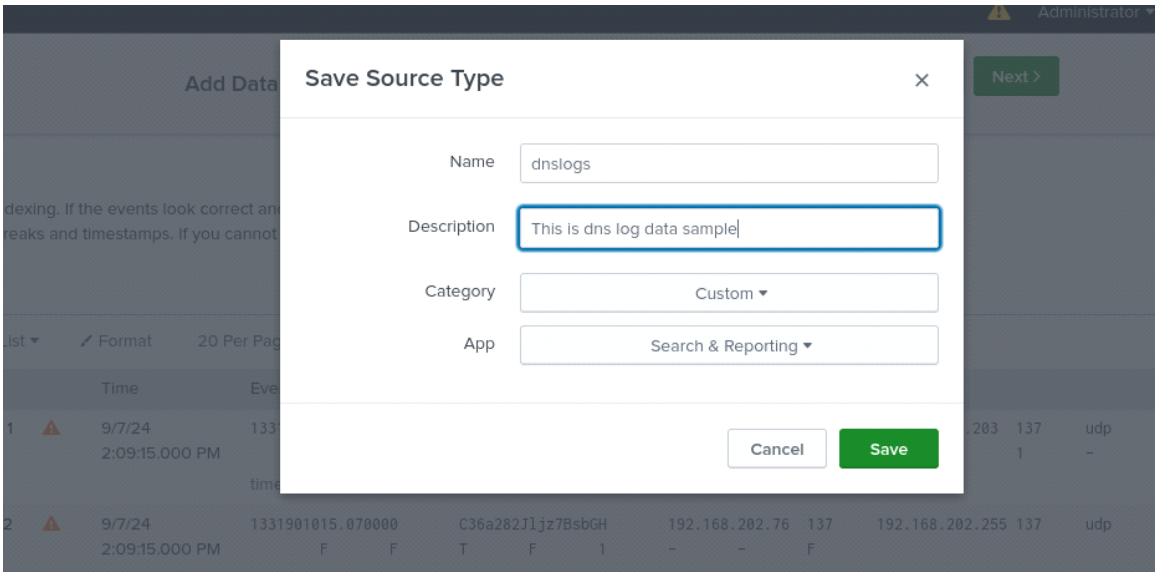


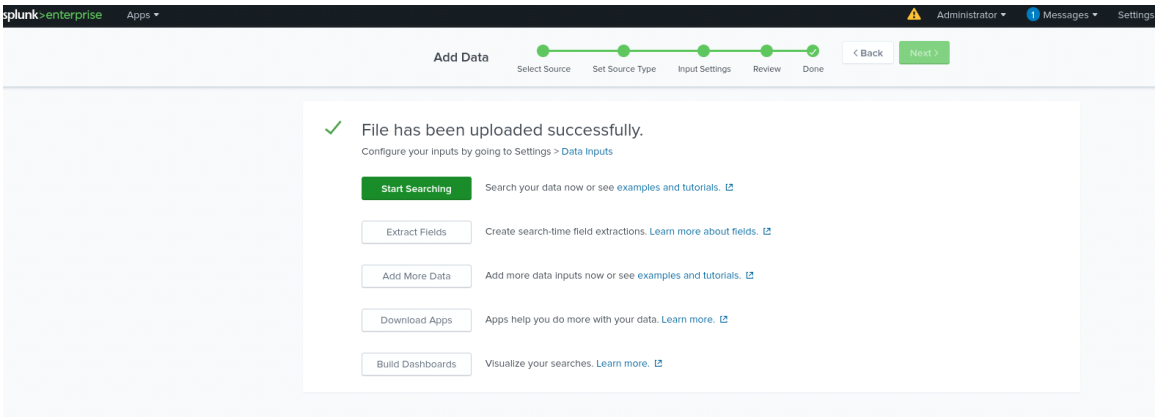


Drag and drop the dns log file

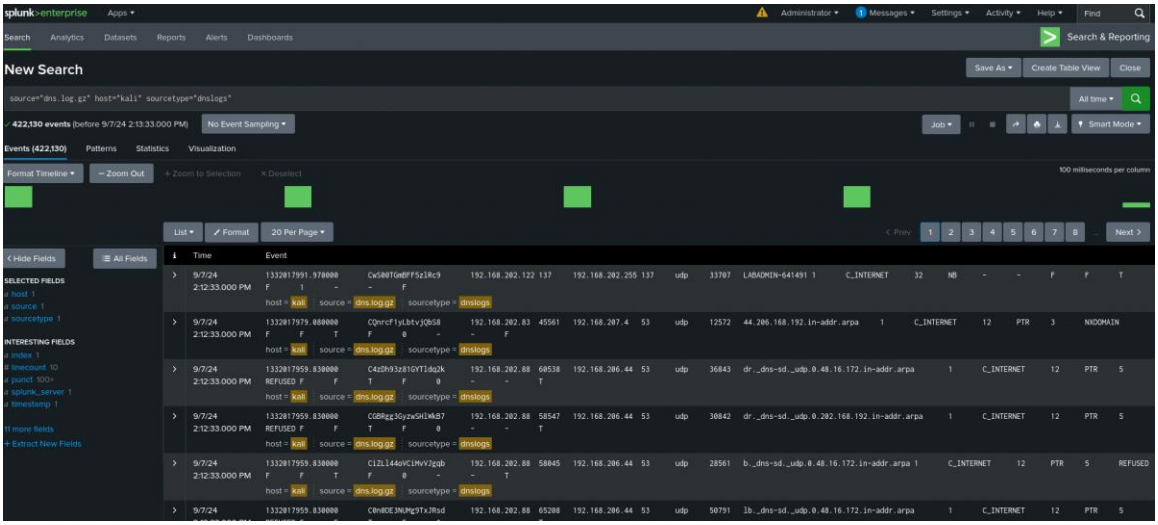


Click next, save and upload.





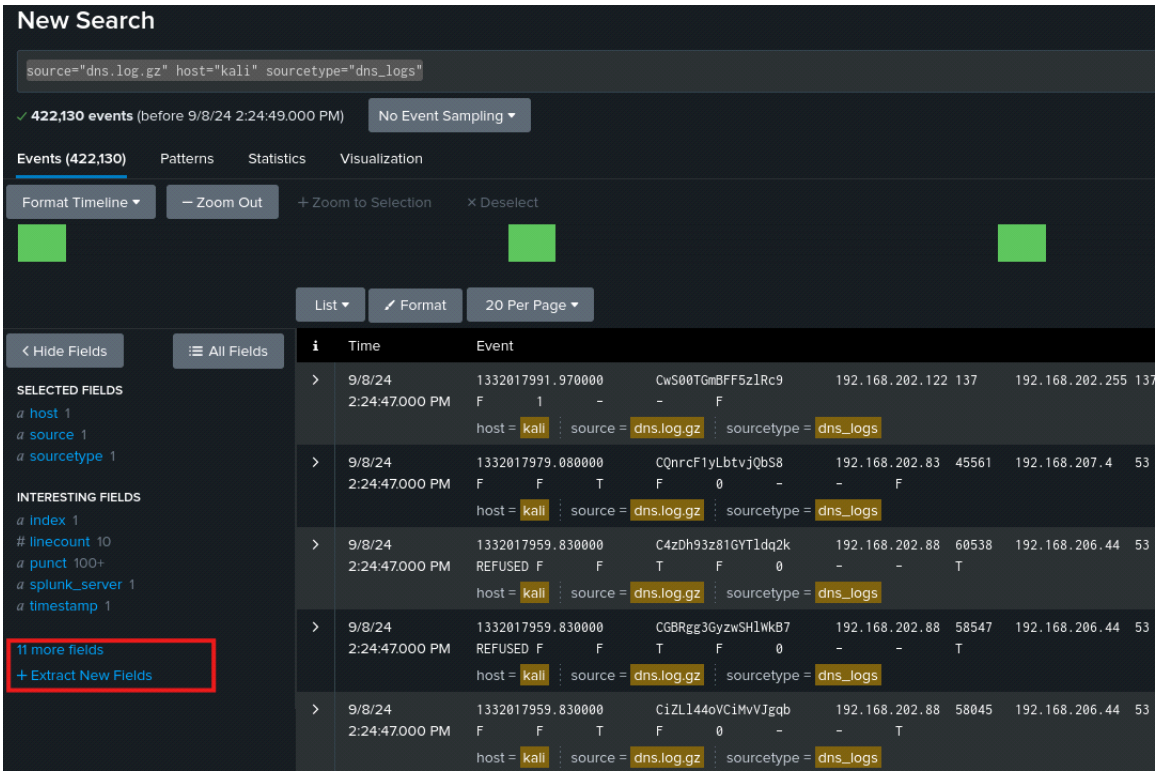
Click on **Start Searching**

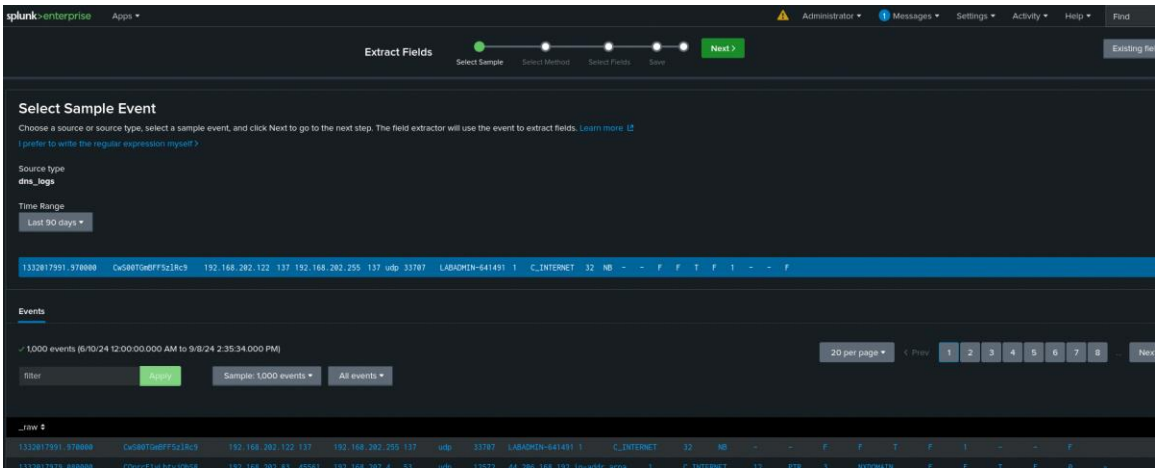


Steps to Analyze DNS Log Files in Splunk SIEM:

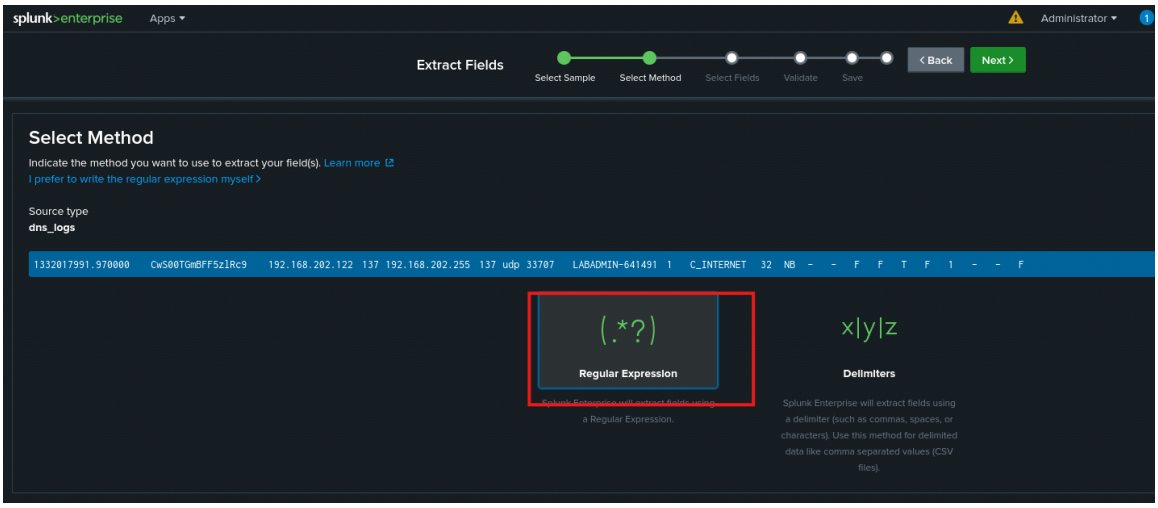
To Parse dns events and retrieve relevant dns data:

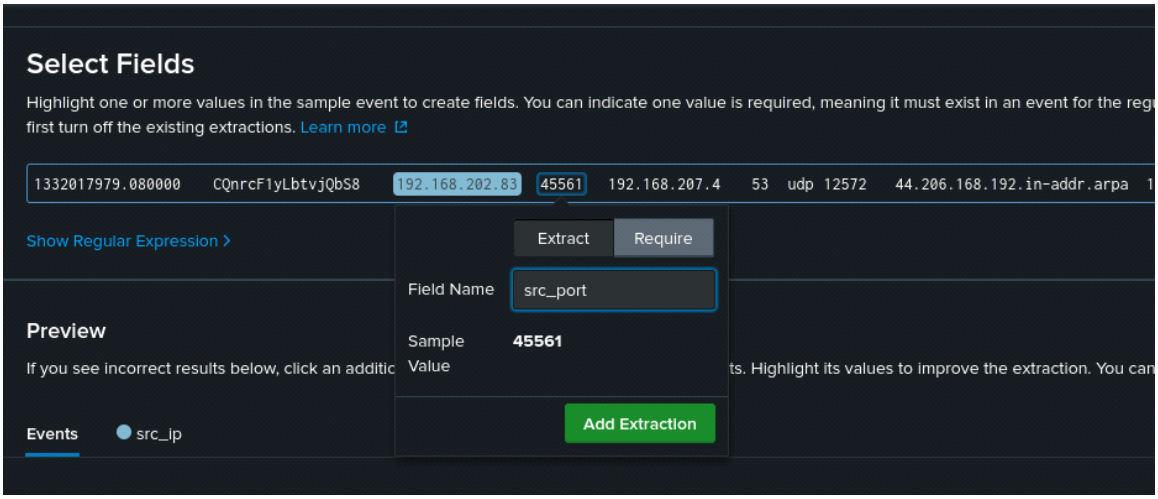
Click on **Extract New Fields** and select any event.





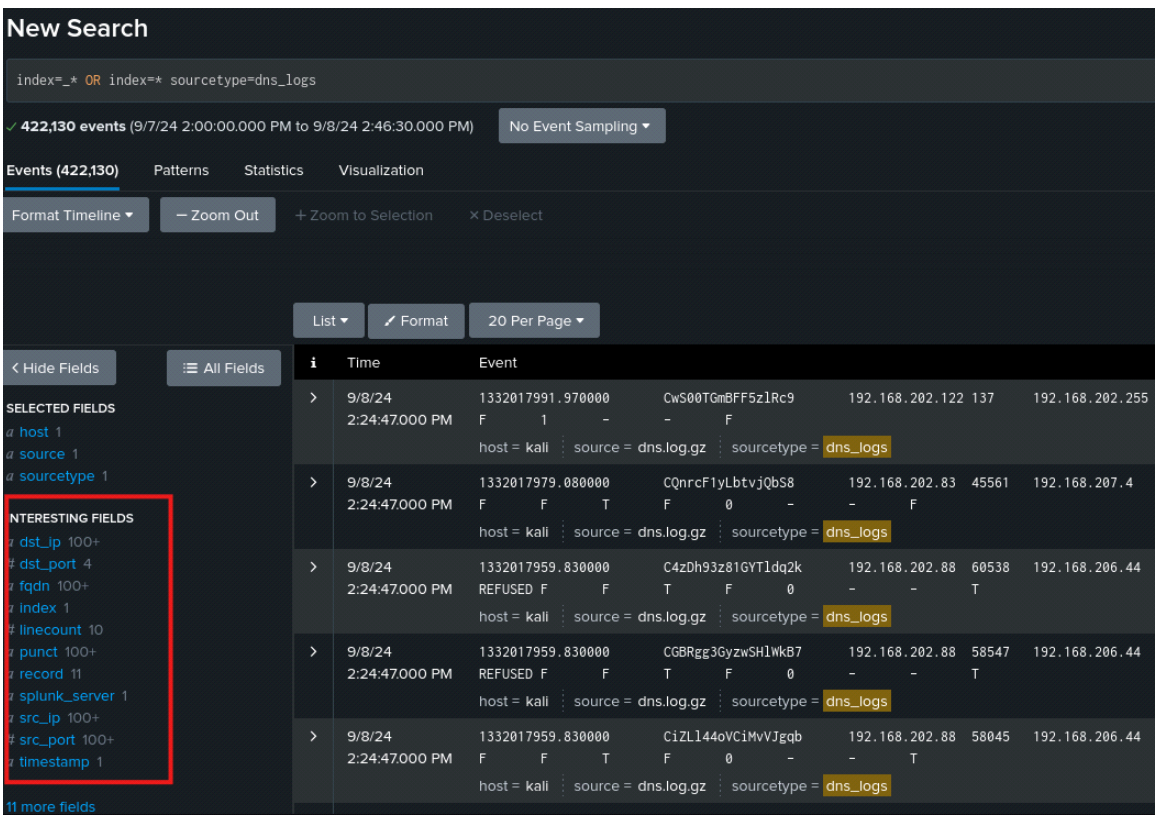
Select **Regular Expression** and select any relevant fields to parse.





Once you have selected relevant fields, hit Finish.


Extract Fields
Select Sample
Select Method
Select Fields
Validate
Save
Back
Finish
Save
Name the extraction and set permissions.
Extractions Name
EXTRACT- src_ip,src_port,dst_ip,dst_port,fqdn,re
Owner
arpan
App
search
Permissions
Owner
App
All apps
Source type
dns_logs
Sample event
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
Fields
src_ip,src_port,dst_ip,dst_port,fqdn,record
Regular Expression
^(?:[^\t\n]*\t){2}(?P<src_ip>[^\t]+)\t(?P<src_port>\d+)\t(?P<dst_ip>[^\t]+)\t(?P<dst_port>\d+)\t\w+\t\d+\t(?P<fqdn>[^\t]+)
\t\d+\t\w+_\w+\t\d+\t(?P<record>\w+)

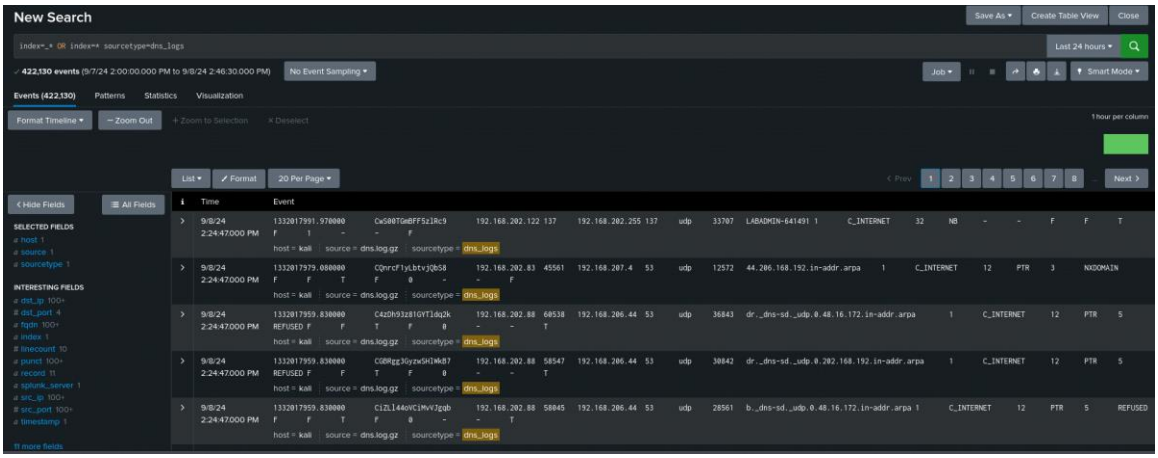

New Search
index=_* OR index=* sourcetype=dns_logs
422,130 events (9/7/24 2:00:00.000 PM to 9/8/24 2:46:30.000 PM)
No Event Sampling
Events (422,130)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
dst_ip 100+
dst_port 4
fqdn 100+
index 1
linecount 10
punct 100+
record 11
splunk_server 1
src_ip 100+
src_port 100+
timestamp 1
11 more fields
Time
Event
9/8/24 2:24:47.000 PM 1332017991.970000 CwS00TGmBFF5zlRc9 192.168.202.122 137 192.168.202.255
F 1 - - F
host = kali source = dns.log.gz sourcetype = dns_logs
9/8/24 2:24:47.000 PM 1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4
F F T F 0 - - F
host = kali source = dns.log.gz sourcetype = dns_logs
9/8/24 2:24:47.000 PM 1332017959.830000 C4zDh93z81GYTldq2k 192.168.202.88 60538 192.168.206.44
REFUSED F F T F 0 - - T
host = kali source = dns.log.gz sourcetype = dns_logs
9/8/24 2:24:47.000 PM 1332017959.830000 CGBRgg3GyzwSHlWkB7 192.168.202.88 58547 192.168.206.44
REFUSED F F T F 0 - - T
host = kali source = dns.log.gz sourcetype = dns_logs
9/8/24 2:24:47.000 PM 1332017959.830000 CiZLl44oVCiMvVJgqb 192.168.202.88 58045 192.168.206.44
F F T F 0 - - T
host = kali source = dns.log.gz sourcetype = dns_logs

1. Search for DNS Events

Open Splunk interface and navigate to the search bar.

Enter the following search query to retrieve DNS events

index=* sourcetype=dns_logs



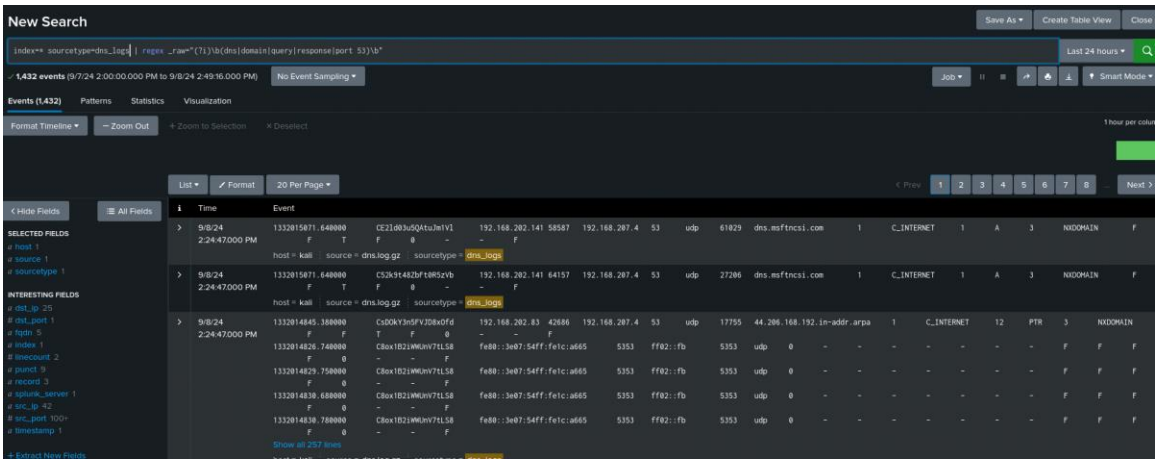
2. Extract Relevant Fields

Identify key fields in DNS logs such as source IP, destination IP, domain name, query type, response code, etc.

As mentioned below, | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b": This regex searches for common DNS-related keywords in the raw event data.

Example extraction command:

index=* sourcetype=dns_logs | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"

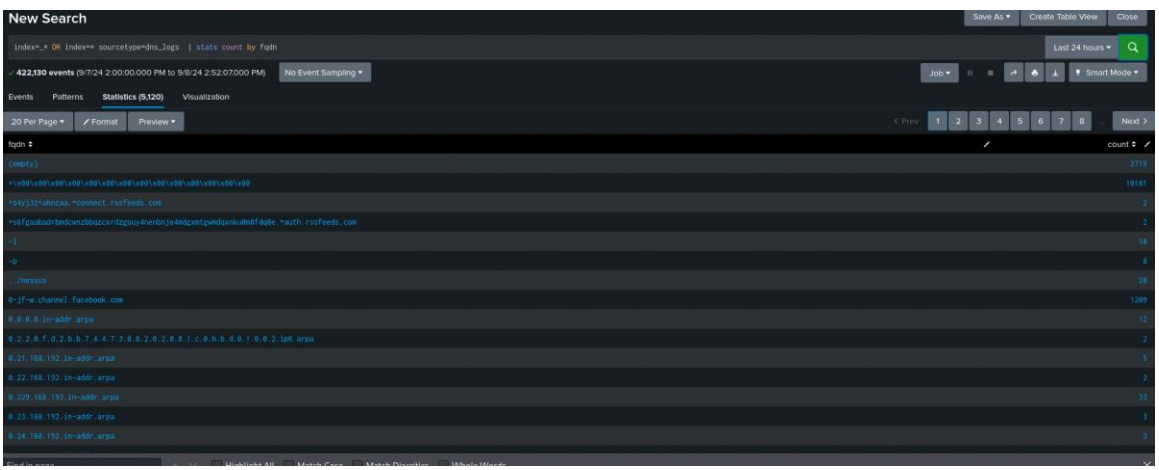


3. Identify Anomalies

Look for unusual patterns or anomalies in DNS activity.

Example query to identify spikes

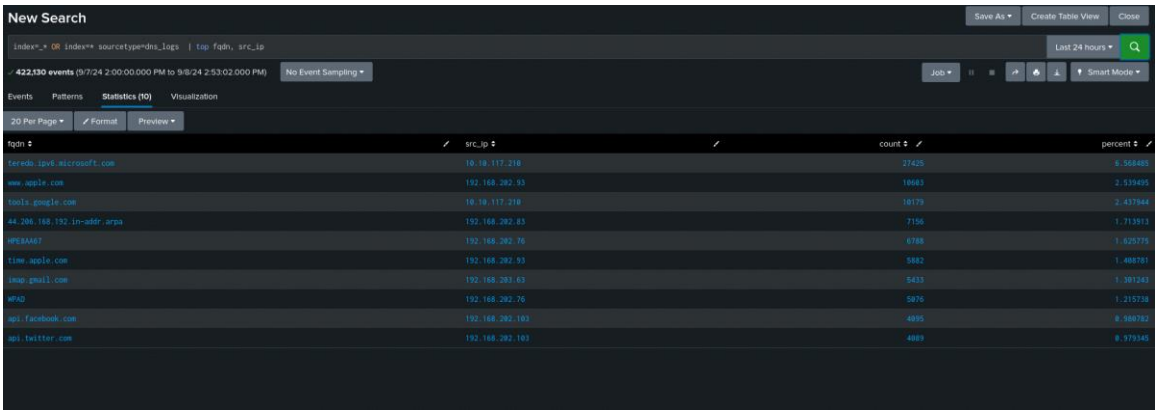
index=_* OR index=* sourcetype=dns_logs | stats count by fqdn



4. Find the top DNS sources

Use the top command to count the occurrences of each query type:

index=* sourcetype=dns_logs | top fqdn, src_ip



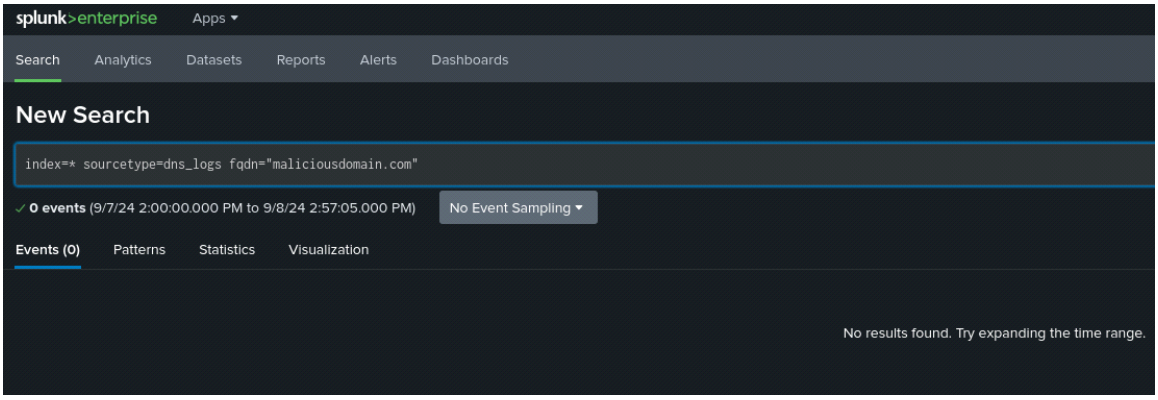
5. Investigate Suspicious Domains

Search for domains associated with known malicious activity or suspicious behavior.

Utilize threat intelligence feeds or reputation databases to identify malicious domains such virustotal.com

Example search for known malicious domains:

index=* sourcetype=dns_logs fqdn="maliciousdomain.com"



This concludes the project on dns log analysis