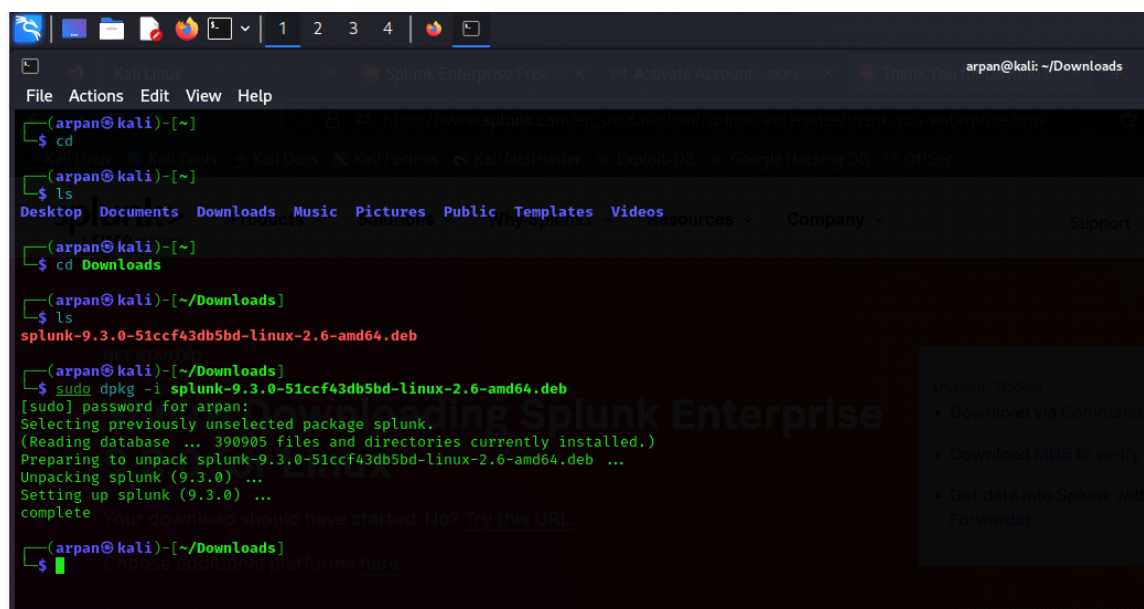


This project covers splunk enterprise installation and analysis of DNS log files

Installing splunk on kali :



```
(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
Your download should have started. No? Try this URL:
(arpan@kali)~/Downloads$
```

Useful tools

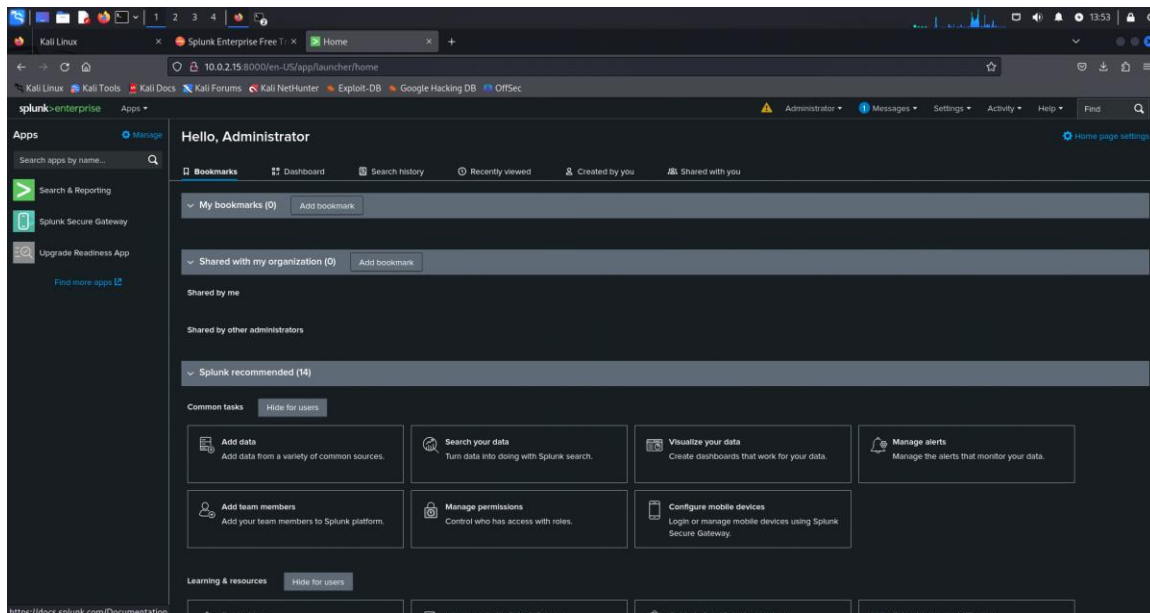
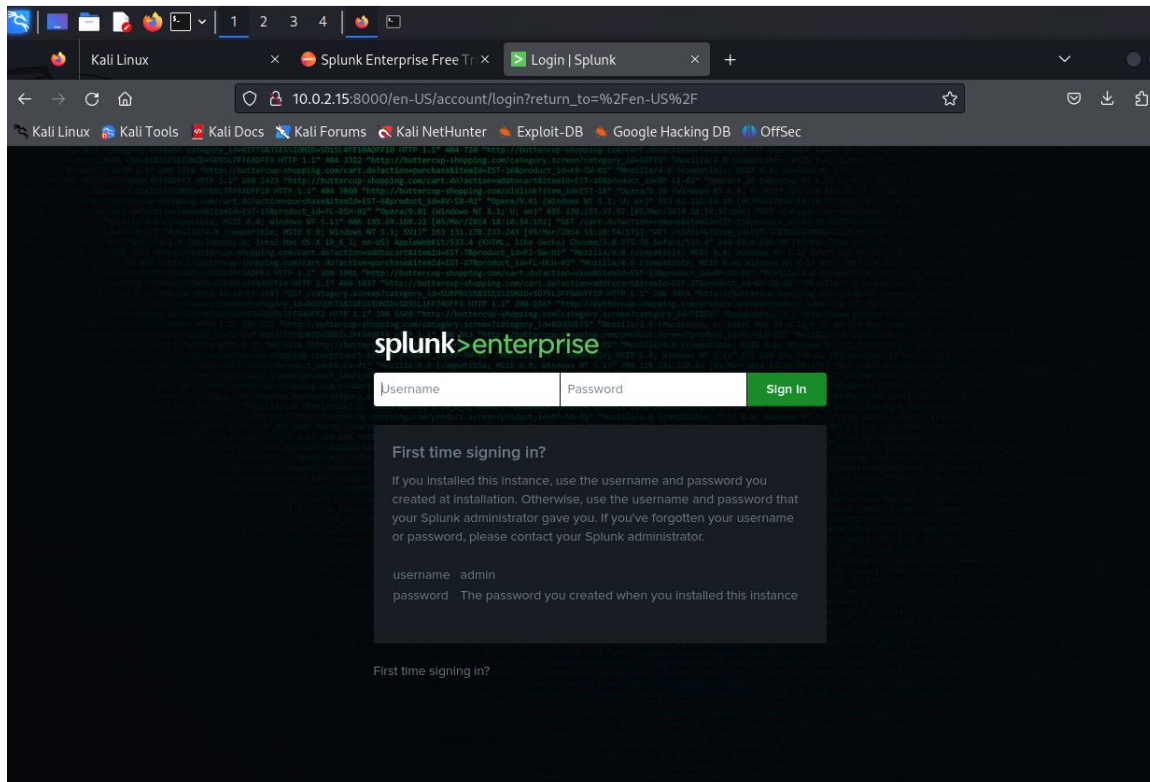
- Download via Command Line
- Download MD5 to verify
- Get data into Splunk with Forwarder

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

sudo /opt/splunk/bin/splunk start

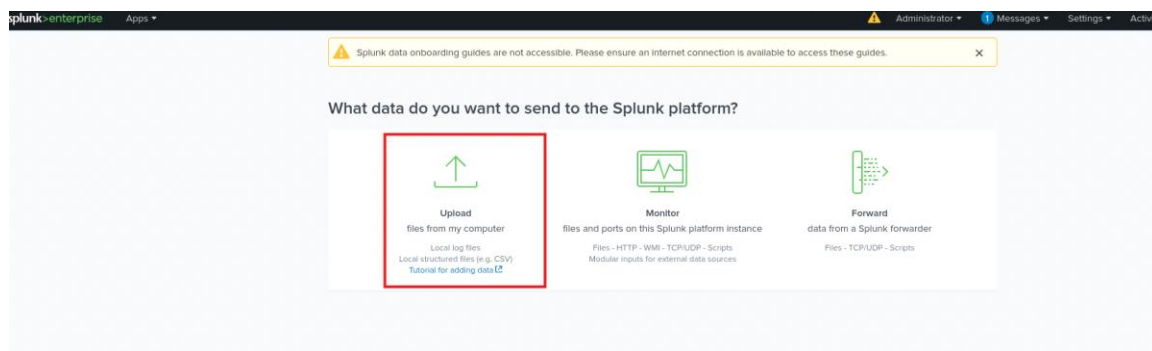
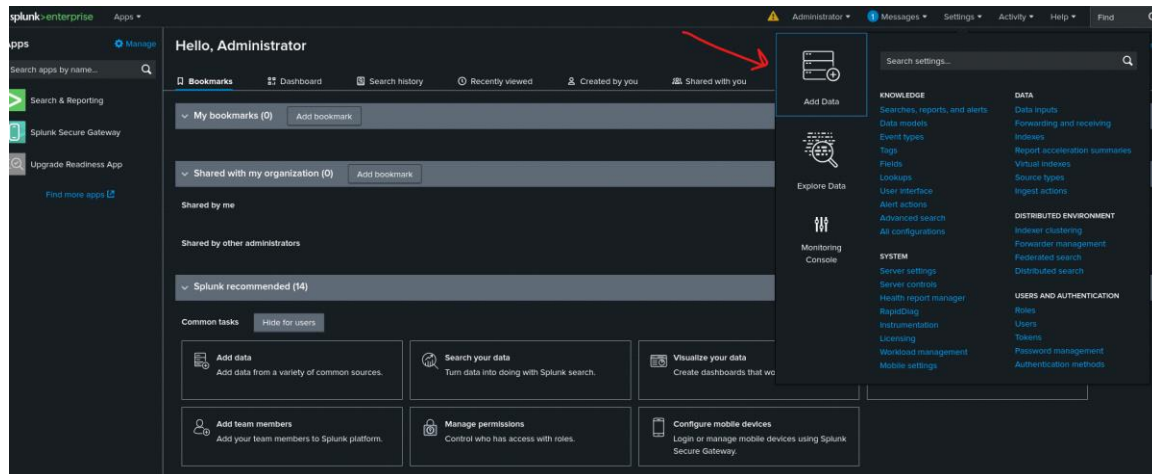
```
(arpan@kali)-[~]
$ cd
(arpan@kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(arpan@kali)-[~]
$ cd Downloads
(arpan@kali)-[~/Downloads]
$ ls
splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb
GET STARTED
(arpan@kali)-[~/Downloads]
$ sudo dpkg -i splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb
[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
Your download should have started. No? Try this URL.
(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
Getting Data In Search and Alerts Reports and Dashboards
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.

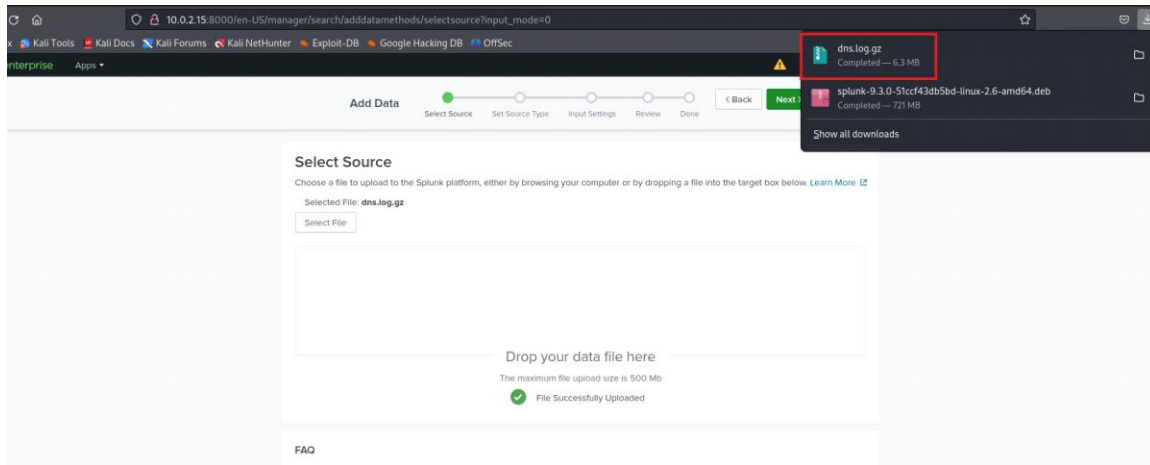


Analysing DNS logs

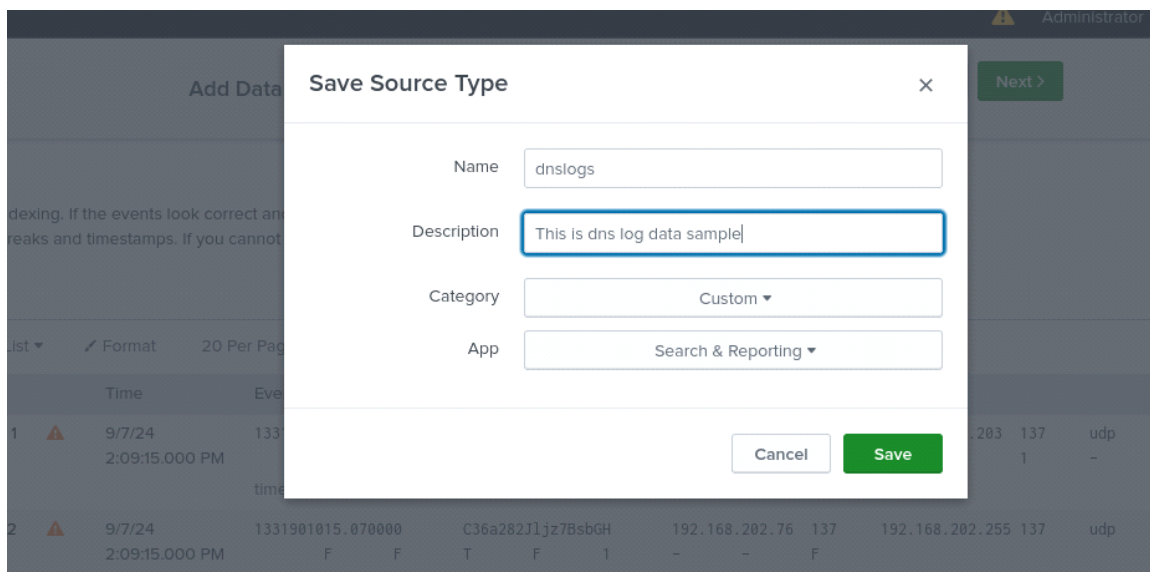
To add dns log file, click on **Settings >> Add Data >> Upload**

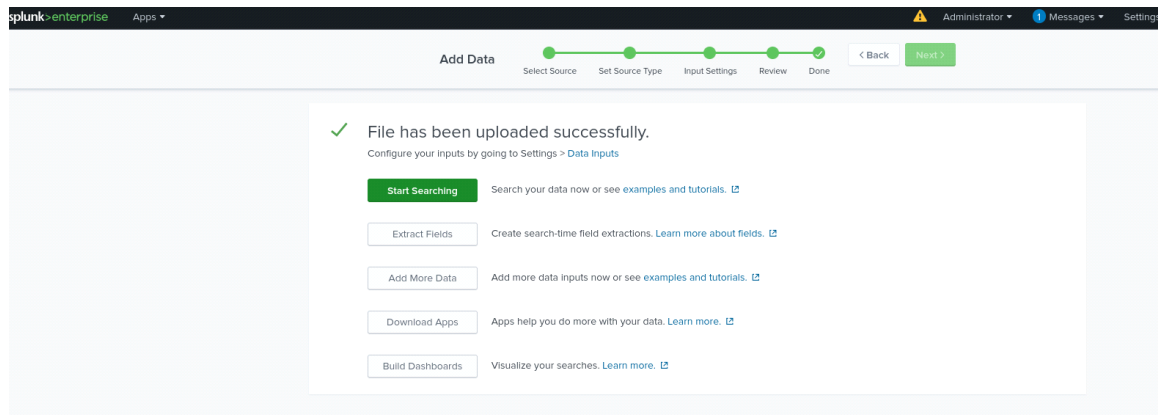


Drag and drop the dns log file

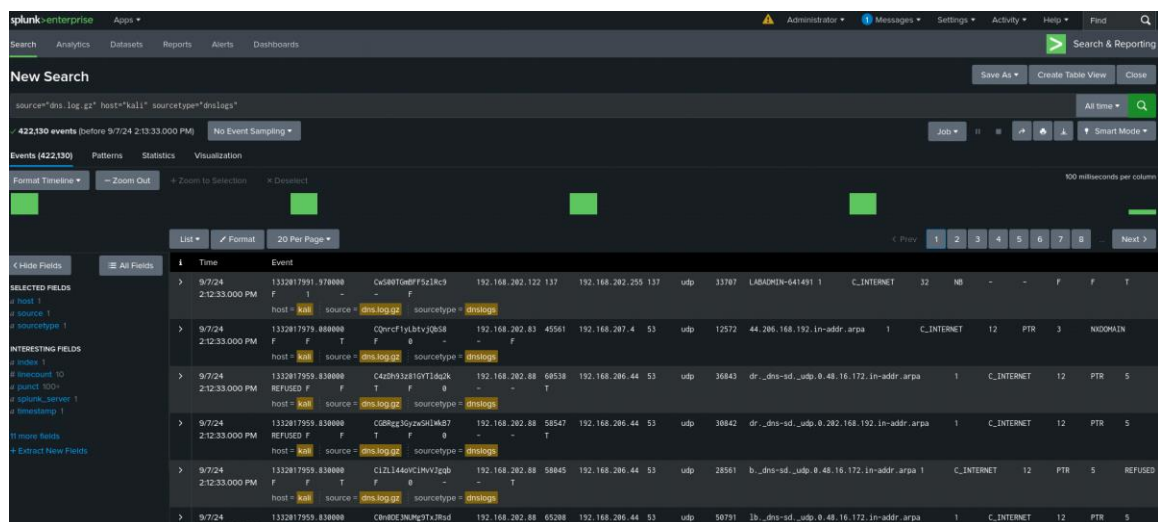


Click next, save and upload.





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.

New Search

source="dns.log.gz" host="kali" sourcetype="dns_logs"

✓ 422,130 events (before 9/8/24 2:24:49.000 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

- index 1
- linecount 10
- punct 100+
- splunk_server 1
- timestamp 1

11 more fields
+ Extract New Fields

>	Time	Event
>	9/8/24 2:24:47.000 PM	1332017991.970000 CwS00TgmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 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 53 F F T F - - 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 53 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 CGBRgg3GyzwSH1wkB7 192.168.202.88 58547 192.168.206.44 53 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 53 F F T F 0 - - T host = kali source = dns.log.gz sourcetype = dns_logs

splunk>enterprise Apps ▾

Administrator Messages Settings Activity Help Find

Extract Fields Select Sample Select Method Select Fields Save Next Existing Fields

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more](#)

I prefer to write the regular expression myself >

Source type
dns_logs

Time Range
Last 90 days ▾

1332017991.970000 CwS00TgmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LAB4QDN-841491 1 C_INTERNET 32 ND - - F F T F 1 - - F

Events

✓ 1,000 events (8/10/24 12:00:00.000 AM to 9/8/24 2:35:34.000 PM)

filter Apply Sample: 1,000 events ▾ All events ▾

20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next

...row <

1332017991.970000 CwS00TgmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LAB4QDN-841491 1 C_INTERNET 32 ND - - F F T F 1 - - F

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

splunk>enterprise Apps Administrator

Extract Fields

Select Sample Select Method Select Fields Validate Save
< Back Next >

Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#)

[I prefer to write the regular expression myself >](#)

Source type
dns_logs

```
1332017991.970000 Cw500TGnBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33787 LABADMIN-641491 1 C_INTERNET 32 NB - - F F T F 1 - - F
```

(.*?)

Regular Expression

Spunk Enterprise will extract fields using a Regular Expression.

x|y|z

Delimiters

Spunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

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. If you 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
```

[Show Regular Expression >](#)

Preview

If you see incorrect results below, click an additional value to highlight it. Highlight its values to improve the extraction. You can

Events ● src_ip

Field Name
src_port

Sample Value
45561

Add Extraction

Once you have selected relevant fields, hit Finish.

Extract Fields

< 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"]\W)(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+\t\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 x Deselect

List ▾ Format 20 Per Page ▾

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a 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

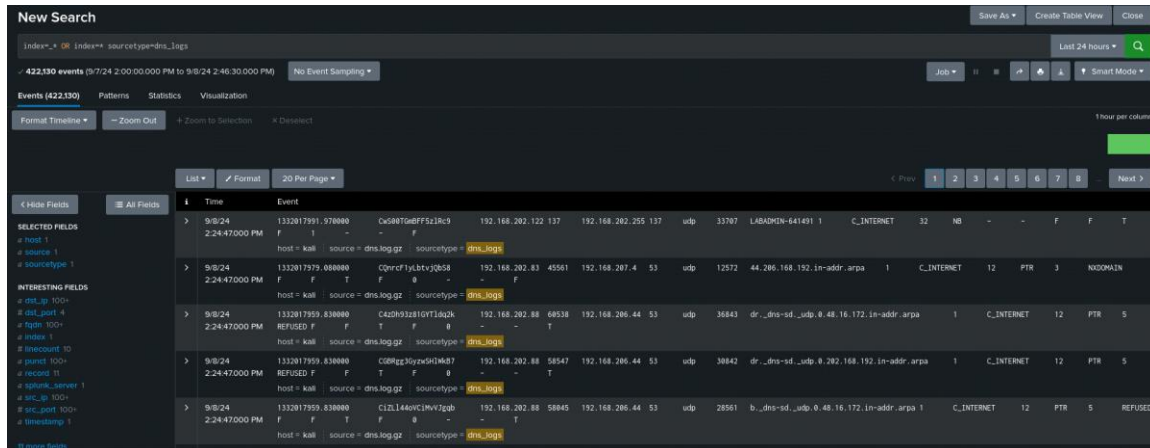
i	Time	Event
>	9/8/24 2:24:47.000 PM	1332017991.970000 CwS00TGmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 F 1 - - F host = kali : source = dns.log.gz : sourcetype = dns_logs
>	9/8/24 2:24:47.000 PM	1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 F F T F 0 - - F host = kali : source = dns.log.gz : sourcetype = dns_logs
>	9/8/24 2:24:47.000 PM	1332017959.830000 C4zDh93z81GYT1dq2k 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 CGBRgg3GyzwSH1wkB7 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 CiZL144oVCiMvVJgqb 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



The screenshot shows the Splunk search results interface for the query `index=* sourcetype=dns_logs`. The search bar at the top displays the query and the number of events found: 422,130. Below the search bar, there are tabs for `Events (422,130)`, `Patterns`, `Statistics`, and `Visualization`. The `Events (422,130)` tab is selected, showing a list of events. The interface includes a sidebar on the left with `SELECTED FIELDS` and `INTERESTING FIELDS` sections. The main table displays event data with columns for `Time`, `Event`, and various fields related to the DNS logs. The table is paginated, showing 20 events per page.

Time	Event
9/8/24 2:24:47:000 PM	1332817991.978888 Cw588T0e0FF5z1A9 192.168.282.122 137 192.168.282.255 137 udp 33787 LABADMIN-641491 1 C_INTERNET 32 MB - - F F T
9/8/24 2:24:47:000 PM	1332817979.088888 QPr0f1yLbtvJ0b58 192.168.282.83 45561 192.168.287.4 53 udp 12572 44.286.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NODOMAIN
9/8/24 2:24:47:000 PM	1332817959.838888 C42Dh312810Y1Jaq2k 192.168.282.88 68538 192.168.286.44 53 udp 36843 dr...sd...udp.0.48.16.172.in-addr.arpa 1 C_INTERNET 12 PTR 5
9/8/24 2:24:47:000 PM	1332817959.838888 REFUSED F F T F 0 - - T
9/8/24 2:24:47:000 PM	1332817959.838888 C08Rg30yze5HkM687 192.168.282.88 58547 192.168.286.44 53 udp 36842 dr...sd...udp.0.282.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 5
9/8/24 2:24:47:000 PM	1332817959.838888 REFUSED F F T F 0 - - T
9/8/24 2:24:47:000 PM	1332817959.838888 C1ZL1440VC1Mv7Jgb 192.168.282.88 58845 192.168.286.44 53 udp 28561 b...ds-sd...udp.0.48.16.172.in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED

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="(?)\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="(?)\b(dns|domain|query|response|port 53)\b"

New Search Save As Create Table View Close

index=* OR index= sourcetype=dns_logs | top fqdn, src_ip

422,130 events (9/7/24 2:00:00.000 PM to 9/8/24 2:53:02.000 PM) No Event Sampling Last 24 hours Job Smart Mode

Events Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

fqdn	src_ip	count	percent
teredo.ipv6.microsoft.com	19.19.117.218	27425	8.568495
www.apple.com	192.168.282.83	18683	2.539495
tools.google.com	19.19.117.218	18179	2.431944
44.206.168.192.in-addr.arpa	192.168.282.83	7156	1.713913
HP89A467	192.168.282.76	6386	1.625775
time.apple.com	192.168.282.83	5882	1.408761
usage.gmail.com	192.168.282.83	5433	1.301243
WPAD	192.168.282.76	5076	1.215738
api.facebook.com	192.168.282.193	4895	0.988762
api.twitter.com	192.168.282.193	4889	0.979345

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 as [virustotal.com](https://www.virustotal.com)

Example search for known malicious domains:

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

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

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

0 events (9/7/24 2:00:00.000 PM to 9/8/24 2:57:05.000 PM) No Event Sampling

Events (0) Patterns Statistics Visualization

No results found. Try expanding the time range.

This concludes the project on dns log analysis

