

## Introduction:

DNS logs play an important role in tracking how a network is being used and in spotting possible security risks. With the help of Splunk SIEM, these logs can be analyzed to identify unusual patterns, detect signs of cyberattacks, and improve overall visibility into network activity. Project Overview

In this project, I analyzed sample DNS logs using Splunk and created queries to extract important fields such as source IP, destination IP, and domain names. By studying the query patterns, I was able to identify unusual domains that might suggest network misconfigurations or tunneling activity. This hands-on work helped me strengthen my skills in SIEM log analysis, field extraction using regex, and detecting anomalies in a practical cybersecurity setting.

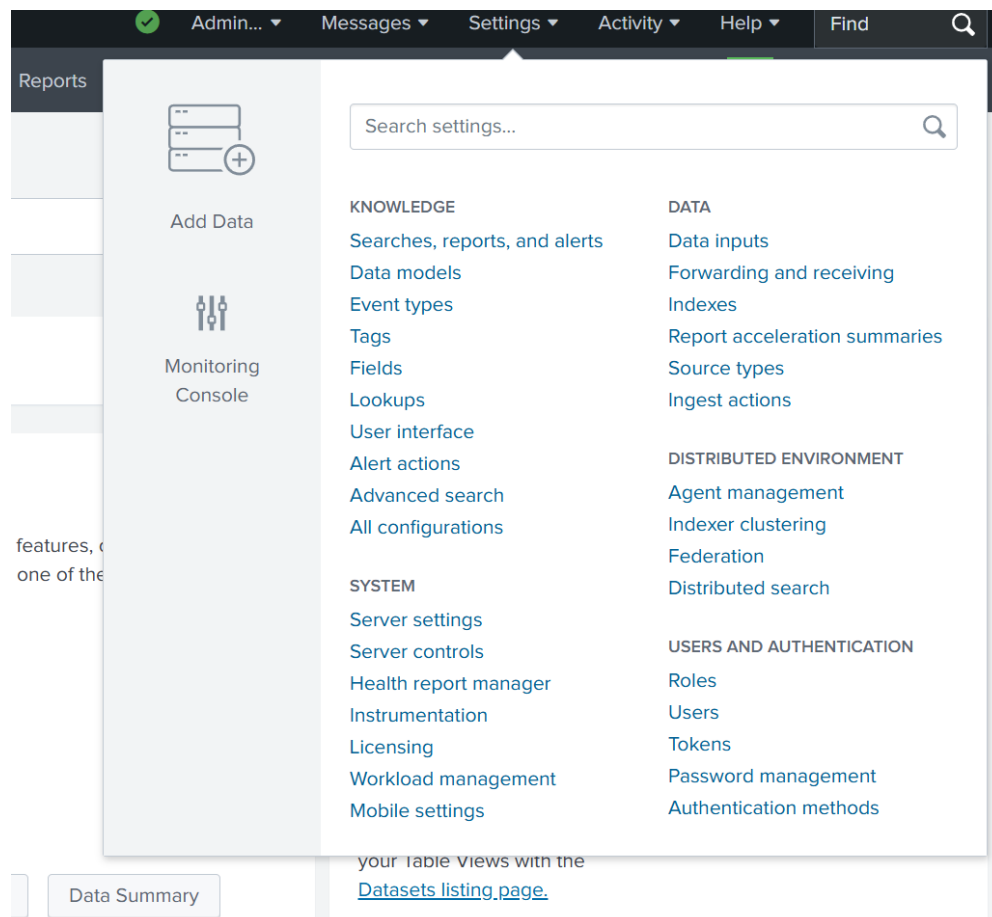
## Steps to Upload Sample DNS Log Files to Splunk SIEM

### 1. Data Preparation

Create or collect a sample DNS log file and ensure it includes relevant DNS event records

### 2. Importing Data into Splunk

In Splunk, go to Settings → Add Data → Upload, and upload the prepared DNS log file



## Or get data in with the following methods



### Upload

files from my computer

Local log files  
Local structured files (e.g. CSV)  
[Tutorial for adding data](#)



### Monitor

files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts  
Modular inputs for external data sources



### Forward

data from a Splunk forwarder

Files - TCP/UDP - Scripts

### 3. Select File

Choose your DNS log file or drag and drop it into the upload box.

Add Data

< 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

#### 4. Set Source Type

Once the DNS log is uploaded, click “Save As” and provide a meaningful name and description for easy identification

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **`dns.log.gz`**

Source type: Select Source Type ▾
Save As

	Format ▾	Select... ▾	Select... ▾																
		Time	Event																
➤ Event Breaks	1 ▲	10/11/25 4:15:45.000 AM	1331901005.510000 \\x00\\x00\\x00\\x00\\x00\\x00 timestamp = none	CWGtK43IH9XuaTN4f1	192.168.202.100	45658	SRV	0	NODERR	F	F	F	F	F	1	-	-	-	F
➤ Timestamp	2 ▲	10/11/25 4:15:45.000 AM	1331901015.070000 T 32 NB timestamp = none	C36a2821jz7BsbGH	192.168.202.76	137	T F	1 -	-	-	F	57402	HPEBAAG7	1	C_INTERNET				
➤ Advanced	3 ▲	10/11/25 4:15:45.000 AM	1331901015.820000 T 32 NB timestamp = none	C36a2821jz7BsbGH	192.168.202.76	137	F T F	1 -	-	-	F	57402	HPEBAAG7	1	C_INTERNET				
	4 ▲	10/11/25 4:15:45.000 AM	1331901016.570000 T 32 NB timestamp = none	C36a2821jz7BsbGH	192.168.202.76	137	F T F	1 -	-	-	F	57402	HPEBAAG7	1	C_INTERNET				
	5 ▲	10/11/25 4:15:45.000 AM	1331901005.860000 2 NB timestamp = none	C36a2821jz7BsbGH	192.168.202.76	137	T F 1	-	-	-	F	57398	WPAD	1	C_INTERNET			3	
	6 ▲	10/11/25 4:15:45.000 AM	1331901006.610000 2 NB timestamp = none	C36a2821jz7BsbGH	192.168.202.76	137	T F 1	-	-	-	F	57398	WPAD	1	C_INTERNET			3	

### Save Source Type

Name

DNS

Description

DNS log

Category

Custom ▾

App

Search & Reporting ▾

Cancel

Save

## 5. Review Settings

Double-check important configurations such as **Host** and **Index** to ensure they are correctly set

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The progress bar indicates the current step is 'Input Settings', with previous steps 'Select Source' and 'Set Source Type' completed, and 'Review' and 'Done' yet to be reached. The 'Review' button is highlighted in green. Below the progress bar, the 'Input Settings' section is displayed. It includes a description of the 'Host' field, options for how to set the host value (Constant value, Regular expression on path, Segment in path), a text input field for the 'Host field value' containing 'LAPTOP-8HQPDA3I', and a section for the 'Index' with a dropdown menu set to 'Default' and a link to 'Create a new index'.

**Input Settings**

Optionally set additional input parameters for this data input as follows:

**Host**

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value  
☐ Regular expression on path  
☐ Segment in path

Host field value

**Index**

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index  [Create a new index](#)

## 6. Submit and Upload Data

Do a final review of all settings, then click “Submit” to complete the data upload process into Splunk.

The screenshot shows the 'Add Data' wizard in Splunk Enterprise, now at the 'Review' step. The progress bar shows that 'Select Source', 'Set Source Type', and 'Input Settings' are completed, and 'Review' is the current step. The 'Submit' button is highlighted in green. Below the progress bar, the 'Review' section displays a summary of the configuration: Input Type (Uploaded File), File Name (dns.log.gz), Source Type (DNS), Host (LAPTOP-8HQPDA3I), and Index (Default).

**Review**

Input Type ..... Uploaded File  
File Name ..... dns.log.gz  
Source Type ..... DNS  
Host ..... LAPTOP-8HQPDA3I  
Index ..... Default

To confirm that your file has been uploaded successfully, run the following query:

```
index=* sourcetype=<your_sourcetype>
```

## 7. Parsing Data

On the left side, you'll see a table displaying your log data. In my case, I modified the fields to include additional details such as `dest_ip` and `dest_port`.

You can do this by selecting Extract New Fields in Splunk to define and extract new custom fields from your logs.

### SELECTED FIELDS

*a* host 1

*a* source 1

*a* sourcetype 1

### INTERESTING FIELDS

*a* dest\_ip 100+

*#* dest\_port 4

*a* full\_qualify\_domain\_name 100+

*a* index 1

*#* linecount 10

*a* punct 100+

*a* query\_id 100+

*a* record 12

*a* splunk\_server 1

*a* src\_ip 100+

*#* src\_port 100+

*a* timestamp 1

11 more fields

+ Extract New Fields

I intend to add additional field as shown below, so we will add Query ID, Source IP, Source Port, Destination IP, Destination Port, Full Quality Domain Name and Record.

Fields	
Source type: <b>DNS</b>	
The field extractions below have been previously defined for this source type. For a complete list of field objects, please see the <a href="#">Fields page</a> .	
Field Name	Pattern Name
query_id	EXTRACT- query_id,src_ip,src_port,dest_ip
src_ip	EXTRACT- query_id,src_ip,src_port,dest_ip
src_port	EXTRACT- query_id,src_ip,src_port,dest_ip
dest_ip	EXTRACT- query_id,src_ip,src_port,dest_ip
dest_port	EXTRACT- query_id,src_ip,src_port,dest_ip
full_qualify_domain_name	EXTRACT- query_id,src_ip,src_port,dest_ip
record	EXTRACT- query_id,src_ip,src_port,dest_ip

From the event below, select any event and click next

splunk>enterpriseAppsAdministra...MessagesSettingsActivityHelpFind

Extract FieldsSelect SampleSelect MethodSelect FieldsSaveNext>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**

Time Range  
Last 90 days

1332017959.830000	CGBRgg3GyzwSH1kkB7	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

Events

✓ 1,000 events (7/13/25 12:00:00.000 AM to 10/11/25 4:01:34.000 AM) < Prev12345678...Next >

20 per page

filterApplySample: 1,000 eventsAll events

_raw														
1332017991.970000	CwS00TGmBFF5zIrc9	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		
1332017979.080000	CQnrcFlyLbtvjQb58	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														
1332017959.830000	C4zDh93z81GYT1dq2k	192.168.202.88	60538	192.168.206.44	53	udp	36843	dr._dns-						
sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED	F	F	T	F	0			

## Select Regular Expression

**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**

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

**Regular Expression**

Splunk Enterprise will extract fields using a Regular Expression.

**Delimiters**

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

Select the field **192.168.202.88**, which is the client IP address, and click “Add Extraction”. It will then be grouped and highlighted in a unique color as shown below.

## 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 a 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](#)

Show Regular Expression >

**Preview**

If you see incorrect results below, click a value to remove it. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

Events

query\_id src\_ip

1,000 events (7/13/25 12:00:00.000 AM to 10/11/25 4:04:02.000 AM) < Prev 1 2 3 4 5 6 7 8 ... | 20 per page

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

	_raw	query_id	src_ip	src_port	dest
✓	1332017991.970000 CwS00TGmBFF5z1Rc9 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	CwS00TGmBFF5z1Rc9	192.168.202.122	137	192.168.202.255
✓	1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa 1	CQnrcF1yLbtvjQbS8	192.168.202.83	45561	192.168.207.4

This is how it looks after you finish grouping all the fields you want. In the Events panel below, you can see the names of your fields along with colors that indicate them and validate your field next.

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](#)

1332017959.830000

CGBRgg3GyzwSH1Wk87

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

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

query\_id

src\_ip

src\_port

dest\_ip

dest\_port

full\_qualify\_domain\_name

record

✓ 1,000 events (7/13/25 12:00:00.000 AM to 10/11/25 4:07:18.000 AM)

< Prev

1

2

3

4

5

6

7

8

...

Next >

20 per page ▾

filter

Apply

Sample: 1,000 events ▾

All events ▾

All Events

Matches

Non-Matches

_raw ▾	query_id ▾	src_ip ▾	src_port ▾	dest_ip ▾
✓ 1332017991.970000	CwS00TGmBFF5zIRc9	192.168.202.122	137	192.168.202.255
137	udp	33707	LABADMIN-641491	1
C_INTERNET	32	NB	-	F
T	F	1	-	F
✓ 1332017979.080000	CQnrcFlyLbtvjQbS8	192.168.202.83	45561	192.168.207.4
192.168.202.83	45561	192.168.207.4	53	udp

Extract Fields

Select Sample

Select Method

Select Fields

Validate

Save

< Back

Next >

Existing fields >

### Validate

Validate your field extractions and remove values that are incorrectly highlighted in the Events tab. In the field tabs, inspect the extracted values for each field, and optionally click a value to apply it as a search filter to the Events tab event list.

Show Regular Expression >

View in Search >

Events

query\_id

src\_ip

src\_port

dest\_ip

dest\_port

full\_qualify\_domain\_name

record

✓ 1,000 events (7/13/25 12:00:00.000 AM to 10/11/25 4:07:18.000 AM)

< Prev

1

2

3

4

5

6

7

8

...

Next >

20 per page ▾

filter

Apply

Sample: 1,000 events ▾

All events ▾

All Events

Matches

Non-Matches

_raw ▾	query_id ▾	src_ip ▾	src_port ▾	dest_ip ▾
✓ 1332017991.970000	CwS00TGmBFF5zIRc9	192.168.202.122	137	192.168.202.255
192.168.202.122	137	192.168.202.255	LABADMIN-641491	1
137	udp	33707	NB	-
C_INTERNET	32	-	-	F
T	F	1	-	F
✓ 1332017979.080000	CQnrcFlyLbtvjQbS8	192.168.202.83	45561	192.168.207.4
192.168.202.83	45561	192.168.207.4	53	udp
53	udp	12572	44.206.168.192.in-addr.arpa	1
C_INTERNET	12	PTR	3	NXDOMAIN
F	T	F	0	-



Finally, check the newly extracted field, and if everything is correct, click “Finish”.

Extract Fields

Select Sample

Select Method

Select Fields

Validate

Save

< Back

Finish >

## Save

Name the extraction and set permissions.

Extractions Name

EXTRACT-

query\_id,src\_ip,src\_port,dest\_ip,dest\_

Owner

navee

App

search

Permissions

Owner

App

All apps

---

Source type

DNS

Sample event

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

Fields

query\_id,src\_ip,src\_port,dest\_ip,dest\_port,full\_qualify\_domain\_name,record

Regular Expression

^\\d+\\.\\d+\\.\\d+\\.\\d+(?P<query\_id>[^\t]+)\t(?P<src\_ip>[^\t]+)[^\t\n]\*(?P<src\_port>\d+)\t(?P<dest\_ip>[^\t]+)\t(?P<dest\_port>\d+)\t\\w+\\.\\d+\\.\\d+\\.\\d+(?P<full\_qualify\_domain\_name>[^\t]+)(?:[^\t\n]\*\t){4}(?P<record>\w+)

It shows that you successfully extracted additional fields.

Extract Fields

Select Sample

Select Method

Select Fields

Validate

Save

✓

## Success!

You have extracted additional fields from your data (sourcetype=DNS).

Edit your field extractions at any time by going to [Field Extractions](#).

What would you like to do next?

- [Explore the fields I just created in Search](#)
- [Extract more fields](#)

Now, additional fields have been added to the Interesting Fields section, including **dest\_ip**, **dest\_port**, and others.

#### SELECTED FIELDS

*a* host 1  
*a* source 1  
*a* sourcetype 1

#### INTERESTING FIELDS

*a* dest\_ip 100+  
# dest\_port 4  
*a* full\_qualify\_domain\_name 100+  
*a* index 1  
# linecount 10  
*a* punct 100+  
*a* query\_id 100+  
*a* record 12  
*a* splunk\_server 1  
*a* src\_ip 100+  
# src\_port 100+  
*a* timestamp 1

11 more fields

+ Extract New Fields

## Steps to Analyze DNS Log Files in Splunk SIEM

### 1. Search for DNS Events

- Launch the Splunk interface and navigate to the search bar.
- Use the following query to pull all DNS-related events:

**index=\* sourcetype="DNS"**

Note: "DNS" is the sourcetype name you assigned when uploading the data.

The screenshot shows the Splunk Search interface. The search bar contains the query `index=* sourcetype=DNS`. The results table displays several DNS events. The first event is at 10/11/25 4:19:04.000 AM, with host `LAPTOP-SHQPD33` and source `dns.log.gz`. The event details show a PTR record for `192.168.202.122` pointing to `192.168.202.255`. The interface includes tabs for Events, Patterns, Statistics, and Visualization, and a sidebar for field management.

If you navigate to the fields, it shows you interesting information like top value count and more.

The screenshot shows the Splunk Fields interface. The field `dest_ip` is selected, and the interface displays a list of top values with their counts and percentages. The top values are 192.168.207.4, 192.168.202.255, 172.19.1.100, ff02::1:3, 8.26.56.26, 156.154.70.22, 172.16.42.255, 68.87.64.150, 68.87.75.198, and 192.168.206.44.

Top 10 Values	Count	%
192.168.207.4	462,246	62.599%
192.168.202.255	120,910	16.374%
172.19.1.100	43,745	5.924%
ff02::1:3	26,568	3.598%
8.26.56.26	11,020	1.492%
156.154.70.22	10,450	1.415%
172.16.42.255	9,924	1.344%
68.87.64.150	8,451	1.144%
68.87.75.198	7,251	0.982%
192.168.206.44	3,297	0.446%

## 2. Extract Relevant Fields

- Identify important fields in DNS logs, such as **source IP**, **destination IP**, **domain name**, **query type**, **response code**, and more.
- You can use a regex to search for common DNS-related keywords in the raw event data. For example:

```
| regex _raw="(?(i)\b(dns|domain|query|response|port 53)\b"
```

- Full example query:

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

This helps isolate DNS-specific information from the raw logs for easier analysis.

## New Search

Save As ▾

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

2,864 events (10/10/25 4:00:00.000 AM to 10/11/25 4:24:13.000 AM)

Job ▾

No Event Sampling ▾

Events (2,864) Patterns Statistics Visualization

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

New Search

Save ▾ Create Table View Close

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

Time range: Last 24 hours

2,864 events (10/10/25 4:00:00.000 AM to 10/11/25 4:24:13.000 AM) No Event Sampling ▾

Job ▾

Timeline format ▾ Zoom Out Zoom to Selection Deselect

1 hour 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 dest\_ip 25  
a full\_quality\_domain\_name 5  
a index 1  
a linecount 2  
a punct 9  
a query\_id 100+  
a record 3  
a splunk\_server 1  
a src\_ip 42  
a src\_port 100+  
a timestamp 1  
+ Extract New Fields

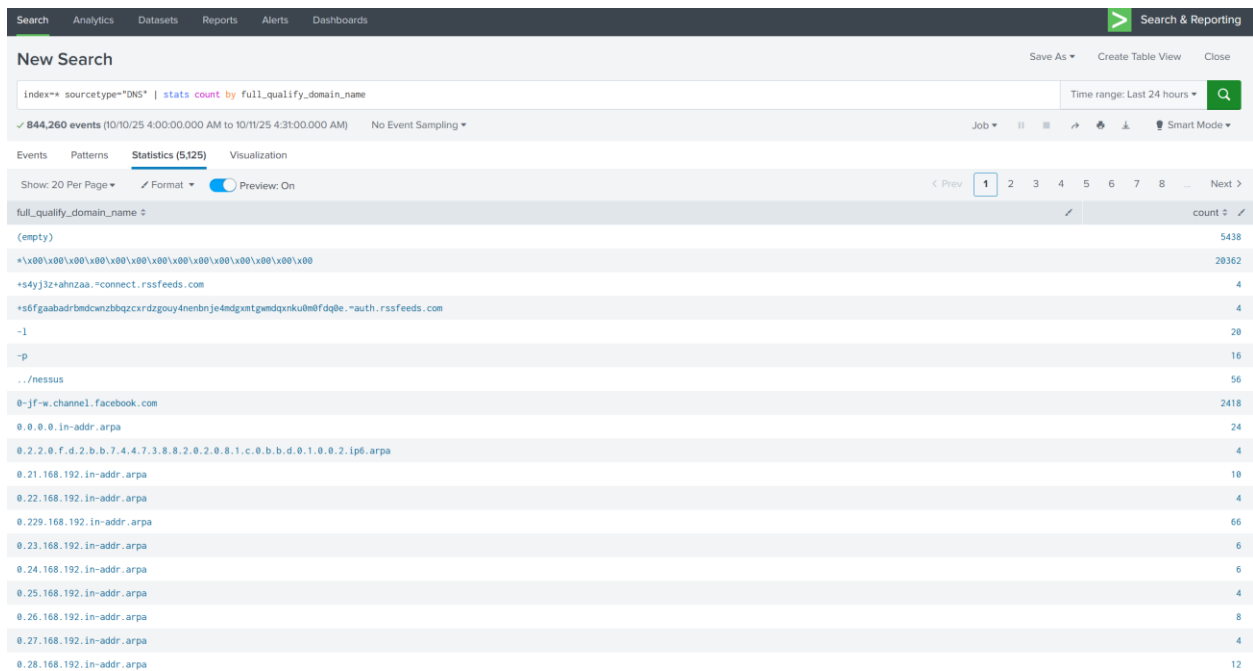
i	Time	Event
>	10/11/25 4:19:04.000 AM	1332015071.640000 CE21d03u5QatuJm1V1 192.168.202.141 58587 192.168.207.4 53 udp 61029 dns.msftncsi.com 1 C_INTERNET 1 A 3 NXDOMAIN F F T F 0 - - F
		host = LAPTOP-8HQPDA3I source = dns.log.gz sourcetype = DNS
>	10/11/25 4:19:04.000 AM	1332015071.640000 C52k91482zF10R5zVb 192.168.202.141 64157 192.168.207.4 53 udp 27206 dns.msftncsi.com 1 C_INTERNET 1 A 3 NXDOMAIN F F T F 0 - - F
		host = LAPTOP-8HQPDA3I source = dns.log.gz sourcetype = DNS
>	10/11/25 4:19:04.000 AM	1332014845.380000 CsD0kY3n5FVJD8xOfd 192.168.202.83 42686 192.168.207.4 53 udp 17755 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NXDOMAIN F F T F 0 - - F
		1332014826.740000 C8ox1B21WUnV7TL58 fe80::3e07:54ff:fe1c:a665 5353 ff02::fb 5353 udp 0 - - - - - - F F F 0 - - F
		1332014829.750000 C8ox1B21WUnV7TL58 fe80::3e07:54ff:fe1c:a665 5353 ff02::fb 5353 udp 0 - - - - - - F F 0 - - F
		1332014830.680000 C8ox1B21WUnV7TL58 fe80::3e07:54ff:fe1c:a665 5353 ff02::fb 5353 udp 0 - - - - - - F F 0 - - F
		1332014830.780000 C8ox1B21WUnV7TL58 fe80::3e07:54ff:fe1c:a665 5353 ff02::fb 5353 udp 0 - - - - - - F F 0 - - F
		Show all 257 lines host = LAPTOP-8HQPDA3I source = dns.log.gz sourcetype = DNS
>	10/11/25 4:19:04.000 AM	1332013421.100000 CkpEv51TPAr6DCsR53 192.168.202.157 55712 192.168.207.4 53 udp 14826 dns.msftncsi.com 1 C_INTERNET 1 A 3 NXDOMAIN F F T F 0 - - F
		host = LAPTOP-8HQPDA3I source = dns.log.gz sourcetype = DNS

### 3. Identity Threat or Unusual Pattern

- Analyze DNS activity to spot any unusual or suspicious patterns.
- Example query to highlight such events:

```
index=* sourcetype="DNS" | stats count by full_qualified_domain_name
```

This query counts the number of occurrences for each domain, helping to identify domains with abnormal or excessive query activity.



The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query: `index=* sourcetype="DNS" | stats count by full_qualified_domain_name`. The results are displayed in a table with two columns: `full_qualified_domain_name` and `count`. The table shows various domains and their corresponding counts, including some unusual entries like `*\x00\x00\x00` and `0.xxx.168.192.in-addr.arpa`.

full_qualified_domain_name	count
(empty)	5438
*\x00\x00\x00	20362
+s4yJ3z+ahnZaa.-connect.rssfeeds.com	4
+s6fgaabdrbmdcmzbbqzcxrdzgouy4nenbnje4mdgxtgwmqnxku@mfqle.-auth.rssfeeds.com	4
-l	20
-p	16
./nessus	56
0-jf-w.channel.facebook.com	2418
0.0.0.0.in-addr.arpa	24
0.2.2.0.f.d.2.b.b.7.4.4.7.3.8.8.2.0.2.0.8.1.c.0.b.b.d.0.1.0.0.2.ip6.arpa	4
0.21.168.192.in-addr.arpa	10
0.22.168.192.in-addr.arpa	4
0.229.168.192.in-addr.arpa	66
0.23.168.192.in-addr.arpa	6
0.24.168.192.in-addr.arpa	6
0.25.168.192.in-addr.arpa	4
0.26.168.192.in-addr.arpa	8
0.27.168.192.in-addr.arpa	4
0.28.168.192.in-addr.arpa	12

With this search, we see the anomalies in DNS activity

- `*\x00\x00\x00` look like encoded entries, it might be from corrupted DNS packet or malformed queries.
- `0.xxx.168.192.in-addr.arpa`, this one is reverse DNS lookups, so it is when an IP address is queried to find its hostname. It is normal but the large number of these could indicate that malicious activity going on here.

**New Search** Save As Create Table View Close

Index\*\* sourcetype="DNS" | top full\_qualify\_domain\_name,src\_ip Time range: Last 24 hours Q

✓ 844,260 events (10/10/25 4:00:00.000 AM to 10/11/25 4:34:18.000 AM) No Event Sampling Job || ≡ ↶ ↷ ⬇ ⬆ Smart Mode

Events Patterns **Statistics (10)** Visualization

Show: 20 Per Page Format Preview: On

full_qualify_domain_name	src_ip	count	percent
teredo.ipv6.microsoft.com	10.10.117.210	54850	6.554826
www.apple.com	192.168.202.93	21206	2.534214
tools.google.com	10.10.117.210	20358	2.432874
44.206.168.192.in-addr.arpa	192.168.202.83	14312	1.710350
HPE8AA67	192.168.202.76	13576	1.622394
time.apple.com	192.168.202.93	11764	1.405852
imap.gmail.com	192.168.203.63	10866	1.298537
WPAD	192.168.202.76	10152	1.213211
api.facebook.com	192.168.202.103	8190	0.978743
api.twitter.com	192.168.202.103	8178	0.977308

Now we get the top queried domains and can see what stand out.

### 1.Random looking names

- Here, the example is HPE8AA67, which looks like a random hostname or misconfigured local device but it is not a standard fully qualified domain name

### 2. Extremely high query count

- in this case, teredo.ipv6.microsoft.com has 54850 queries. Teredo is a Windows IPv6 tunneling protocol, but with so many queries like this could indicate automated or misconfiguration. Should check the source ip (10.10.117.210)

### 3. Reverse DNS lookups

- 44.206.168.192.in-addr.arpa, this is a reversed lookup, which is normal, but with the high count could indicate something.

### 4. Well-known service

- The rest like [www.apple.com](http://www.apple.com), [imap.gmail.com](mailto:imap.gmail.com), or [api.twitter.com](https://api.twitter.com) are normal network activity from users.

So in this case, HPE8AA67 and teredo. ipv6.microsoft is suspicious and worth investigating further.

## Conclusion

Analyzing DNS (Domain Name System) logs with Splunk helps security teams quickly detect and investigate suspicious activity. By studying DNS traffic and spotting unusual patterns, organizations can improve their security and reduce the risk of cyber threats.