



DNS Log Analysis Using Splunk Project

By Gaurav Ghandat

📌 Project Overview

This project demonstrates how to **ingest, parse, and analyze DNS logs** using **Splunk Enterprise**.

By leveraging **Zeek-style JSON DNS logs**, we perform meaningful security and traffic analysis using **Splunk Search Processing Language (SPL)**.

The lab focuses on identifying:

- Frequently queried domain names
- Most active client IPs
- Distribution of DNS record types
- Potential anomalies in DNS behavior

🎯 Objectives

By completing this project, you will learn how to:

- Ingest JSON-formatted DNS logs into Splunk
- Extract useful DNS metadata (queries, IPs, record types)
- Write SPL queries for DNS traffic analysis
- Detect suspicious or abnormal DNS activity
- Build a strong foundation for DNS-based threat detection

🛠 Tools & Technologies

- **Splunk Enterprise**
- **Zeek DNS Logs (JSON format)**
- **Search Processing Language (SPL)**

Dataset Information

The dataset consists of **Zeek-style DNS logs** in JSON format with fields such as:

ts → Timestamp

id.orig_h → Source IP address

id.resp_h → DNS server IP

qtype → DNS query type (A, AAAA, PTR, CNAME)

query → Queried domain name

answers → DNS response

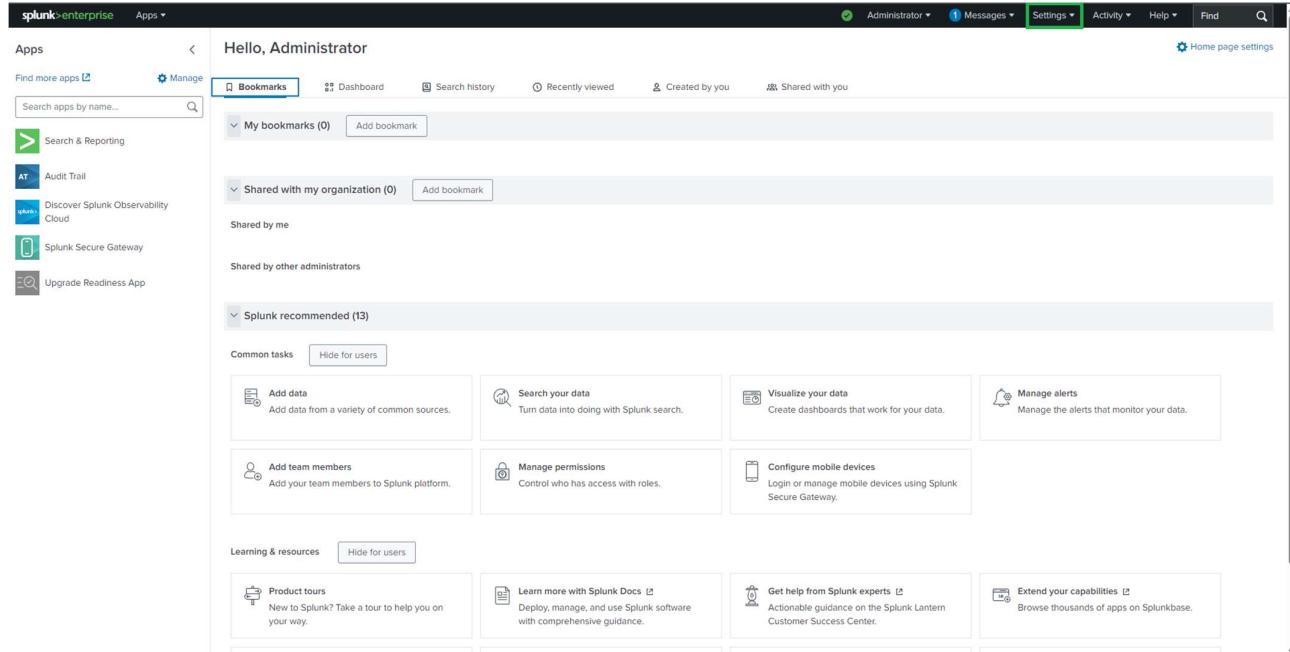
rcode → DNS response code

rtt → Round Trip Time

Lab Setup & Data Ingestion

Step 1: Upload DNS Logs

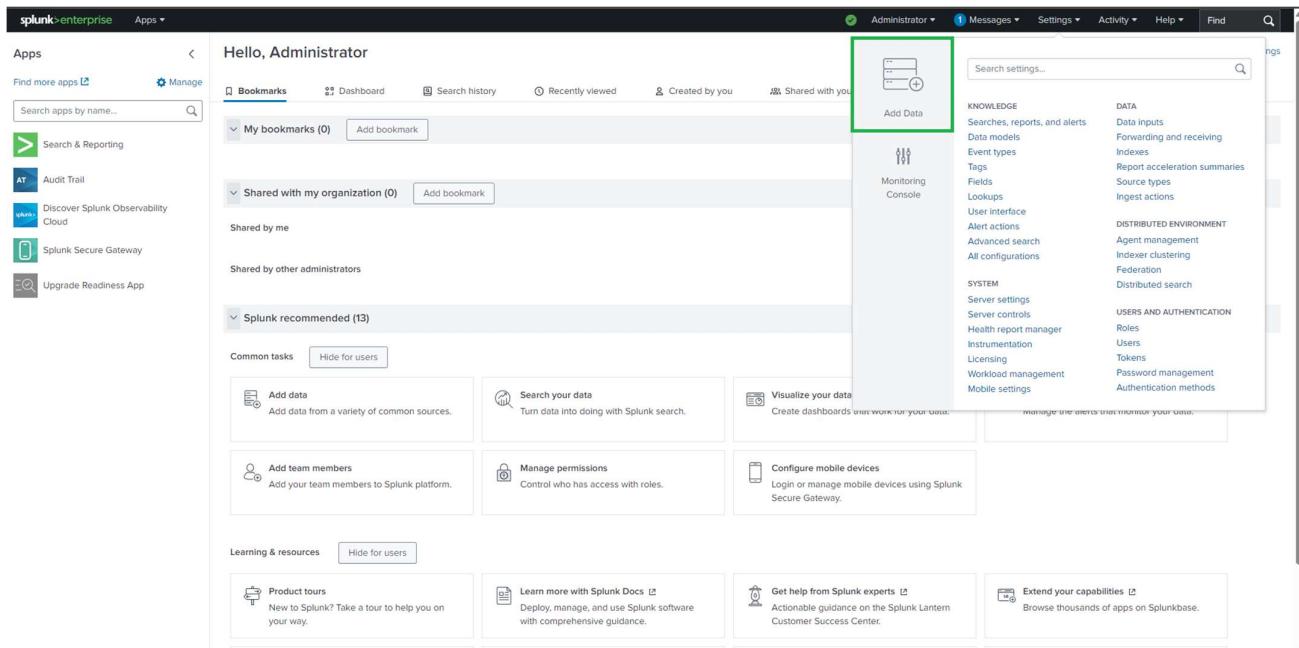
1. Open Splunk Web



The screenshot shows the Splunk Web interface for an administrator. The top navigation bar includes links for Administrator, Messages, Settings, Activity, Help, Find, and a search bar. The main content area starts with a "Hello, Administrator" greeting. Below it is a "Bookmarks" section with a button to "Add bookmark". Further down are sections for "Shared with my organization" and "Splunk recommended (13)" which lists various tasks: Add data, Search your data, Visualize your data, Manage alerts, Add team members, Manage permissions, Configure mobile devices, Product tours, Learn more with Splunk Docs, Get help from Splunk experts, and Extend your capabilities.

2. Navigate to:

Settings → Add Data → Upload



The screenshot shows the Splunk Enterprise homepage with the 'Administrator' user logged in. A green box highlights the 'Add Data' icon in the top navigation bar. The main content area displays various common tasks and recommended actions. On the right side, a sidebar menu is open, also with a green box highlighting the 'Add Data' section. The sidebar includes categories such as KNOWLEDGE, DATA, SYSTEM, and USERS AND AUTHENTICATION.

Splunk Recommended (13)

- Add data
- Search your data
- Visualize your data
- Add team members
- Manage permissions
- Configure mobile devices
- Product tours
- Learn more with Splunk Docs
- Get help from Splunk experts
- Extend your capabilities

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

- Cloud computing: 10 data sources
- Networking: 2 data sources
- Operating System: 1 data source
- Security: 3 data sources

4 data sources in total

Or get data in with the following methods

- Upload files from my computer
- Monitor files and ports on this Splunk platform instance
- Forward data from a Splunk forwarder

127.0.0.1:8000/en-USmanager/search/adddatamethods/selectsource?input_mode=1

3. Select the file:

The screenshot shows the Splunk Add Data interface with the 'Select Source' step highlighted. The 'Selected File: No file selected' message is displayed. A green box highlights the 'Select File' button and the 'Open' button in the file selection dialog.

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: No file selected
Select File

Drop your data file here
The maximum file upload size is 500 Mb

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?

Open
File name: dns_logs
File type: All Files
Open Cancel

Drop your data file here
The maximum file upload size is 500 Mb

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/manage/search/adddatamethods/selectsource?input_mode=0#

4. dns_logs.json

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The current step is 'Select Source'. A file named 'dns_logs.json' has been selected and uploaded successfully. The 'Next >' button is highlighted in green.

5. Set the following:

- **Source Type:** json (or custom zeek:dns)
- **Index:** dns_lab (recommended)

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The current step is 'Set Source Type'. A preview of the DNS log data is shown in a table format. The first few rows of the table are as follows:

	_time	aa	answers	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	IN	qclass	qtype	query	ra	rcode	rd	rejected	rtt
1	4/23/25 2:51:09.069 PM	false	alias.google.com	192.168.1.12	58167	192.168.1.11	53	udp	IN	CNAME	google.com	true	NOERROR	true	false	0.397165	
2	4/23/25 2:51:09.069 PM	false	192.168.10.114	192.168.1.12	13629	192.168.1.3	53	udp	IN	A	fileserver.local	true	NOERROR	true	false	0.451793	
3	4/23/25 2:51:09.069 PM	false	192.168.40.147	192.168.1.18	40231	192.168.1.3	53	udp	IN	A	backup.local	true	NOERROR	true	false	0.458119	
4	4/23/25 2:51:09.069 PM	false	alias.fileserver.local	192.168.1.17	3446	192.168.1.2	53	udp	IN	CNAME	fileserver.local	true	NOERROR	true	false	0.23946	
5	4/23/25 2:51:09.069 PM	false	192.168.1.17.in-addr.arpa	192.168.1.17	25615	192.168.1.2	53	udp	IN	PTR	google.com	true	NOERROR	true	false	0.30075	
6	4/23/25 2:51:09.069 PM	false	192.168.1.17.in-addr.arpa	192.168.1.17	16271	192.168.1.2	53	udp	IN	PTR	ipv6test.local	true	NOERROR	true	false	0.134111	
7	4/23/25 2:51:09.069 PM	false	192.168.208.219	192.168.1.16	63770	192.168.1.2	53	udp	IN	A	google.com	true	NOERROR	true	false	0.091741	
8	4/23/25 2:51:09.069 PM	false	192.168.195.9	192.168.1.10	19707	192.168.1.3	53	udp	IN	A	microsoft.com	true	NOERROR	true	false	0.167656	
9	4/23/25 2:51:09.069 PM	false	alias.backup.local	192.168.1.14	32719	192.168.1.3	53	udp	IN	CNAME	backup.local	true	NOERROR	true	false	0.342481	
10	4/23/25 2:51:09.069 PM	false	192.168.82.34	192.168.1.12	8592	192.168.1.11	53	udp	IN	A	router.local	true	NOERROR	true	false	0.44890	
11	4/23/25 2:51:09.069 PM	false	alias.printer.local	192.168.1.17	29930	192.168.1.2	53	udp	IN	CNAME	printer.local	true	NOERROR	true	false	0.319641	
12	4/23/25 2:51:09.069 PM	false	192.168.70.240	192.168.1.21	57366	192.168.1.3	53	udp	IN	A	google.com	true	NOERROR	true	false	0.411965	

splunk enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done

Input Settings

Optional 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: LAPTOP-EHJ3QFJI

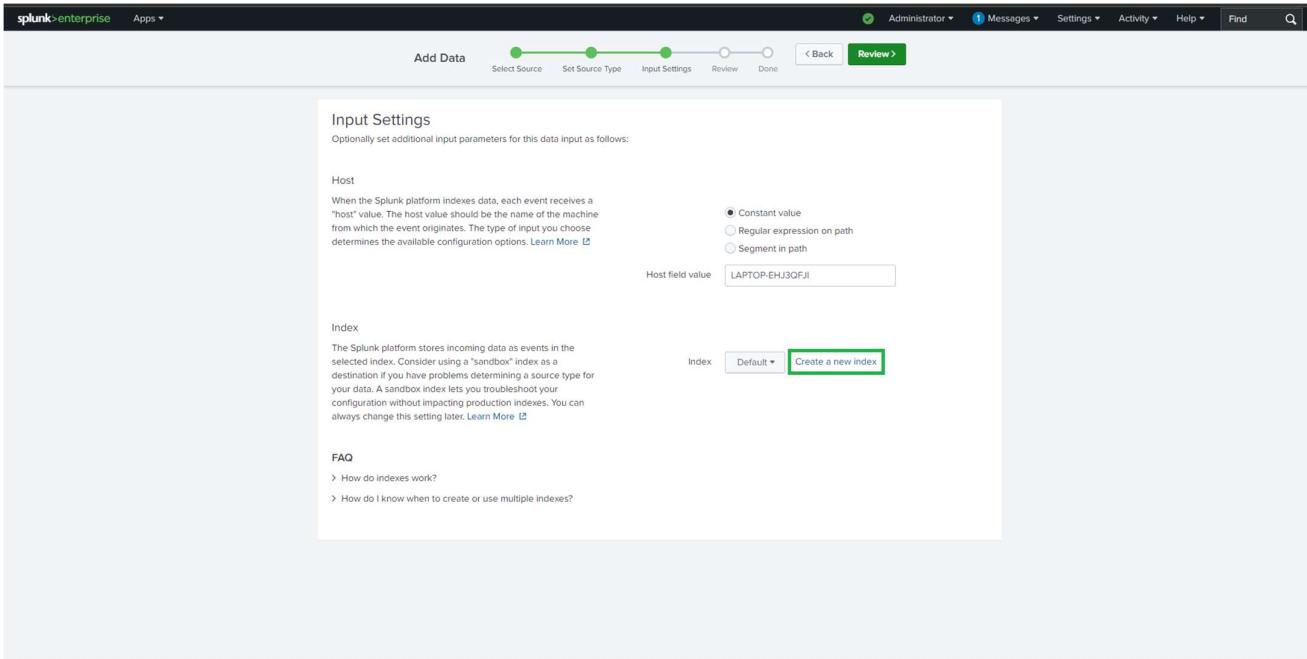
Index

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: Default ▾ **Create a new Index**

FAQ

> How do indexes work?
> How do I know when to create or use multiple indexes?



splunk enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

New Index

General Settings

Index Name: Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events Metrics

Home Path: optional Hot/warm db path. Leave blank for default (\$\$SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional Cold db path. Leave blank for default (\$\$SPLUNK_DB/INDEX_NAME/coldb).

Thawed Path: optional Thawed/resurrected db path. Leave blank for default (\$\$SPLUNK_DB/INDEX_NAME/thawedb).

Data Integrity Check: Enable Disable

Max Size of Entire Index: 500 GB ▾ Maximum target size of entire index.

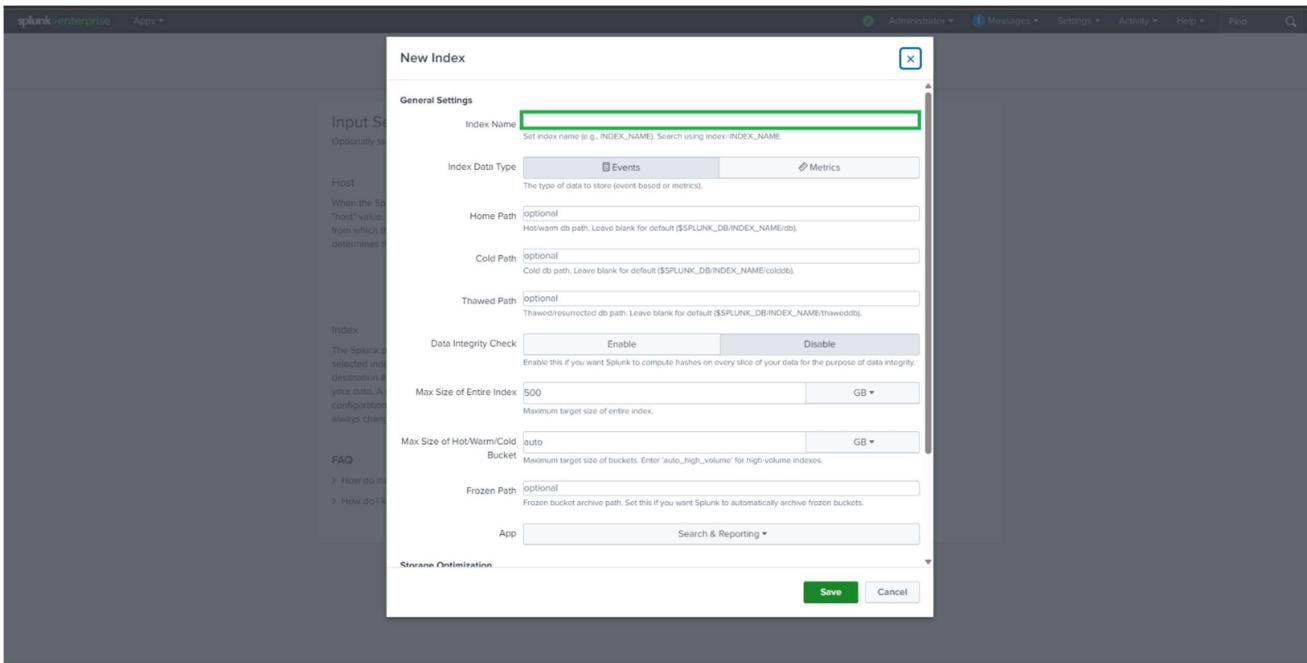
Max Size of Hot/Warm/Cold Bucket: auto GB ▾ Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting ▾

Storage Optimization

Save Cancel



New Index

General Settings

Index Name: dns_lab

Index Data Type: Events

Home Path: optional

Cold Path: optional

Thawed Path: optional

Data Integrity Check: Enable

Max Size of Entire Index: 500 GB

Max Size of Hot/Warm/Cold Bucket: auto

Frozen Path: optional

App: Search & Reporting

Storage Optimization

Save **Cancel**

Add Data

Select Source **Set Source Type** Input Settings Review Done **Review >**

Input Settings

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: LAPTOP-EHJ3QFJI

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 Default Create a new index

- ✓ Default
 - dns_lab
 - history
 - main
 - summary

FAQ

> How do indexes work?
 > How do I know when to create or use multiple indexes?

127.0.0.1:8000/en-USmanager/search/adddatamethods/inputsettings#

splunk>enterprise Apps ▾

Administrator ▾ i Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Review >

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: LAPTOP-EHJ3QFJI

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: dns_lob Create a new index

FAQ

- › How do indexes work?
- › How do I know when to create or use multiple indexes?

splunk>enterprise Apps ▾

Administrator ▾ i Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

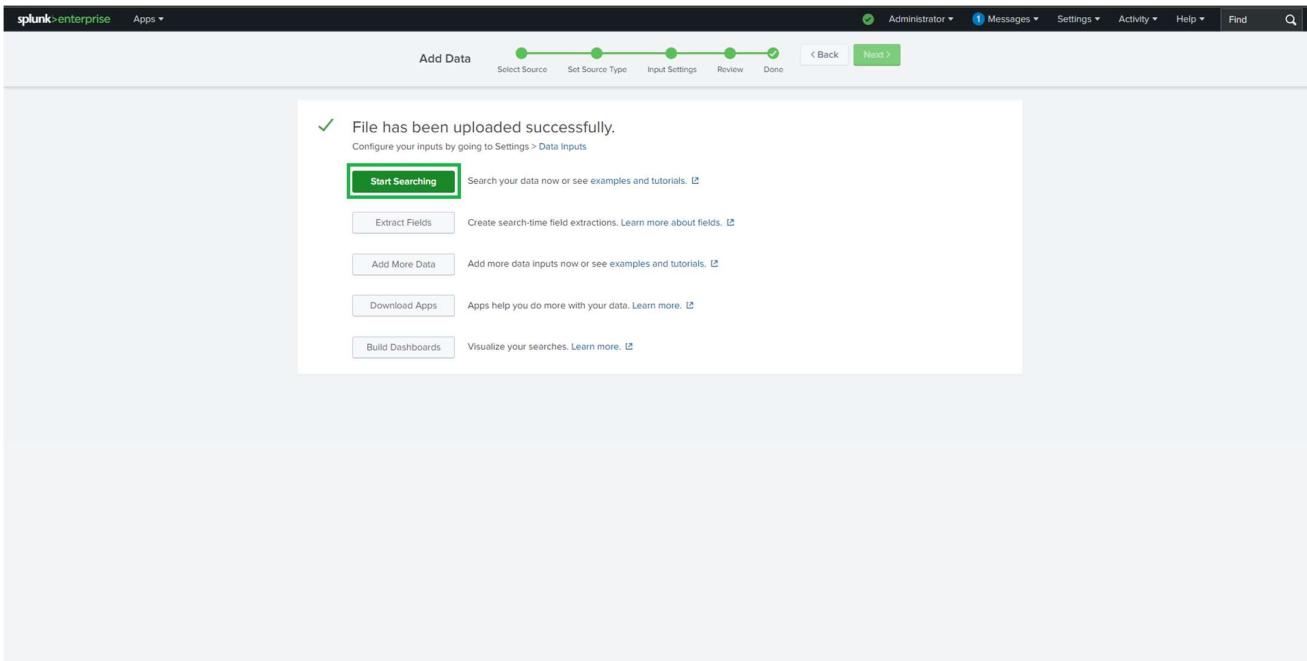
Add Data

Select Source Set Source Type Input Settings Review Done

< Back Submit >

Review

Input Type: Uploaded File
File Name: dns_logs.json
Source Type: json
Host: LAPTOP-EHJ3QFJI
Index: dns_lob



Step 2: Verify Data Ingestion

Run the following query to confirm logs are indexed:

index=dns_lab | head 5

The screenshot shows the search results for the query 'index=dns_lab | head 5'. The search bar at the top contains the query. The results table shows one event from April 23, 2025, at 2:51:09.087 PM. The event details are as follows:

Time	Event
4/23/25 2:51:09.087 PM	<pre>> 4/23/25 2:51:09.087 PM { [-] aa: false answers: 192.168.1.18.in-addr.arpa id.orig_h: 192.168.1.18 id.orig_p: 21008 id.resp_h: 192.168.1.1 id.resp_p: 53 proto: udp qClass: IN qType: PTR query: yahoo.com rai: true rcode: NOERROR rd: true rejected: false rtt: 8.169253 tc: false trans_id: 10013 ts: 2025-04-23T09:21:09.087977Z ttl: 185 uid: C672252Y2156 }</pre>

Below the table, it says 'Show as raw text' and lists the host, source, and sourcetype: 'host = LAPTOP-EHJ3QFJL | source = dns_logs.json | sourcetype = _json'.

Lab Tasks & SPL Queries

◆ Task 1: Most Frequently Queried Domain Names

Identify which domains are queried most often.

```
index=dns_lab
```

```
| stats count by query
```

```
| sort -count
```

📌 **Use Case:** Detect suspicious domains, beaconing behavior, or malware C2 lookups.

The screenshot shows the Splunk Enterprise search interface. The search bar at the top contains the SPL command: `index=dns_lab | head 5 | stats count by query | sort -count`. Below the search bar, the results table displays the following data:

query	count
microsoft.com	2
google.com	1
printer.local	1
yahoo.com	1

◆ Task 2: Most Active Client IPs

Find which internal hosts generate the most DNS traffic.

```
index=dns_lab
```

```
| stats count by "id.orig_h"
```

```
| sort -count
```

📌 **Use Case:** Identify compromised systems or misconfigured devices.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=dns_lab | stats count by "id.orig_h" | sort -count
- Results:** 1,200 events (before 12/27/25 7:52:37.000 PM) No Event Sampling
- Statistics View:** Shows 12 rows of IP addresses and their counts.
- Table Data:**

id.orig_h	count
192.168.1.10	113
192.168.1.18	113
192.168.1.21	112
192.168.1.20	105
192.168.1.12	102
192.168.1.13	99
192.168.1.16	97
192.168.1.17	96
192.168.1.19	95
192.168.1.11	92
192.168.1.15	89
192.168.1.14	87

◆ Task 3: DNS Query Type Breakdown

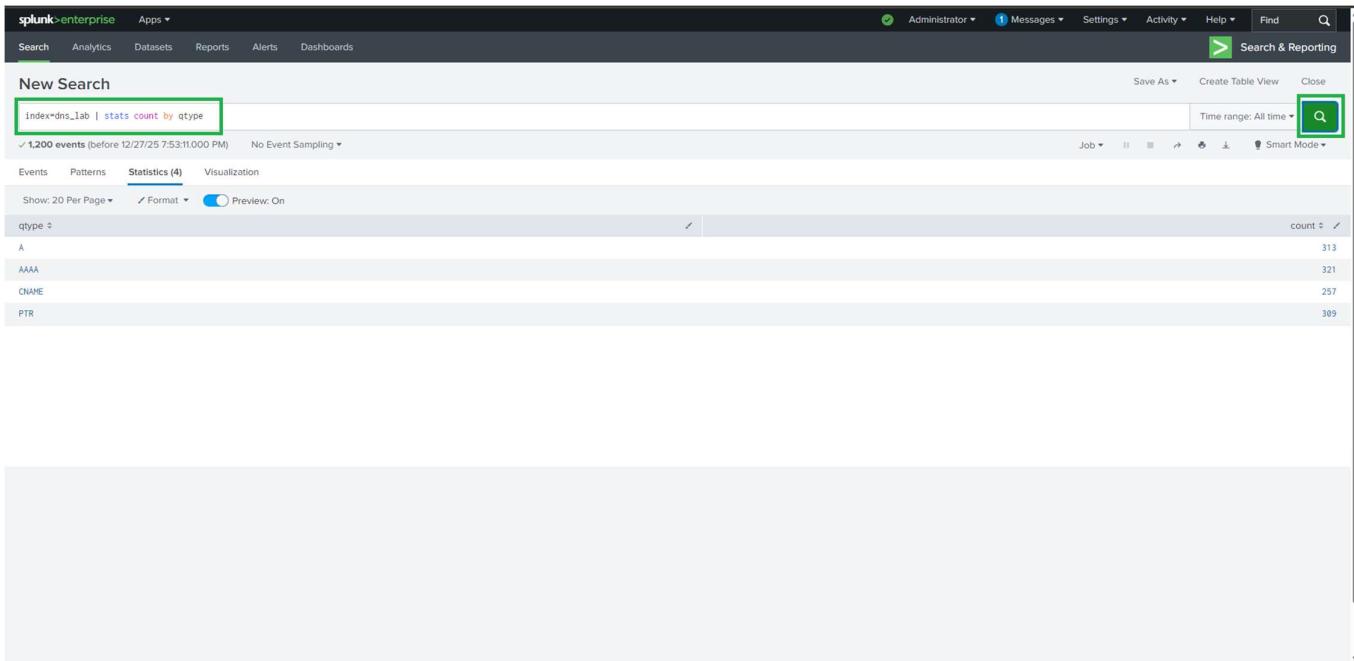
Analyze DNS record types used in the environment.

index=dns_lab

| stats count by qtype

📌 Use Case:

- PTR → Reverse lookups
- Excessive AAAA → IPv6 behavior
- CNAME → Redirect or alias usage



📈 Key Findings & Analysis

- Identified **top queried domains** such as Google, Microsoft, and Yahoo
- Detected **high-volume DNS-generating hosts**
- Observed distribution of **A, AAAA, CNAME, and PTR records**
- Analyzed **response times (RTT)** and failed lookups (NXDOMAIN)
- Established baseline DNS behavior for anomaly detection

Security Insights

This project enables detection of:

- DNS tunneling patterns
 - Malware beaconing via repeated queries
 - Suspicious reverse DNS lookups
 - Unusual DNS latency or failed resolutions
-

Dashboards & Alerts (Optional Enhancements)

You can extend this project by:

- Creating Splunk dashboards for DNS activity visualization
 - Setting alerts for:
 - High DNS query volume
 - Rare domain lookups
 - Excessive failed DNS responses
-

Conclusion

By completing this lab, you have:

- ✓ Successfully ingested and parsed DNS logs in Splunk
- ✓ Built SPL queries for DNS traffic analysis
- ✓ Identified top domains and active clients
- ✓ Analyzed DNS record types
- ✓ Gained hands-on experience in security-focused log analysis

This project serves as a **strong foundation for SOC, SIEM, and threat-hunting roles.**
