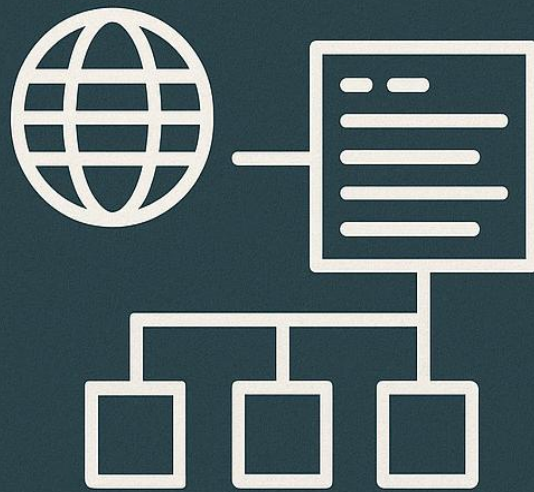


Splunk & DNS Log Analysis



MADE BY
Moez Javed

Splunk & DNS Log Analysis Lab Manual

Introduction

Splunk is a powerful SIEM (Security Information and Event Management) tool that allows cybersecurity professionals to analyze machine data, including logs from network devices, servers, and applications. This lab will guide students in installing Splunk, uploading logs (including DNS logs), analyzing the log data, and filtering it using Splunk's search and visualization capabilities.

Objectives

- By the end of this lab, students will be able to:
- Install and configure Splunk on their system.
- Upload various log files into Splunk.
- Perform DNS log analysis using Splunk queries.
- Understand how to extract meaningful information using Splunk Search Processing Language (SPL).
- Filter events using host, source, and regex.

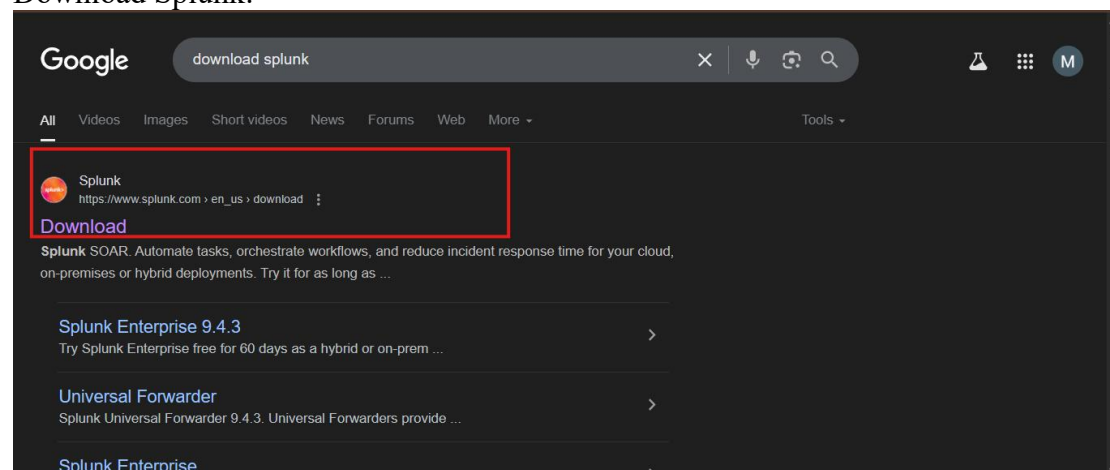
Lab Tasks

1. Install and configure Splunk on your system.
2. Upload a DNS log file.
3. Use Splunk queries to filter specific DNS events.
4. Analyze DNS traffic including queries, responses, and port information.
5. Generate a report based on your findings.

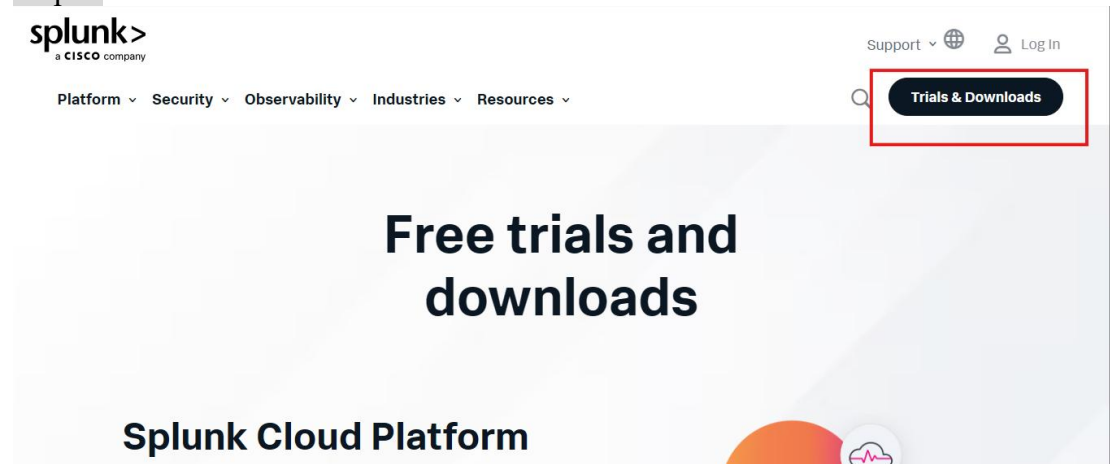
Step-by-Step Guide with Description

Step 1:

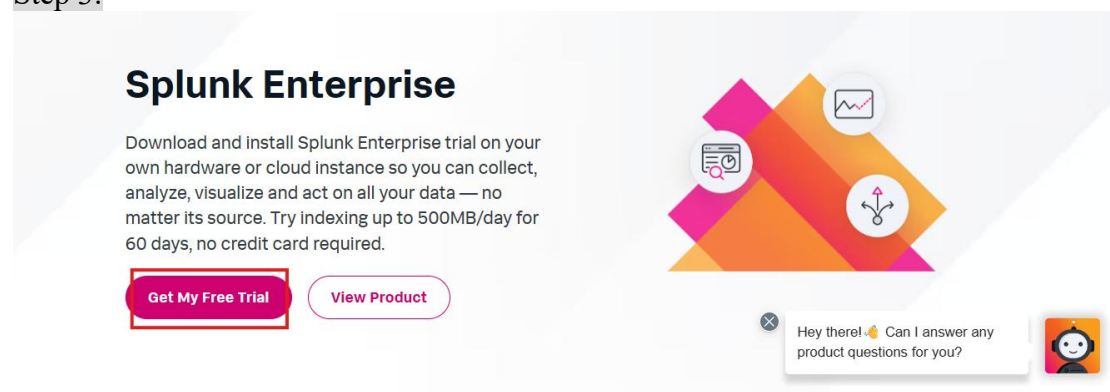
Download Splunk:



Step 2:

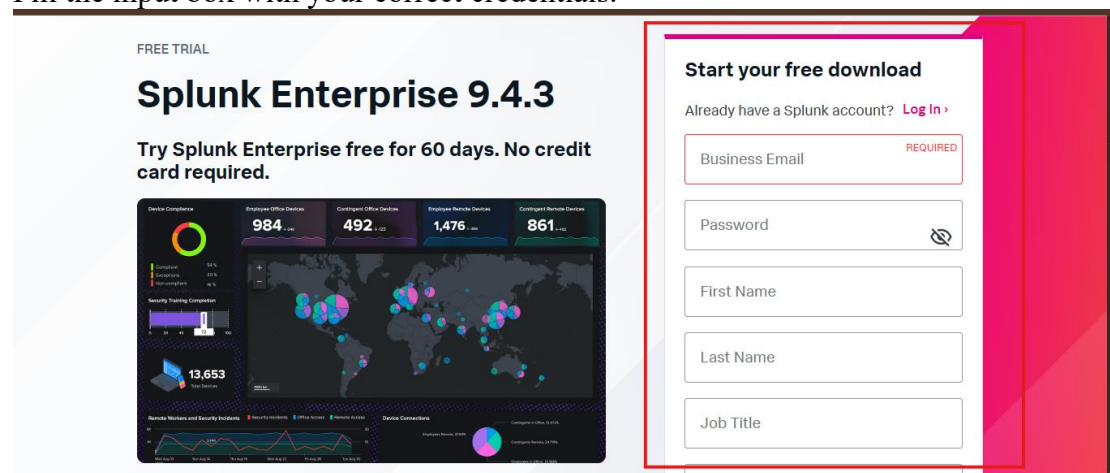


Step 3:



Step 4:

Fill the input box with your correct credentials.



Step 5:

Splunk Enterprise 9.4.3

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows

Linux

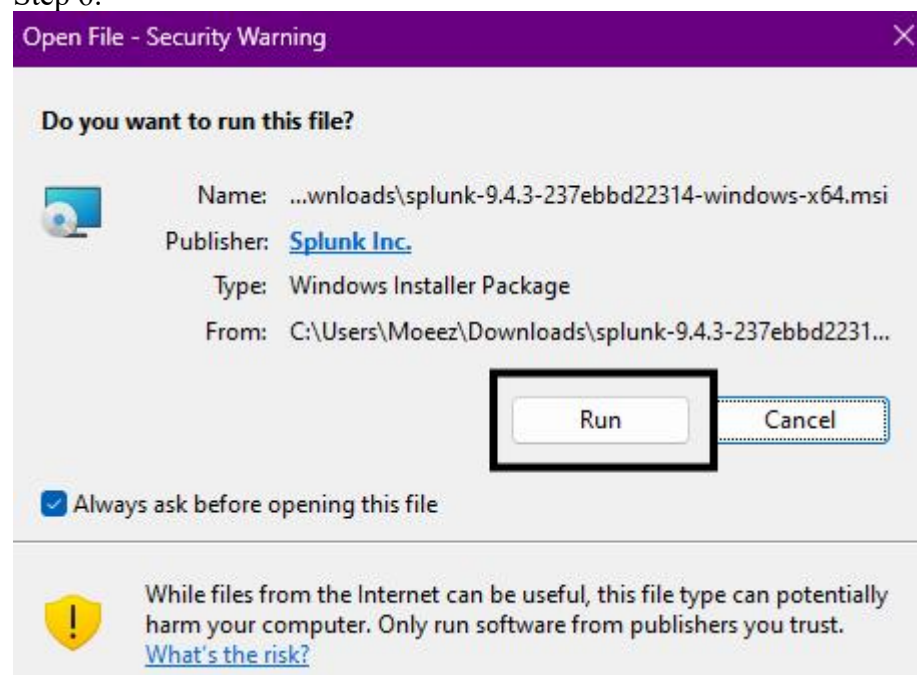
Mac OS

64-bit	Windows 10 Windows Server 2019, 2022	.msi	797.57 MB	Download Now	Copy wget link	More
--------	---	------	-----------	---------------------	----------------	------

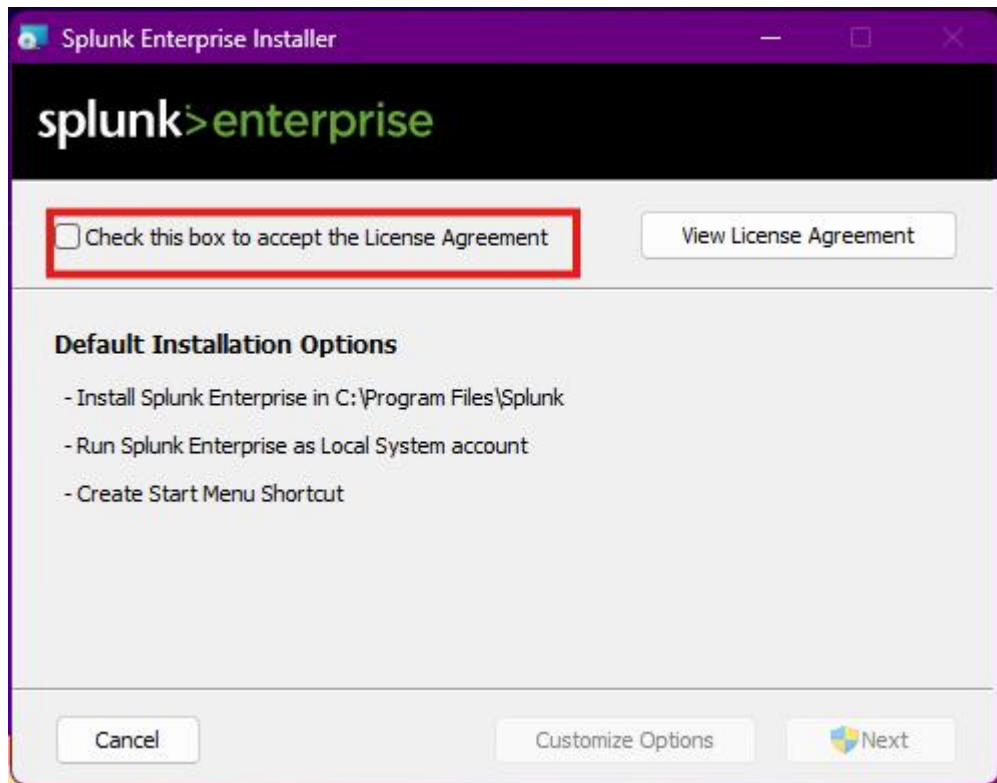
[Release Notes](#) | [System Requirements](#) | [Product Questions](#)

Hey there! Can I answer any product questions for you?

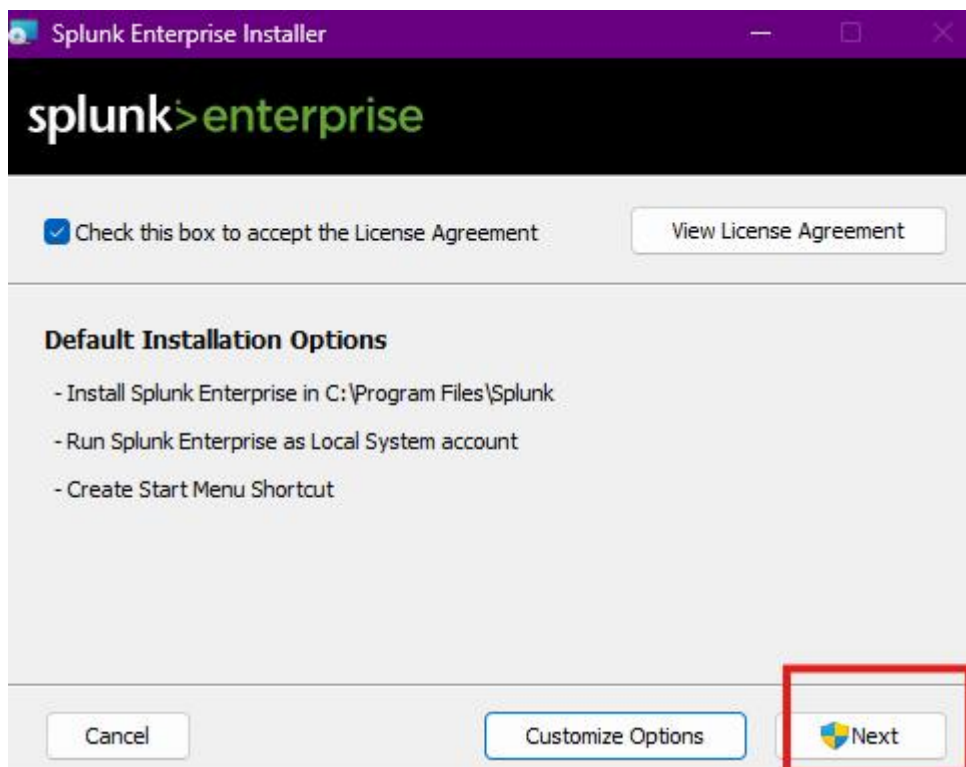
Step 6:



Step 7:

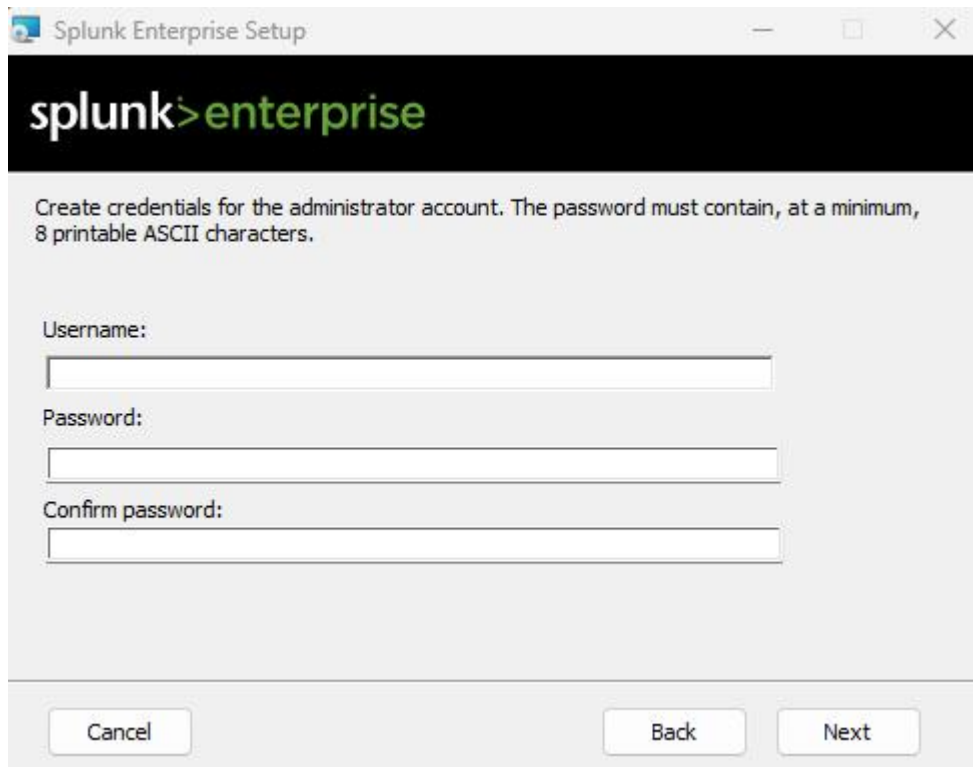


Step 8:



Step 9:

Your name and make password and remember your credentials for login further



Splunk Enterprise Setup

splunk>enterprise

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

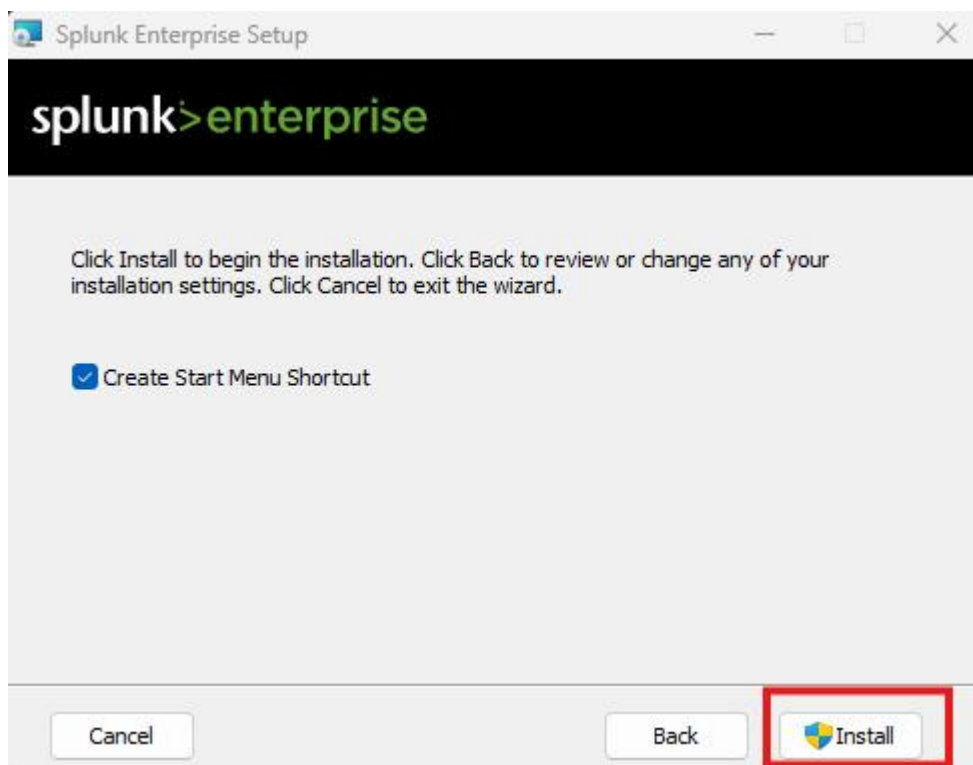
Username:

Password:

Confirm password:

Cancel Back Next

Step 10:



Splunk Enterprise Setup

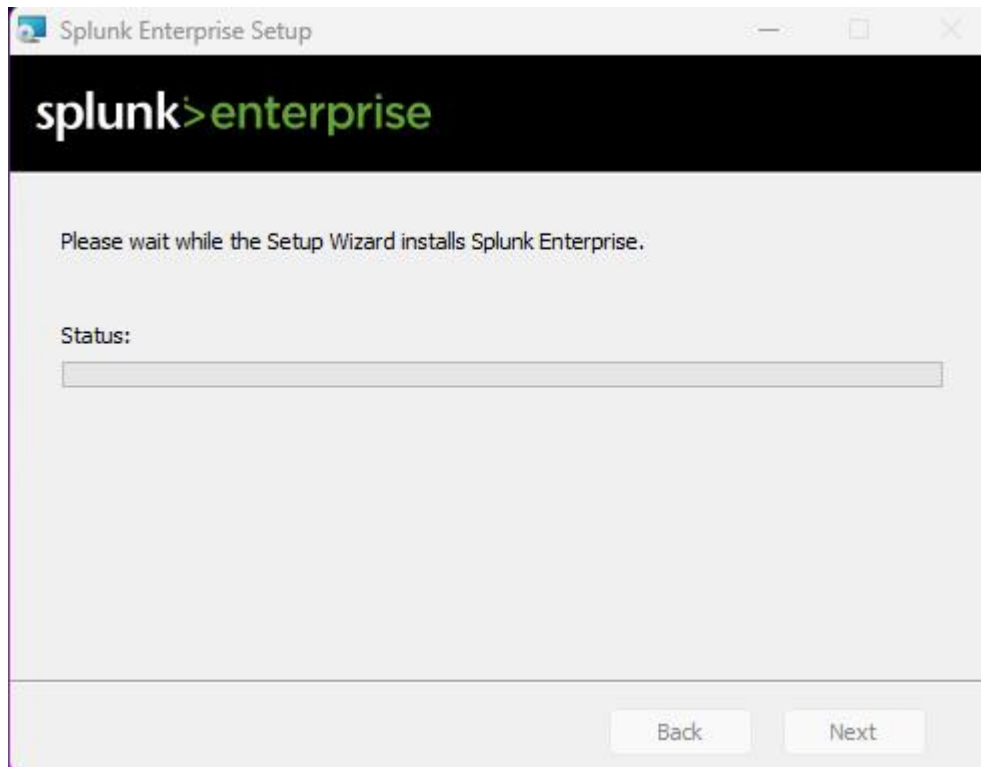
splunk>enterprise

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

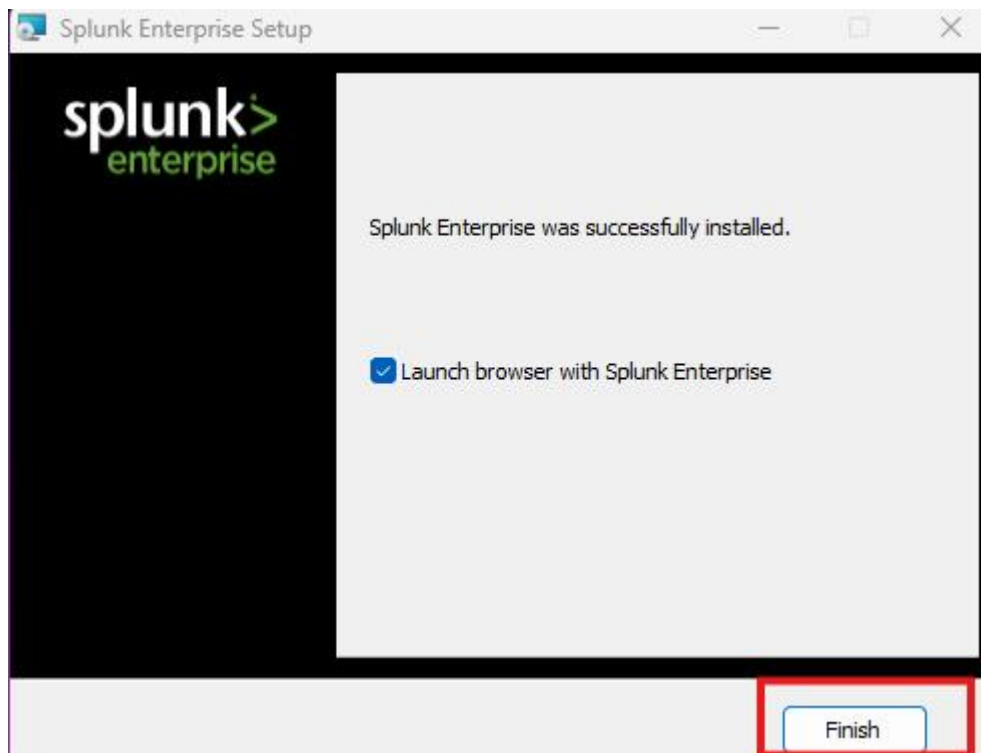
☒ Create Start Menu Shortcut

Cancel Back **Install**

Step 11:



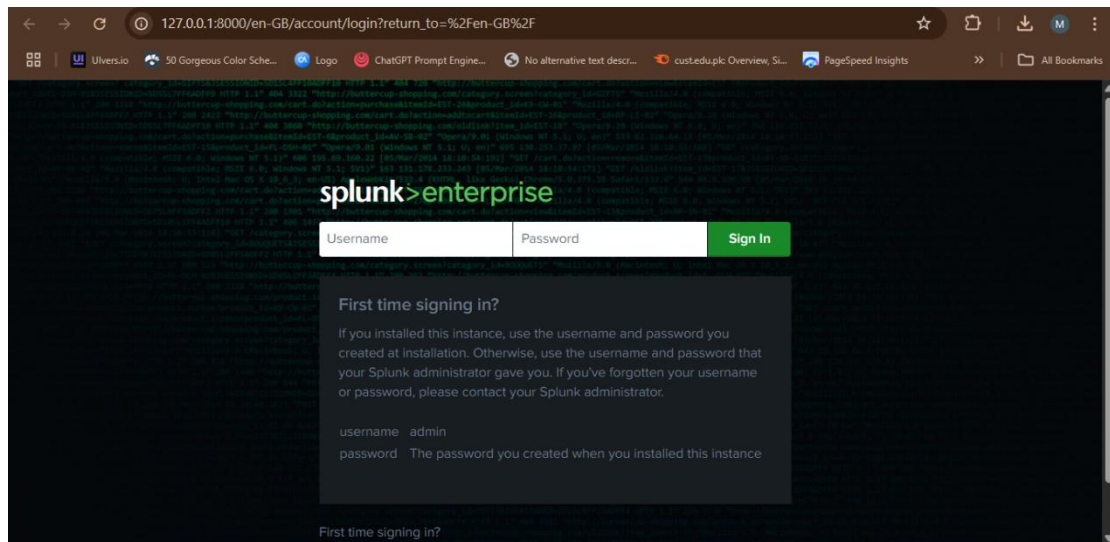
Step 12:



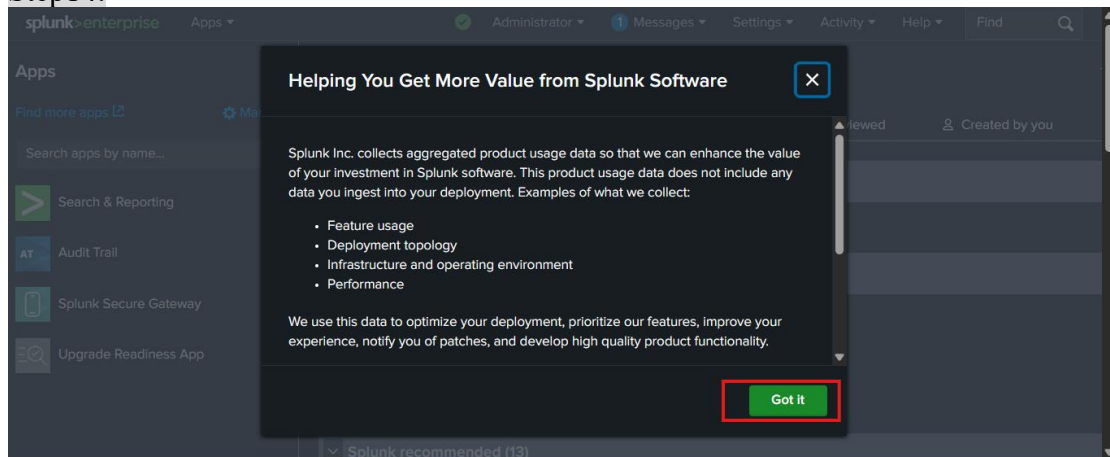
Step 13:

When you will click finish button than this will displayed.

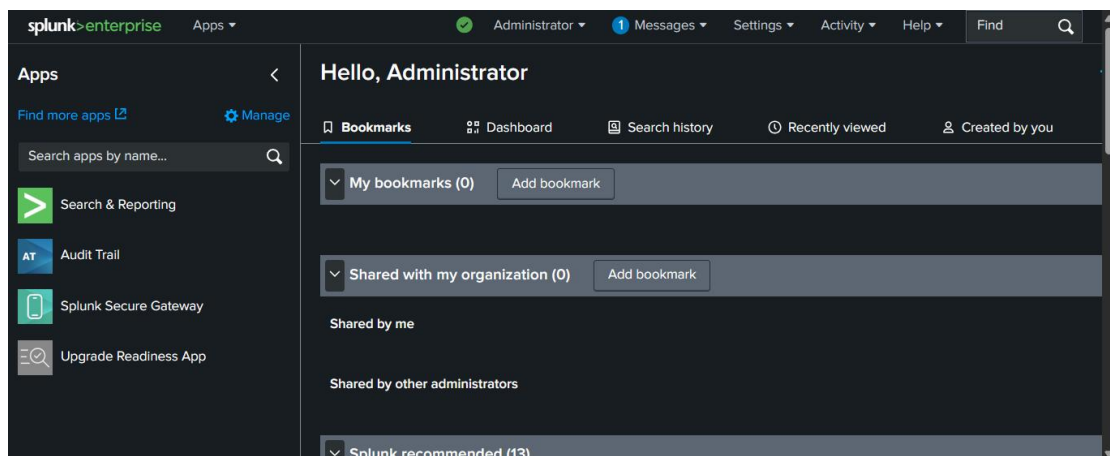
Made by Moez Javed



Step14:

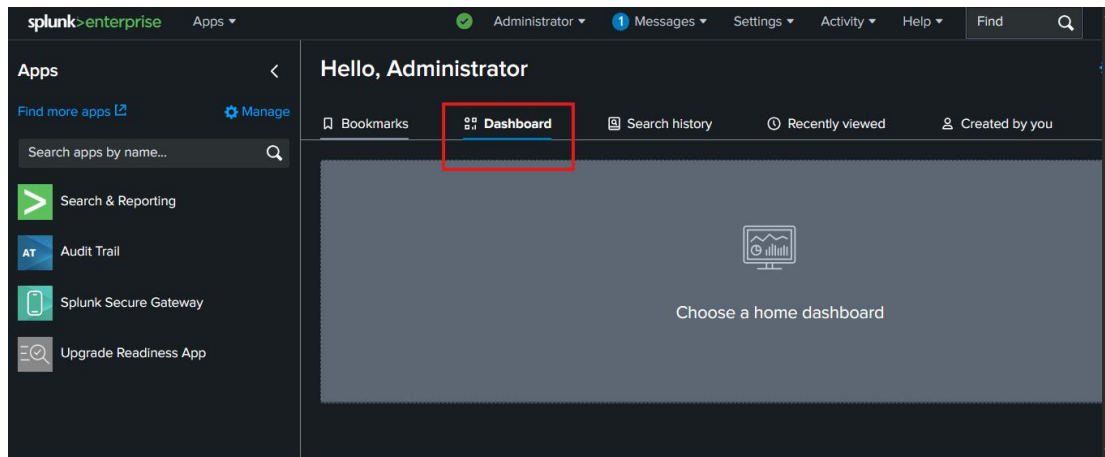


Step15:



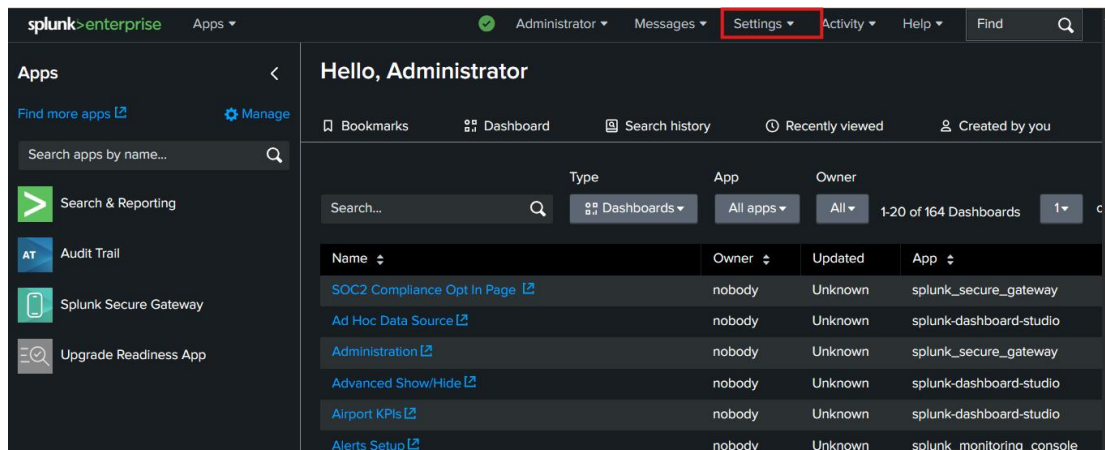
Step 16:

Made by Moez Javed

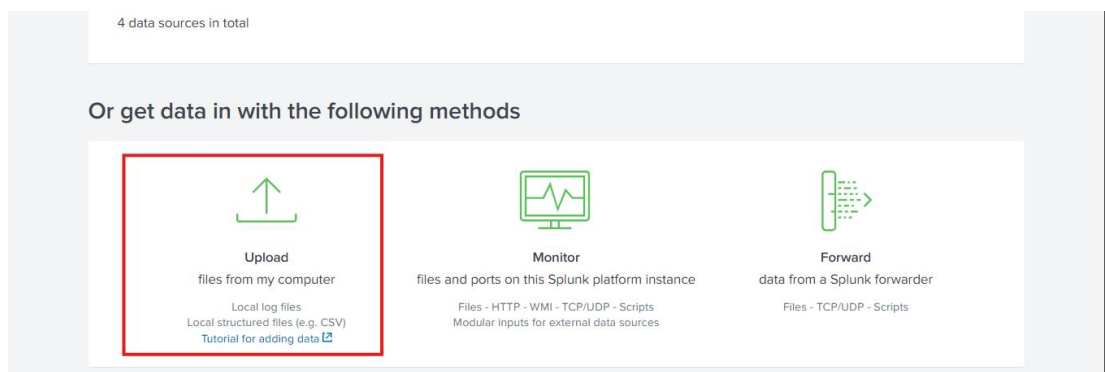


Part 2: Upload Log Files

Step 1:



Step 2:



Step 3:

splunk>enterprise Apps ▾ Administrator ▾ 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: **No file selected**

Select File

Drop your data file here

Step 4:

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

Add Data Select Source Set Source Type Input Settings Review Done < Back Next >

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**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

Step 5:

Select the source file and save it.

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** [View Event Summary](#)

Source type: default Save As

filter

Default Settings
Splunk's default source type settings

Application
Database
Email
Log to Metrics
Metrics

Format ▾ Show: 20 Per Page ▾ View: List ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

	Time	Event
		timestamp = none
2	17/06/2025 12:36:23.000	1331901015.070000 C36a282J1jz7BsbGH 192.168.202.76 137 192.168.202.255 137 udp 57402 HPE8AA67 1 C_INTERNET 32 NB - - F F T F 1 - - F

Step 6:

Save Source Type

×

Name

Database

Description

I found it from the link

Category

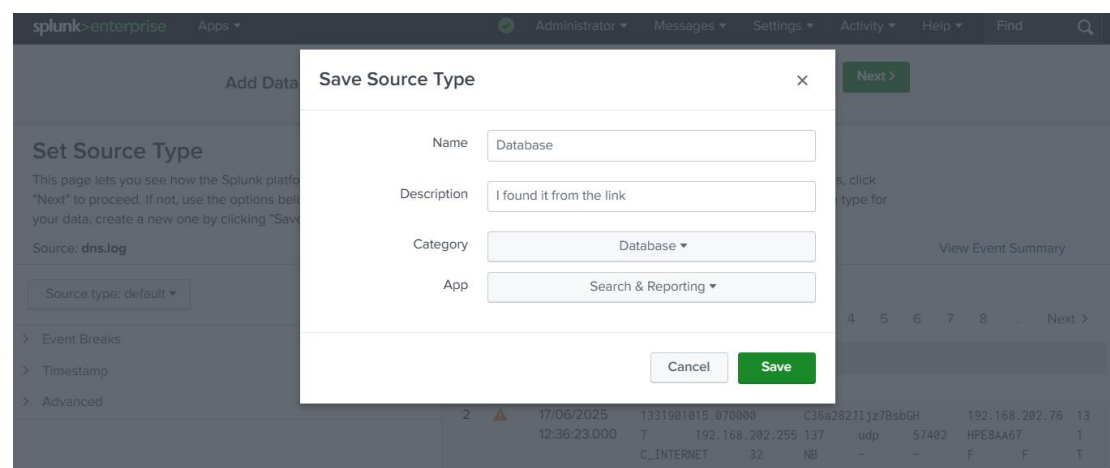
Database ▼

App

Search & Reporting ▼

Cancel

Save



Step 7:

Step 7:

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Next >

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**

Source type: default ▾

Save As

Format ▾

Show: 20 Per Page ▾

View: List ▾

< Prev

1

2

3

4

5

6

7

8

...

Next >

	Time	Event
1	17/06/2025 12:36:23.000	<div> <div>658</div> <div>192.168.27.203</div> <div>137</div> <div>udp</div> <div>33008</div> <div>*\x00\x00\x00\x00</div> <div>\x00\x00\x00\x00\x00\x00\x00\x00</div> <div>33</div> <div>SRV</div> <div>0</div> <div>NOERROR</div> <div>F</div> <div>F</div> <div>F</div> <div>F</div> <div>1</div> </div>

Event Breaks

Timestamp

Advanced

View Event Summary

Step 8:

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

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:

Index

Step :9

Add Data Select Source Set Source Type Input Settings **Review** Done < Back **Submit >**

Review

Input Type Uploaded File
File Name dns.log
Source Type Database
Host DESKTOP-FIH108V
Index Default

splunk>enterprise Apps ▾ Administrator ▾ 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](#).

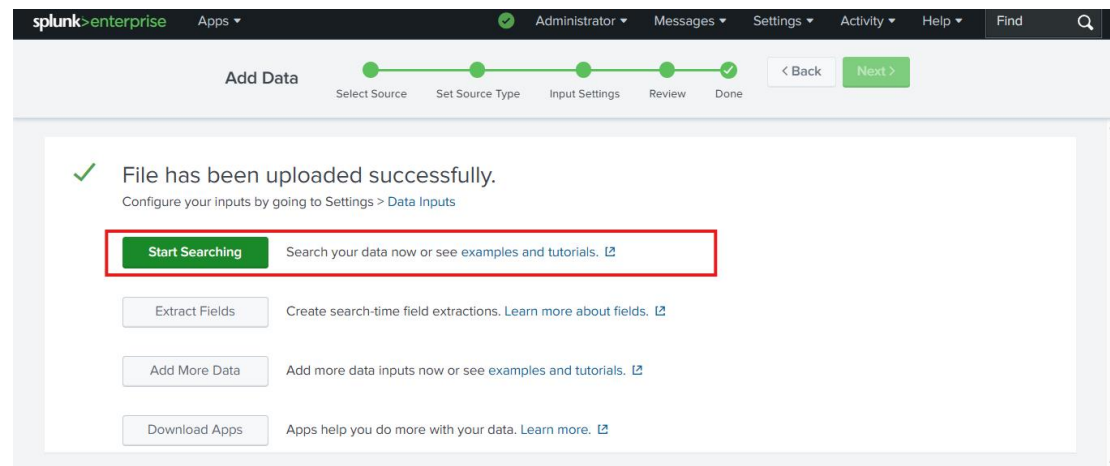
Extract Fields Create search-time field extractions. [Learn more about fields](#).

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](#).

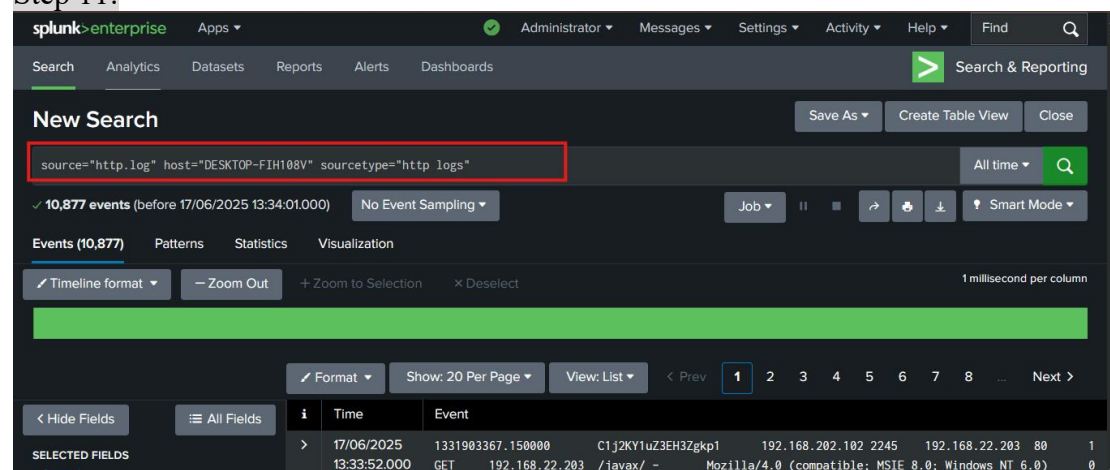
Build Dashboards Visualize your searches. [Learn more](#).

Step 10:

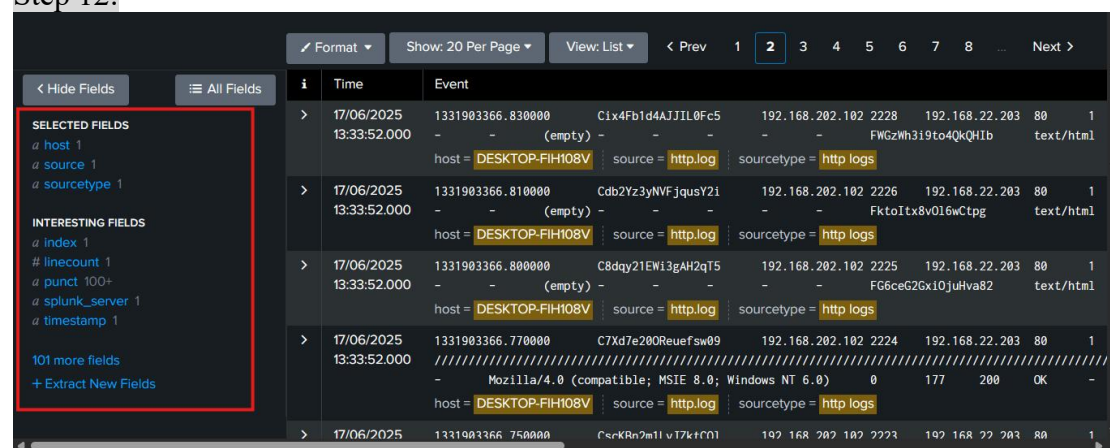


Part 3: Analyzing DNS Logs

Step 11:



Step 12:



Step 13:

How much total logs and source of logs.

source

1 Value, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
http.log	10,877	100%

Step 14:

source

1 Value, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
http.log	10,877	100%

Step 15:

source

1 Value, 100% of events

Selected Yes No

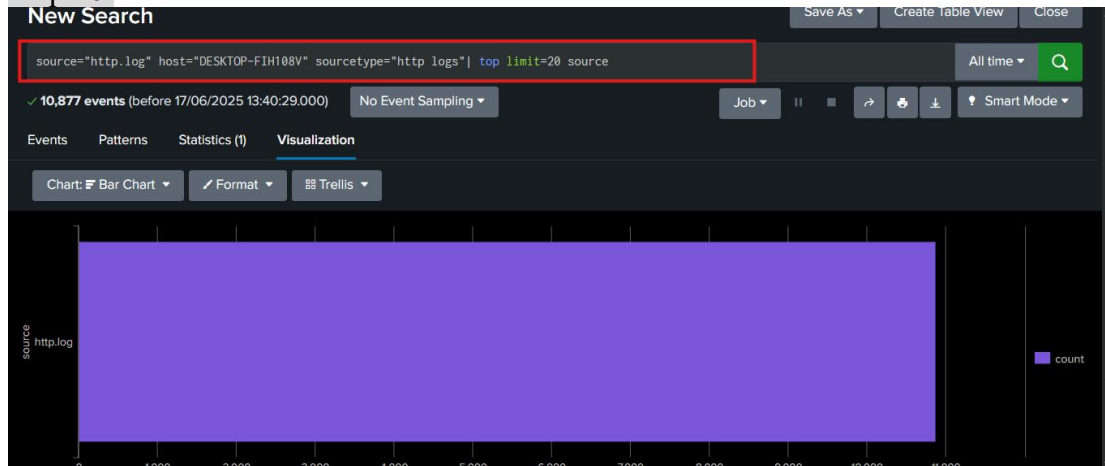
Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
http.log	10,877	100%

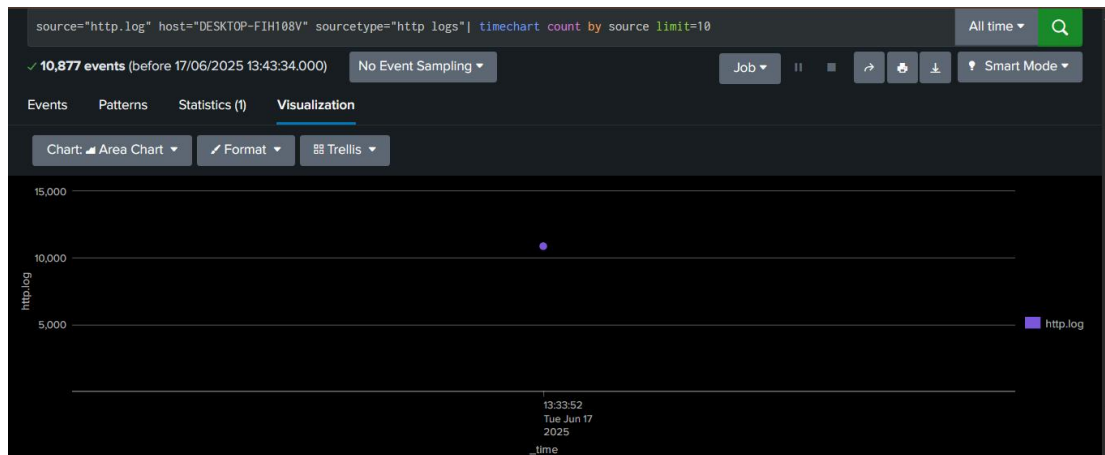
Step 16:



Step 17:

Now Select the Top value by Time:

Made by Moez Javed



Step 18 :

It show splunk server details

The image shows the 'splunk_server' field details in Splunk. The left sidebar lists interesting fields: `index` (1), `linecount` (1), `punct` (100+), `splunk_server` (1), and `timestamp` (1). The main panel shows the field's value, reports, and a table of values.

Values	Count	%
DESKTOP-FIH108V	10,877	100%

Part 4: Installing Add-ons in Splunk

Now in this we learn how to download more application in splunk.

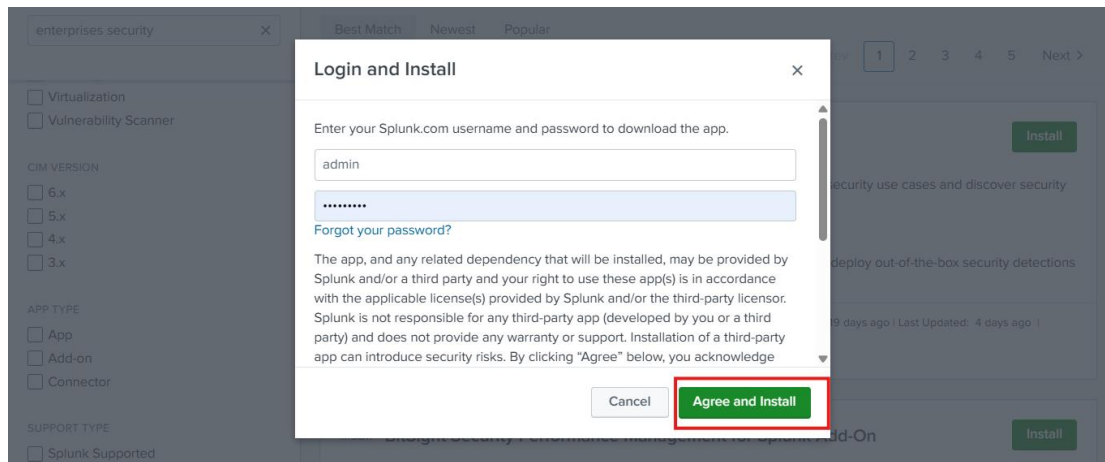
Step 1:

The image shows the Splunk App Store interface with the following details:

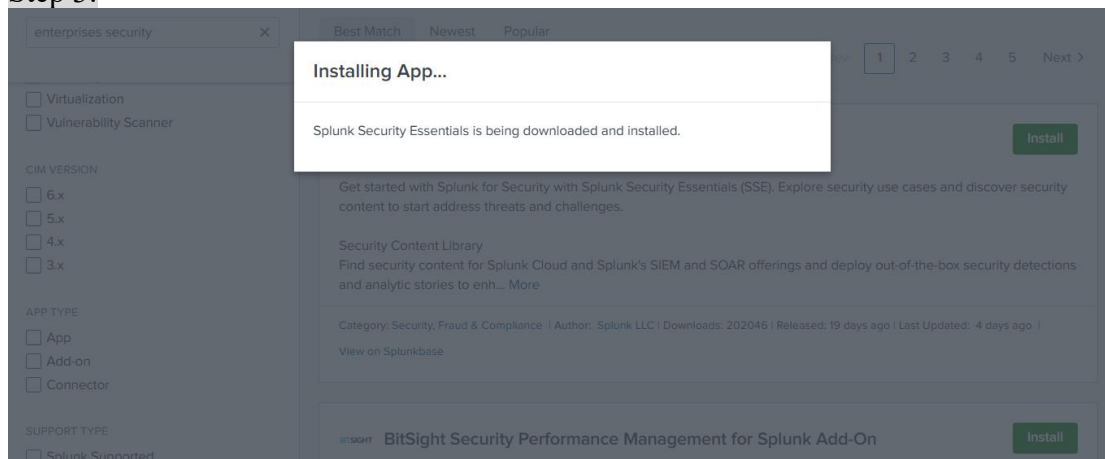
- Search Bar:** `enterprises security`
- Filters:** Virtualization, Vulnerability Scanner, CIM VERSION (6.x, 5.x, 4.x, 3.x), APP TYPE (App, Add-on, Connector), SUPPORT TYPE (Splunk Supported).
- Results:** 89 Apps. The first result is 'Splunk Security Essentials' (SSE) with an 'Install' button highlighted. The second result is 'BitSight Security Performance Management for Splunk Add-On' with an 'Install' button.

Step 2:

Made by Moez Javed



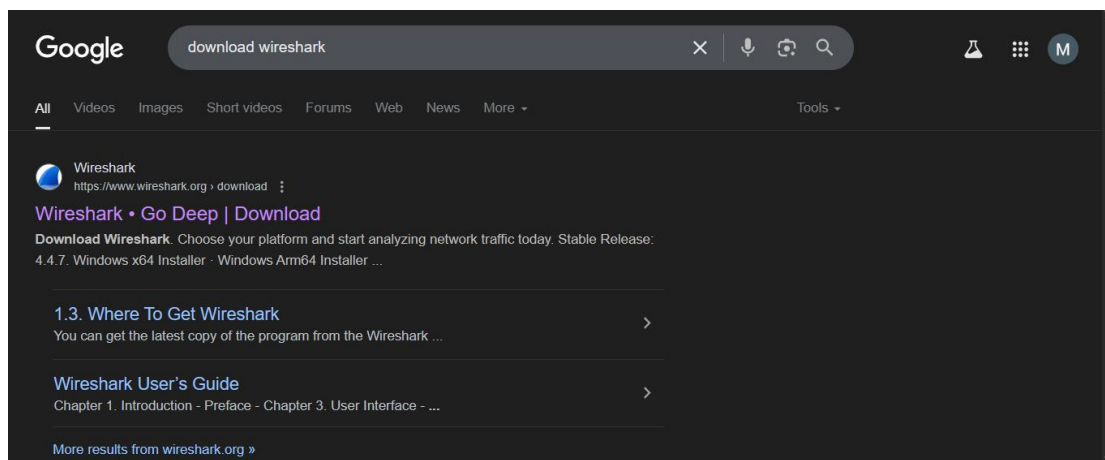
Step 3:



Part 5: Wireshark Log Collection

Step 1:

Download Wireshark:

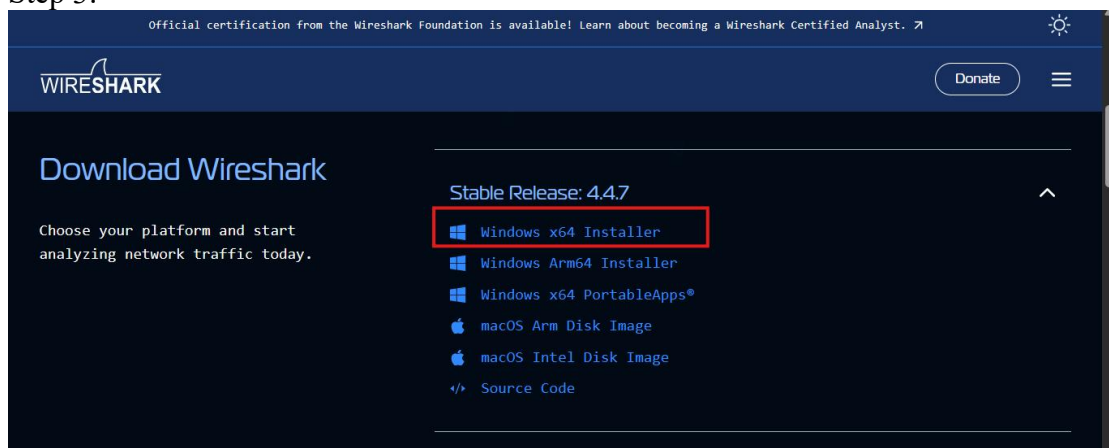


Step 2:

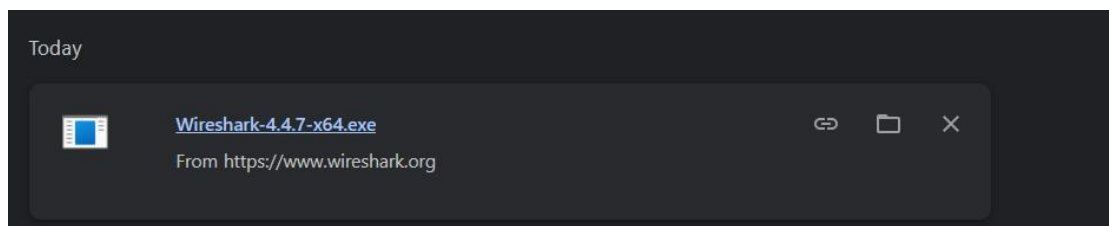
Made by Moez Javed



Step 3:

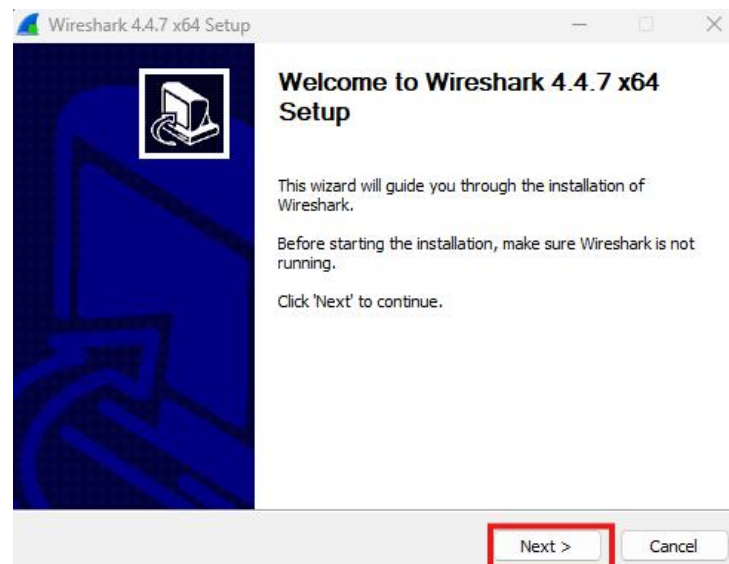


Step 4:

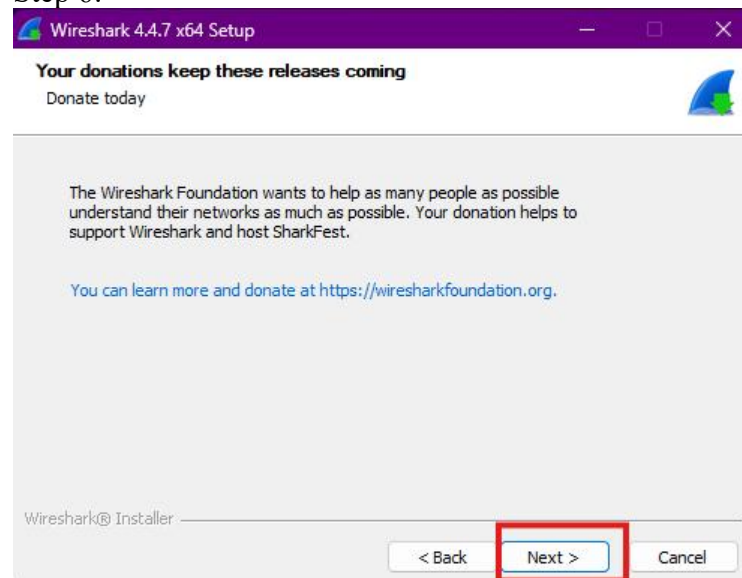


Step 5:

Made by Moez Javed

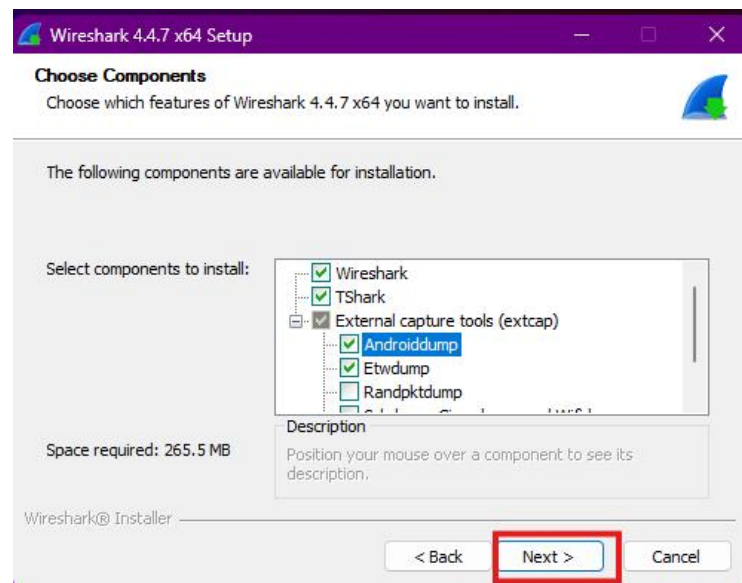


Step 6:

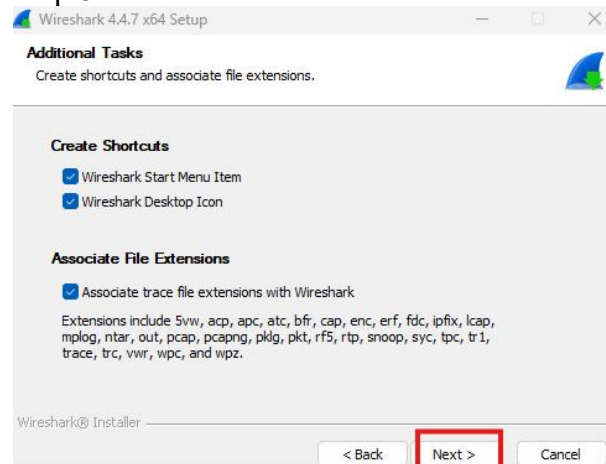


Step 7:

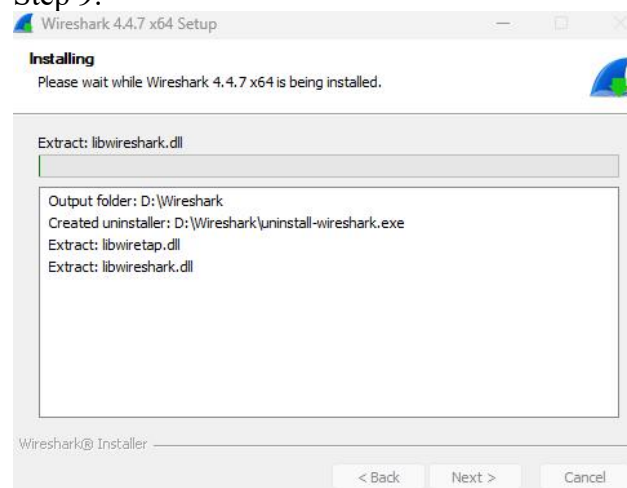
Made by Moez Javed



Step 8:

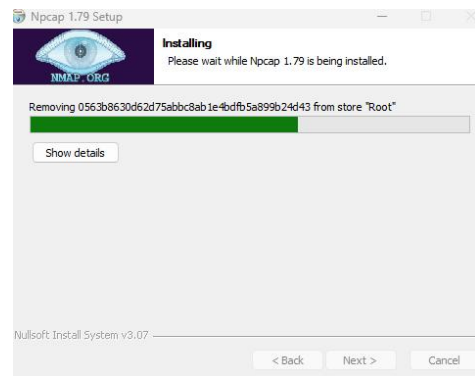


Step 9:

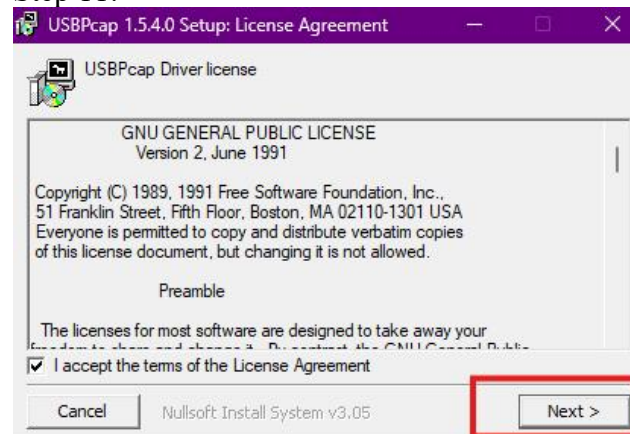


Step 10:

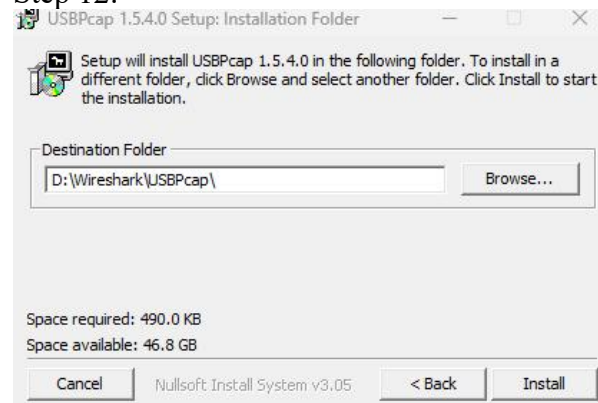
Made by Moez Javed



Step 11:



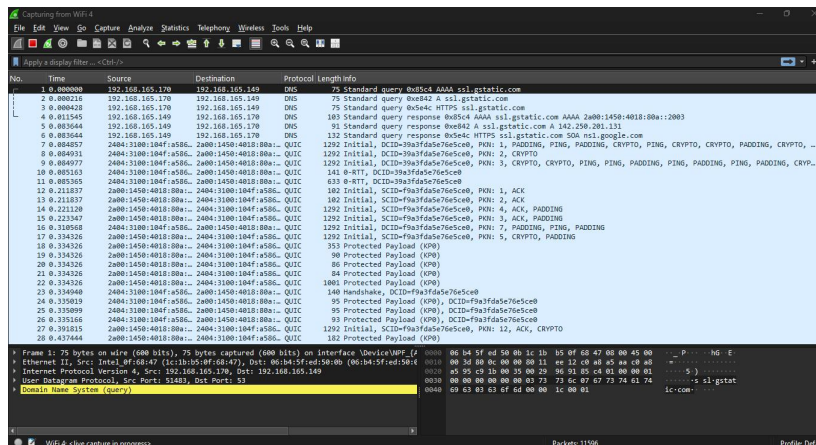
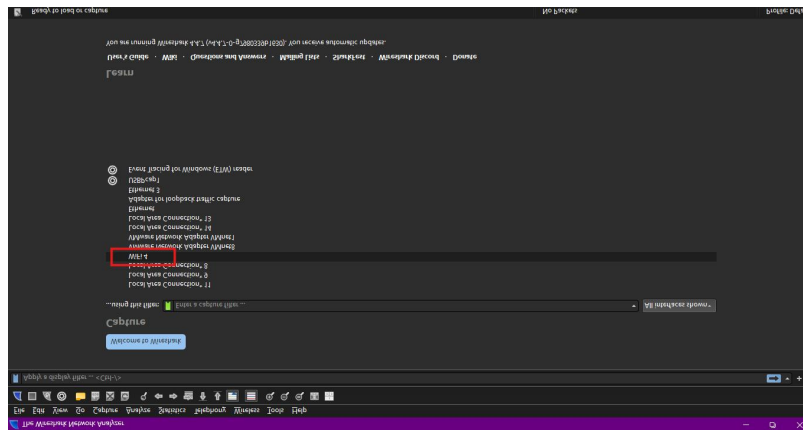
Step 12:



Now installed.

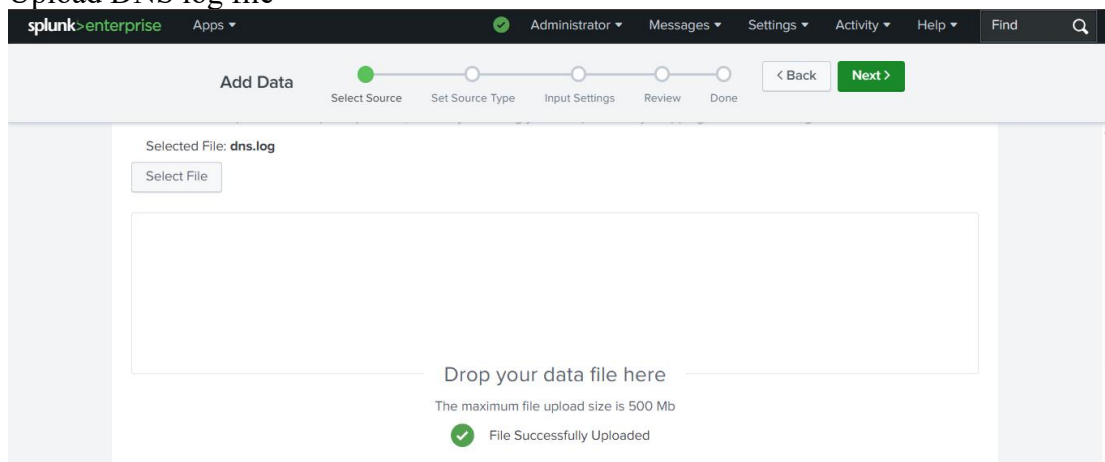
Now opening the Wireshark:

Made by Moez Javed



You may download the log and check it in splunk.
DNS Log Analysis:

Step 1: Upload DNS log file



Step 2:

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

Add Data ● ● ○ ○ ○ < Back Next >

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** View Event Summary

Source type: default ▾ **Save As** ✓ Format ▾ Show: 20 Per Page ▾ View: List ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

	Time	Event
1	17/06/2025 13:56:56.000	1331901005.510000 CWGtK431H9XuaTN4f1 192.168.202.100 45 658 192.168.27.203 137 udp 33008 *\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00 1 C_INTERNET 33 SRV 0 NOERROR F F F F 1

Step 3:

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

Add Data ● ● ● ○ ○ < Back Next >

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** View Event Summary

Source type: default ▾

> Event Breaks
> Timestamp
> Advanced

Save Source Type ✕

Name

Description

Category

App

Cancel **Save**

Step 4:

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

Add Data ● ● ● ○ ○ < 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](#)

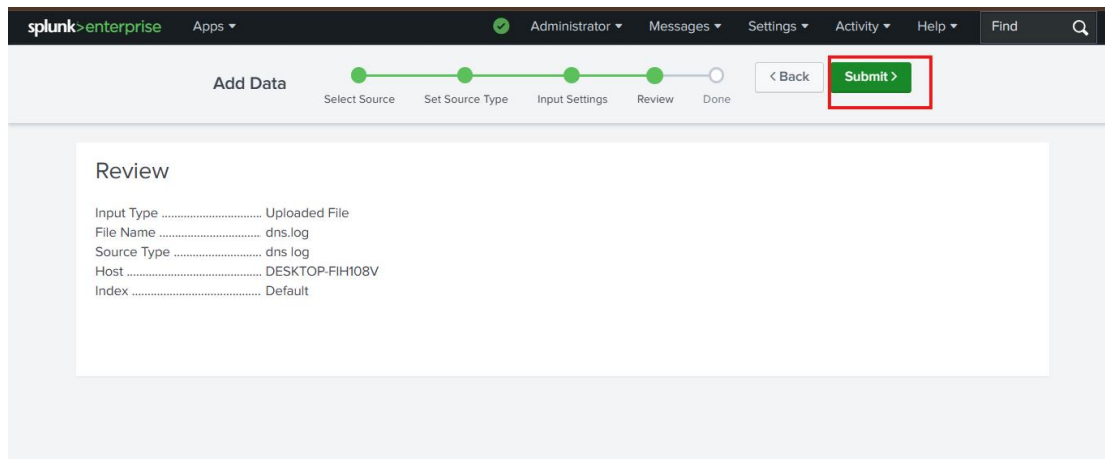
Host field value

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

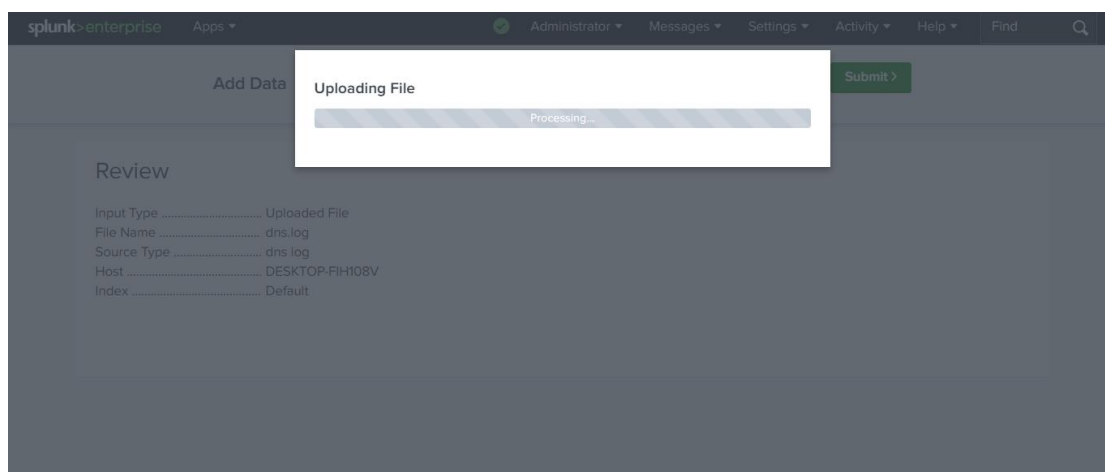
Index

Step 5:

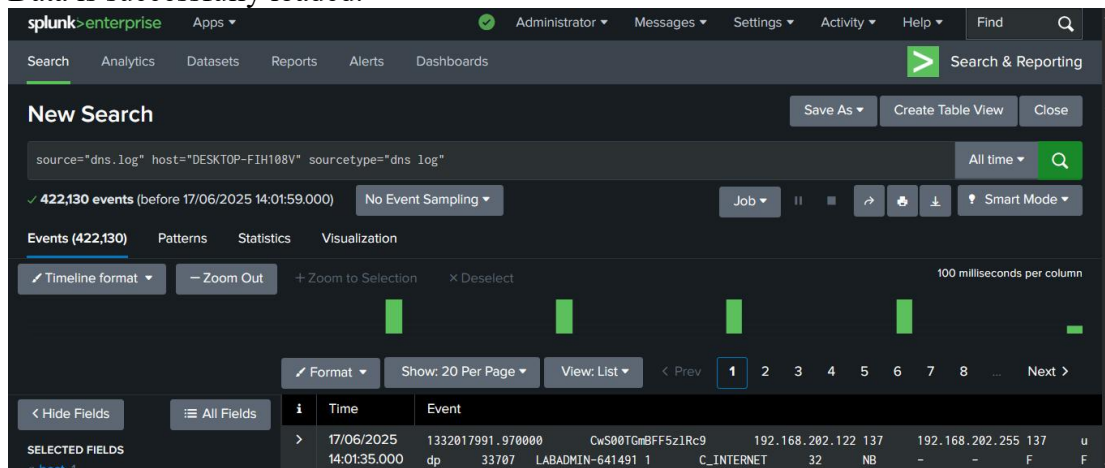
Made by Moez Javed



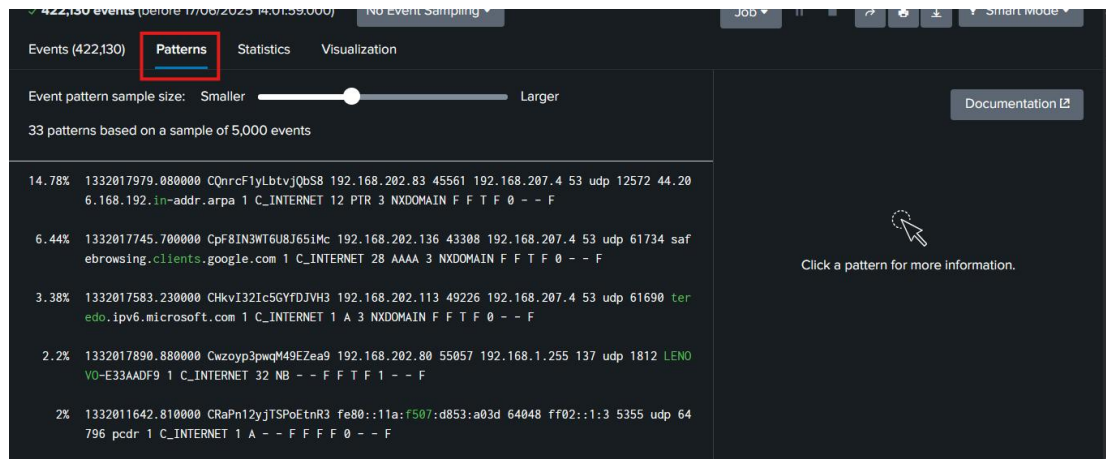
Step 6:



Step 7:
Data is successfully loaded.



Step 8:



Step 9:

```
source="dns.log"
```

This filters logs where the source file is dns.log.

source refers to the file from which the data was ingested.

```
host="DESKTOP-FIH108V"
```

This limits results to logs coming from the host (machine) with the name DESKTOP-FIH108V.

```
sourcetype="dns log"
```

Restricts the search to events tagged with sourcetype dns log, indicating the format or source type of the data.

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

This is a pipe (|) which means take the filtered logs and then apply the next operation.

regex applies a regular expression to filter further.

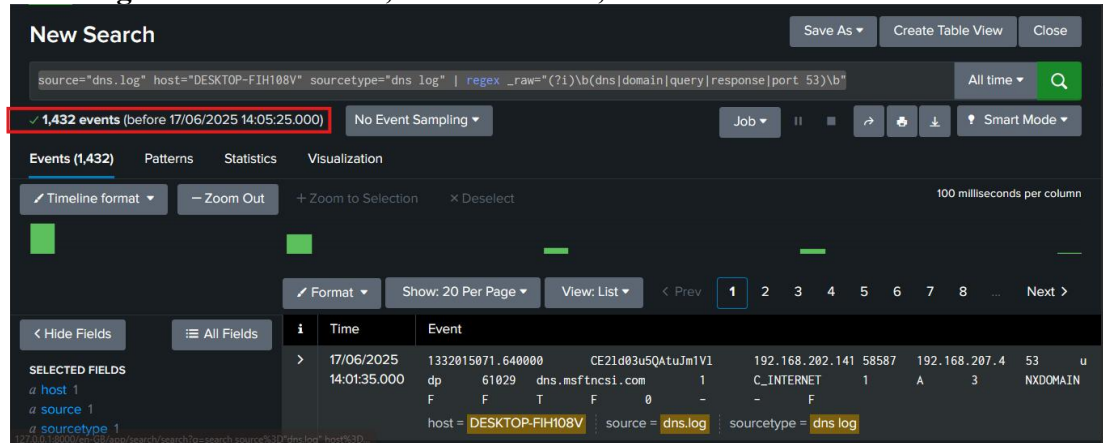
_raw means the raw log data is being searched.

(?!i) makes the search case-insensitive.

\b(dns|domain|query|response|port 53)\b matches whole words such as dns, domain, query, response, or port 53.

```
source="dns.log" host="DESKTOP-FIH108V" sourcetype="dns log" | regex _raw="(?!i)b(dns|domain|query|response|port 53)b"
```

When I give this commands, it shows that 1,432 events.



Lab Tasks and Student Practice

Follow the instructions and complete each task. Document your progress with screenshots and notes.

Task 1: Install and Configure Splunk

1. Download the Splunk installer from <https://www.splunk.com>.
 2. Launch the installer and accept all default installation settings.
 3. Create your admin credentials. Note them for future login.
 4. Open Splunk via your browser (typically at <http://localhost:8000>).
 5. Log in using your created credentials.
 6. After successful login, you will be taken to the Splunk dashboard.
- Take a screenshot of your dashboard with the menu and search bar visible.

Task 2: Upload DNS Log File to Splunk

7. Click on 'Add Data' from the homepage.
 8. Select 'Upload', then choose your local dns.log file.
 9. Set the source type as 'dns log' and give it a recognizable name.
 10. Select or create a new index (e.g., dns_index).
 11. Click 'Review' → 'Submit' → 'Start Searching'.
 12. Confirm that logs are indexed by previewing event samples.
- Take a screenshot of the upload summary page and the first few log entries.

Task 3: Perform Basic Search on DNS Logs

Use the Splunk search bar to perform the following:

```
source="dns.log"
```

Answer: How many events are found? What fields are auto-detected?

Task 4: Host-Based Log Filtering

```
source="dns.log" host="student-pc"
```

Answer: How many events belong to your host?

Task 5: Filter Logs Using sourcetype

```
sourcetype="dns log"
```

Try combining filters:

```
source="dns.log" sourcetype="dns log"
```

Question: What is the result difference between using source, sourcetype, or both?

Task 6: Regex-Based DNS Filtering

```
source="dns.log" host="student-pc" sourcetype="dns log" | regex  
_raw="(?!i)b(dns|domain|query|response|port 53)b"
```

Answer:

- How many results were found using the regex?
 - Provide 3 examples of matched log entries.
- Screenshot required: Include the regex filter results.

Task 7: Visualize Top DNS Queries

```
source="dns.log" | top query
```

Answer:

- What's the top queried domain?
 - How many times was it requested?
- Screenshot required: Your graph output.

Task 8: Generate a Time-Based Chart

```
source="dns.log" | timechart count by host
```

Answer: At what time was peak activity observed?

Screenshot required: Your timechart.

Task 9: Bonus Challenge – Investigate Suspicious DNS Activity

Search for long domain names (common in tunneling):

```
source="dns.log" | eval length=len(query) | where length > 50 | table _time,  
query, length
```

Look for subdomains with random characters:

```
source="dns.log" | regex query=".*[a-z0-9]{10,}.*"
```

Export results to a CSV and write a 100-word summary.

Answer:

- How many suspicious entries found?
 - Which domain or subdomain patterns were suspicious?
- Deliverable: A brief report and exported CSV file.