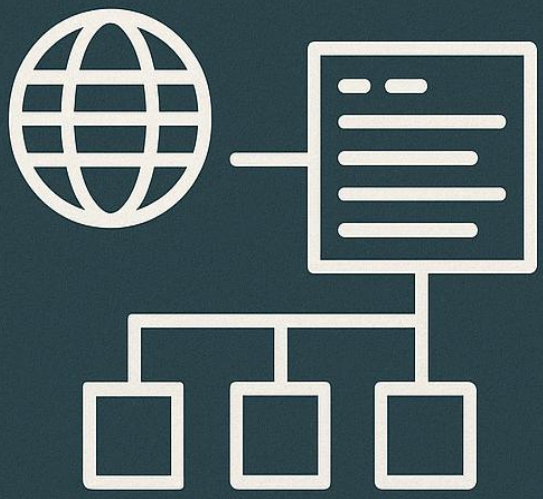
Splunk & DNS Log Analysis



MADE BY

Moeez 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.

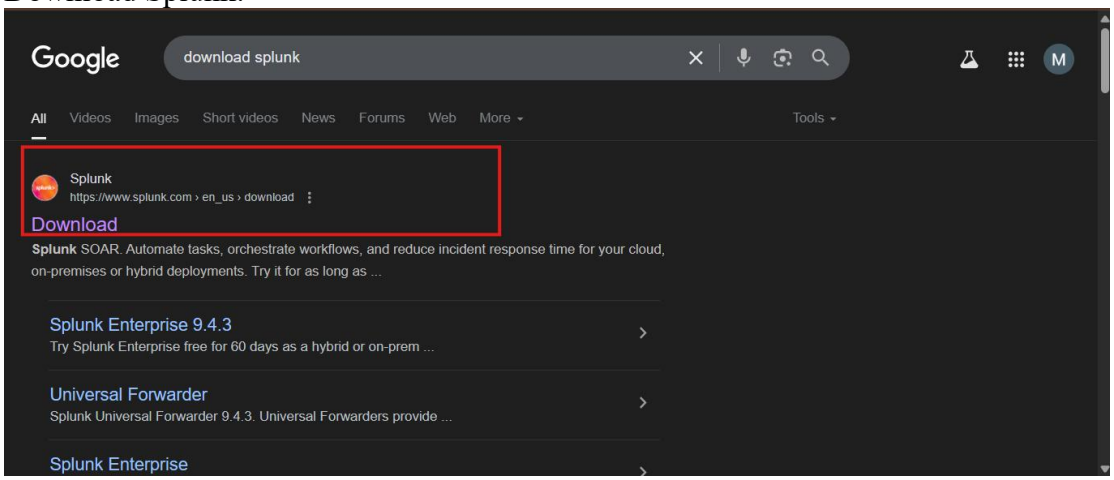
Lab Tasks

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.

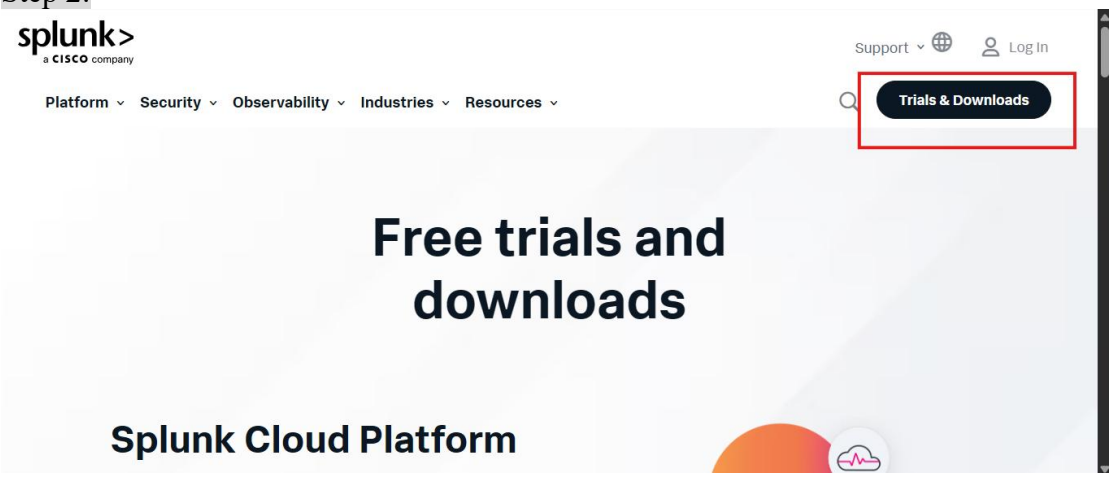
Step-by-Step Guide with Description

Step 1:

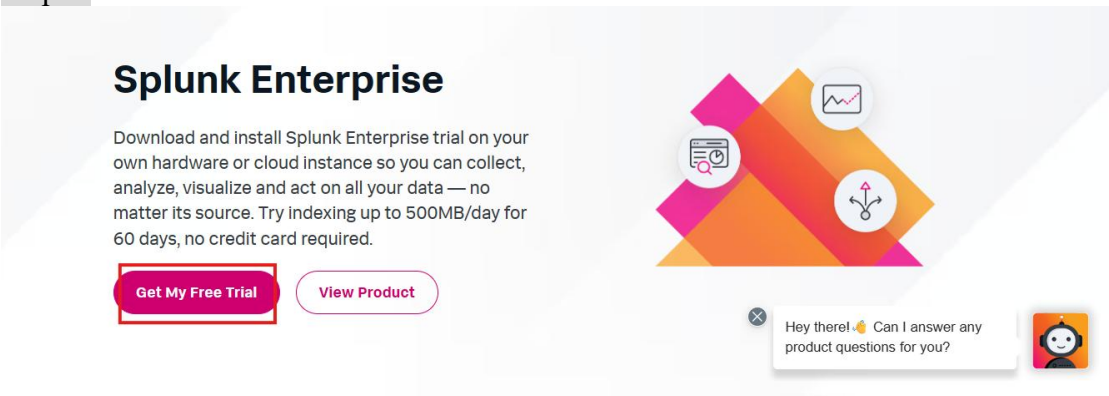
Download Splunk:



Step 2:

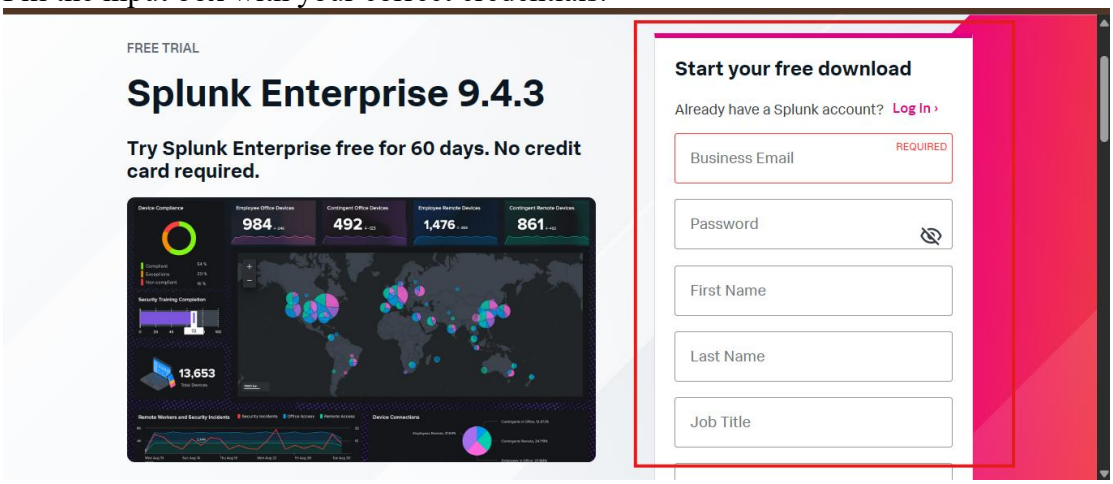


Step 3:

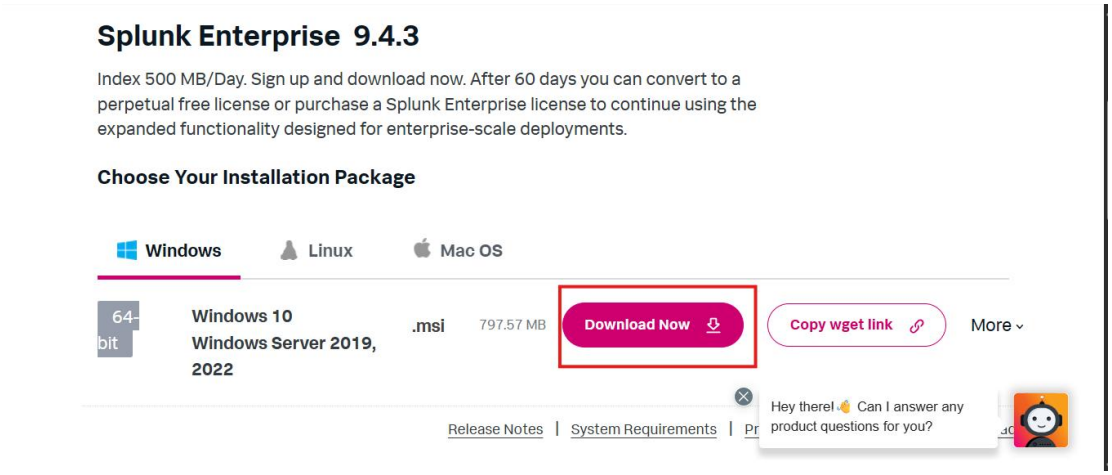


Step 4:

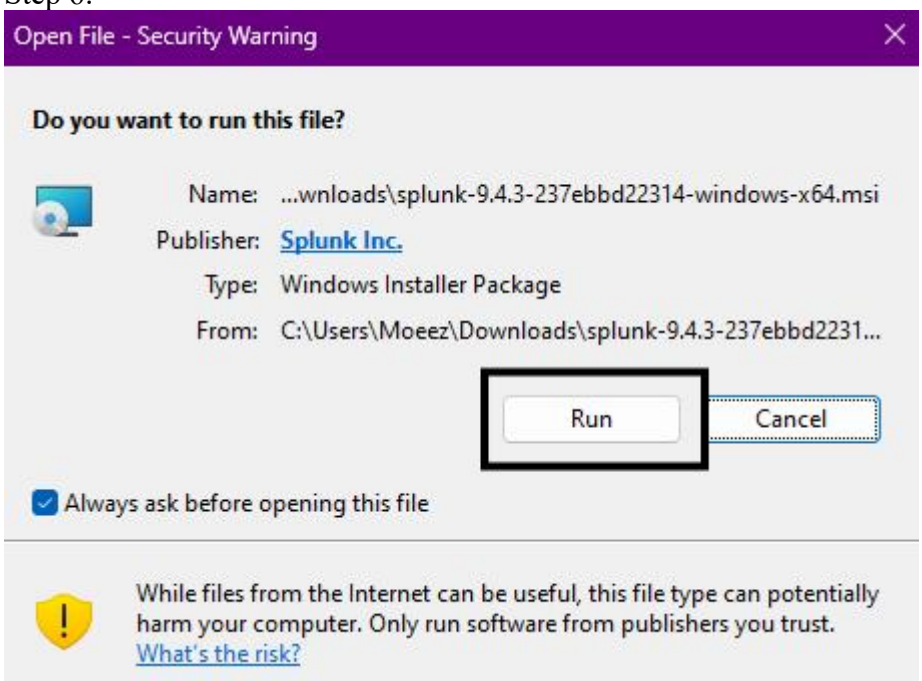
Fill the input box with your correct credentials.



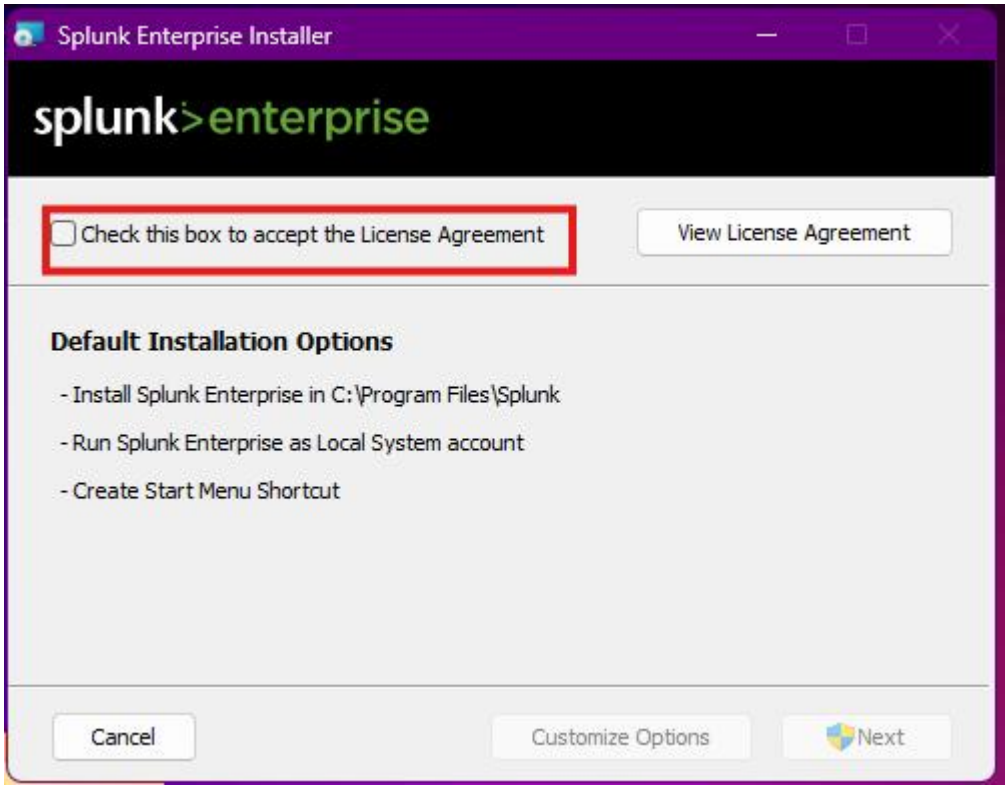
Step 5:


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

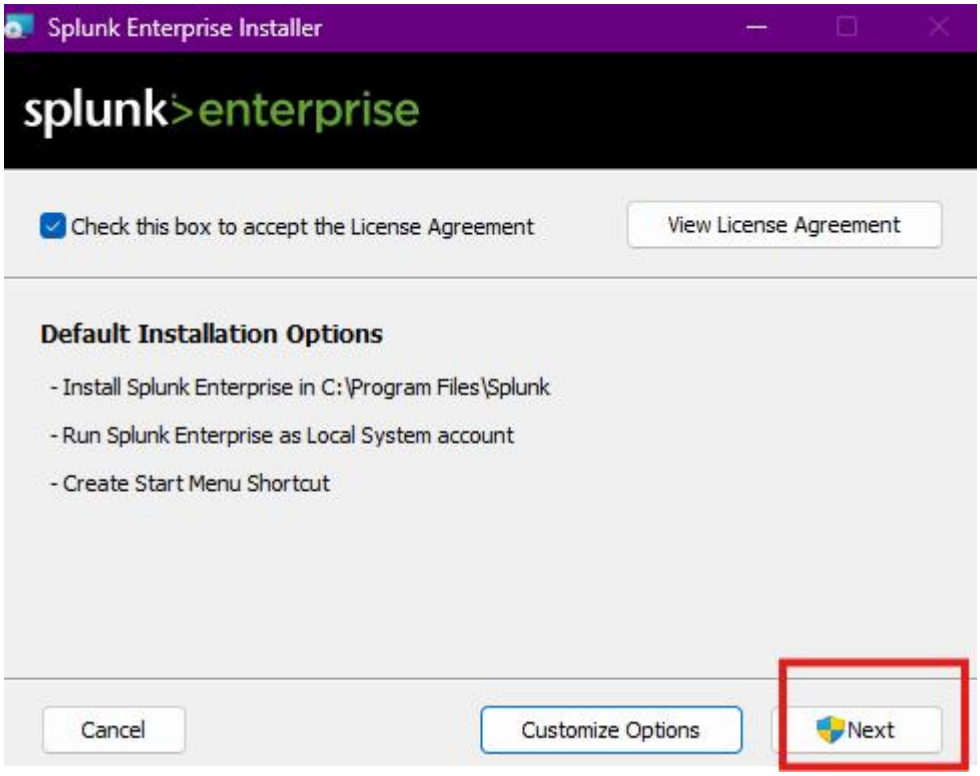
Step 6:


Open File - Security Warning
Do you want to run this file?
Name: ...wnloads\splunk-9.4.3-237ebbd22314-windows-x64.msi
Publisher: Splunk Inc.
Type: Windows Installer Package
From: C:\Users\Moeez\Downloads\splunk-9.4.3-237ebbd2231...
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.
What's the risk?

Step 7:

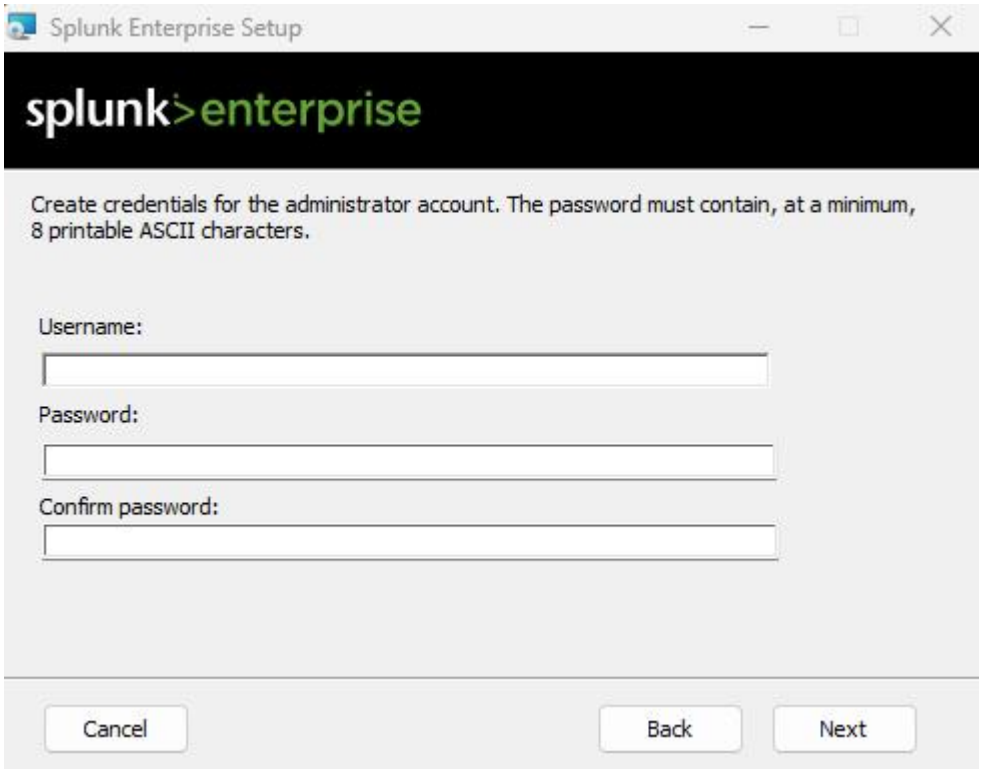


Step 8:

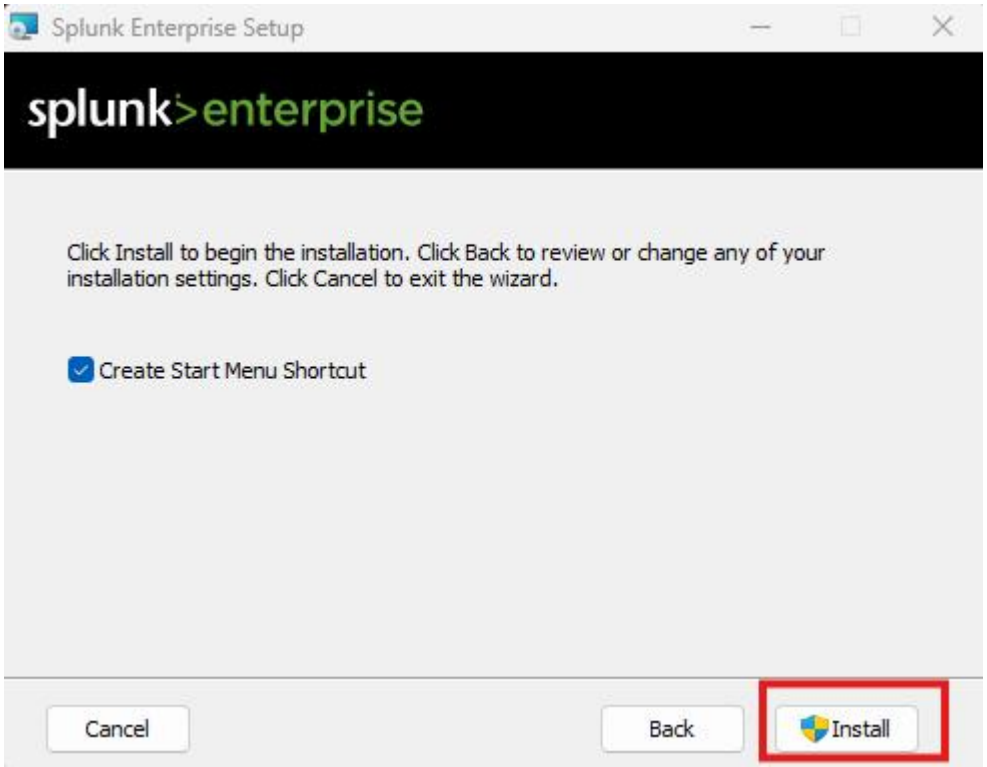


Step 9:

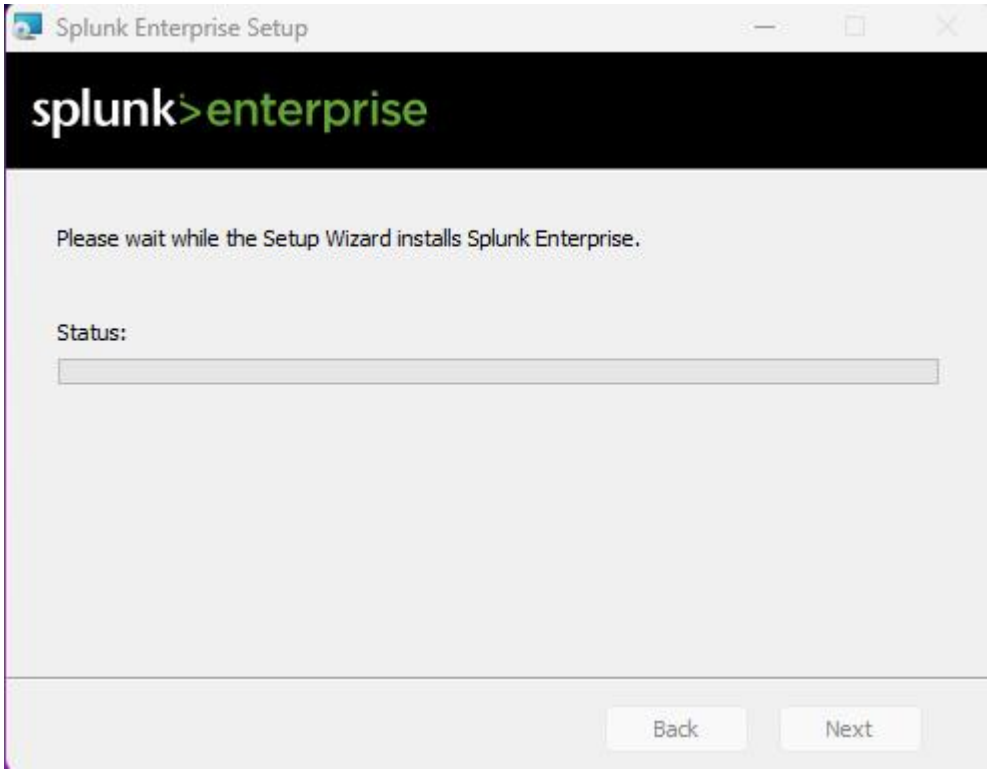
Your name and make password and remember your credentials for login further



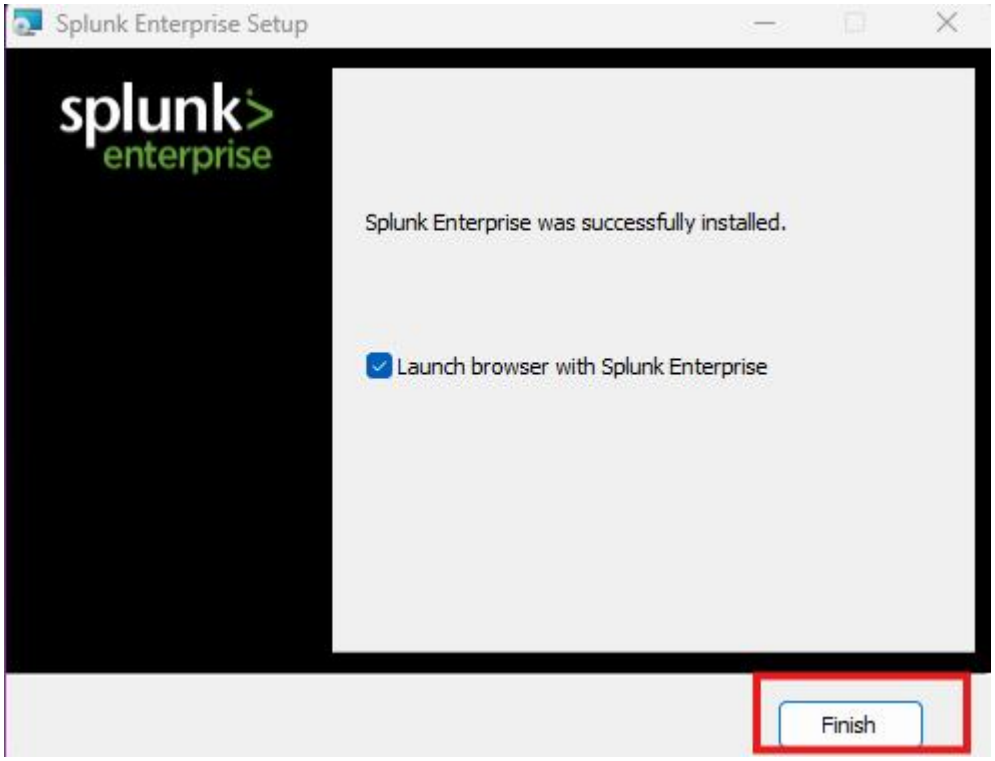
Step 10:



Step 11:

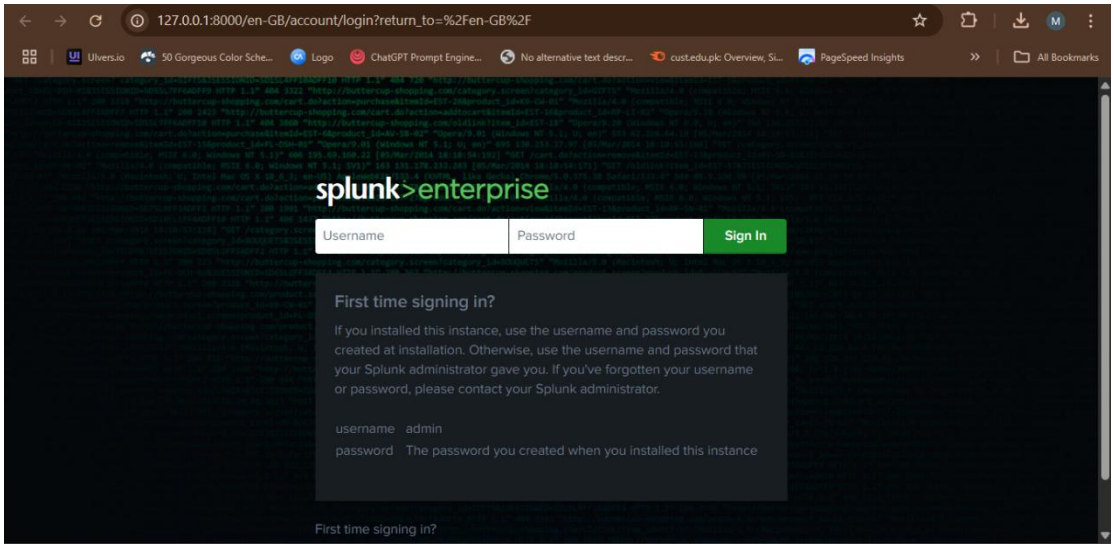


Step 12:

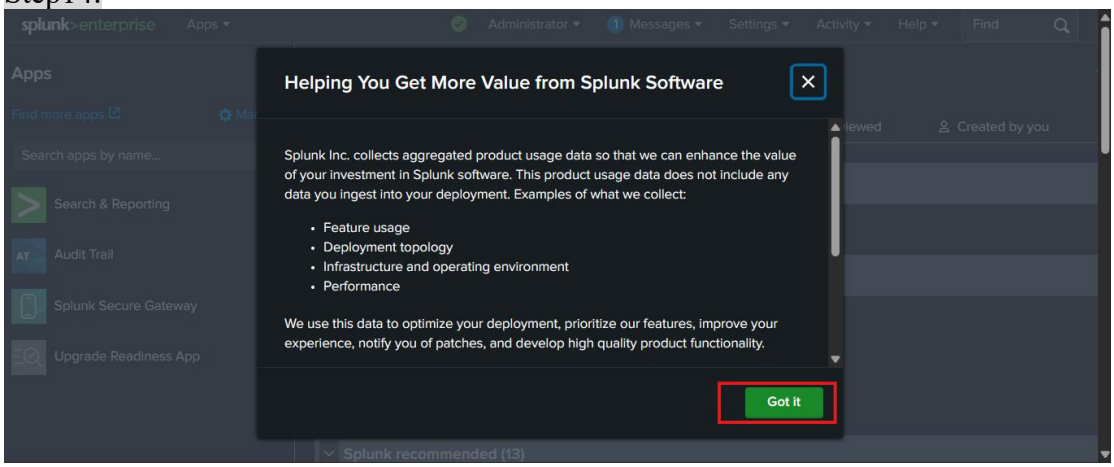


Step 13:
When you will click finish button than this will displayed.

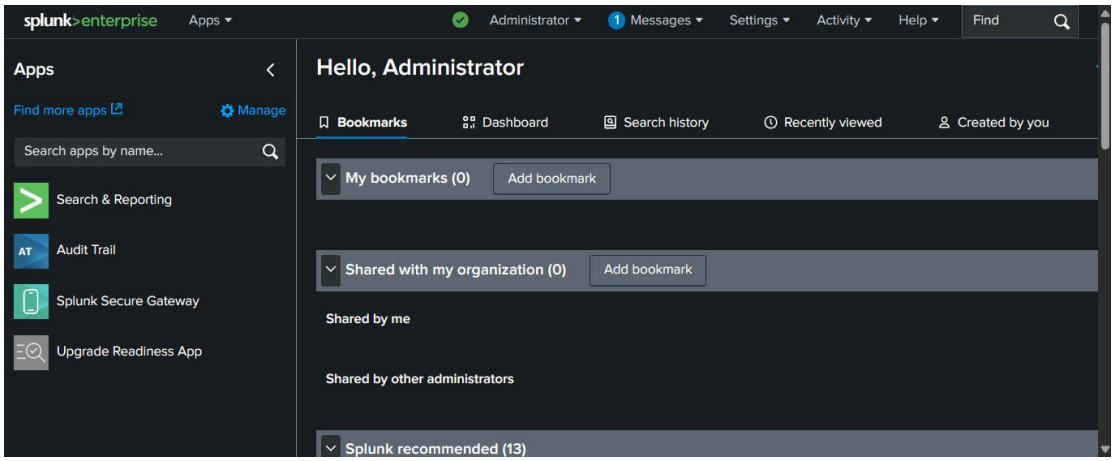
Made by Moeez Javed



Step14:

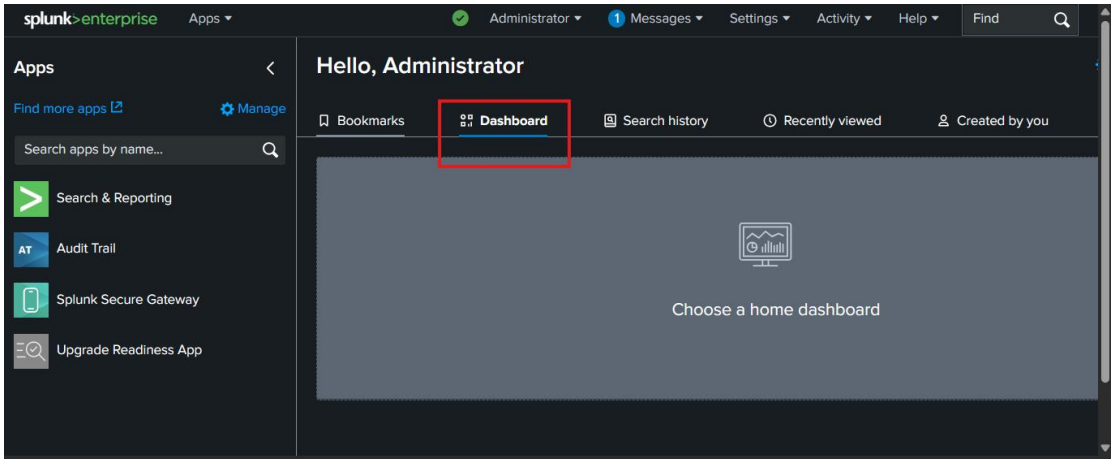


Step15:



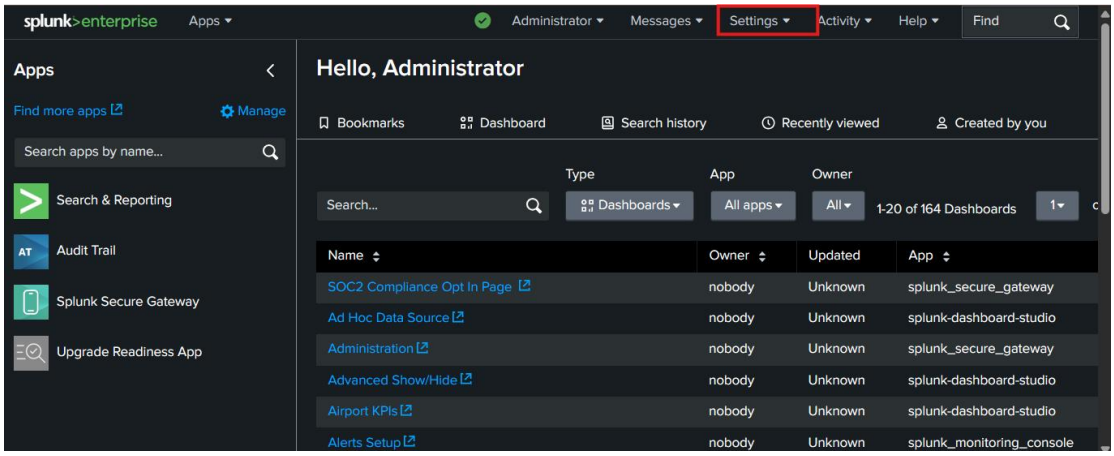
Step 16:

Made by Moeez Javed

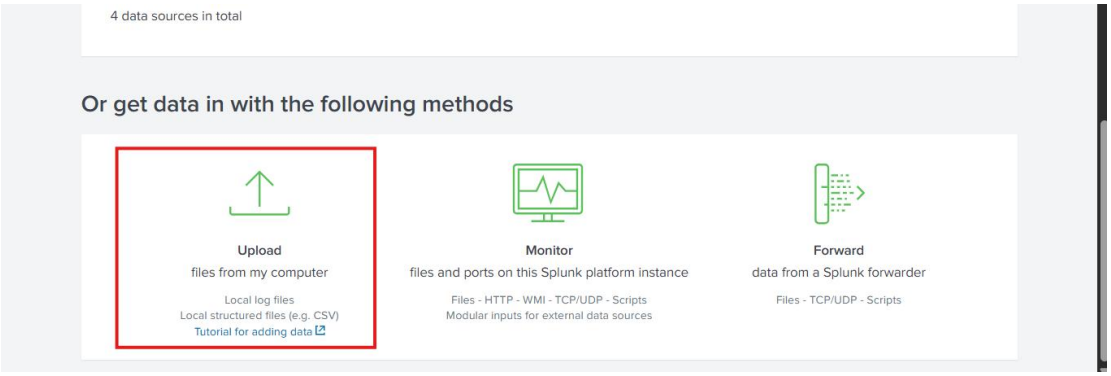


Part 2: Upload Log Files

Step 1:

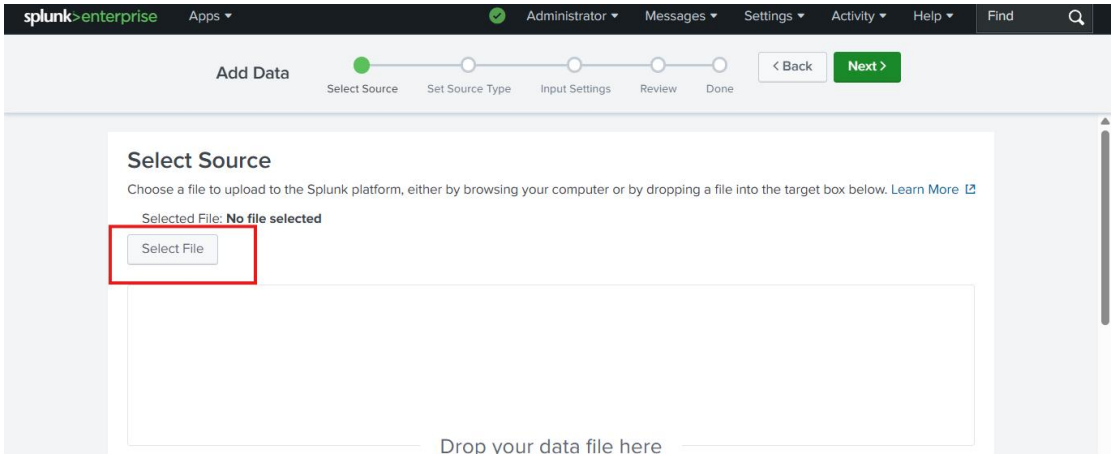


Step 2:

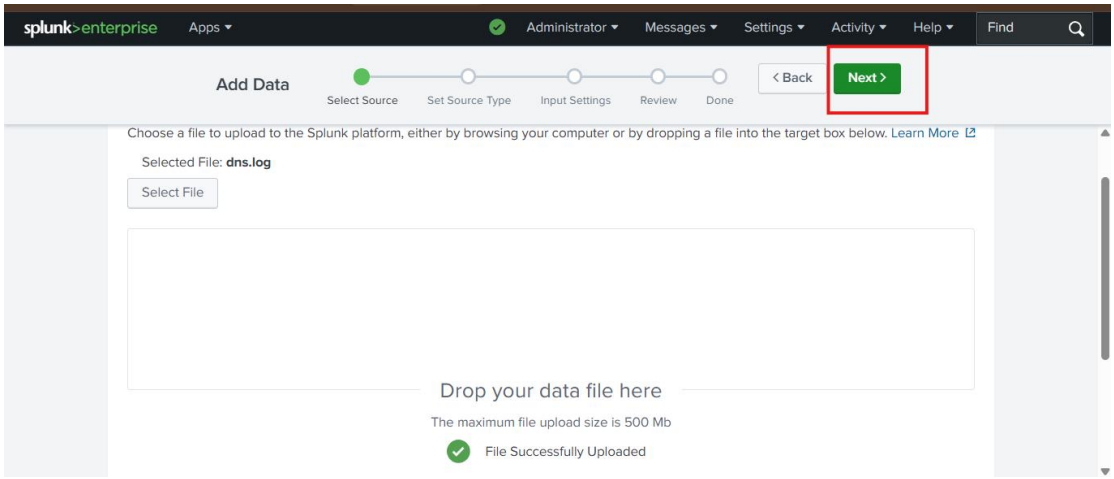


Step 3:

Made by Moeez Javed

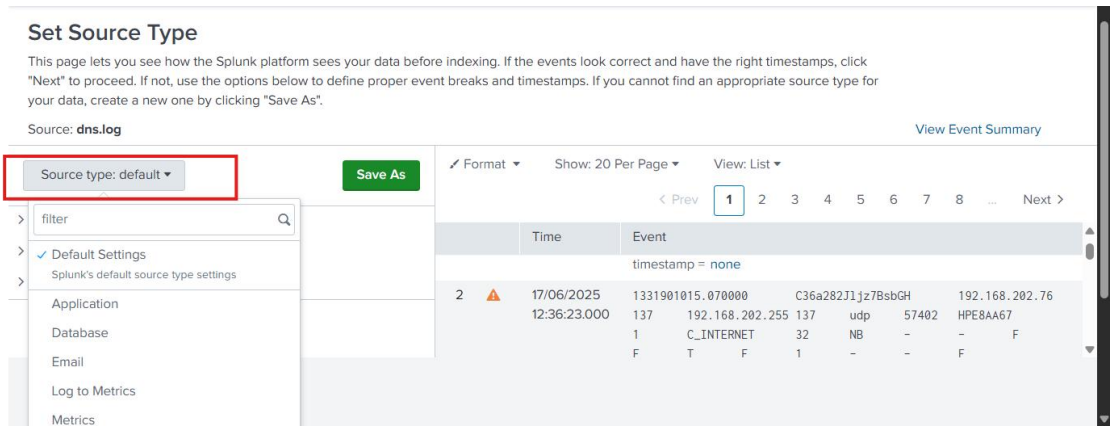


Step 4:

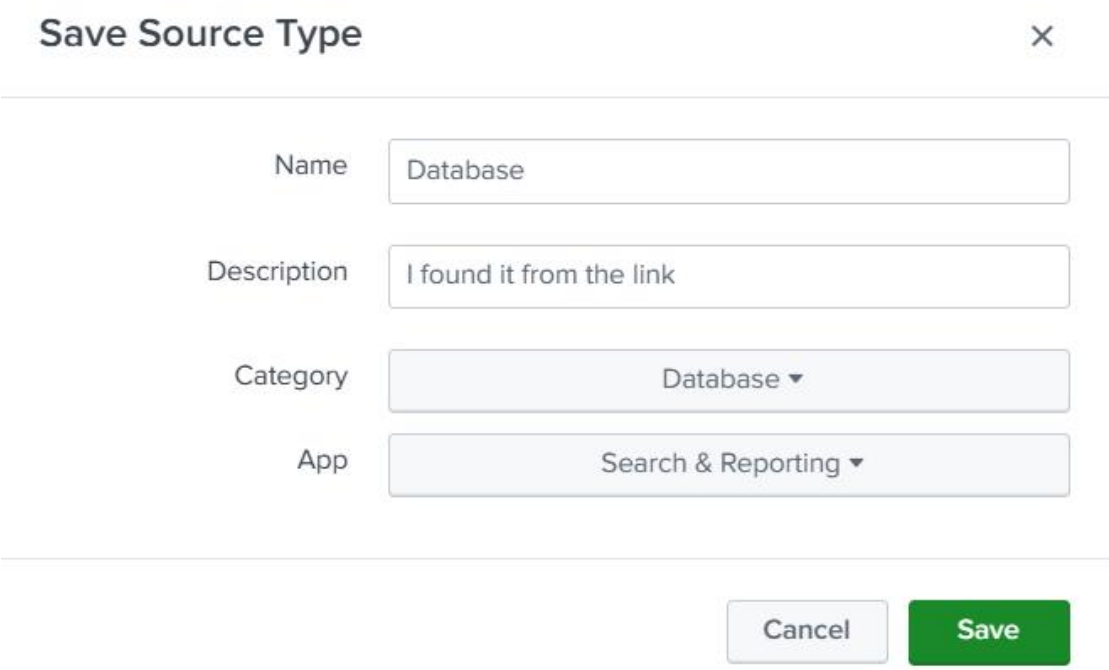


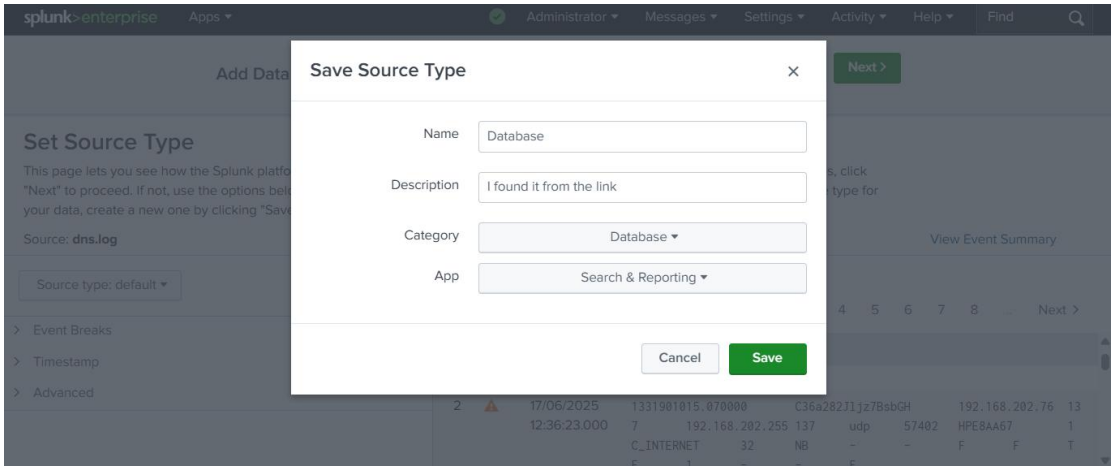
Step 5:

Select the source file and save it.

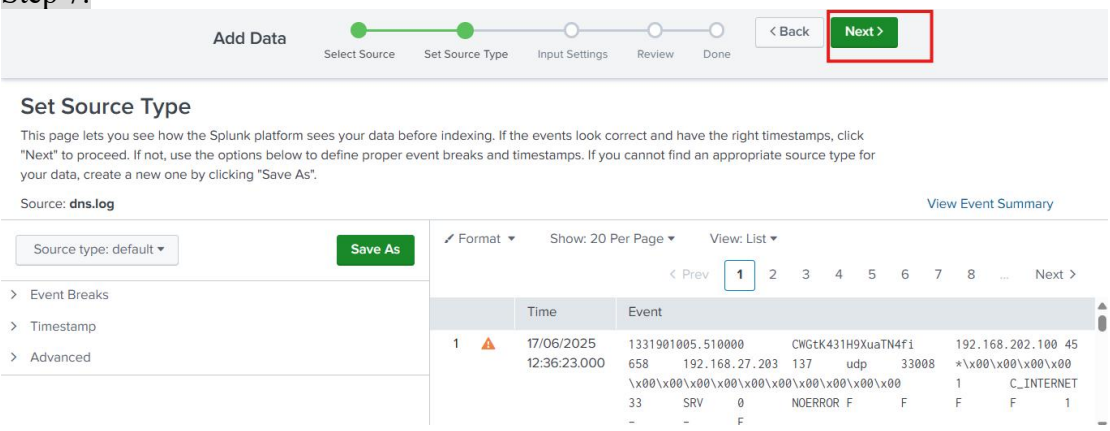


Step 6:


Save Source Type
Name
Database
Description
I found it from the link
Category
Database
App
Search & Reporting
Cancel
Save

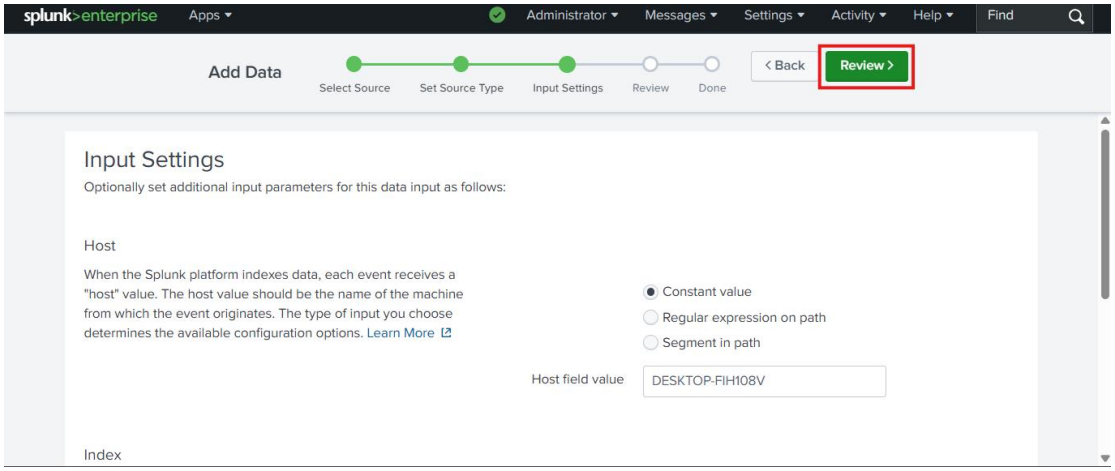

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Next
Save Source Type
Name
Database
Description
I found it from the link
Category
Database
App
Search & Reporting
Cancel
Save
Set Source Type
Source: dns.log
View Event Summary
Source type: default
Event Breaks
Timestamp
Advanced

Step 7:

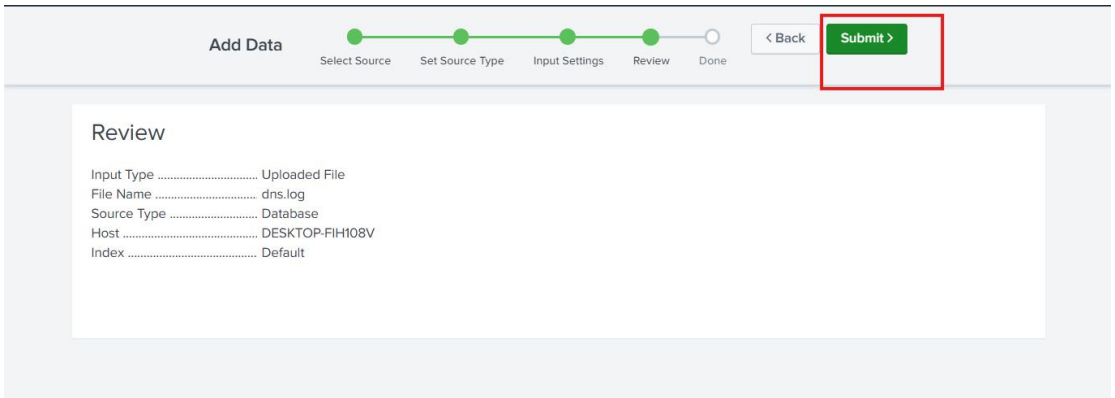

Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper 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
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
Event Breaks
Timestamp
Advanced
Time
Event
17/06/2025
12:36:23.000

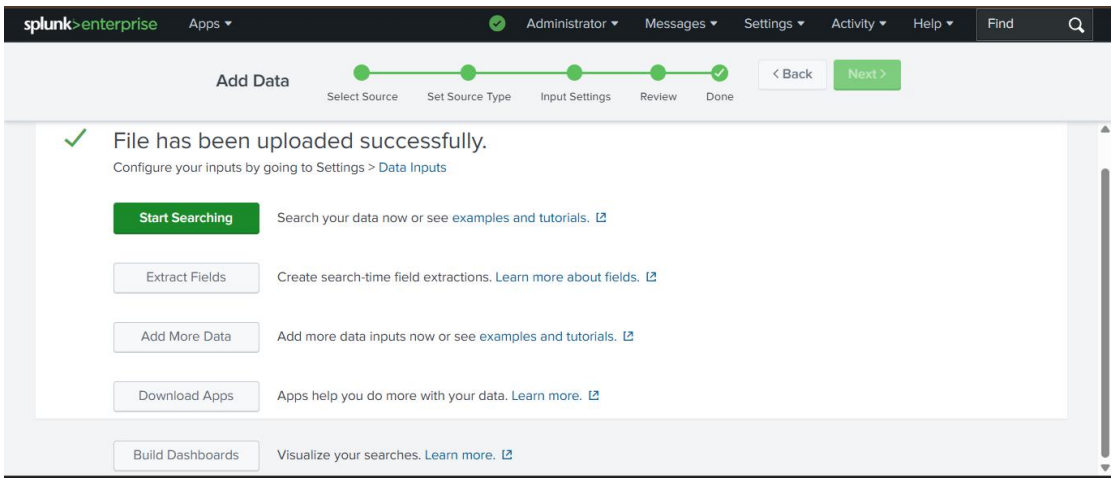
Step 8:

Made by Moeez Javed



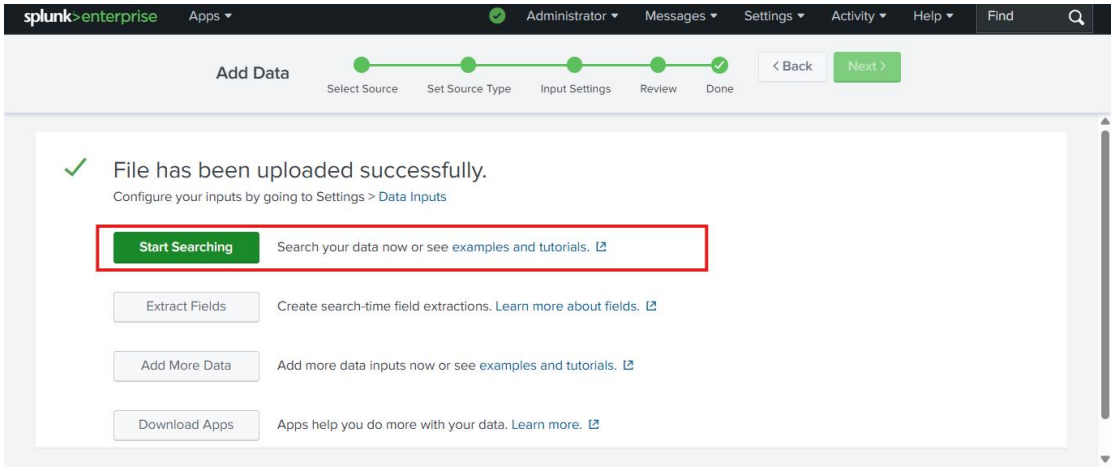
Step :9





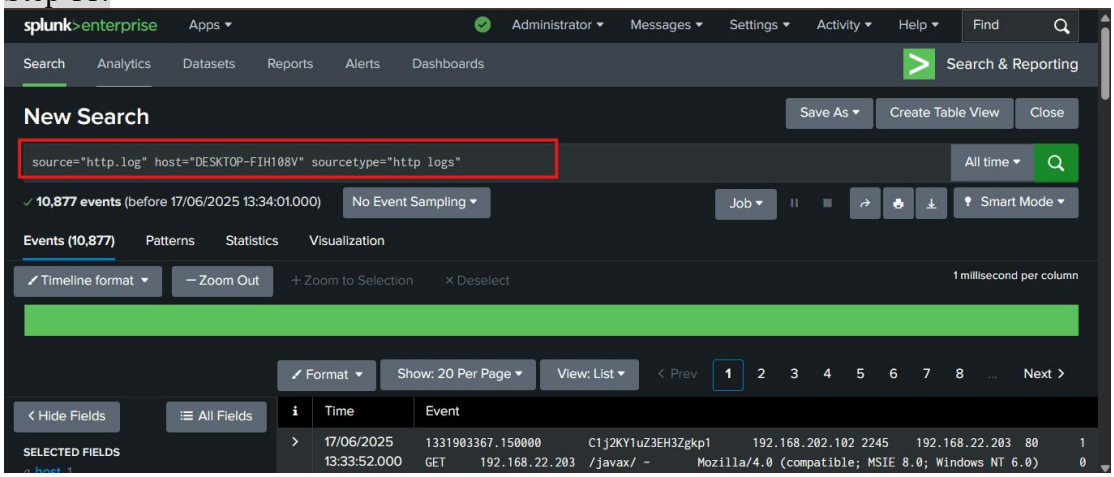
Step 10:

Made by Moeez Javed

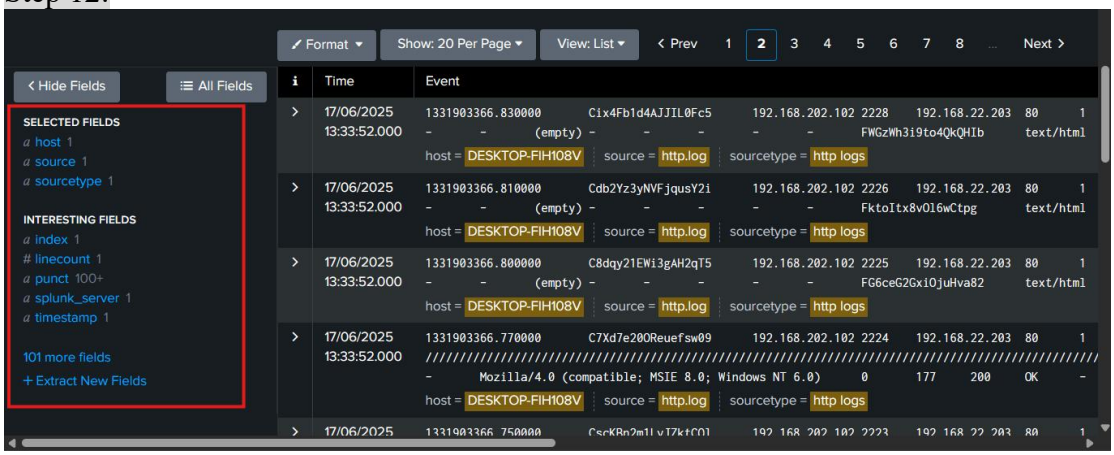


Part 3: Analyzing DNS Logs

Step 11:



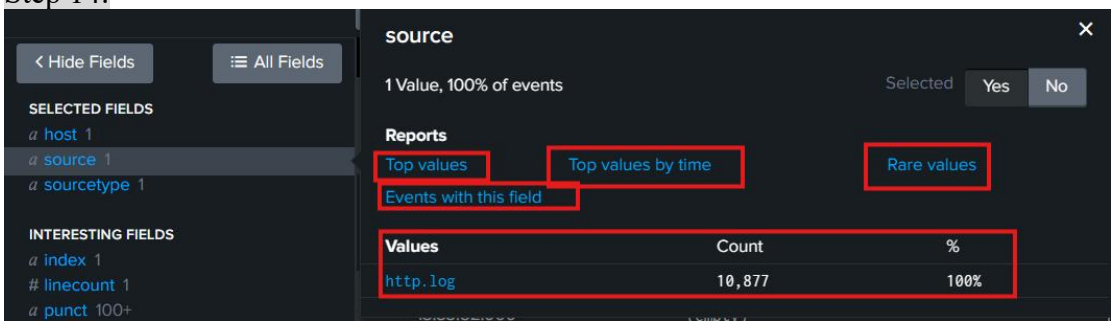
Step 12:



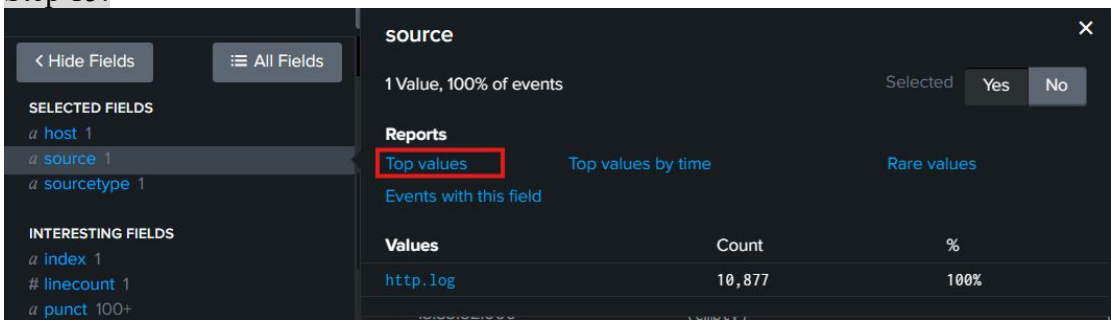
Step 13:

How much total logs and souce of logs.

Step 14:



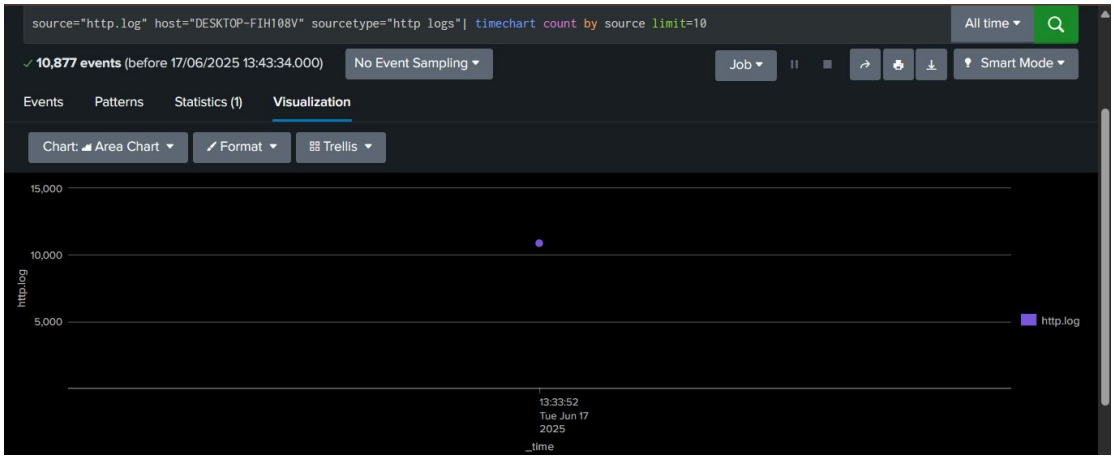
Step 15:



Step 16:

Step 17:

Now Select the Top value by Time:



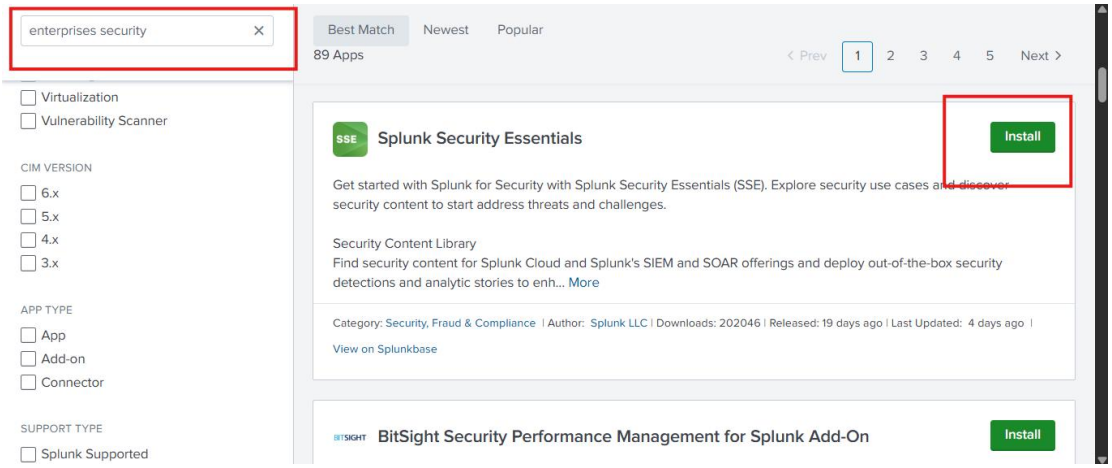
Step 18 :

It show splunk server detials

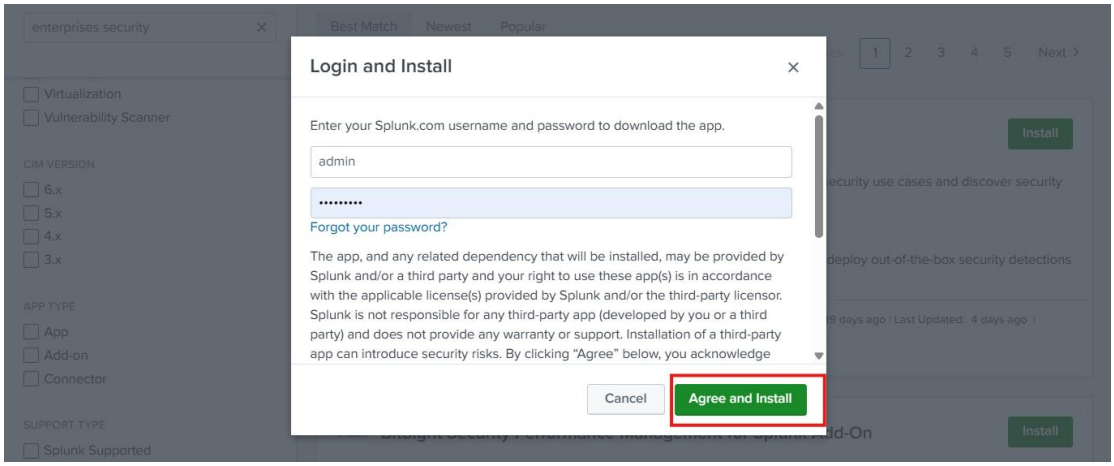
Part 4: Installing Add-ons in Splunk

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

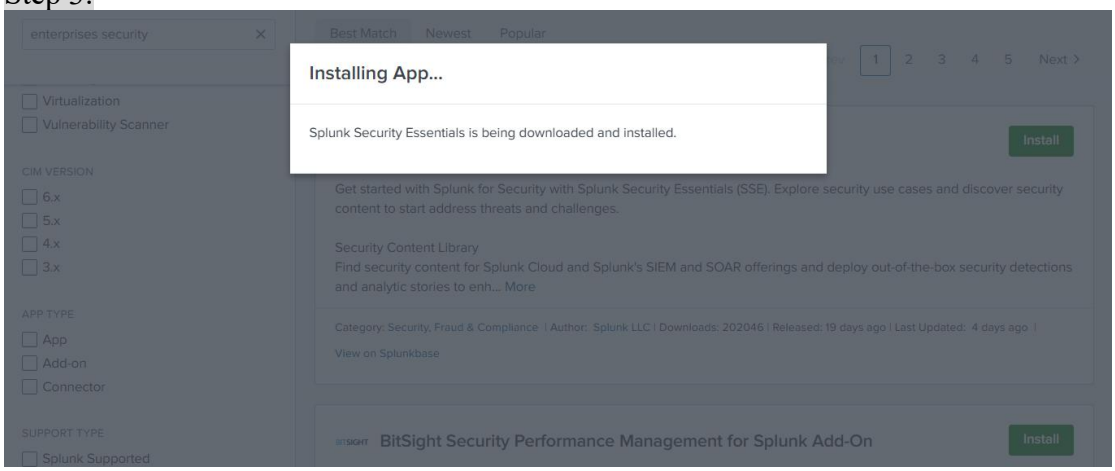
Step 1:



Step 2:



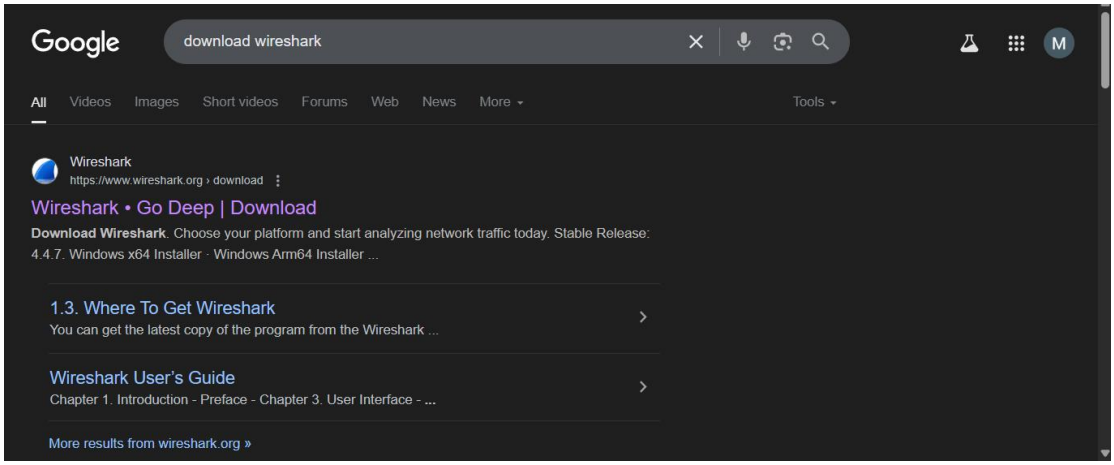
Step 3:



Part 5: Wireshark Log Collection

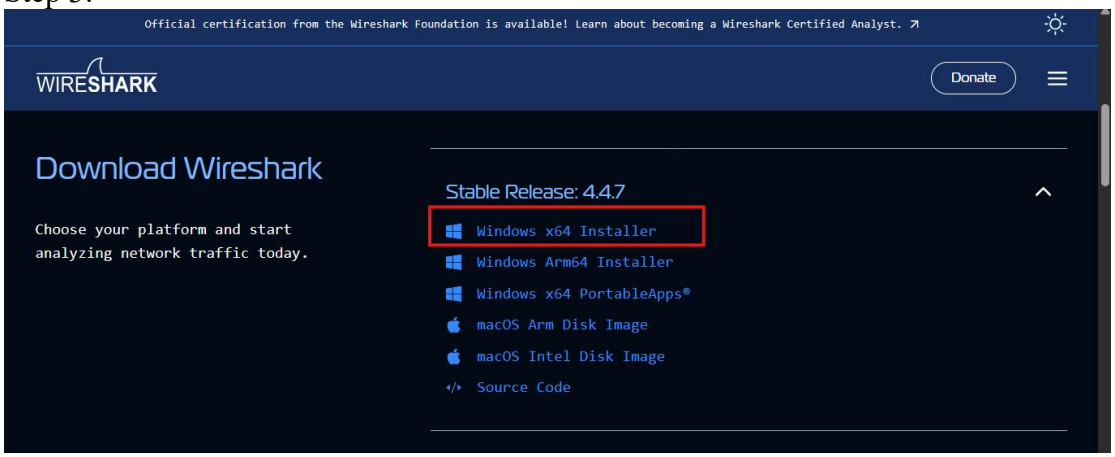
Step 1:

Download Wireshark:

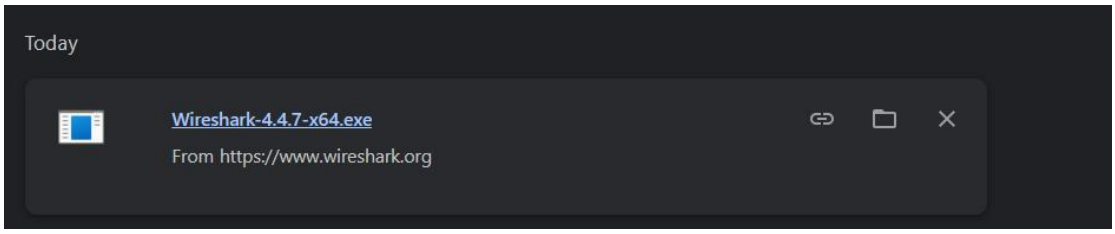


Step 2:

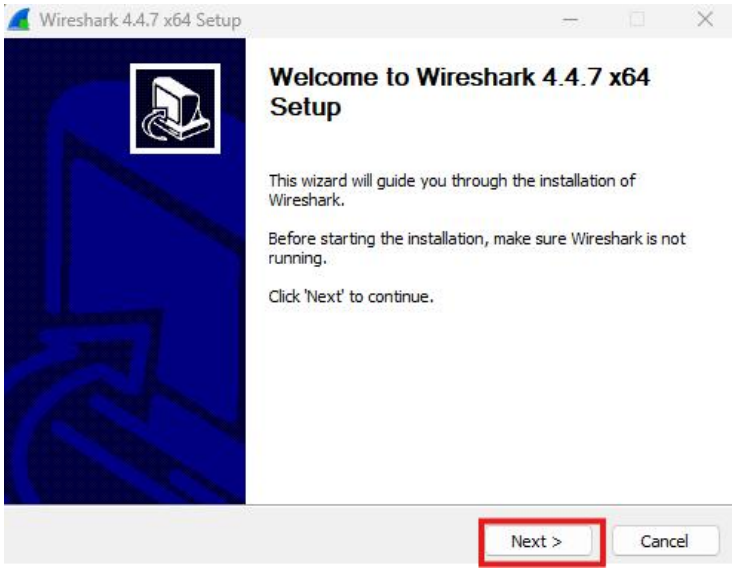
Step 3:



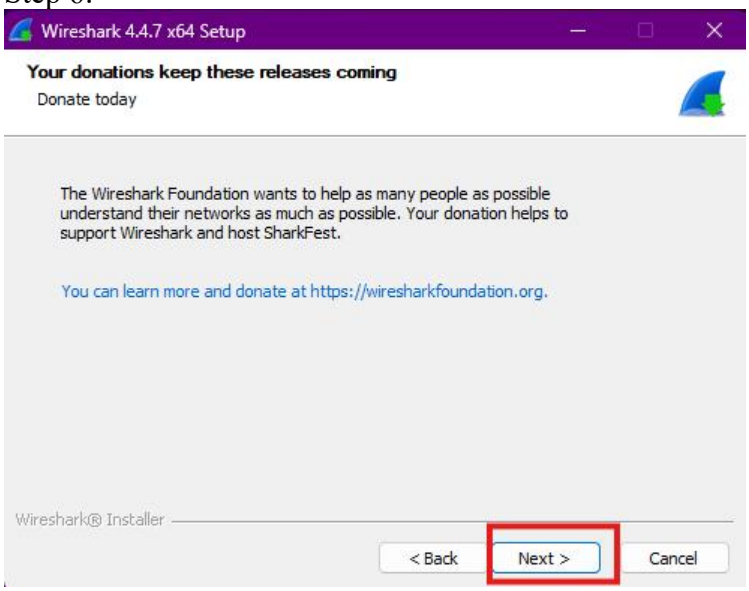
Step 4:



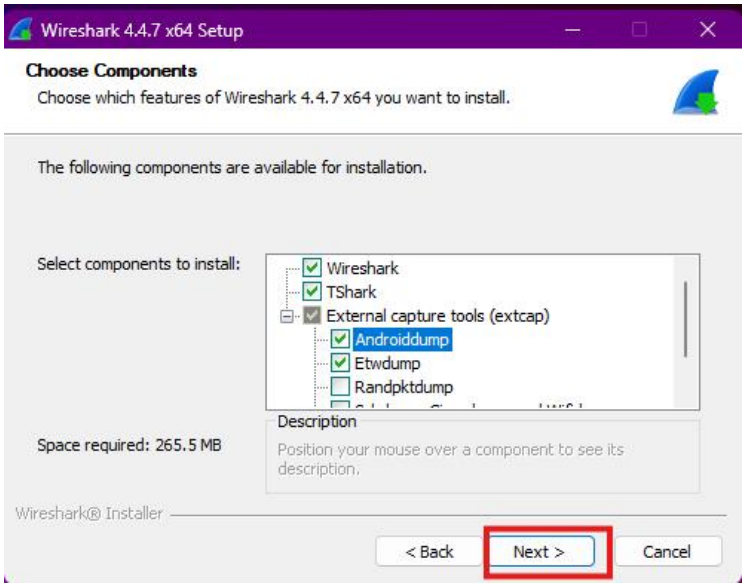
Step 5:


Wireshark 4.4.7 x64 Setup
Welcome to Wireshark 4.4.7 x64 Setup
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click 'Next' to continue.
Next >
Cancel

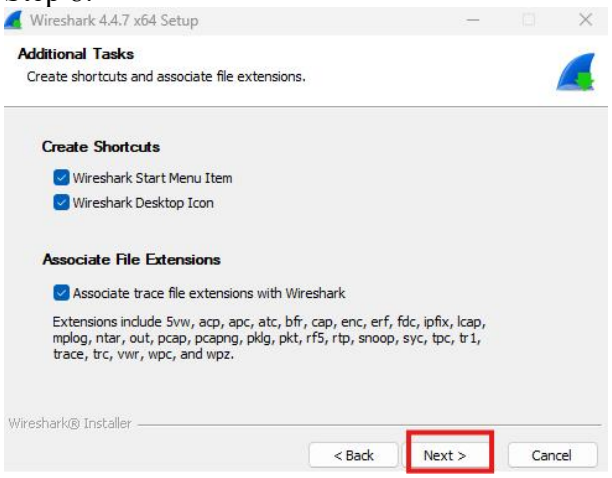
Step 6:


Wireshark 4.4.7 x64 Setup
Your donations keep these releases coming
Donate today
The Wireshark Foundation wants to help as many people as possible understand their networks as much as possible. Your donation helps to support Wireshark and host SharkFest.
You can learn more and donate at https://wiresharkfoundation.org.
Wireshark® Installer
< Back
Next >
Cancel

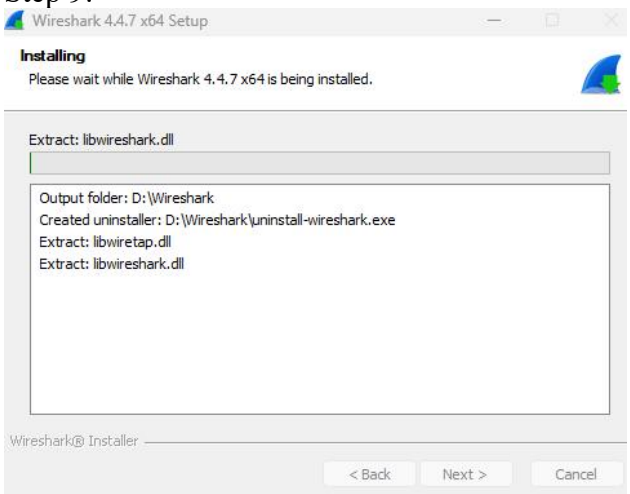
Step 7:



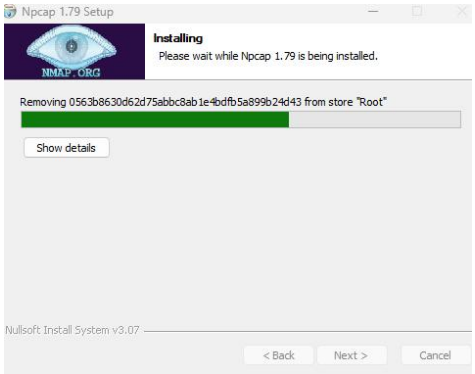
Step 8:



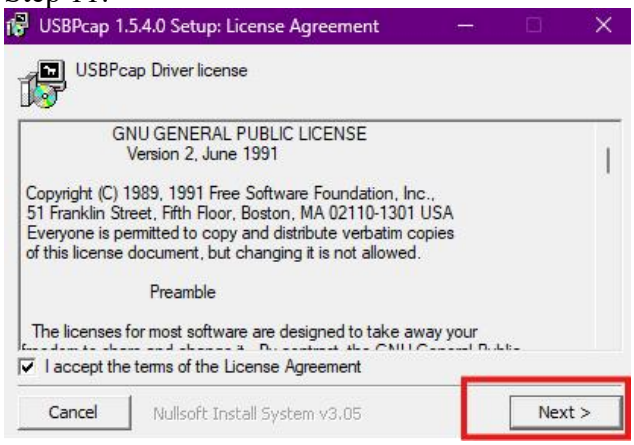
Step 9:



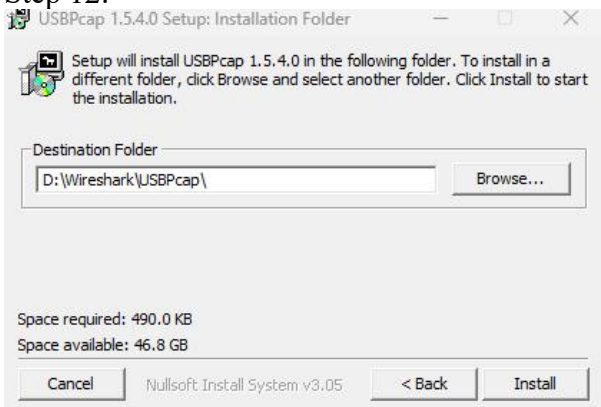
Step 10:



Step 11:



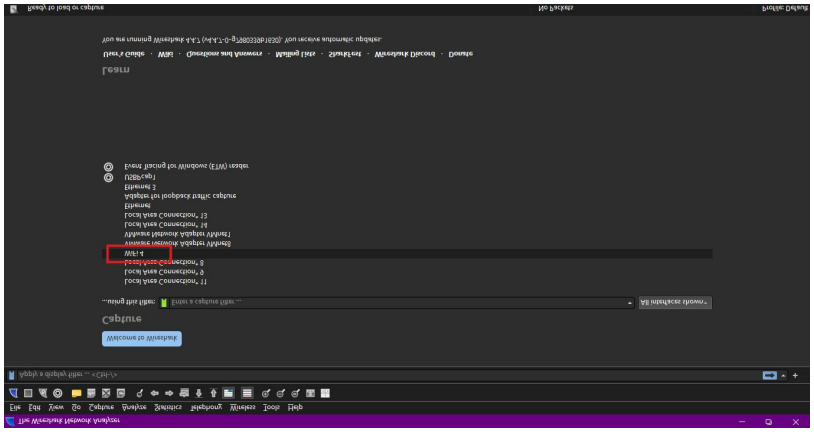
Step 12:

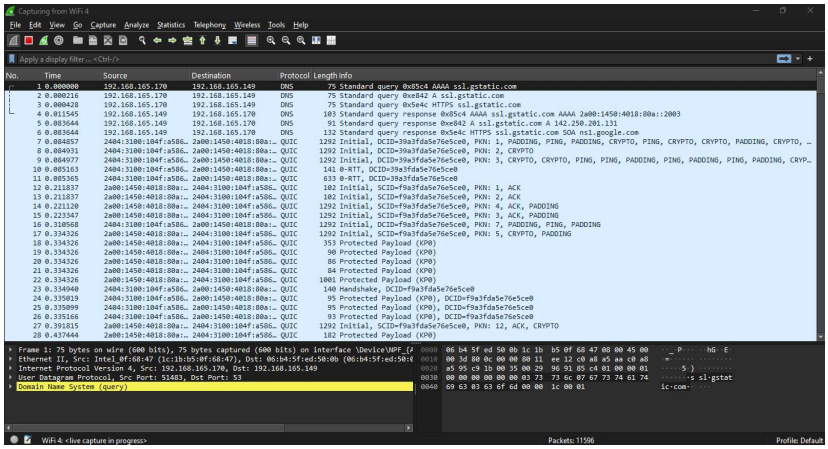


Now installed.

Now opening the Wireshark:

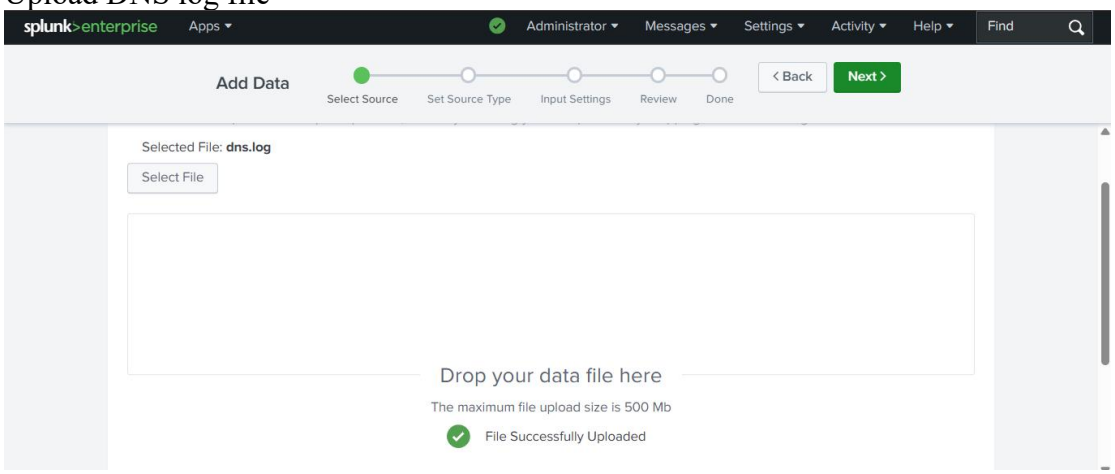
Made by Moeez Javed





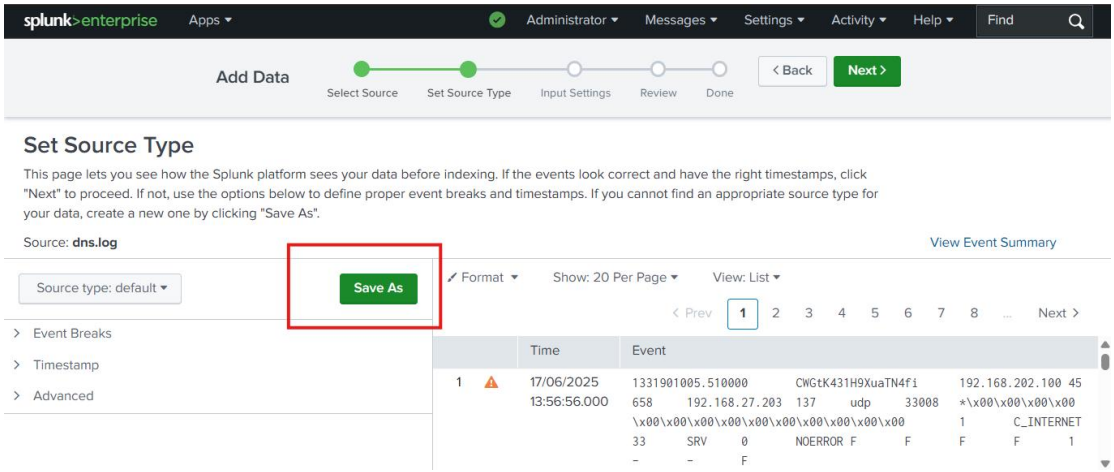
You may download the log and check it in splunk.
DNS Log Analysis:

Step 1:
Upload DNS log file

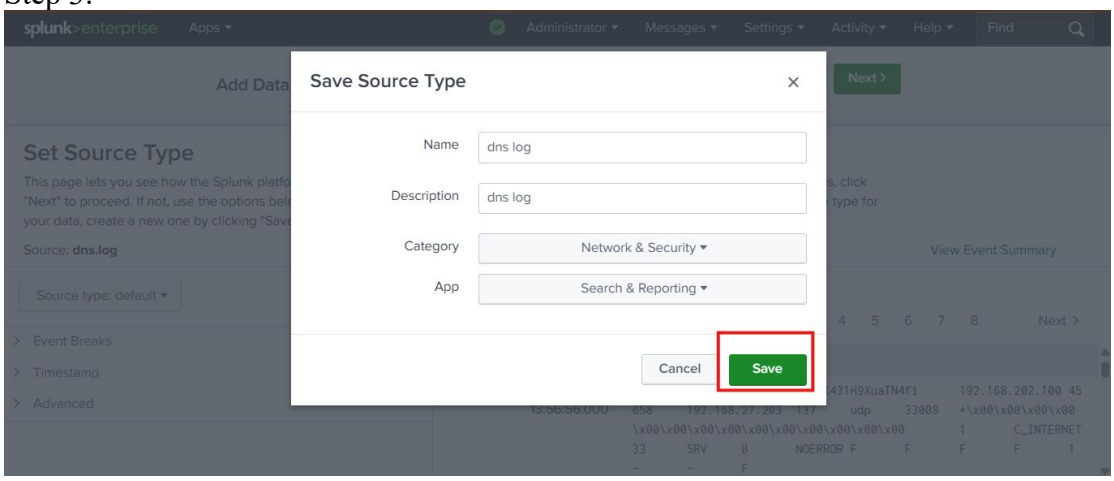


Step 2:

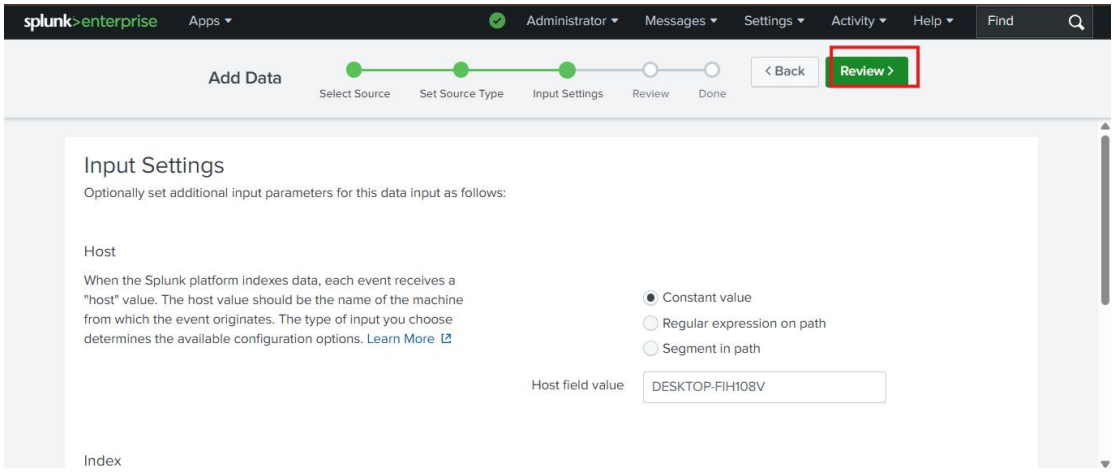
Made by Moeez Javed



Step 3:

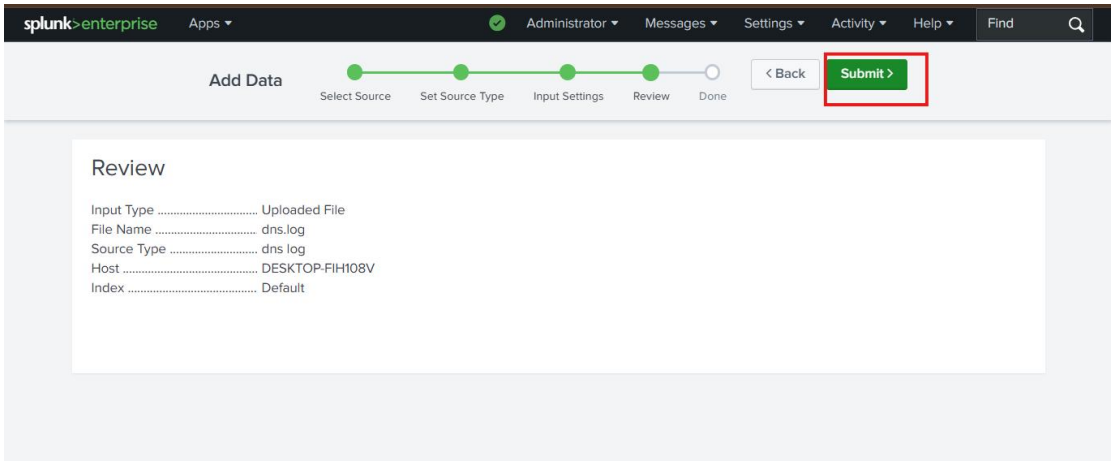


Step 4:

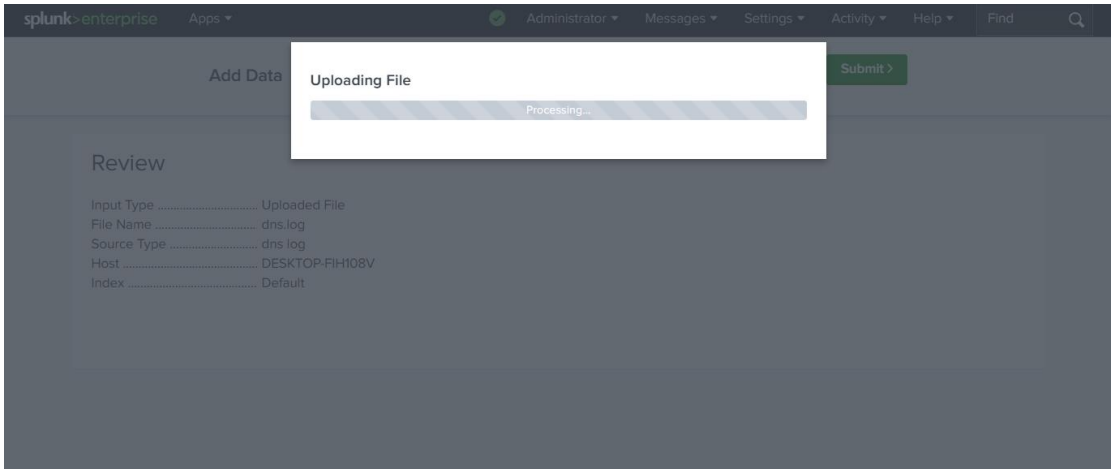


Step 5:

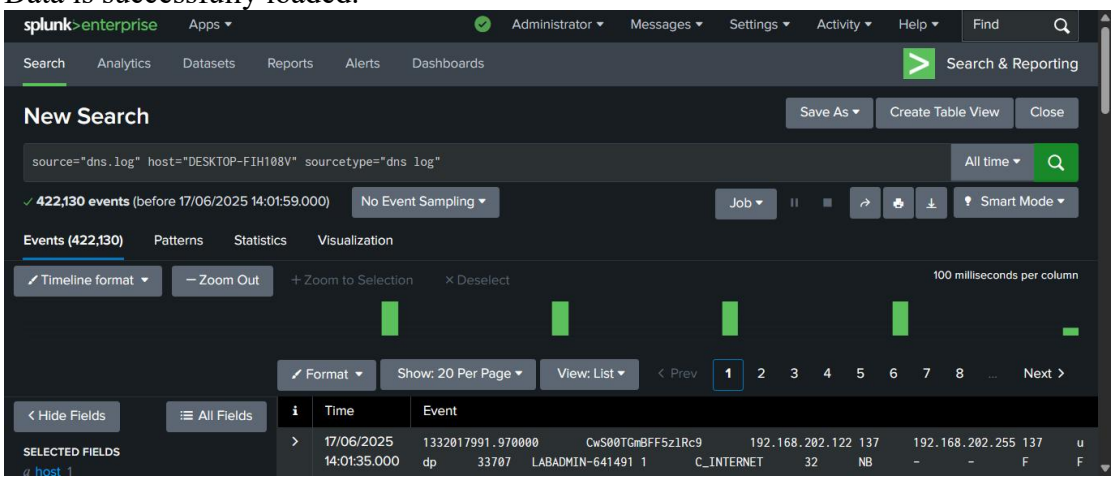
Made by Moeez Javed



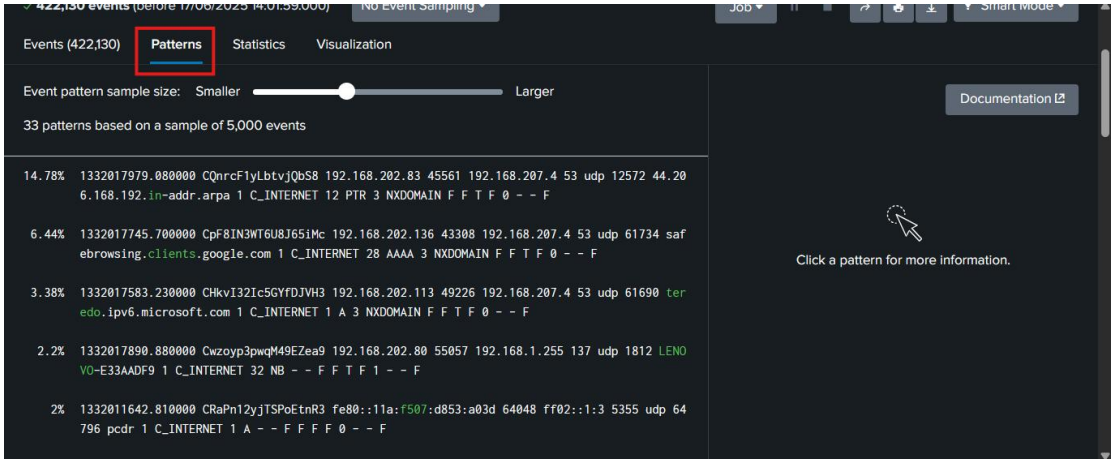
Step 6:



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.

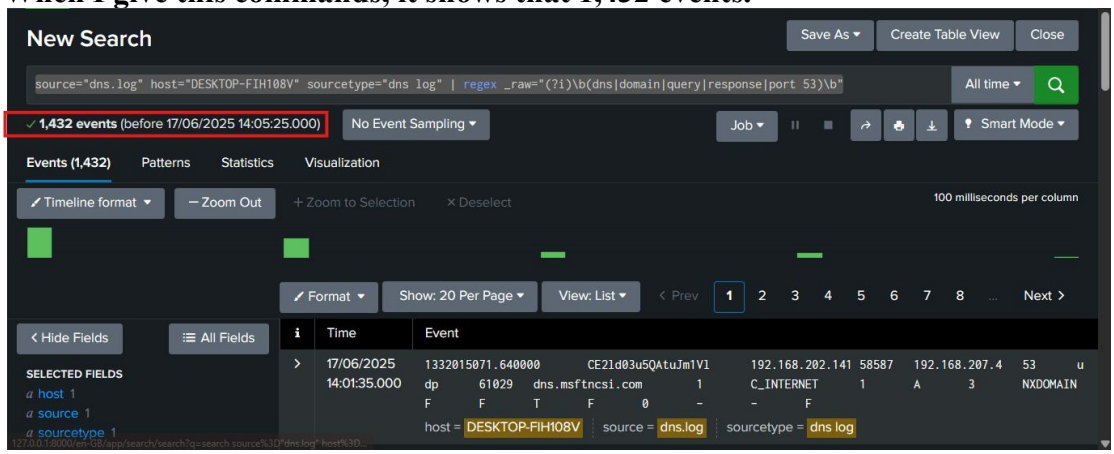
_raw means the raw log data is being searched.

(?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.