Splunk [SIEM] Lab Walkthrough

Lab 1 — Analyzing DNS Log Files Using Splunk

Hassen Hannachi

November 21, 2025

Contents

List of Figures

1 Introduction

Domain Name System (DNS) logs serve as an essential source of information for monitoring network behavior and identifying potential security threats. By leveraging the advanced analytical capabilities of Splunk Security Information and Event Management (SIEM), DNS log data can be systematically examined to detect anomalies, uncover indicators of compromise, and enhance overall situational awareness within the network environment.

2 Project Overview

This project involves ingesting sample DNS (Domain Name System) log files into the Splunk SIEM platform to analyze and interpret network activity. After onboarding the DNS logs using proper data inputs and field extractions, the data is indexed and normalized to enable efficient searching, correlation, and visualization.

Using SPL queries, dashboards, and visual analytics, the project examines critical DNS-related behaviors such as domain lookup patterns, query volume trends, client request activity, and potential indicators of malicious behavior. This includes identifying unusual domain queries, detecting high-frequency lookups, correlating client IPs with suspicious DNS activity, and uncovering signs of phishing, command-and-control (C2) traffic, or DNS tunneling.

The objective of this project is to transform raw DNS logs into actionable insights that support threat hunting, network monitoring, and early detection of security anomalies within the environment.

2.1 Prerequisites

Before analyzing DNS logs in Splunk, ensure the following:

- Splunk instance is installed and configured.
- DNS log data sources are configured to forward logs to Splunk.

3 Lab Walkthrough

3.1 Prepare Sample DNS Log Files

- Splunk instance is installed and configured. DNS log data sources are configured to forward logs to Splunk.
- Obtain sample DNS log file [1] in a suitable format (e.g., text files).
- Ensure the log files contain relevant DNS events, including source IP, destination IP, domain name, query type, response code, etc.
- Save the sample log files in a directory accessible by the Splunk instance.

[1] https://www.secrepo.com/maccdc2012/dns.log.gz/

3.2 Upload Log Files to Splunk

- Log in to the Splunk web interface.
- Navigate to **Settings** > **Add Data**.

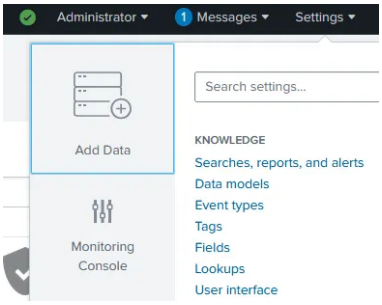

Figure 1: add DNS log data

- Select Upload as the data input method

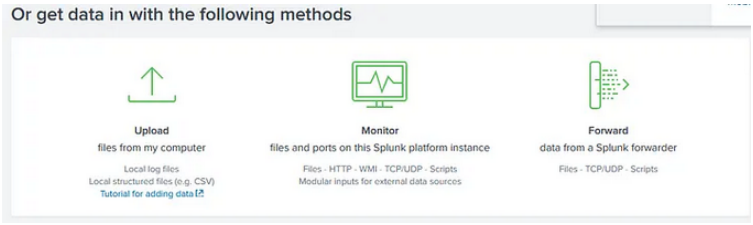

Figure 2: upload DNS log data

3.3 Choose File

- Click on Select File and choose the sample DNS log file you prepared earlier.

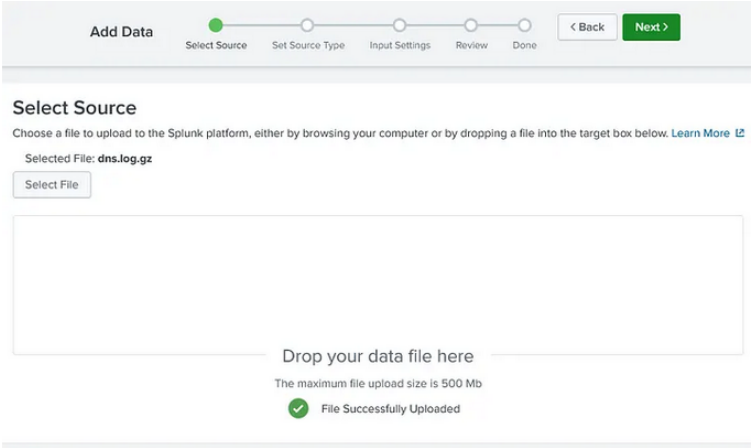

Figure 3: select dns.log.gz file

3.4 Set Source Type

- In the Set Source Type section, specify the source type for the uploaded log file.
- Choose the appropriate source type for DNS logs (e.g., dns or a custom source type if applicable).

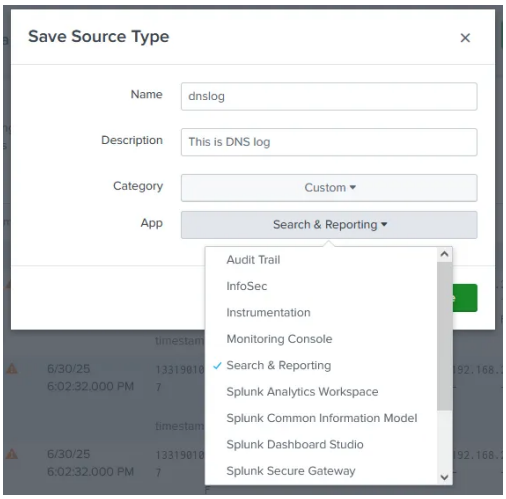

Figure 4: set source type

3.5 Review Settings

- Review other settings such as index, host, and sourcetype.
- Ensure the settings are configured correctly to match the sample DNS log file.

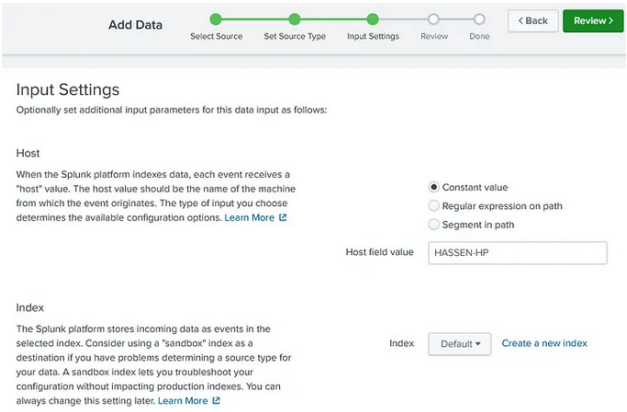

Figure 5: review settings

3.6 Click Upload

- Once all settings are configured, click on the Review button.
- Review the settings one final time to ensure accuracy.
- Click Submit to upload the sample DNS log file to Splunk.

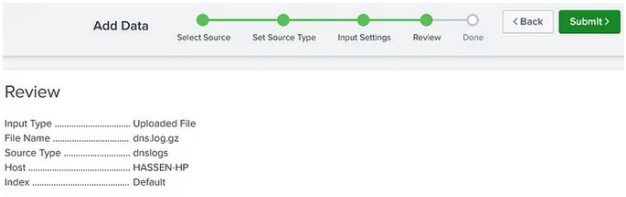

Figure 6: submit to upload DNS log file

3.7 Verify Upload

- After uploading, navigate to the search bar in the Splunk interface.

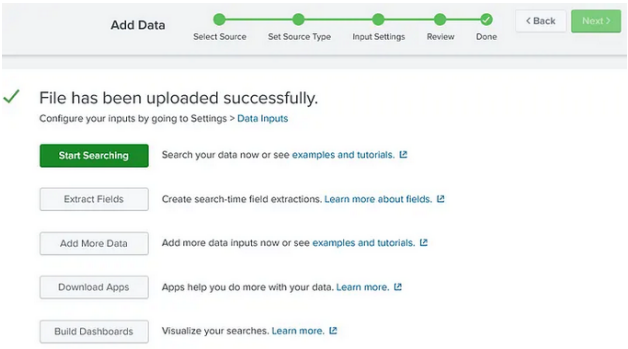

Figure 7: verify and start search

- Run a search query to verify that the uploaded DNS events are visible.

```
index=<your_dns_index> sourcetype=<your_dns_sourcetype>
```

3.8 Parsing Data

- After uploading, navigate to the search bar in the Splunk interface.

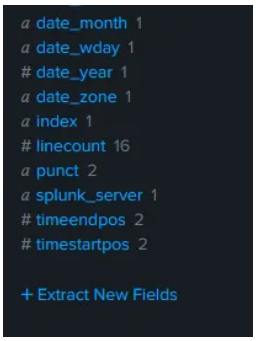

Figure 8: extract new field

- Select any event and click Next.

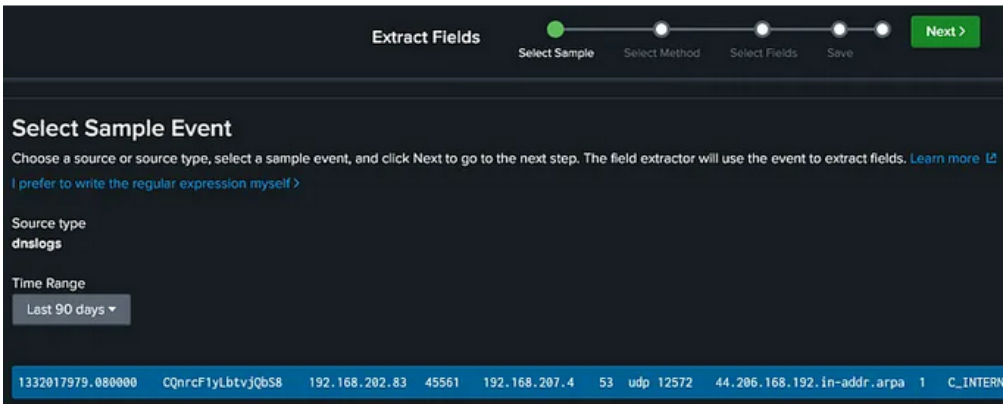

Figure 9: select event

- Select Regular Expression (you can use Delimiters too), and click Next.

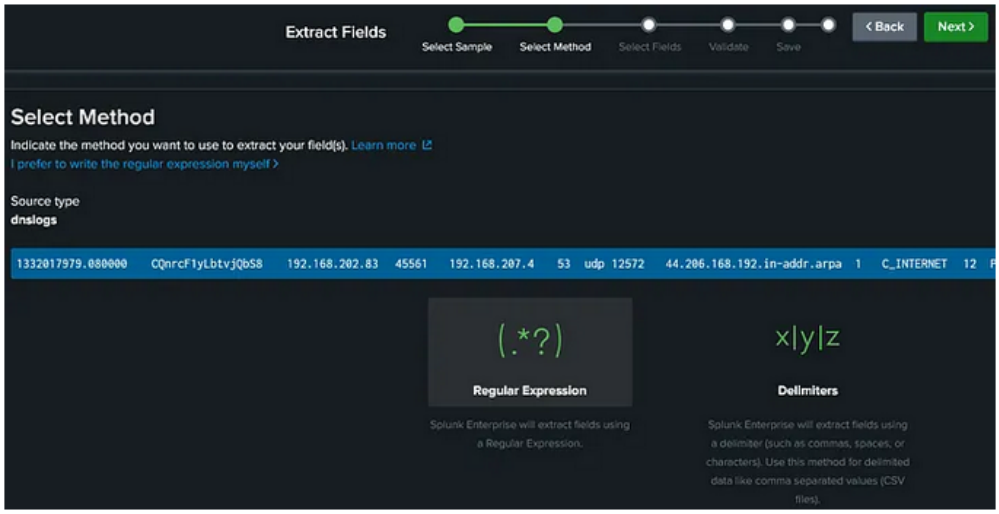

Figure 10: regular expression

- Select field 192.168.202.83 (Client machine address), and click Add Extraction.

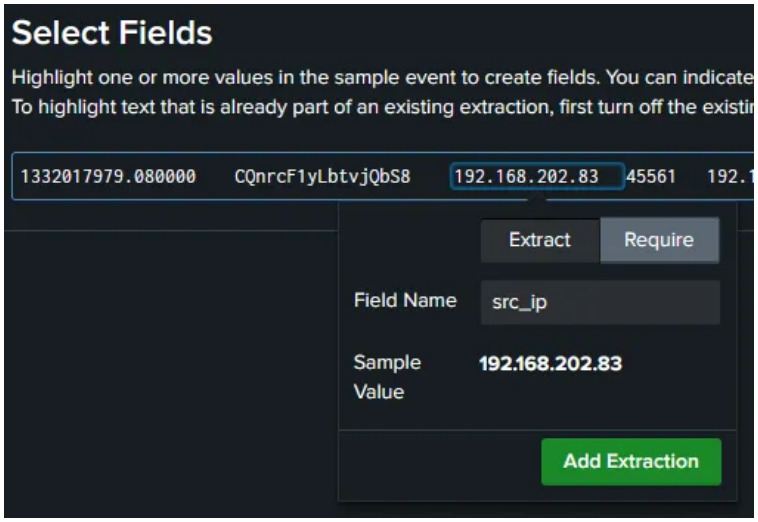

Figure 11: client machine IP address

- Select field 192.168.207.4 (DNS server address), click Add Extraction.

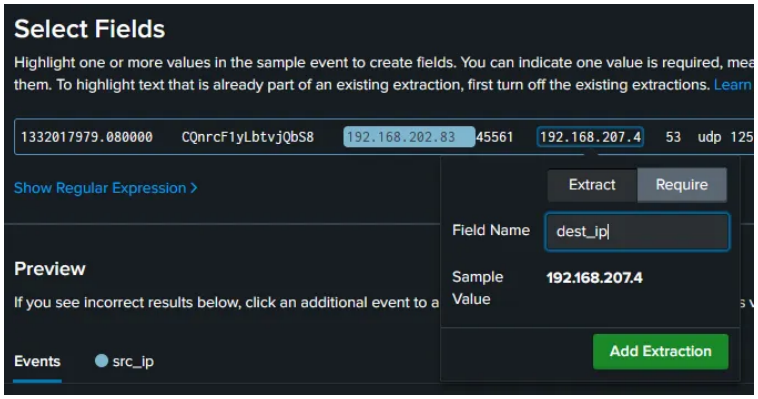

Figure 12: DNS server IP address

- Select filed 45561, give a name of src_port and click Add Extraction
- Select filed 53, give a name of dest_port and click Add Extraction

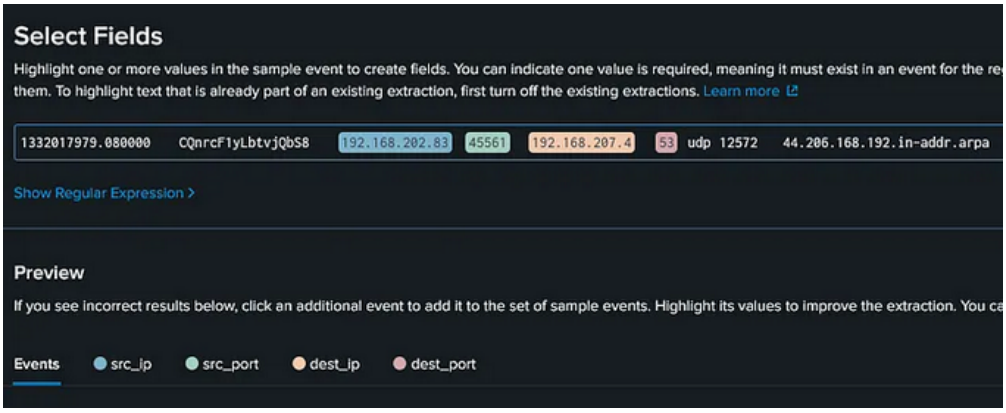

Figure 13: Source and destination ports

- Select field 44.206.168.192.in-add.arpa, give a name of fqdm (Full Qualify Domain Name) fields and Click Add Extraction.

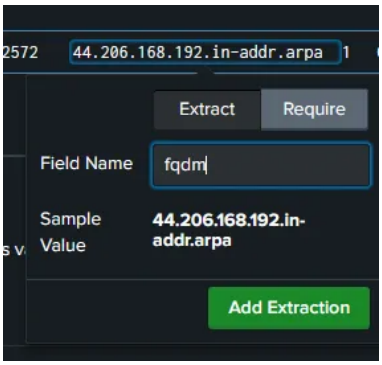

Figure 14: full qualify domain name

- Select field PTR, give a name of record and Click Add Extraction.

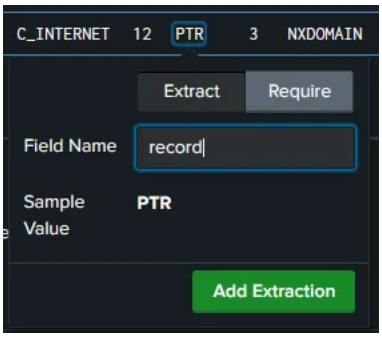

Figure 15: record field

- Select field PTR, give a name of record and Click Add Extraction.

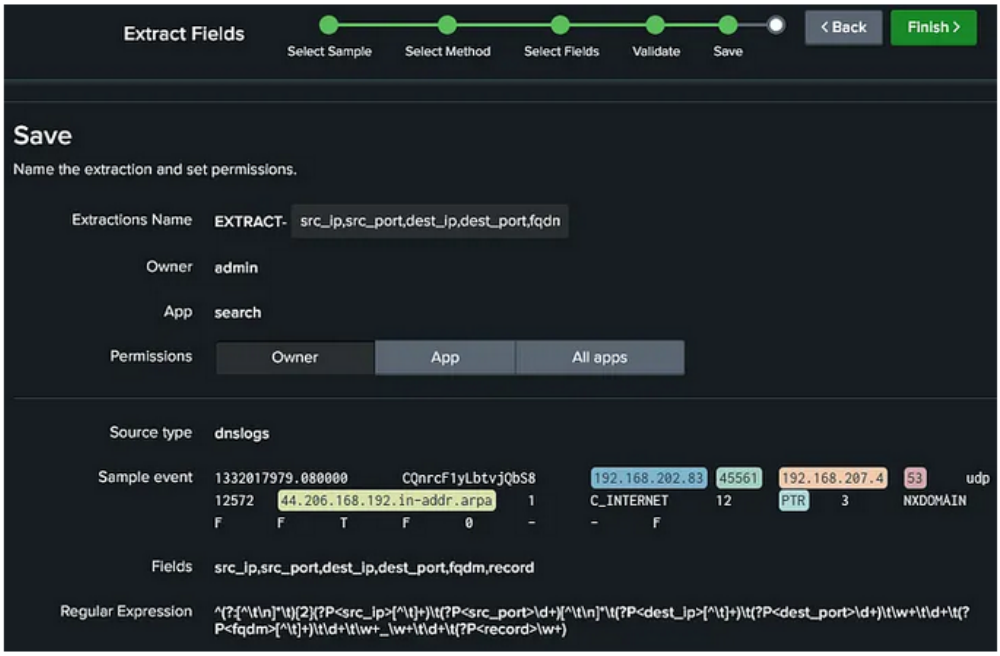

Figure 16: extract fields

- After the Select fields are validate and saved, last step is to check the new extract fields and Click Finish.

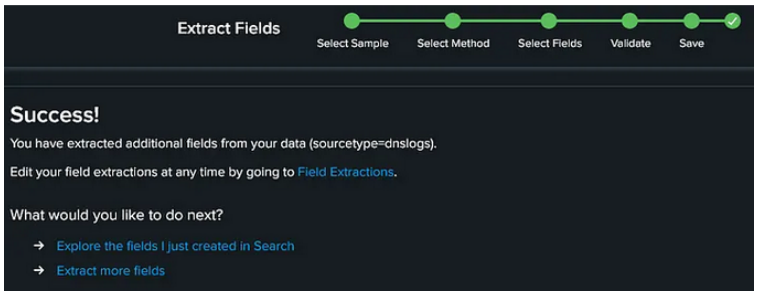

Figure 17: extract fields (success)

- Interesting Fields now contains the fields we extract dest_ip, dest_port, fqdm, src_ip, and src_port

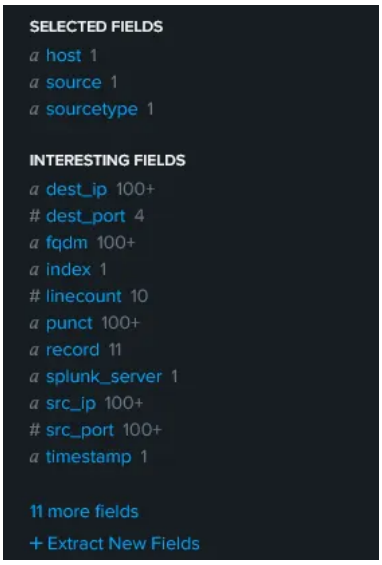

Figure 18: new fields extracted

4 Steps to Analyze DNS Log Files in Splunk

4.1 Search for DNS Events

- Open Splunk interface and navigate to the search bar.
- Enter the following search query to retrieve DNS events

```
index=_* OR index=* sourcetype=dnslogs
```

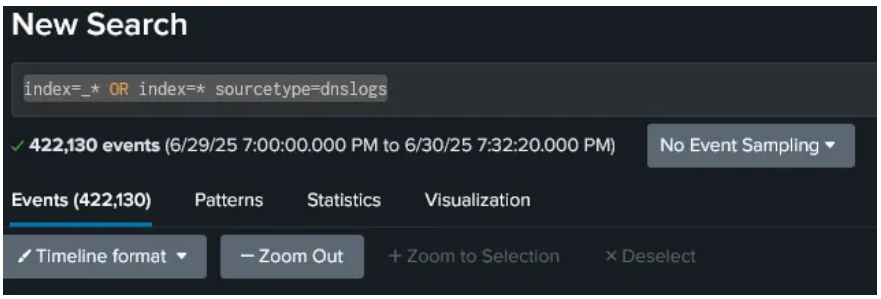

Figure 19: SPL query

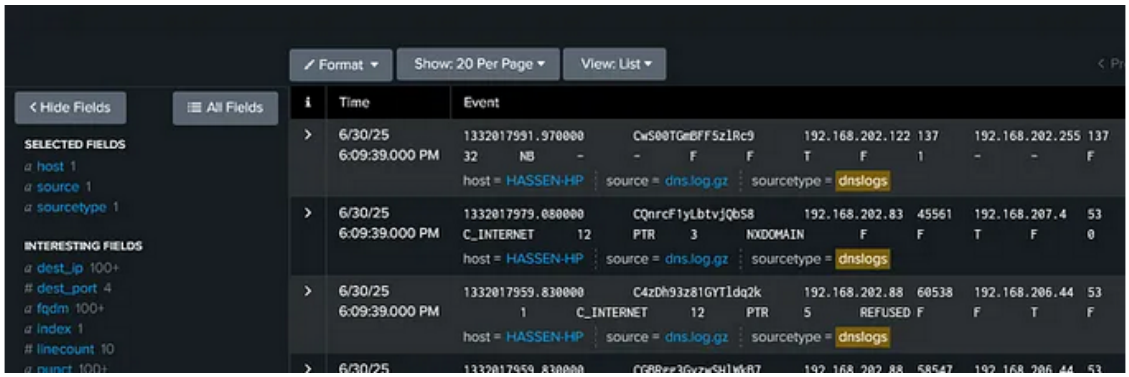

Figure 20: query results

4.2 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="(?i)(dns|domain|query|response|port 53)": This regex searches for common DNS-related keywords in the raw event data.
- Example extraction command:

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

Figure 21: extract relevant fields

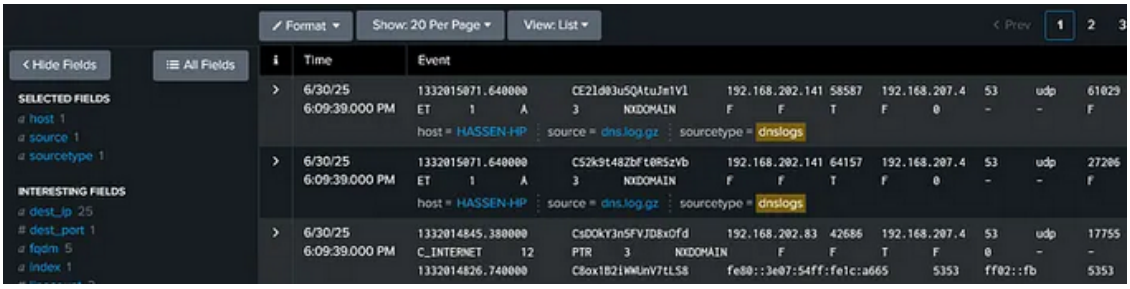

Figure 22: relevant fields results

4.3 Identify Anomalies

- Look for unusual patterns or anomalies in DNS activity.
- Example query to identify spikes

```
index=_* OR index=* sourcetype=dns_sample | stats count by fqdm
```

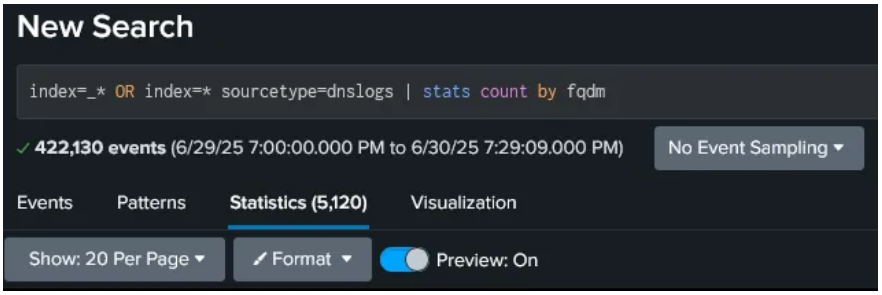

Figure 23: identify spikes

Figure 24: query result

4.4 Find the top DNS sources

- Use the top command to count the occurrences of each query type:

```
index=* sourcetype=dns_sample | top fqdn, src_ip
```

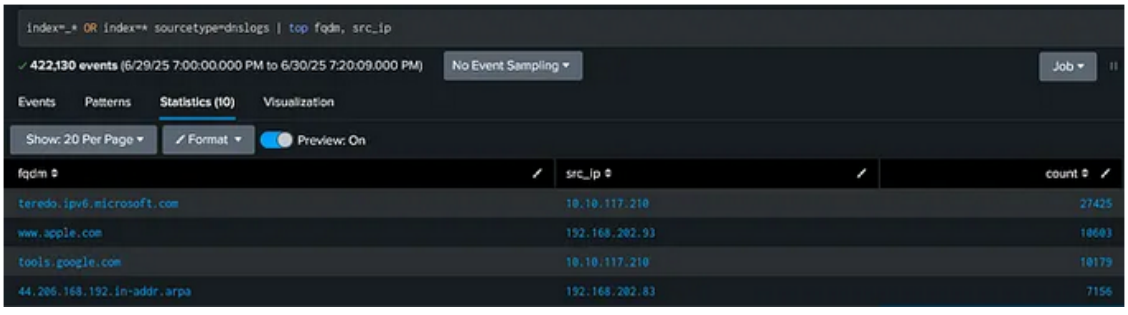

Figure 25: fields extract

4.5 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 virustotal.com
- Example search for known malicious domains:

```
index=* sourcetype=dns_sample fqdn="maliciousdomain.com"
```

```
index=_* OR index=* sourcetype=dnslogs fqdm"=44.206.168.192.in-
   addr."arpa
```

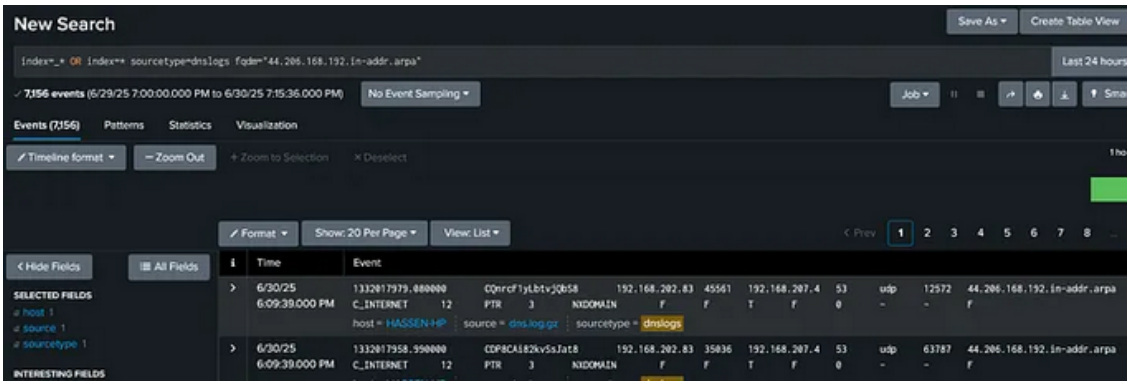

Figure 26: auspicious domains

5 Conclusion

The analysis of DNS (Domain Name System) log files using Splunk SIEM enables security professionals to efficiently detect, investigate, and respond to potential security incidents. Through comprehensive examination of DNS activity and the identification of anomalous patterns, organizations can significantly strengthen their security posture and mitigate a wide range of cyber threats. [2]

[2]The outlined procedures may be adapted as necessary to accommodate specific use cases and organizational requirements. Proceed with your analysis accordingly.