

Splunk [SIEM] Lab Walkthrough

Lab 1 — Analyzing DNS Log Files Using Splunk

Hassen Hannachi

November 21, 2025

Contents

1	Introduction	4
2	Project Overview	4
2.1	Prerequisites	4
3	Lab Walkthrough	4
3.1	Prepare Sample DNS Log Files	4
3.2	Upload Log Files to Splunk	5
3.3	Choose File	5
3.4	Set Source Type	6
3.5	Review Settings	6
3.6	Click Upload	7
3.7	Verify Upload	7
3.8	Parsing Data	7
4	Steps to Analyze DNS Log Files in Splunk	12
4.1	Search for DNS Events	12
4.2	Extract Relevant Fields	13
4.3	Identify Anomalies	14
4.4	Find the top DNS sources	14
4.5	Investigate Suspicious Domains	15
5	Conclusion	15

List of Figures

1	add DNS log data	5
2	upload DNS log data	5
3	select dns.log.gz file	5
4	set source type	6
5	review settings	6
6	submit to upload DNS log file	7
7	verify and start search	7
8	extract new field	8
9	select event	8
10	regular expression	8
11	client machine IP address	9
12	DNS server IP address	9
13	Source and destination ports	10
14	full qualify domain name	10
15	record field	10
16	extract fields	11
17	extract fields (success)	11

18	new fields extracted	12
19	SPL query	12
20	query results	13
21	extract relevant fields	13
22	relevant fields results	13
23	identify spikes	14
24	query result	14
25	fields extract	14
26	auspicious domains	15

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**.

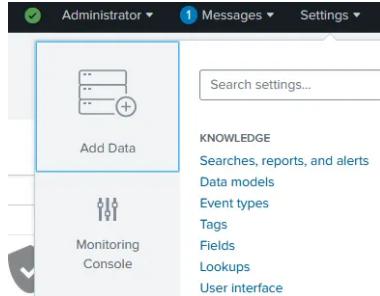


Figure 1: add DNS log data

- 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.

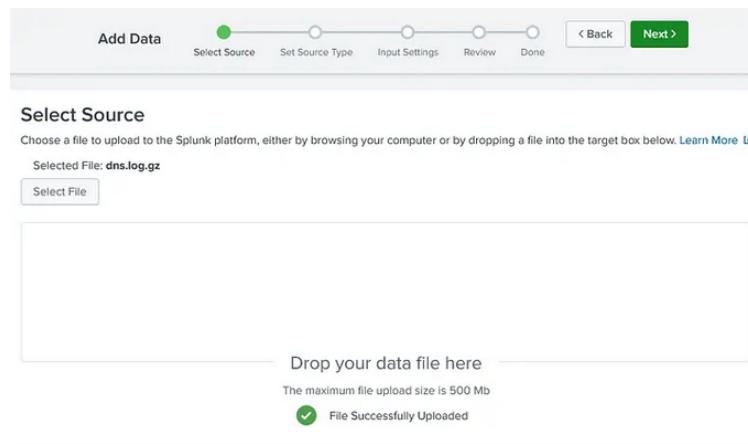


Figure 3: select dns.log.gz file

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).

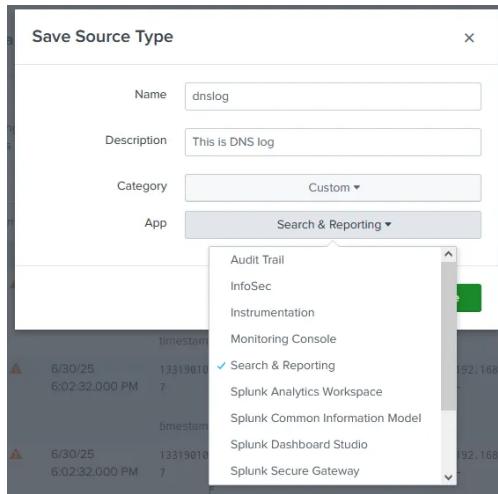


Figure 4: set source type

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.

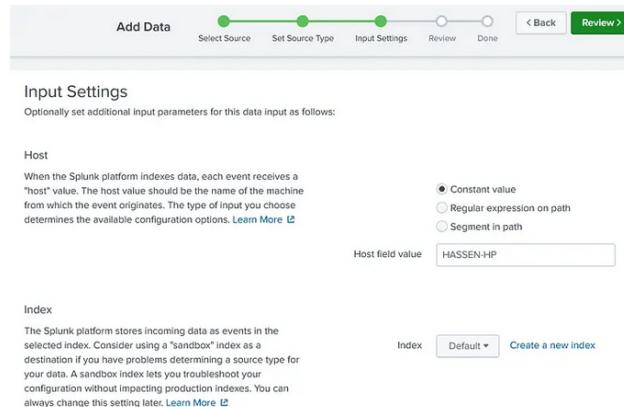


Figure 5: review settings

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.

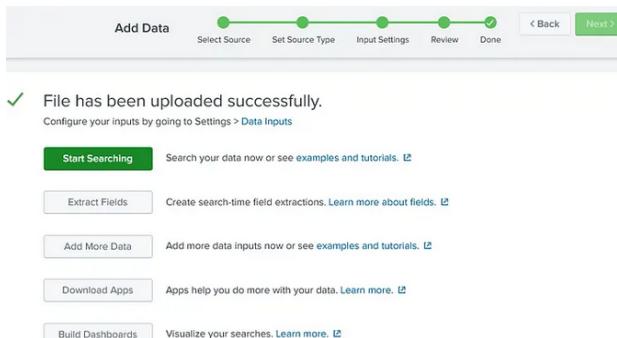


Figure 7: verify and start search

- 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.

```

a date_month 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1
# linecount 16
a punct 2
a splunk_server 1
# timeendpos 2
# timestamppos 2

+ Extract New Fields

```

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.

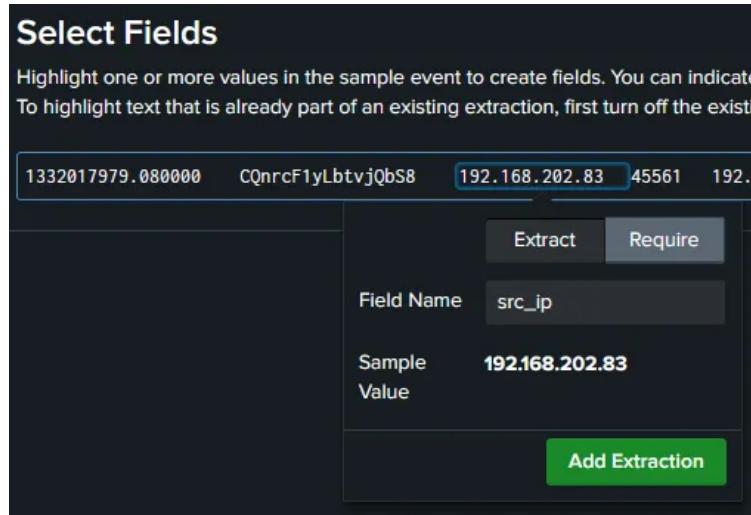


Figure 11: client machine IP address

- 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

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 rest of the event to be valid. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more [↗](#)

1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa

Show Regular Expression >

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 also click the 'Events' tab to switch back.

Events src_ip src_port dest_ip dest_port

Figure 13: Source and destination ports

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

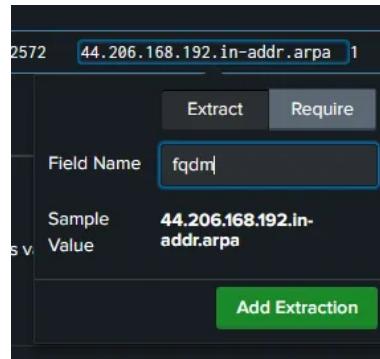


Figure 14: full qualify domain name

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

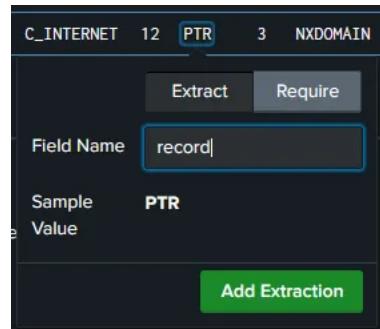


Figure 15: record field

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

Extract Fields

Select Sample Select Method Select Fields Validate Save < Back **Finish >**

Save

Name the extraction and set permissions.

Extractions Name	EXTRACT- src_ip,src_port,dest_ip,dest_port,fqdn
Owner	admin
App	search
Permissions	Owner App All apps

Source type **dnslogs**

Sample event

1332017979.080000	CQnrcF1yLbtvjqbS8	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
F	F	T	F	0	-	F

Fields **src_ip,src_port,dest_ip,dest_port,fqdn,record**

Regular Expression **^(?:(^|\n|^")|(?P<src_ip>[^"]+)|(?P<src_port>\d+)|(^|\n)^(?P<dest_ip>[^"]+)|(?P<dest_port>\d+)|(\w+\d+\w+)|(?P<fqdn>[^"]+)|(\d+\w+\d+)|(\w+\d+)(?P<record>\w+)**

Figure 16: extract fields

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

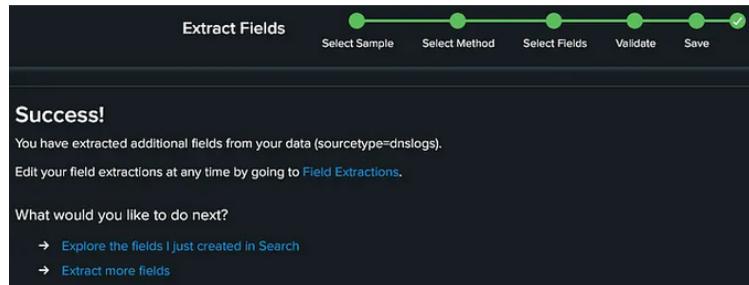


Figure 17: extract fields (success)

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

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a dest_ip 100+
- # dest_port 4
- a fqdn 100+
- a index 1
- # linecount 10
- a punct 100+
- a record 11
- a splunk_server 1
- a src_ip 100+
- # src_port 100+
- a timestamp 1

11 more fields
[+ Extract New Fields](#)

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
```

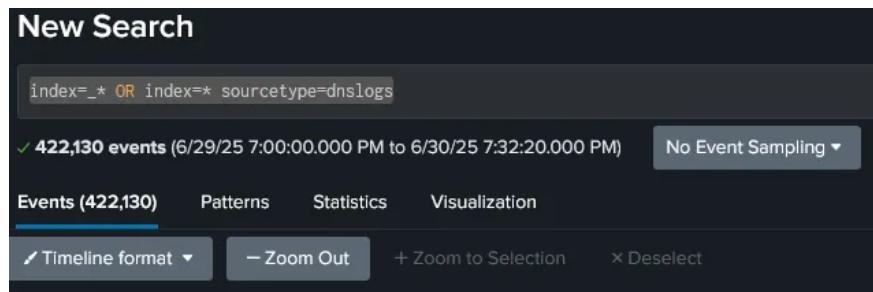


Figure 19: SPL query

Event											
	Time										
SELECTED FIELDS											
a_host 1 a_source 1 a_sourcetype 1	> 6/30/25 6:09:39.000 PM	1332017991.970000	CwS00TGeBF5z1Rc9	-	F	T	F	1	-	-	F
INTERESTING FIELDS											
a_dest_ip 100+ #dest_port 4 a_fqdn 100+ a_index 1 #linecount 10 a_pcount 100+	> 6/30/25 6:09:39.000 PM	1332017979.080000	CQnrcF1yLbtvjQbS8	12	PTR	3	NXDOMAIN	F	F	T	F
		host = HASSEN-HP	source = dns.log.gz	sourcetype = dnslogs							
	> 6/30/25 6:09:39.000 PM	1332017959.830000	C4zDh93z81GYt1dq2k	1	C_INTERNET	12	PTR	5	REFUSED	F	F
		host = HASSEN-HP	source = dns.log.gz	sourcetype = dnslogs							
	> 6/30/25	1332017959.830000	CGBrx3GyzxSH1wR7	-	-	-	-	-	-	-	-
		host = HASSEN-HP	source = dns.log.gz	sourcetype = dnslogs							

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"
```

New Search

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

✓ 1,432 events (6/29/25 7:00:00.000 PM to 6/30/25 7:34:38.000 PM) No Event Sampling ▾

Figure 21: extract relevant fields

Event											
	Time										
SELECTED FIELDS											
a_host 1 a_source 1 a_sourcetype 1	> 6/30/25 6:09:39.000 PM	1332015071.640000	CE21d03u5QAtuJmV1	ET	1	A	3	NXDOMAIN	F	F	T
INTERESTING FIELDS											
a_dest_ip 25 #dest_port 1 a_fqdn 5 a_index 1	> 6/30/25 6:09:39.000 PM	1332015071.640000	CS2k9t482bfte8SzvB	ET	1	A	3	NXDOMAIN	F	F	T
		host = HASSEN-HP	source = dns.log.gz	sourcetype = dnslogs							
	> 6/30/25 6:09:39.000 PM	1332014845.380000	Cs0OKY3n5FYJD8x0fd	C_INTERNET	12	PTR	3	NXDOMAIN	F	F	T
		1332014826.740000	CBox1B21WklnV7tLS8	host = HASSEN-HP	source = dns.log.gz	sourcetype = dnslogs					
		fe80::3e07:54ff:fe1c:a665	fe80::3e07:54ff:fe1c:a665	5353	5353	5353	5353	5353	5353	5353	5353

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 fqdn
```

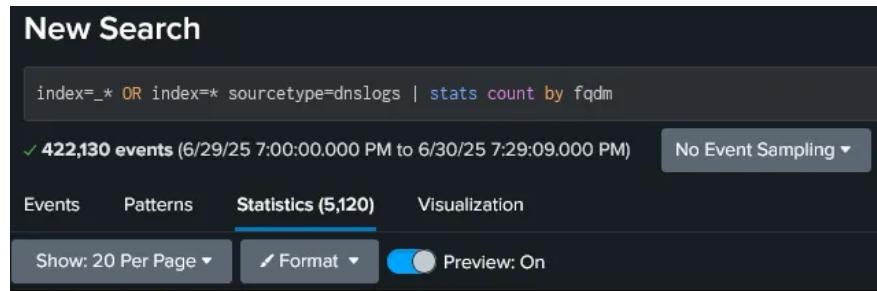


Figure 23: identify spikes

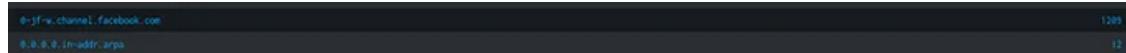


Figure 24: query result

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
```

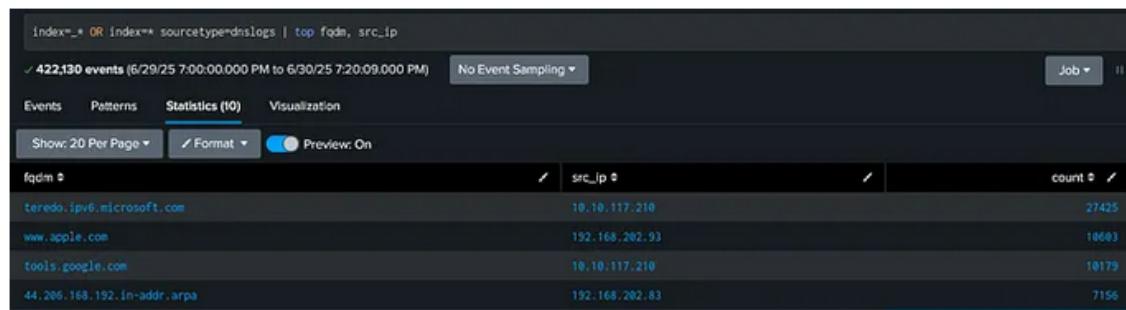
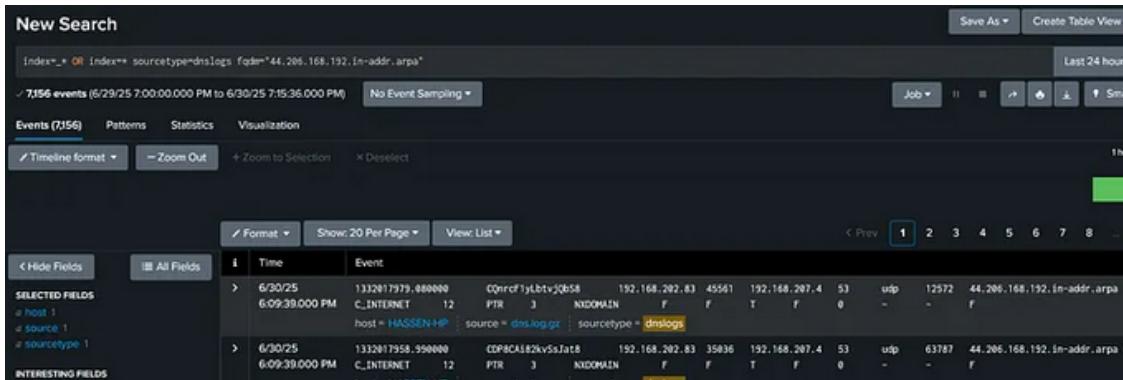


Figure 25: fields extract

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
```



The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query: "index=_* OR index=* sourcetype=dnslogs fqdm='44.206.168.192.in-addr.arpa'". Below the search bar, it says "7156 events (6/29/25 7:00:00:00 PM to 6/30/25 7:15:36:00 PM) No Event Sampling". The main area displays a table of search results with columns: #, Time, and Event. The first event is highlighted with a yellow background. The table shows two entries, both from 6/30/25 at 6:09:39.000 PM. The first entry is for host "HASSEN.HP" with source "dns.log.gz" and sourcetype "dnslogs". The second entry is for host "C_INTERNET" with source "dns.log.gz" and sourcetype "dnslogs". The table has a header row and several data rows. At the bottom, there are buttons for "Format", "Show: 20 Per Page", and "View: List". There are also navigation buttons for "Prev" and "Next".

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

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