Analyzing DNS Logs Using Splunk SIEM:

Introduction:

DNS (Domain Name System) logs are crucial for understanding network activity and identifying potential security threats. Splunk SIEM (Security Information and Event Management) provides powerful capabilities for analyzing DNS logs and detecting anomalies or malicious activities.

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.

Steps to Upload Sample DNS Log Files to Splunk SIEM

1. Prepare Sample DNS Log Files

- Obtain sample [DNS log file] (https://www.secrepo.com/maccdc2012/dns.log.gz) 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.

2. Upload Log Files to Splunk

- Log in to the Splunk web interface.
- Navigate to **Settings** > **Add Data**.
- Select **Upload** as the data input method.

3. Choose File

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

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).

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.

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.

7. Verify Upload

- After uploading, navigate to the search bar in the Splunk interface.
- Run a search query to verify that the uploaded DNS events are visible.

SPL:

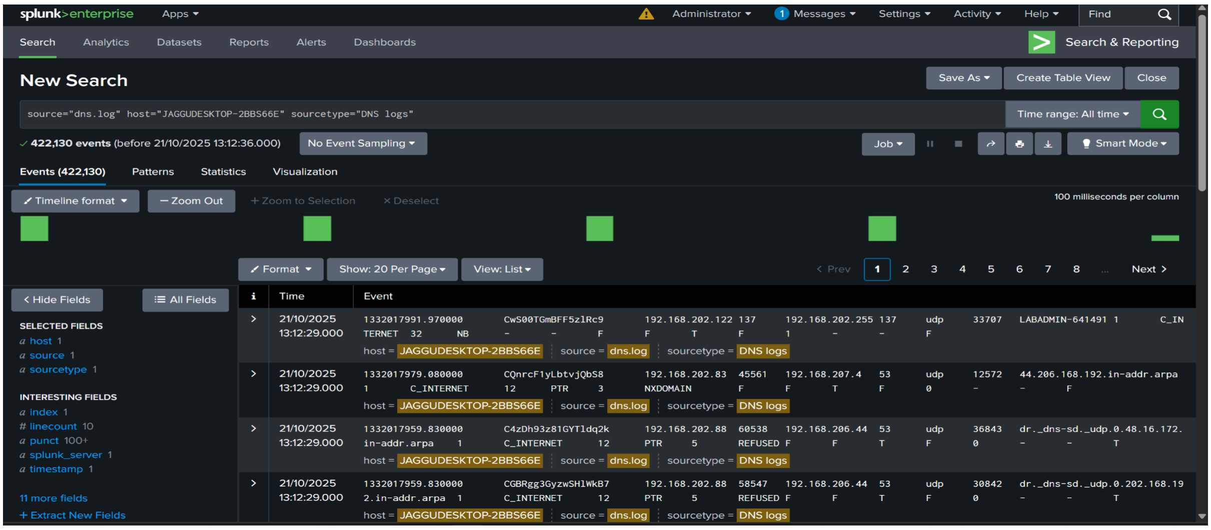
index=_* OR index=* sourcetype="DNS logs"

Steps to Analyze DNS Log Files in Splunk SIEM:

1. Search for DNS Events

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

SPL: index=_* OR index=* sourcetype="DNS logs" | source="dns.log" host="JAGGUDESKTOP-2BBS66E" sourcetype="DNS logs"



```
source="dns.log" host="JAGGUDESKTOP-2BBS66E" sourcetype="DNS logs"
```

✓ 422,130 events (before 21/10/2025 13:12:36.000)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

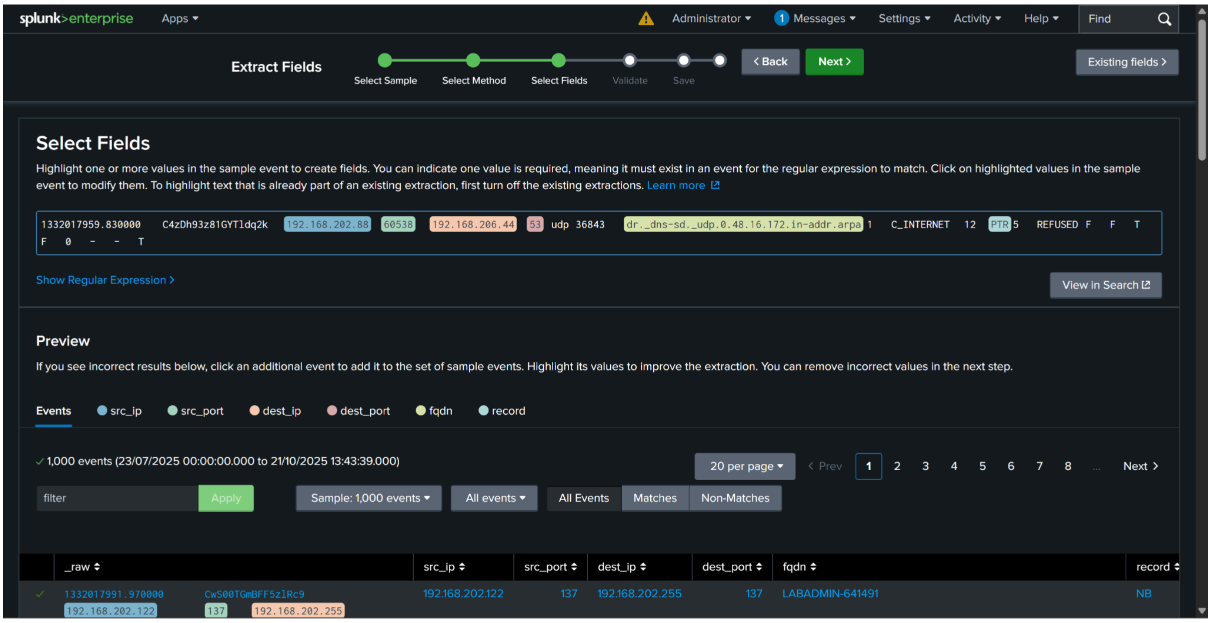
INTERESTING FIELDS
- a index 1
- # linecount 10
- a punct 100+
- a splunk_server 1
- a timestamp 1

```
i  Time          Event
>  21/10/2025    1332017991.970000    CwS00TGmBFF5zlRc9    192.168.202.122 137    192.168.202.255 137    udp    33707    LABADMIN-641491 1    C_IN
   13:12:29.000  TERNET   32    NB    -    -    F    F    T    F    1    -    -    F
                 host = JAGGUDESKTOP-2BBS66E | source = dns.log | sourcetype = DNS logs
>  21/10/2025    1332017979.080000    CQnrcF1yLbtvjQbS8    192.168.202.83  45561  192.168.207.4   53     udp    12572    44.206.168.192.in-addr.arpa
   13:12:29.000  1    C_INTERNET    12    PTR    3    NXDOMAIN    F    F    T    F    0    -    -    F
                 host = JAGGUDESKTOP-2BBS66E | source = dns.log | sourcetype = DNS logs
>  21/10/2025    1332017959.830000    C4zDh93z81GYTldq2k    192.168.202.88  60538  192.168.206.44  53     udp    36843    dr._dns-sd._udp.0.48.16.172.
   13:12:29.000  in-addr.arpa    1    C_INTERNET    12    PTR    5    REFUSED F    F    T    F    0    -    -    T
                 host = JAGGUDESKTOP-2BBS66E | source = dns.log | sourcetype = DNS logs
>  21/10/2025    1332017959.830000    CGBRgg3GyzwSHlWkB7    192.168.202.88  58547  192.168.206.44  53     udp    30842    dr._dns-sd._udp.0.202.168.19
   13:12:29.000  2.in-addr.arpa    1    C_INTERNET    12    PTR    5    REFUSED F    F    T    F    0    -    -    T
                 host = JAGGUDESKTOP-2BBS66E | source = dns.log | sourcetype = DNS logs
```

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)\b(dns|domain|query|response|port 53)\b": This regex searches for common DNS-related keywords in the raw event data.

SPL: source="dns.log" host="JAGGUDESKTOP-2BBS66E" sourcetype="DNS logs" | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"



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 regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more

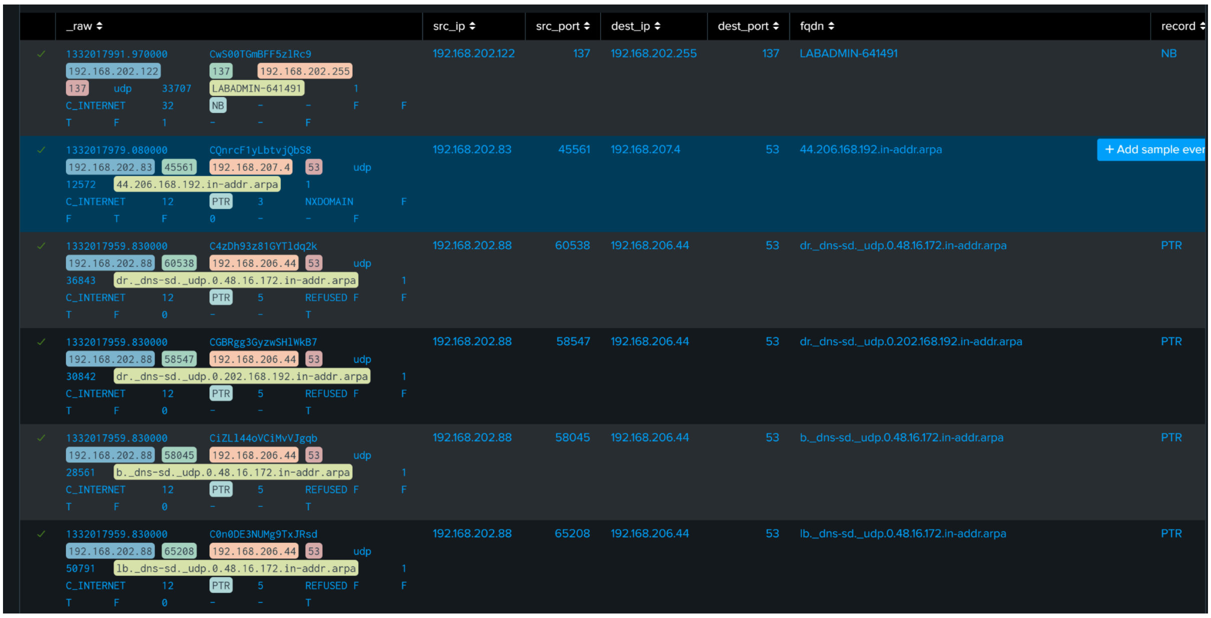
```
1332017959.830000    C4zDh93z81GYTldq2k  192.168.202.88  60538  192.168.206.44  53  udp  36843   dr._dns-sd._udp.0.48.16.172.in-addr.arpa 1   C_INTERNET   12  PTR 5   REFUSED F   F   T
F   0   -   -   T
```

Preview

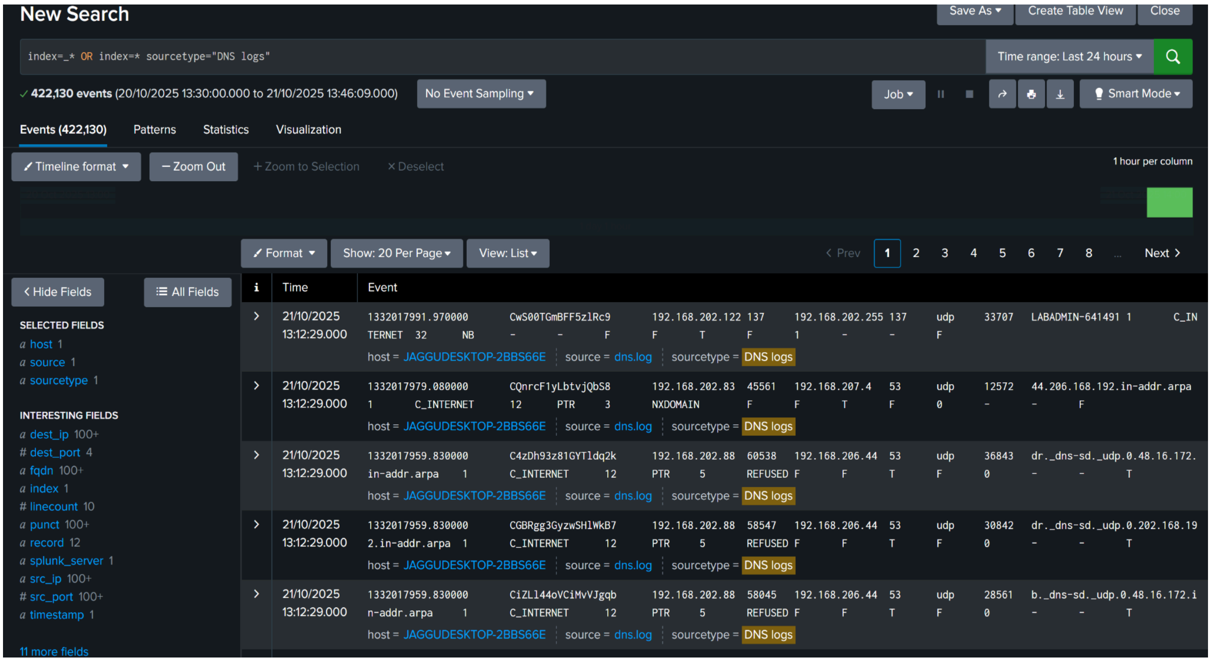
If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

✓ 1,000 events (23/07/2025 00:00:00.000 to 21/10/2025 13:43:39.000)

	_raw	src_ip	src_port	dest_ip	dest_port	fqdn	record
✓	1332017991.970000 CwS00TGmBFF5zlRc9 192.168.202.122 137 192.168.202.255	192.168.202.122	137	192.168.202.255	137	LABADMIN-641491	NB



	_raw	src_ip	src_port	dest_ip	dest_port	fqdn	record
✓	1332017991.970000 CwS00TGmBFF5zlRc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_INTERNET 32 NB - - F F T F 1 - - F	192.168.202.122	137	192.168.202.255	137	LABADMIN-641491	NB
✓	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 NXDOMAIN F F T F 0 - - F	192.168.202.83	45561	192.168.207.4	53	44.206.168.192.in-addr.arpa	
✓	1332017959.830000 C4zDh93z81GYTldq2k 192.168.202.88 60538 192.168.206.44 53 udp 36843 dr._dns-sd._udp.0.48.16.172.in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T	192.168.202.88	60538	192.168.206.44	53	dr._dns-sd._udp.0.48.16.172.in-addr.arpa	PTR
✓	1332017959.830000 CGBRgg3GyzwSHlWkB7 192.168.202.88 58547 192.168.206.44 53 udp 30842 dr._dns-sd._udp.0.202.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T	192.168.202.88	58547	192.168.206.44	53	dr._dns-sd._udp.0.202.168.192.in-addr.arpa	PTR
✓	1332017959.830000 CiZLl44oVCiMvVJgqb 192.168.202.88 58045 192.168.206.44 53 udp 28561 b._dns-sd._udp.0.48.16.172.in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T	192.168.202.88	58045	192.168.206.44	53	b._dns-sd._udp.0.48.16.172.in-addr.arpa	PTR
✓	1332017959.830000 C0n0DE3NUMg9TxJRsd 192.168.202.88 65208 192.168.206.44 53 udp 50791 lb._dns-sd._udp.0.48.16.172.in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T	192.168.202.88	65208	192.168.206.44	53	lb._dns-sd._udp.0.48.16.172.in-addr.arpa	PTR



New Search

```
index=_* OR index=* sourcetype="DNS logs"
```

✓ 422,130 events (20/10/2025 13:30:00.000 to 21/10/2025 13:46:09.000)

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 12
- a splunk_server 1
- a src_ip 100+
- # src_port 100+
- a timestamp 1

11 more fields

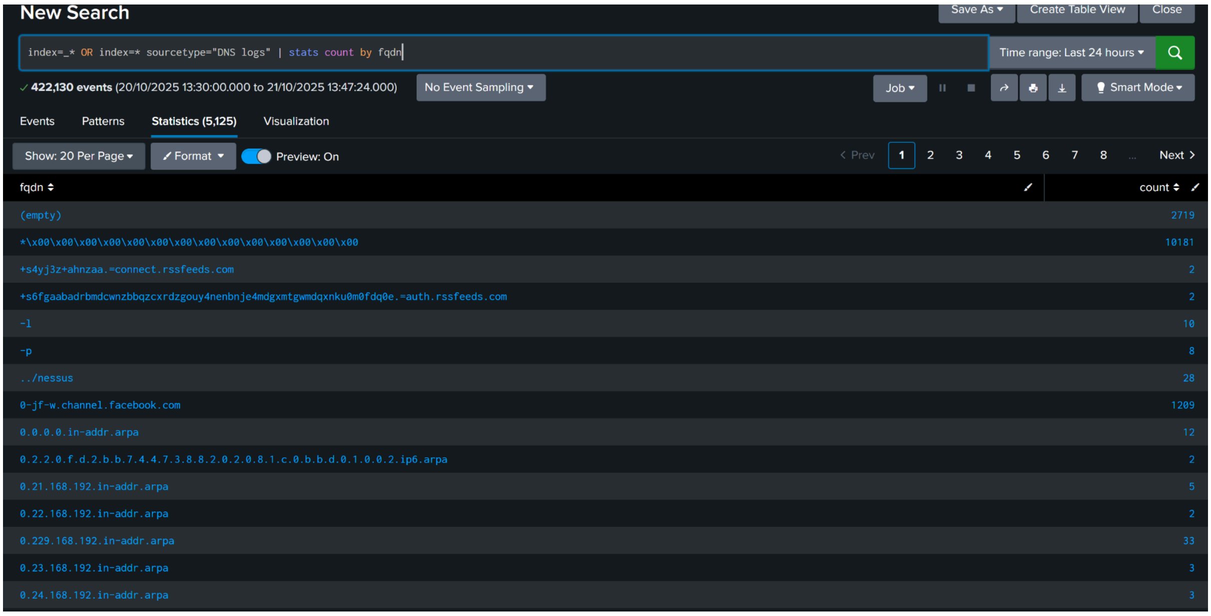
i	Time	Event
›	21/10/2025 13:12:29.000	1332017991.970000 CwS00TGmBFF5zlRc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_IN TERNET 32 NB - - F F T F 1 - - F host = JAGGUDESKTOP-2BBS66E ¦ source = dns.log ¦ sourcetype = DNS logs
›	21/10/2025 13:12:29.000	1332017979.080000 CQnrcF1yLbtvjQbS8 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 NXDOMAIN F F T F 0 - - F host = JAGGUDESKTOP-2BBS66E ¦ source = dns.log ¦ sourcetype = DNS logs
›	21/10/2025 13:12:29.000	1332017959.830000 C4zDh93z81GYTldq2k 192.168.202.88 60538 192.168.206.44 53 udp 36843 dr._dns-sd._udp.0.48.16.172. in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T host = JAGGUDESKTOP-2BBS66E ¦ source = dns.log ¦ sourcetype = DNS logs
›	21/10/2025 13:12:29.000	1332017959.830000 CGBRgg3GyzwSHlWkB7 192.168.202.88 58547 192.168.206.44 53 udp 30842 dr._dns-sd._udp.0.202.168.19 2.in-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T host = JAGGUDESKTOP-2BBS66E ¦ source = dns.log ¦ sourcetype = DNS logs
›	21/10/2025 13:12:29.000	1332017959.830000 CiZLl44oVCiMvVJgqb 192.168.202.88 58045 192.168.206.44 53 udp 28561 b._dns-sd._udp.0.48.16.172.i n-addr.arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - T host = JAGGUDESKTOP-2BBS66E ¦ source = dns.log ¦ sourcetype = DNS logs

3. Identify Anomalies

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

SPL:

index=_* OR index=* sourcetype=dns_sample | stats count by fqdn



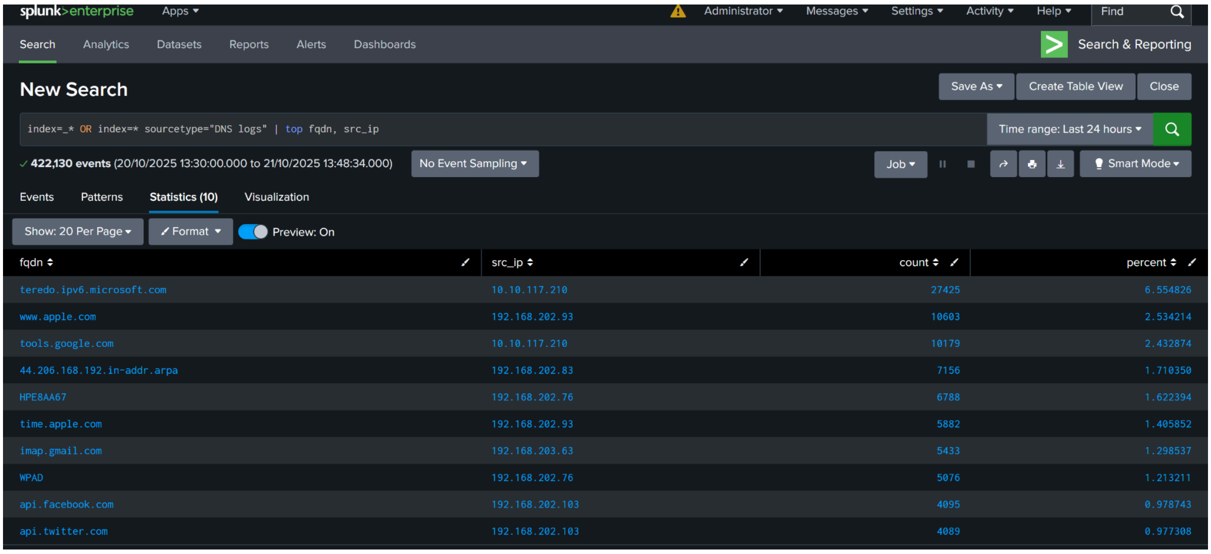
```
index=_* OR index=* sourcetype="DNS logs" | stats count by fqdn
```

✓ **422,130 events** (20/10/2025 13:30:00.000 to 21/10/2025 13:47:24.000)

fqdn	count
(empty)	2719
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	10181
+s4yj3z+ahnzaa.=connect.rssfeeds.com	2
+s6fgaabadrbmdcwnzbbqzcxrdzgouy4nenbnje4mdgxmtgwmdqxnku0m0fdq0e.=auth.rssfeeds.com	2
-l	10
-p	8
../nessus	28
0-jf-w.channel.facebook.com	1209
0.0.0.0.in-addr.arpa	12
0.2.2.0.f.d.2.b.b.7.4.4.7.3.8.8.2.0.2.0.8.1.c.0.b.b.d.0.1.0.0.2.ip6.arpa	2
0.21.168.192.in-addr.arpa	5
0.22.168.192.in-addr.arpa	2
0.229.168.192.in-addr.arpa	33
0.23.168.192.in-addr.arpa	3
0.24.168.192.in-addr.arpa	3

4. Find the top DNS sources

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



```
index=_* OR index=* sourcetype="DNS logs" | top fqdn, src_ip
```

✓ **422,130 events** (20/10/2025 13:30:00.000 to 21/10/2025 13:48:34.000)

fqdn	src_ip	count	percent
teredo.ipv6.microsoft.com	10.10.117.210	27425	6.554826
www.apple.com	192.168.202.93	10603	2.534214
tools.google.com	10.10.117.210	10179	2.432874
44.206.168.192.in-addr.arpa	192.168.202.83	7156	1.710350
HPE8AA67	192.168.202.76	6788	1.622394
time.apple.com	192.168.202.93	5882	1.405852
imap.gmail.com	192.168.203.63	5433	1.298537
WPAD	192.168.202.76	5076	1.213211
api.facebook.com	192.168.202.103	4095	0.978743
api.twitter.com	192.168.202.103	4089	0.977308

SPL: index=* sourcetype=dns_sample | top fqdn, src_ip

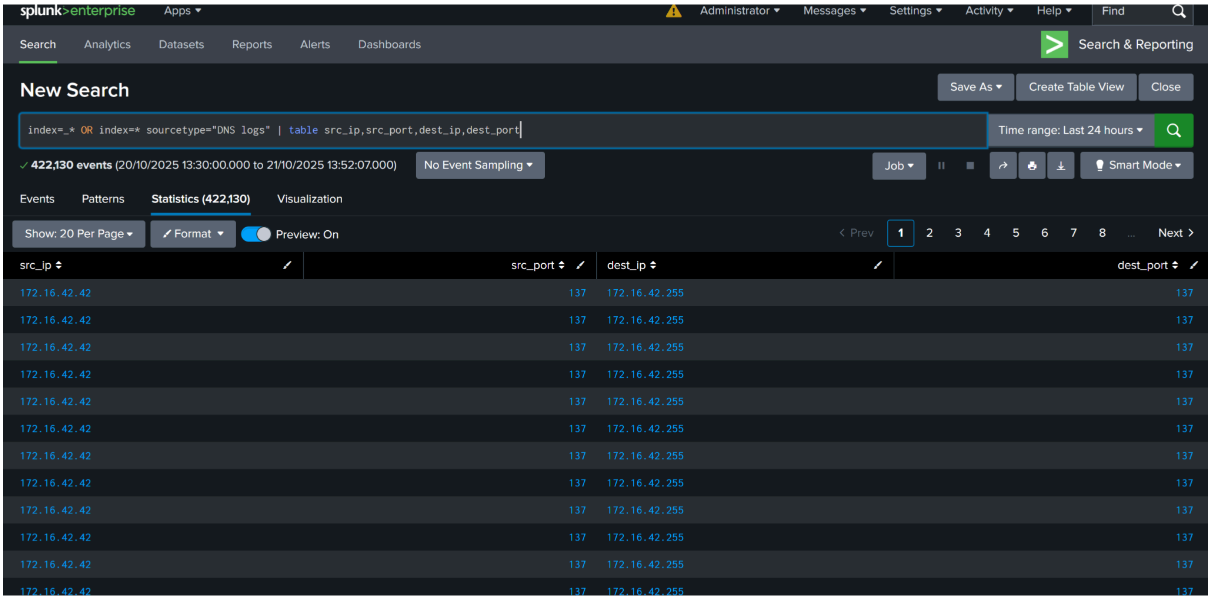
5. Investigate Suspicious Domains

- 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:

SPL: index=* sourcetype=dns_sample fqdn="maliciousdomain.com"

No Malicious Domains found in the uploaded data.

- Created a table view of src_ip,src_port,dest_ip,dest_port



```
index=_* OR index=* sourcetype="DNS logs" | table src_ip,src_port,dest_ip,dest_port
```

✓ 422,130 events (20/10/2025 13:30:00.000 to 21/10/2025 13:52:07.000)

src_ip	src_port	dest_ip	dest_port
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137
172.16.42.42	137	172.16.42.255	137

<u>Conclusion:</u>

Analyzing DNS log files using Splunk SIEM enables security professionals to detect and respond to potential security incidents effectively. By understanding DNS activity and identifying anomalies, organizations can enhance their overall security posture and protect against various cyber threats.