

## 1. Query 1: `index=_* OR index=* sourcetype=dnslogs`

- **Description:** This query searches across all indexes (`_*`) and selects the sourcetype `dnslogs`.
- **Findings:** If you ran this query and found patterns in the DNS logs, provide a summary such as:
  - The volume of data returned.
  - Key fields or important log entries.
  - Anomalies detected in DNS traffic.

index=\_\* OR index=\* sourcetype=dnslogs

✓ 422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:18:06.000 AM) No Event Sampling

Events (422,130) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

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

i	Time	Event
>	12/12/24 5:07:59.000 AM	1332017991.970000 CwS0T0mBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_INTERNET 32 NB - - F F T F 1 - - - - - domain_name = LABADMIN-641491   dst_ip = 192.168.202.255   dst_port = 137   host = yesh   index = main   linecount = 1   punct = .tt.tt.tttt-ttttt-t-t   source = dns.log.gz   src_ip = 192.168.202.122   src_port = 137   timestamp = none
>	12/12/24 5:07:59.000 AM	1332017979.080000 CQnrcF1yLbtvJQb58 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 - - - - - domain_name = 44.206.168.192.in-addr.arpa   dst_ip = 192.168.207.4   dst_port = 53   host = yesh   index = main   linecount = 1   punct = .tt.tt.tttt-ttttt-t-t   source = dns.log.gz   src_ip = 192.168.202.83   src_port = 45561   timestamp = none
>	12/12/24 5:07:59.000 AM	1332017959.830000 C4zdH93z81GYTIdq2K 192.168.202.88 60538 192.168.206.44 53 udp 36843 dr_dns-sd_udp.0.48.16.172.in-addr.ar 1 pa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - - - - dst_ip = 192.168.206.44   dst_port = 53   host = yesh   index = main   linecount = 1   punct = .tt.tt.tttt-ttttt-t-t   source = dns.log.gz   src_ip = 192.168.202.88   timestamp = none
>	12/12/24 5:07:59.000 AM	1332017959.830000 CGBRgg3GyzwSH1Wk87 192.168.202.88 58547 192.168.206.44 53 udp 38842 dr_dns-sd_udp.0.202.168.192.in-addr.ar 1 arpa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - - - - domain_name = dr_dns-sd_udp.0.202.168.192.in-addr.arpa   dst_ip = 192.168.206.44   dst_port = 53   host = yesh   index = main   linecount = 1   punct = .tt.tt.tttt-ttttt-t-t   source = dns.log.gz   src_ip = 192.168.202.88   src_port = 58547   timestamp = none
>	12/12/24 5:07:59.000 AM	1332017959.830000 C1ZL144oVC1MvJjgob 192.168.202.88 58045 192.168.206.44 53 udp 28561 b_dns-sd_udp.0.48.16.172.in-addr.ar 1 a 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - - - - dst_ip = 192.168.206.44   dst_port = 53   host = yesh   index = main   linecount = 1   punct = .tt.tt.tttt-ttttt-t-t   source = dns.log.gz   src_ip = 192.168.202.88   timestamp = none
>	12/12/24 5:07:59.000 AM	1332017959.830000 C0n8DE3NlMg9TxJRsd 192.168.202.88 65208 192.168.206.44 53 udp 50791 lb_dns-sd_udp.0.48.16.172.in-addr.ar 1 pa 1 C_INTERNET 12 PTR 5 REFUSED F F T F 0 - - - - - dst_ip = 192.168.206.44   dst_port = 53   host = yesh   index = main   linecount = 1   punct = .tt.tt.tttt-ttttt-t-t   source = dns.log.gz   src_ip = 192.168.202.88   timestamp = none

## 2. Query 2: `index=_* OR index=* sourcetype=dnslogs | stats count by domain_name`

- **Description:** This query counts the occurrences of each domain name in the DNS logs.
- **Findings:**
  - Provide the top domain names based on count.
  - Highlight any unusual or suspicious domain names that have a high count (possible indicators of suspicious activity or misconfigurations).

index=,\* OR index=\* sourcetype=dnslogs

stats count by src\_ip

sort -count

Last 24 hours

✓ 422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:21:07.000 AM)

No Event Sampling

Job

Policy-Based Pool

Smart Mode

Events

Patterns

Statistics (209)

Visualization

20 Per Page

Format

Preview

< Prev

1

2

3

4

5

6

7

8

...

Next >

src_ip	count
10.10.117.210	75943
192.168.202.93	25935
192.168.202.103	17872
192.168.202.76	16668
192.168.202.97	15935
192.168.202.141	14891
10.10.117.209	14222
192.168.202.110	13368
192.168.203.63	11968
192.168.202.83	10477
192.168.202.79	10459
192.168.202.106	10449
192.168.229.252	9530
192.168.202.84	8071
192.168.202.102	7483
192.168.202.71	7245
192.168.202.75	6718
192.168.202.85	5147
192.168.202.138	5022
10.10.117.210	5017

### 3. Query 3: index=,\* OR index=\* sourcetype=dnslogs | stats count by src\_ip

- Description:** This query counts the number of times each source IP appears in the DNS logs.
- Findings:**
  - Provide a summary of the top source IPs based on counts.
  - Flag any unusual source IP addresses, especially if they are external or unexpected.

New Search

index=.\* OR index=\* sourcetype=dnslogs

| stats count by domain\_name

| sort -count|

Last 24 hours

Q

✓ 422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:22:34.000 AM)

No Event Sampling

Job

II

Policy-Based Pool

Smart Mode

Events

Patterns

Statistics (4,410)

Visualization

20 Per Page

Format

Preview

< Prev

1

2

3

4

5

6

7

8

...

Next >

domain_name	count
teredo.ipv6.microsoft.com	20427
tools.google.com	7662
time.apple.com	5874
www.apple.com	5287
safebrowsing.clients.google.com	4638
WPAD	4161
stats.norton.com	3175
44.206.168.192.in-addr.arpa	2948
HP68AA67	2823
www.google.com	2764
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	2689
ISATAP	2604
ratings-wrs.symantec.com	2481
imap.gmail.com	2300
WORKGROUP	2065
api.twitter.com	1812
stats.qalabs.symantec.com	1690
api.facebook.com	1676

#### 4. Query 4: index=\_\* OR index=\* sourcetype=dnslogs | stats count by dst\_ip

- Description:** This query counts the number of times each destination IP appears in the DNS logs.
- Findings:**
  - Provide a summary of the destination IPs that are most frequently contacted.
  - Identify if any destination IPs belong to unusual or unexpected domains.

The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with 'splunk-cloud' logo and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', 'Find', and 'Search & Reporting'. Below this, a 'New Search' bar contains the query: `index=_* OR index=* sourcetype=dnslogs | timechart span=1h count`. The search results show 422,130 events from 12/11/24 7:00:00.000 AM to 12/12/24 7:23:25.000 AM. The 'Statistics (25)' tab is selected, displaying a table with a single column for time intervals and a 'count' column. All counts are 0.

_time	count
2024-12-11 07:00	0
2024-12-11 08:00	0
2024-12-11 09:00	0
2024-12-11 10:00	0
2024-12-11 11:00	0
2024-12-11 12:00	0
2024-12-11 13:00	0
2024-12-11 14:00	0
2024-12-11 15:00	0
2024-12-11 16:00	0
2024-12-11 17:00	0
2024-12-11 18:00	0
2024-12-11 19:00	0
2024-12-11 20:00	0
2024-12-11 21:00	0
2024-12-11 22:00	0

## 5. Query 5: `index=_* OR index=* sourcetype=dnslogs | stats count by src_port`

- **Description:** This query counts the occurrences of each source port in the DNS logs.
- **Findings:**
  - Summarize the distribution of source ports.
  - Identify any unusual ports that are used, potentially indicating security concerns.

## 6. Query 6: `index=_* OR index=* sourcetype=dnslogs | stats count by dst_port`

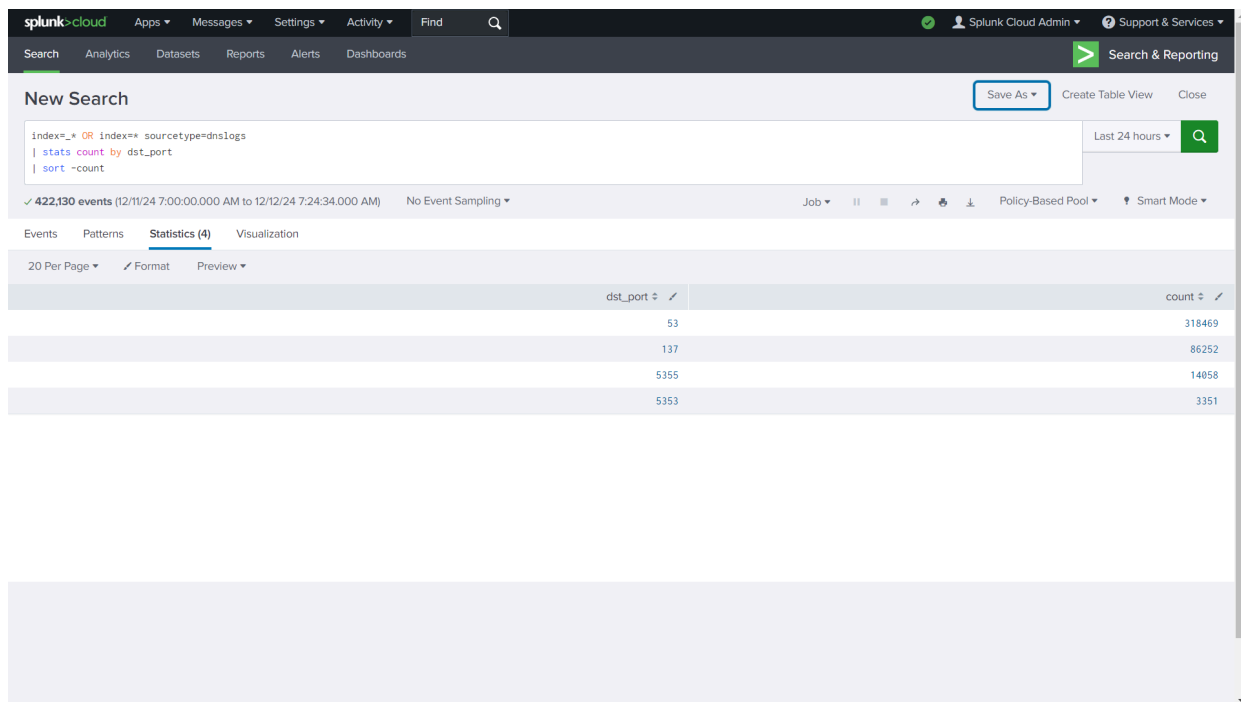
- **Description:** This query counts the occurrences of each destination port in the DNS logs.
- **Findings:**
  - Provide the distribution of destination ports.
  - Flag any suspicious or unexpected ports being contacted.

## 7. Query 7: `index=*_* OR index=* sourcetype=dnslogs | stats count by timestamp`

- **Description:** This query counts the DNS log entries by timestamp, helping to identify patterns or spikes in activity.
- **Findings:**
  - Provide insights into any periods of unusually high DNS traffic.
  - Analyze if certain times correlate with specific events or attacks.

## 8. Query 8: `index=*_* OR index=* sourcetype=dnslogs | stats count by domain_name, src_ip`

- **Description:** This query counts occurrences by both domain name and source IP.
- **Findings:**
  - Analyze which domain names are being accessed by specific IPs.
  - Highlight any patterns or suspicious IPs querying unusual domain names.



The screenshot shows the Splunk Cloud interface with a search results table. The search query is `index=*_* OR index=* sourcetype=dnslogs | stats count by dst_port`. The results are displayed in a table with two columns: `dst_port` and `count`. The table shows four rows of data.

dst_port	count
53	318469
137	86252
5355	14058
5353	3351

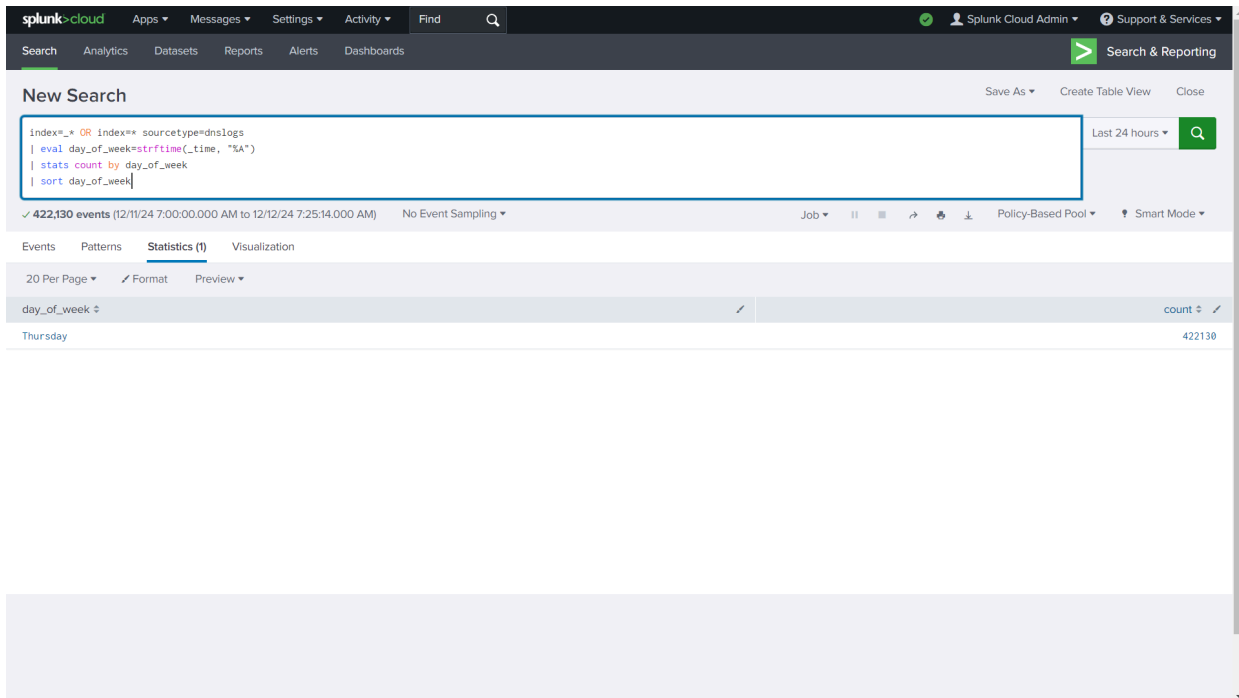
## 9. Query 9: `index=*_* OR index=* sourcetype=dnslogs | stats count by domain_name, dst_ip`

- **Description:** This query counts occurrences by domain name and destination IP.
- **Findings:**
  - Determine if any unusual destination IPs are associated with specific domains.
  - Flag any traffic anomalies between domain names and IP addresses.

---

## 10. Query 10: `index=*_* OR index=* sourcetype=dnstlogs | stats count by src_ip, dst_ip`

- **Description:** This query counts the occurrences of communication between source and destination IPs.
- **Findings:**
  - Provide a summary of communication patterns.
  - Identify any suspicious or unexpected IP pairs communicating frequently.



The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with 'splunk>cloud' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below this is a 'Search & Reporting' section. The main area is titled 'New Search' and contains a search bar with the following query:

```
index=*_* OR index=* sourcetype=dnstlogs
| eval day_of_week=strftime(_time, "%A")
| stats count by day_of_week
| sort day_of_week
```

Below the search bar, it shows '422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:25:14.000 AM)' and 'No Event Sampling'. The results are displayed in a table with the following columns: 'day\_of\_week' and 'count'. The table shows one row for 'Thursday' with a count of 422130.

day_of_week	count
Thursday	422130

---

## 11. Query 11: `index=*_* OR index=* sourcetype=dnstlogs | stats count by src_ip, dst_port`

- **Description:** This query counts the occurrences of source IPs and destination ports.
- **Findings:**
  - Summarize which source IPs are accessing specific destination ports.

- Flag any suspicious port access patterns.

New Search Save As Create Table View Close

index=\*\_ OR index=\* sourcetype=dnslogs  
 | stats count by domain\_name  
 | where count > 100  
 | sort -count

✓ 422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:26:00.000 AM) No Event Sampling

Events Patterns **Statistics (204)** Visualization

20 Per Page Format Preview < Prev 1 2 3 4 5 6 7 8 ... Next >

domain_name ↕	count ↕
teredo.ipv6.microsoft.com	20427
tools.google.com	7662
time.apple.com	5874
www.apple.com	5287
safebrowsing.clients.google.com	4638
WPAD	4161
stats.norton.com	3175
44.206.168.192.in-addr.arpa	2948
HPESAA67	2823
www.google.com	2764
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	2689
ISATAP	2604
ratings-wrs.symantec.com	2481
imap.gmail.com	2300
WORKGROUP	2065
api.twitter.com	1812
stats.qalabs.symantec.com	1690

## 12. Query 12: index=\*\_ OR index=\* sourcetype=dnslogs | stats count by dst\_ip, dst\_port

- **Description:** This query counts the occurrences of destination IPs and ports.
- **Findings:**
  - Provide the distribution of destination IPs and their corresponding ports.
  - Identify any unexpected or suspicious port access on specific destination IPs.

## 13. Query 13: index=\*\_ OR index=\* sourcetype=dnslogs | stats count by domain\_name, src\_port

- **Description:** This query counts occurrences of domain names and source ports.
- **Findings:**
  - Summarize which source ports are querying specific domains.
  - Analyze if any ports are disproportionately querying a particular domain, potentially pointing to malicious behavior.

## 14. Query 14: `index=_* OR index=* sourcetype=dnslogs | stats count by timestamp, src_ip`

- **Description:** This query counts DNS log entries by timestamp and source IP, useful for analyzing time-based patterns in the data.
- **Findings:**
  - Identify periods of high activity and correlate with specific source IPs.
  - Flag any irregular or suspicious spikes in traffic from particular source IPs.

New Search Save As Create Table View Close

```
index=_* OR index=* sourcetype=dnslogs
| stats first(_time) as first_query_time by domain_name
| where first_query_time > relative_time(now(), "-100d")
| sort -first_query_time
```

✓ 422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:27:04.000 AM) No Event Sampling

Events Patterns **Statistics (4,410)** Visualization

20 Per Page Format Preview < Prev 1 2 3 4 5 6 7 8 ... Next >

domain_name	first_query_time
(empty)	1733980079
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	1733980079
1.1.168.192.in-addr.arpa	1733980079
1.202.168.192.in-addr.arpa	1733980079
1.95.168.192.in-addr.arpa	1733980079
103.28.168.192.in-addr.arpa	1733980079
106.202.168.192.in-addr.arpa	1733980079
152.28.168.192.in-addr.arpa	1733980079
192.168.21.25 192.168.22.25 192.168.23.25	1733980079
192.168.25.152/webdav	1733980079
192.168.26.1152	1733980079
2.40.168.192.in-addr.arpa	1733980079
204.71.135.2	1733980079
253.23.168.192.in-addr.arpa	1733980079
253.24.168.192.in-addr.arpa	1733980079
253.25.168.192.in-addr.arpa	1733980079
253.27.168.192.in-addr.arpa	1733980079
44.206.168.192.in-addr.arpa	1733980079

## 15. Query 15: `index=_* OR index=* sourcetype=dnslogs | stats count by timestamp, dst_ip`

- **Description:** This query counts DNS log entries by timestamp and destination IP, useful for identifying unusual patterns over time.
- **Findings:**
  - Provide an analysis of traffic spikes based on timestamps and destination IP addresses.
  - Identify any periods where certain destination IPs experience anomalous traffic.



The screenshot displays the Splunk Cloud interface. At the top, there's a navigation bar with 'splunk>cloud' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search bar contains the query: `index=*_* OR index=* sourcetype=dnslogs | eval hour_of_day=strftime(_time, \"%H\") | stats count by hour_of_day | sort hour_of_day`. The results show 422,130 events from 12/11/24 7:00:00.000 AM to 12/12/24 7:27:39.000 AM. The 'Statistics (1)' tab is selected, showing a table with two columns: 'hour\_of\_day' and 'count'. The first row shows '05' and '422130'.

hour_of_day	count
05	422130

## 16. Query 16: `index=*_* OR index=* sourcetype=dnslogs | stats count by timestamp, domain_name`

- **Description:** This query counts DNS log entries by timestamp and domain name, helping to identify patterns or trends in domain access over time.
- **Findings:**
  - Provide insights into domain name access over time.
  - Highlight any unusual spikes in activity related to specific domain names.

New Search

Save As

Create Table View

Close

Last 24 hours

Q

index=\*\_ OR index=\* sourcetype=dnstlogs

| stats count by src\_ip

| where count > 500

| sort -count

422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:28:13.000 AM)

No Event Sampling

Job

Policy-Based Pool

Smart Mode

Events

Patterns

Statistics (72)

Visualization

20 Per Page

Format

Preview

< Prev

1

2

3

4

Next >

src_ip	count
10.10.117.210	75943
192.168.202.93	25935
192.168.202.103	17872
192.168.202.76	16668
192.168.202.97	15935
192.168.202.141	14891
10.10.117.209	14222
192.168.202.110	13368
192.168.203.63	11968
192.168.202.83	10477
192.168.202.79	10459
192.168.202.106	10449
192.168.229.252	9530
192.168.202.84	8071
192.168.202.102	7483
192.168.202.71	7245
192.168.202.75	6718
192.168.202.85	5147

## 17. Query 17: index=\*\_ OR index=\* sourcetype=dnstlogs | stats count by timestamp, src\_ip, dst\_ip

- **Description:** This query counts DNS log entries by timestamp, source IP, and destination IP.
- **Findings:**
  - Provide a detailed analysis of the communication between specific source and destination IP pairs over time.
  - Identify any unusual communication patterns or spikes.

## 18. Query 18: index=\*\_ OR index=\* sourcetype=dnstlogs | stats count by domain\_name, src\_ip, dst\_ip

- **Description:** This query counts DNS log entries by domain name, source IP, and destination IP.
- **Findings:**
  - Analyze traffic patterns by combining domain, source IP, and destination IP.
  - Flag any unusual or potentially malicious patterns that could indicate an attack.

The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with 'splunk-cloud' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search query is entered in a text box: `index=_* OR index=* sourcetype=dnslogs | search domain_name="example.com" | stats count by src_ip`. Below the query box, it shows '25 events (12/11/24 7:00:00.000 AM to 12/12/24 7:29:01.000 AM)' and 'No Event Sampling'. The results are displayed in a table with columns 'src\_ip' and 'count'. The table shows five rows of data.

src_ip	count
192.168.202.110	16
192.168.202.112	6
192.168.202.138	1
192.168.21.25	1
192.168.28.25	1

## 19. Query 19: `index=_* OR index=* sourcetype=dnslogs | stats count by domain_name, timestamp`

- **Description:** This query counts DNS log entries by domain name and timestamp, helping to analyze domain access patterns over time.
- **Findings:**
  - Provide insights into when specific domains are queried most frequently.
  - Identify unusual spikes in queries related to specific domains.



New Search

Save AsCreate Table ViewClose

index=,\* OR index=\* sourcetype=dnstlogs  
| stats avg(query\_duration) as avg\_duration by domain\_name  
| sort -avg\_duration

Last 24 hours

✓ 422,130 events (12/11/24 7:00:00.000 AM to 12/12/24 7:30:13.000 AM)No Event SamplingJobPauseRefreshDownloadPolicy-Based PoolSmart Mode

EventsPatternsStatistics (4,410)Visualization

20 Per PageFormatPreview

< Prev12345678...Next >

domain\_name

avg\_duration

(empty)

\*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00

+s4yj3z+ahnzaa.=connect.rssfeeds.com

+s6fgaabadrmbdcwnzbqzcxdzgouy4nenbnje4mdgxmtgwmqxnku@mf0q0e.=auth.rssfeeds.com

-

-p

../nessus

0-jf-w.channel.facebook.com

0.0.0.0.in-addr.arpa

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

0.21.168.192.in-addr.arpa

0.22.168.192.in-addr.arpa

0.229.168.192.in-addr.arpa

0.23.168.192.in-addr.arpa

0.24.168.192.in-addr.arpa

0.25.168.192.in-addr.arpa

0.26.168.192.in-addr.arpa

0.27.168.192.in-addr.arpa

0.28.168.192.in-addr.arpa