SPLUNK - TUTORIAL

This is the basic level tutorial to use Splunk (SIEM tool). To this is a basic-level tutorial on using Splunk (a SIEM tool). Here we analysing sample data of :

- DNS log data for this analysis.

DNS LOG ANALYSES:

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:

1) Running Splunk in localhost after downloading from web.
2) Import sample log data to Splunk by :
    - Settings -> Add data.

Verify Uploading data:

Cmd : **index=<your_dns_index> sourcetype=<your_dns_sourcetype>**

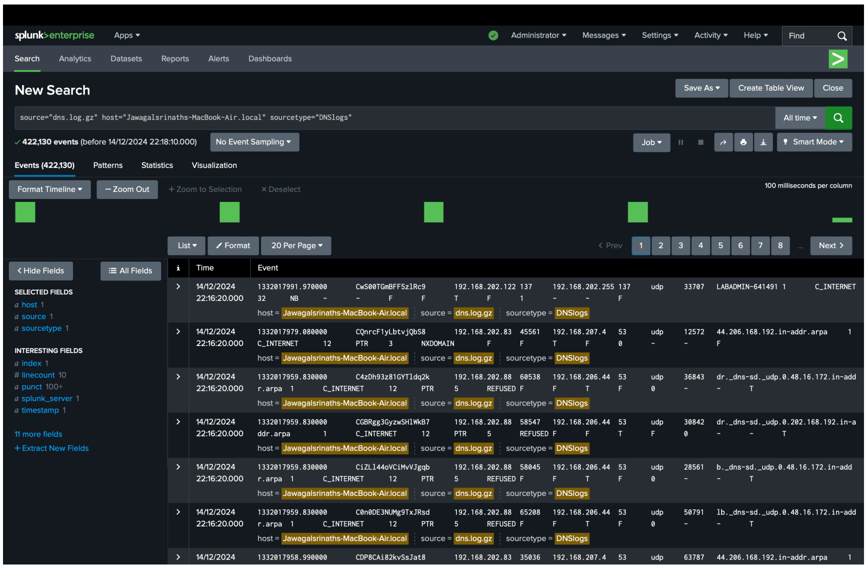
Now lets see how to use Splunk to use data to find valuable insights:

STEPS TO ANALYSE DATA WITH SPLUNK:

1.Searching for DNS events:

- Open Splunk and navigate to search tab.
- Type this command to retrieve data

Cmd : **index=* sourcetype=dns_sample**



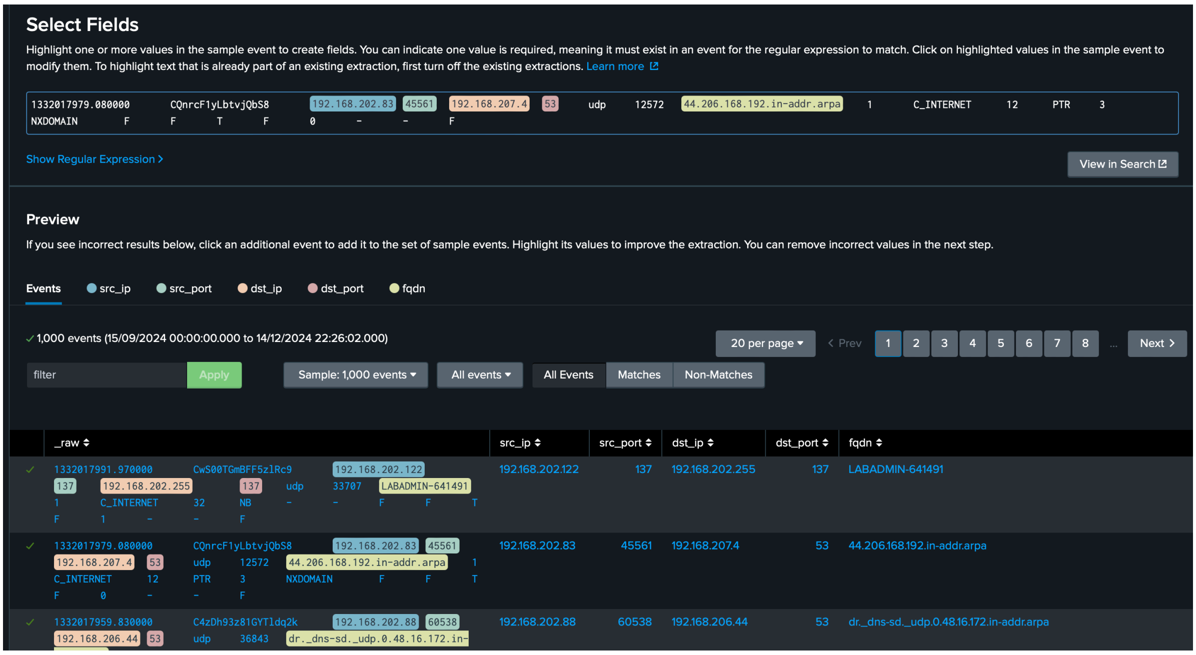
```
source="dns.log.gz" host="Jawagalsrinaths-MacBook-Air.local" sourcetype="DNSlogs"
```

✓ 422,130 events (before 14/12/2024 22:18:10.000)

```
i  Time          Event
>  14/12/2024    1332017991.970000       CwS00TGmBFF5zlRc9       192.168.202.122 137     192.168.202.255 137     udp     33707   LABADMIN-641491 1       C_INTERNET
   22:16:20.000  32      NB      -       -       F       F       T       F       1       -       -       F
                 host = Jawagalsrinaths-MacBook-Air.local | source = dns.log.gz | sourcetype = DNSlogs
>  14/12/2024    1332017979.080000       CQnrcF1yLbtvjQbS8       192.168.202.83  45561   192.168.207.4   53      udp     12572   44.206.168.192.in-addr.arpa     1
   22:16:20.000  C_INTERNET      12      PTR     3       NXDOMAIN        F       F       T       F       0       -       -       F
                 host = Jawagalsrinaths-MacBook-Air.local | source = dns.log.gz | sourcetype = DNSlogs
>  14/12/2024    1332017959.830000       C4zDh93z81GYTldq2k      192.168.202.88  60538   192.168.206.44  53      udp     36843   dr._dns-sd._udp.0.48.16.172.in-add
   22:16:20.000  r.arpa  1       C_INTERNET      12      PTR     5       REFUSED F       F       T       F       0       -       -       T
                 host = Jawagalsrinaths-MacBook-Air.local | source = dns.log.gz | sourcetype = DNSlogs
>  14/12/2024    1332017959.830000       CGBRgg3GyzwSHlWkB7      192.168.202.88  58547   192.168.206.44  53      udp     30842   dr._dns-sd._udp.0.202.168.192.in-a
   22:16:20.000  ddr.arpa        1       C_INTERNET      12      PTR     5       REFUSED F       F       T       F       0       -       -       T
                 host = Jawagalsrinaths-MacBook-Air.local | source = dns.log.gz | sourcetype = DNSlogs
>  14/12/2024    1332017959.830000       CiZLl44oVCiMvVJgqb      192.168.202.88  58045   192.168.206.44  53      udp     28561   b._dns-sd._udp.0.48.16.172.in-add
   22:16:20.000  r.arpa  1       C_INTERNET      12      PTR     5       REFUSED F       F       T       F       0       -       -       T
                 host = Jawagalsrinaths-MacBook-Air.local | source = dns.log.gz | sourcetype = DNSlogs
>  14/12/2024    1332017959.830000       C0n0DE3NUMg9TxJRsd      192.168.202.88  65208   192.168.206.44  53      udp     50791   lb._dns-sd._udp.0.48.16.172.in-add
   22:16:20.000  r.arpa  1       C_INTERNET      12      PTR     5       REFUSED F       F       T       F       0       -       -       T
                 host = Jawagalsrinaths-MacBook-Air.local | source = dns.log.gz | sourcetype = DNSlogs
>  14/12/2024    1332017958.990000       CDP8CAi82kvSsJat8       192.168.202.83  35036   192.168.207.4   53      udp     63787   44.206.168.192.in-addr.arpa     1
```

2. Creating “INTERESTING FIELDS” for analysis:

- Click open “extract interesting fields”
- Click any of the log data
- Choose “regular expression” , now choose data form log and add them to interesting fields.
- Example fields : src_ip, src_port, dst_ip, dst_port and FQDN.



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

```
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
```

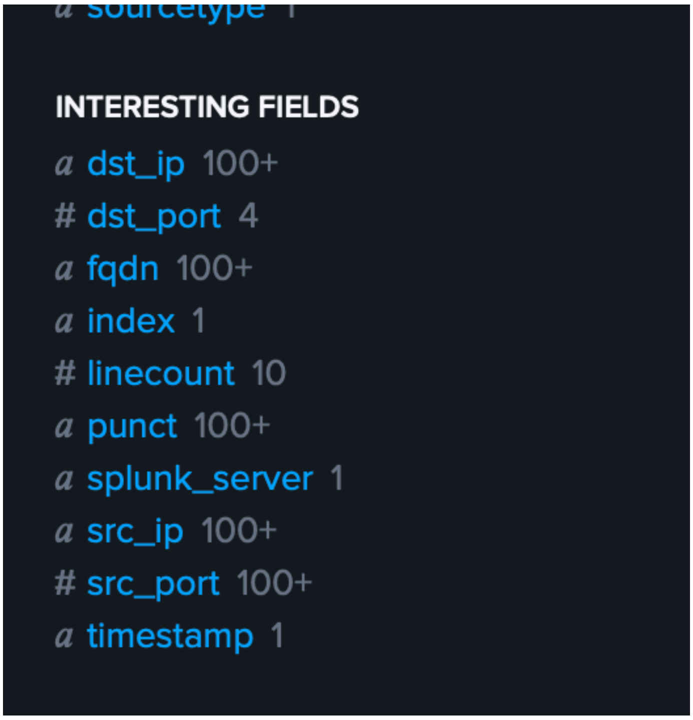
Preview

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 (15/09/2024 00:00:00.000 to 14/12/2024 22:26:02.000)

	_raw	src_ip	src_port	dst_ip	dst_port	fqdn
✓	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
✓	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-	192.168.202.88	60538	192.168.206.44	53	dr._dns-sd._udp.0.48.16.172.in-addr.arpa

- Now you can see them in the interesting fields

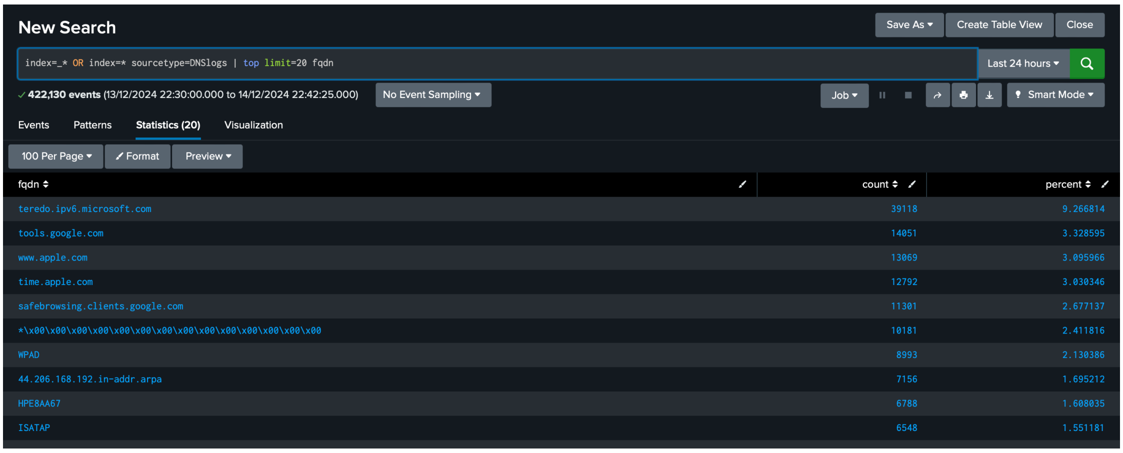


a sourcetype 1

INTERESTING FIELDS

a	dst_ip	100+
#	dst_port	4
a	fqdn	100+
a	index	1
#	linecount	10
a	punct	100+
a	splunk_server	1
a	src_ip	100+
#	src_port	100+
a	timestamp	1

3. Identify high demanded domains:
    - Using “top” and “limit” , we can retrieve the high traffic found domains
    - Cmd : **| top limit=20 fqdn**
    - pipe “|” , limit : to limit output to 20 entries.

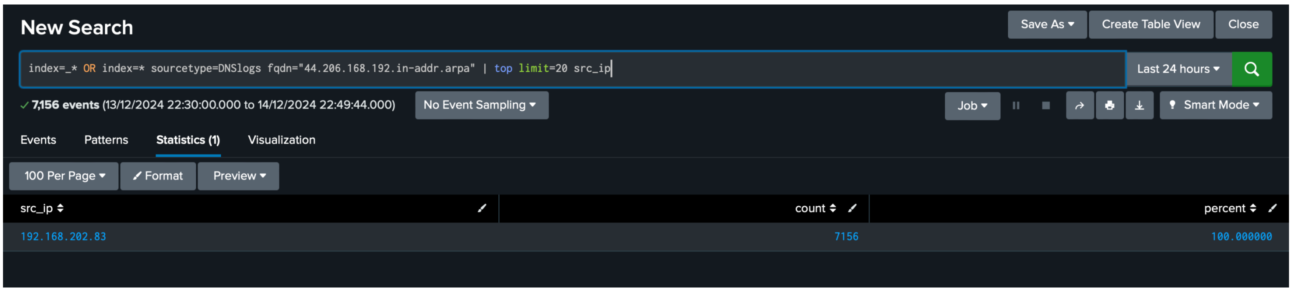


```
index=_* OR index=* sourcetype=DNSlogs | top limit=20 fqdn
```

✓ **422,130 events** (13/12/2024 22:30:00.000 to 14/12/2024 22:42:25.000)

fqdn	count	percent
teredo.ipv6.microsoft.com	39118	9.266814
tools.google.com	14051	3.328595
www.apple.com	13069	3.095966
time.apple.com	12792	3.030346
safebrowsing.clients.google.com	11301	2.677137
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	10181	2.411816
WPAD	8993	2.130386
44.206.168.192.in-addr.arpa	7156	1.695212
HPE8AA67	6788	1.608035
ISATAP	6548	1.551181

4. Identify domain’s frequent requesting “src_ip” :
    - Using “fqdn”, “top” and “Limit” , we can retrieve the frequent request sending src_ip.
    - Cmd : **fqdn="44.206.168.192.in-addr.arpa" | top limit=20 src_ip**

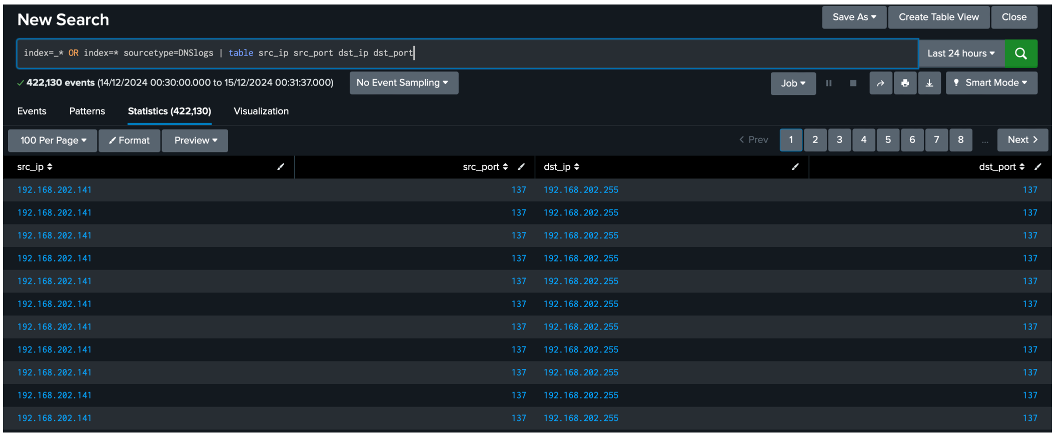


```
index=_* OR index=* sourcetype=DNSlogs fqdn="44.206.168.192.in-addr.arpa" | top limit=20 src_ip
```

✓ **7,156 events** (13/12/2024 22:30:00.000 to 14/12/2024 22:49:44.000)

src_ip	count	percent
192.168.202.83	7156	100.000000

5. To table required fields:
    - Using “table” , we can have the required fields as a table.
    - Cmd : **| table src_ip src_port dst_ip dst_port**



```
index=_* OR index=* sourcetype=DNSlogs | table src_ip src_port dst_ip dst_port
```

✓ **422,130 events** (14/12/2024 00:30:00.000 to 15/12/2024 00:31:37.000)

src_ip	src_port	dst_ip	dst_port
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137
192.168.202.141	137	192.168.202.255	137