

DNS Log Analysis Using Splunk

Analyzing sample DNS Log data using SIEM tool Splunk

DNS Log Ingestion

The screenshot shows the Splunk Search interface. The search bar contains the query: `source="dns.log.gz" host=NULL sourcetype=dnslogs`. The search results show 422,130 events. The interface includes a timeline view and a table of events. The table has columns for Time, Event, and various fields extracted from the DNS logs.

Time	Event
2/13/25 8:36:09.000 PM	1332017991.970000 C:\Internet 12 PTR 3 NODOMAIN 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa 1
2/13/25 8:36:09.000 PM	1332017959.830000 C:\Internet 12 PTR 5 REFUSED 192.168.206.44 53 udp 36843 dr.dns-sd._udp.0.48.16.172.in-addr.arpa 1
2/13/25 8:36:09.000 PM	1332017959.830000 C:\Internet 12 PTR 5 REFUSED 192.168.206.44 53 udp 36843 dr.dns-sd._udp.0.202.168.192.in-addr.arpa 1

Parsing the data by extracting new field

selecting a sample event for extracting new field

The screenshot shows the Splunk Extract Fields interface. The 'Select Sample Event' step is active. The source type is 'dnslogs' and the time range is 'Last 90 days'. The interface displays a table of events for selection.

Time	Event
2/13/25 8:36:09.000 PM	1332017991.970000 C:\Internet 12 PTR 3 NODOMAIN 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa 1
2/13/25 8:36:09.000 PM	1332017959.830000 C:\Internet 12 PTR 5 REFUSED 192.168.206.44 53 udp 36843 dr.dns-sd._udp.0.48.16.172.in-addr.arpa 1
2/13/25 8:36:09.000 PM	1332017959.830000 C:\Internet 12 PTR 5 REFUSED 192.168.206.44 53 udp 36843 dr.dns-sd._udp.0.202.168.192.in-addr.arpa 1

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 him to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

1332017979.080000	CQnrcFlyLbtvjQbS8	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									

Extract

Require

Field Name

src_ip

Sample Value

192.168.202.83

Add Extraction

modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

1332017979.080000	CQnrcFlyLbtvjQbS8	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					

Show Regular Expression >

View in Search

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.

Events src_ip

✓ 1,000 events (1/15/24 12:00:00.000 AM to 2/13/25 8:57:35.000 PM) 20 per page < Prev 1 2 3 4 5 6 7 8 ... Next >

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

_raw	src_ip
✓ 1332017991.970000 CWS00TGe0FF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADN-641491 1 C_INTERNET 32 NB - 192.168.202.122	192.168.202.122
✓ 1332017979.080000 CQnrcFlyLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp 12572 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 192.168.202.83	192.168.202.83
✓ 1332017959.830000 C42oH93z81GYT1d2k 192.168.202.88 68538 192.168.206.44 53 udp 36843 dr_dns-adj_udp.0.48.16.172.in-addr.arpa 1 192.168.202.88	192.168.202.88
✓ 1332017959.830000 C0BRgg30yzwSH1Mk87 192.168.202.88 58547 192.168.206.44 53 udp 38842 dr_dns-adj_udp.0.202.168.192.in-addr.arpa 1 192.168.202.88	192.168.202.88
✓ 1332017959.830000 C1ZL144oVC1HwVJgab 192.168.202.88 58045 192.168.206.44 53 udp 28561 b_dns-adj_udp.0.48.16.172.in-addr.arpa 1 C_INTERNET 192.168.202.88	192.168.202.88

Selecting 45561 as source port src_port

splunk>enterprise Apps Administrator Messages Settings

Extract Fields Select Sample Select Method Select Fields Validate Save < Back Next >

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 him to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

1332017979.080000	CQnrcFlyLbtvjQbS8	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					

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 remove incorrect values in the next step.

Events src_ip

Extract

Require

Field Name

src_port

Sample Value

45561

Add Extraction

Selecting 192.168.207.4 as destination ip dst_ip

The screenshot shows the Splunk 'Extract Fields' interface. At the top, a progress bar indicates the steps: Select Sample, Select Method, Select Fields (current), Validate, and Save. The 'Select Fields' section displays a sample event with various fields highlighted. A modal dialog is open, showing the 'Field Name' as 'dst_ip' and the 'Sample Value' as '192.168.207.4'. The 'Add Extraction' button is visible. Below the sample event, there is a 'Preview' section and a list of events. The bottom of the interface shows a filter bar with an 'Apply' button and a sample size of 1,000 events.

splunk>enterprise Apps Administrator

Extract Fields

Select Sample Select Method Select Fields Validate Save < Back

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. 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.8
NXDOMAIN F F T F 0 -

Show Regular Expression >

Preview

If you see incorrect results below, click an additional event to add it to the set of samples to improve the extraction. You can remove incorrect extractions.

Events src_ip src_port

✓ 1,000 events (11/15/24 12:00:00.000 AM to 2/13/25 8:59:02.000 PM) 20 per page

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

And 53 the dns server port

The screenshot shows the Splunk 'Extract Fields' interface. At the top, a progress bar indicates the steps: Select Sample, Select Method, Select Fields (current), Validate, and Save. The 'Select Fields' section displays a sample event with various fields highlighted. A modal dialog is open, showing the 'Field Name' as 'dst_port' and the 'Sample Value' as '53'. The 'Add Extraction' button is visible. Below the sample event, there is a 'Preview' section and a list of events. The bottom of the interface shows a filter bar with an 'Apply' button and a sample size of 1,000 events.

Select Sample Select Method Select Fields Validate Save

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. 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
NXDOMAIN F F T F 0 - -

Show Regular Expression >

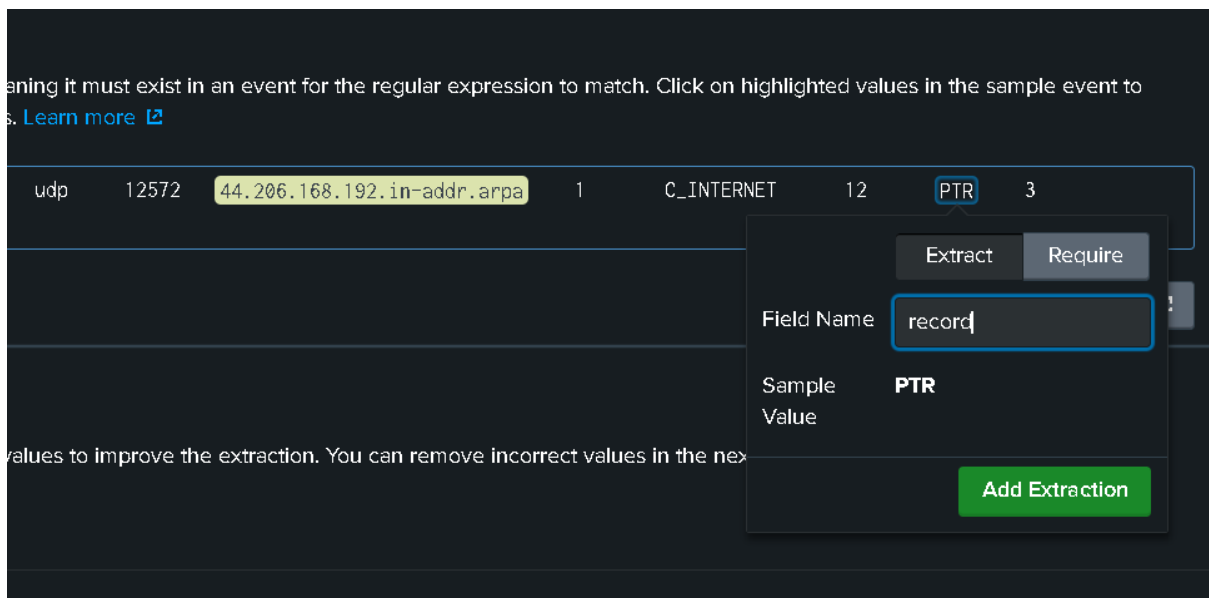
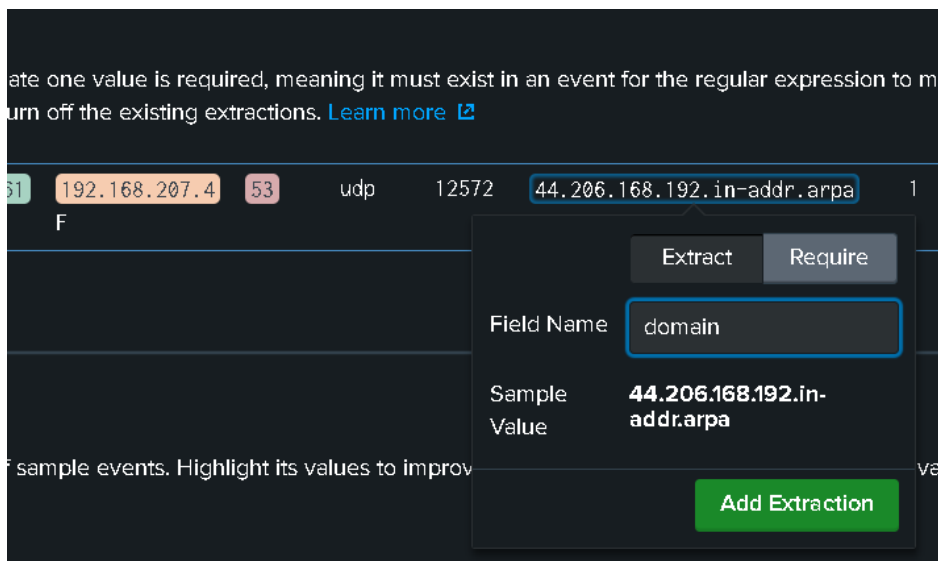
Preview

If you see incorrect results below, click an additional event to add it to the set of samples to improve the extraction. You can remove incorrect extractions.

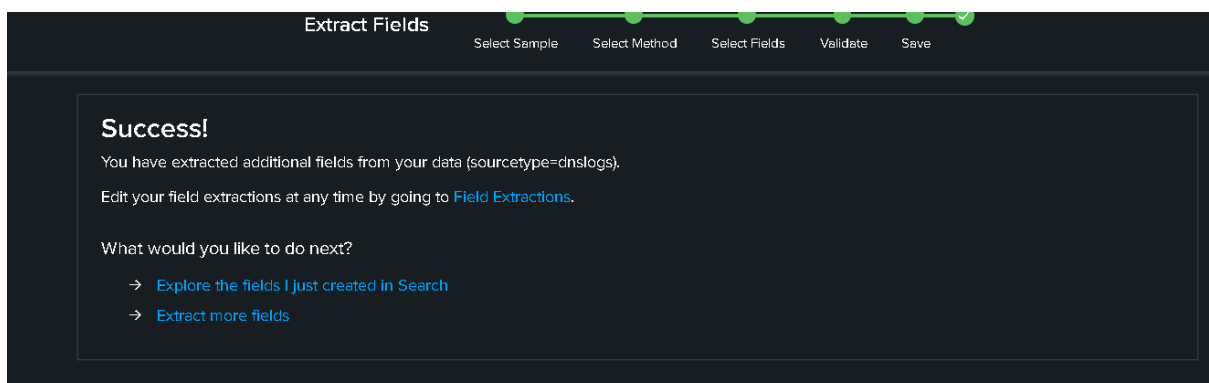
Events src_ip src_port dst_ip

✓ 1,000 events (11/15/24 12:00:00.000 AM to 2/13/25 9:01:12.000 PM) 20 per page < Prev

44.206.168.192.in-addr.arpa is the domain name



PTR - Type of record



Successfully extracted the field from log

The extracted field lists are now on the interesting fields list

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a domain 100+

a dst_ip 100+

dst_port 4

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

Format

Show: 20 Per Page

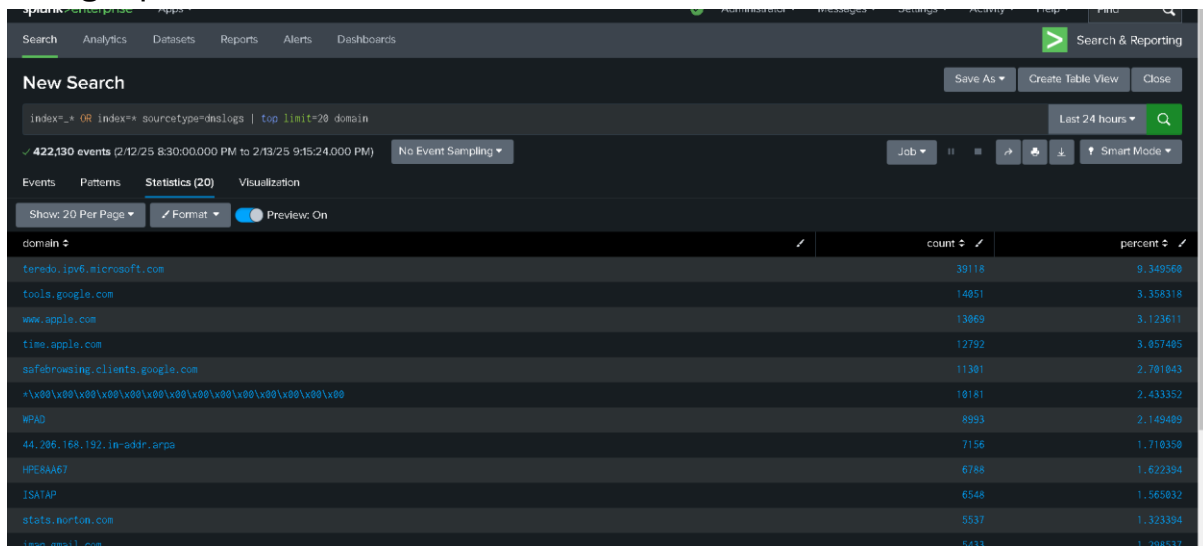
View: List

i	Time	Event
>	2/13/25 8:36:09.000 PM	1332017991.970000 CwS007 32 NB - - host = NULL source = dns.log.g
>	2/13/25 8:36:09.000 PM	1332017979.080000 CQnrcF C_INTERNET 12 PTR host = NULL source = dns.log.g
>	2/13/25 8:36:09.000 PM	1332017959.830000 C4zDh9 r.arpa 1 C_INTERNET host = NULL source = dns.log.g
>	2/13/25 8:36:09.000 PM	1332017959.830000 CGBRgg ddr.arpa 1 C_INTE host = NULL source = dns.log.g
>	2/13/25 8:36:09.000 PM	1332017959.830000 CiZL14 r.arpa 1 C_INTERNET host = NULL source = dns.log.g
>	2/13/25	1332017959.830000 C0n0D5

Stats count by domain name

New Search		Save As ▾	Create Table View	Close
index=* OR index=* sourcetype=dnslogs stats count by domain		Last 24 hours 🔍		
✓ 422,130 events (2/12/25 8:30:00.000 PM to 2/13/25 9:12:36.000 PM)		No Event Sampling ▾	Job ▾	Smart Mode ▾
Events	Patterns	Statistics (5,125)	Visualization	
Show: 20 Per Page ▾	Format ▾	Preview: On	< Prev 1 2 3 4 5 6 7 8 ... Next >	
domain				count
(empty)				2719
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00				10181
rsdyj3zrahzaw.*connect.rsafeeds.com				2
rs6fgasbdrbwczwbzbxrdzgouy4nenbnje4mgxntgwedgxuku@0fd90e.*auth.rsafeeds.com				2
-1				10
-p				8
.../messus				28
0-jf-w.channel.facebook.com				1289
0.0.0.0.in-addr.arpa				12
0.2.2.0.f.d.2.b.b.7.4.7.3.8.8.2.0.2.0.8.1.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

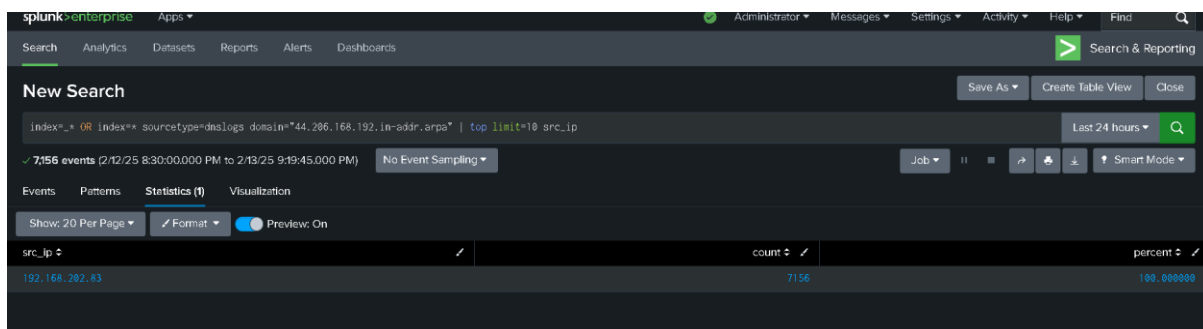
Using top filter



The screenshot shows the Splunk Search interface. The search bar contains the query: `index=* OR index=* sourcetype=dnslogs | top limit=20 domain`. The results show 422,130 events. The 'Statistics (20)' tab is selected, displaying a table of the top 20 domains by count.

domain	count	percent
teredo.ipv6.microsoft.com	39118	9.349568
tools.google.com	14851	3.358318
www.apple.com	13869	3.123611
time.apple.com	12792	3.057405
safebrowsing.clients.google.com	11301	2.701043
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	10181	2.433352
WPAD	8993	2.149489
44.206.168.192.in-addr.arpa	7156	1.710358
HPERAA67	6788	1.622394
ISATAP	6548	1.565832
stats.morton.com	5537	1.323384
www.casill.com	5433	1.296537

Now checking which source ip has requested more on specific domains

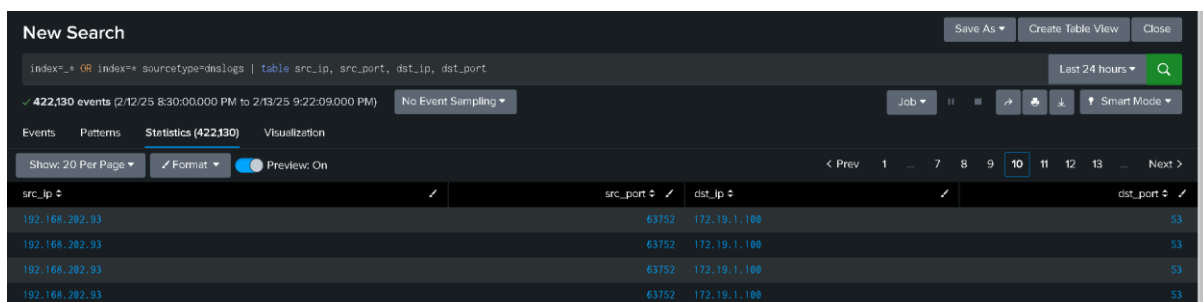


The screenshot shows the Splunk Search interface. The search bar contains the query: `index=* OR index=* sourcetype=dnslogs domain="44.206.168.192.in-addr.arpa" | top limit=10 src_ip`. The results show 7,156 events. The 'Statistics (1)' tab is selected, displaying a table of the top 10 source IPs by count.

src_ip	count	percent
192.168.202.83	7156	100.000000

From this we can suspect that 192.168.202.83 as the compromised machine

Table view of source ip, destination ip and ports



The screenshot shows the Splunk Search interface. The search bar contains the query: `index=* OR index=* sourcetype=dnslogs | table src_ip, src_port, dst_ip, dst_port`. The results show 422,130 events. The 'Table' view is selected, displaying a table of source IP, source port, destination IP, and destination port.

src_ip	src_port	dst_ip	dst_port
192.168.202.93	63752	172.19.1.100	53
192.168.202.93	63752	172.19.1.100	53
192.168.202.93	63752	172.19.1.100	53
192.168.202.93	63752	172.19.1.100	53