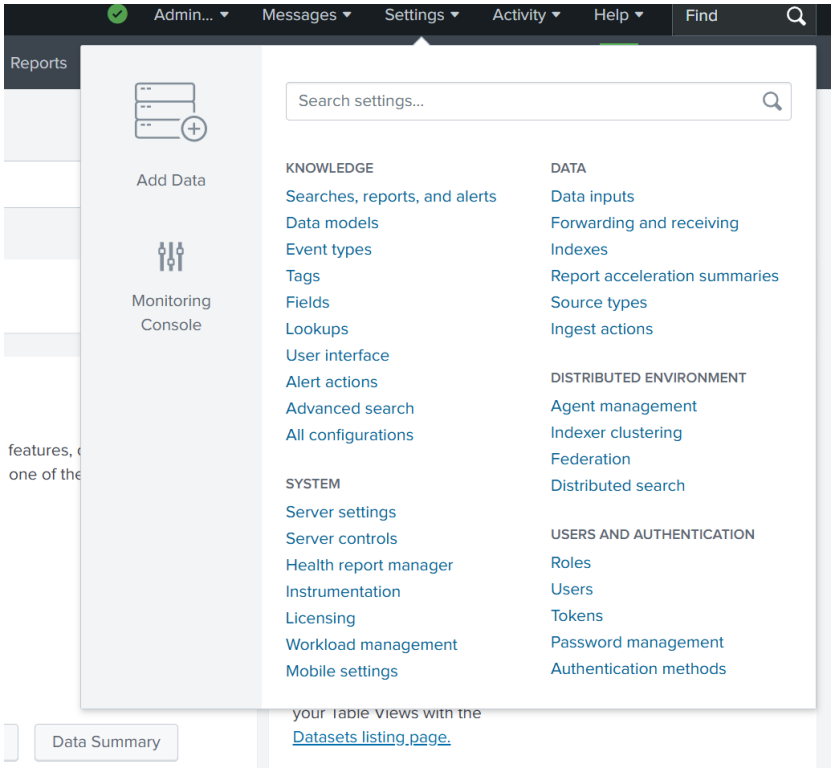
Introduction:

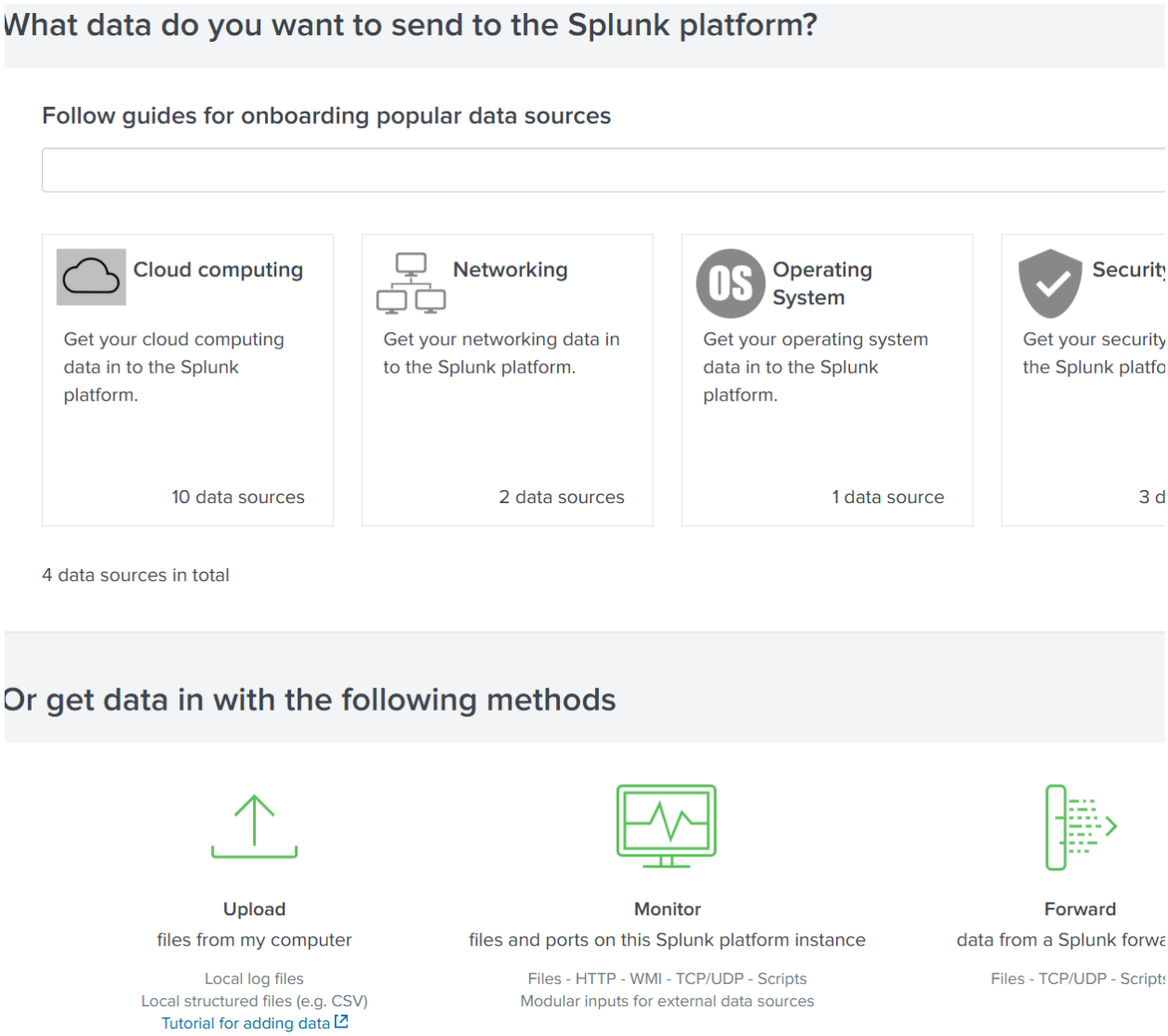
DNS logs play an important role in tracking how a network is being used and in spotting possible security risks. With the help of Splunk SIEM, these logs can be analyzed to identify unusual patterns, detect signs of cyberattacks, and improve overall visibility into network activity.Project Overview

In this project, I analyzed sample DNS logs using Splunk and created queries to extract important fields such as source IP, destination IP, and domain names. By studying the query patterns, I was able to identify unusual domains that might suggest network misconfigurations or tunneling activity. This hands-on work helped me strengthen my skills in SIEM log analysis, field extraction using regex, and detecting anomalies in a practical cybersecurity setting.

Steps to Upload Sample DNS Log Files to Splunk SIEM

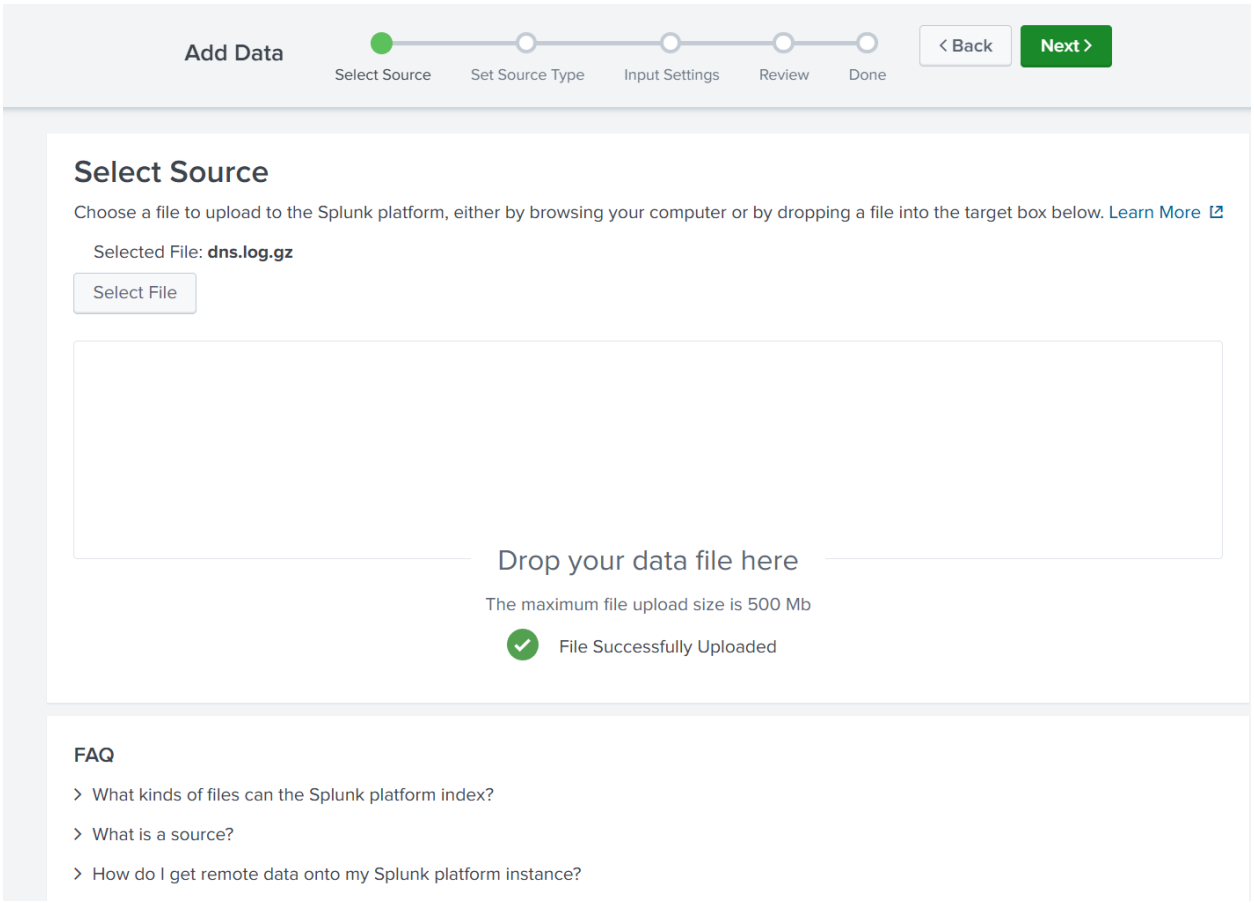
1. **Data Preparation**
   Create or collect a sample DNS log file and ensure it includes relevant DNS event records
2. **Importing**
3. **Data into Splunk**
   - **In Splunk, go to Settings → Add Data → Upload, and upload the prepared DNS log file**





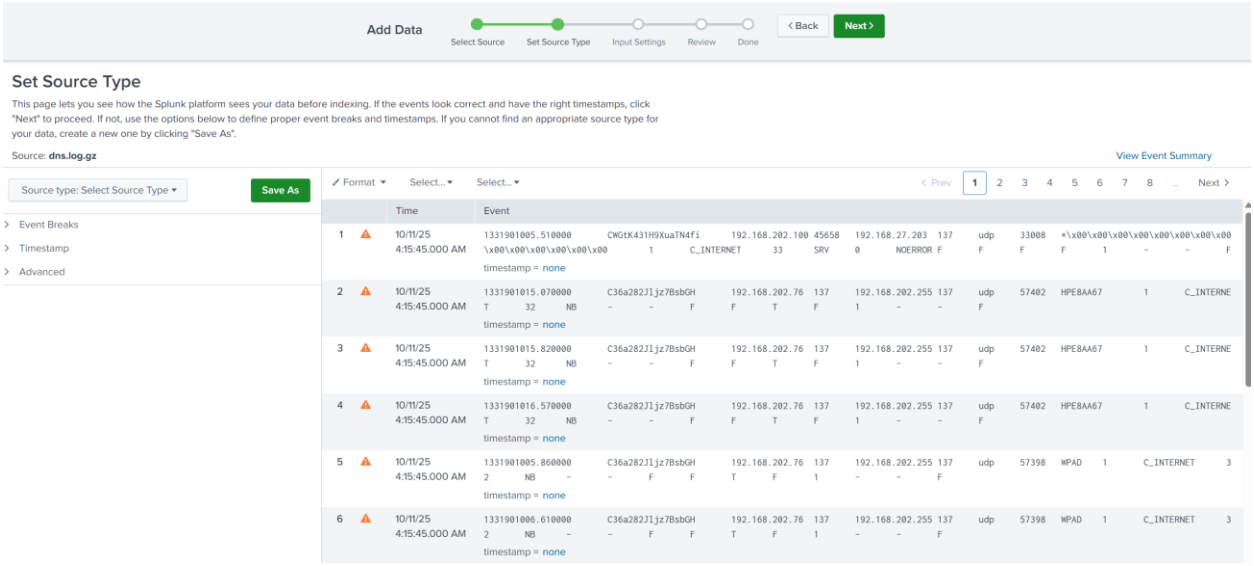
4. **Select File**

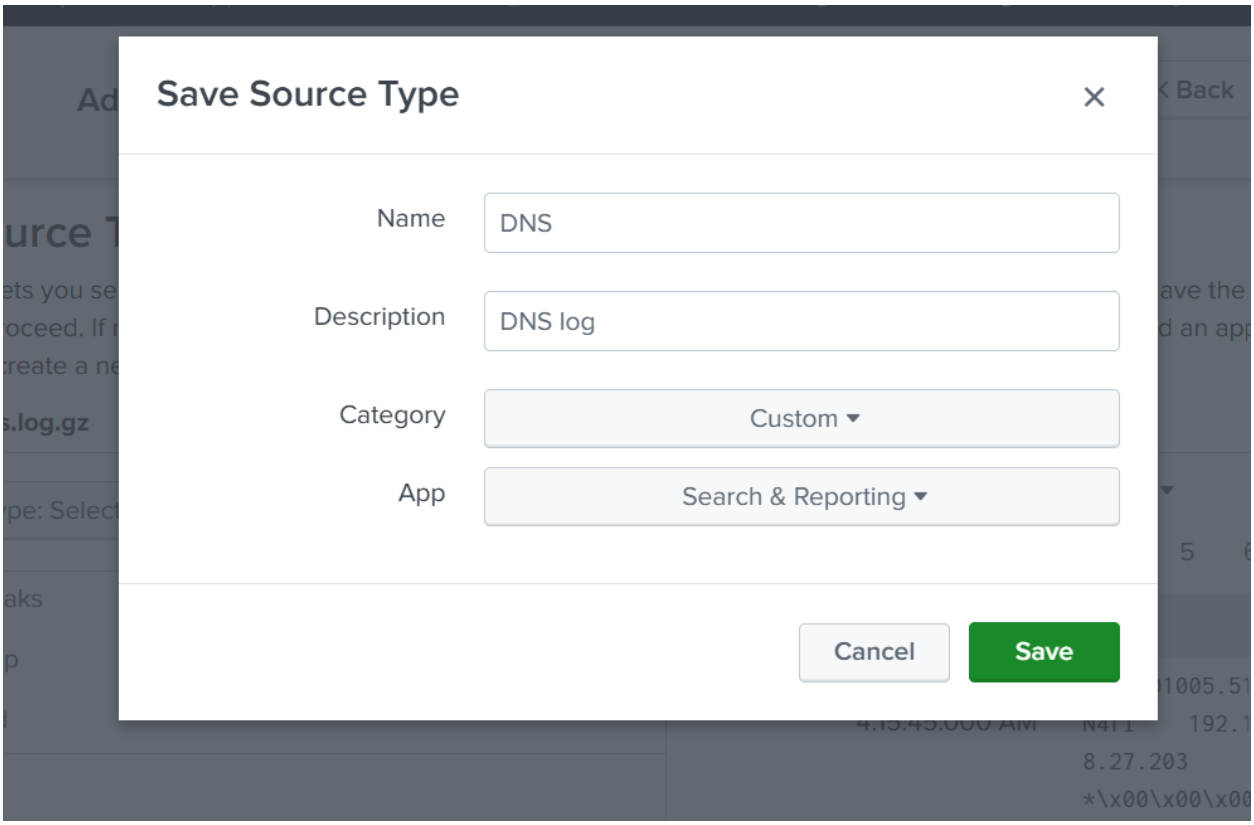
- Choose your DNS log file or drag and drop it into the upload box.



5. **Set Source Type**

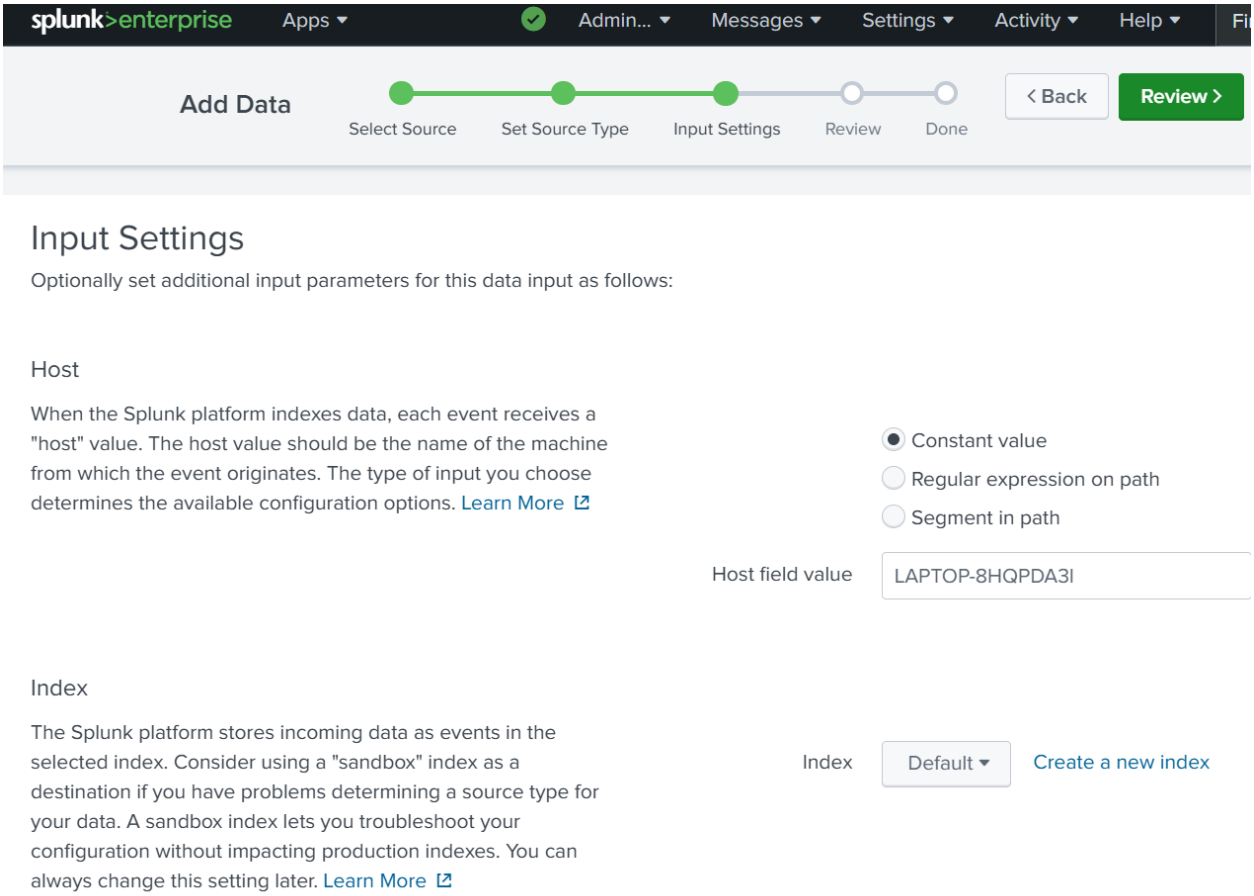
- Once the DNS log is uploaded, click **Save As** and provide a meaningful name and description for easy identification





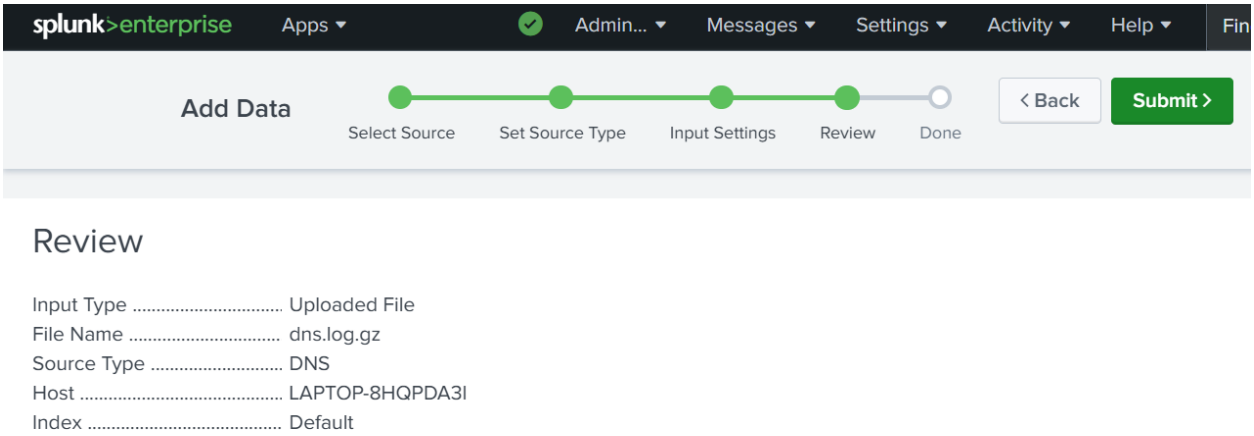
6. **Review Settings**

- Double-check important configurations such as **Host** and **Index** to ensure they are correctly set



7. **Submit and Upload Data**

- Do a final review of all settings, then click **Submit** to complete the data upload process into Splunk.



To confirm that your file has been uploaded successfully, run the following query:
`index=* sourcetype=<your_sourcetype>`

4. Parsing Data

On the left side, you'll see a table displaying your log data. In my case, I modified the fields to include additional details such as **dest_ip** and **dest_port**.
You can do this by selecting **Extract New Fields** in Splunk to define and extract new custom fields from your logs.

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a dest_ip 100+
dest_port 4
a full_qualify_domain_name 100+
a index 1
linecount 10
a punct 100+
a query_id 100+
a record 12
a splunk_server 1
a src_ip 100+
src_port 100+
a timestamp 1

11 more fields

+ Extract New Fields

- I intend to add additional field as shown below, so we will add Query ID, Source IP, Source Port, Destination IP, Destination Port, Full Quality Domain Name and Record.

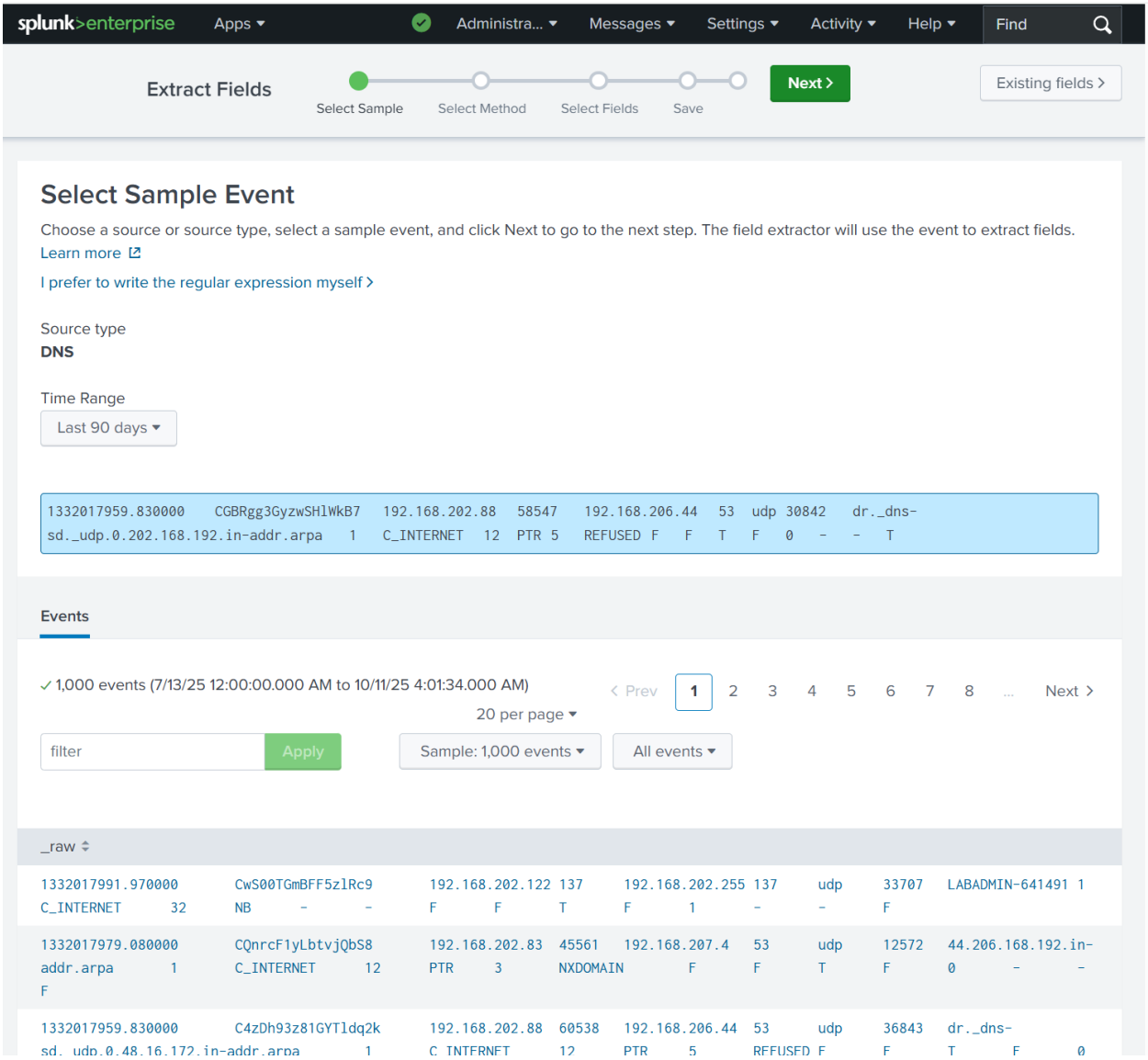
Fields

Source type: **DNS**

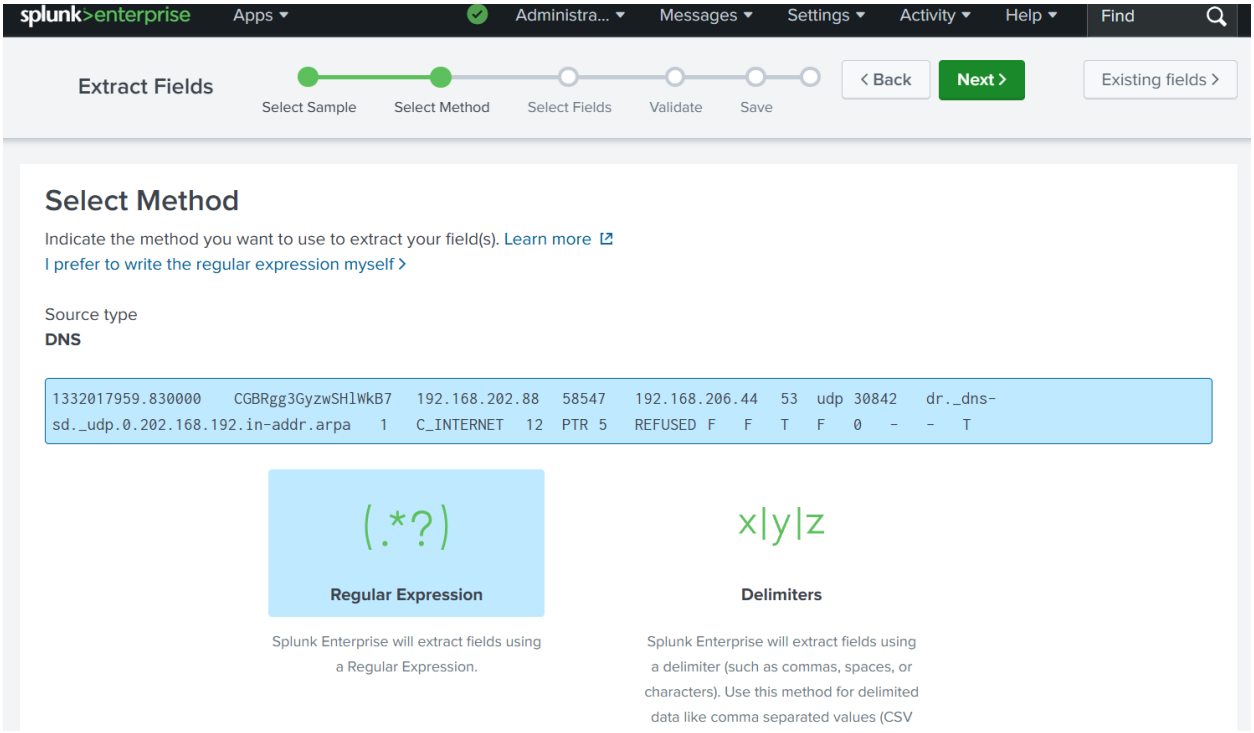
The field extractions below have been previously defined for this source type. For a complete list of field objects, please see the Fields page.

Field Name	Pattern Name
query_id	EXTRACT-query_id,src_ip,src_port,dest_ip
src_ip	EXTRACT-query_id,src_ip,src_port,dest_ip
src_port	EXTRACT-query_id,src_ip,src_port,dest_ip
dest_ip	EXTRACT-query_id,src_ip,src_port,dest_ip
dest_port	EXTRACT-query_id,src_ip,src_port,dest_ip
full_qualify_domain_name	EXTRACT-query_id,src_ip,src_port,dest_ip
record	EXTRACT-query_id,src_ip,src_port,dest_ip

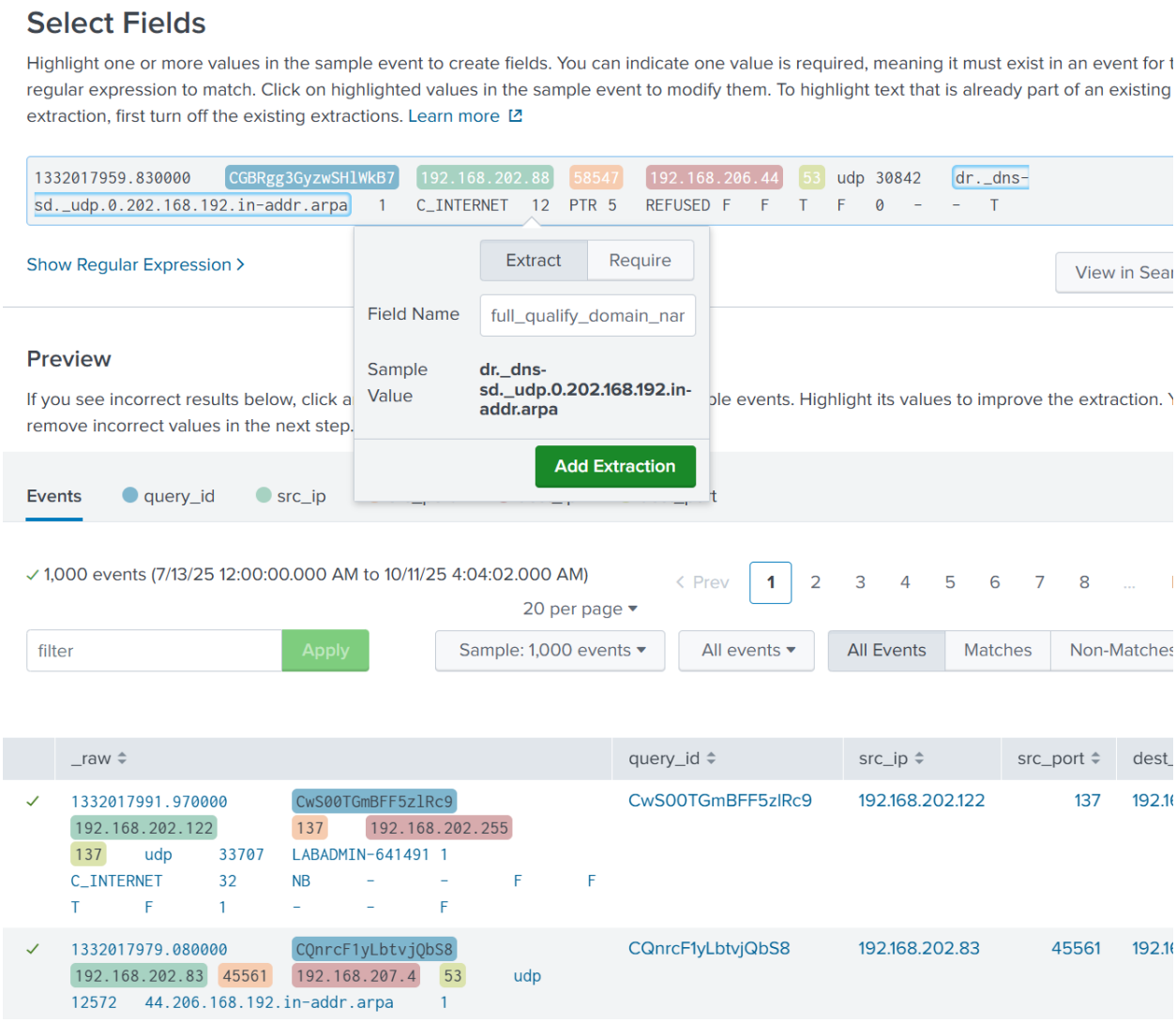
- From the event below, select any event and click next



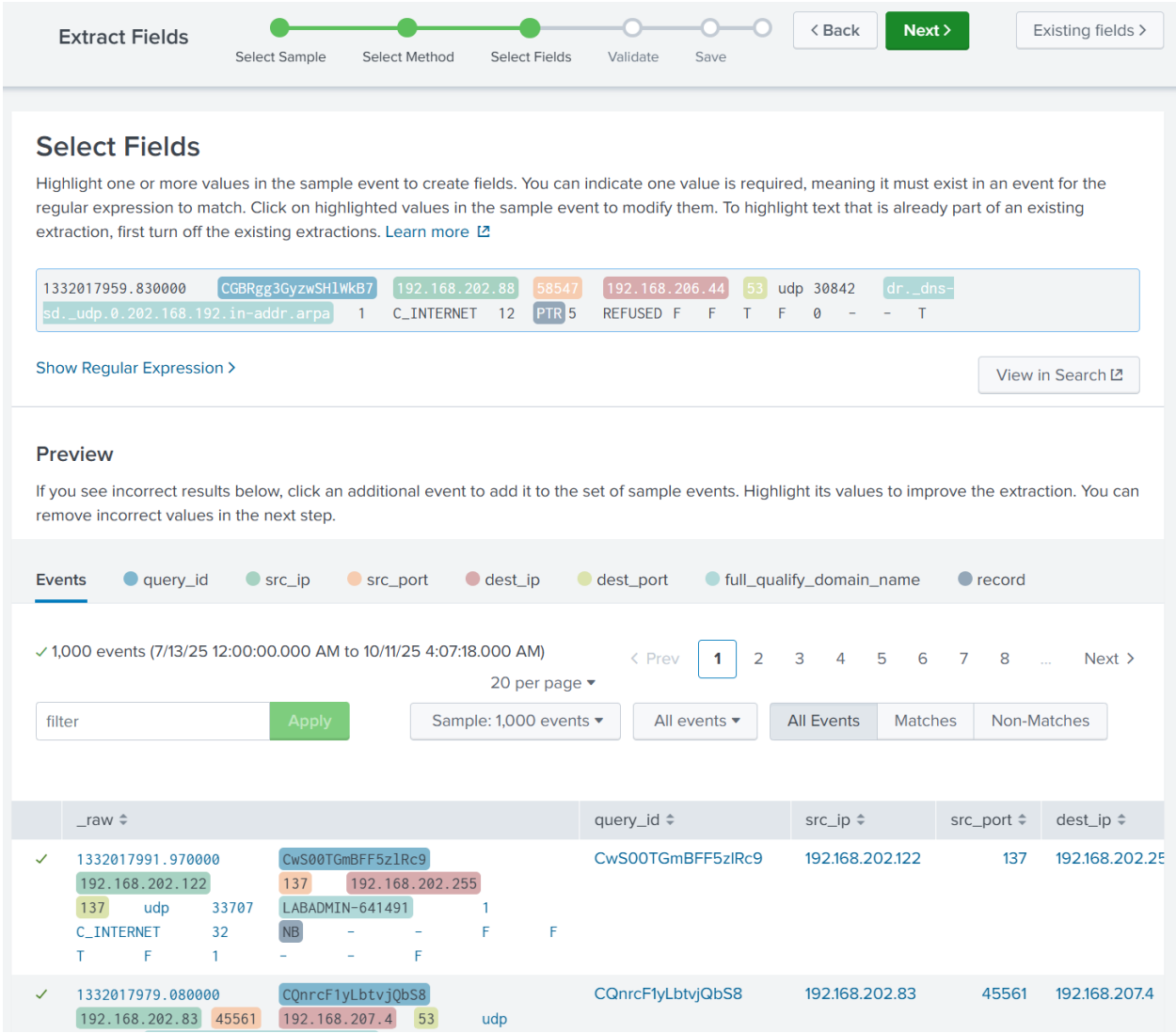
- Select Regular Expression



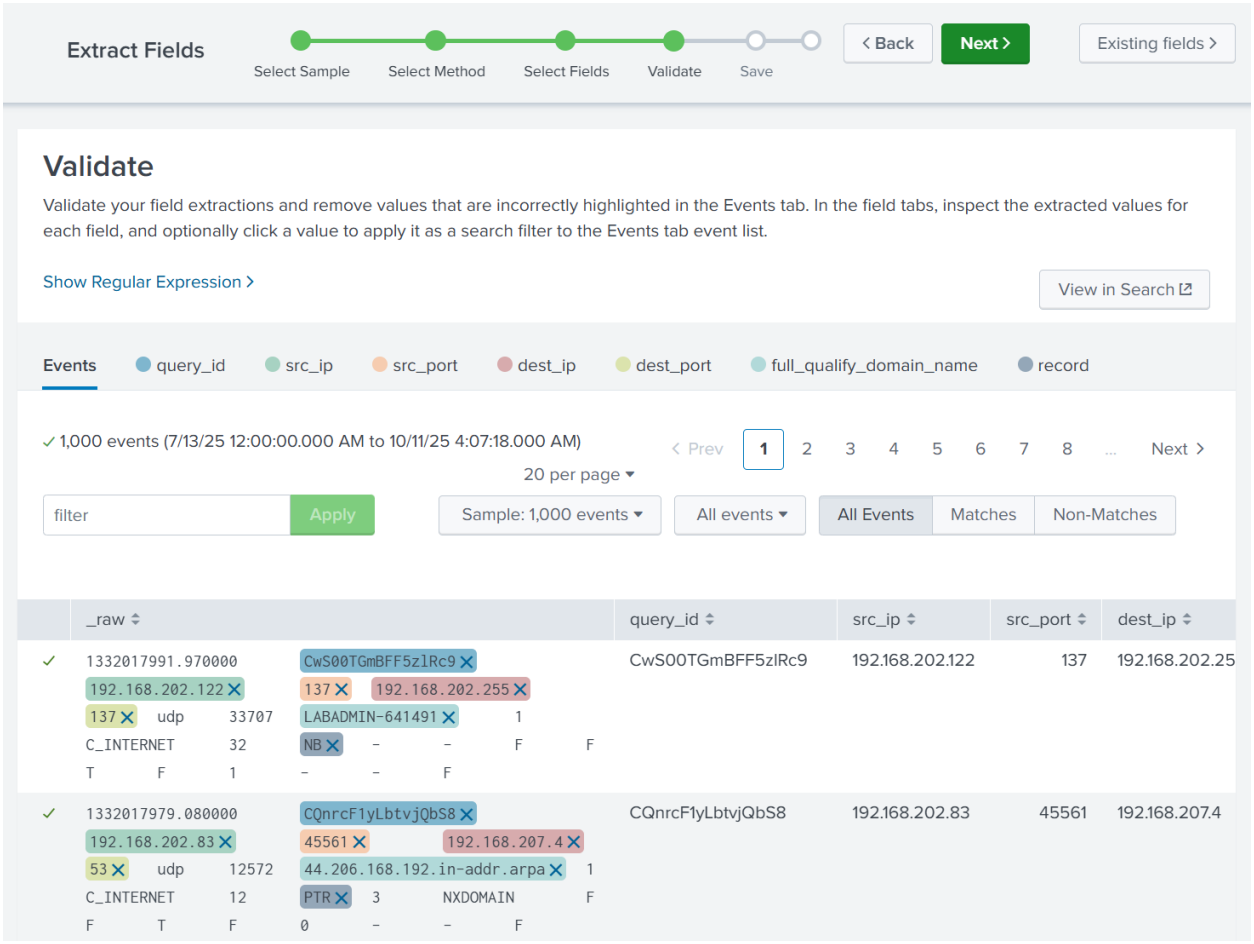
Select the field **192.168.202.88**, which is the client IP address, and click **Add Extraction**. It will then be grouped and highlighted in a unique color as shown below.



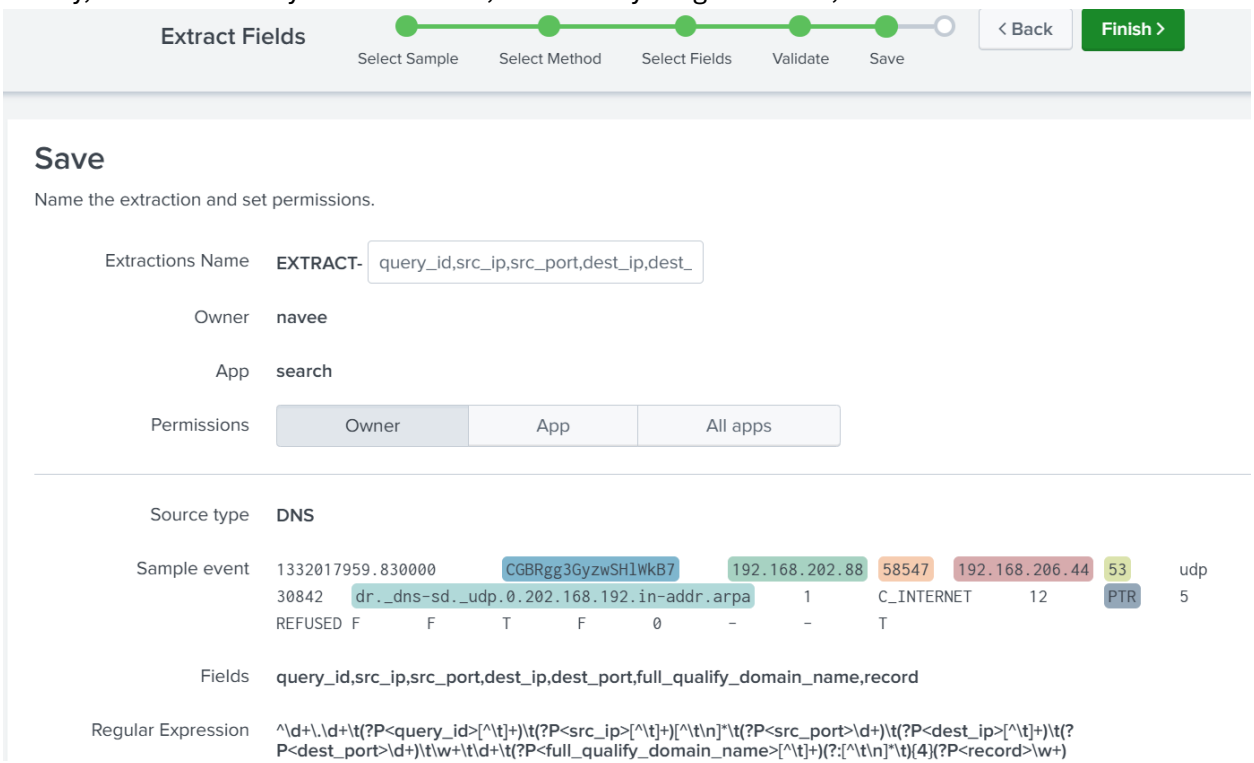
This is how it looks after you finish grouping all the fields you want. In the **Events** panel below, you can see the names of your fields along with colors that indicate them.


Extract Fields
Select Sample
Select Method
Select Fields
Validate
Save
Back
Next
Existing fields
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 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
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
query_id
src_ip
src_port
dest_ip
dest_port
full_qualify_domain_name
record
1,000 events (7/13/25 12:00:00.000 AM to 10/11/25 4:07:18.000 AM)
Prev
1
2
3
4
5
6
7
8
Next
20 per page
filter
Apply
Sample: 1,000 events
All events
All Events
Matches
Non-Matches
_raw
query_id
src_ip
src_port
dest_ip
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
CwS00TGmBFF5zlRc9
192.168.202.122
137
192.168.202.25
1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp
CQnrcF1yLbtvjQbS8
192.168.202.83
45561
192.168.207.4

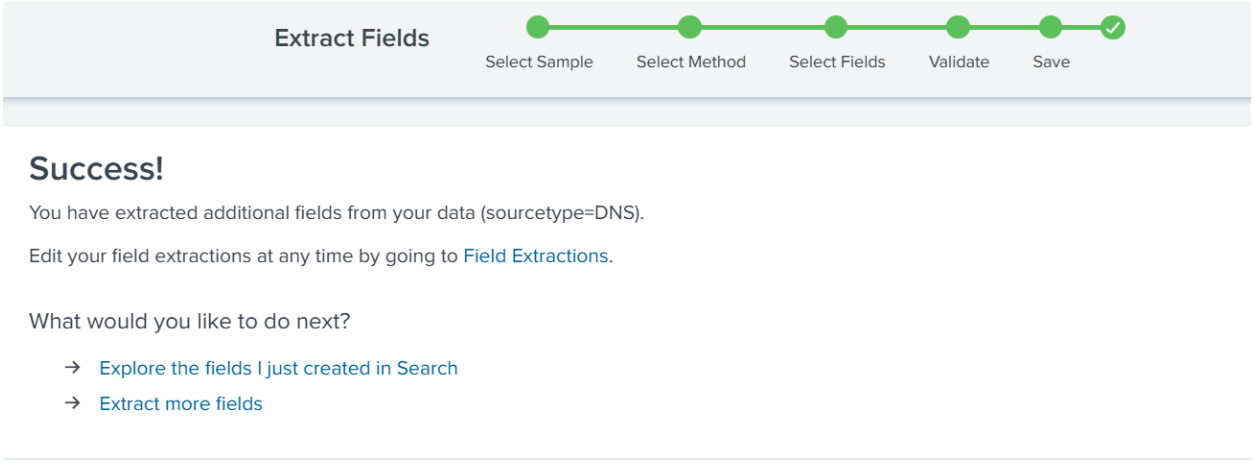
- Validate your fields.



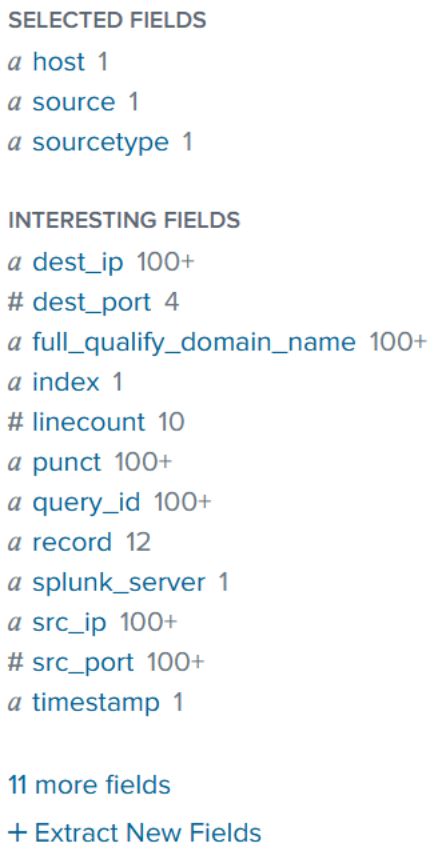
Finally, check the newly extracted field, and if everything is correct, click **Finish**.



- It shows that you successfully extracted additional fields.



Now, additional fields have been added to the **Interesting Fields** section, including **dest_ip**, **dest_port**, and others.



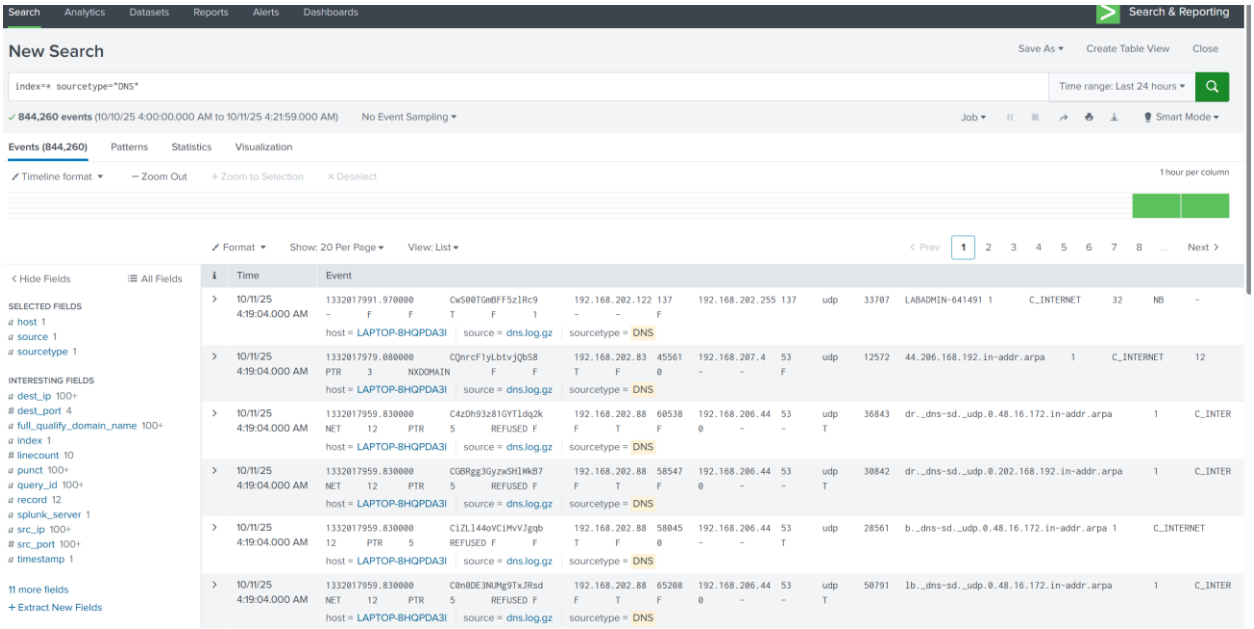
Steps to Analyze DNS Log Files in Splunk SIEM

1. **Search for DNS Events**

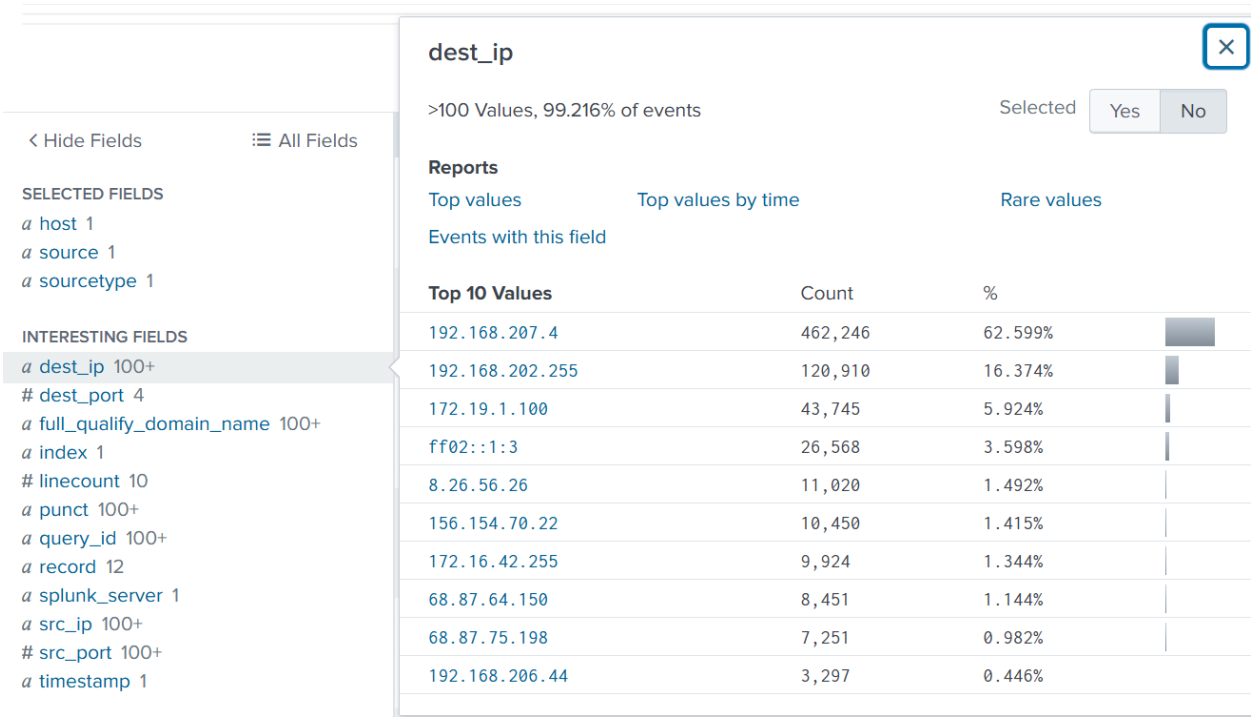
- Launch the Splunk interface and navigate to the search bar.
- Use the following query to pull all DNS-related events:

```
index=* sourcetype="DNS"
```

Note: "DNS" is the sourcetype name you assigned when uploading the data.



- If you navigate to the fields, it shows you interesting information like top value count and more



2. Extract Relevant Fields

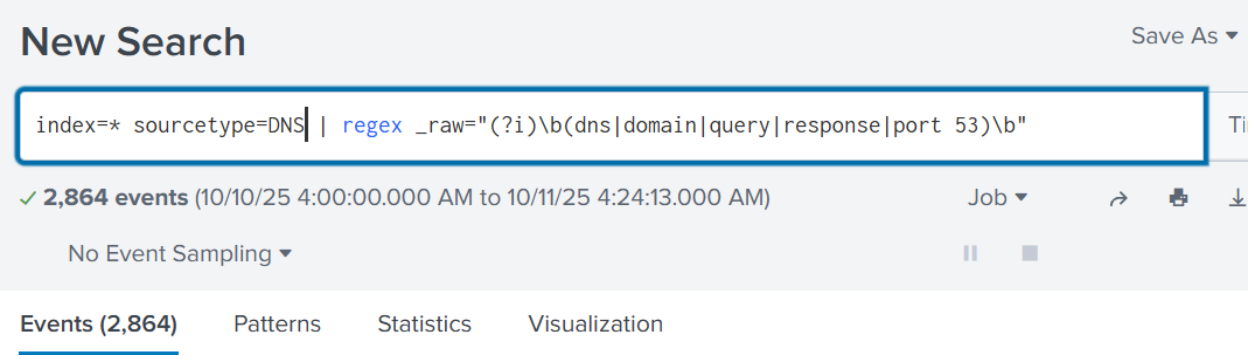
- Identify important fields in DNS logs, such as **source IP**, **destination IP**, **domain name**, **query type**, **response code**, and more.
- You can use a regex to search for common DNS-related keywords in the raw event data. For example:

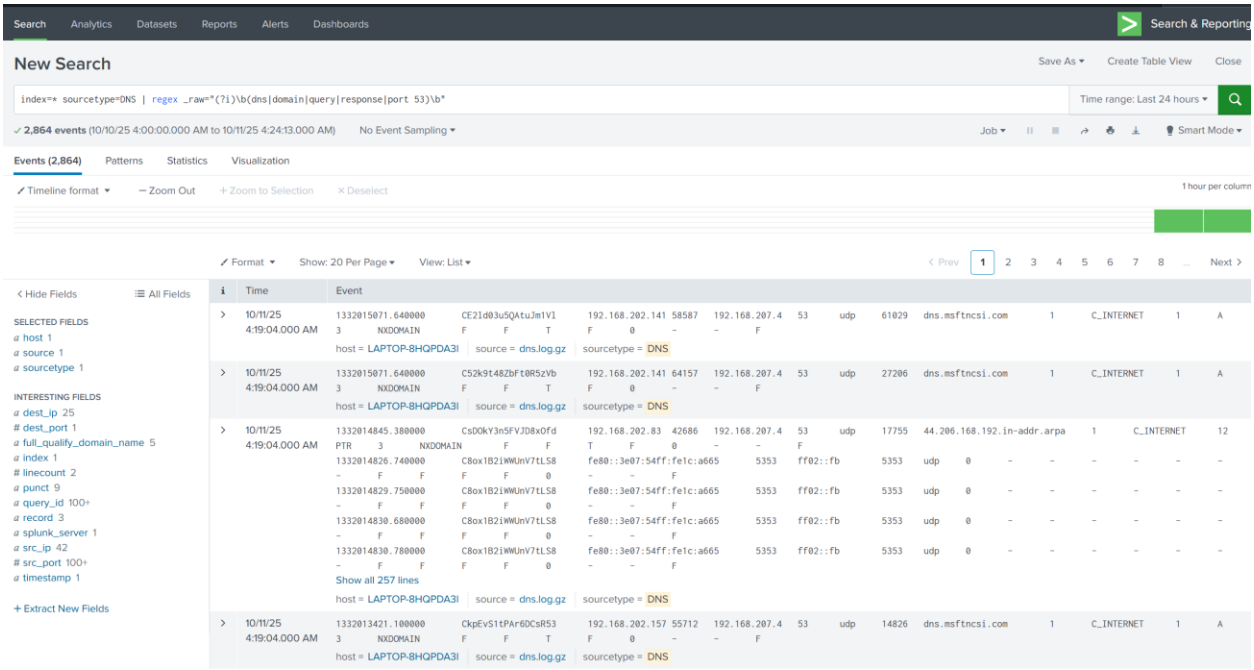
| regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"

- Full example query:

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

This helps isolate DNS-specific information from the raw logs for easier analysis.



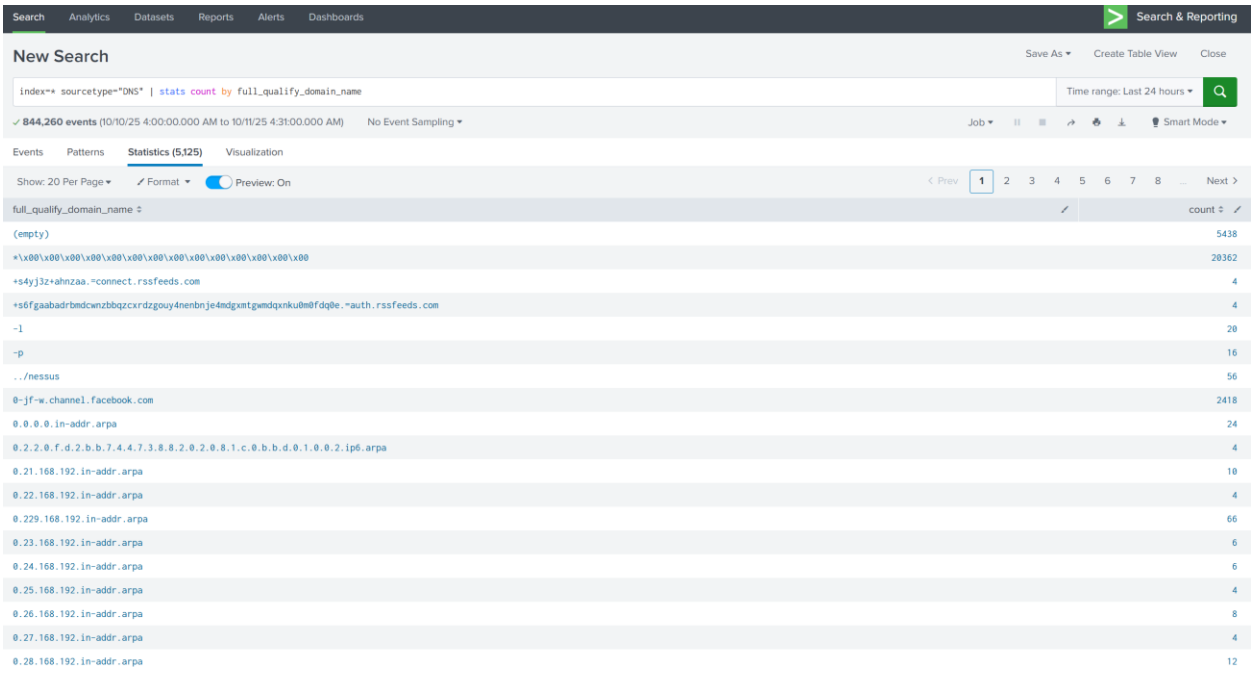


3. Identity Threat or Unusual Pattern

- - Analyze DNS activity to spot any unusual or suspicious patterns.
- Example query to highlight such events:

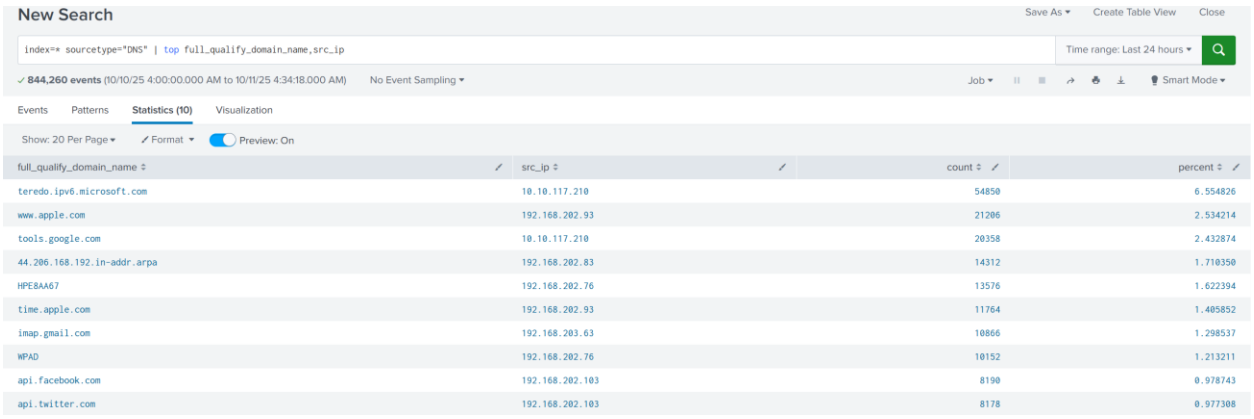
index=* sourcetype="DNS" | stats count by full_qualified_domain_name

This query counts the number of occurrences for each domain, helping to identify domains with abnormal or excessive query activity.



With this search, we see the anomalies in DNS activity

- *\x00\x00\x00 look like encoded entries, it might be from corrupted DNS packet or malformed queries.
- 0.xxx.168.192 in-addr.arpa, this one is reverse DNS lookups, so it is when an IP address is queried to find its hostname. It is normal but the large number of these could indicate that malicious activity going on here.



Now we get the top queried domains and can see what stand out.

1.Random looking names

- Here, the example is HPE8AA67 which look like a random hostname or misconfigured local device but it is not a standard full qualified domain name

2. Extremely high query count

- in this case, teredo.ipv6.microsoft.com has 54850 queries. Teredo is a windows IPv6 tunneling protocol, but with so many queries like this could indicate automated or misconfiguration. Should check the source ip (10.10.117.210)

3. Reverse DNS lookups

- 44.206.168.192.in-addr.arpa, this is reversed lookup which is normal, but with the high count could indicate something.

4. Well known service

-The rest like www.apple.com, imap.gmail.com, or api.twitter.com are normal network activity from users.

So in this case, HPE8AA67 and teredo.ipv6.microsoft is suspicious and worth to investigate more.

Conclusion

Analyzing DNS (Domain Name System) logs with Splunk helps security teams quickly detect and investigate suspicious activity. By studying DNS traffic and spotting unusual patterns, organizations can improve their security and reduce the risk of cyber threats.