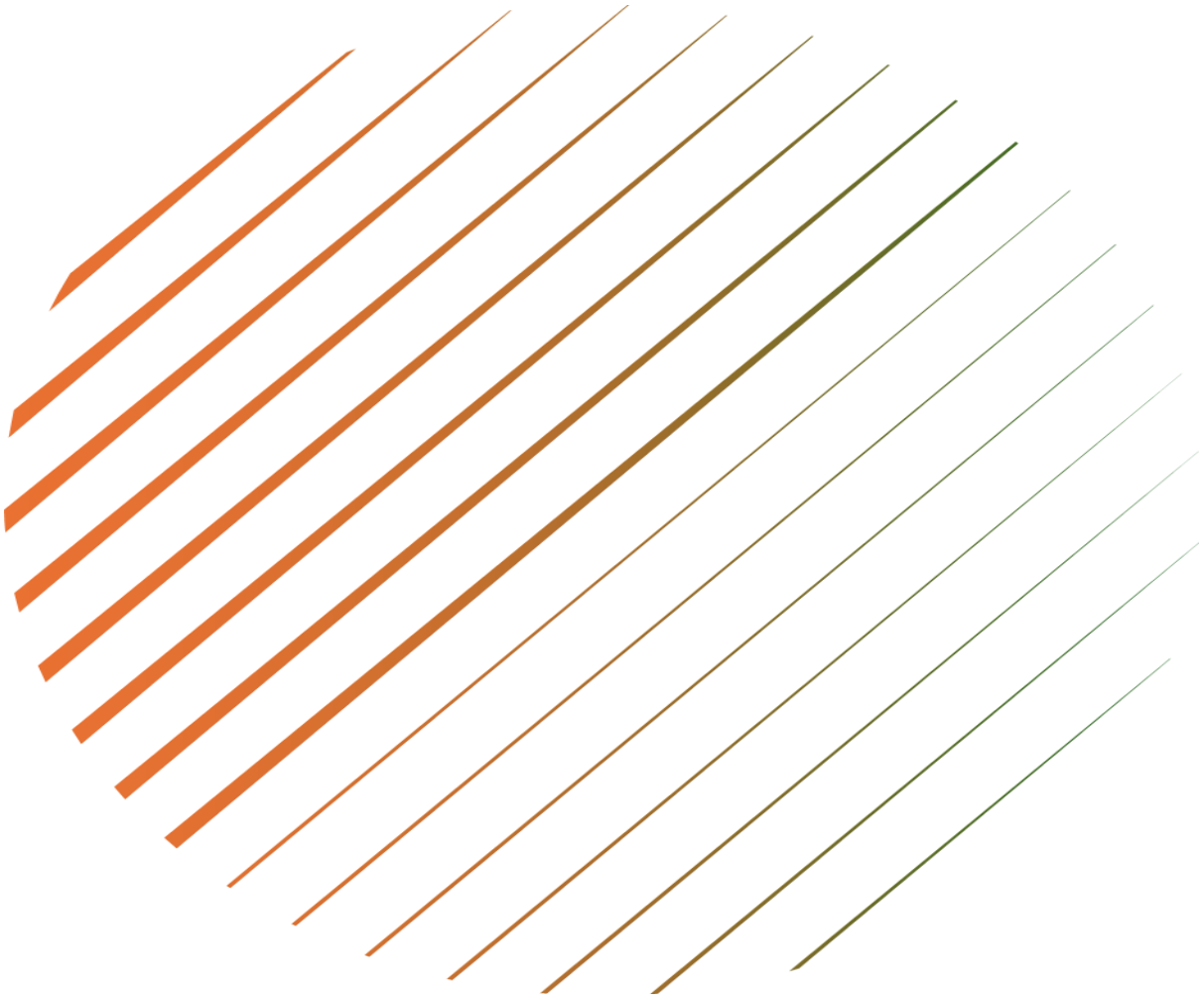
ADVANCED DNS SECURITY MONITORING WITH SPLUNK SPL



PREPARED BY: PRANIT KALAMBATE

ROLE/PROGRAM: TRAINED IN CEH CURRICULUM / CYBERSECURITY ANALYST TRAINING

DATE COMPLETED: 10-12-2025

1.PROJECT OVERVIEW

1.1 Goal

The primary goal of this project is to perform DNS log analysis using Splunk Enterprise to:

Extract key fields from raw DNS log data.

Identify the most frequently queried Fully Qualified Domain Names (FQDNs).

Determine the most active source IP addresses (clients) generating DNS requests.

1.2 Data Source

The project utilizes DNS logs ingested into a Splunk index.

Source: dns.log.gz

Sourcetype: dnslogs (This is inferred from the search queries and events).

Index: index=sources/pendnslogs (This is inferred from the search queries).

2.FIELD EXTRACTION PROCESS

Since the raw DNS logs did not have all the desired fields automatically extracted, a Field Extraction process was required. This was done using the Splunk Field Extractor utility.

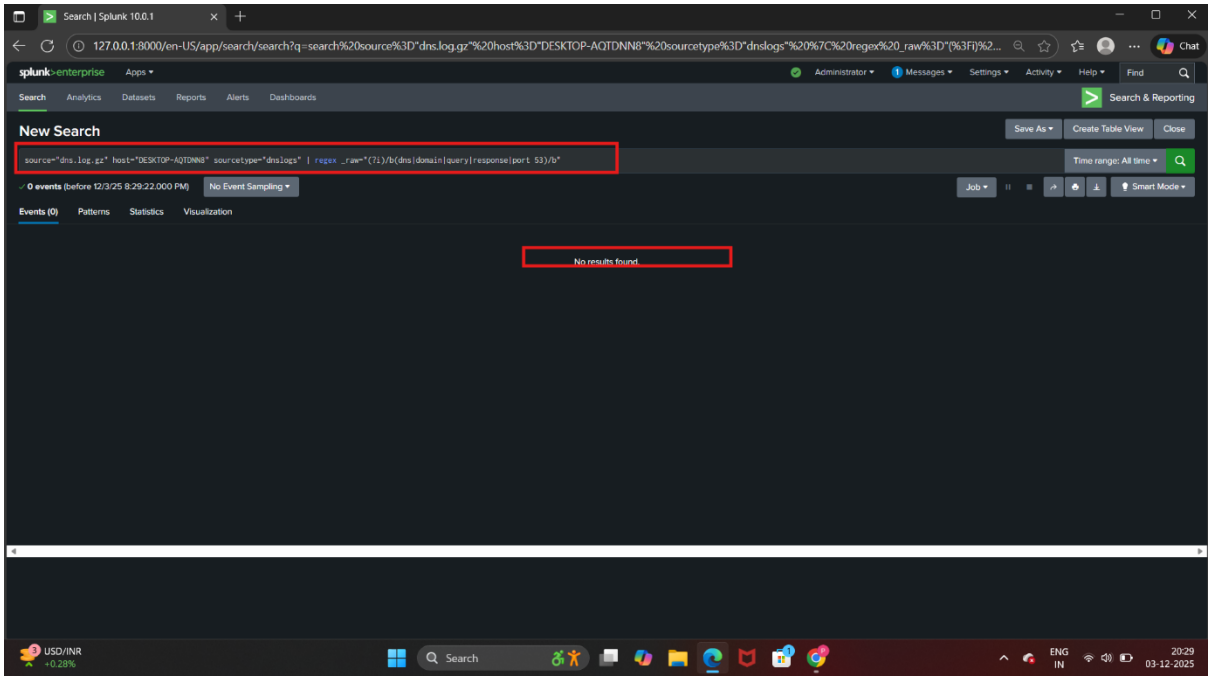
2.1 Starting the Extraction

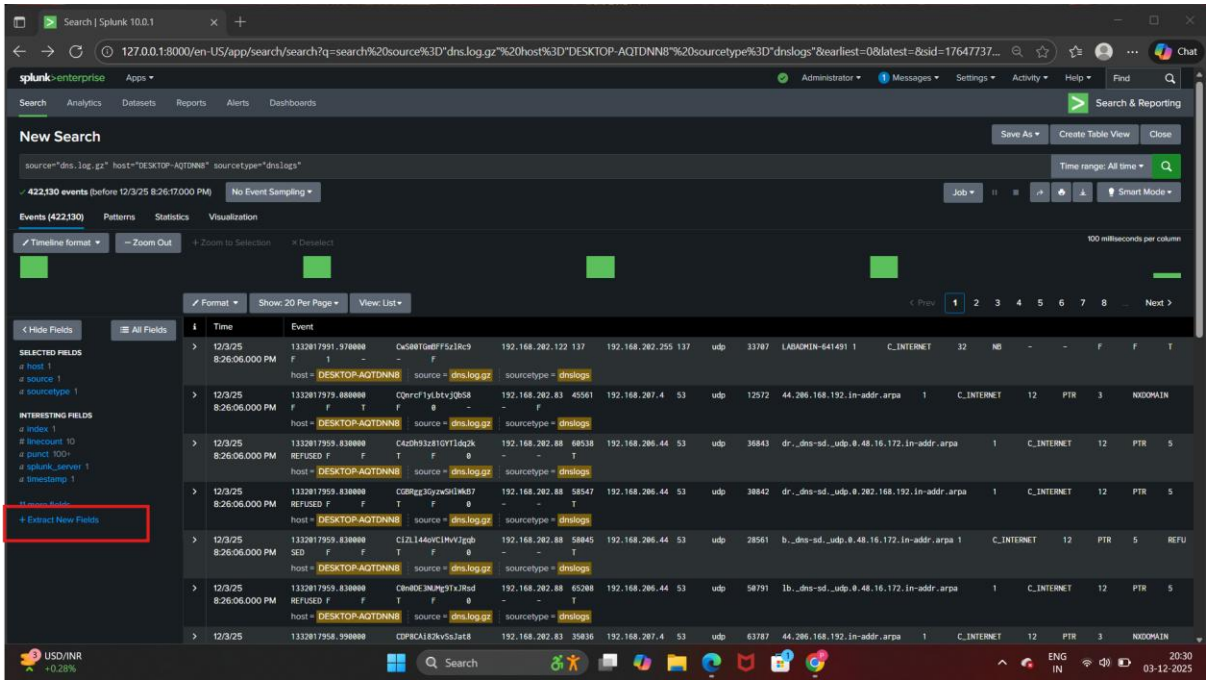
The field extraction process begins from an event search, by selecting the "Extract New Fields" option.

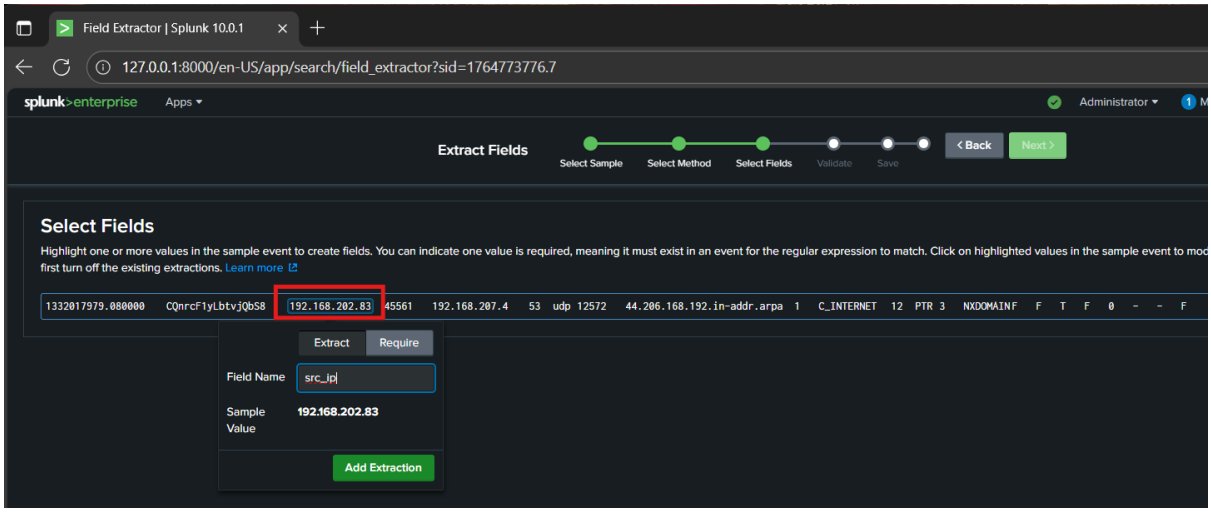
2.2 Extracted Fields

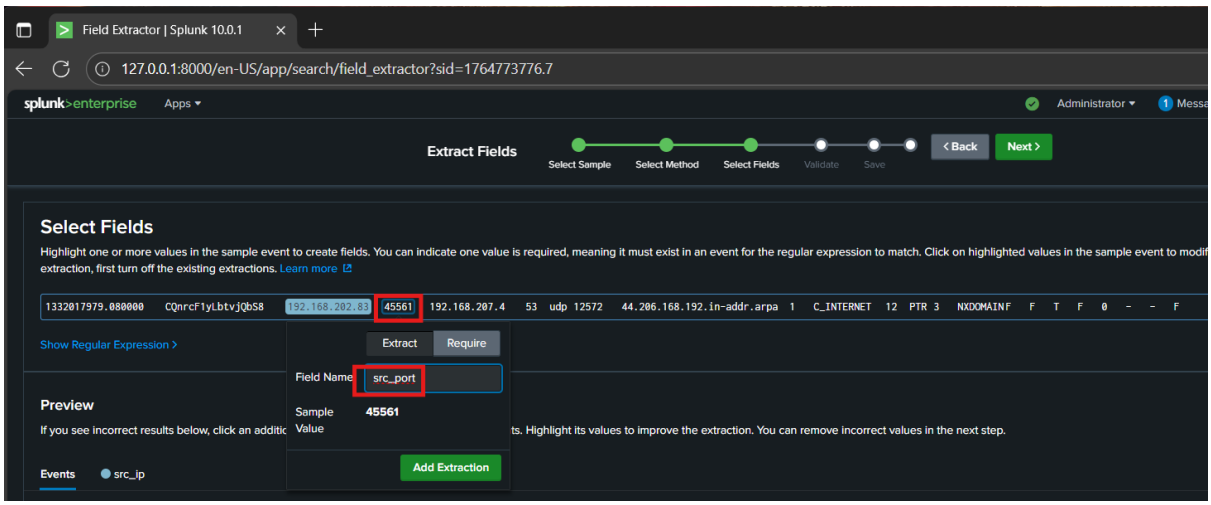
The following critical fields were manually extracted to enrich the log data:

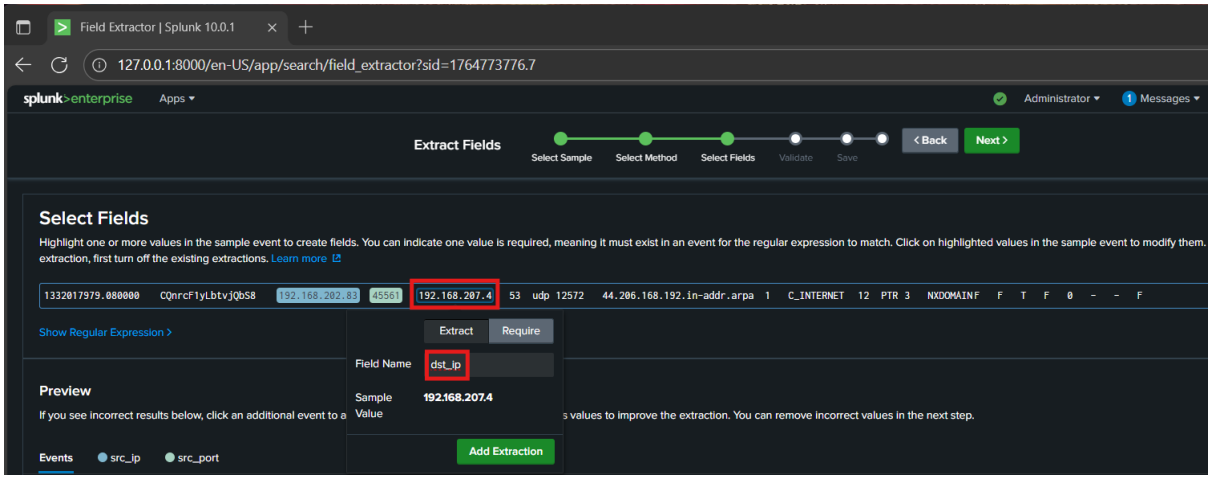
Field Name	Description
src_ip	The IP address of the client making the DNS request.
src_port	The source port used by the client for the DNS request.
dst_ip	The IP address of the destination DNS server.
fqdn	The Fully Qualified Domain Name being queried.

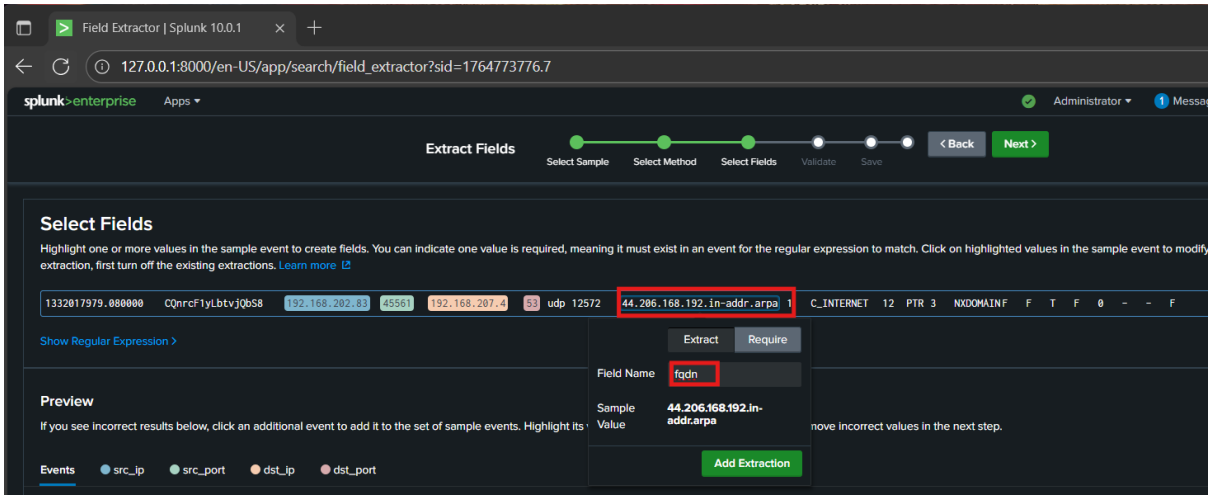

Search | Splunk 10.0.1
New Search
source="dns.log.gz" host="DESKTOP-AQTDNN8" sourcetype="dnslogs" | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"
0 events (before 12/3/25 8:29:22.000 PM)
No Event Sampling
Events (0)
Patterns
Statistics
Visualization
No results found.


Search | Splunk 10.0.1
New Search
source="dns.log.gz" host="DESKTOP-AQTDNN8" sourcetype="dnslogs"
422,130 events (before 12/3/25 8:26:17.000 PM)
No Event Sampling
Events (422,130)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
INTERESTING FIELDS
+ Extract New Fields
Time
Event


Field Extractor | Splunk 10.0.1
127.0.0.1:8000/en-US/app/search/field_extractor?sid=1764773776.7
splunk>enterprise
Apps
Administrator
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 highlighted values in the sample event to mod
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 NXDOMAINF F T F 0 - - F
Extract
Require
Field Name
src_ip
Sample Value
192.168.202.83
Add Extraction

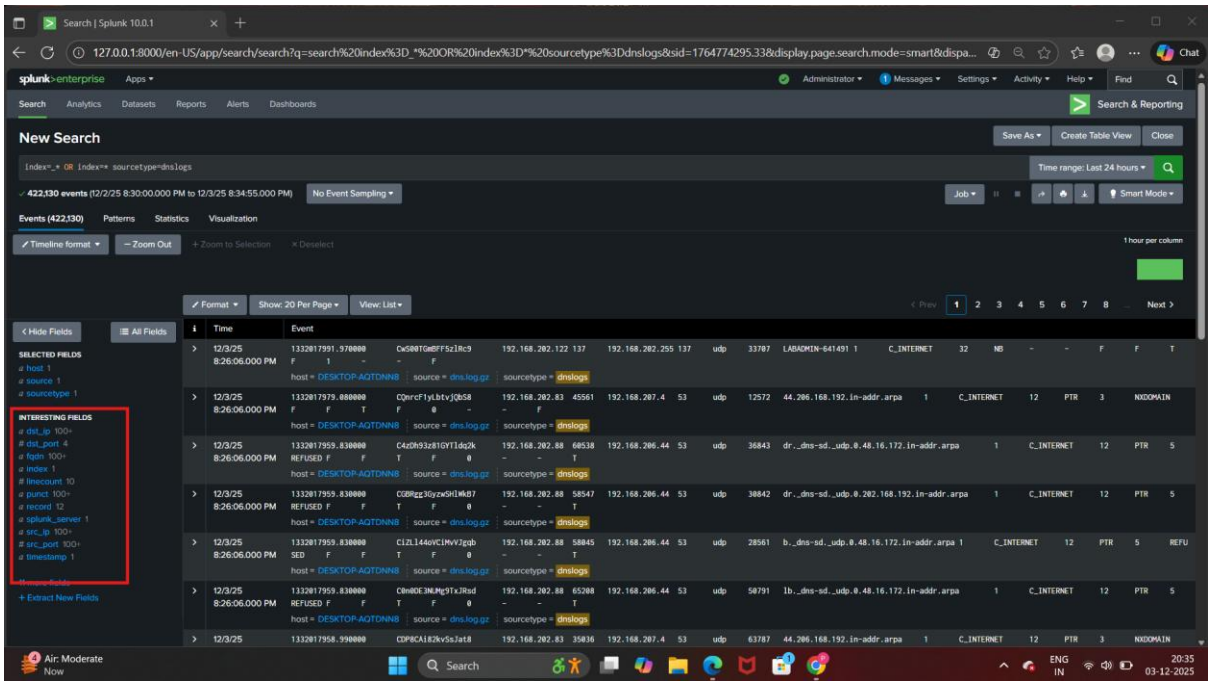

Field Extractor | Splunk 10.0.1
127.0.0.1:8000/en-US/app/search/field_extractor?sid=1764773776.7
splunk>enterprise
Apps
Administrator
Extract Fields
Select Sample
Select Method
Select Fields
Validate
Save
Back
Next
Select Fields
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modif
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 NXDOMAINF F T F 0 - - F
Show Regular Expression
Extract
Require
Field Name
src_port
Sample Value
45561
Add Extraction
Preview
If you see incorrect results below, click an additic
ts. Highlight its values to improve the extraction. You can remove incorrect values in the next step.
Events
src_ip


Field Extractor | Splunk 10.0.1
127.0.0.1:8000/en-US/app/search/field_extractor?sid=1764773776.7
splunk>enterprise
Apps
Administrator
Messages
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 highlighted values in the sample event to modify them.
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 NXDOMAINF F T F 0 - - F
Show Regular Expression
Extract
Require
Field Name
dst_ip
Sample Value
192.168.207.4
Add Extraction
Preview
If you see incorrect results below, click an additional event to a
s values to improve the extraction. You can remove incorrect values in the next step.
Events
src_ip
src_port



2.3 Post-Extraction Verification

After the field extraction was completed, the new fields (src_ip, src_port, dst_ip, fqdn, etc.) appeared in the "Interesting Fields" sidebar, confirming successful extraction and availability for further searches and analysis.



3. ANALYSIS AND RESULTS

The extracted fields were used with Splunk Search Processing Language (SPL) commands to perform the required analysis.

3.1 Most Frequent FQDNs Queried

This analysis identifies the domain names that were queried most often in the log set, providing insight into the most commonly accessed external resources or internal services.

SPL Query Used:

index=* OR index=sources/pendnslogs | top limit=20 fqdn

- The top command is an efficient way to find the most frequent values in the fqdn field.
- limit=20 ensures that only the top 20 results are displayed.

The top command automatically calculates the frequency (count) and the percentage of the total events (percent).

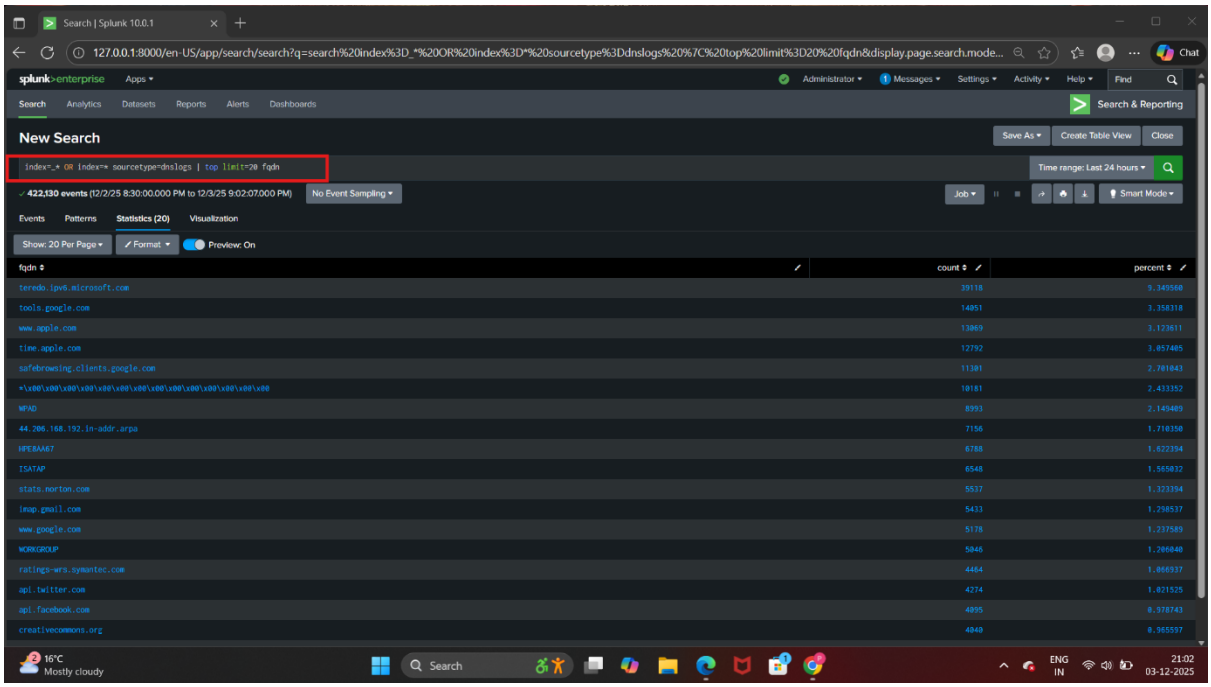
Results (Partial): The search results successfully list the top 20 most frequent FQDNs. The output table clearly shows the domain name, the total count of times it was queried, and the percent this count represents of the total search results.

The top queried domains prominently include:

teredo.ipv6.microsoft.com

tools.google.com

www.apple.com



3.2 Most Active Source IP Addresses

This analysis identifies the source IP addresses (clients) that generated the highest number of DNS requests. This is crucial for identifying high-traffic clients or potentially compromised systems.

SPL Query Used:

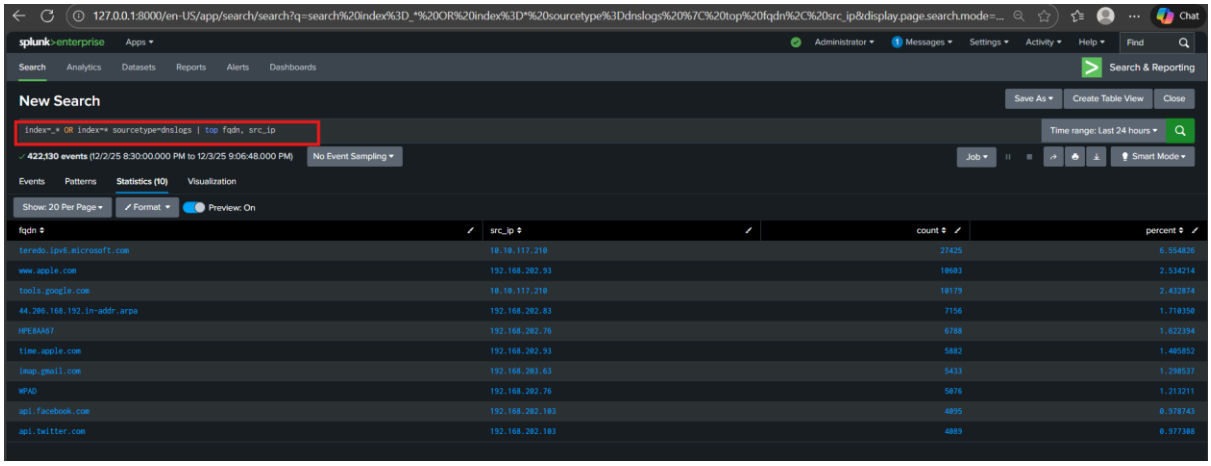
index=* OR index=sources | top fqdn, src_ip

- This command shows the most frequent pairings of FQDNs and the src_ip that queried them.

Results (Partial): The resulting table allows for the immediate identification of the most active source IP addresses based on the sheer volume of requests they generate.

Example Output Snippets:

- The IP address 18.18.117.218 is associated with the highest volume of queries for teredo.ipv6.microsoft.com.
- The IP addresses in the 192.168.202.x range are prominent for querying domains like www.apple.com and others, indicating high client activity from these internal hosts.



3.3 Identifying Rare DNS Query Types (Security Evasion Detection)

The DNS protocol can be exploited for covert data exfiltration or Command-and-Control (C2) communication, a technique known as DNS Tunneling. Attackers often use less common record types (like TXT or SRV) instead of the standard A or AAAA records. By using the rare command, I could quickly identify these unusual types.

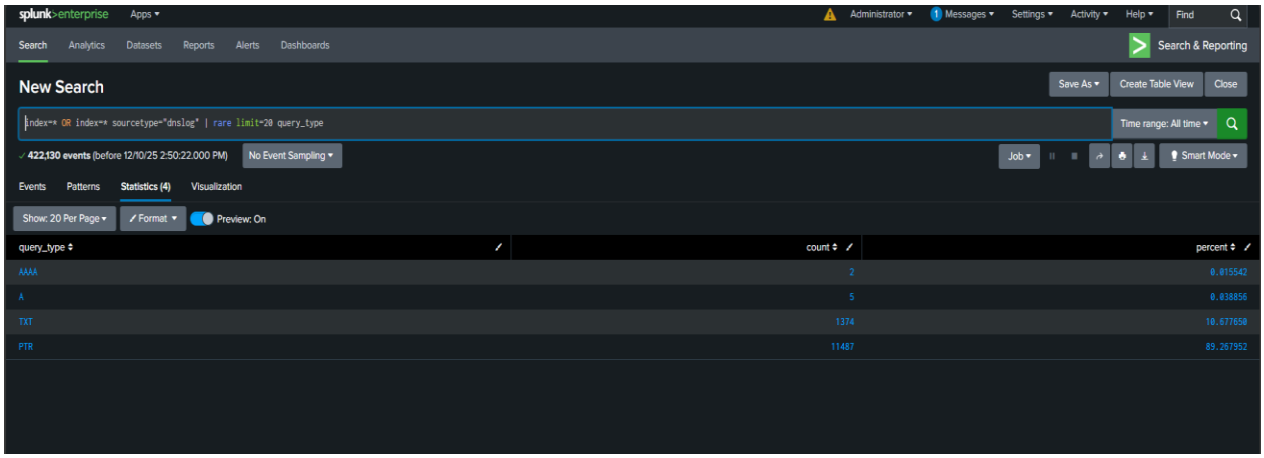
Recruiter Value: Demonstrates the ability to apply frequency analysis to detect subtle, potentially malicious evasion techniques and understand DNS protocol nuances.

SPL Query Used:

index=* OR index=* sourcetype=dnslog | rare limit=20 query_type

rare: This is a transforming command used to find the least common values in a specified field, serving as the inverse of the top command.

query_type: This field represents the type of DNS record requested (e.g., A, PTR, TXT).



3.4 Analysis of Unique Queried Domains per Source IP (Identifying Chatty Hosts)

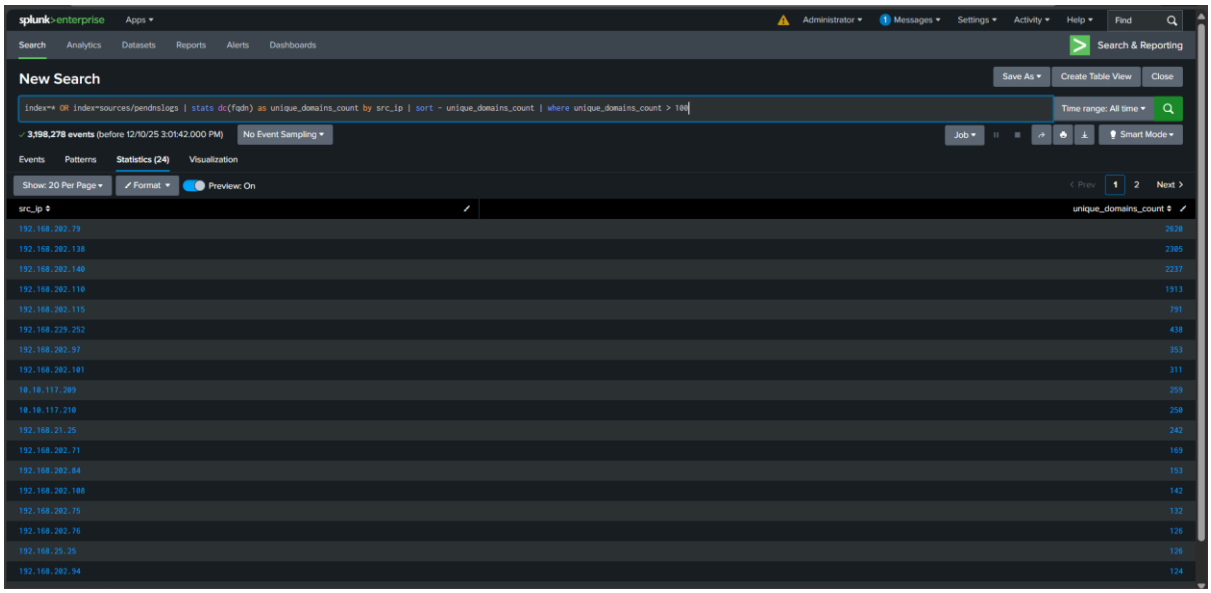
This analysis is vital for identifying "Chatty Hosts"—client machines that query an unusually high number of unique domains over a short period. This behavior is often a signature of Domain Generation Algorithm (DGA) malware or reconnaissance/scanning activity. Identifying these outliers is a fundamental component of proactive threat hunting.

SPL Query Used:

```
index=* OR index=* sourcetype="dnslog" | stats dc(fqdn) as unique_domains_count by src_ip | sort - unique_domains_count | where unique_domains_count > 100
```

- stats: Used to calculate statistics on groups of events.
- dc(fqdn): The Distinct Count function calculates the number of unique FQDNs for each group.
- as unique_domains_count: Renames the resulting count field for clarity.
- by src_ip: Groups the counts based on the source IP address.

- sort - unique_domains_count: Orders the results to put the highest counts at the top.
- where unique_domains_count > 100: Filters the results to only show potential outliers (hosts querying over 100 unique domains), making the output actionable.



4.CONCLUSION

This project successfully demonstrated proficiency in leveraging Splunk Enterprise for critical DNS log analysis and proactive threat hunting. Beginning with the essential step of manually enriching raw data by extracting key fields like src_ip and fqdn, the analysis quickly established a network baseline using frequency analysis (top). Most notably, the project progressed to advanced security analytics by utilizing the rare command to identify anomalies in query_type (a key indicator for DNS Tunneling and data exfiltration), and applying stats dc(fqdn) to calculate unique domain counts per source IP—a vital technique for detecting Domain Generation Algorithm (DGA)-based malware. This work validates my technical mastery of Splunk Search Processing Language (SPL), foundational knowledge of network protocol exploitation, and ability to translate unstructured logs into actionable security intelligence, which are core competencies for a modern Security Operations Center (SOC) role.