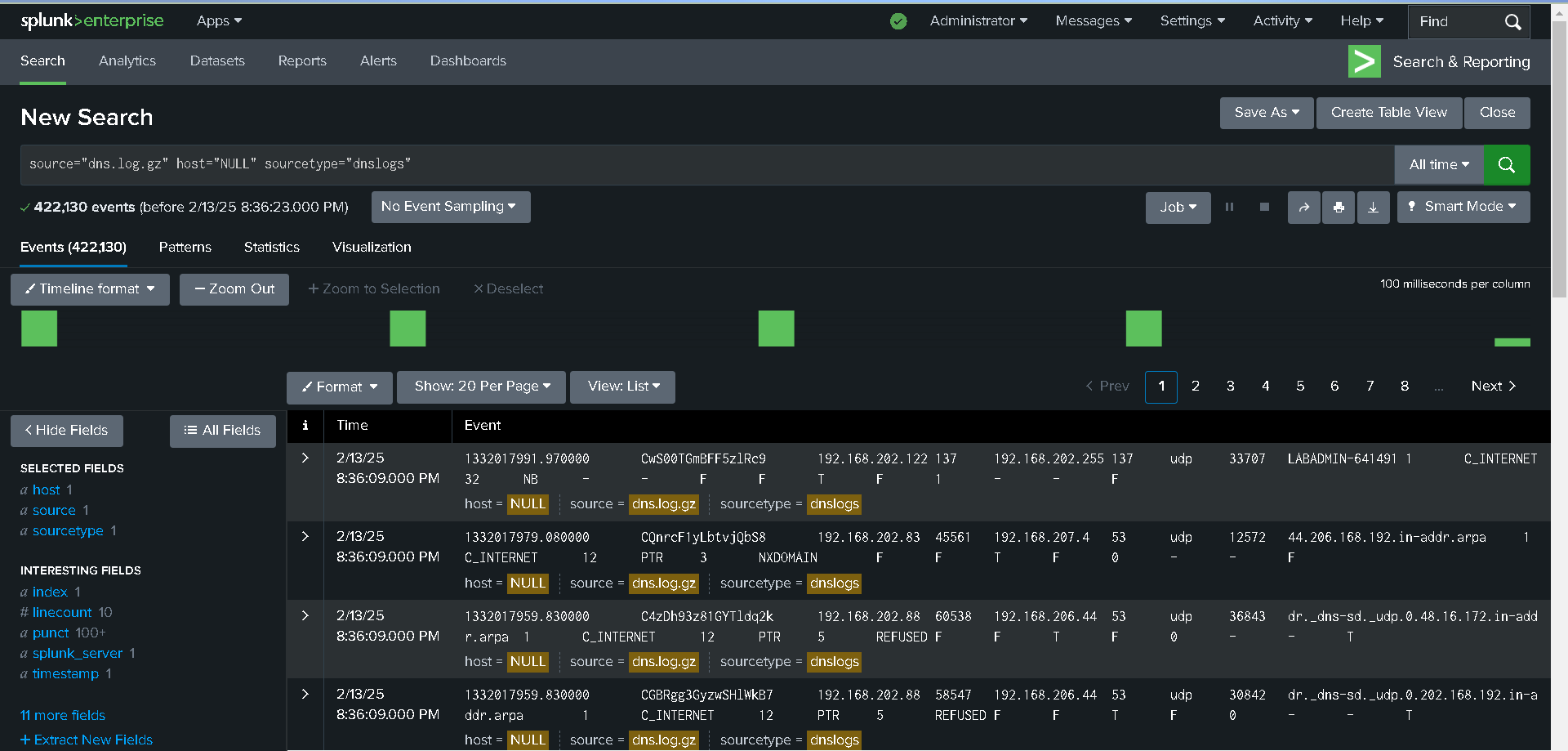
**DNS Log Analysis Using Splunk**Analyzing sample DNS Log data using SIEM tool SplunkDNS Log Ingestion  
  
  
  
Parsing the data by extracting new field  
  
selecting a sample event for extracting new field  
  
A screenshot of a computer

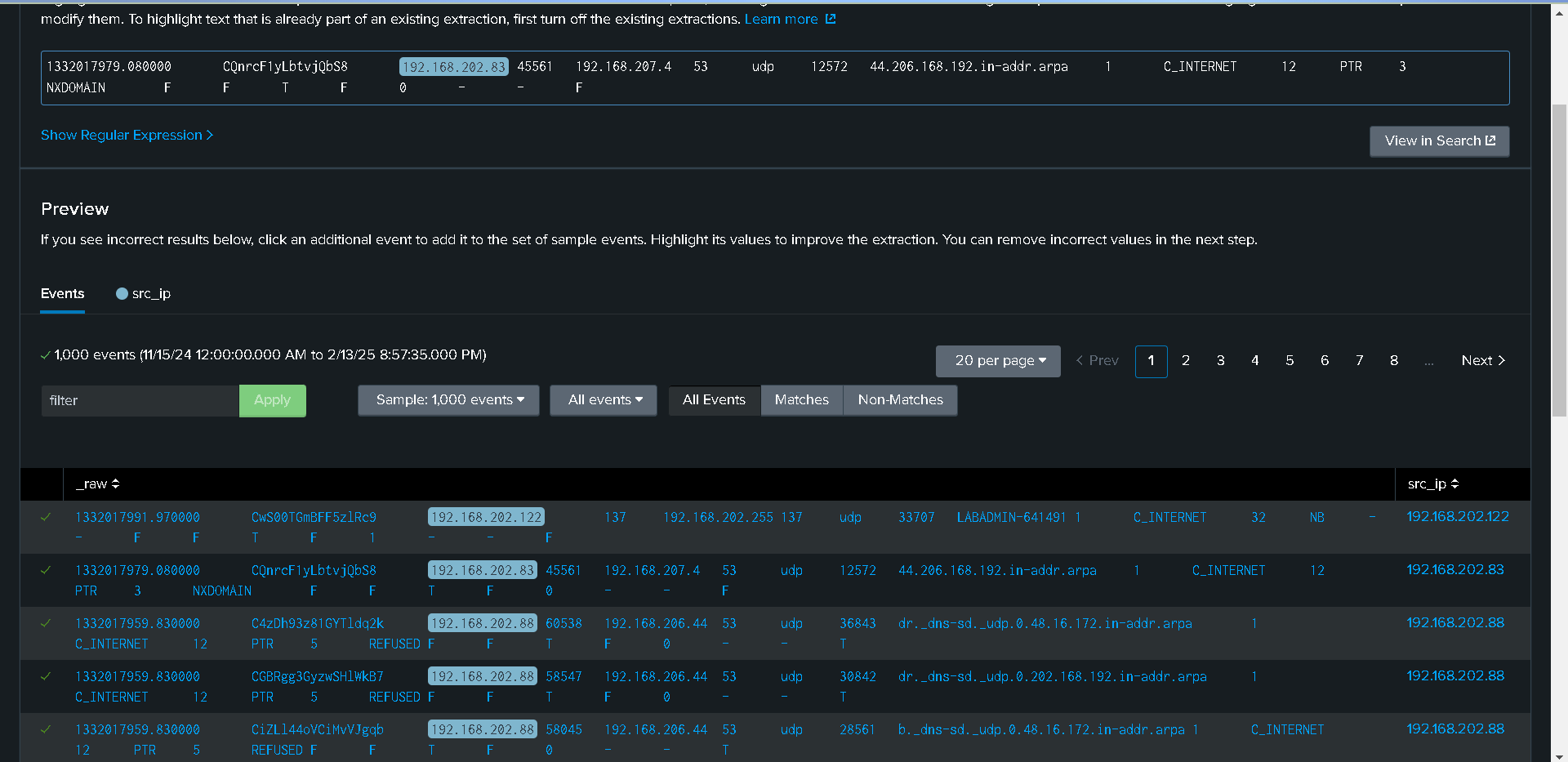
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.  
  
Choosing Regular Expression method  
  
A screenshot of a computer

AI-generated content may be incorrect.  
  
A screenshot of a computer

AI-generated content may be incorrect.  
  
Choosing 192.168.202.83 as source ip src\_ip  
A screenshot of a computer program

AI-generated content may be incorrect.  
  


Selecting 45561 as source port src\_port  
A screenshot of a computer

AI-generated content may be incorrect.

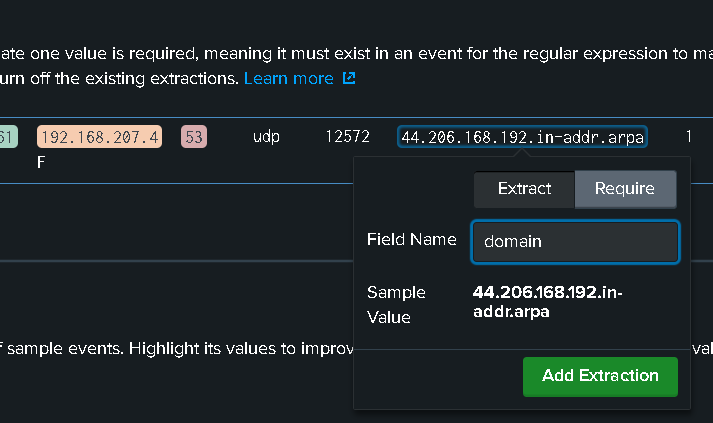
Selecting 192.168.207.4 as destination ip dst\_ip  
A screenshot of a computer

AI-generated content may be incorrect.

And 53 the dns server port  
A screenshot of a computer

AI-generated content may be incorrect.

44.206.168.192.in-addr.arpais the domain name



A screenshot of a computer

AI-generated content may be incorrect.  
PTR - Type of record  
  
A screenshot of a computer

AI-generated content may be incorrect.  
Successfully extracted the field from log

The extracted field lists are now on the interesting fields list

A screenshot of a computer

AI-generated content may be incorrect.

Stats count by domain name

A screenshot of a computer

AI-generated content may be incorrect.

Using top filter   
A screenshot of a computer

AI-generated content may be incorrect.  
  
Now checking which source ip has requested more on specific domains  
  
A screenshot of a computer

AI-generated content may be incorrect.  
  
From this we can suspect that 192.168.202.83 as the compromised machine  
  
  
  
  
Table view of source ip, destination ip and ports  
  
A screenshot of a computer

AI-generated content may be incorrect.