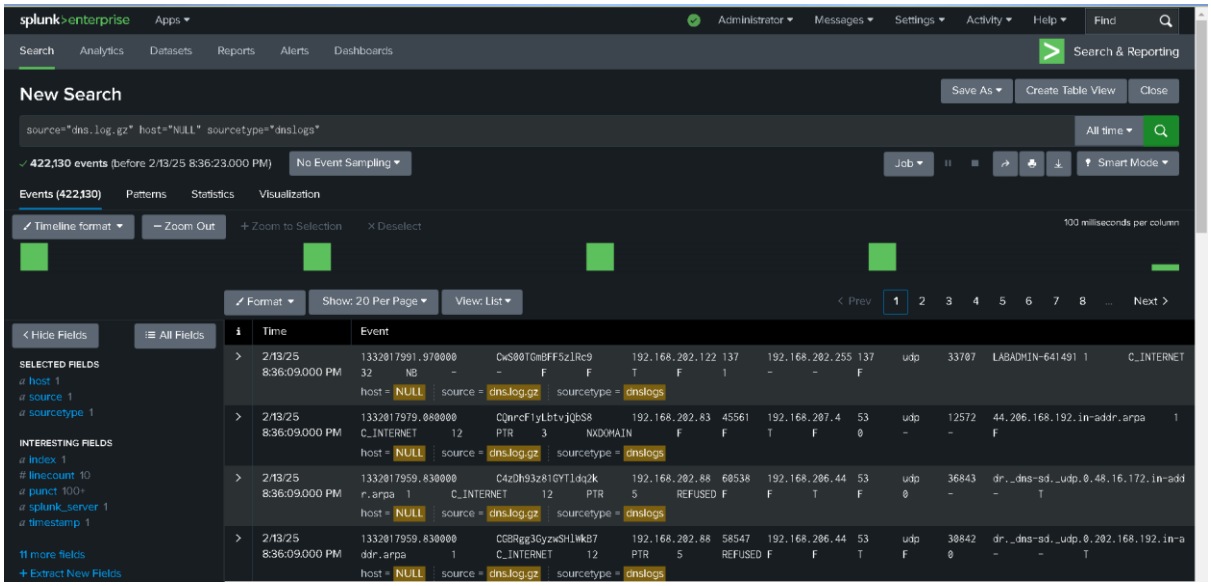
DNS Log Analysis Using Splunk

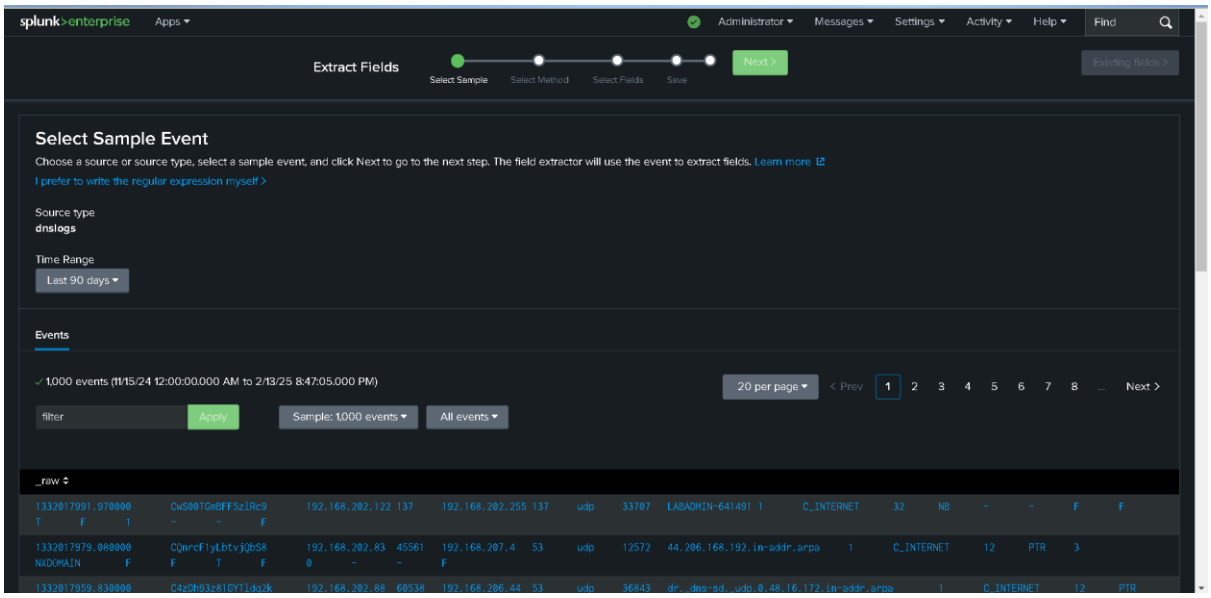
Analyzing sample DNS Log data using SIEM tool Splunk

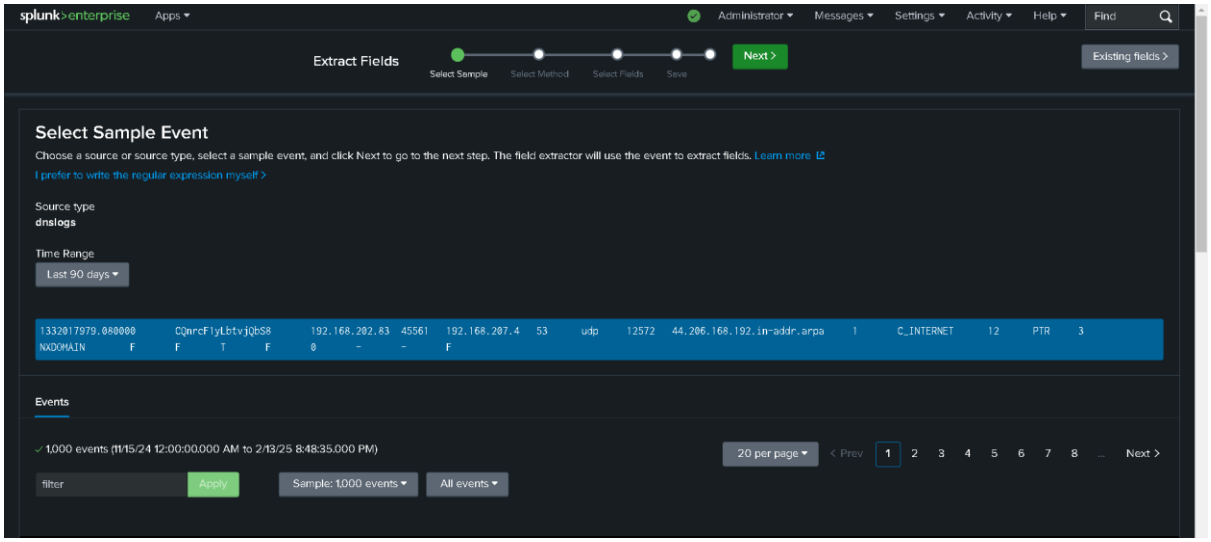
DNS Log Ingestion



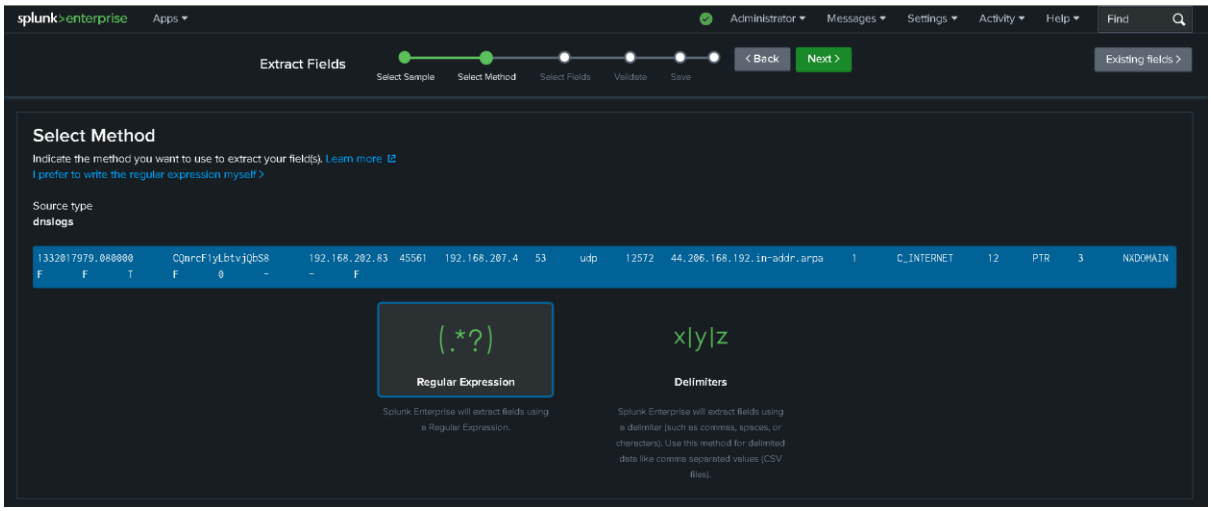
Parsing the data by extracting new field

selecting a sample event for extracting new field

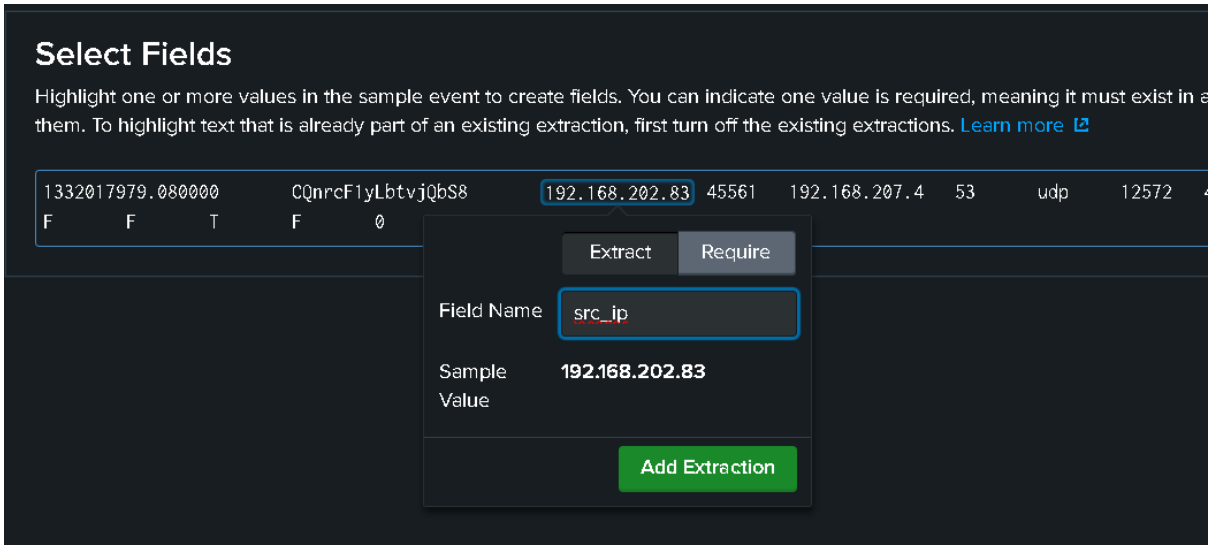


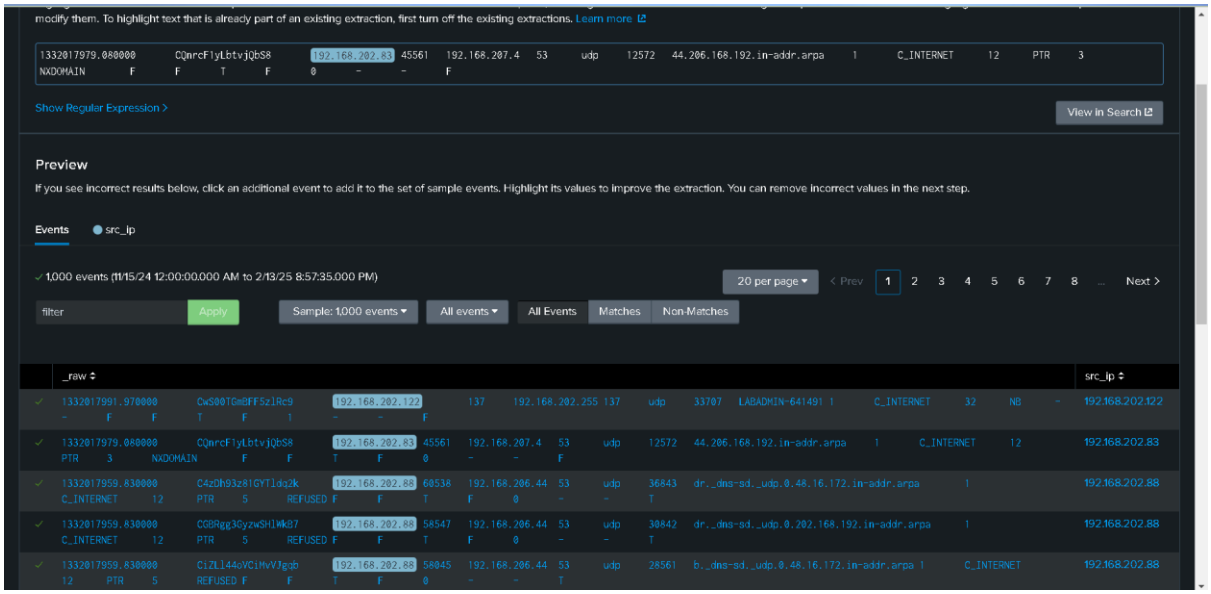


Choosing Regular Expression method

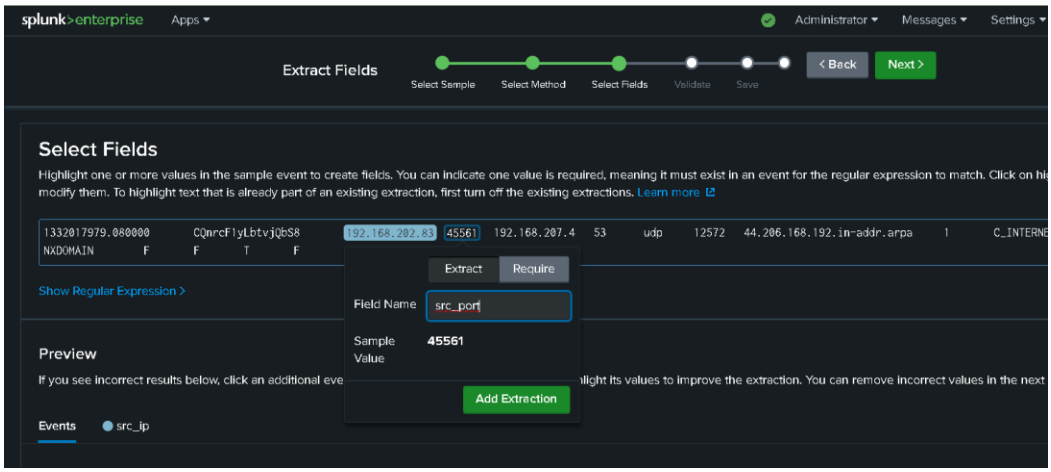


Choosing 192.168.202.83 as source ip src_ip

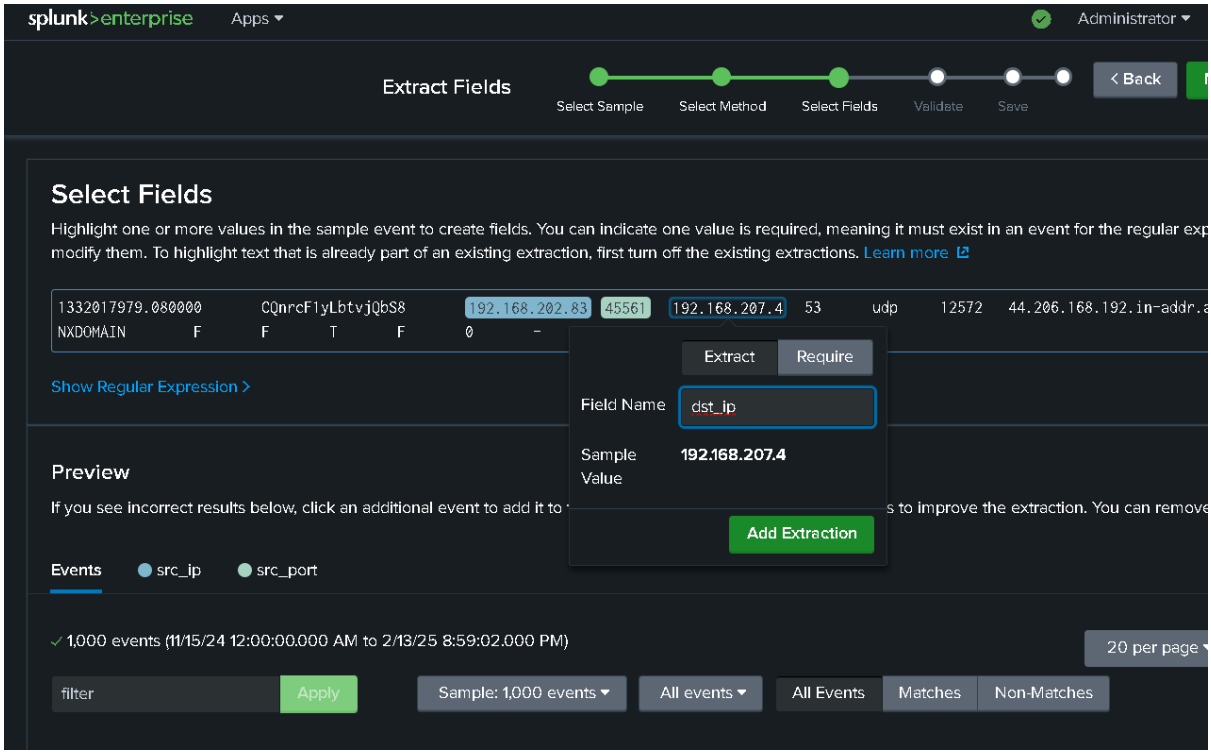




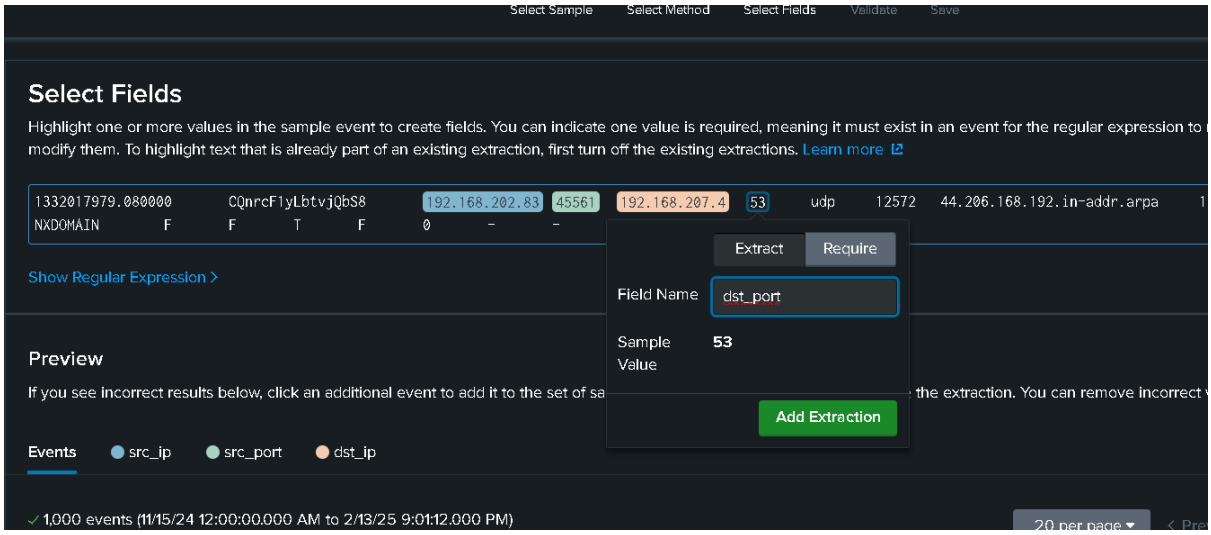
Selecting 45561 as source port src_port



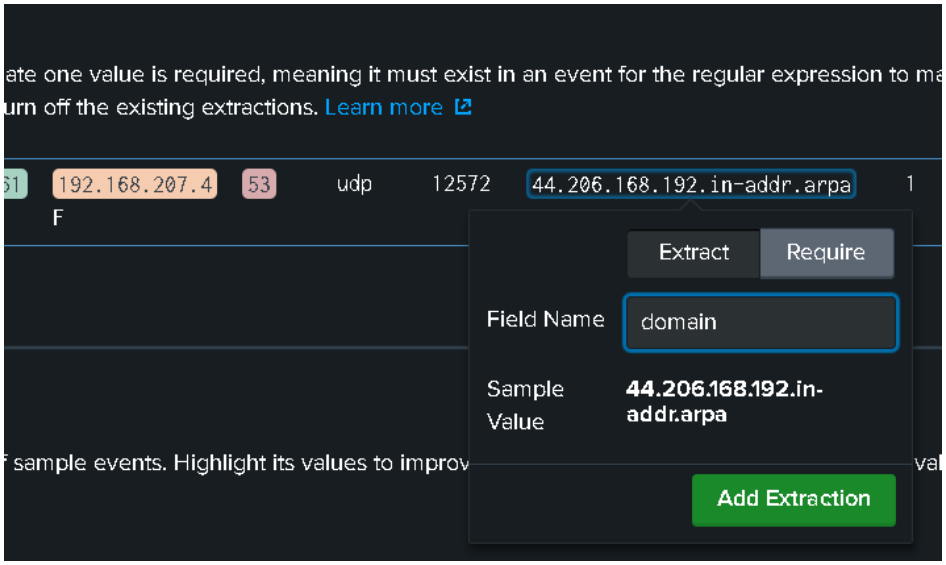
Selecting 192.168.207.4 as destination ip dst_ip

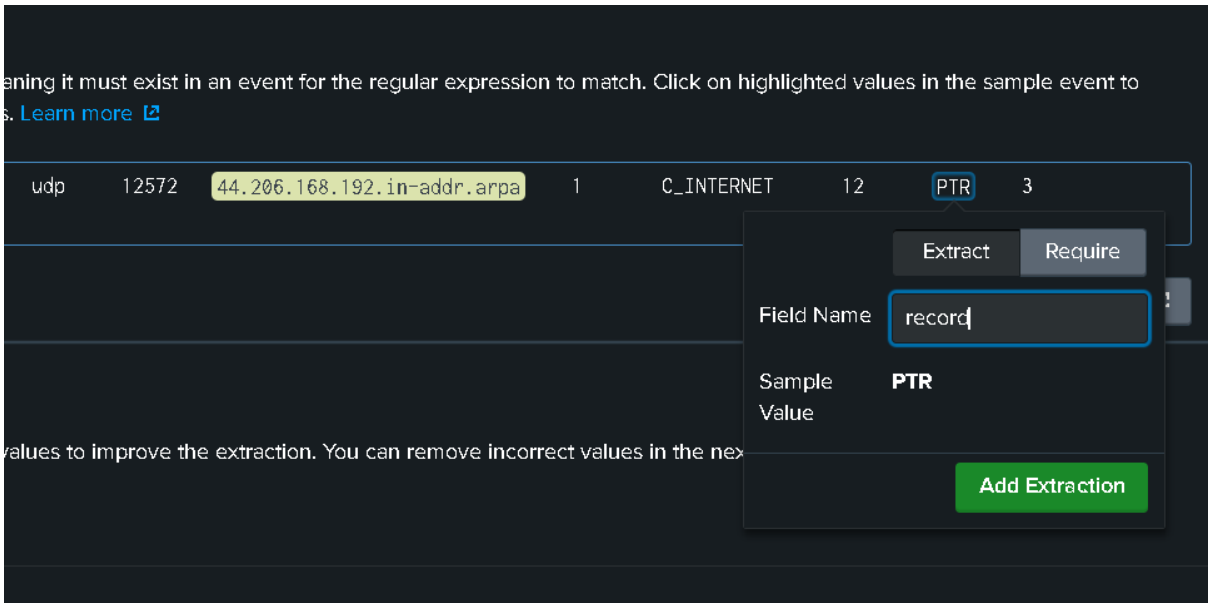


And 53 the dns server port

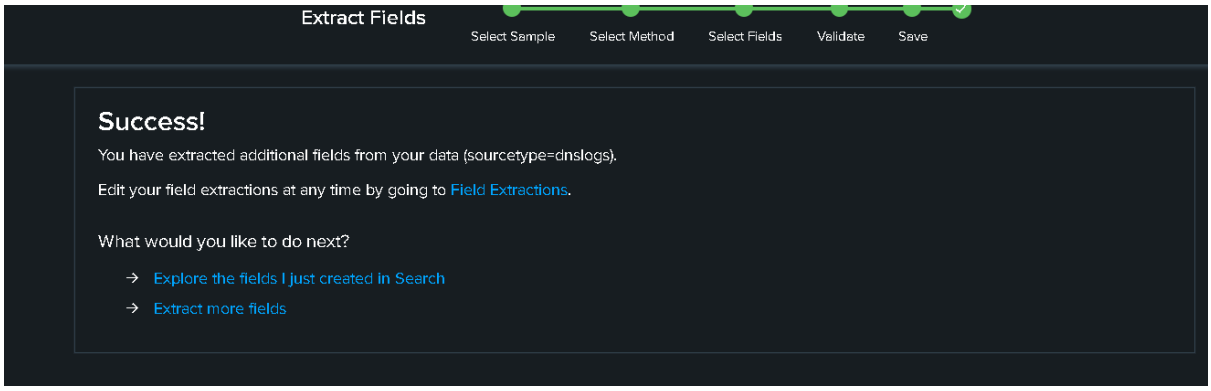


44.206.168.192.in-addr.arpa is the domain name



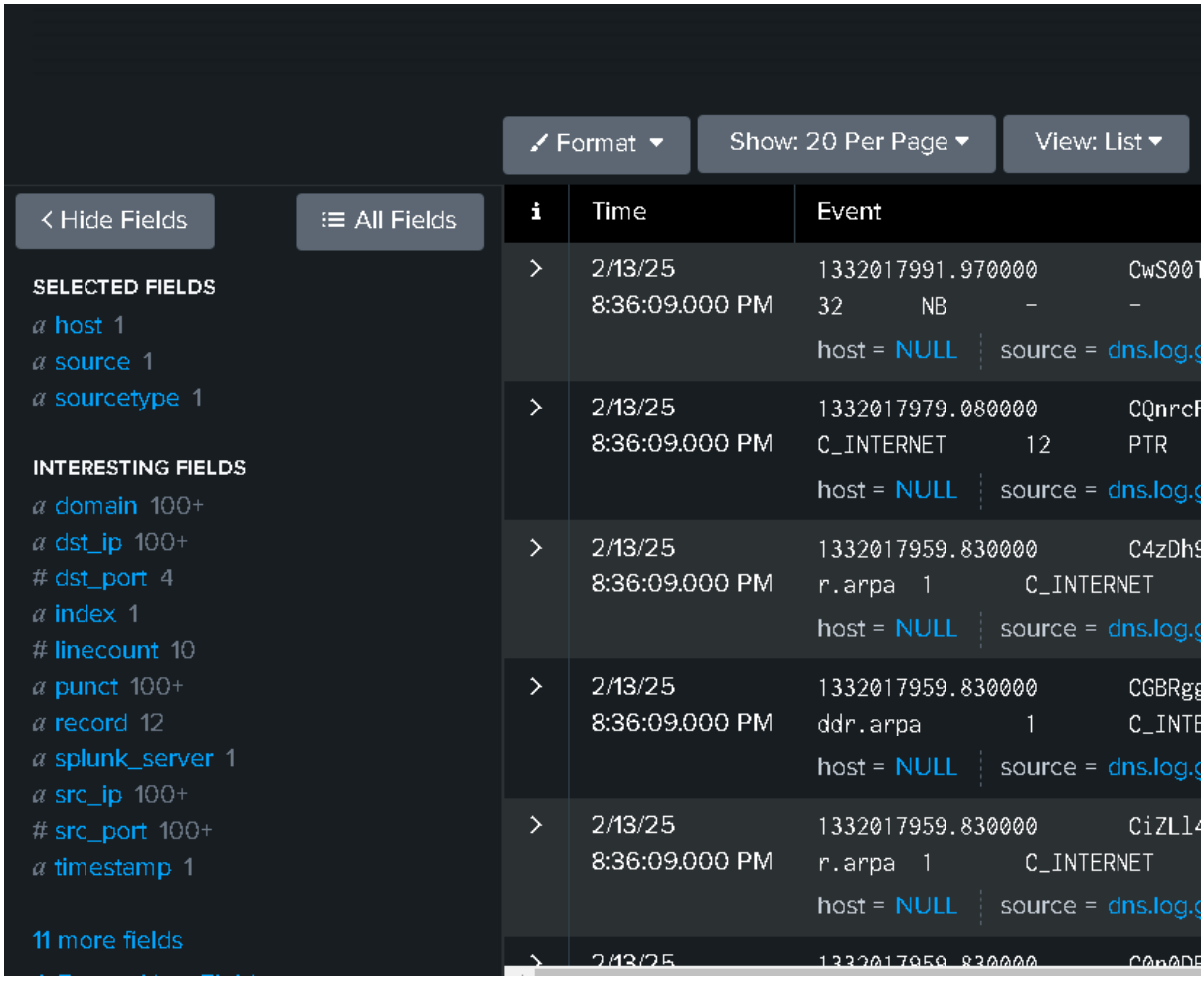


PTR - Type of record

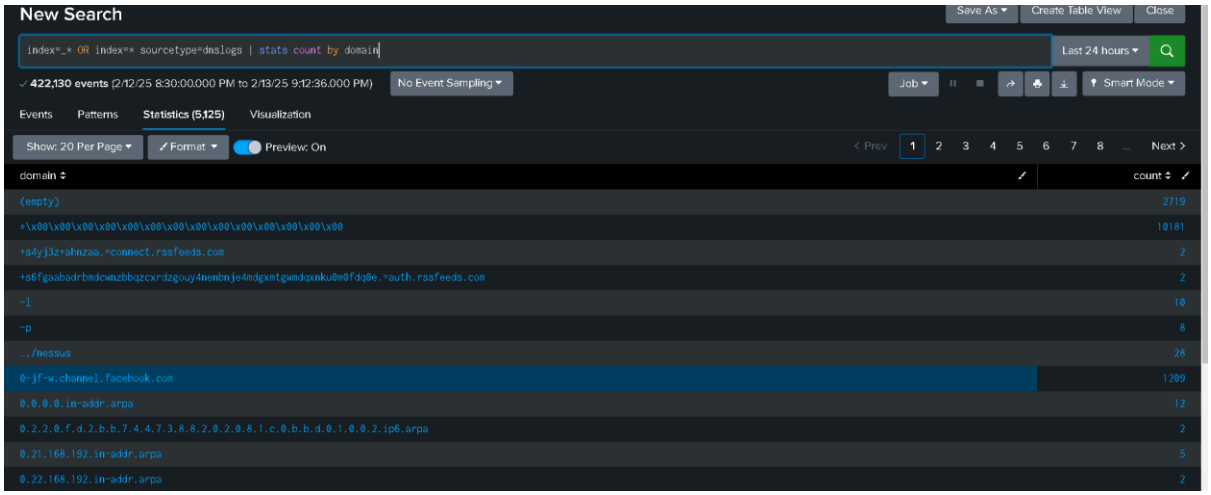


Successfully extracted the field from log

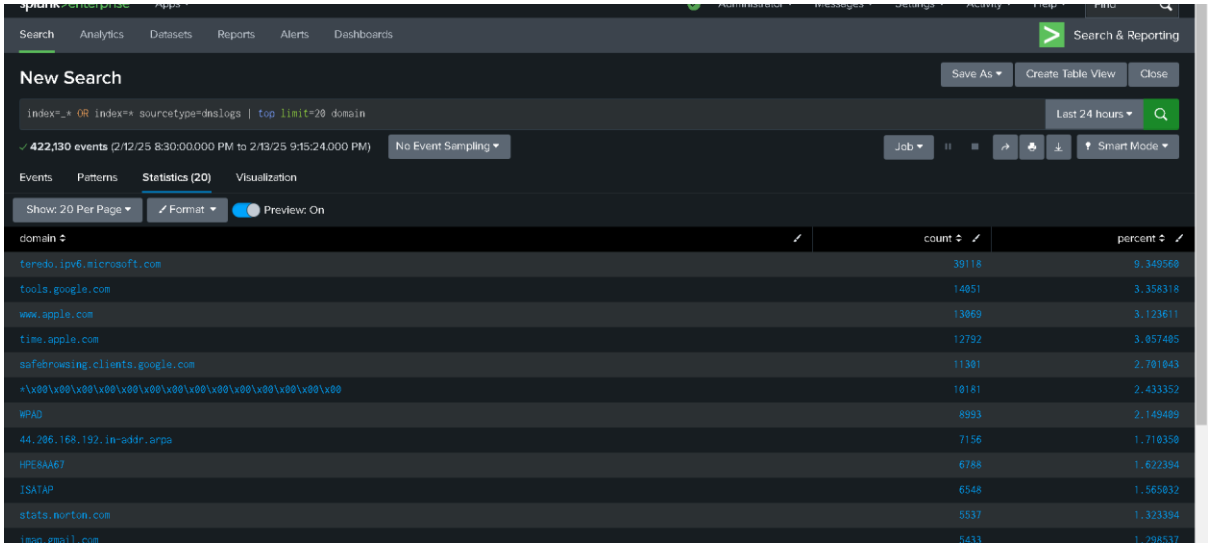
The extracted field lists are now on the interesting fields list



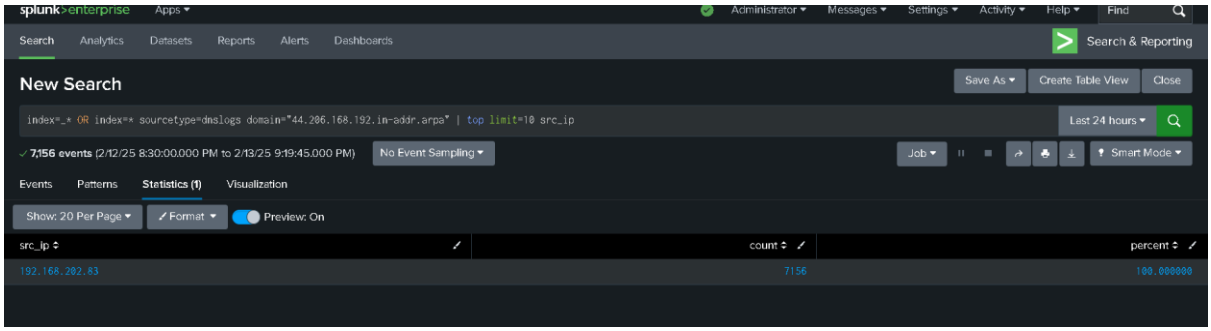
Stats count by domain name



Using top filter



Now checking which source ip has requested more on specific domains



From this we can suspect that 192.168.202.83 as the compromised machine

Table view of source ip, destination ip and ports