Analysis of Apache logs using grok filter and geoip plugins

## Logstash Configuration:

input{

beats {

port => "5044"

}

}

filter {

grok {

match => {

"message" => '%{IPORHOST:clientip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "%{WORD:verb} %{DATA:request} HTTP/%{NUMBER:httpversion}" %{NUMBER:response:int} (?:-|%{NUMBER:bytes:int}) %{QS:referrer} %{QS:agent}'

}

}

}

geoip {

source => "clientip"

}

}

output{

stdout{ codec => rubydebug }

elasticsearch{

hosts => ["http://localhost:9200"]

index => "filebeat-logstash-grok"

}

}

# Parsing logs with Grok filter plugin:

The grok filter plugin enables you to parse the unstructured log data into something structured and queryable because the grok filter plugin looks for patterns in the incoming log data, configuring the plugin requires you to make decisions about how to identify the patterns that are of interest to your use case.

# Enhancing data with Geoip filter plugin:

In addition to parsing log data for better searches, filter plugins can derive supplementaryinformation from existing data. As an example, the geoip plugin looks up IP addresses, derives geographic location information from the addresses, and adds that location information to the logs.

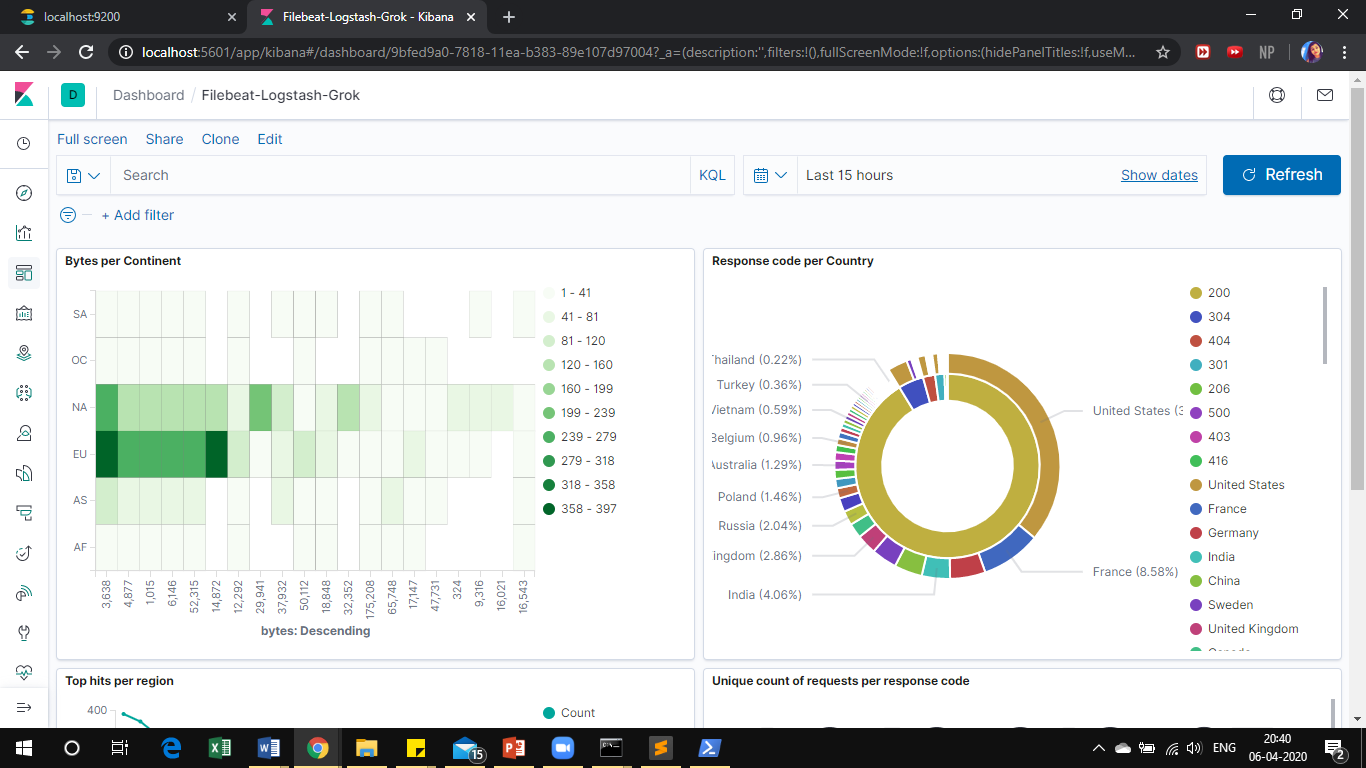
Configure your Logstash instance to use the geoip filter plugin by adding the following lines to the filter section of the Logstash.conf file:

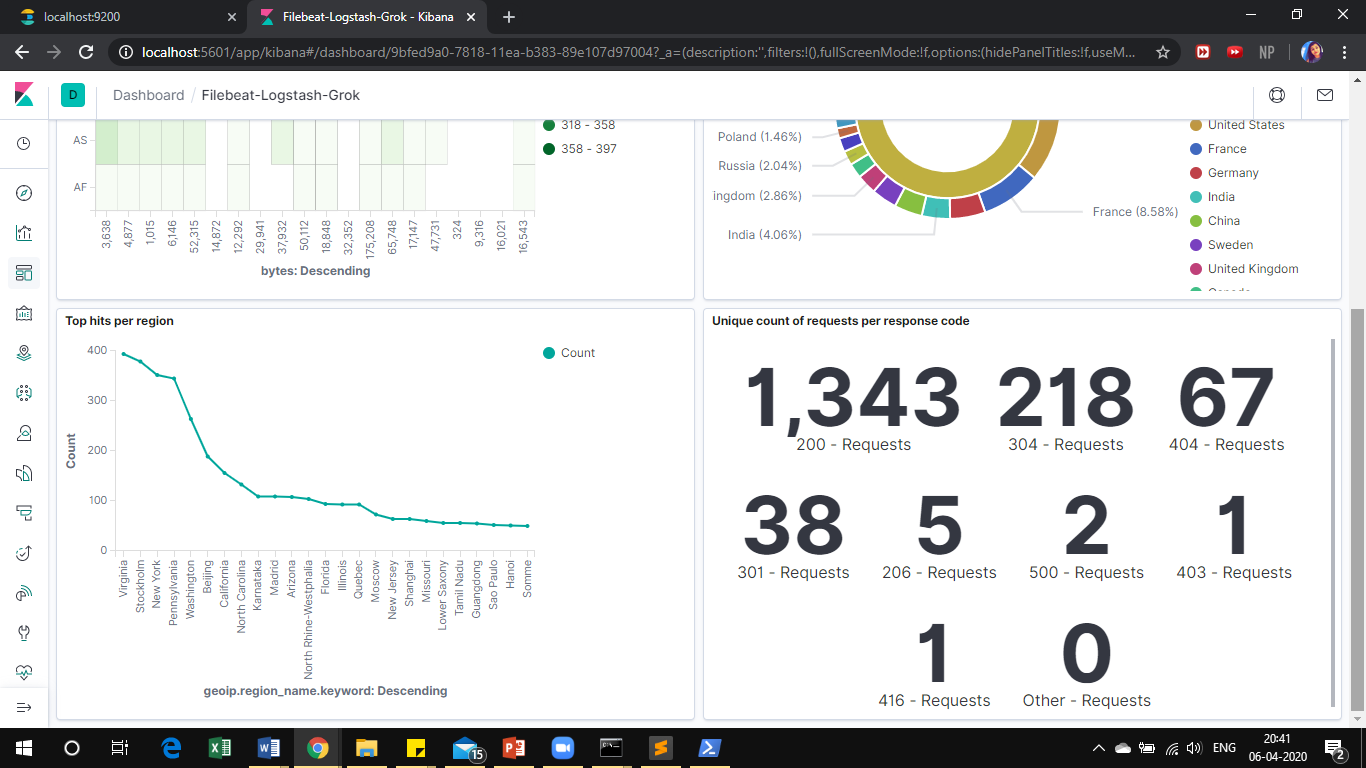
**geoip {**

**source => "clientip"**

**}**

The geoip plugin configuration requires you to specify the name of the source field that contains the IP address to look up.

****

****Analysis of Covid-19 dataset (Logstash-File input)

Logstash configuration:

input{

file{

path => "D:/Projects/ELK/covid19cases.csv"

start\_position => "beginning"

sincedb\_path => "NULL"

}

}

filter{

csv{

separator => ","

columns => ["Table Names","Case\_Type","Cases","Difference","Date","Country\_Region","Province\_State","Admin2","FIPS","Combined\_Key","Lat","Long","Prep\_Flow\_Runtime","Latest\_Date"]

}

}

output{

elasticsearch{

hosts => ["http://localhost:9200"]

index => "covid19us"

}

stdout{}

}

