**ELK Stack**

**What is the ELK Stack?**

The ELK Stack is a collection of three open-source products i,e Elasticsearch, Logstash, and Kibana.

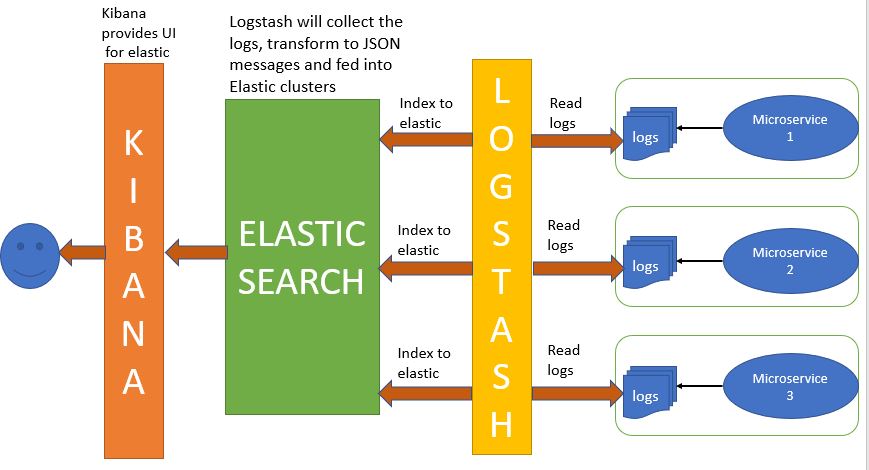
* E - ElasticSearch: used for storing logs.
* L - LogStash : used for both shipping as well as processing and storing logs.
* K - Kibana: is a visualization tool (a web interface)

ELK Stack is designed to allow users to take to data from any source, in any format, and to search, analyze, and visualize that data in real time.

ELK provides centralized logging that be useful when attempting to identify problems with servers or applications. It allows you to search all your logs in a single place. It also helps to find issues that occur in multiple servers by connecting their logs during a specific time frame.

## ELK Stack Architecture

Here is the simple architecture of ELK stack



* Logs: Server logs that need to be analyzed are identified
* Logstash: Collect logs and events data. It even parses and transforms data
* ElasticSearch: The transformed data from Logstash is Store, Search, and indexed.
* Kibana: Kibana uses Elasticsearch DB to Explore, Visualize, and Share

## What is Logstash?

Logstash is the data collection pipeline tool. It collects data inputs and feeds into the Elasticsearch. It gathers all types of data from the different source and makes it available for further use.

Logstash can unify data from disparate sources and normalize the data into your desired destinations. It allows you to cleanse and democratize all your data for analytics and visualization of use cases.

## What is Elasticsearch?

## Elasticsearch is a NoSQL database. It is based on Lucene search engine, and it is built with RESTful APIS. It offers simple deployment, maximum reliability, and easy management. It is helpful for executing a quick search of the documents. Elasticsearch also allows you to store, search and analyze big volume of data. It is mostly used as the underlying engine to powers applications that completed search requirements.

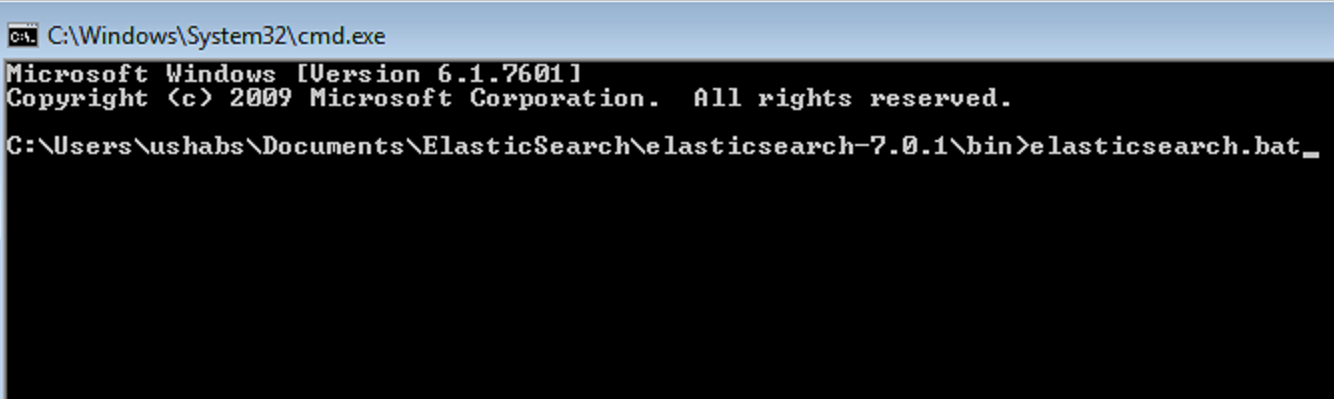
## What is Kibana?

## Kibana is a data visualization which completes the ELK stack. This tool is used for visualizing the Elasticsearch documents and helps developers to have a quick insight into it. It can be used for search, view, and interact with data stored in Elasticsearch directories. Kibana helps you to perform advanced data analysis and visualize your data in a variety of tables, charts, and maps.

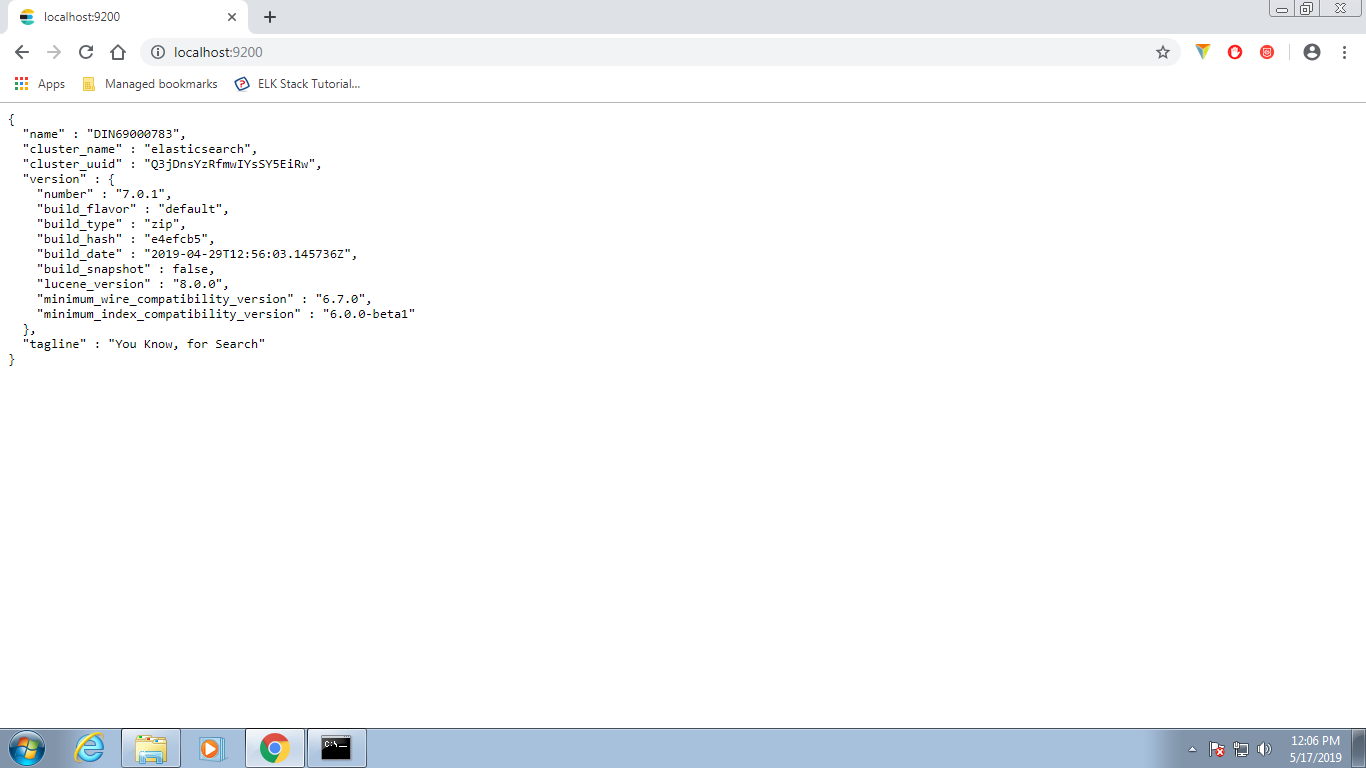
**Configuring ELK Stack:**

**Step1:First download latest versions of Elasticsearch , Kibana and logstash and unzip in one folder.**

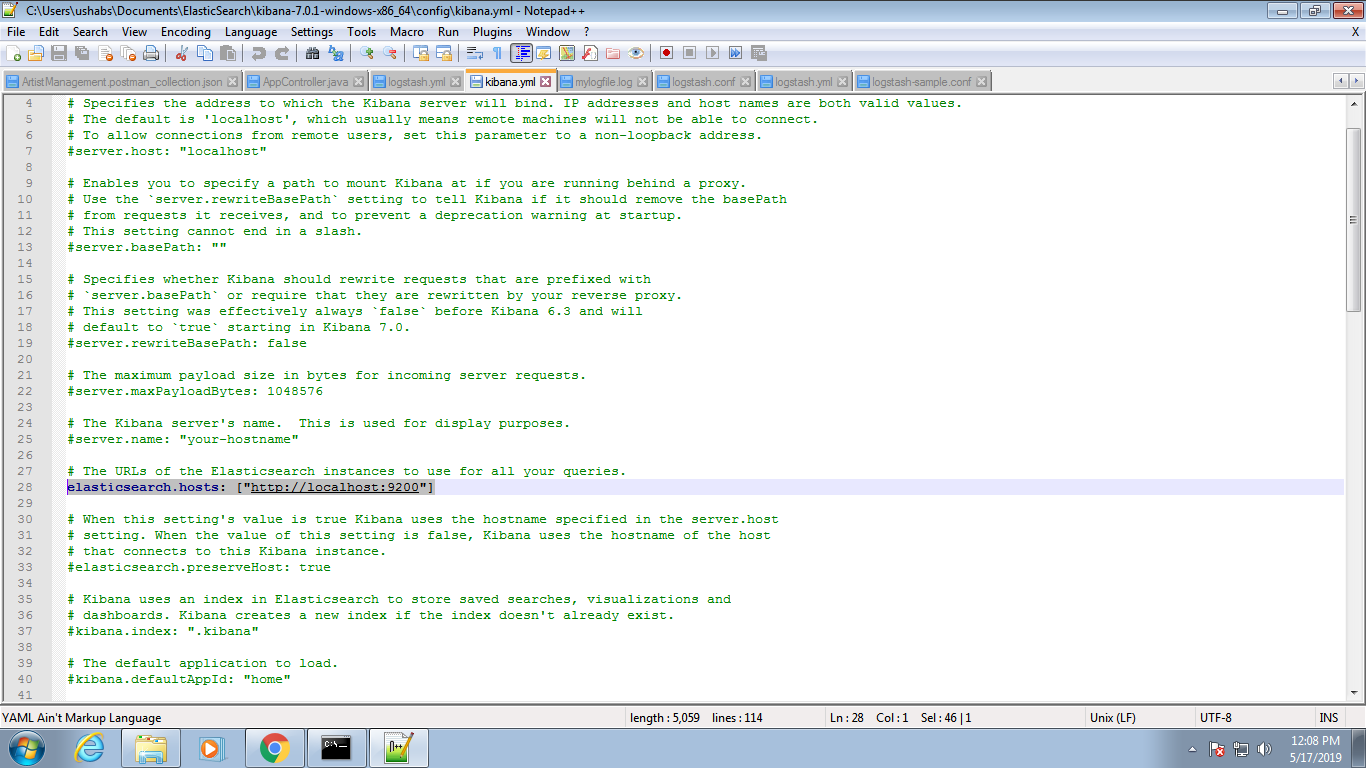
**Step2:Go to elasticsearch🡪bin🡪run elasticsearch.bat in cmd.**



**Step3:run localhost:9200**

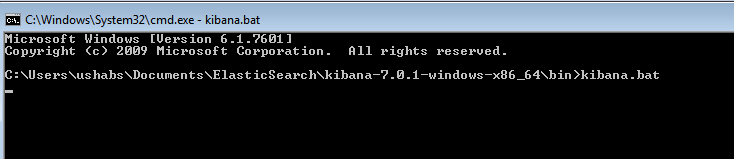


**Step4:Kibana🡪config🡪uncomment the localhost of elasticsearch in this file.**

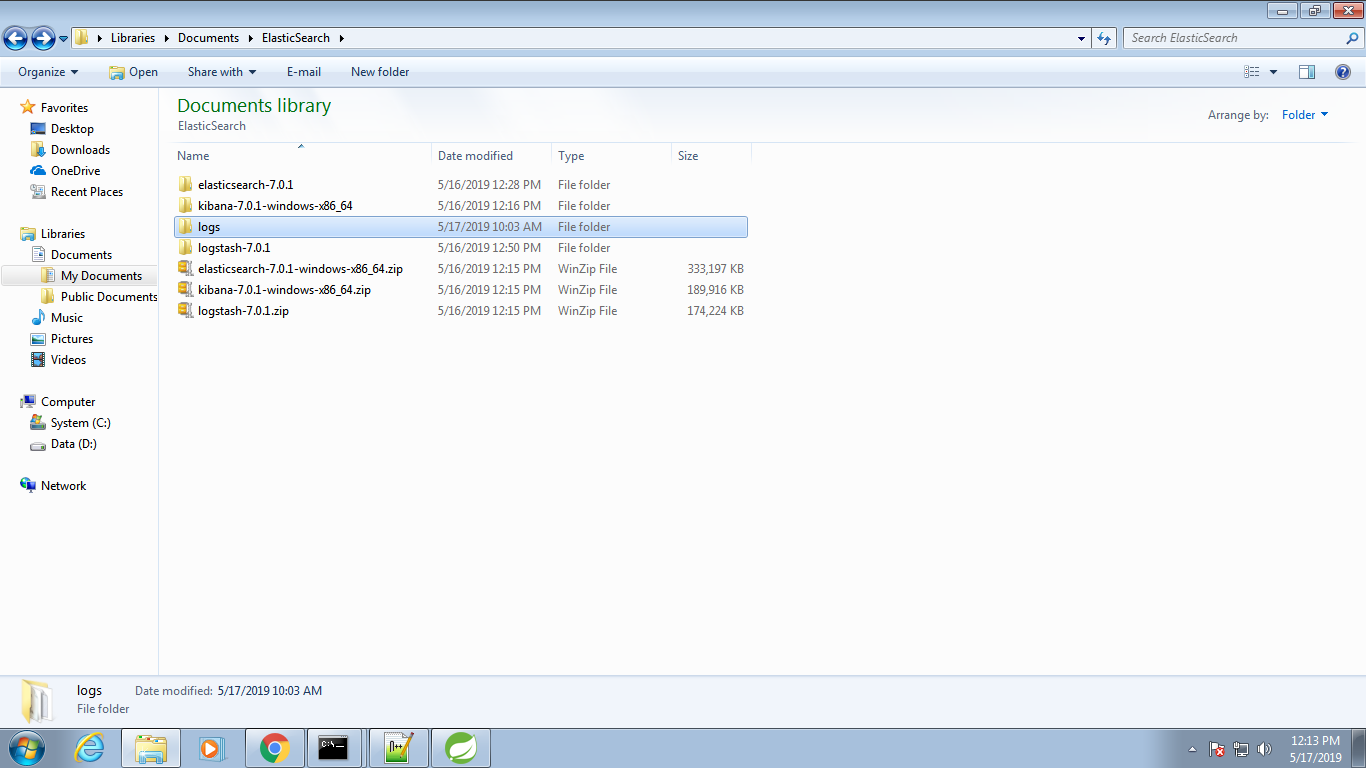


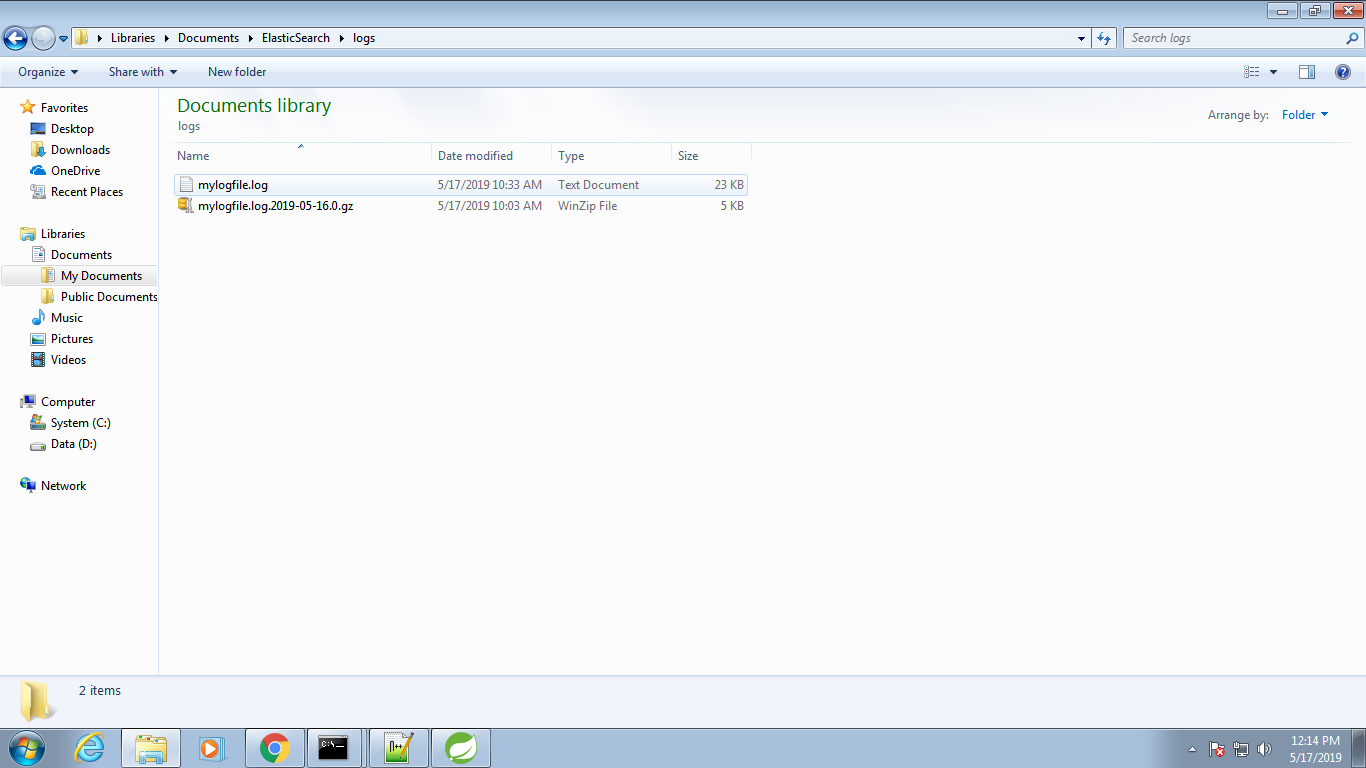
elasticsearch.hosts: ["http://localhost:9200"].

**Step5:kibana🡪bin🡪run kibana.bat in cmd**

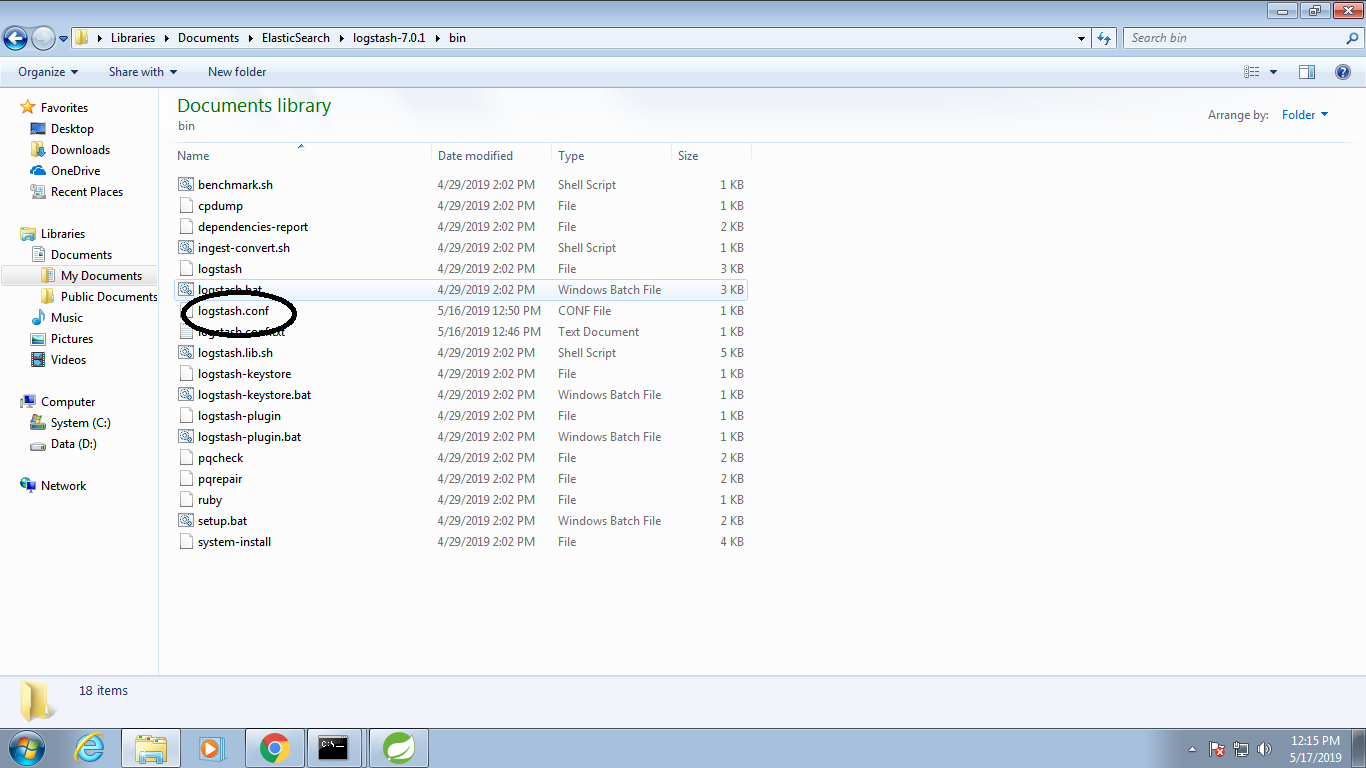


**Step6:create one folder by name logs and file with .log extension where the logs will be stored.**

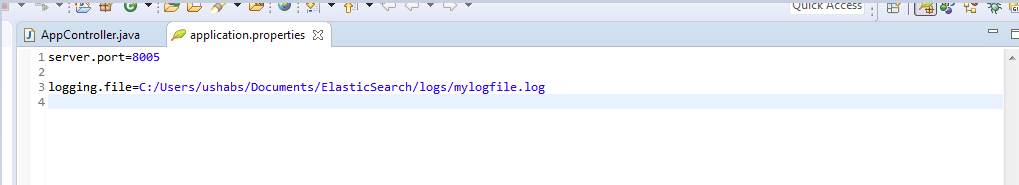




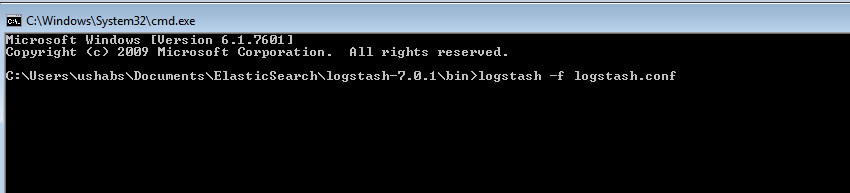
**Step7:create configuration file in logstash🡪bin🡪config file.**



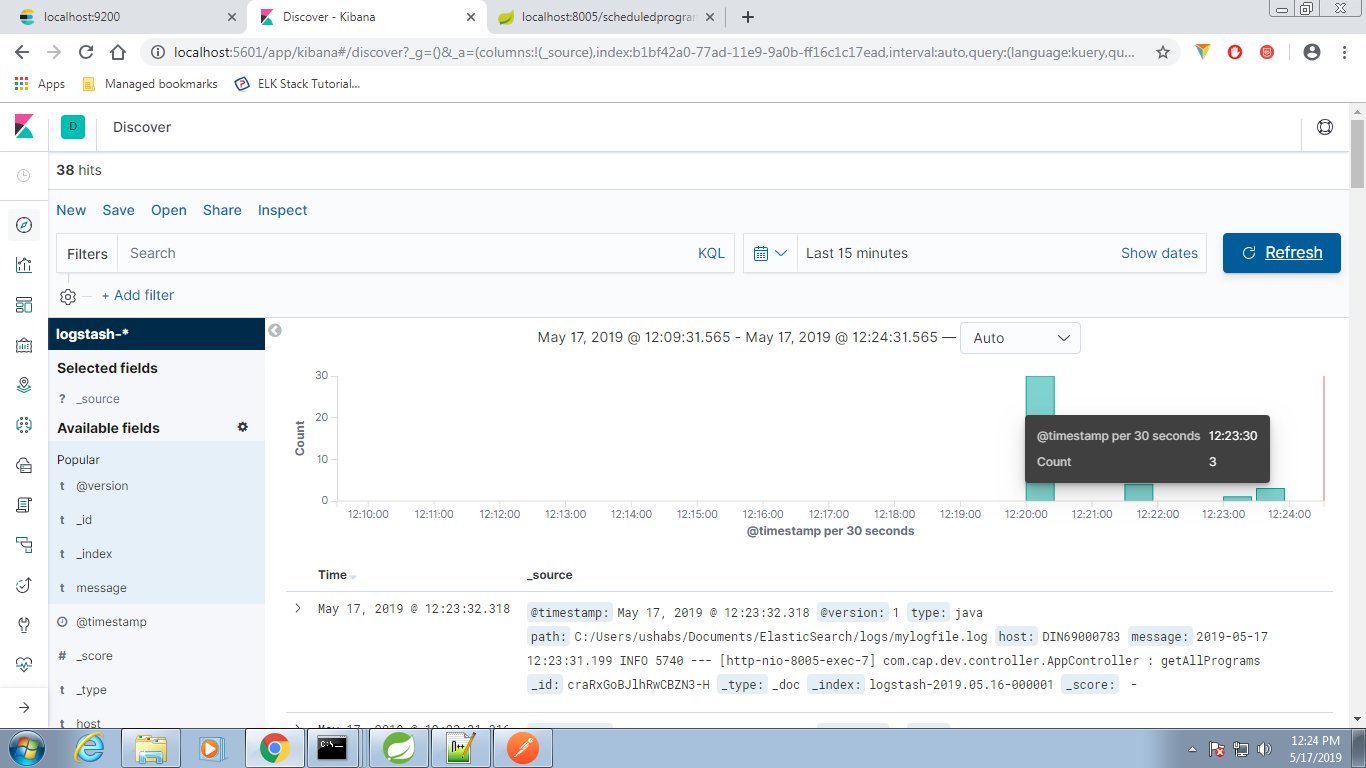
**Step8:give the path in your application.**



**Step9:logstash🡪b9in🡪cmd🡪run the command logstash –f logstash.conf.**



**Step10:Hit the request in postman/browser and test the logs in kibana dashboard.**



Here it shows the number of times requested and we can filter the logs based on version ,id,timestamp,message,host etc

Role of kibana in ELK