```
============
ELK Stack
============

=> ELK is the combination of 3 open source products

1) Elastic Search   : It is used to store and process logs

2) Logstash  : It is used to collect application logs and store in Elastic Search

3) Kibana : It will provide user interface to monitor application logs

=> By using the above 3 products we can implement Log Aggregation and Logs Monitoring


===========
ELK Setup
===========

1) Download ELK Softwares

                =>  Elastic Search : https://www.elastic.co/downloads/elasticsearch

                =>  Kibana : https://www.elastic.co/downloads/kibana

                =>  Logstash : https://www.elastic.co/downloads/logstash

2) Extract all zip files

3) Run elasticsearch using elasticsearch.bat file (make sure all security settings disable in
elasticsearch.yml before running)

                $ elasticsearch.bat

4) Check Elastic Search Running or not (URL  : http://localhost:9200/ )

5) Run kibana using kibana.bat file (before running kibana, enable elasticsearch url in kibana.yml
file)

                $ kibana.bat

6) Check Kibana running or not ( URL : http://localhost:5601/app/home )

7) Run Spring Boot Application and generate log file with log messages

8) create logstash.conf file like below

# Sample Logstash configuration for creating a simple
# Beats -> Logstash -> Elasticsearch pipeline.

input {
  file {
        path => "C:/Users/ashok/classes/22-JRTP/workspace/SpringBoot_REST_API/app.log"
        start_position => "beginning"
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
  }
}

9) Run logstash server using below command
```

```
$ logstash -f logstash-sample.conf
```

10) Check logstash server is running or not (http://localhost:9600)

11) Check application logs in Kibana dashboard