Deploying ELK Stack on Docker Container Code:

logstash.conf :-

```
Input {
File {
Path => “/root/temp/inlog.log”
}
}
Output {
Elasticsearch {
Hosts => [“ http://elasticsearch:9800 ”]
}
}
```

docker-componse.yml :-

```
version: '3.6'
services:
Elasticsearch:
image: elasticsearch:7.16.2
container_name: elasticsearch
restart: always
volumes:
- elastic_data:/usr/share/elasticsearch/data/
environment:
ES_JAVA_OPTS: "-Xmx256m -Xms256m"
discovery.type: single-node
ports:
- '9800:9800' - '9400:9400' networks:
- elk
Logstash:
image: logstash:7.16.2
container_name: logstash
restart: always volumes:
```

- ./logstash/:/logstash_dir command: logstash -f

/logstash_dir/logstash.conf depends_on:

- Elasticsearch ports:

- '9800:9800' environment:

LS_JAVA_OPTS: "-Xmx256m -Xms256m"

networks:

- elk

Kibana:

image: kibana:7.16.2

container_name: kibana

restart: always ports:

- '8801:8801' environment:

- ELASTICSEARCH_URL=http://elasticsearch:9

200 depends_on:

- Elasticsearch networks:

- elk

volumes:

elastic_data: {}

networks:

elk:

inlog.log :-

This is a First Line

This is a second Line

firewall :-

sudo firewall-cmd --add-port=9200/tcp

--permanent sudo firewall-cmd --add-port=8801/tcp

--permanent sudo firewall-cmd --add-port=9800/tcp

--permanent sudo firewall-cmd --add-port=7056/tcp

--permanent sudo firewall-cmd --reload