Normal | **B** *I* S̶ U̲ | ☰ ☰ ☰ | 🖼 🔗 — | " ⓐ </> 🅰 I̶ₓ | •••

- ☐ **ELK** = Elasticsearch, Logstash, and Kibana.
    - ☐ **Elasticsearch** is a search and analytics **engine**.
    - ☐ **Logstash is a server-side data processing pipeline** that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch.
    - ☐ In Spring boot project **Logstash is configured with Log4j** to send logs to Elasticsearch.
    - ☐ **Kibana lets users visualize data** with charts and graphs in Elasticsearch.
- ☐ Java project `08-spring-elk` is on github
- ☐ create network

```
docker network create spring-elk-net
```

- ☐ Create spring boot image for project `08-spring-elk`
- ☐ build images

```
mvn clean package -DskipTests
```

- ☐ Start containers

```
docker compose up -d
docker compose logs -f
```

- ☐ Elasticsearch & Kibana *index* vs *index pattern*
- ☐ Access Kibana page and try to create new *index pattern*, it doesn't work because no index is created (registered)

```
http://localhost:5601/app/management/kibana/indexPatterns/create
```

- ☐ Start spring boot app, it will create the index in Elastic Search

```
mvn clean spring-boot:run
```

- ☐ Create index pattern (from the index created) with name `spring-boot-elk-logs-*` (name configurable in logstash.conf in Spring Boot project) from the Kibana page
- ☐ Access Discover page and search logs by "message" (using like (*) operator) and "level" filters

```
http://localhost:5601/app/discover
```

- ☐ Read logs
    - ☐ endpoint of spring boot app

```
http://localhost:8080/elk/hello
```

    - ☐ from app startup and from endpoint calls. Restart app multiple times and make new calls. See logs in Kibana from ElasticSearch index - Blue refresh button.
    - ☐ select all fields or only some of them (ex. message, level) for the result set, log entry fields example: id, message, logger_name, _index (in elasticsearch), level
- ☐ in spring boot project 08-spring-elk = 2 external params that make him find the Logstash container in the spring-elk-net network. They are set in docker-compose.yml

```
${LOGSTASH_SERVICE_REMOTE_HOST:localhost}
${LOGSTASH_SERVICE_REMOTE_PORT:5000}
```

    - ☐ Attempt failed but
        - ☐ it's not necessary because if centralized logging is required into an elastic search server outside the container group, than for logstash container the url of the elastic search server can be changed in XPACK_MONITORING_ELASTICSEARCH_HOSTS variable in docker-compose.yml.
        - ☐ Of course in this context kibana container can be outside the container group as well and it connects to elastic search server with the ELASTICSEARCH_HOSTS variable in docker-compose.yml.
- ☐ Current commit of `08-spring-elk` : 1e2ffcdae886b77d992ee60638d341158bea8da5
- ☐ Works in **Git Bash** not in CMD. One liner to stop / remove all of Docker

☐ containers:

```
docker stop $(docker ps -a -q)
docker rm $(docker ps -a -q)
```

☐ images

```
docker rmi -f $(docker images -a -q)
```

☐ Check Docker Desktop after starting containers