**Present System**

A spring boot application is created. It contains a class called 'User.java' in spring boot with two fields, 'id' and 'name'. There is a controller class named 'ElkStackExampleApplication.java', with a method, which will return list of objects for user. From controller, based on the id, it fetches the user from the list. If there is no user object with that id, return null and throw exception.

Elastic search batch file is run and kibana is configured. It takes a couple of second to up the nosql elasticsearch database. Now go to kibana folder. We open the 'kibana.yml' file to configure. We want to inform kibana where our elasticsearch is running. Now go to bin folder. There will be a 'kibana.bat' batch file. Then kibana and elasticsearch is verified in the browser using ‘localhost’ with their respective ports.

Then we generate the log file of this application. In 'logstash.conf', we gave input, filter and output. In input, the file path is given and the start\_position as 'begginning'. In output section, we are giving the log from specified path of input to elasticsearch. In logstash console, you will be able to see logs with timestamp.

Now in kibana console we create index pattern. We go to management. Click on 'create an index pattern'. Give the index name which is current time stamp index. We do nnot enable the time filter. Now we will be able to see all logs in kibana console. Using ‘discover’ in kibana we will see the index pattern.

**Proposed System**

Develop a spring boot application. Create a class called 'User.java' in spring boot with two fields, 'id' and 'name'. Then create a controller class named 'ElkStackExampleApplication.java'. There write a method, which will return list of objects for user. From controller, based on the id, fetch the user from the list. If there is no user object with that id, return null and throw exception.

Before developing this application, run the elasticsearch batch file. Also configure the kibana.yml file. Type 'cmd' to run that. In prompt type 'elasticsearch.bat'. It will take a couple of second to up the nosql elasticsearch database. Now go to kibana folder. Go to the config folder. Open 'kibana.yml' file to configure. Scroll down a bit. There you will find a localhost line. Uncomment that line. We want to inform kibana where our elasticsearch is running. Now go to bin folder. There will be a 'kibana.bat' batch file. Open command prompt and run kibana.bat in it. To verify elasticsearch, go to browser and type 9200 localhost. There you will see a response. To verify kibana console, check in prompt it's port no. and go to browser. There you will see an interactive kibana dashboard.

After that generate the log file of this application. To generate log file in logstash, go to application.yml and type their 'logging' and specify the file and give file path of logs and give name of log-file, 'elk-stack.log'. Go to logstash folder, go to bin, and run the logstash batch file. In 'logstash.conf', give input, filter and output. In input, specify the file path and start\_position as 'begginning'. In output section, we are giving the log from specified path of input to elasticsearch. Mention the elasticsearch host port there

Download and unzip the logstash. Then create a 'logstash.conf' file. Inside that config file, we need to tell out logstash, where our log-file is located. Copy this conf file into bin folder of logstash and paste file. Now type command and run the 'logstash.bat' file. Then give file name, which is 'logstash.conf'. The command is 'logstash -f logstash.conf'.

There you can get the logstash running port. Now try to hit the API and get user info, with valid and invalid id's.

In logstash console, you will be able to see logs with timestamp.

Now go to kibana and create index pattern with the same index. To create your own index, you need to make changes in 'logstash.conf' file, by giving index in output folder.

To create index pattern go to management. Click on 'create an index pattern'. Give your index name which is current time stamp index. You may or may not enable the time filter. Now will be able to see all logs in kibana console. Click on 'Discover'. There you will see your index pattern.

**Data Implementation and program execution**

First download the three components which are elasticseach, logstash and kibana.

Go the downloaded folder. Go to bin. There will be a batch file, named elasticseach.bat.

Type 'cmd' to run that. In prompt type 'elasticsearch.bat'. It will take a couple of second to up the nosql elasticsearch database.

Now go to kibana folder. Go to the config folder. Open 'kibana.yml' file to configure.

Scroll down a bit. There you will find a localhost line. Uncomment that line. We want to inform kibana where our elasticsearch is running.

Now go to bin folder. There will be a 'kibana.bat' batch file. Open command prompt and run kibana.bat in it.

To verify elasticsearch, go to browser and type 9200 localhost. There you will see a response.

To verify kibana console, check in prompt it's port no. and go to browser. There you will see an interactive kibana dashboard.

Create the spring boot application and the two APIs. One will fetch the user info and other will produce error.

To generate log file in logstash, go to application.yml and type their 'logging' and specify the file and give file path of logs and give name of log-file, 'elk-stack.log'.

Go to logstash folder, go to bin, and run the logstash batch file.

In 'logstash.conf', give input, filter and output. In input, specify the file path and start\_position as 'begginning'. In output section, we are giving the log from specified path of input to elasticsearch. Mention the elasticsearch host port there

Download and unzip the logstash. Then create a 'logstash.conf' file. Inside that config file, we need to tell out logstash, where our log-file is located.

Copy this conf file into bin folder of logstash and paste file. Now type command and run the 'logstash.bat' file. Then give file name, which is 'logstash.conf'. The command is 'logstash -f logstash.conf'.

**System Testing**

Copy the URL 'get\_user'. Check the port form application.yml file, which is 9898 in this case. Type 'localhost:9898/get\_user/3'. If we have user id, it will display in browser. If we type a user id which is not present, the console will show exception with the error message.

In logstash running port, '9600'. Now try to hit the API and get user info, with valid and invalid id's.

Go to browser. Type 'localhost:9200/cat', to verify indexes. There you will find 'indices'. Type it as 'localhost:9200/cat/indices', there you will find index internally created by elk.

For logging purpose, the logstash with current time-stamp was created. You can view that content in kibana console. Copy that, and give that index 'localhost:9200/logstash-202004-05-000001' and seacrh it. You will see logs.