International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

Live Log Query Analysis

Nayana N. Ghuikar, Prof. Shraddha A. Kale

Department of Computer Science and Engineering, Rajshri Shahu College of Engineering Buldhana443001, Maharashtra India

Department of Computer Science and Engineering, Siddhivinayak Technical Campus College of Engineeringand Technology Shegaon444203, Maharashtra India

Submitted: 15-06-2022 Revised: 25-06-2022 Accepted: 27-06-2022

ABSTRACT-- Utilizing logs to identify and analyse issues in computer program frameworks is now not an attainable human handle. The ever expanding sum of by present day frameworks calls for more progressed strategies to empower log query Analysis. As applications and framework components are getting to be greater more complex, and quicker, the going with increment in log information delivered is obvious. Whereas in prior days human administrators were able to diagnose issues by hand utilizing the logs, this not applies to today's frameworks. The ever expanding estimate of frameworks has come about in present-day applications that effectively produce millions of log messages on a day by day premise. It has been expressed that human translation is not do able on this scale and robotized approaches have gotten to be a need. This is troublesome for professionals to recognize what is significant for them, and for analysts to decide curiously points to investigate. Presently we are reaching to propose a framework system that encourages successful log analysis. **Keywords:** PyCharm, ElasticSearch, Django, Kibana.

I. INTRODUCTION

Logging within the field of computer science is the hone of recording occasions that give data approximatelythe execution of an application. Log messages are a viable way to induce what has happened amid the execution of a generation framework to analyse issues viably. In a test setting a engineer can investigate an application to find the beginning of a disappointment. In any case, in a live execution environment investigating isnow not doable due to the ever expanding complexity of frameworks. In expansion, making core dumps to analyse issues in expansive applications isn't doable any longer for the same reason. This underlines the significance of logs and their application is nearly any framework.

Logging within the field of computer science is the hone of recording occasions that give data around the execution of an application. Log messages are a compelling way to gather what has happened amid the execution of a generation framework to analyze issues successfully. In a test setting a designer can investigatean application to find the beginning of a disappointment. Be that as it may, in a live execution environment investigating is now not attainable due to the ever expanding complexity of frameworks. In expansion, making core dumps to analyze issues in huge applications isn't attainable any longer for the same reason. This underlines the significance of logs and their application is nearly any framework. Presently we propose frameworks that encourage successful log query Analysis. Our framework is empowering conclusion to bargain with millions of log messages. In expansion to this, endeavours are made to consequently identify failures and inconsistencies. We display a diagram of the current state of the craftsmanship of log examination in investigate. With this outline we endeavour to donate experiences into the work concerned with managing with huge numbers of logs. In addition, the objective is to layout the conceivable outcomes to extricate the required data from logs, e.g., failures or inconsistencies. [1]

II. LITERATURE REVIEW

Applications have logged framework occasions since the starting of the computer time. It is be that as it may hazy what the primary prove of logging is. Logs have an application in a wide extend of diverse areas. There were more logs to analyze Workingframeworks kept isolated logs for assignments like boot-up and framework occasions.

Application frequently kept their possess logs, as well, in spite of the fact that not fundamentally in a centralized area. For this

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

reason, logging may be a non-specific point indeed when scoped application logging. They experienced an assortment of terms to indicate logs that are either equivalent words or covering in meaning. To evacuate a few equivocalness and disarray. They go through the contrasts and utilize this to scope the overview.

In expansion, program organizations were beginning to end up dispersed, expanding the significance of farther log accumulation. These requests driven to the creation of a modern era of log query Analysis devices, such as syslog-ng and rsyslog, which debuted in 1998 and 2004, individually. These two devices advertised the pivotal highlight of supporting log collection over the arrange. At the same time, a reiteration of exclusive log query Analysis instruments emerged within the Windows world, with numerous of them devoted to particular assignments. For case, there was BootHawk which bolstered examination of boot and log information in arrange to make strides startup and login times for Windows frameworks. [2]

III. ANALYSIS OF PROBLEM

i. Problem Statement

In prior days human administrators were able to analyze issues by hand utilizing the logs, this now not applies to today's frameworks. Since applications and framework components are getting to be greater, more complex, and quicker, the going with increment in log information created is obvious. The ever expanding measure of frameworks has come about in present-day applications that effectively create millions of log messages on a day by day basis. It has been expressed that human elucidation is now not doable on this scale and computerized approaches have gotten to be a need. In a testing a developer can debug an application to locate the origin of a failure but now days it becomes impossible because complexity of application are increased rapidly and parsing logs to check a specific issue is a very tough task.

Solution on Problem

Here we created two solutions for above problem that are

i. Using Search Engine (Elasticsearch)

In this approach log file is core of our system. Log file is parsing using different delimiters to create a JSON objects. A created JSON file passes to django server, which passes the file to Elasticsearch search engine. Elasticsearch search engine creates the index of JSON file histogram, line graph, etc. Kibana has inbuilt function for filter. There are multiple filters in kibana such as timestamp, id, method, message, method, level, etc. Which helps to detect anomalies and failures within the application?

ii. **Using Database (Mongo DB)**

The log file on which we want to work is in present in our folder or not. If it is present then there is no need to open and save file in our system, otherwise you must open and save log file using interface.

Once you got log file in system then parse using parse button using interface. The parse button creates a database in MongoDB in form of JSON object. For viewing database we provide one view button on interface.

There is one more option name as filter. Filters are main part of system because it provides filter out data which is helpful to detect anomalies and failure within application.

IV. DESIGN PROCESS

i. Design of Solution 1(By Using Elastic SearchSearch Engine)

Log messages are an effective way to infer what has happened during the execution of a production system to diagnose problems effectively. In earlier days human operators were able to diagnose problems by hand using the logs; this no longer applies to today's systems. But now day's applications easily generate millions of log messages on a daily basis.

Algorithm

Step 1: Start

Step 2: Execute ElasticSearch search engine on localhost 9200.

Step 3: Run Django server on localhost 8000. Step 4: Run Kibana on localhost 5601.

Step 5: Apply filters.Step 6: Stop.

Kibana is visualization tool which is specially used for index representation in form of bar graph, pie chart,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

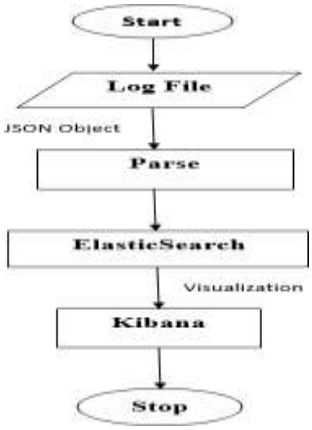


Figure 1: Flowchart of Live Log Query Software(Elasticsearch)

For easy understanding of log we can parse the log files and creates JSON object. Then created JSON object is pass to ElasticSearch search engine and dump into Django server. ElasticSearch pass the JSON file to Kibana for further processing. Kibana can create index for log file and visualize in different form such as Bar graph, line graph, Histogram, pie chart, etc. There are multiples inbuilt filters in Kibana. Filtersare applied on index to get filtered logs which helps to diagnose anomalies and failures.

ii. **Design of Solution 2 (By Using database MongoDB Database)**

In solution 2 we can create our own GUI for easy handling. GUI can be design by using Tkinter in python Tkinter is Python's de-facto standard GUI(Graphical User Interface)package. It is a thin object-oriented layer on top of Tk. Tkinter is not the only GUI Programming toolkit for Python It is however the most commonly used one.

Algorithm

Step 1: start.
Step 2: Interface will be displayed after executing python file.
Step 3: open and save the log file using Interface.
Step 4: click on parse button to parse and create database.
Step 5: click on view
Step 6: filter are applied using interface and display the filter data on interface.
Step 7: stop

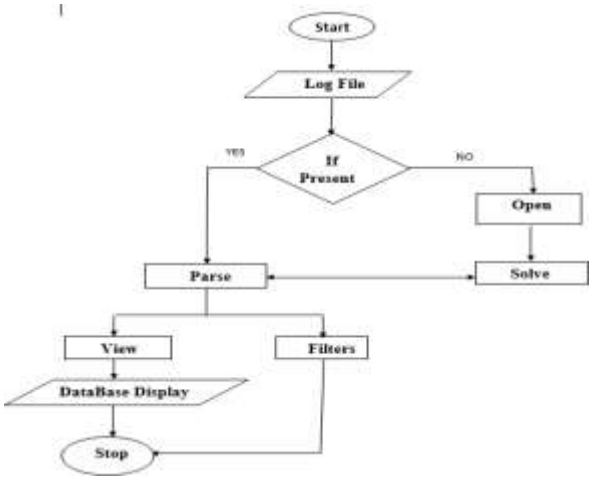


Figure 2: Flowchart of Live Log query softwareusing Mongodb

V. IMPLEMENTATION

i. **Installation steps for pyCharm**

PyCharm is a cross-platform editor developed by JetBrains. Pycharm provides all the tools you need for productive Python development. Below are the detailed steps for installing Python and PyCharm are as follow.

- **Python Installation:**

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

Step 1: To download and install Python visit the official website of Python http://www.python.org/downloads/ and choose your version. We have chosen Python version 3.7
Step 2: Once the download is complete, run the exe for install Python. Now clickon Install Now.
Step 3: When it finishes, you can see a screen that says the Setup was successful. Now click on "Close".

- **PyCharm Installation:**

Step 1: To download PyCharm visit the website https://www.jetbrains.com/pycharm/download/ and Click the "DOWNLOAD" linkunder the Professional Section.
Step 2: Once the download is complete, run the exe for install PyCharm. The setup wizard should have started. Click "Next".
Step 3: On the next screen, Change the installation path if required. Click "Next".
Step 4: On the next screen, you can create a desktop shortcut if you want and clickon "Next".
Step 5: Choose the start menu folder. Keep selected JetBrains and click on "Install".
Step 6: Once installation finished, you should receive a message screen that PyCharm is installed. If you

want to go ahead and run it, click the "Run PyCharm Professional Edition" box first and click "Finish".
Step 7: After successful installation, Pycharm get start.[3]

Screenshot 1: PyCharm Window

ii. ElasticSearch Installation

Step 1: To download ElasticSearch visit the websitehttps://www.elastic.co/downloads/elasticsearch and Click on WINDOWS inDownload.
Step 2: Download jre8 because ElasticSearch is a highly scalable full-text search and analytics engine. Step 3: Open elasticsearch-6.5.4 folder and run the batch file in bin folder.
Step 4: Batch file shows the port on which ElasticSearch search engine is running,ElasticSearch normally run on localhost: 9200. [5]

iii. Creating Django Project

Step 1: In the main menu, choose File | New Project..., or click the New Project button on the Welcome screen. New Project dialog box opens.
Step 2: In the New Project dialog box Specify project type Django, Specifyproject location, click on Next. **Step 3:** Click on More Settings, and specify theDjango application name. The name of a Djangoapplication should not be the same as the Djangoproject name.
Step 4: Click on Create.

iv. Kibana Installation:

Step1: To download Kibana visit the website https://www.elastic.co/downloads/kibana and Clickon WINDOWS in Download.
Step 2: Open kibana-6.5.4-windows-x86_64folderand run the batch file in binfolder.
Step 3: Batch file shows the port on which Kibana is running, Kibana normally runon localhost: 5601.[6]

v. **Implementation of Solution 1(By Using ElasticSearch Search Engine)**

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

Log messages are an effective way to infer what has happened during the execution of a production system to diagnose problems effectively. In earlier day's human operators we able to diagnose problems by hand using the logs, this no longer applies to today's systems. But now day's applications easily generate millions of log messages on a daily basis.

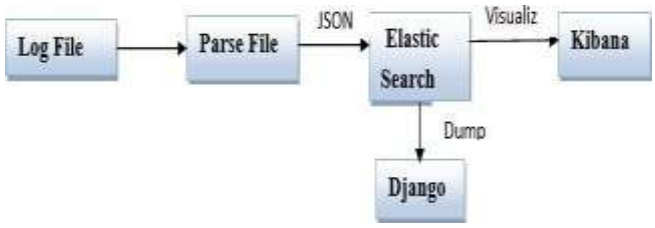


Figure 3: Block diagram (using Search Engine)

For easy understanding of log we can parse the log files and creates JSON object. Then created JSON object is pass to ElasticSearch search engine and dump into Django server. ElasticSearch pass the JSON file to Kibana for further processing. Kibana can create index for log file and visualize in different form such as Bar graph, line graph, Histogram, pie chart, etc. There are multiples inbuilt filters in Kibana. Filtersare applied on index to get filtered logs which helps to diagnose anomalies and failures. For easy understanding of log we can parse the log files and creates JSON object. Then created JSON object is pass to ElasticSearch search engine and dump into Django server. ElasticSearch pass the JSON file to Kibana for further processing. Kibana can creates index for log file and visualize in different form such as Bar graph, line graph, Histogram, pie chart, etc. There are multiples inbuilt filters in Kibana. Filtersare applied on index to get filtered logs which helps to diagnose anomalies and failures.

Implementation of Solution 2 (By Using databaseMongoDB Database)

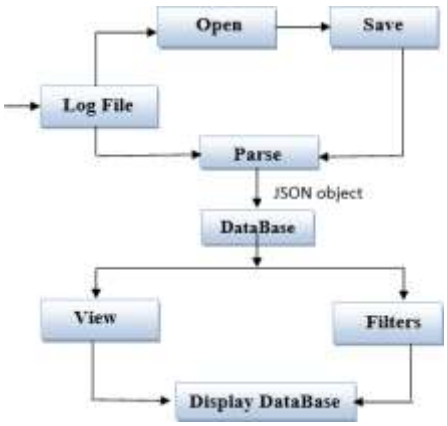
In solution 2 we can create our own GUI for easy handling. GUI can be design by using Tkinter in python Tkinter is Python's de-facto standard GUI(Graphical User Interface)package. It is a thin object-oriented layer on top of Tk. Tkinter is not the only GUI Programming toolkit for Python It is however the most commonly used one.

Figure 4: Block diagram (Using Database)

VI. RESULT

a. Solution 1 (by using Search Engine) Following Screenshot shown the Stepwise solution of Live Log Query Software

- Following Screenshot shows the output after executing parse file the output in the JSON format



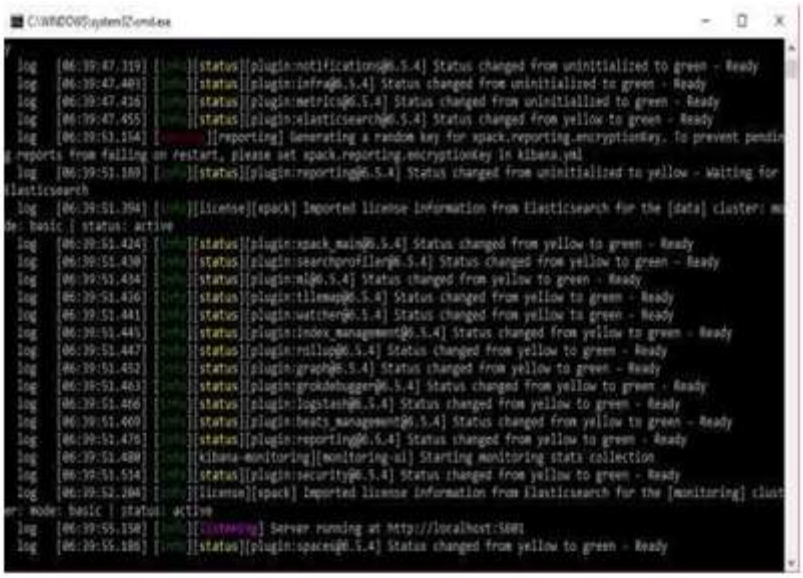
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

Screenshot 2: Output of parsing file in the form ofJSON Format

The above JSON object passes to the Elastic-Search Search Engine.

- **Run the Search Engine**

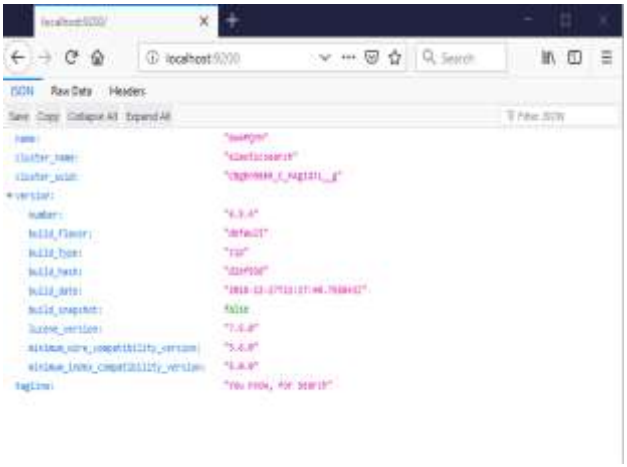
To activate the ElasticSearch Search engine is to runthe batch file of inElasticSearch Folder.
In the batch file the status change red to yellow that issearch engine ready tofetch the file.
Run on localhost 9200



Screenshot 3: Run the batch file of ElasticSearch

- **Elasticsearch Search Engine run on local host9200**

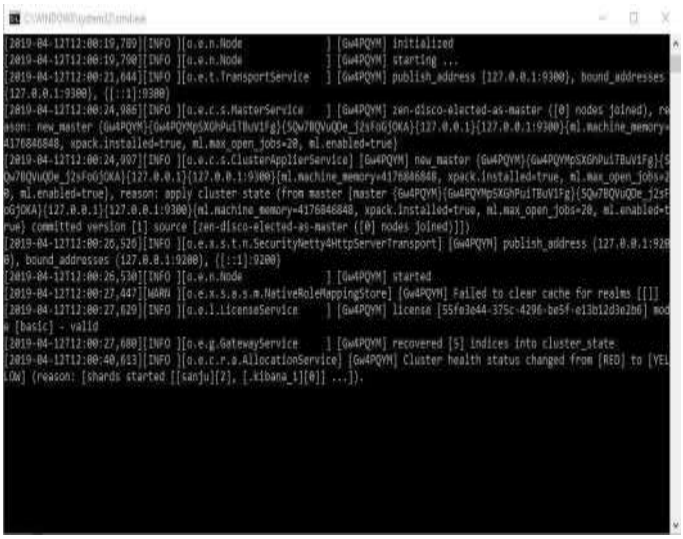
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252



Screenshot 4: Activate Elasticsearch Search Engine

- Elasticsearch search engine used the visualizationtool kibana that run onlocalhost 5601

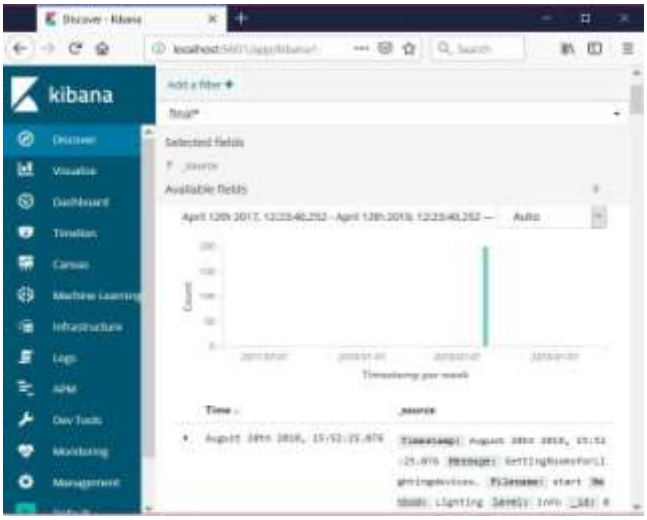
First run the batch file



Screenshot 5: Running batch file of Kibana

- **Final Output of Log Analysis**

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252

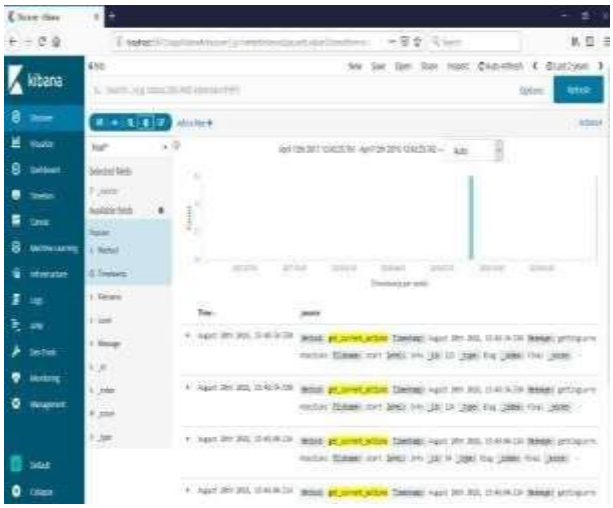


Screenshot 6: output of live log query on Kibana

Kibana is visualization tool which is specially use forindex representation in formof bar graph, pie chart, histogram, line graph, etc. Kibana has inbuilt function for filter. There are multiple filters in kibana such as timestamp, id, method, message, method, level, etc.

- **Output after applying the Filter**

By applying filter on method Get_current_action which shows the how many times this methods hits in the log file and shows the logs in which Get_current_action method is present.



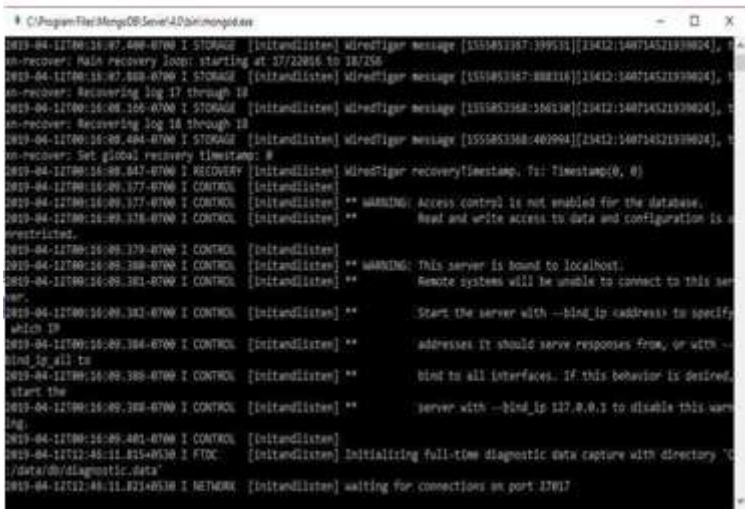
Screenshot 7: Apply filter (method=get_current_action)

b. **Solution 2 (By using MongoDB Database)**

Start Mongodb server

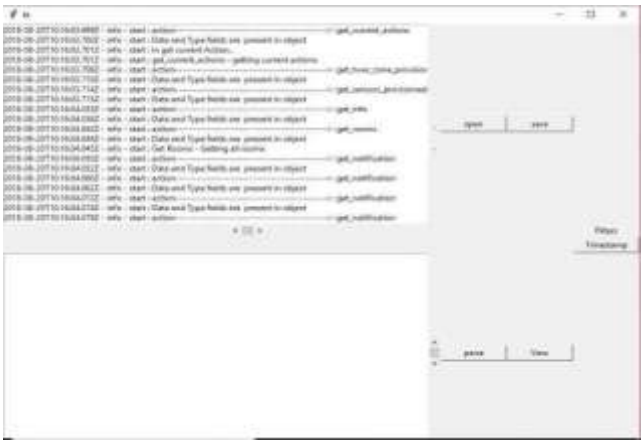
Run the batch file of Mongod in the mongodb server

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 2280-2289 www.ijaem.net ISSN: 2395-5252



Screenshot 8: Run the batch file mongod The Mongodb server run on localhost the port number is 27017 and ready toaccept the data intodatabase collection.

- **Live Log Query Software interface as shown inbelow screenshot**



Screenshot 9: Interface of Live Log Query Project

We are created the above GUI in this GUI we can create open, save, parse andview button and also the one button for applying the filter that is timestamp button.

Following are the working description of each button as followOpen: - This button used to open the log filefrom your system.Save: - This button is used to save the log file.

Parse: - By using the parse button to parse file and save into the database in the json format.

View: - View button shows the database view.

Timestamp: - By using the timestamp to apply filter on logs.

VII. CONCLUSION

Logs and log analysis are of vital importance in today's software systems. By means of analysis system failures and anomalies can be detected from event logs and the problem diagnosis process can be improved. However, the ever increasing number of log messages that present-day systems produce renders exclusive human analysis unfeasible. Live Log Query Software is introduced to reduce the amount of data to consider in log analysis or detection. By using log parsing to ease analysis. The Live Log Query Software used range from source code parsing to simple JSON object. Furthermore, filtering is also used to reduce the amount of data to consider. The abstracted data can be used as input for failure detection, failure diagnosis or anomaly detection. Again, wide ranges of filter are available for this purpose ranging from simple hypothesis.

VIII. FUTURE SCOPE

Live Log Query Software provides the facility to detect, failure diagnosis or anomaly detection of the software or application. The future scope of this project is to provide Solution on the failure or anomalies detected by Live Log Query Software.

REFERENCES

[1]. Log Analysis from A to Z: A Literature Survey Author: Joop Au´e
[2]. Rakesh Agrawal, Tomasz Imieli´nski, and Arun Swami. "Mining association rules betweensets of items in large databases". In ACM SIGMOD: International Conference on Management of Data, 1993.
[3]. RP Jagadeesh Chandra Bose and Wil MP van der Aalst. "Discovering signature patterns from event logs". In IEEE Symposium on Computational Intelligence and Data Mining, 2013..
[4]. Onlinehttp://www.python.org/downloads/.
[5]. Onlinehttps://www.elastic.co/downloads/elasticsearch.
[6]. Onlinehttps://www.elastic.co/downloads/kibana.
[7]. Onlinehttps://www.mongodb.codownload-center.