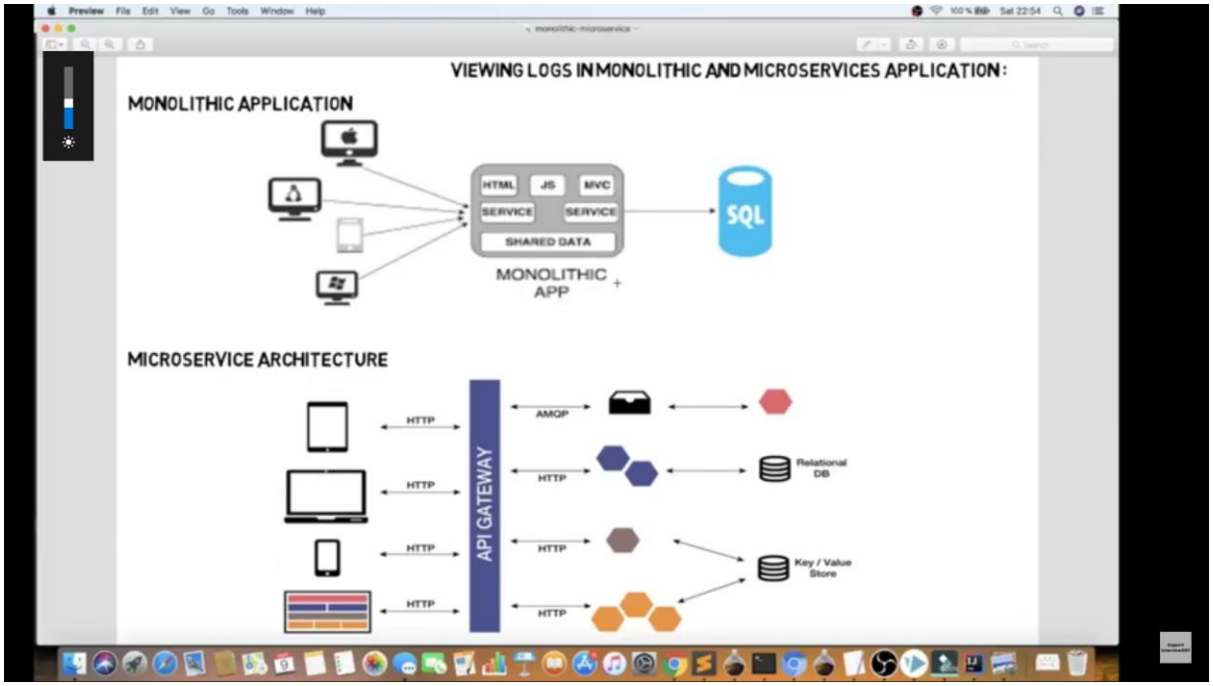
ELK – Elastic search- Logstash- Kibana

It is collection of three open-source products — Elasticsearch, Logstash, and Kibana.

Example:

Viewing logs actually we do in Monolithic and Microservices application:



For **monolithic application**, if any error occurs or something happened means we can go and view the log file and know what happened in the application.

For **microservices application**, we are create log files for each services separately, if something happens means we can go and view each log file for each services.

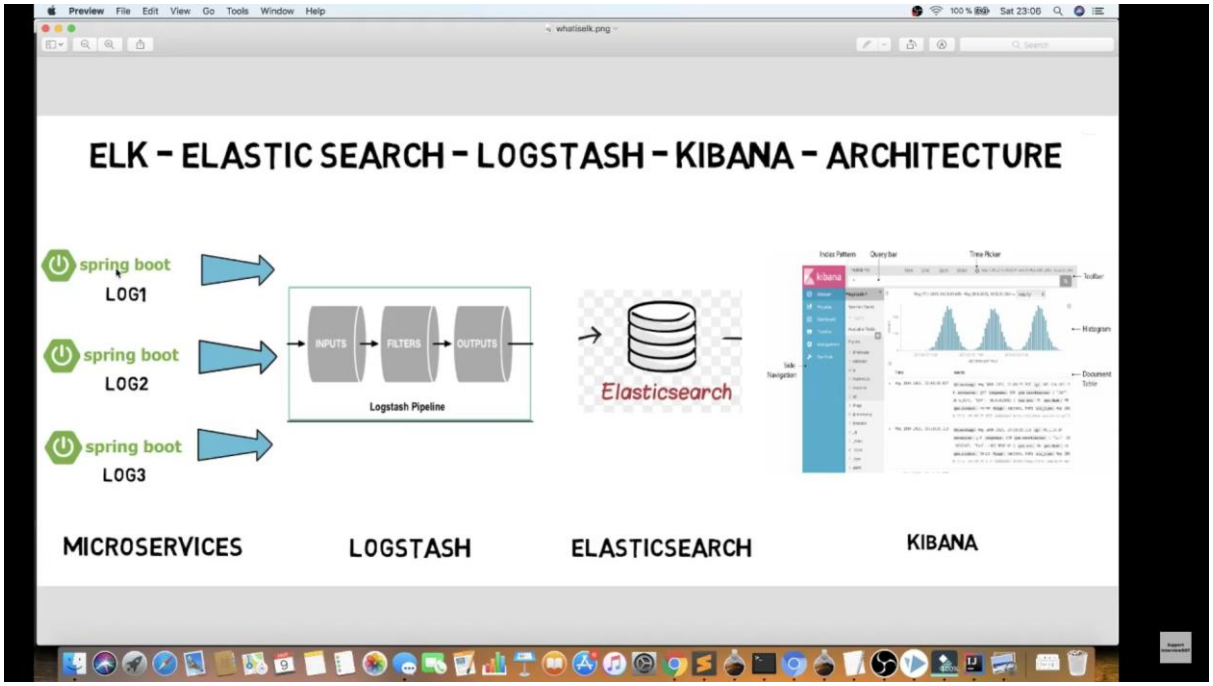
Do you think for this kind of situation, If all logs are manage in place means it will useful that's what ELK stack provides.

ELK Stack:

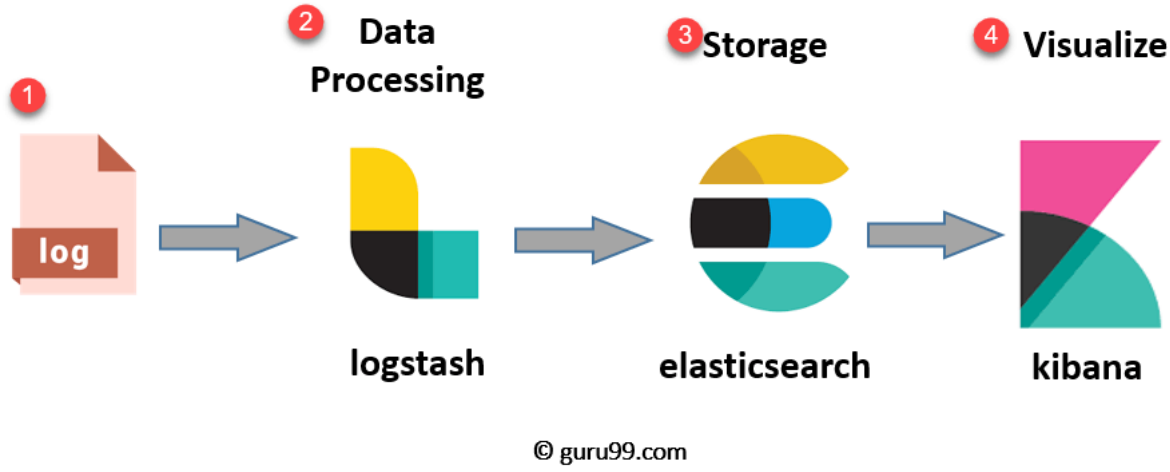
ELK stack provides centralized logging in order to identify problems with servers or applications.

It allows you to search all the logs in a single place.

It also helps to find issues in multiple servers by connecting logs during a specific time frame.



- **E** stands for ElasticSearch: used for storing logs
- **L** stands for LogStash : used for both shipping as well as processing and storing logs
- **K** stands for Kibana: is a visualization tool (a web interface)



References :

Steps to understand the concepts:

You can visit the below links one by one then only understand the concepts:

1.https://www.youtube.com/watch?v=dcROIwJBtm4 - You tube video for understand the concepts on ELK.

2.https://www.guru99.com/elk-stack-tutorial.html - For knowing each and everything about ELK

3. Installation process for ELK for windows 10-

https://www.youtube.com/watch?v=8iXZTS7f_hY

4. Middleware create logger file for request and response using Winston npm:

1- https://www.youtube.com/watch?v=PdVlAi7nrRU – create log file using winston

2- https://www.youtube.com/watch?v=1jhdfS1Bwcc – store req and res in log file

3- https://www.npmjs.com/package/winston - **winston npm** for more understand

5. For transport our log details to ELK for that I prefer **Winston-elastic search**

https://www.npmjs.com/package/winston-elasticsearch

sample you tube video may be useful - https://www.youtube.com/watch?v=x0W5OPU1nek

6. Elastic APM- Application performance Monitoring

Elastic APM is an application performance monitoring system which is built on top of the ELK Stack

Elastic APM allows you to track key performance-related information such as requests, responses, database transactions, errors, etc.

Reference : https://logz.io/blog/application-performance-monitoring/