ELK Stack Research (In Progress)

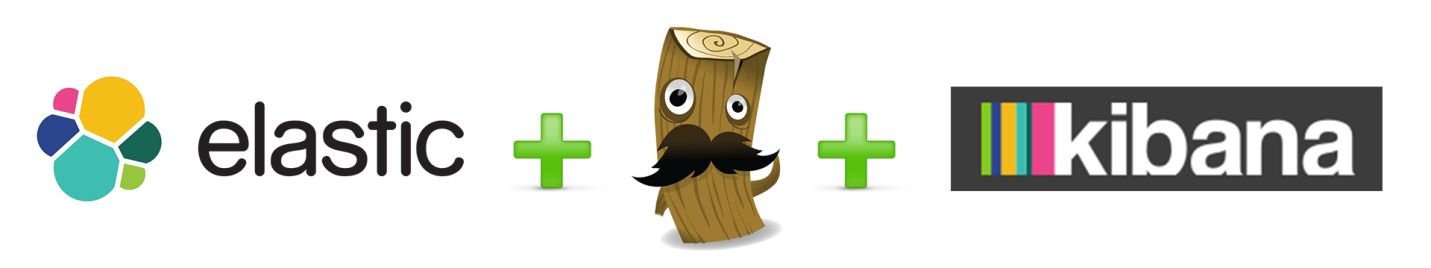
Terms

Analytics: Examination and interpretation of data

Logfile: File that records actions and request to a server, made by users

Open-source: Computer program that’s source code is available to the general public for use. Meant to be improved, modified, and shared by its users.

ELK Stack



WHAT:

Combination of three programs: ElasticSearch, Logstash, and Kibana, which work together to create and easy to understand visualization of data.

PURPOSE FOR US:

Easy visualization for the everyman, of log data such as location, gender, age, alignment, etc.

LINKS:

ElasticSearch



WHAT:

Open-source search and analytics engine. Allows for storage of large amounts of data, and near real time search and analyze of that data.

PURPOSE FOR US:

Backend for are ELK stack, will hold all the data gathered from user logs and allow for quick search through it.

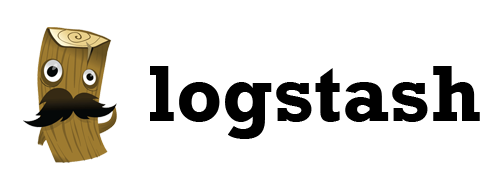
RUN:

Execute the *elasticsearch.bat* program, then internet window go to *localhost:9200*

LINKS:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html>

Logstash



WHAT:

Open-source data collection engine. Allows for data from multiple sources to be modified into a unified format and sent to a single destination.

PURPOSE FOR US:

Works as a pipeline, modifies the log file of multiple types and from multiple sources into a json files of a unified format then ships it to ElasticSearch.

RUN:

In command window, navigate to folder containing *logstash.bat*, then execute *logstash –f file.cong* (file.config being your conf file you wrote).

Sometimes pipeline won’t grab the logs. Open log file copy and delete the logs, save, paste the logs and save again, that should solve the issue.

LINKS:

<https://www.elastic.co/guide/en/logstash/current/introduction.html>

Kibana



WHAT:

Open-source platform use for analyzes and visualization of data, designed to specifically to work with ElasticSearch.

PURPOSE FOR US:

Frontend. Displays the data from ElasticSearch in a dashboard, in charts, graphs, maps, etc.

RUN:

Execute the **kibana.bat** program, then in an internet window go to *localhost:5601*

LINKS:

<https://www.elastic.co/guide/en/kibana/current/getting-started.html>