# Log Analysis

## Overview

Log files are commonly used to log computer operations and activities. It has become increasingly important to trace these operations and understand them through data analysis. In this project, we are looking for a way to analyze and report log data in a secure way. The system needs to be deployed in cloud and properly secured with controlled access.

## Major work and expected outcomes

* Research and study log analysis platforms and systems.
* Set up a system that runs the Elastic platform including Logstash, Elasticsearch, and Kibana
* Collect and analyze sample log files coming from different source.
* Secure the system with controlled access.

## Type of project (estimation)

* Research and analysis 30%
* Implementation 70%

## Skills/knowledge involved

* System admin
* Log file and data processing
* Access control

## Recommended team size

1 team of 4 to 5 students

## Project owner/sponsor

* Hossain Shahriar, Assistant Professor, IT Department, hshahria@kennesaw.edu

## Reference

* <https://www.elastic.co/products>
* <https://en.wikipedia.org/wiki/Log_analysis>