**Log Analysis**

* Every logging mechanism will have levels, most widely adopted levels are
  + INFO: This is informational log
  + DEBUG: This is informative log
  + ERROR: This represents errors
  + CRITICAL/FATAL: This represents serious system failures
* Logs are time-based information.
* In Elastic Stack we have logstash which can extract the logs, transform and load into elastic search for querying/visualizations
* Logstash does the transformations with the help of plugins
  + input plugins: to read from different sources <https://www.elastic.co/guide/en/logstash/current/input-plugins.html> for input plugins supported by logstash
  + filter plugins: to transform the log <https://www.elastic.co/guide/en/logstash/current/filter-plugins.html> for filter plugins
  + output plugins: to store the output to different sources <https://www.elastic.co/guide/en/logstash/current/output-plugins.html> for output plugins
* Installing logstash:
  + <https://www.elastic.co/guide/en/logstash/current/installing-logstash.html#_apt>
* Ideal use case for us  
  