This was my first time using Logstash, and it has absolutely been a very enjoyable and challenging experience thus far. I have been leaning heavily on both my troubleshooting experience, web searching, debugging, and log files to teach myself how to use Logstash and work through the CSE Skills Test.

I initially downloaded and configured the full ELK stack and was using for testing, which included Elasticsearch, Logstash, and Kibana. I built a Logstash conf file and had a basic test output working with Elasticsearch and Kibana, but then ran into issues when trying to change it over to a file input. This led me down a bit of a rabbit hole which ended up expanding my knowledge with Logstash. At that point I decided to simplify things and fall back to using a file input and file output. I continued troubleshooting issues with both inputs and ultimately created a working solution.

Data is ingested using into Logstash using a file input. During testing I set my logstash.conf file to not utilize a “sincedb”, which allowed me to test with the same file repeatedly in between adjustments to my logstash.conf file. I removed this from the logstash.conf file so that other data in the same log message could be ingested as per the CSE Skills Test requirements.

I filtered the ingested data using “grok” and “mutate”. “Grok” was used to parse data from the log file into the required fields outlined in the CSE Skills Test while “mutate” was used to translate the “severity” from a number to a descriptive word (High). I utilized a file output with a json codec to create a file with the parsed data.

In closing I know I would need to make more changes to my logstash.conf file cleanup the output, and also investigate other types of outputs. There are also probably much more efficient ways of filtering than what I have in my config, but I am proud of how things turned out and plan to dive deeper into these types of tools in my studies.