**Mock Interview Questions**

Security analysts deal with analyzing data logs from servers to websites. One challenge security analysts face is collecting mass amounts of log data and sorting it out in a legible function.
In one of my projects I dealt with sample log data and simulated log data.
The sample log data was a log about Web Traffic in a website, while the simulated log data was running a command to stress test a virtual machine to simulate a machine overload of sorts.
In the sample log data I was dealing with a vast amount of data, such as graphs about unique visitors and bytes used and charts that show where in the world these ip addresses originated from.

Primarily, I was looking through the different types of graphs and filters in kibana.
The information I needed in that sample log is where in the world is the most web traffic located from, and to look through any sort of suspicious activity that could be recognized as malicious.
What analysts need to analyze these mass amounts of data are clear and concise graphs. With these graphs and filters you can sort through any data and read through more important information.

The tools I used were Kibana discovery and dashboard. Dashboard brought all the statistical data, while Discover lists all log files.

I used the kibana dashboard to get a broad scope of what was going on in the sample data, such as what kind of errors clients were experiencing, unique visitors, byte and file type graphs. Using these graphs in combination with the filters I can get a more precise look at data in the graphs, such as geological location and specific time and dates.

Using Kibana, I can look through the log files and see specifically what clients were doing, what
websites they accessed, where they were coming from, etc.
One of the disadvantages of having huge quantities of data being sorted and filtered through is that most of the filtered data are just regular filler and don't provide as much insight into specific data I am looking for so many charts and graphs went unused.

Having access to this data would have least likely changed my process. Because many of the logs were get requests and responses, one might not find some of those logs useful in their research.