Elk Stack Project 1- Kibana Review Questions Jaquan Stevenson

1. Add the sample web log data to Kibana.
2. Answer the following questions:
   * In the last 7 days, how many unique visitors were located in India? 252
   * In the last 24 hours, of the visitors from China, how many were using Mac OSX? 10
   * In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 404 errors: 5.88% and 503 errors: 1.176%
   * In the last 7 days, what country produced the majority of the traffic on the website? China
   * Of the traffic that's coming from that country, what time of day had the highest amount of activity? 1pm (hour 13)
   * List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).
     + Gz 🡪 .gz files are compressed files created using the gzip compression utility.
     + Css 🡪: .css files can help define font, size, color, spacing, border and location of HTML information on a webpage. They are downloaded with their .html counterparts and rendered by the browser.
     + Zip 🡪: .zip file may contain one or more files or directories that have been compressed. Also known as a lossless compression file.
     + Deb 🡪 .deb file extension is a Debian (Linux) Software Package file. These files are installed when using the apt package manager
     + Rpm 🡪 .rpm file formats are a Red Hat Software Package file. RPM stands for Red Hat Package Manager
3. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.
   * Locate the time frame in the last 7 days with the most amount of bytes (activity).
   * In your own words, is there anything that seems potentially strange about this activity? It is strange that there is an unusually high usage of bytes being used by one person.
4. Filter the data by this event.
   * What is the timestamp for this event? May 22, 2022 @ 20:00 (8pm) 🡪 May 23, 2022 00:00
   * What kind of file was downloaded? Rpm file
   * From what country did this activity originate? India
   * What HTTP response codes were encountered by this visitor? 200 OK
5. Switch to the Kibana Discover page to see more details about this activity.
   * What is the source IP address of this activity? 35.143.166.159
   * What are the geo coordinates of this activity? "lat": 43.34121, "lon": -73.6103075
   * What OS was the source machine running? Windows 8
   * What is the full URL that was accessed? https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm
   * From what website did the visitor's traffic originate? Facebook
6. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing?
   * Was the file they downloaded malicious? If not, what is the file used for?
   * Is there anything that seems suspicious about this activity?
   * Is any of the traffic you inspected potentially outside of compliance guidlines?