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? 215

   - In the last 24 hours, of the visitors from China, how many were using Mac OSX? 6

   - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 32, 37

   - 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? 12 pm - 1pm

   - 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 File Extension: Open GZ Files Now With WinZip

     Css CSS - Wikipedia

     Zip ZIP File - What is it and how do I open it?

     Deb DEB File - What is it and how do I open it?

     Rpm RPM File - What is it and how do I open it?

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? Only 1 user

4. Filter the data by this event.

   - What is the timestamp for this event? `Mar 6, 2021 @ 19:06:40.169`
   - What kind of file was downloaded? doc
   - From what country did this activity originate? Canada
   - What HTTP response codes were encountered by this visitor? 200

5. Switch to the Kibana Discover page to see more details about this activity.

   - What is the source IP address of this activity? `86.158.95.250`
   - What are the geo coordinates of this activity? `lat": 33.12936111,`
   - `  "lon": -94.97563889`
   - `}`
   - What OS was the source machine running? Windows XP
   - What is the full URL that was accessed? `https://www.elastic.co/downloads/beats`
   - From what website did the visitor's traffic originate? `http://www.elastic-elastic-elastic.com/success/gregory-linteris`

6. Finish your investigation with a short overview of your insights.

   - What do you think the user was doing? Downloading a doc about beats on elastic.co looks like sample data
   - Was the file they downloaded malicious? If not, what is the file used for? no
   - Is there anything that seems suspicious about this activity? no
   - Is any of the traffic you inspected potentially outside of compliance guidlines? no