Exploring Kibana

- In the last 7 days, how many unique visitors were located in India? **225**
- In the last 24 hours, of the visitors from China, how many were using Mac OSX? **9**
- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? **404 0% 503 0%**
- In the last 7 days, what country produced the majority of the traffic on the website? **US**
- Of the traffic that's coming from that country, what time of day had the highest amount of activity? **11**
- 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, css, zip, deb,rpm**

2. 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? **There was only one unique visitor**.
3. Filter the data by this event.
   - What is the timestamp for this event? **08-08-21 21:00**
   - What kind of file was downloaded? **RPM**
   - From what country did this activity originate? **India**
   - What HTTP response codes were encountered by this visitor? **200**
4. 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? **Win 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**
5. Finish your investigation with a short overview of your insights.
   - What do you think the user was doing? **Downloading a RPM file**
   - Was the file they downloaded malicious? If not, what is the file used for? **No. Linux**
   - Is there anything that seems suspicious about this activity? **Yes it was downloaded from Facebook.**

- Is any of the traffic you inspected potentially outside of compliance guidlines? **Yes.**