1. Answer the following questions:  
   * In the last 7 days, how many unique visitors were located in India?

227

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

1 visit 100% MAC OS

* + In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

775-65= received 404 errors= 8%

775-0= 0 percent received 505 errors

* + In the last 7 days, what country produced the majority of the traffic on the website?

The United States

* + Of the traffic that's coming from that country, what time of day had the highest amount of activity?

8pm

* + 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, deb, zip, rpm

1. 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).

3pm- 15:00

* + In your own words, is there anything that seems potentially strange about this activity?

1. Filter the data by this event.  
   * What is the timestamp for this event?

1/7/2021- 15:00

* + What kind of file was downloaded?

zip

* + From what country did this activity originate?

United States

* + What HTTP response codes were encountered by this visitor?

1. Switch to the Kibana Discover page to see more details about this activity.  
   * What is the source IP address of this activity?
   * What are the geo coordinates of this activity?

United States

* + What OS was the source machine running?

Win

* + What is the full URL that was accessed?
  + From what website did the visitor's traffic originate?

China

1. 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?