1. Answer the following questions:

    - In the last 7 days, how many unique visitors were located in India? 248
    - In the last 24 hours, of the visitors from China, how many were using Mac OSX? 8
    - In the last 2 days, what percentage of visitors received 404 errors? 50% How about 503 errors? 58.3%

    - In the last 7 days, what country produced the majority of the traffic on the website? United States

    - Of the traffic that's coming from that country, what time of day had the highest amount of activity? 9am

    - 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).
        i. css - cascading style sheet, used to style web pages
        ii. gz - a **archive file** compressed by the standard GNU zip (gzip) compression algorithm
        iii. zip - an archive file format that supports lossless data compression
        iv. rpm - a Red Hat Package Manager **file** that's used to store installation packages on Linux operating systems.

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? Large amount of data being accessed.
3. Filter the data by this event.

    - What is the timestamp for this event? Feb 7@ 21:55:00:00 > Feb 7@ 22:00:00:00
    - What kind of file was downloaded? .rpm
    - From what country did this activity originate? China
    - 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: 43.34120996296406, Long: -73.61030758358538

- 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? `http://facebook.com/success/jay-c-buckey`

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

    - What do you think the user was doing? It appears the user was trying to access metricbeat data.
    - Was the file they downloaded malicious? If not, what is the file used for? No, it's used to store package information.
    - Is there anything that seems suspicious about this activity? User spent a long time accessing this site
    - Is any of the traffic you inspected potentially outside of compliance guidelines