1. Answer the following questions:

    - In the last 7 days, how many unique visitors were located in India?

      There were 228 unique visitors from India

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

      There were 10 users

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

      For the past two days every 4 hour the percentage vary on the ff

      404 - 0%-12.5%

      503 - 0%-8.696%

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

      China produced the majority of traffic on the website

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

      6:00 had the highest amount of activity

    - 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).

      css - cascading style sheet used for formatting webpages

      deb - Debian Software Package file

      gz - archive file compressed using GNU algorith

      rpm - Red Hat Package Manager File

zip - archive file format used for compressing files

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).

      The most amount of bytes is during 18:00 - 21:00

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

      There was only one visitor during this timeframe.

3. Filter the data by this event.

    - What is the timestamp for this event? 19:57:18.552
    - What kind of file was downloaded? an rpm file
    - 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? `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? The user was trying to download and install metricbeat
- Was the file they downloaded malicious? If not, what is the file used for? The file is not malicious. RPM files are used for installing packages in the Red Hat Linux operating system
- Is there anything that seems suspicious about this activity? The traffic was redirected from a facebook page.
- Is any of the traffic you inspected potentially outside of compliance guidlines? The machine OS is very old (Win 8) which would not be updated with the latest security patches and fixes.