1. Answer the following questions:

    - In the last 7 days, how many unique visitors were located in India?
    - 228
    - In the last 24 hours, of the visitors from China, how many were using Mac OSX?
    - 19.15%
    - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?404-100% 503- 23%

    - 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?Hour 7-10

    - 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 Sheets is used to format the layout of a webpage
    - Deb - Debian Software Package file
    - Gz - file compressed by the standard GNU zip
    - Rpm - Red Hat Package Manager
    - Zip - compressed 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).
    - 05/01/2022
    - In your own words, is there anything that seems potentially strange about this activity?
    - It is almost double the typical avg bytes
3. Filter the data by this event.

    - What is the timestamp for this event?
    - 22:00
    - 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?
    - What are the geo coordinates of this activity?
    - What OS was the source machine running?
    - What is the full URL that was accessed?
    - From what website did the visitor's traffic originate?
5. Finish your investigation with a short overview of your insights.

    - What do you think the user was doing? Downloading a redhat file
    - Was the file they downloaded malicious? If not, what is the file used for? No, not malicious. Red Hat is used by enterprise security teams.
    - Is there anything that seems suspicious about this activity? The size of the download
    - Is any of the traffic you inspected potentially outside of compliance guidlines?
    - No