1. Answer the following questions:
   * In the last 7 days, how many unique visitors were located in India?
     + 223
   * In the last 24 hours, of the visitors from China, how many were using Mac OSX?
     + 13
   * In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?
     + 404: 0-7%
     + 503: 0-3.8%
   * 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?
     + 12pm-1pm
   * 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: Compressed files
     + CSS: HTML elements to find page
     + ZIP: Archive zip
     + Deb: files to upgrade Deb commands/install files
     + RPM: specific to redhat install 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).
     + 6/24/2021 3:58pm
   * In your own words, is there anything that seems potentially strange about this activity?
     + Nothing was to strange it was a large download gz file from Kibana.
3. Filter the data by this event.
   * What is the timestamp for this event?
     + 15:58
   * What kind of file was downloaded?
     + GET /kibana/kibana-6.3.2-linux-x86\_64.tar.gz
   * From what country did this activity originate?
     + China
   * What HTTP response codes were encountered by this visitor?
     + HTTP/1.1" 200 16750
4. Switch to the Kibana Discover page to see more details about this activity.
   * What is the source IP address of this activity?
     + 1.145.31.121
   * What are the geo coordinates of this activity?
     + "lat": 28.28980556, "lon": -81.43708333
   * What OS was the source machine running?
     + Win 8
   * What is the full URL that was accessed?
     + https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-linux-x86\_64.tar.gz
   * From what website did the visitor's traffic originate?
     + http://www.elastic-elastic-elastic.com/success/aleksandr-serebrov
5. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing?
     + Downloading log data from Kibana on web server
   * Was the file they downloaded malicious? If not, what is the file used for?
     + It received a 200-status code so I don’t believe it was malicious I think it was a simple request to get information from Kibana on web server data analytics
   * Is there anything that seems suspicious about this activity?
     + At first glance it looks like everything is ok and nothing to dig more into.
   * Is any of the traffic you inspected potentially outside of compliance guidelines?
     + The fact that a large zip file was downloaded and can be run through Linux could potentially have some compliance issues as we would not want anyone downloading anything typically other then admins.