Instructions

1. Add the sample web log data to Kibana.

2. 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?
      11

    - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?
      0%

    - 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?
      10 AM

    - 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. gz - a compressed archive file.
        ii. css - style sheets - describes how html elements should be displayed on a screen.
        iii. zip - one or more compressed files.
        iv. deb - a software package for Debian.
        v. rpm - a red hat package manager file.

3. 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?
      It’s strange that the file is an rpm but they’re on Windows 8.

4. Filter the data by this event.

    - What is the timestamp for this event? 22:55
    - 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
5. 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? Windows 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? Facebook
6. Finish your investigation with a short overview of your insights.

    - What do you think the user was doing? The user was downloading metricbeats.
    - Was the file they downloaded malicious? If not, what is the file used for? Not malicious, it's for installing metricbeats.
    - Is there anything that seems suspicious about this activity? Strange that it says the OS is Linux under message, but under machine.os it says Windows 8.
    - Is any of the traffic you inspected potentially outside of compliance guidelines? No