1. Answer the following questions:  
   * In the last 7 days, how many unique visitors were located in India?

246

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

64

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

404 5.814% 503 1.163%

* + In the last 7 days, what country produced the majority of the traffic on the website?  
    India, Poland, and Japan
  + Of the traffic that's coming from that country, what time of day had the highest amount of activity?

Hours 10 and13 10 am and 1 pm

* + 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 that were done using the gzip compression utility

css: They help define the font, size, color, spacing, border, and location of the HTML information on any website

Zip: A lossless compression format. May contain multiple files or directories.

Deb: Debian software package file. Installed using apt

Rpm: stands for Red Hat Package Manager

1. 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?

In 2021-09-10 15:00 There is one user that uses an avg of 8,780 bytes. That’s a lot for one user.

1. Filter the data by this event.  
   * What is the timestamp for this event?

Sep 11, 2021 @ 10:00:00.000→Sep 11, 2021 @ 21:00:00.00

* + What kind of file was downloaded?

Css file

* + From what country did this activity originate?

India

* + What HTTP response codes were encountered by this visitor?

200 ok

1. Switch to the Kibana Discover page to see more details about this activity.  
   * What is the source IP address of this activity?

151.203.180.69

* + What are the geo-coordinates of this activity?
  + {
  + "lat": 21.57947361,
  + "lon": -158.1972814
  + }
  + What OS was the source machine running?

osx

* + What is the full URL that was accessed?

https%3A//www.elastic.co/downloads/beats/metricbeat,-utc\_time

* + From what website did the visitor's traffic originate?

http%3A//twitter.com/success/valeri-polyakov,-request

1. Finish your investigation with a short overview of your insights.  
   * What do you think the user was doing?

The user was trying to download metric beats from the website.

* + Was the file they downloaded malicious? If not, what is the file used for?

Not necessarily, It all depends where the user goes to download the file. Can be someone trying to set up metric beats with no ill intent.

* + Is there anything that seems suspicious about this activity?

Not really only that it came from Twitter.

* + Is any of the traffic you inspected potentially outside of compliance guidelines?

The idea that Twitter is sending him here or is where the user came from is a little strange since that’s not what twitter focuses on providing.