1. Answer the following questions:  
   * In the last 7 days, how many unique visitors were located in India? **251**
   * In the last 24 hours, of the visitors from China, how many were using Mac OSX? **9**
   * In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?  
     **89.655%-404 3.448%-503**
   * In the last 7 days, what country produced the majority of the traffic on the website? **CN**
   * Of the traffic that's coming from that country, what time of day had the highest amount of activity? **Noon**
   * 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-is a cascading style sheet (CSS) file used to format the contents of a webpage**
   * **DEB-is a Debian Software Package file. They're used mainly in Unix-based** [**operating systems**](https://www.lifewire.com/operating-systems-2625912)**, including Ubuntu and iOS. Every DEB file consists of two** [**TAR**](https://www.lifewire.com/tar-file-2622386) **archives that make up the executable files, documentation, and libraries**
   * **GZ**-**The Dzip software is a command line application designed to integrate encoding and compression specifications into files and folders selected for compression**
   * **RPM-A** [**file**](https://www.lifewire.com/what-is-a-file-2625878) **with the RPM** [**file extension**](https://www.lifewire.com/what-is-a-file-extension-2625879) **is a Red Hat Package Manager file that's used to store** [**installation packages**](https://www.lifewire.com/guide-to-linux-packages-2202801) **on Linux** [**operating systems**](https://www.lifewire.com/operating-systems-2625912)**.**
   * **ZIP- like other archive file formats, is simply a collection of one or more files and/or folders but is compressed into a single file for easy transportation and compression.**
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).
   * In your own words, is there anything that seems potentially strange about this activity? **This event is almost double the events for the rest of the week, it could be someone attempting to gain access to a system or exploit it.**
3. Filter the data by this event.  
   * What is the timestamp for this event? **19:55**
   * What kind of file was downloaded? **RPM**
   * From what country did this activity originate? **IN**
   * 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? **Windows 8**
   * What is the full URL that was accessed?- **http://facebook.com/success/jay-c-buckey**
   * From what website did the visitor's traffic originate? **Facebook**
5. Finish your investigation with a short overview of your insights.  
   * What do you think the user was doing? **The user downloaded metricbeat I would assume to collect data**
   * Was the file they downloaded malicious? If not, what is the file used for? **I do not think the metric beat file was downloaded as malicious, I think the user wanted it to gather info.**
   * Is there anything that seems suspicious about this activity? **It seems suspicious to me that the source location is in India but what is being accessed is in China**