Hayley Paul

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? 14
   * In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 21, 10
   * 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? 2100
   * 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 file: a compressed archive; css file: a file that describes how HTML elements are displayed; zip file: an archive file format that supports data compression; deb file: a file used mainly in Unix-based OS; rpm file: an installation package originally developed for Red Hat Linux
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). 2100
   * In your own words, is there anything that seems potentially strange about this activity? It’s coming from a Windows 8 operating system - which is really old/outdated.
3. Filter the data by this event.  
   * What is the timestamp for this event? 21:57:28
   * What kind of file was downloaded? Rpm file
   * From what country did this activity originate? India
   * What HTTP response codes were encountered by this visitor? HTTP/1.1" 200 15709
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? https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm
   * 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? Downloading a file from Facebook
   * Was the file they downloaded malicious? If not, what is the file used for? Downloading a Linux file
   * Is there anything that seems suspicious about this activity? no
   * Is any of the traffic you inspected potentially outside of compliance guidelines? no