* Answer the following questions:
* In the last 7 days, how many unique visitors were located in India?  
  244 unique visitors were located in India
* In the last 24 hours, of the visitors from China, how many were using Mac OSX?  
  10 unique visitors from China were using Mac OSX
* In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?  
  Percentage of visitors who received 404 errors was 5.556%, and 503 errors were also 5,556%
* 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?  
  At 12pm with 38 unique visitors
* 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: archive file compressed by gzip  
  css: Cascading Style Sheets that describe how HTML elements are displayed  
  zip: lossless data compression archive file  
  deb: debian software package file used for debian based distributions  
  rpm: Installation package for programs on Linux systems
* 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).  
  2021-09-12 had the most amount of bytes at 15,709 with the count of 1
* In your own words, is there anything that seems potentially strange about this activity?  
  One user was averaging 15,709 bytes in that time frame while the other time frames had multiple users averaging under 10,000 bytes.
* Filter the data by this event.
* What is the timestamp for this event?  
  Sep 12, 2021 @ 19:57:28.552
* What kind of file was downloaded?  
  It was an rpm file
* From what country did this activity originate?  
  The activity originated from India
* What HTTP response codes were encountered by this visitor?  
  The response code encountered was 200
* 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 is the source IP address
* What are the geo coordinates of this activity?  
  The geo.coordinates are lat:43.34121, long:-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?  
  The referer was <http://facebook.com/success/jay-c-buckey>
* Finish your investigation with a short overview of your insights.
* What do you think the user was doing?  
  The visitor was downloading a metricbeat file
* Was the file they downloaded malicious? If not, what is the file used for?  
  No, It is most likely a installation package for metricbeat, which helps monitor servers
* Is there anything that seems suspicious about this activity?  
  Yes, the referer was from a facebook link, which could be unsafe
* Is any of the traffic you inspected potentially outside of compliance guidelines?  
  Yes, as grabbing any work related tools from facebook could lead to potential breaches. It is better to find it from trusted sources or only through work related emails.