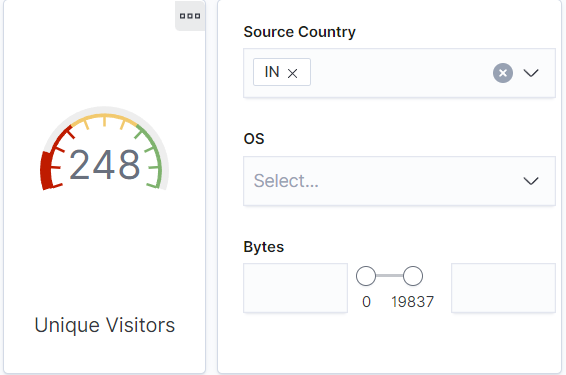
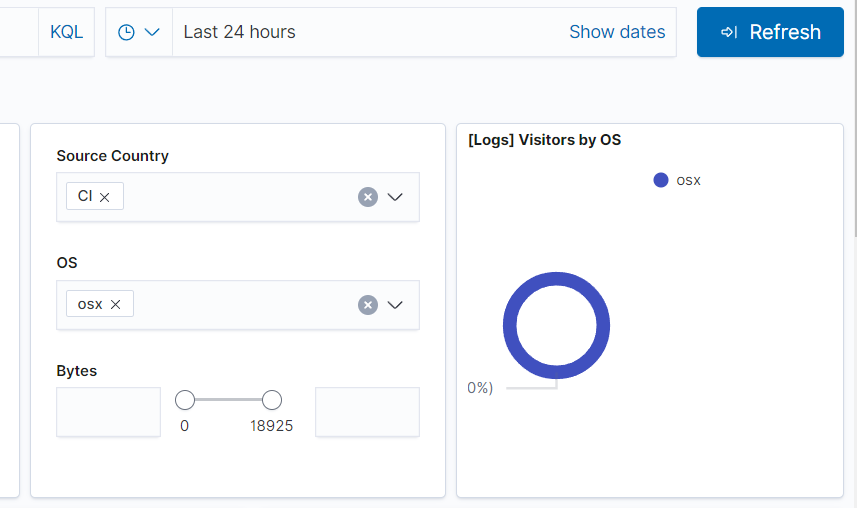
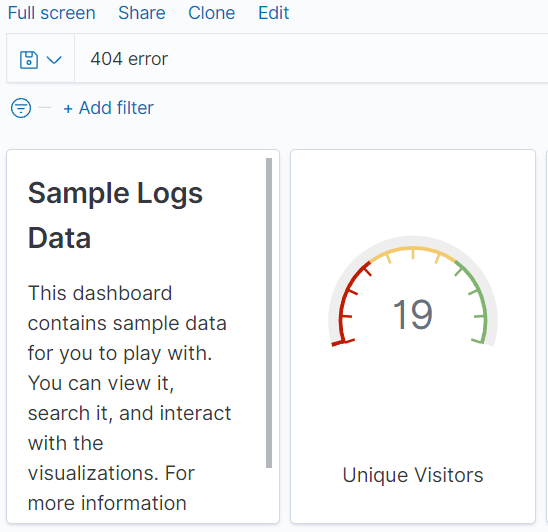
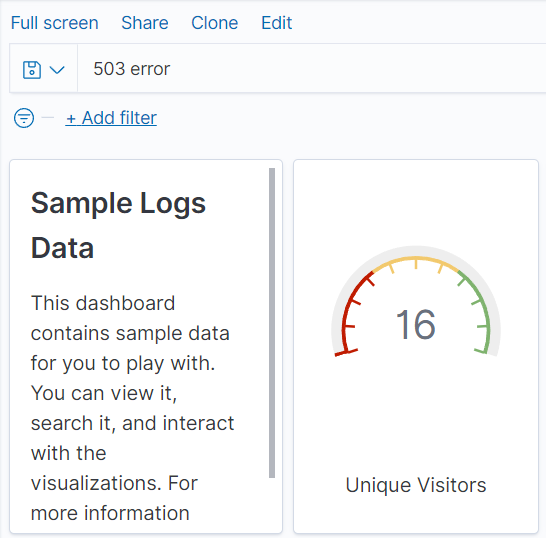
### **Instructions**

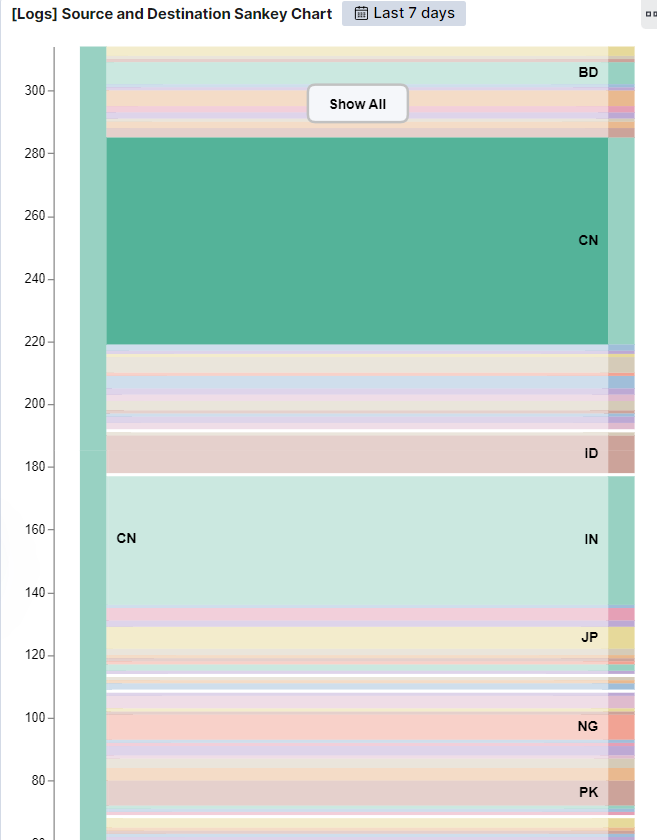
1. Add the sample web log data to Kibana.
2. Answer the following questions:  
   * In the last 7 days, how many unique visitors were located in India?
     1. 248



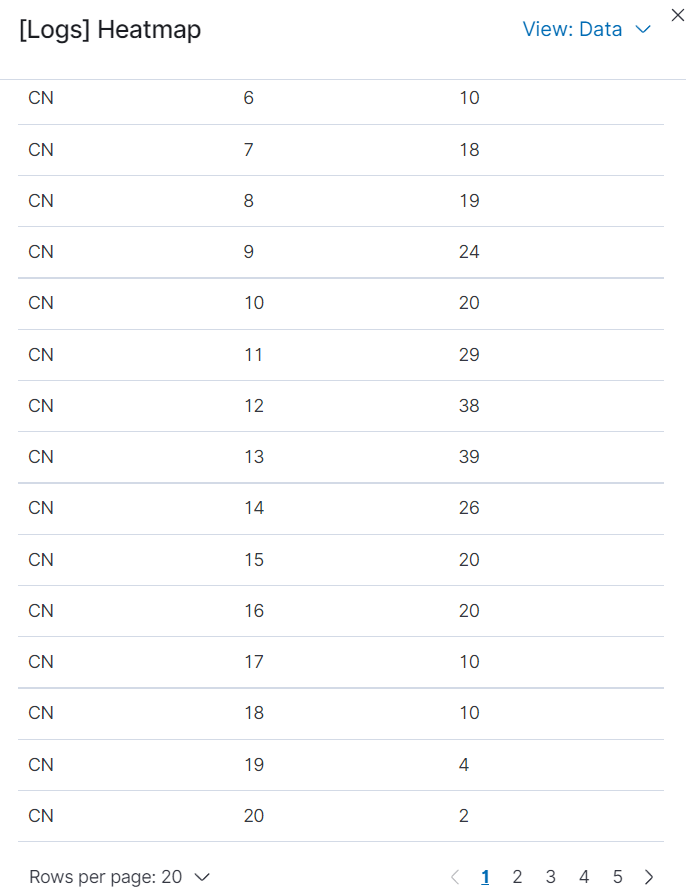
* + In the last 24 hours, of the visitors from China, how many were using Mac OSX?
    1. 0



* + In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?
    1. 
    2. 
  + In the last 7 days, what country produced the majority of the traffic on the website?
    1. China



* + Of the traffic that's coming from that country, what time of day had the highest amount of activity?
    1. Hour 13



* + 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).
    1. CSS - Cascading Style Sheet: used to format the contents of a webpage
    2. DEB - Debian Software Package: used primarily to install or update Unix applications; used by the Debian Linux distribution/variants
    3. GZ - Gnu Zipped Archive: archive file compressed by the standard GNU zip (gzip) compression algorithm
    4. RPM - Red Hat Package Manager File: installation package originally developed for the Red Hat Linux operating system but now is used by many other Linux distributions; commonly used for installing programs on Linux systems
    5. ZIP - Zipped File; archive that contains one or more files compressed with Zip compression; stores files separately from each other which allows the files to be compressed using different methods therefore the files can be decompressed separately

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).
     1. The most amount of bytes shows 16,837 2022-03-21 @ 18:00 hours
   * In your own words, is there anything that seems potentially strange about this activity?
     1. What I find potentially strange about this is that the number of unique visitors/count for this time frame is only 1, which is far lower than the rest of the other time frames with less bytes.
2. Filter the data by this event.  
   * What is the timestamp for this event? 2022-03-21 18:00
   * 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 OK
3. Switch to the Kibana Discover page to see more details about this activity.  
   * What is the source IP address of this activity? 35.143.266.50
   * 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: http://facebook.com/success/jay-c-buckey
4. Finish your investigation with a short overview of your insights.  
   * What do you think the user was doing? It appears that the user was trying to download the metricbeat file installation package (a Linux package).
   * Was the file they downloaded malicious? If not, what is the file used for? I do not believe the file that was downloaded was malicious. It depends on the website as it could be used for updating systems.
   * Is there anything that seems suspicious about this activity? The source originated in IN and the destination was CN.
   * Is any of the traffic you inspected potentially outside of compliance guidelines? I don’t notice anything that would be outside of compliance guidelines other than the “referral link” being from Facebook.com.