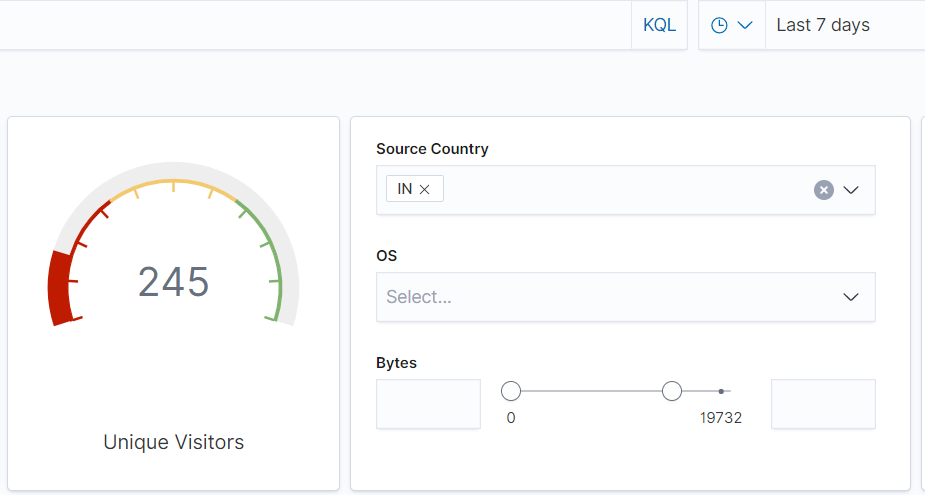
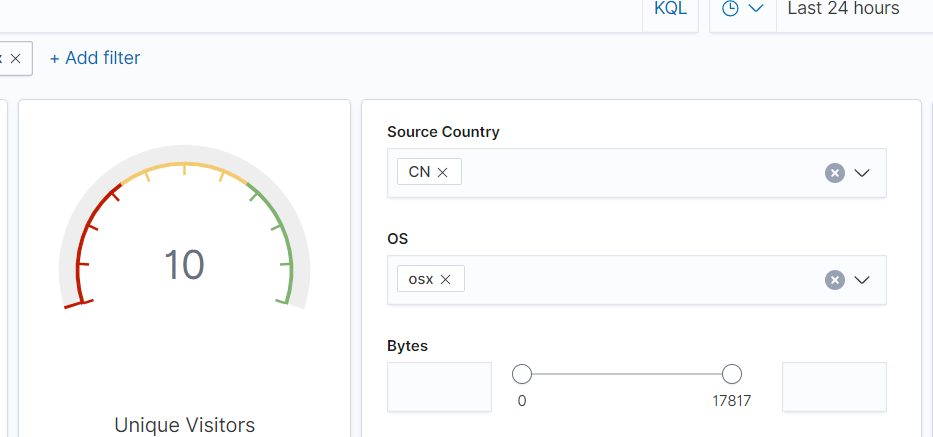
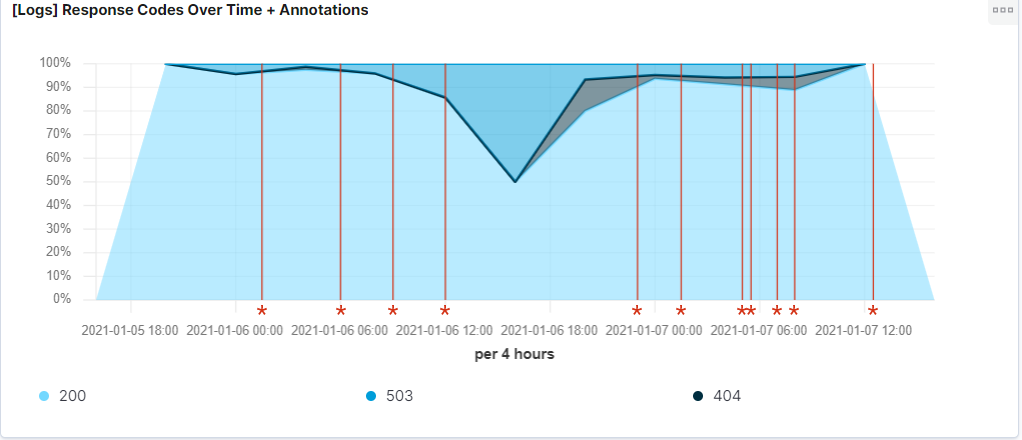
Answer the following questions:

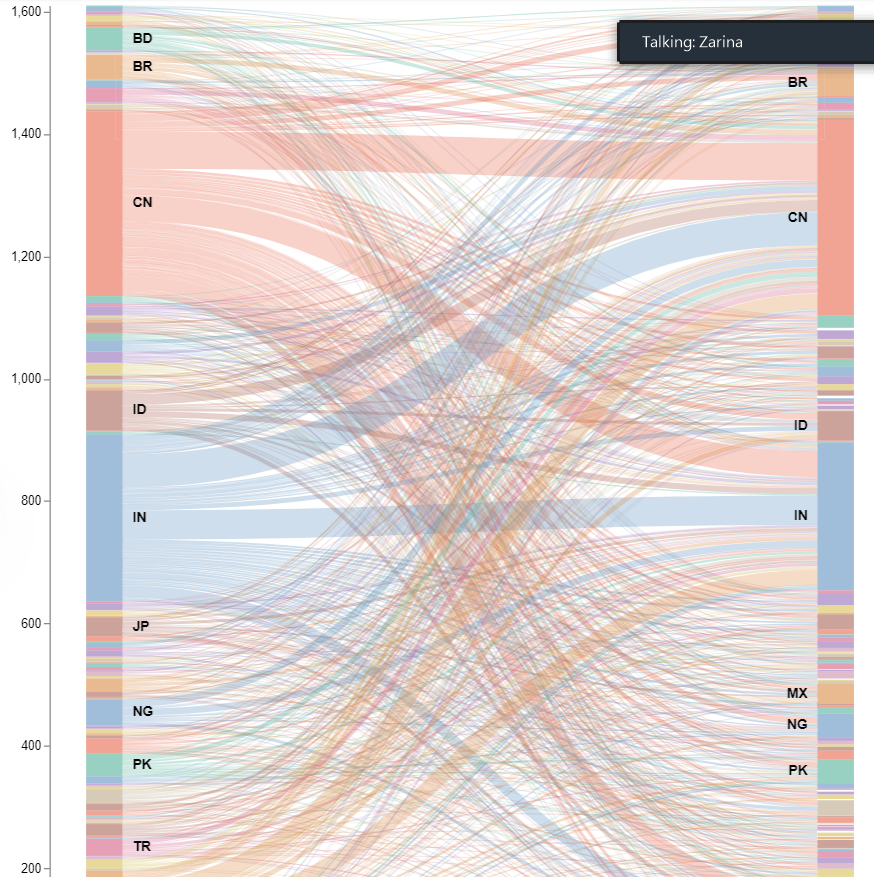
* + In the last 7 days, how many unique visitors were located in India? 245

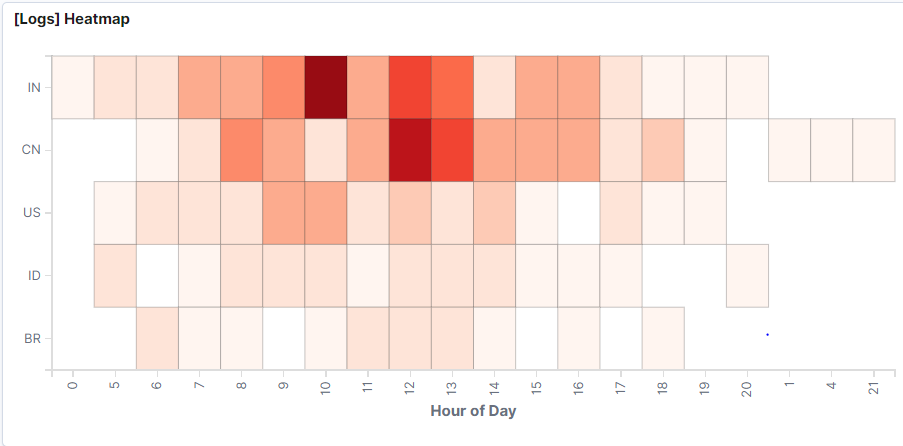


* + In the last 24 hours, of the visitors from China, how many were using Mac OSX? 10 visitors



* + In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 100% (503)1/5/21-1/6/21 & 50%-90% (404) 1/5/21-1/6/21
  + 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? 12 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).

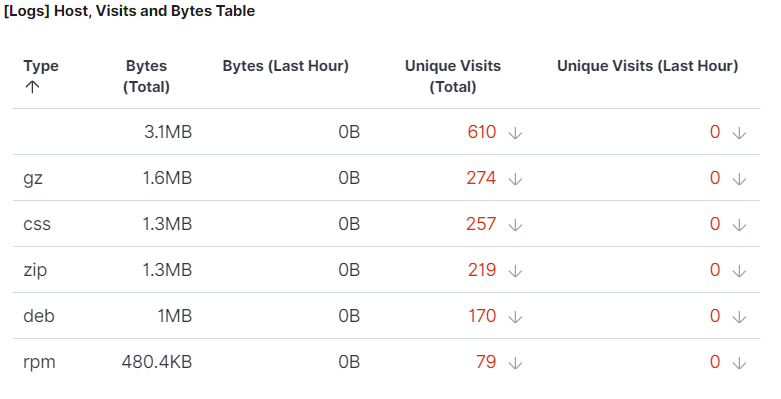
gz- Zipped archive files

css- Used to format the contents of an associated Web page

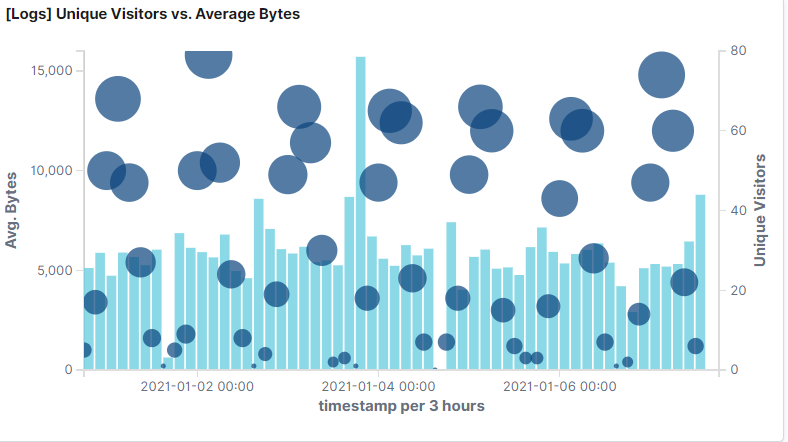
zip- archives file

deb- Two TAR archives that make up the executable files and documents

rpm-Red Hat Package Manager file that's used to store installation packages on Linux

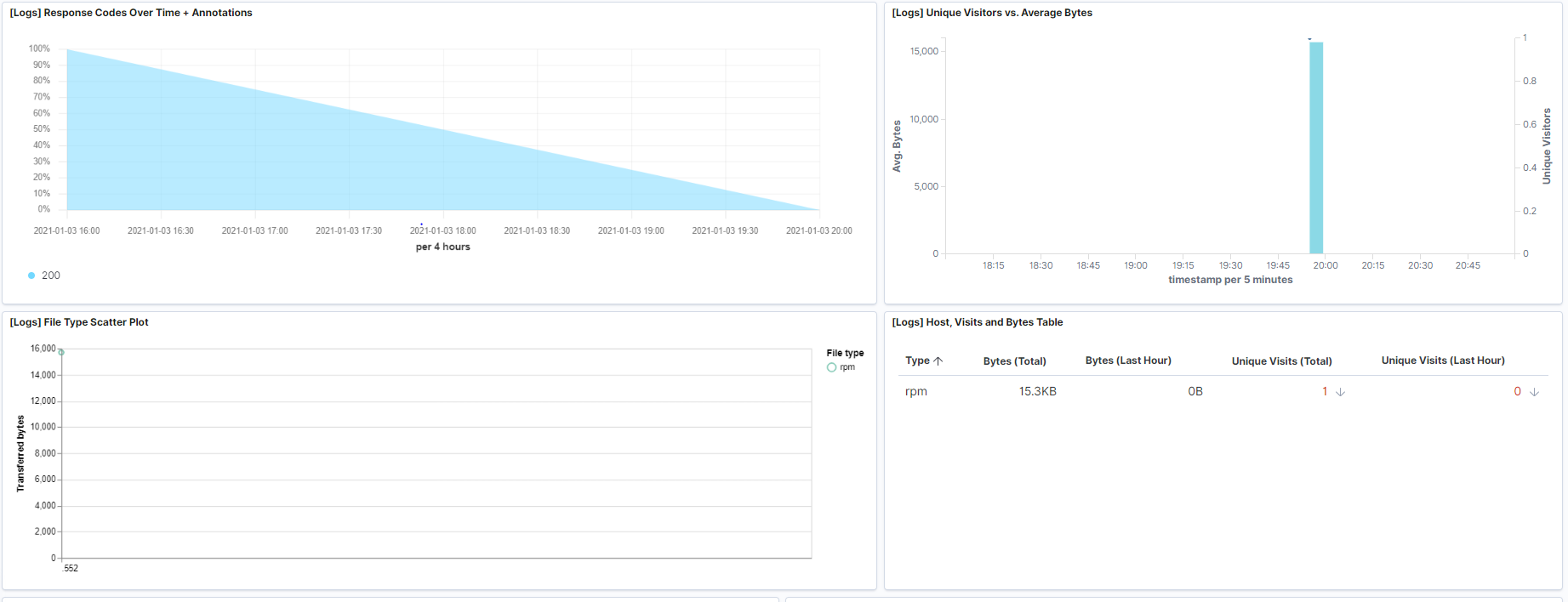


1. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.
   * Locate the time frame in the last 7 days with the most amount of bytes (activity). 1/04/2021

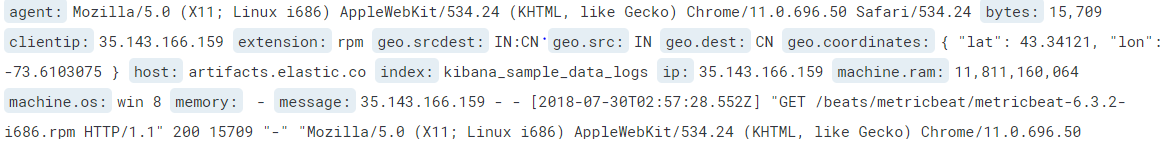


* + In your own words, is there anything that seems potentially strange about this activity? There is more activity on 1/4/21. The baseline is around 5,000 bytes and then there was a huge spike. It was three times the normal amount of traffic for that time of day.

1. Filter the data by this event.
   * What is the timestamp for this event? 8:00 pm
   * 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? 200





1. 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

1. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing? They were downloading a package manager from the server.
   * Was the file they downloaded malicious? If not, what is the file used for? It does not look malicious and is used to install packages.
   * Is there anything that seems suspicious about this activity? Yes, because the byte count was very for that period and this could be a distraction for them doing something else behind the scenes.
   * Is any of the traffic you inspected potentially outside of compliance guidelines? Yes, normal baseline is 5000 bytes and it was outside of that