**Activity File: Exploring Kibana**  
Answer the following questions:  
  
 - In the last 7 days, how many unique visitors were located in India?

There were **245 unique visitors located in India.**

Graphical user interface

Description automatically generated with medium confidence  
  
 - In the last 24 hours, of the visitors from China, how many were using Mac OSX?

**There were** **68 visitors from China in the last 24 hours.**

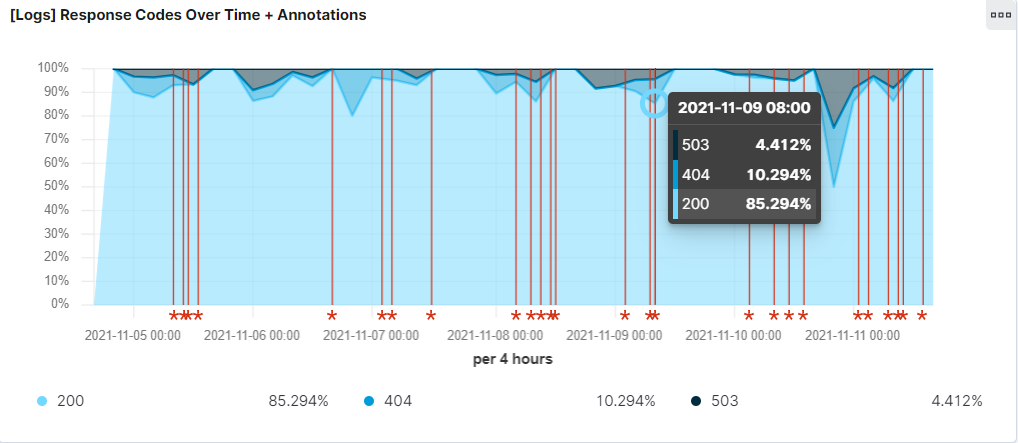
Graphical user interface, application

Description automatically generated

- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

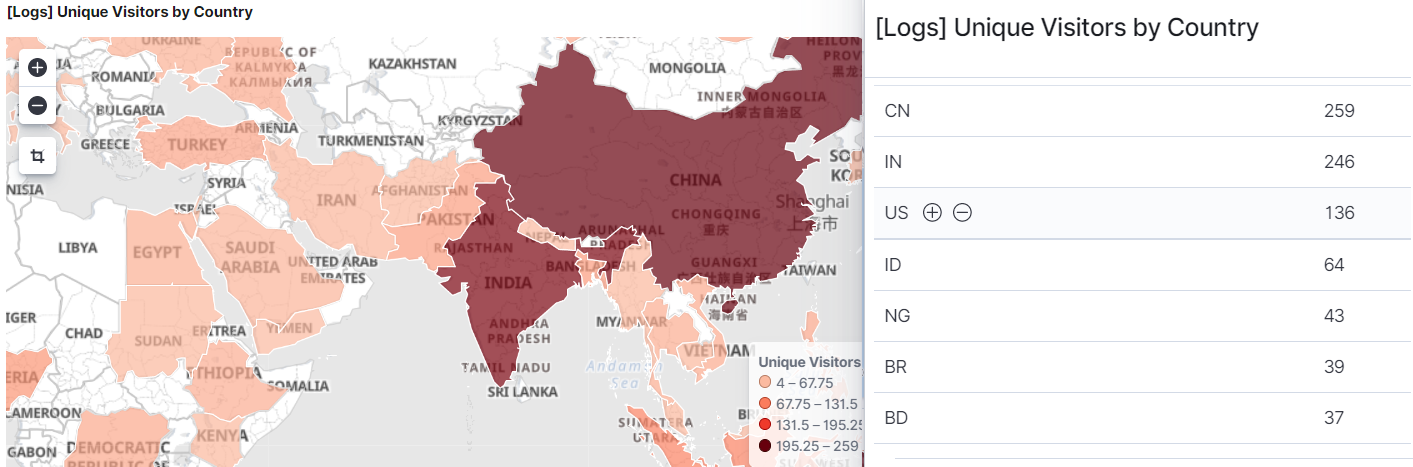
**404: 10.294%**

**503: 4.412%**



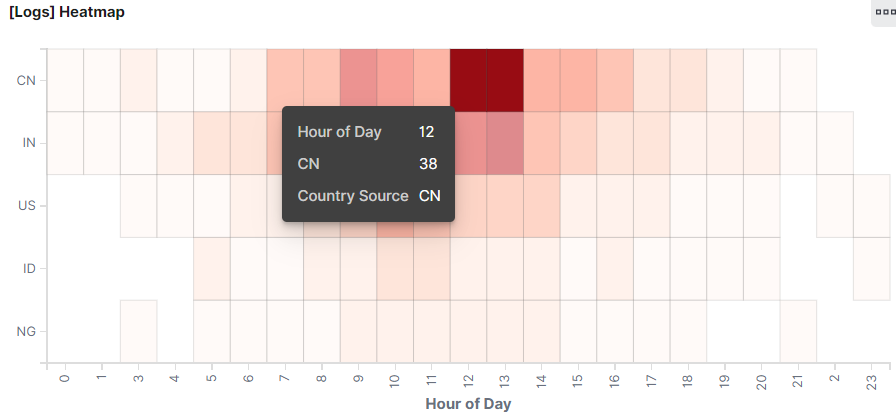
- In the last 7 days, what country produced the majority of the traffic on the website?

**China produced the majority of the traffic on the website in the last 7 days: 259**

****

- Of the traffic that's coming from that country, what time of day had the highest amount of activity?

**Between the hours of 12 P.M. and 1 P.M., the country had the highest amount of activity.**



- 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 –** a compressed zip file using the standard GNU zip compression algorithm.

**.css (Cascading Style Sheets) –** file used to format HTML elements on a webpage.

**.zip –** used to group multiple files in one compressed file to simplify file sharing, especially when sharing large file contents via email.

**.deb –** is a Debian Unix archive that contains software package files for download on a terminal.

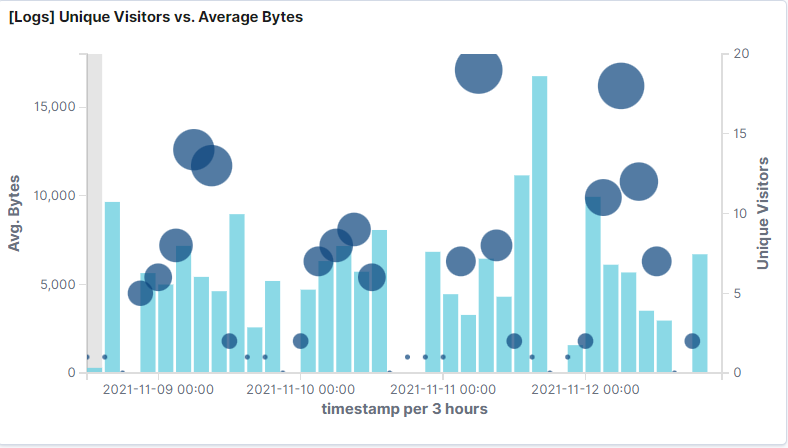
**.rpm (Red Hat Package Manager) –** used to store installation packages on Linux OS.

Table

Description automatically generated

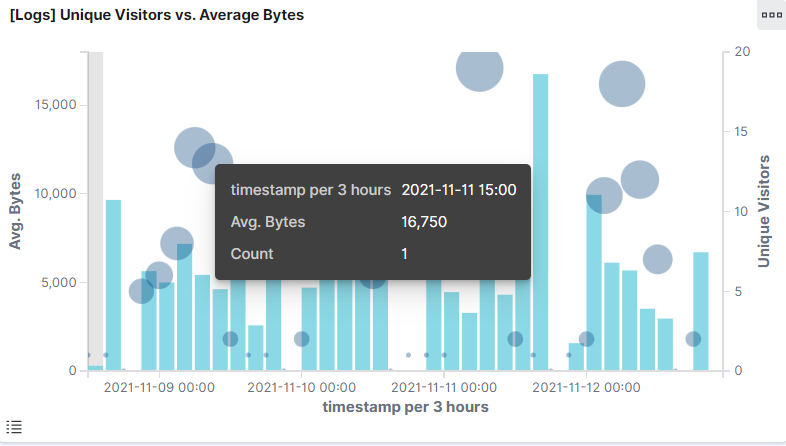
3. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.

- 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?

**There is 1 visitor is using a high volume of bytes compared to usage of other visitors count and avg. bytes**



4. Filter the data by this event.

Graphical user interface, application

Description automatically generated

- What is the timestamp for this event? **Nov 08, 2021 @ 14:03 to Nov 12, 2021 @ 23:00. The time stamp is 15:00.**

Graphical user interface, application, Word

Description automatically generated

- What kind of file was downloaded? **A .gz file was downloaded.**

Chart

Description automatically generated with medium confidence

- From what country did this activity originate? **China**

- What HTTP response codes were encountered by this visitor? **200 ok**

A picture containing timeline

Description automatically generated

5. Switch to the Kibana Discover page to see more details about this activity.  
 - What is the source IP address of this activity? **1.145.31.121**

A picture containing text

Description automatically generated  
 - What are the geo coordinates of this activity? **{‘lat”: 28.28980556, “lon”: -81.43708333**

Text

Description automatically generated

- What OS was the source machine running? **Windows 8**

A picture containing diagram

Description automatically generated

- What is the full URL that was accessed?

[**https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-linux-x86\_64.tar.gz**](https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-linux-x86_64.tar.gz)

Graphical user interface, text, application

Description automatically generated

- From what website did the visitor's traffic originate? **Elastic-elastic-elastic.com**

Text, application

Description automatically generated

6. Finish your investigation with a short overview of your insights.   
  
 - What do you think the user was doing?

**It appears the individual is trying to download a linux file from the website.**

- Was the file they downloaded malicious? If not, what is the file used for?

**The user is downloading a “Free and open-source software browser engine” named Gecko; which is created by Mozilla and used on the Firefox. The downloaded file is not malicious, but alterations to the library list can make it malicious.**

- Is there anything that seems suspicious about this activity?

**The Gecko linux package was designed to support open internet standards, however, by tampering with the library lists, which is loaded automatically, the individual (with malicious intent) can create potential malicious downloads such as: spyware, keyloggers, etc. This malicious download can be bypassed without suspicion.**

- Is any of the traffic you inspected potentially outside of compliance guidelines?

**It doesn’t appear to be outside of compliance guidelines, however, further monitoring of the specified user can help in ascertaining information of any, if at all, suspicious activities.**