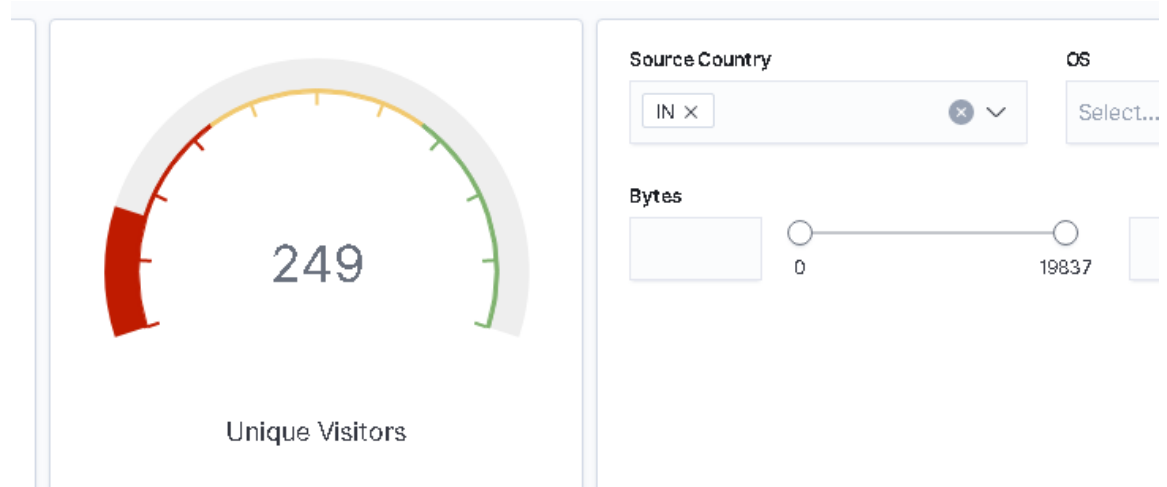
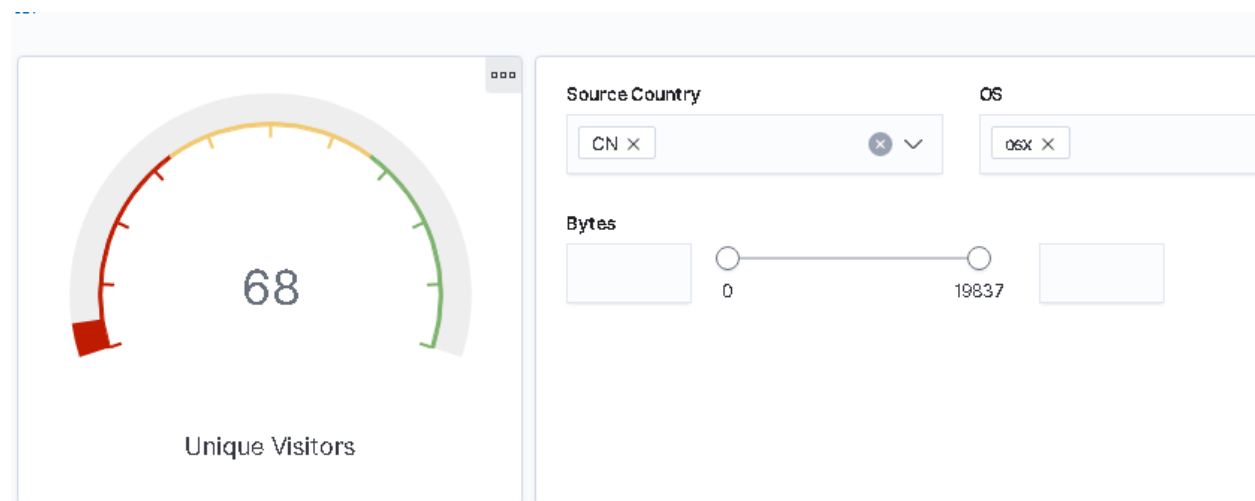


## EXPLORING KIBANA

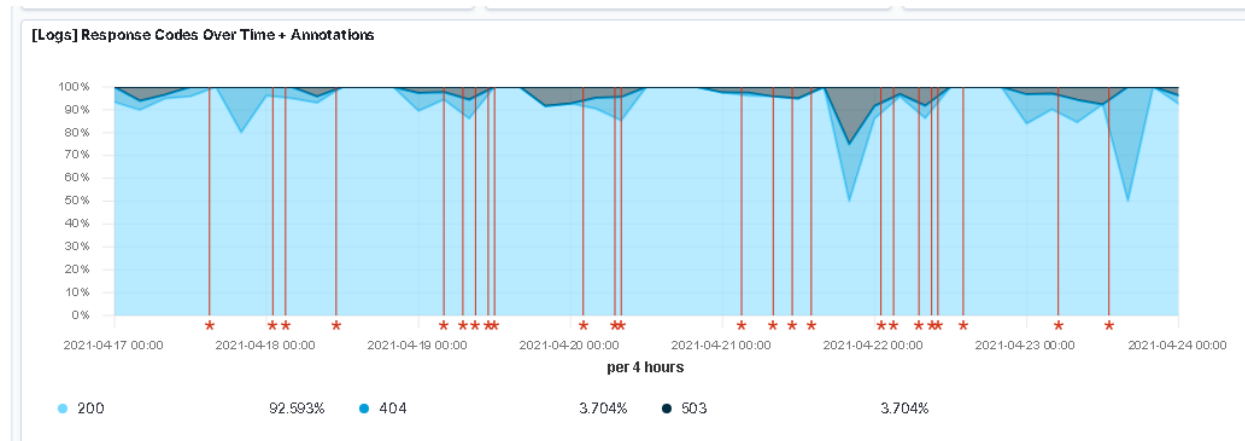
1. Add the sample web log data to Kibana.
2. Answer the following questions:
  - In the last 7 days, how many unique visitors were located in India? **249**



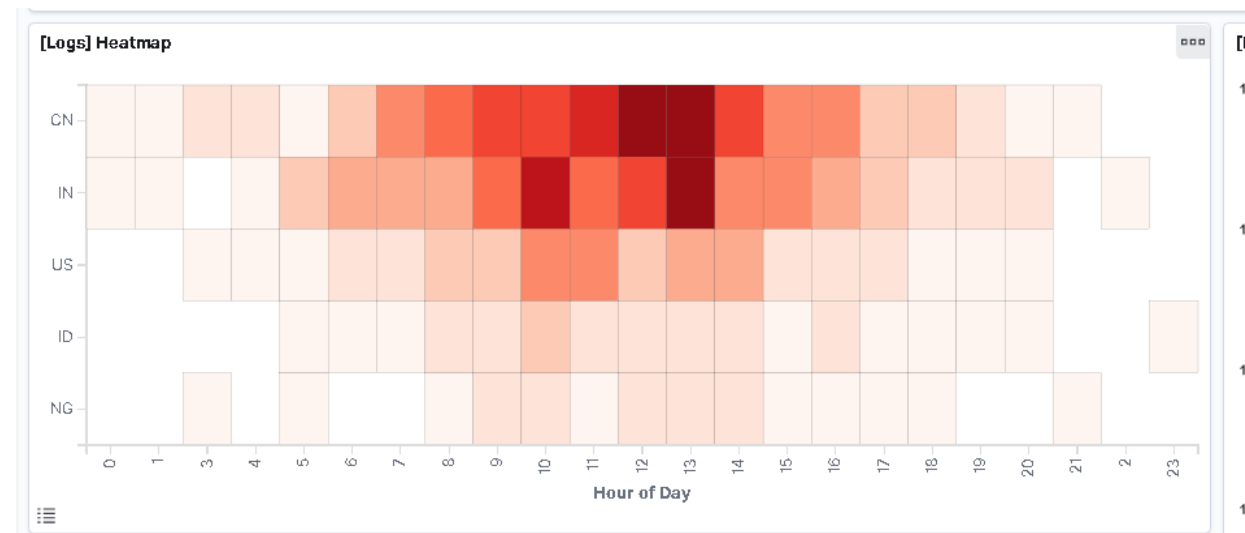
- In the last 24 hours, of the visitors from China, how many were using Mac OSX? **68**



- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? **3.704% and 3.704%**



- 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?

**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).

[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	3.2MB	24KB	618 ↓	5 ↓
gz	1.6MB	13.6KB	286 ↓	2 ↓
css	1.4MB	0B	265 ↓	0 ↓
zip	1.2MB	14.7KB	208 ↓	3 ↓
deb	1.1MB	15.6KB	169 ↓	1 ↓
rpm	441.3KB	0B	67 ↓	0 ↓

**gz:** .gz files that are compressed using the gzip method

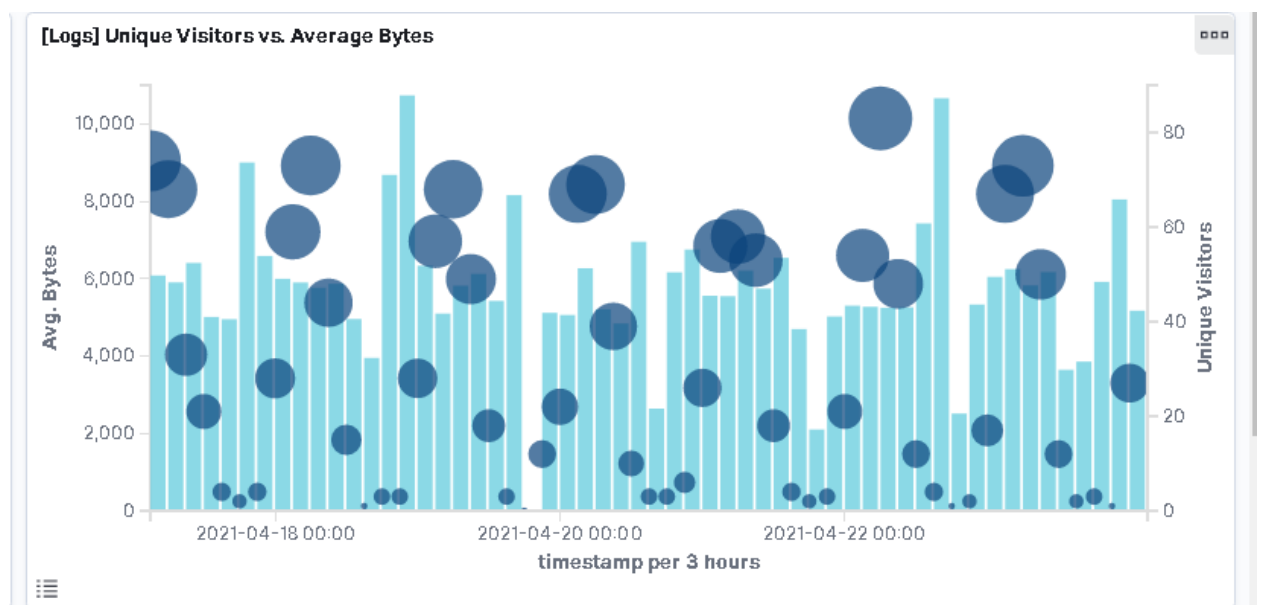
**css:** .css files that can help change the appearance of HTML code on a webpage.

**zip:** Another compression format for files

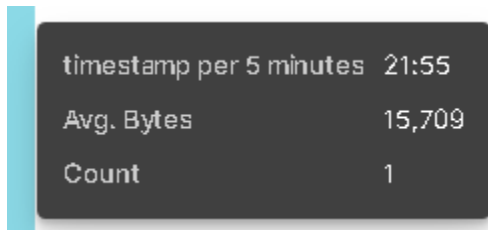
**Deb:** A file that's a Debian (Linux) Software package file and that can be opened by using a package manager.

**rpm:** .rpm file formats are a Red Hat Software Package file

- 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.



4. Locate the time frame in the last 7 days with the most amount of bytes (activity).



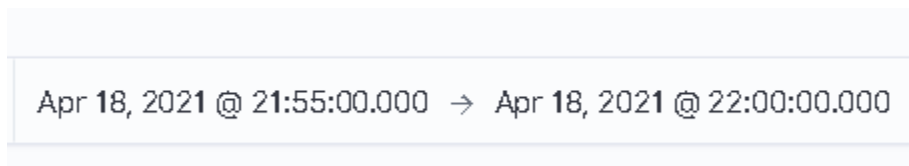
timestamp per 5 minutes	21:55
Avg. Bytes	15,709
Count	1

5. In your own words, is there anything that seems potentially strange about this activity?

- It is potentially strange because that is a lot of bytes for a single user.

6. Filter the data by this event.

- o What is the timestamp for this event?



Apr 18, 2021 @ 21:55:00.000 → Apr 18, 2021 @ 22:00:00.000

- o What kind of file was downloaded?

RPM

Type ↑	Bytes (Total)	Bytes (Last Hour)	U
rpm	15.3KB	15.3KB	

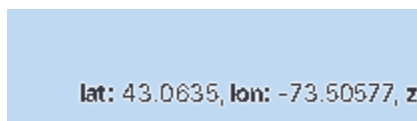
- o From what country did this activity originate?

India

- o What HTTP response codes were encountered by this visitor? 200 OK

7. Switch to the Kibana Discover page to see more details about this activity.

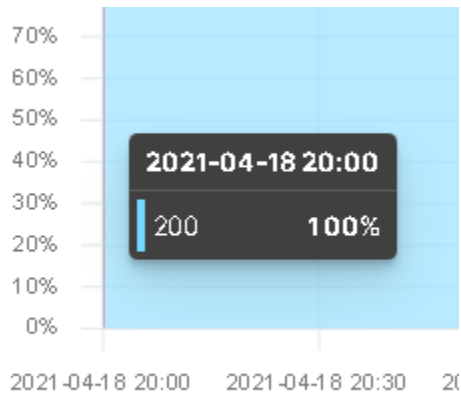
- o What is the source IP address of this activity? 34.143.154.129
- o What are the geo coordinates of this activity?



lat: 43.0635, lon: -73.50577, z

- o

- What HTTP response codes were encountered by this visitor?



- What OS was the source machine running? **Windows 8**
  - From what website did the visitor's traffic originate? **FB**
8. Finish your investigation with a short overview of your insights.
- What do you think the user was doing? Downloading a Linux package
  - Was the file they downloaded malicious? If not, what is the file used for?  
Typically not malicious, but can be. Might be performing an update
  - Is there anything that seems suspicious about this activity? Main concern is that it was through Facebook
  - Is any of the traffic you inspected potentially outside of compliance guidelines? Monitor this person more closely, just in case.