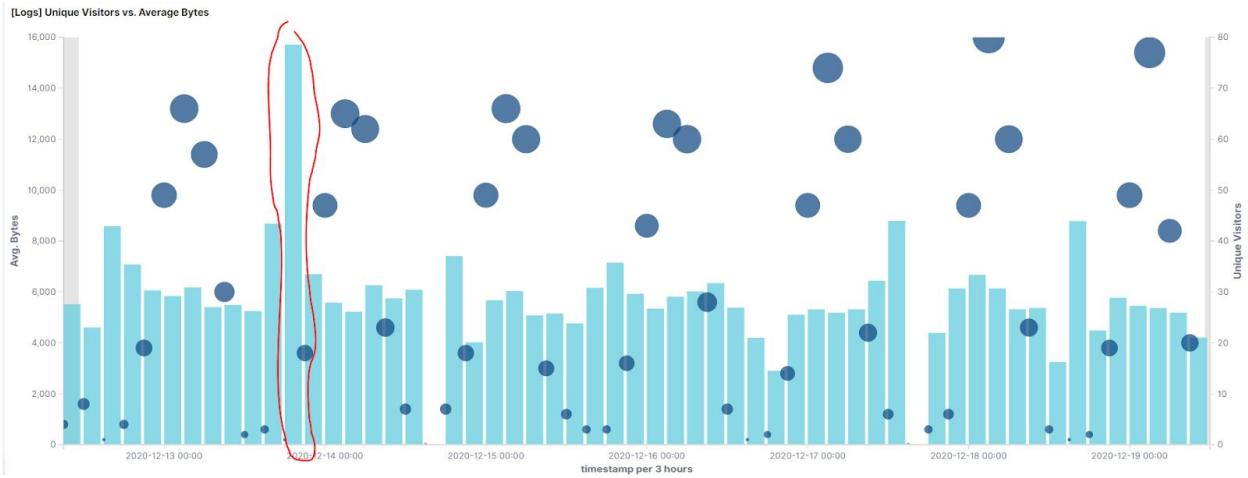
ELK Questions

In the last 7 days, how many unique visitors were located in India?
251
In the last 24 hours, of the visitors from China, how many were using Mac OSX?
9
In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?
404: 100%, 503: 0%
In the last 7 days, what country produced the majority of the traffic on the website?
USA
Of the traffic that's coming from that country, what time of day had the highest amount of activity?
afternoon
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).
css - css stylesheet, tells html how to look
gz - gzip file, it's zipped
zip - zip file - also zipped
deb - UNIX archive, will install a debian-based OS
rpm - red hat package manager, another UNIX archive, red hat this time

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 only one visitor at the time of the largest byte traffic spike

What is the timestamp for this event?
19:55
What kind of file was downloaded?
rpm
From what country did this activity originate?
India

What HTTP response codes were encountered by this visitor?
200

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
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?
http://facebook.com/success/jay-c-buckey

What do you think the user was doing?
Downloading a red hat archive file
Was the file they downloaded malicious? If not, what is the file used for?
No, it is used to set up services on Red Hat OS
Is there anything that seems suspicious about this activity?
No, this is a normal download
Is any of the traffic you inspected potentially outside of compliance guidlines?
No, no error codes were received and the download was a legitimate program and did not compromise server availability.