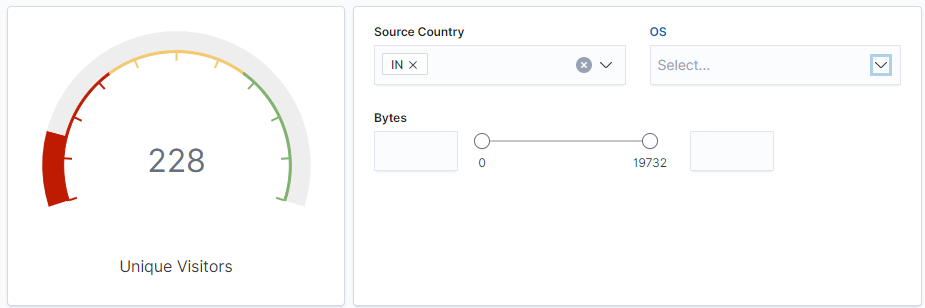
**Exploring Kibana**

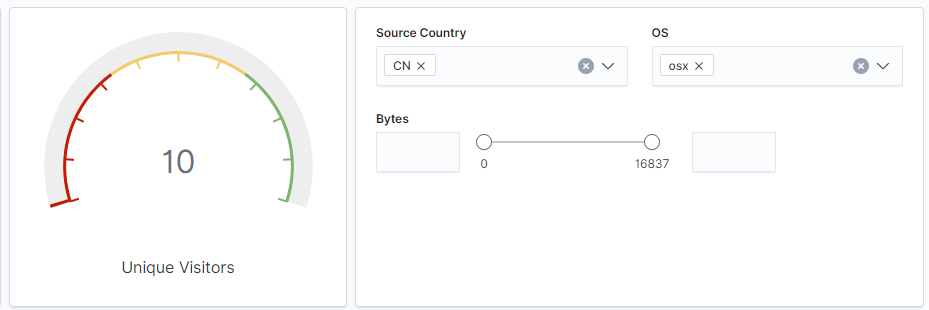
**Aaron Plekan**

1. Answer the following questions:  
     
   * In the last 7 days, how many unique visitors were located in India?



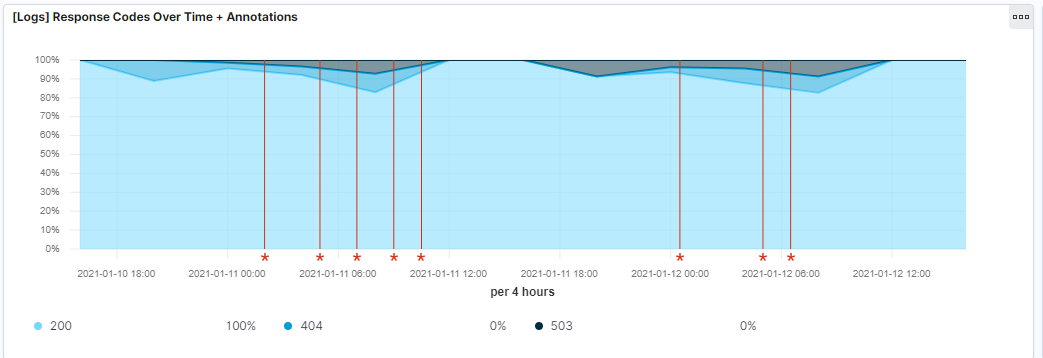
There were a total of 228 unique visitors in the past 7 days.

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



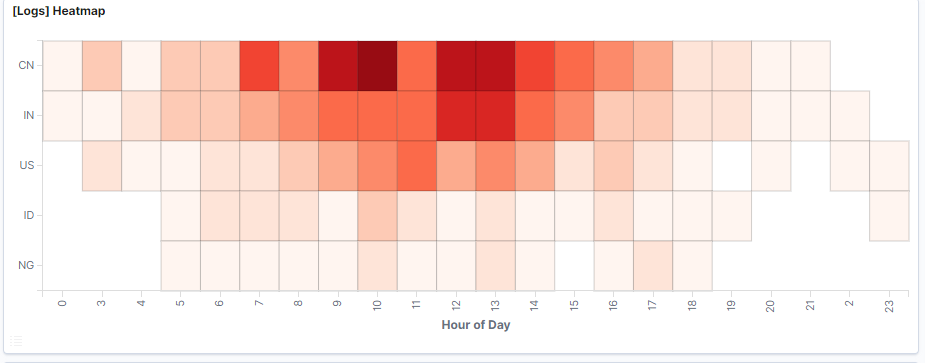
There were a total of 10 visitors using the OSX from China.

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



When looking at this graph, it appears that 0% have received the 404 or 503 errors.

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

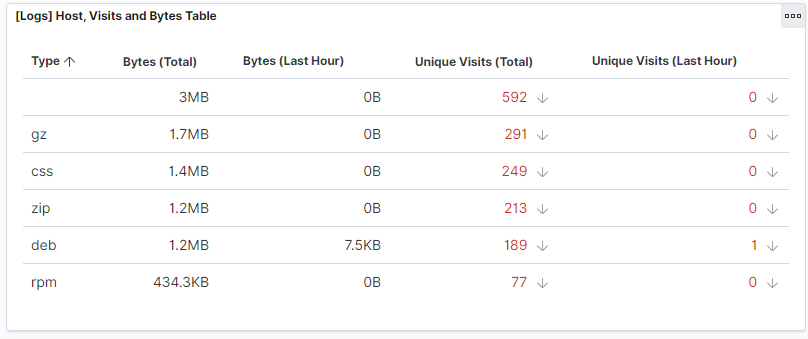


When looking at the logs, China had the most amount of traffic in 7 days.

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

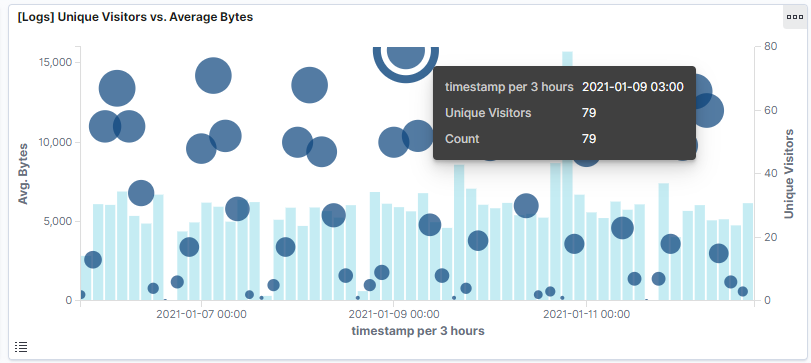
When we are looking at the heat map from the previous question, you can see that the most traffic was coming in around the lunch hour. It was between 7am-3pm.

* 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).



A GZ file is an archive file that is compressed by the standard gzip. It contains one or more files. CSS file stands for cascading style sheet. It is typically used to format the contents of a webpage. It helps with displaying HTML elements. Zip is exactly the same as Gzip above but is a slightly slower method. A deb file is a Debian software package file. They are mostly used in Unix-based operating systems and consist of two TAR archives. The last one is the RPM file, which stands for red package manager file. It is used to store installation packages on the linux operating systems.

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).

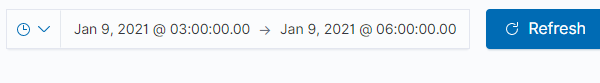


The most amount of activity was on january 9 at 3pm.

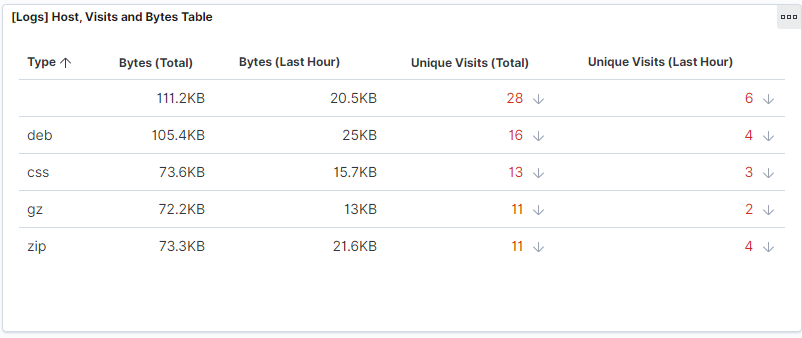
* In your own words, is there anything that seems potentially strange about this activity?

The reason why I could see this activity to be strange is because it is occurring on a saturday. Over the weekend most people are away from their computers/jobs and that can always be a time that people are gonna try and get into stuff. It is always the perfect time to try to hack into something when people aren't at their jobs.

1. Filter the data by this event.  
     
   * What is the timestamp for this event?

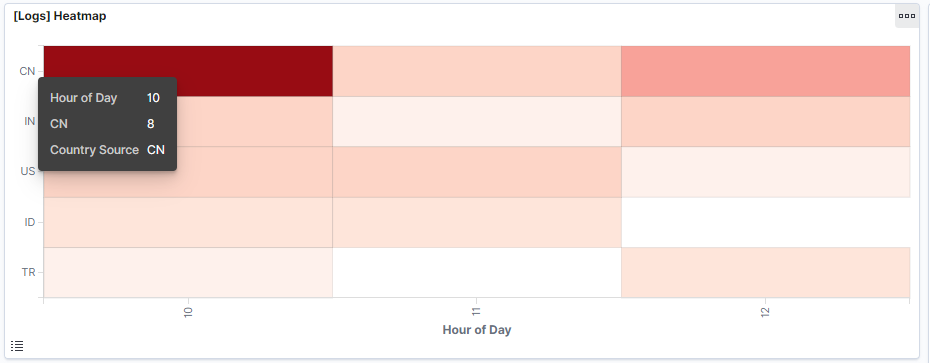


* What kind of file was downloaded?



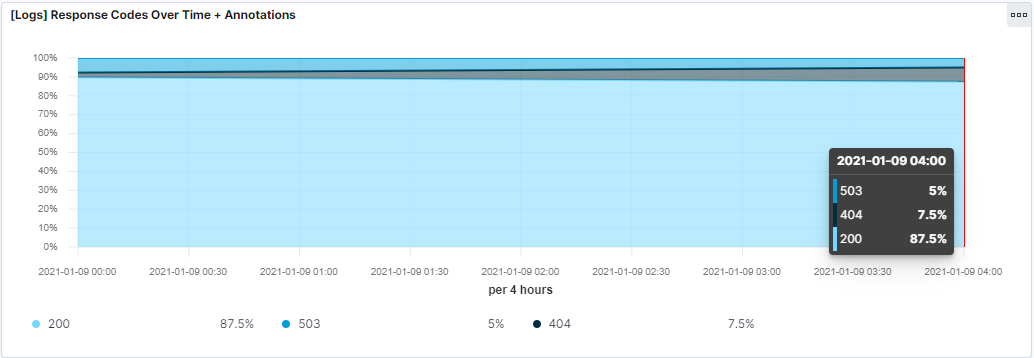
Different types of files were downloaded but the deb file was the most downloaded

* From what country did this activity originate?



China was the country of origin.

* What HTTP response codes were encountered by this visitor?



87.5% were the 200 code and 7% encountered the 404 code. 5% were the 503 code.

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



* What are the geo coordinates of this activity?



* What OS was the source machine running?



* What is the full URL that was accessed?



* From what website did the visitor's traffic originate?



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

From what I see, the user was trying to download something from a twitter account. At least that is what they were coming from and then downloading a zip file.

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

It is hard to tell if it was truly malicious but from what I see, it was not malicious. I believe the viewer saw something that they really liked and wanted to download something for them to save. It looks like something about success and that the viewer maybe saw a good quote that they wanted to save.

* Is there anything that seems suspicious about this activity?

In my opinion I do not see anything suspicious about this activity. I would have to dive deeper potentially but looking at it initially poses no threat.

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

Most of the traffic that I was seeing was actually coming from facebook or twitter. It was mostly stuff about success and a bunch of different names. It doesn't look overly suspicious.