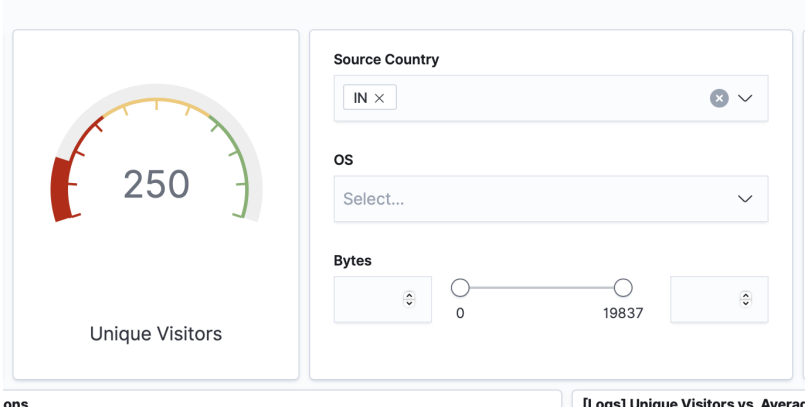
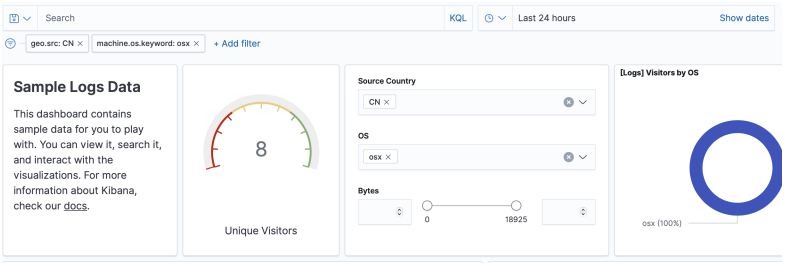
Kaleigh Glatfelter

Exploring Kibana

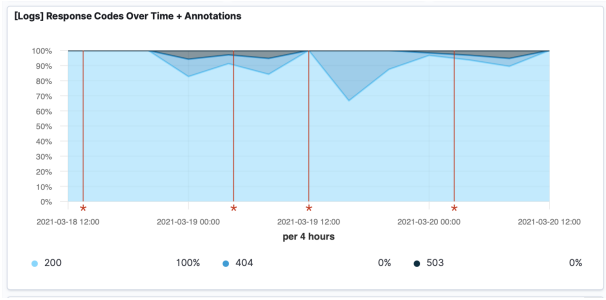
1. Answer the following questions:
    a. In the last 7 days, how many unique visitors were located in India? **250**



    b. In the last 24 hours, of the visitors from China, how many were using Mac OSX? **8**



    c. In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? **404- 0%, 503- 0%**



d. In the last 7 days, what country produced the majority of the traffic on the website? **China - 263 unique visitors**

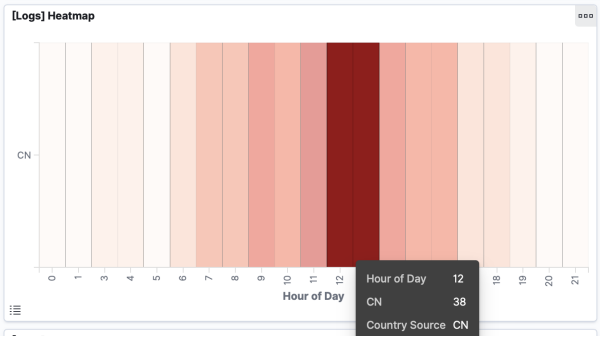
[Logs] Unique Visitors by Country

View: Data

Download CSV

geo.src: Descending	Unique Visitors
CN	263
IN	250
US	122
ID	58

e. Of the traffic that's coming from that country, what time of day had the highest amount of activity? **12pm and 1pm**



f. 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).
   i. gz: compressed files using gzip utility
   ii. zip: file containing one or more files/directories that have been compressed into one file.
   iii. css: defines formatting for HTML information on a webpage (like font, colors, borders, etc).
   iv. deb: Debian (Linux) Software Package file, installed using apt.
   v. rpm: Red Hat Software Package file.

[Logs] Host, Visits and Bytes Table

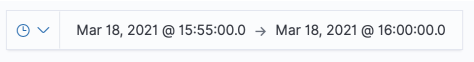
Type	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	553.2KB	3.2KB	113	1
gz	362.2KB	0B	63	0
zip	304.4KB	0B	50	0
css	215.5KB	0B	44	0
deb	278.6KB	0B	37	0
rpm	26.8KB	0B	7	0

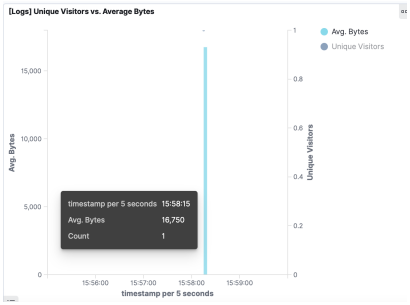
2. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.
   a. Locate the time frame in the last 7 days with the most amount of bytes (activity).

b. In your own words, is there anything that seems potentially strange about this activity? **It is strange that only 1 user is utilizing a considerable amount of bytes, much larger than all the other usage.**

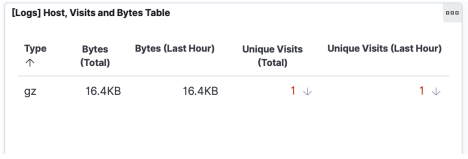
4. Filter the data by this event.

a. What is the timestamp for this event?

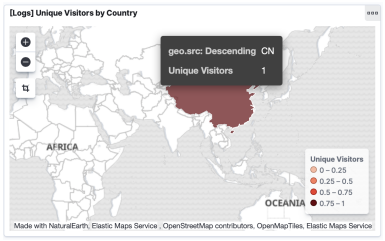




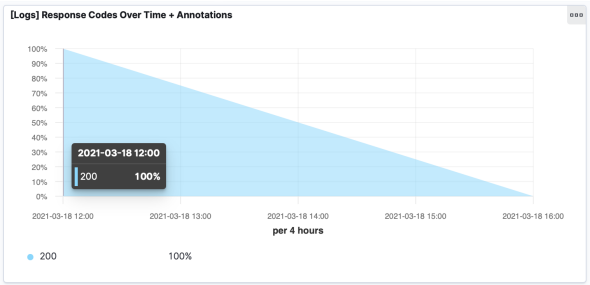
b. What kind of file was downloaded? **A gz compressed file was downloaded.**



c. From what country did this activity originate? **China**



d. What HTTP response codes were encountered by this visitor? **200 OK**



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

a. What is the source IP address of this activity?

clientip 1.145.31.121

b. What are the geo coordinates of this activity?

geo.coordinates
```
{
  "lat": 28.28980556,
  "lon": -81.43708333
}
```

c. What OS was the source machine running?

machine.os win 8

d. What is the full URL that was accessed?

url https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-linux-x86_64.tar.gz

e. From what website did the visitor's traffic originate?

referer http://www.elastic-elastic-elastic.com/success/aleksandr-serebrov

6. Finish your investigation with a short overview of your insights.

a. What do you think the user was doing? **It looks like the user is trying to download a tar file from a linux server for a Kibana download.**

b. Was the file they downloaded malicious? If not, what is the file used for? **More than likely it is not malicious, being that it looks to be an update for Kibana on a Linux server.**
c. Is there anything that seems suspicious about this activity? **I would say no, as it looks like the user is just trying to download the Linux version of Kibana onto his own server.**
d. Is any of the traffic you inspected potentially outside of compliance guidelines? **No, it looks like the user accessed the .gz file from an online Elasticsearch database.**