**Activity File: Exploring Kibana**

You are a DevOps professional and have set up monitoring for one of your web servers. You are collecting all sorts of web log data and it is your job to review the data regularly to make sure everything is running smoothly.

Today, you notice something strange in the logs and you want to take a closer look.

Your task: Explore the web server logs to see if there's anything unusual. Specifically, you will:

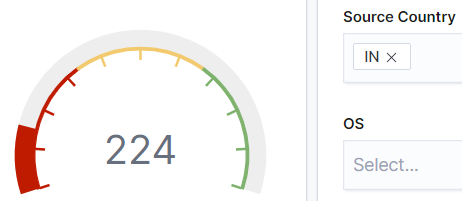
:warning: **Heads Up**: These sample logs are specific to the time you view them. As such, your answers will be different from the answers provided in the solution file.



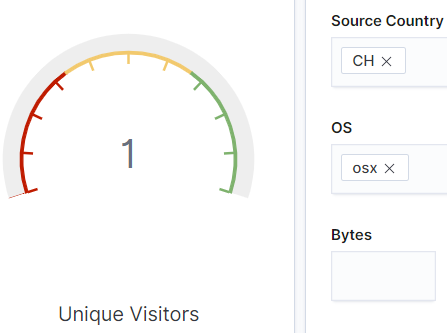
# Instructions

1. Add the sample web log data to Kibana.
2. Answer the following questions:

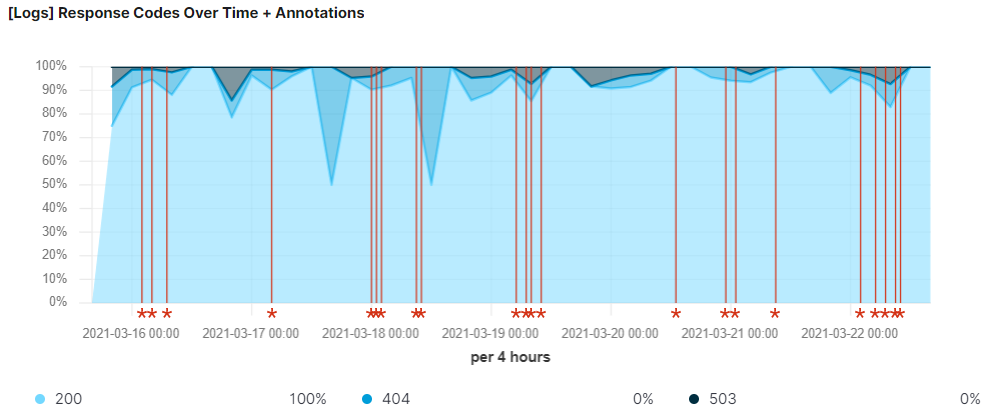
* In the last 7 days, how many unique visitors were located in India?



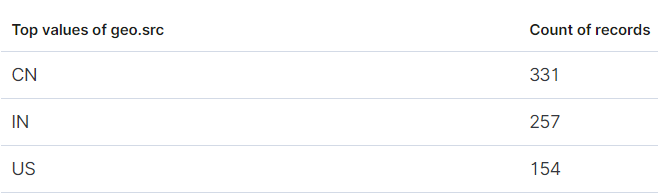
* In the last 24 hours, of the visitors from China, how many were using Mac OSX?



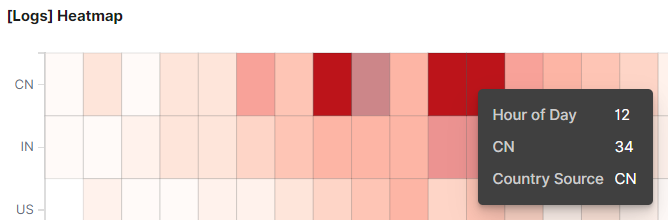
* In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?



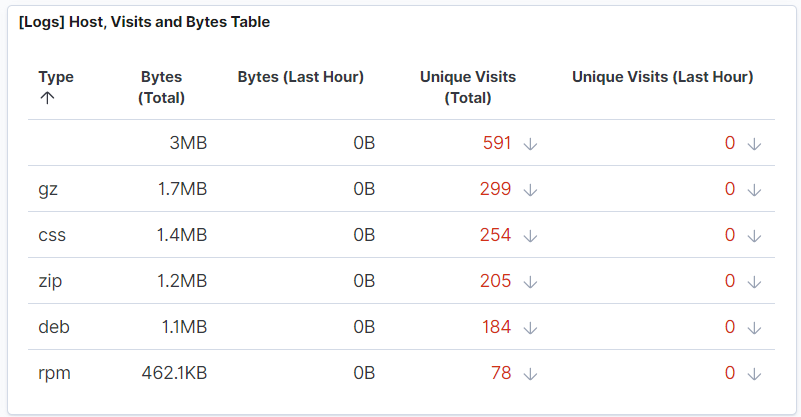
* In the last 7 days, what country produced the majority of the traffic on the website?



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

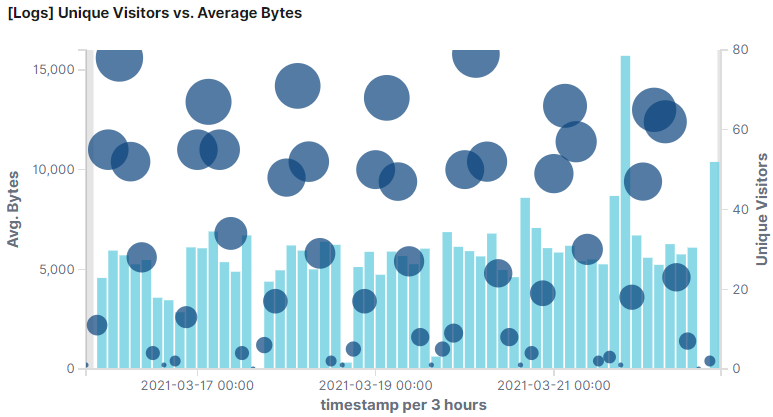


* List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).

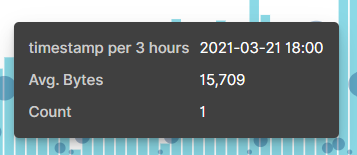


* + gz – An archived compressed file using gzip.
  + css – A cascading style sheet to format the HTML contents and styles for a webpage.
  + zip – An archived compressed file using zip.
  + deb – A file format and extension using the Debian Linux distribution.
  + rpm – A file format and extension using Red Hat Package Manager.

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.



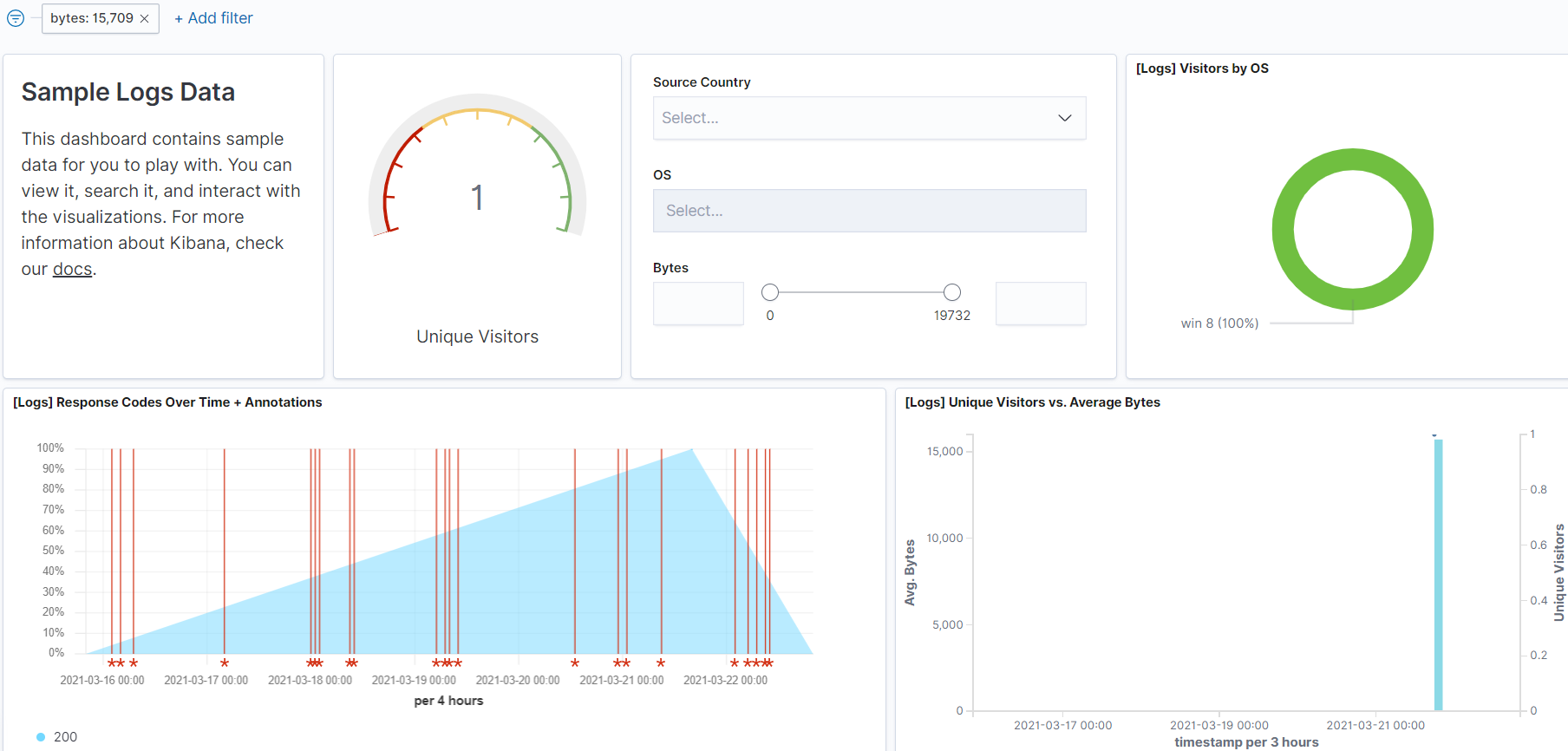
* Locate the time frame in the last 7 days with the most amount of bytes (activity).



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

This is the only visitor that is using a high number of bytes. The next user is using 9,430 bytes.

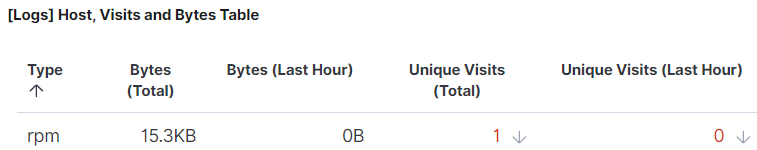
1. Filter the data by this event.



* What is the timestamp for this event?

The time filter shows between 03-16-2021 to 03-22-2021 @ 00:00. The timestamp for this is 18:00.

* What kind of file was downloaded?



* From what country did this activity originate?

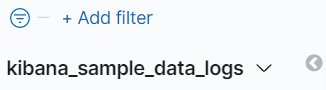


India.

* What HTTP response codes were encountered by this visitor?

200.

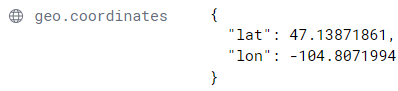
1. Switch to the Kibana Discover page to see more details about this activity.



* 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?

The use was trying to download a RPM package – metricbeat.

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

This could be malicious depending from what website this package is being downloaded from. Usually, RPM downloads are safe.

* Is there anything that seems suspicious about this activity?

The user is trying to update a package within Facebook.

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

No reason to do any updates or even if it’s allowed to do this from Facebook.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.