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:

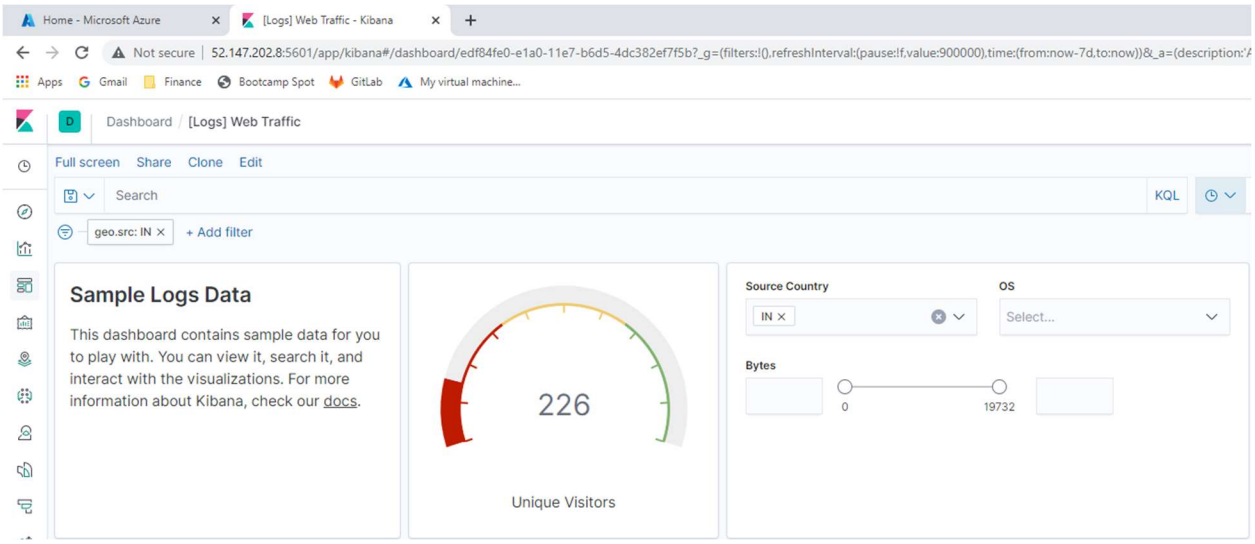
:warning: **Heads Up**: These sample logs are specific to the time you view them. As such, your answers will be different from the answers provided in the solution file.

Instructions

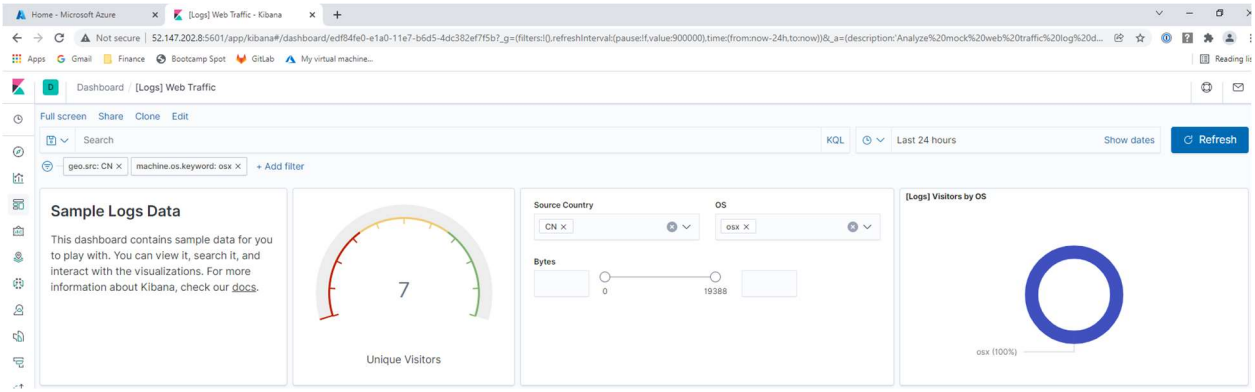
1. Add the sample web log data to Kibana.

2. Answer the following questions:

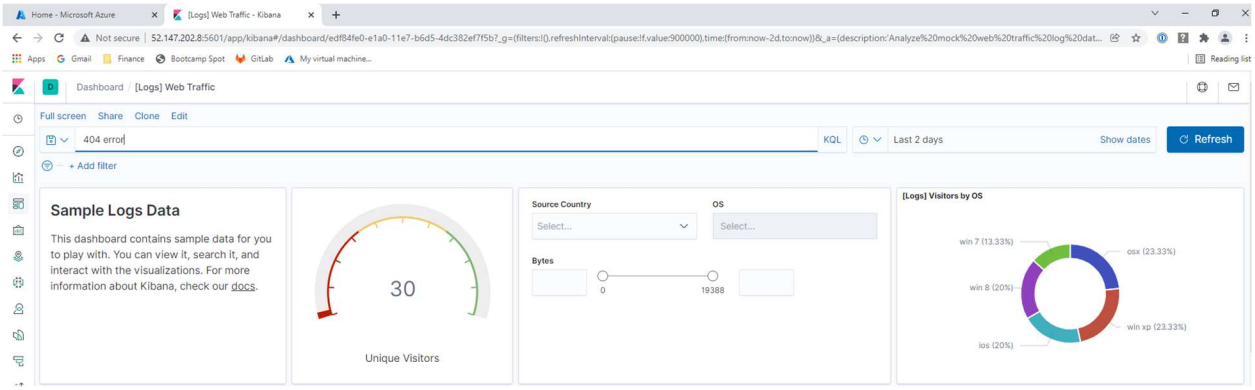
   - In the last 7 days, how many unique visitors were located in India? 226

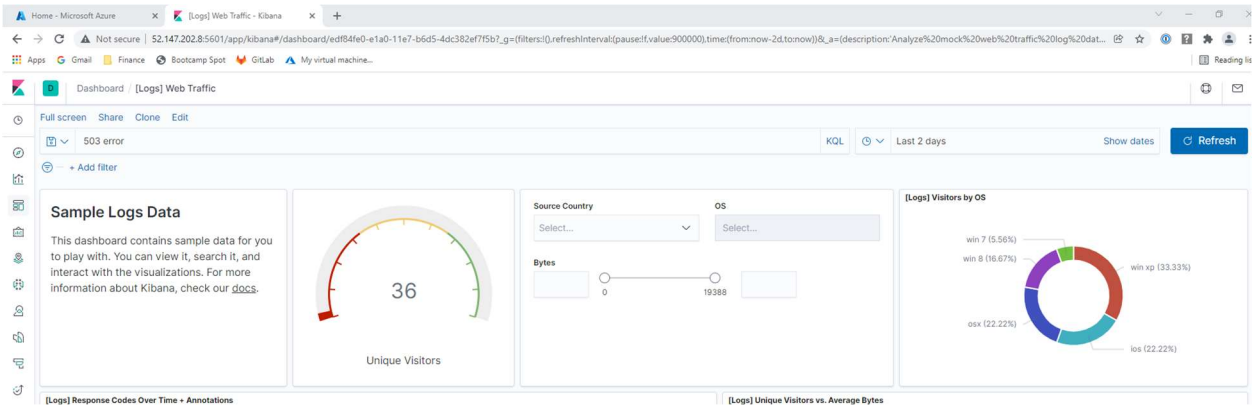


- In the last 24 hours, of the visitors from China, how many were using Mac OSX? 7

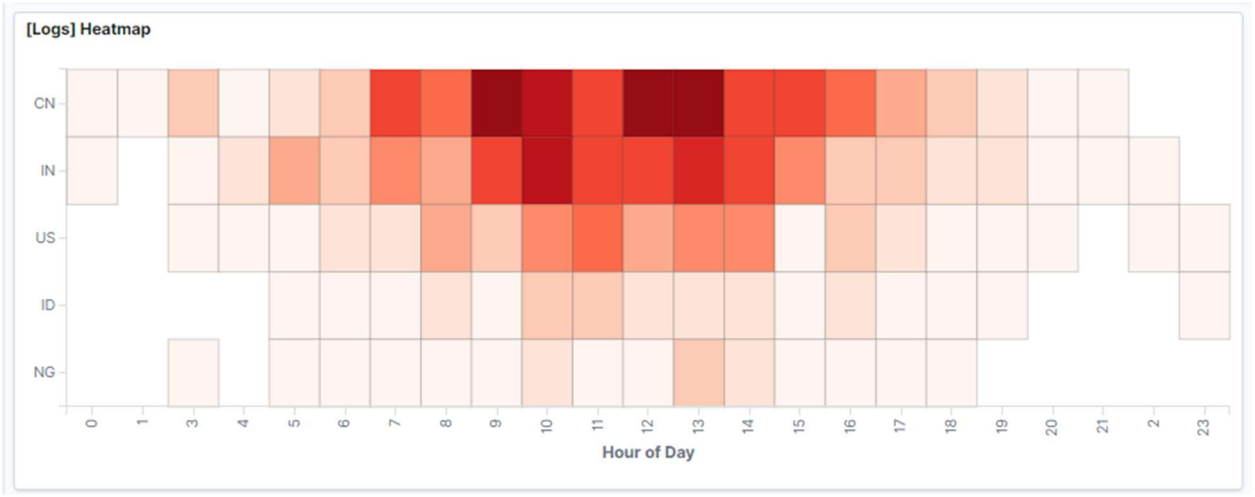


- In the last 2 days, what percentage of visitors received 404 errors? **30** How about 503 errors? **36**



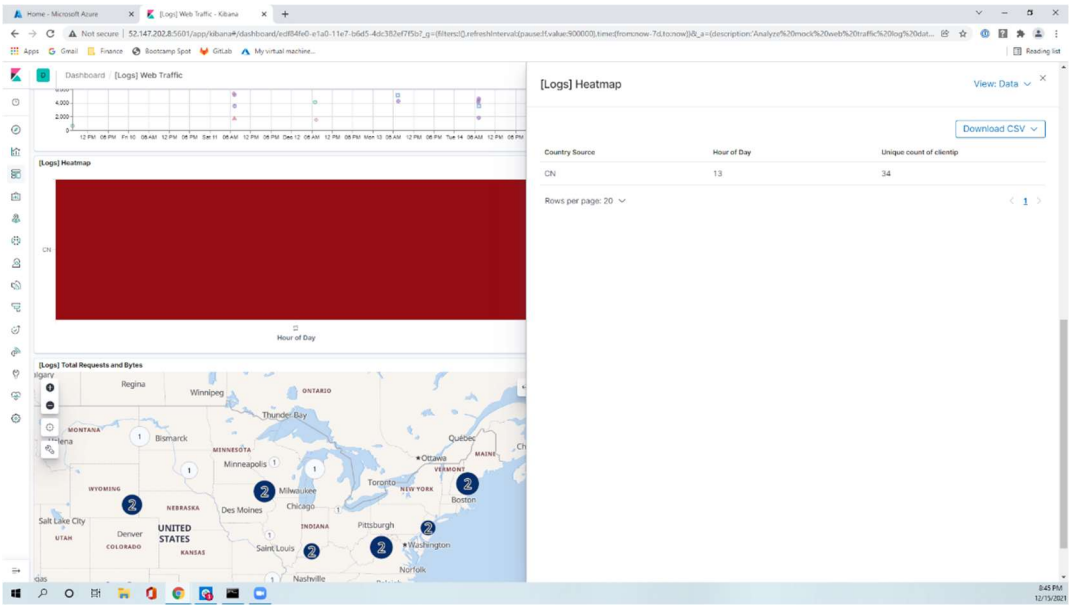


- In the last 7 days, what country produced the majority of the traffic on the website? **China**



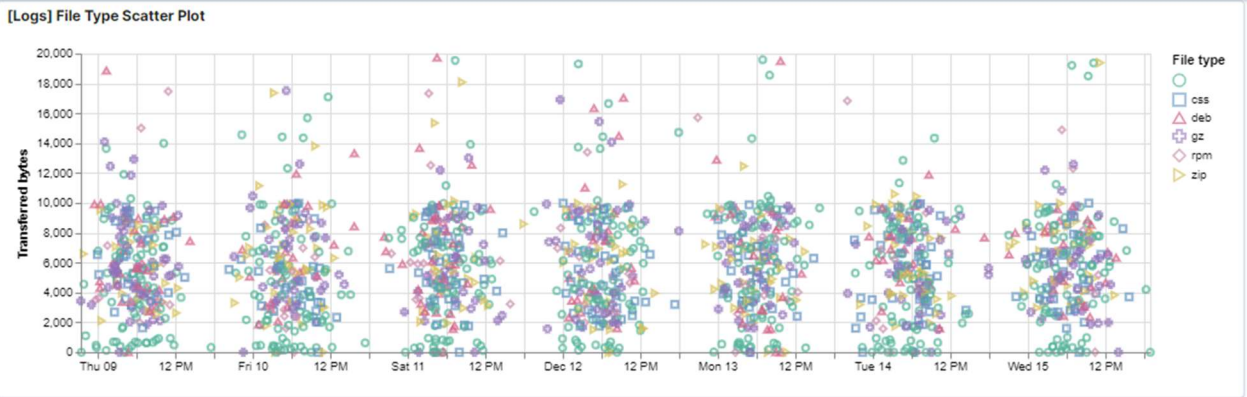
- Of the traffic that's coming from that country, what time of day had the highest amount of activity?

13:00 or 1:00pm



- 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 – Cascading Style Sheet**
- **Deb – Debian Software package**
- **Gz – GNU Zip**
- **RPM – Red Hat Package Manager**
- **Zip – Zip file**



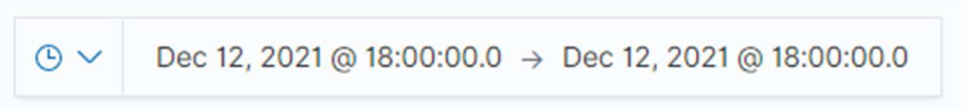
3. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.

- Locate the time frame in the last 7 days with the most amount of bytes (activity). **2021*12-12 18:00 (12851 bytes)**

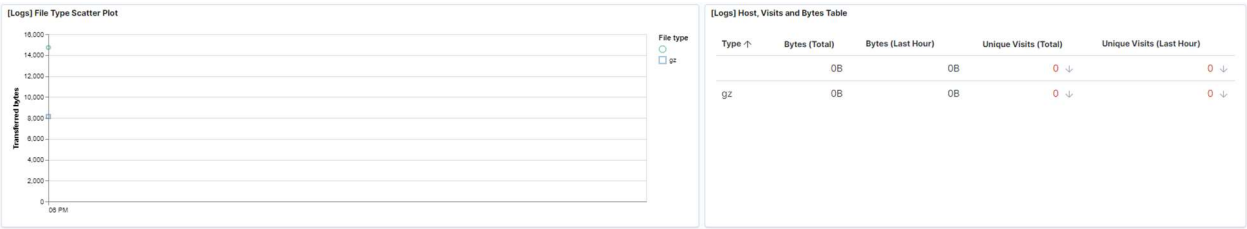
- In your own words, is there anything that seems potentially strange about this activity? **During this time, there was a low count of unique visitors.**

4. Filter the data by this event.

- What is the timestamp for this event? **December 12, 2021 @18:00:00.0**

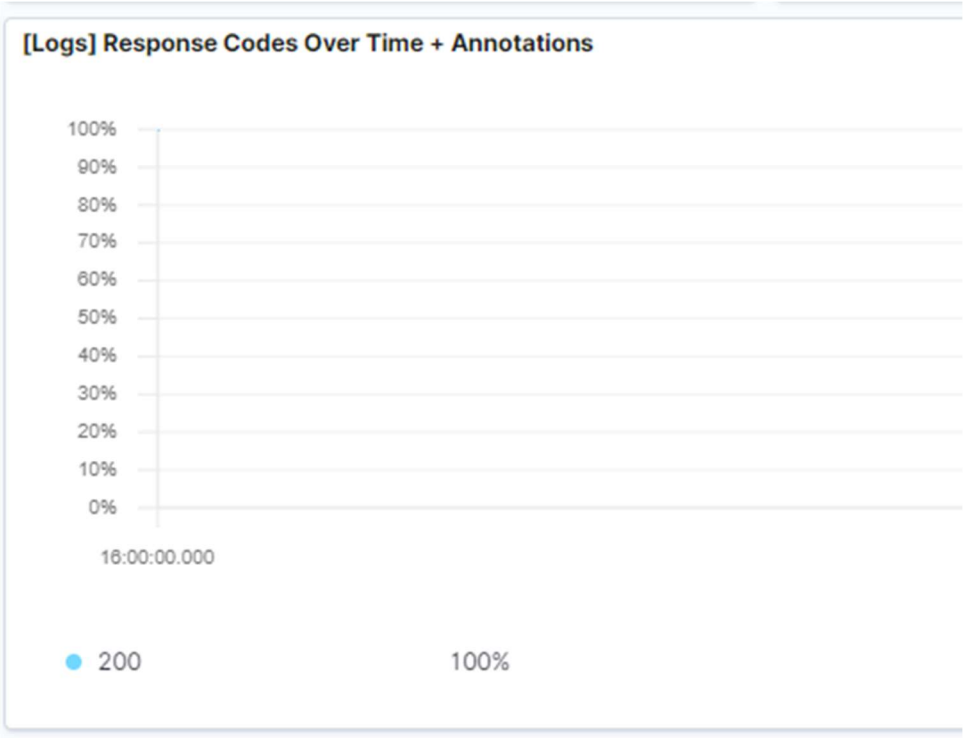


- What kind of file was downloaded? **Gz (RPM)**



- From what country did this activity originate? **India**

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



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

- What is the source IP address of this activity? **35.143.166.159**

clientip 35.143.166.159

- What are the geo coordinates of this activity?

- **Geo dest = China**
- **Geo Source = India**

t geo.dest CN

t geo.src IN

t geo.srcdest IN:CN

- What OS was the source machine running? **Windows 8**

t machine.os win 8

- What is the full URL that was accessed?

t url https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm

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

t referer http://facebook.com/success/jay-c-buckey

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

- What do you think the user was doing? **It appears that the person was downloading a Linux Red Hat file.**

- Was the file they downloaded malicious? **Most Linux files are not considered malicious, but there is a chance that it could have been.** If not, what is the file used for? **More than likely, it was a large Linux system file.**

- Is there anything that seems suspicious about this activity? **Why was the file being downloaded to a Facebook page?**

- Is any of the traffic you inspected potentially outside of compliance guidelines? **I would have to question if there is a compliance issue with the file being downloaded to a Facebook page, and what was the person going to do with it.**