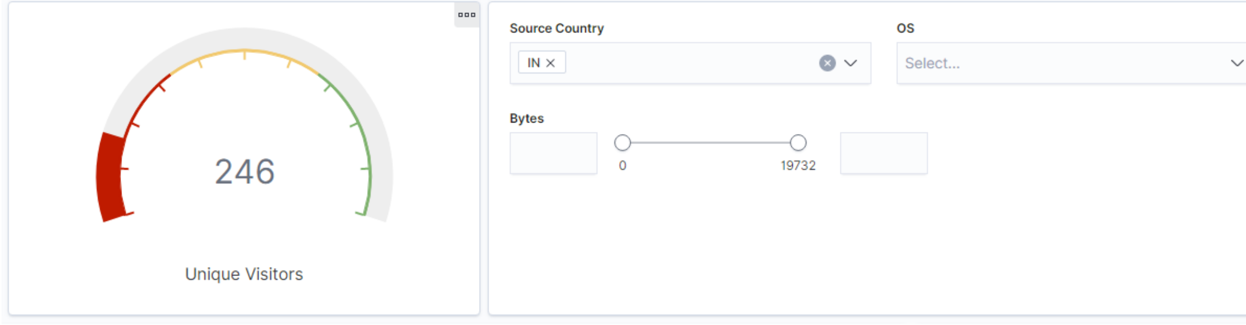
1. Add the sample web log data to Kibana.

2. Answer the following questions:

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



246

Unique Visitors

Source Country

IN ×

OS

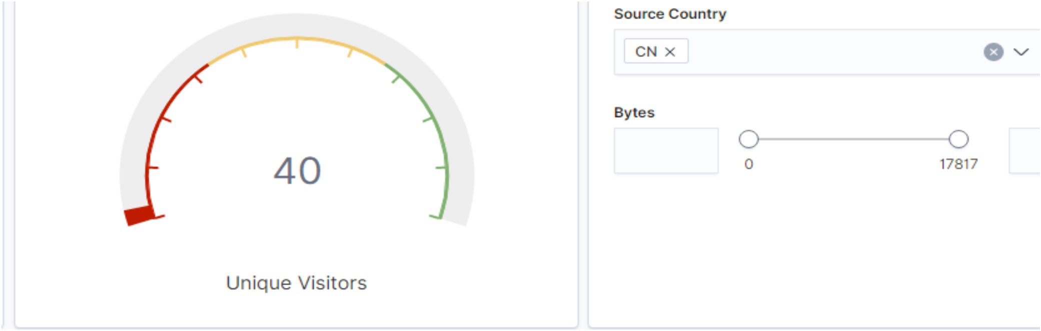
Select...

Bytes

0

19732

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



40

Unique Visitors

Source Country

CN ×

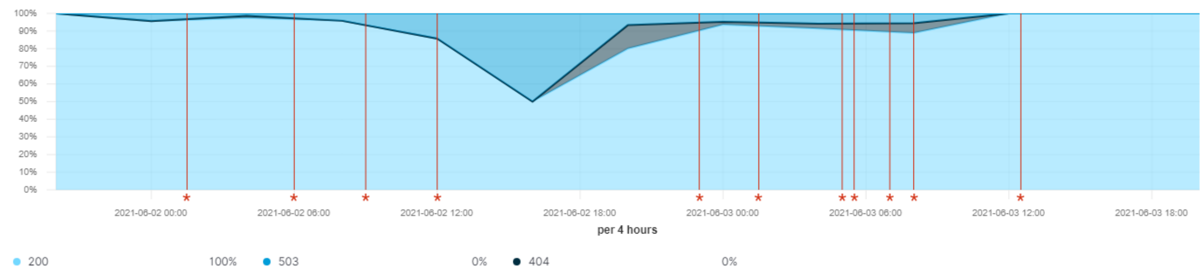
Bytes

0

17817

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

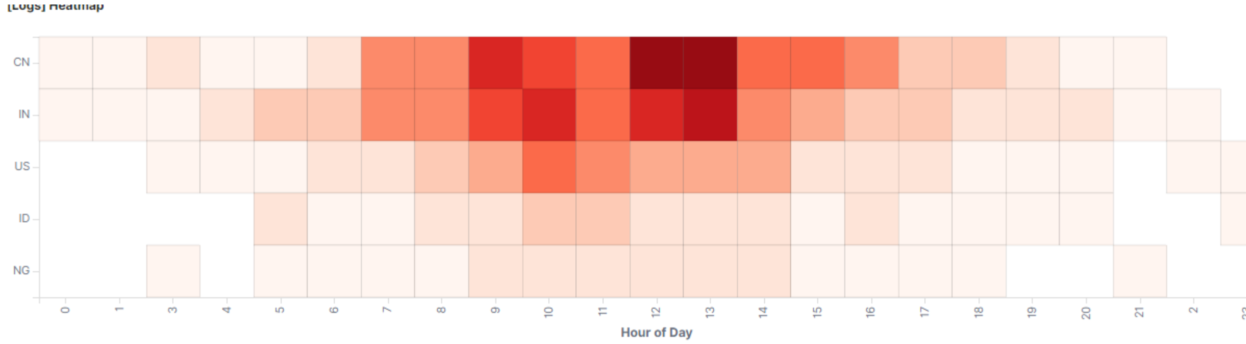
[Logs] Response Codes Over Time + Annotations



404:0% 503: 0%

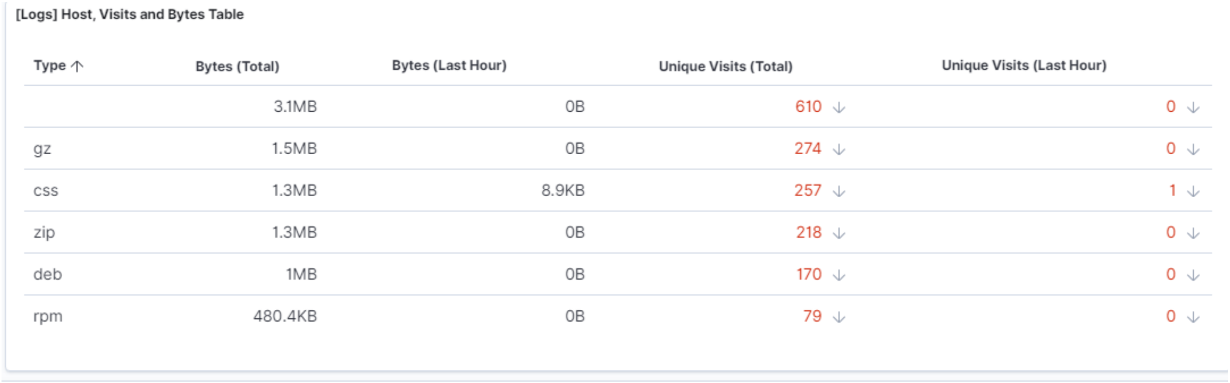
   - In the last 7 days, what country produced the majority of the traffic on the website? **China**

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



12pm and 1pm

- 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).



[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	3.1MB	0B	610 ↓	0 ↓
gz	1.5MB	0B	274 ↓	0 ↓
css	1.3MB	8.9KB	257 ↓	1 ↓
zip	1.3MB	0B	218 ↓	0 ↓
deb	1MB	0B	170 ↓	0 ↓
rpm	480.4KB	0B	79 ↓	0 ↓

gz: .gz files are compressed files created using the gzip compression utility.

- **css:** .css files can help define font, size, color, spacing, border and location of HTML information on a webpage. They are downloaded with their .html counterparts and rendered by the browser.

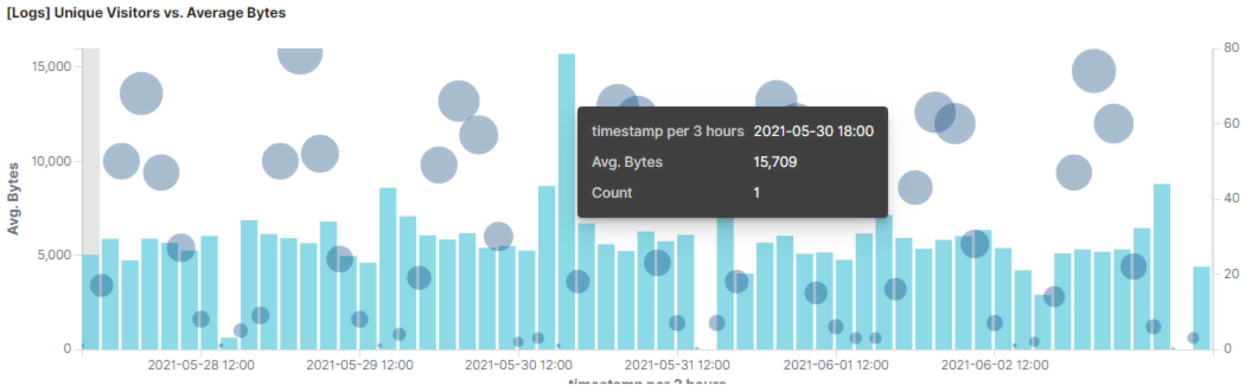
- **zip:** A lossless compression format. A .zip file may contain one or more files or directories that have been compressed.

- **deb:** A file with the .deb file extension is a Debian (Linux) Software Package file. These files are installed when using the apt package manager.

- **rpm:** .rpm file formats are a Red Hat Software Package file. RPM stands for Red Hat Package Manage

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.

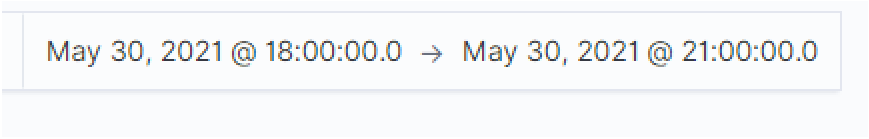
    - Locate the time frame in the last 7 days with the most amount of bytes (activity).



    - In your own words, is there anything that seems potentially strange about this activity? **One user is using the most bytes per 3 hours over the last 7 days.**

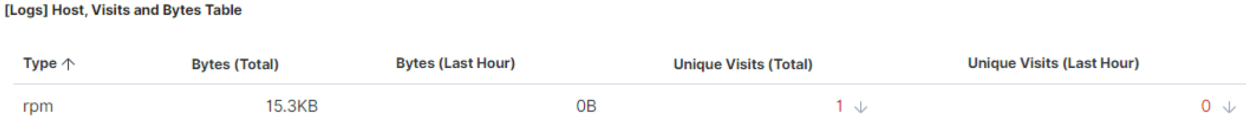
4. Filter the data by this event.

    - What is the timestamp for this event?



May 30, 2021 @ 18:00:00.0 → May 30, 2021 @ 21:00:00.0

    - What kind of file was downloaded?

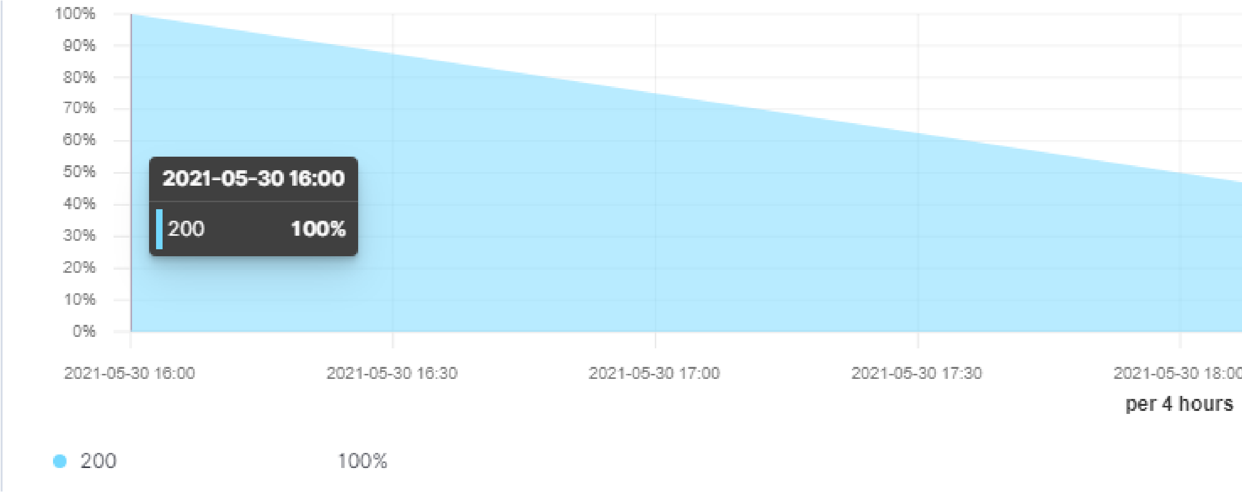


[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
rpm	15.3KB	0B	1 ↓	0 ↓

    - 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?**19:57:28.552**
   - What are the geo coordinates of this activity?**"lat": 43.34121, "lon": -73.6103075**
   - What OS was the source machine running?**Win 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**

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

   - What do you think the user was doing? **Attempting to download a linux package.**
   - Was the file they downloaded malicious? If not, what is the file used for? **Possibly. After doing a search it appears to be Chrome 44 on linux.**
   - Is there anything that seems suspicious about this activity? **If they are not authorized then the download for chrome on a linux machine does seem suspicious.**
   - Is any of the traffic you inspected potentially outside of compliance guidelines? **The link to facebook would more than likely be out of compliance.**