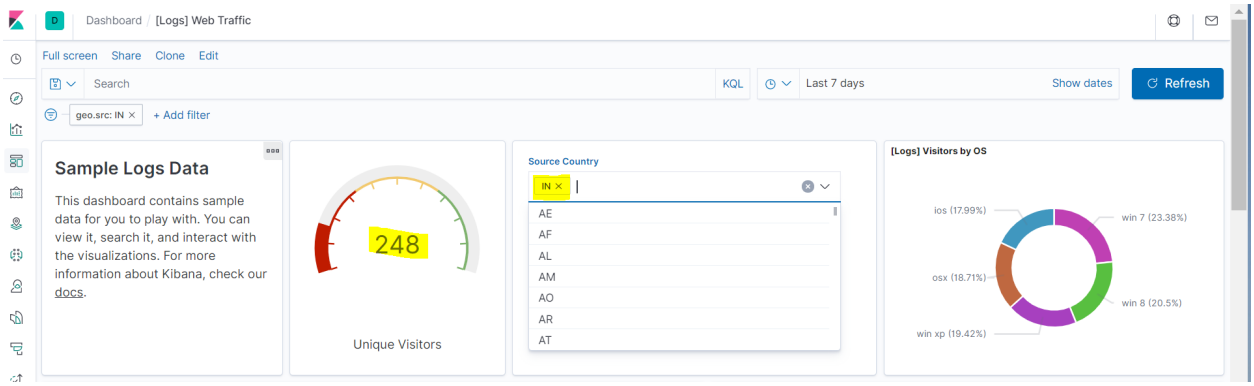
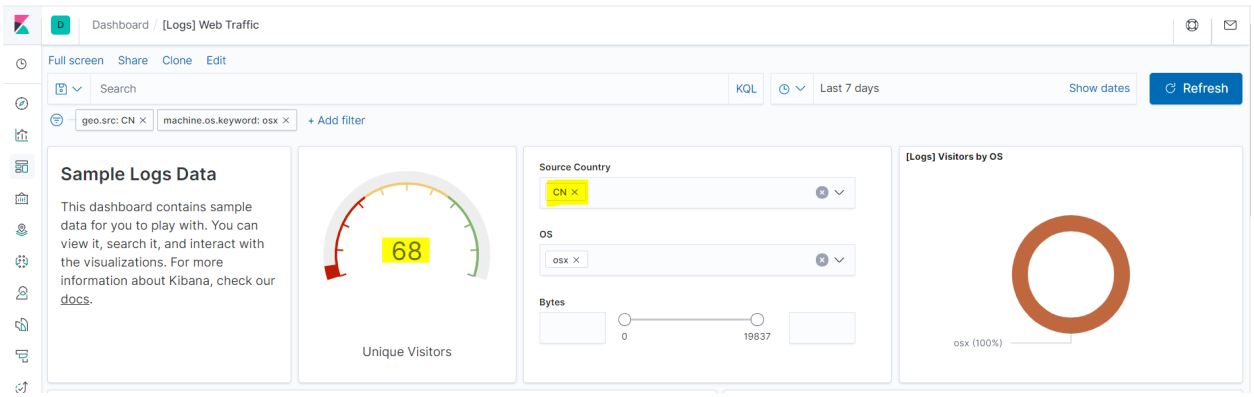
2. - In the last 7 days, how many unique visitors were located in India? = 248

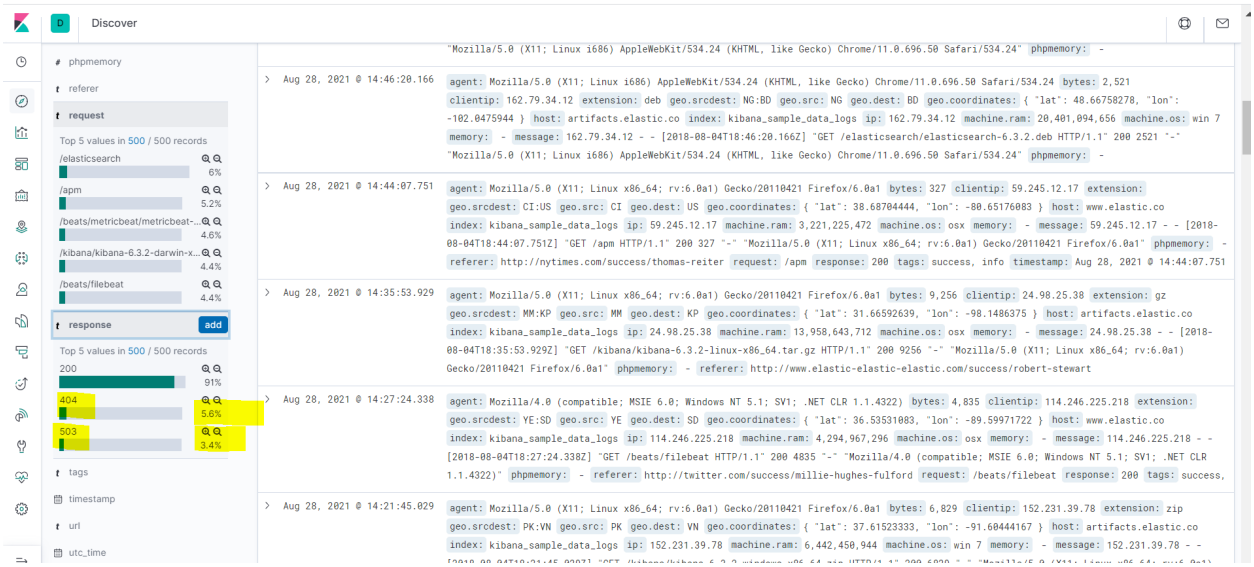


2. - In the last 24 hours, of the visitors from China, how many were using Mac OSX? = 68



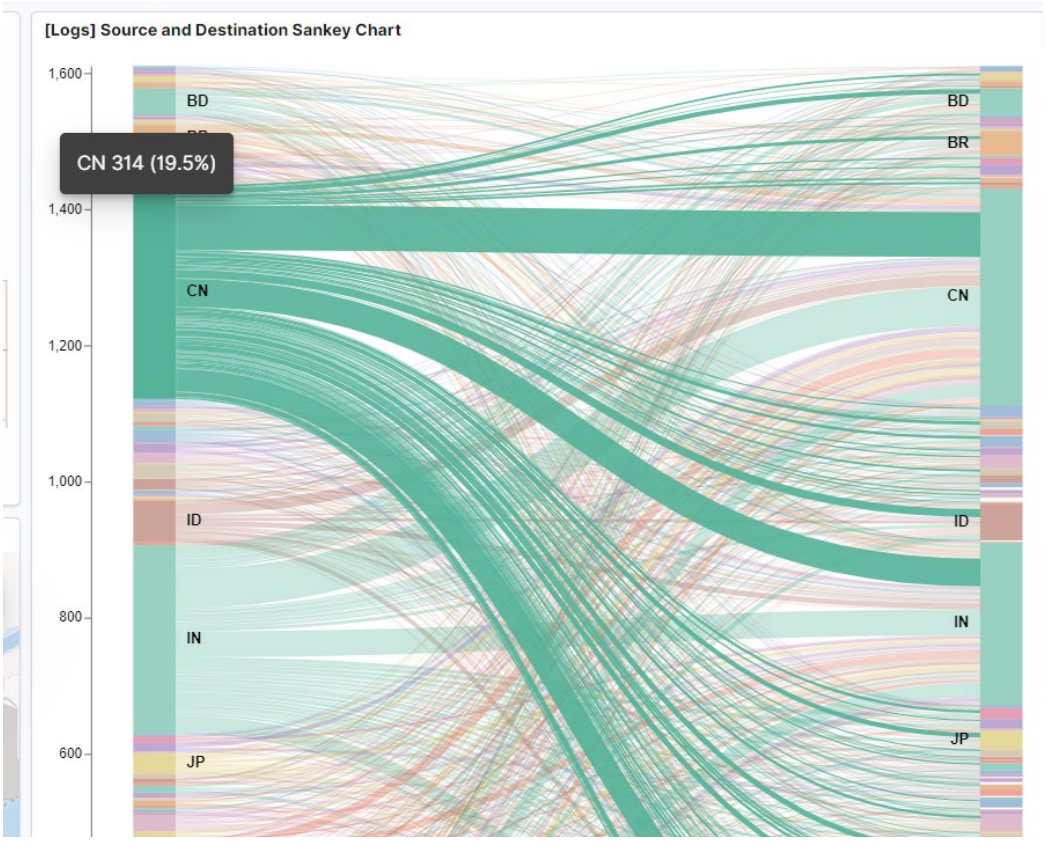
2. - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

404 errors = 5.6% 503 errors = 3.4%



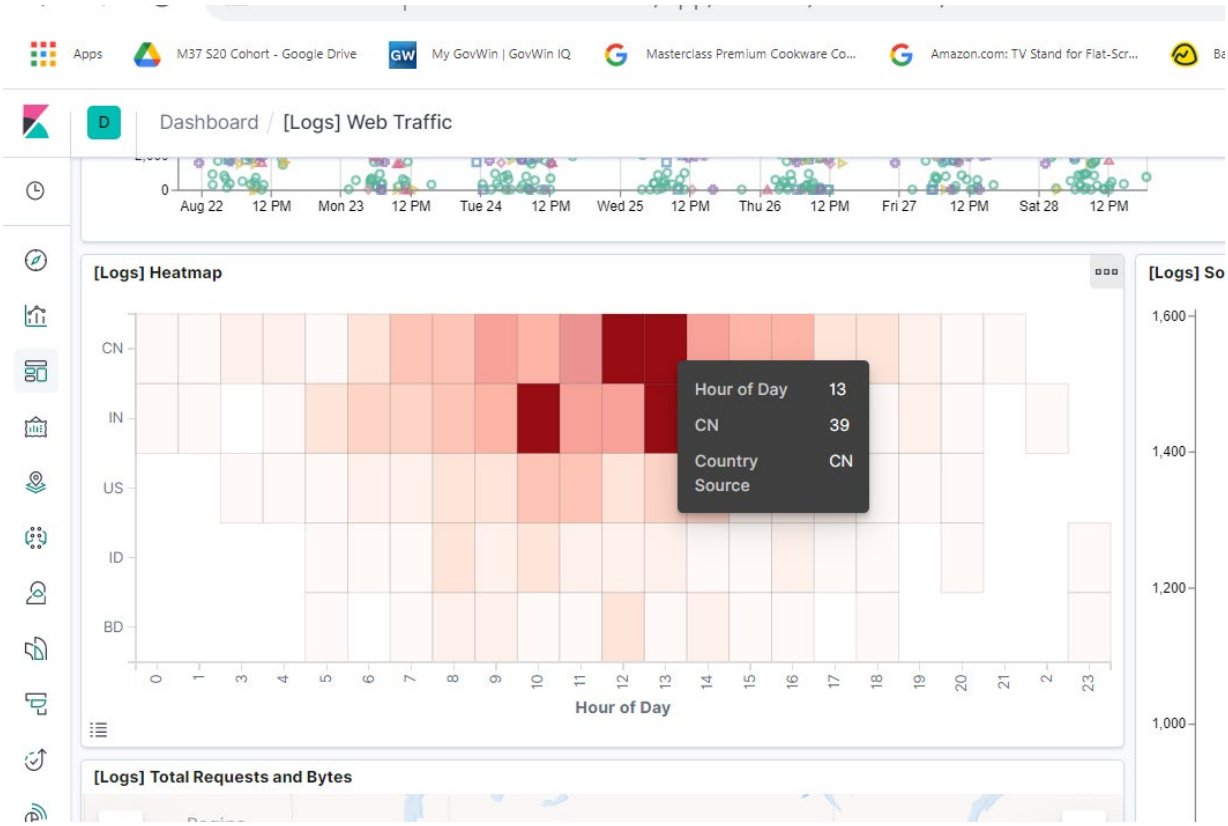
2. - In the last 7 days, what country produced the majority of the traffic on the website?

China with 19.5%



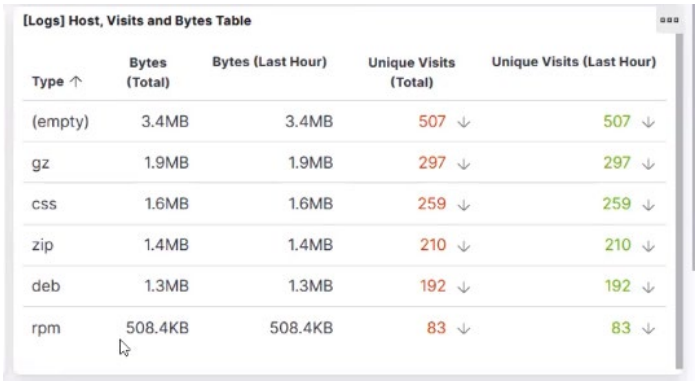
2. - Of the traffic that's coming from that country, what time of day had the highest amount of activity?

China had the most traffic at 1pm.



2. - 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 = compressed archive file
css = **C**ascading **S**tyle **S**heets are files that describe how HTML elements are displayed on the screen, paper, etc
zip = compressed files that take up less storage space and can be transferred to other computers more quickly
deb = A **DEB file** is a Debian Software Package file used mainly in Unix-based operating systems.
rpm = **R**edhat **P**ackage **M**anager is a free and open-source package management system. Most RPM files are "binary RPMs" (or BRPMs) containing the compiled version of some software.

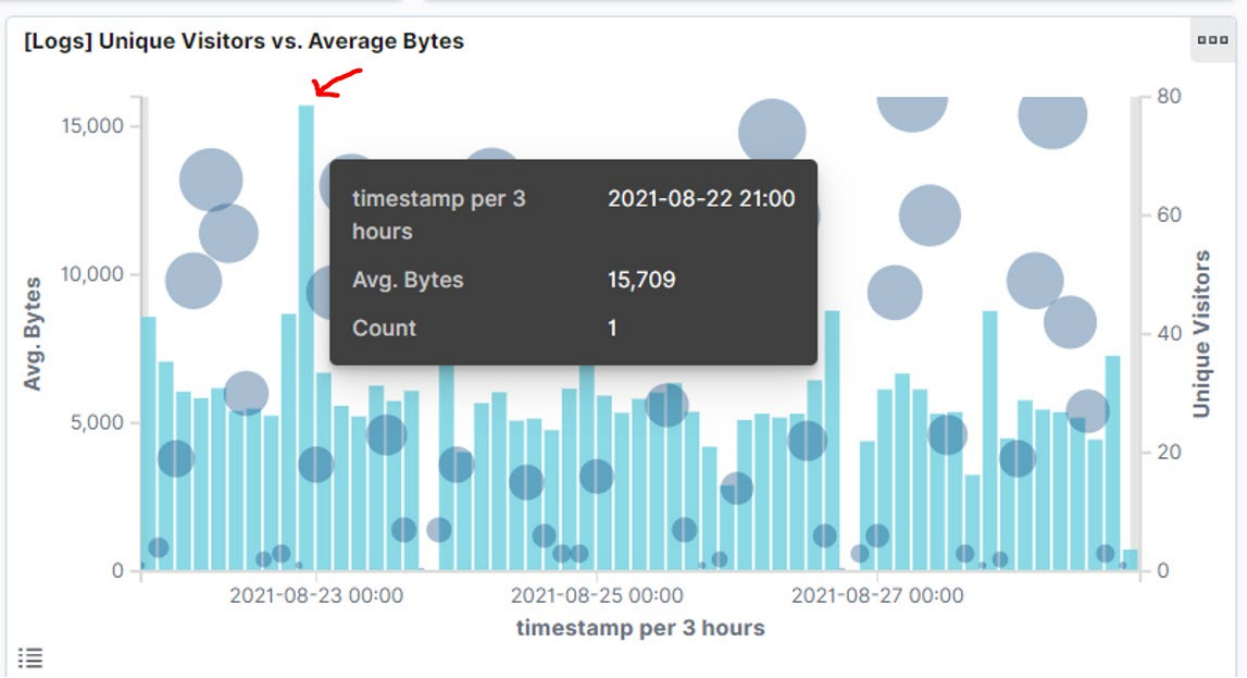


[Logs] Host, Visits and Bytes Table

Type	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
(empty)	3.4MB	3.4MB	507	507
gz	1.9MB	1.9MB	297	297
css	1.6MB	1.6MB	259	259
zip	1.4MB	1.4MB	210	210
deb	1.3MB	1.3MB	192	192
rpm	508.4KB	508.4KB	83	83

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

August 22, 2021 with 15,709 bytes

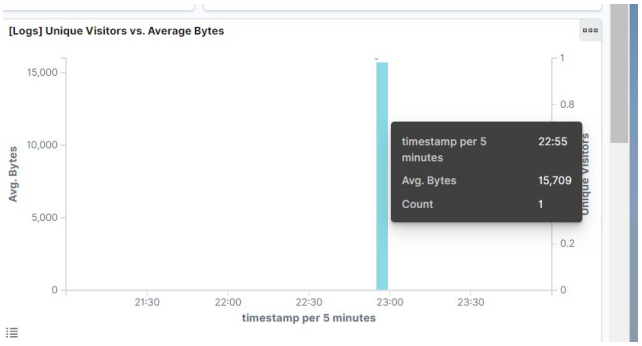


3. -In your own words, is there anything that seems potentially strange about this activity?

Large # of bytes coming from same user.

4. – Filter the data by this event.

- What is the timestamp for this event? - 10:55pm



- What kind of file was downloaded? – rpm (Redhat Package Manager)
- 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`

- 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? `beats/metricbeat/metricbeat-6.3.2-i686.rpm HTTP/1.1`
- 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? User was downloading a linux package.
    - Was the file they downloaded malicious? No. Not malicious because coming from elastic website. If not, what is the file used for?
    - Is there anything that seems suspicious about this activity? Weird traffic but not malicious
    - Is any of the traffic you inspected potentially outside of compliance guidelines? No.