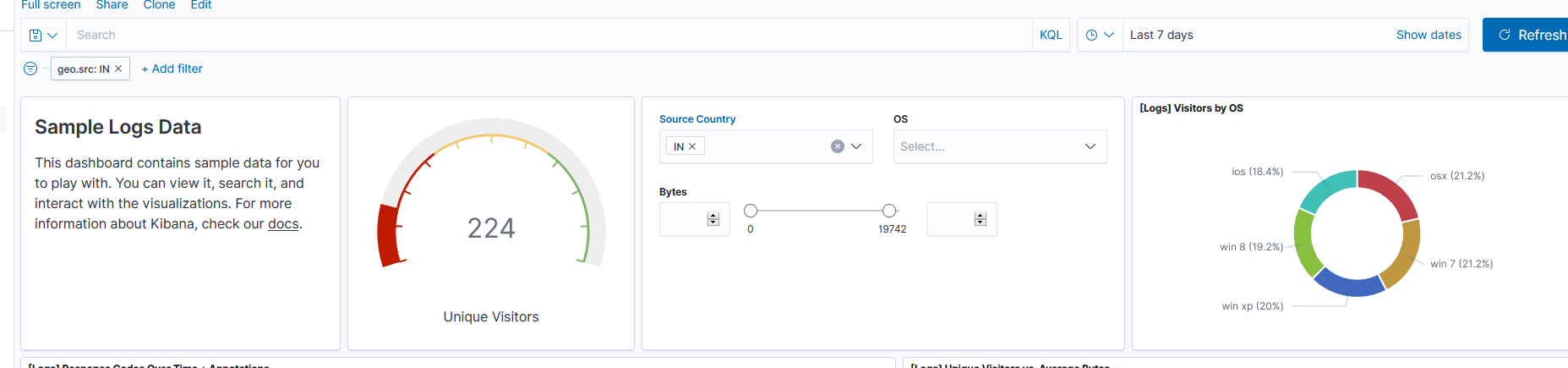
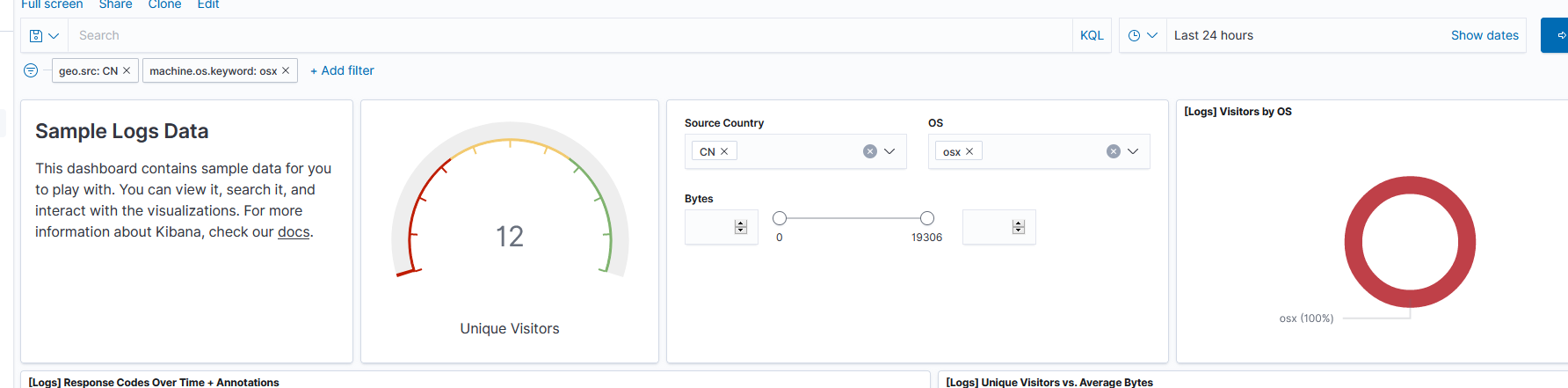
Unit 13-ELK Stack Project: Exploring Kibana Jared Banks 03/27/2021

2. Answer the following questions:

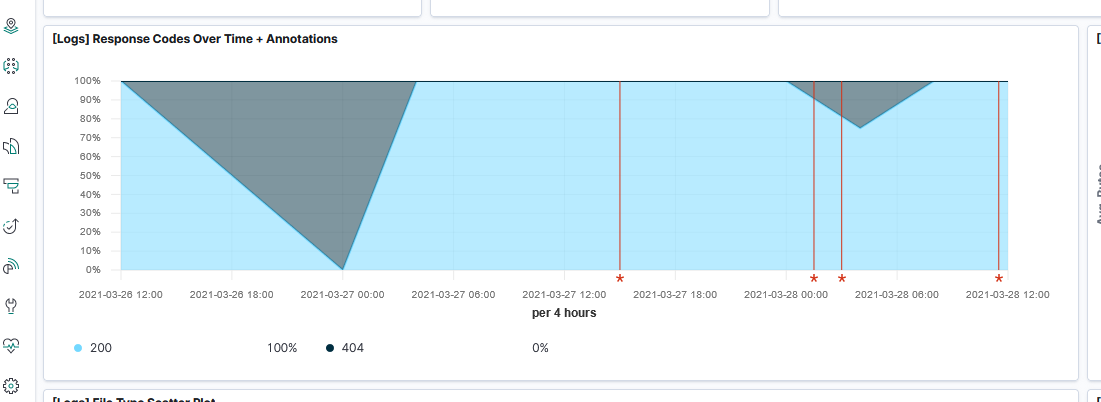
In the last 7 days, how many unique visitors were located in India? 224



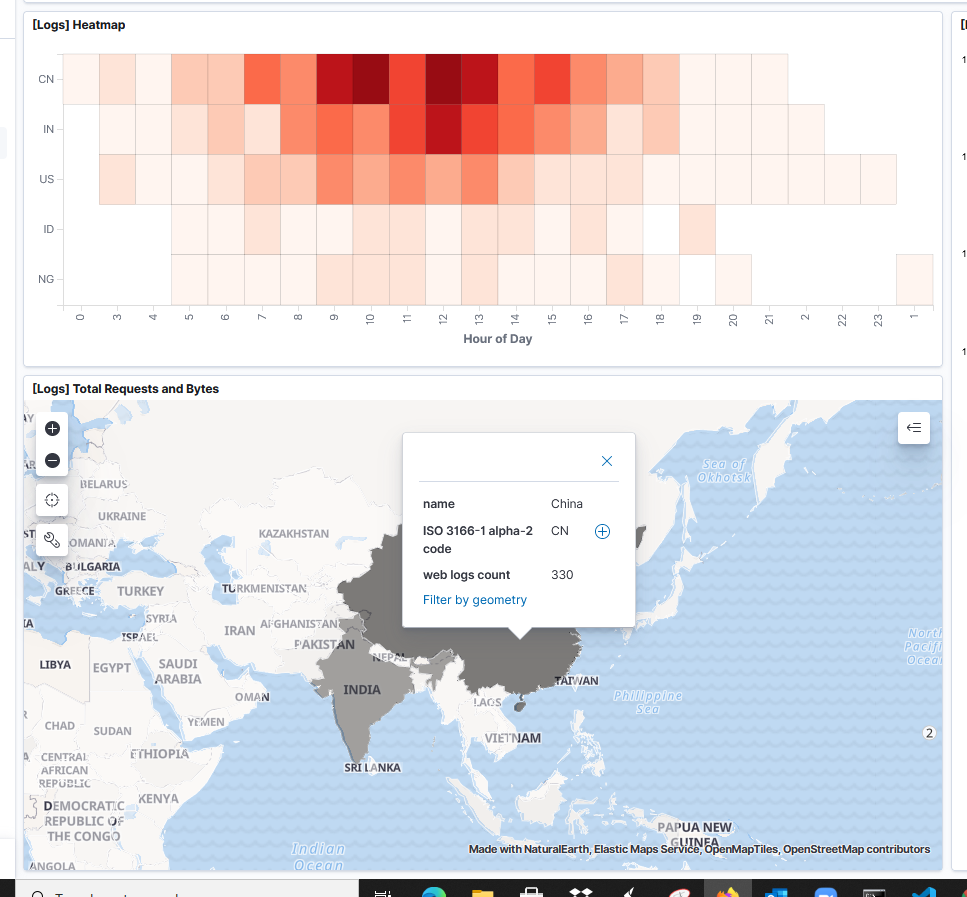
In the last 24 hours, of the visitors from China, how many were using Mac OSX? 12



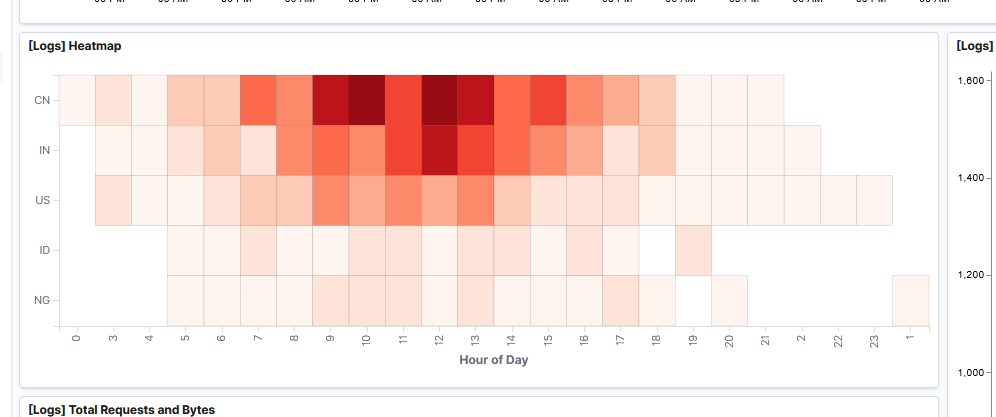
In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 200=91.379%, 303=3.448%, 404=5.172% (I couldn’t get the % numbers to stay on screen while I took the screenshot).



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? 10 a.m. & 12 p.m.



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).

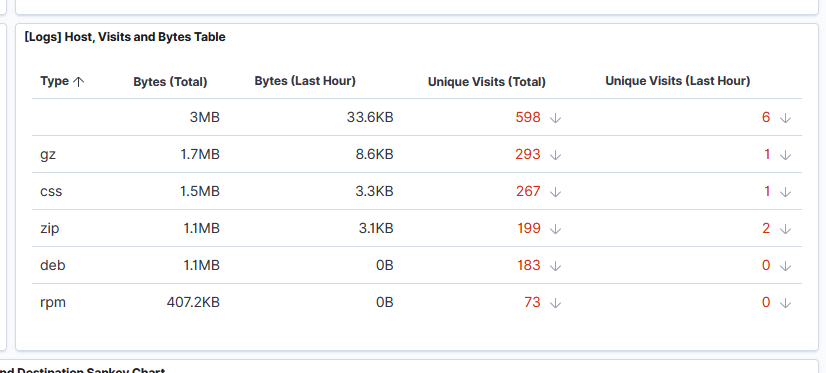
.gz - Compressed files created by using the gzip compression utility.

.css - files that help define font, size, color, spacing and location of HTML information on a webpage. Also, they are downloaded with their HTML counterparts and rendered by the browser.

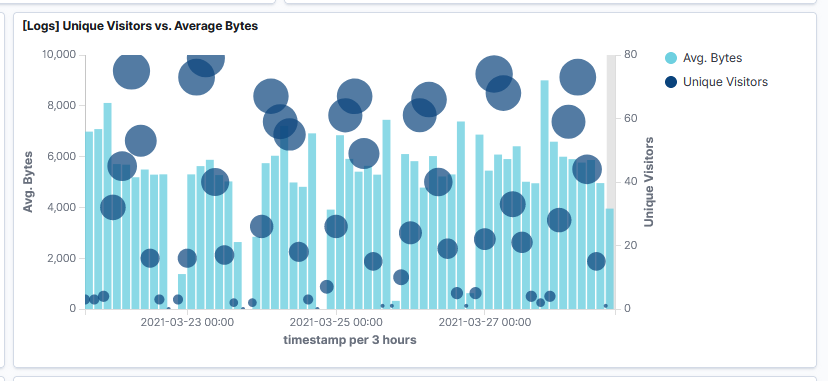
.zip - files that are compressed to save space on a drive. Can be used to email large files that normally would be to big to be sent.

.deb - These are Debian (Linux) Software Package files that are installed when using the “apt” command.

.rpm - These are Red Hat Software Package files.



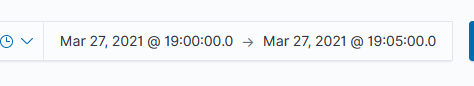
3. Locate the time frame in the last 7 days with the most amount of bytes (activity).



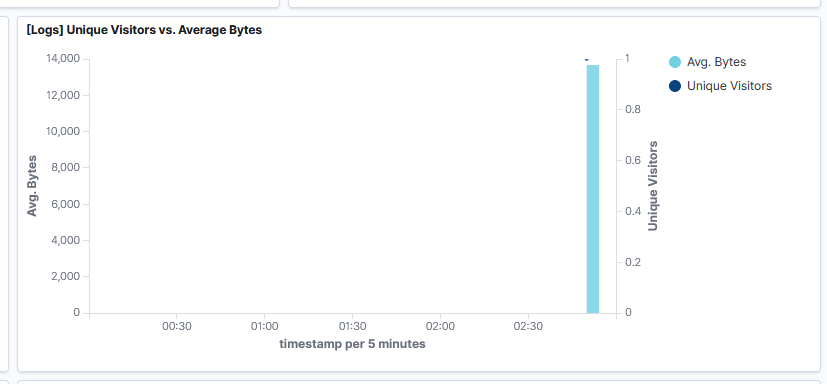
Most amount of bytes the last 7 days was 13,671. Its a higher amount than most and much higher than the average. (I couldn’t get the flag with the actual number to stay on screen while using the snipping tool).

4. Filter the data by this event.

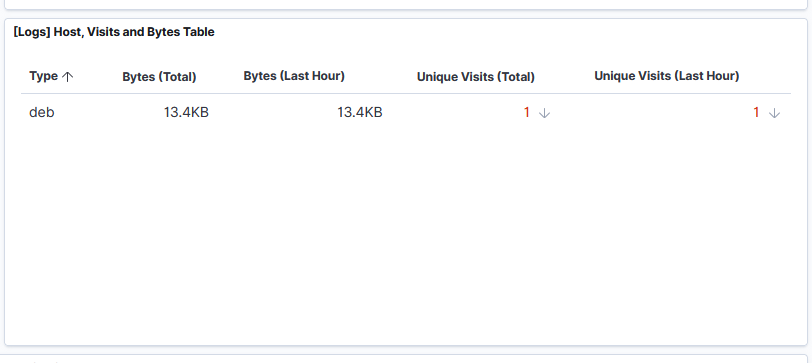
What is the timestamp for this event?



Actual time stamp is 19:00:00



What kind of file was downloaded? A .deb file.



From what country did this activity originate? Brazil, South America.



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

