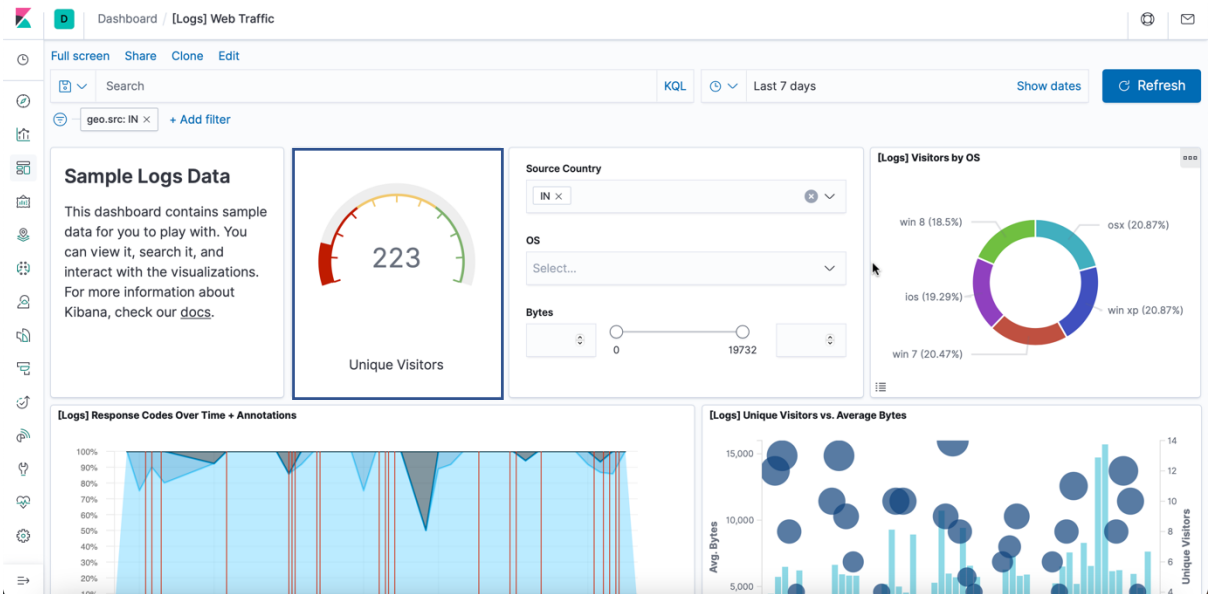
Exploring Kibana

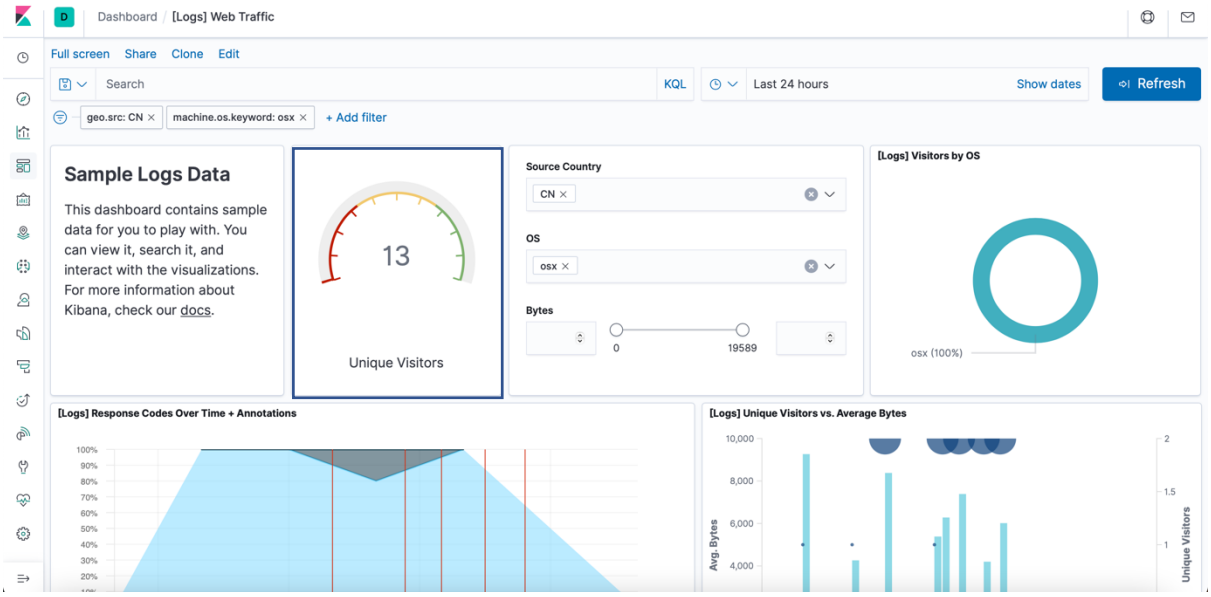
- In the last 7 days, how many unique visitors were located in India?

  Answer : 223



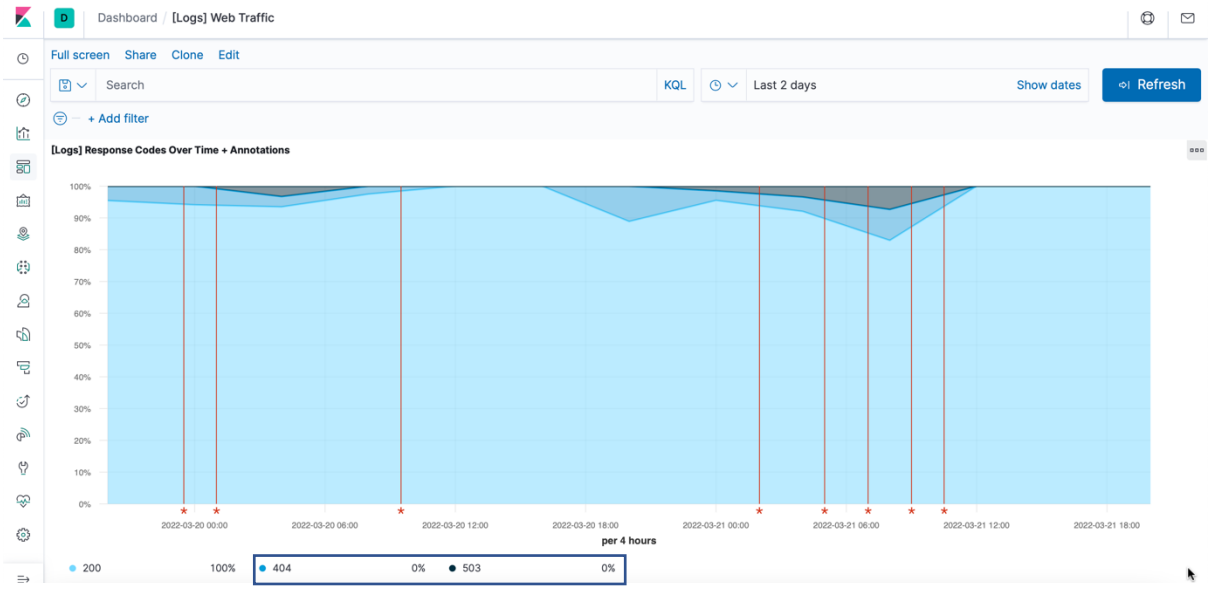
- In the last 24 hours of the visitors from China, how many were using Mac OSX?

  Answer : 13



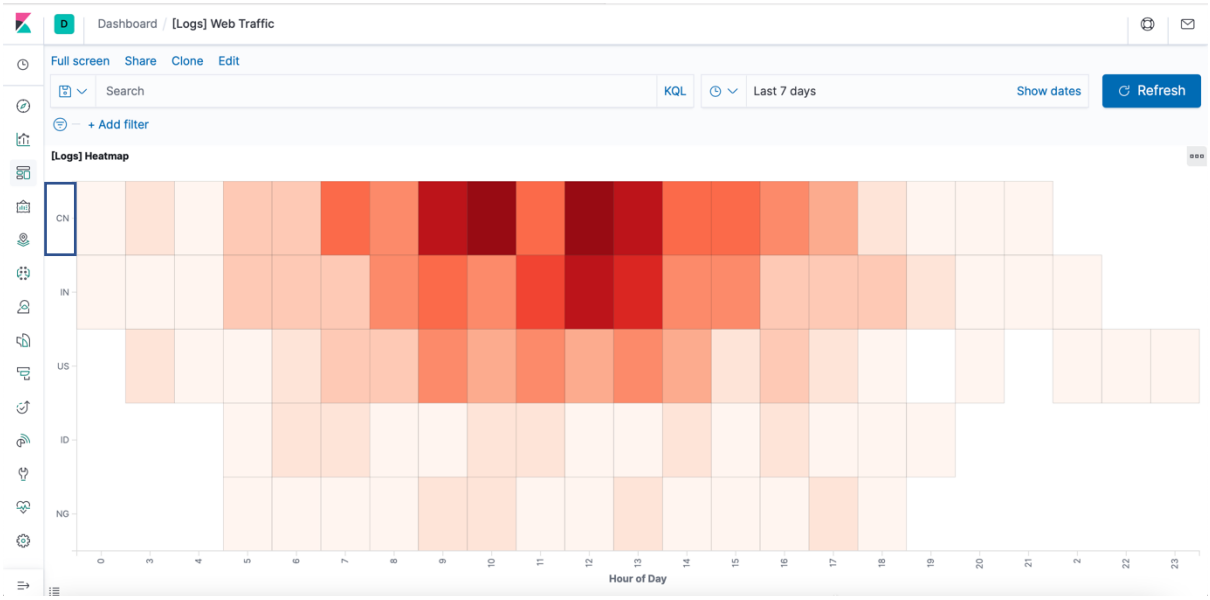
- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

  Answer : 404 – 0% ; 503 – 0%



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

  Answer : China



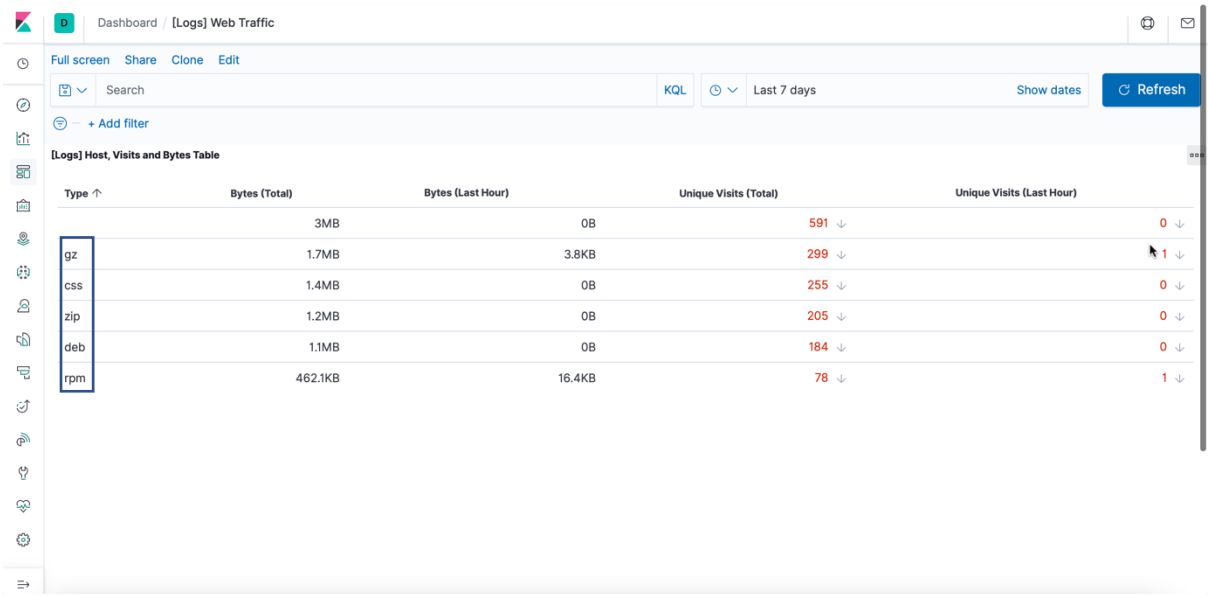
- Of the traffic that's coming from that country, what time of day had the highest amount of activity?

  Answer : 10 am and 12 pm

- 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.

    - **gz:** .gz files are archived files compressed by the standard GNU zip (gzip) compression algorithm. It stands for Gnu Zipped Archive.
    - **css:** .css files are used to format the contents of a webpage like indentation, font, size, color, line spacing, border and location of HTML information on a webpage. It stands for Cascading Style Sheet.
    - **zip:** .zip files are archive file that contains one or more compressed files or directories. It supports lossless data compression. It stands for zipped file.
    - **deb:** A .deb file is a Debian Software Package file used by Debian Linux Distribution and its variants. Each DEB file is a standard Unix archive that contains two .tar archives: one for installer control information and another for installable data.

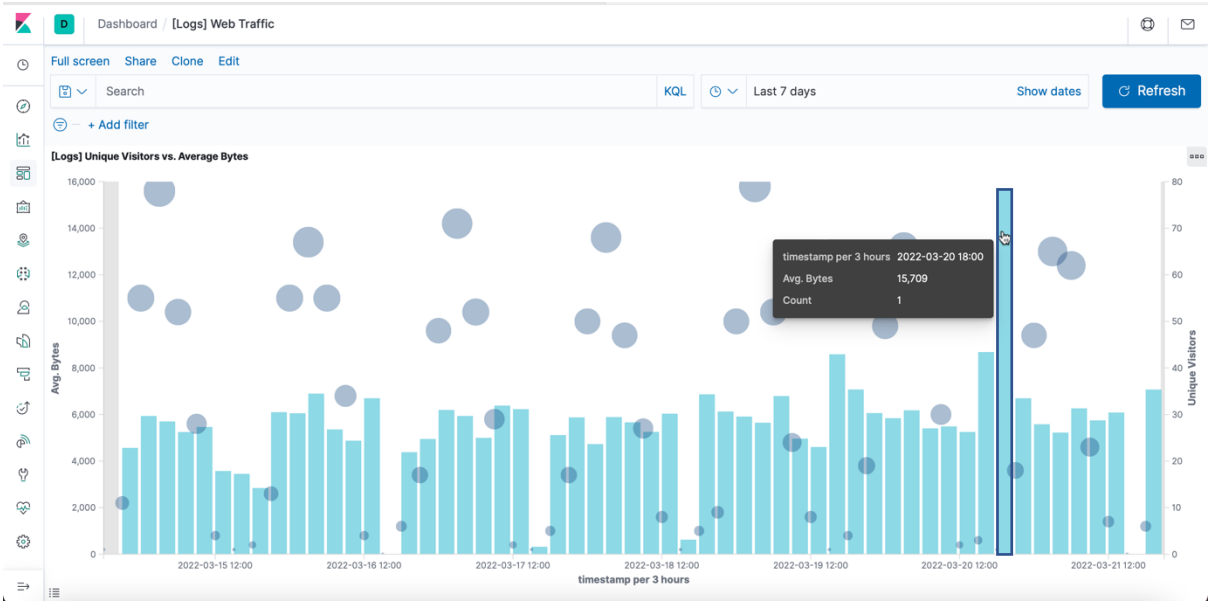
- **rpm:** .rpm file is an installation package originally developed for the Red Hat Linux operating system. It stands for Red Hat Package Manager File.



From Unique Visitors Vs. Average Bytes chart,

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

  Answer: 6 pm on 20th March 2022



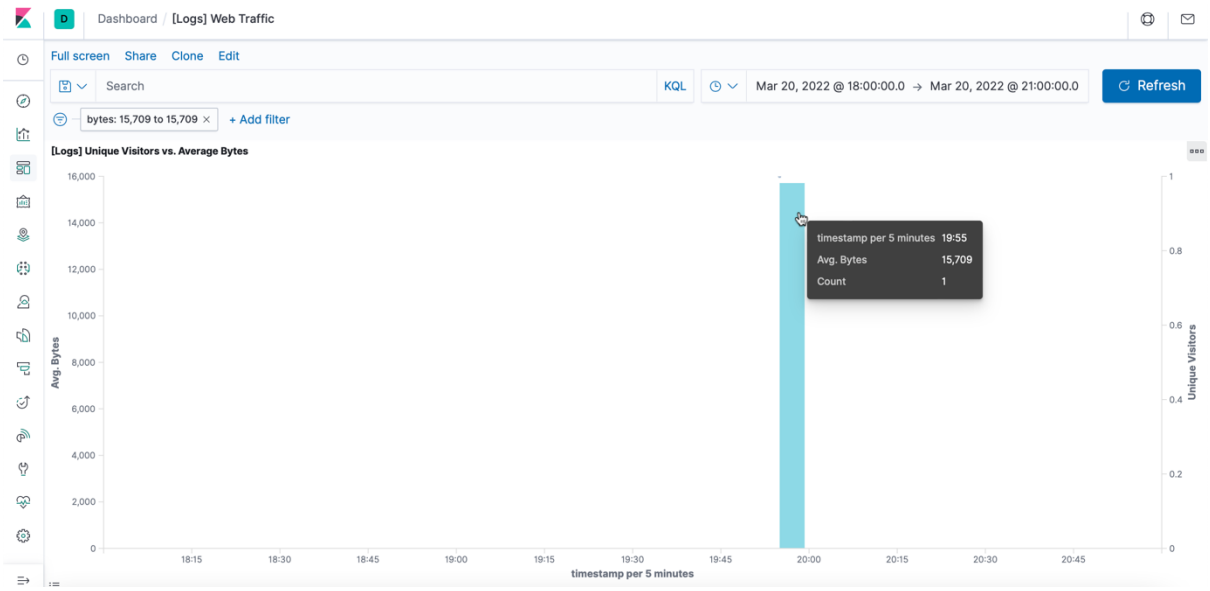
- In your own words, is there anything that seems potentially strange about this activity?

  Answer: It is strange that a single visitor is using a much higher number of bytes (15709) than other visitors.

On filtering the data by this event,

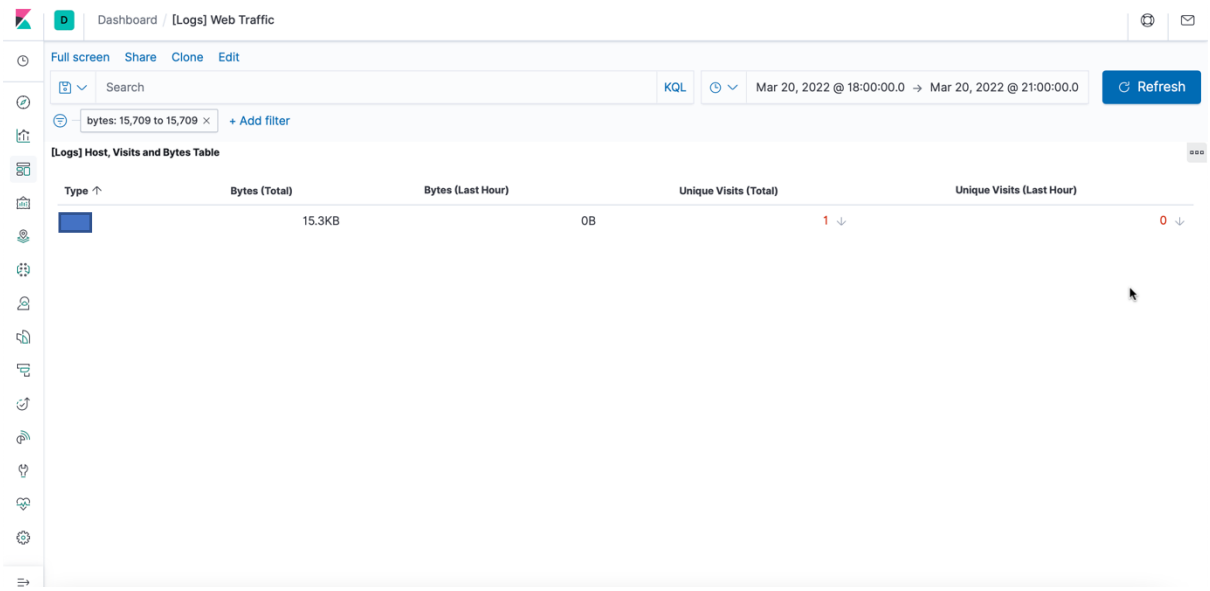
- What is the timestamp for this event?

  Answer: The time stamp is 19:55 for the filter Mar 20, 2022 @ 18:00:0 Mar 20, 2022 @ 21:00:0.



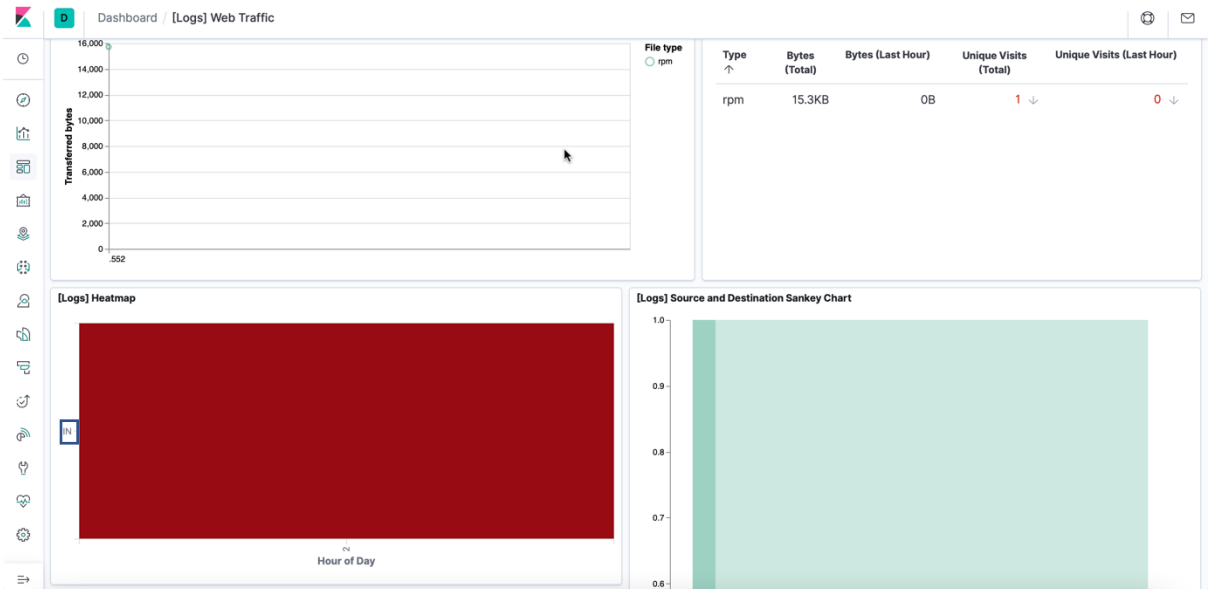
- What kind of file was downloaded?

  Answer: An rpm file



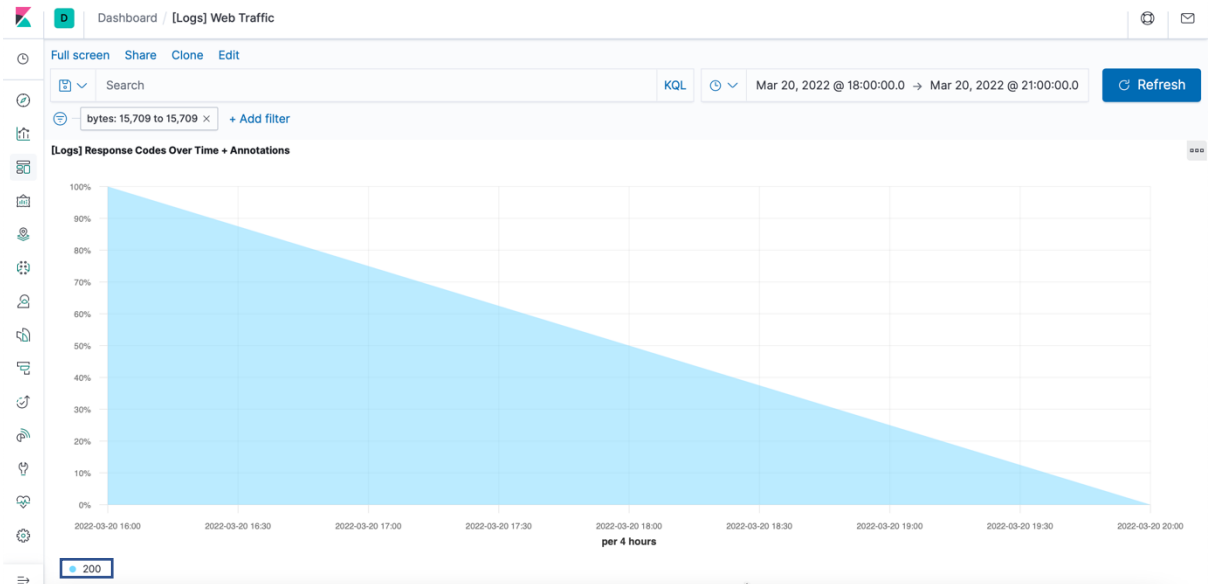
- From what country did this activity originate?

  Answer: India



- What HTTP response codes were encountered by this visitor?

  Answer: 200



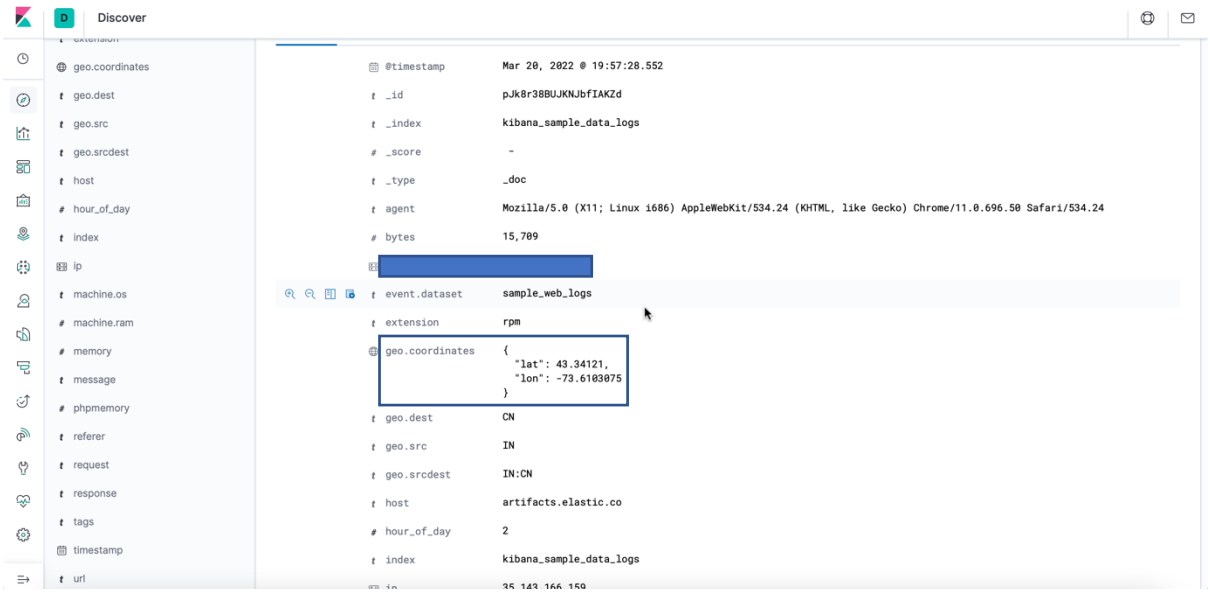
Switch over to the Kibana Discover page,

- What is the source IP address of this activity?

  Answer: 35.143.166.159

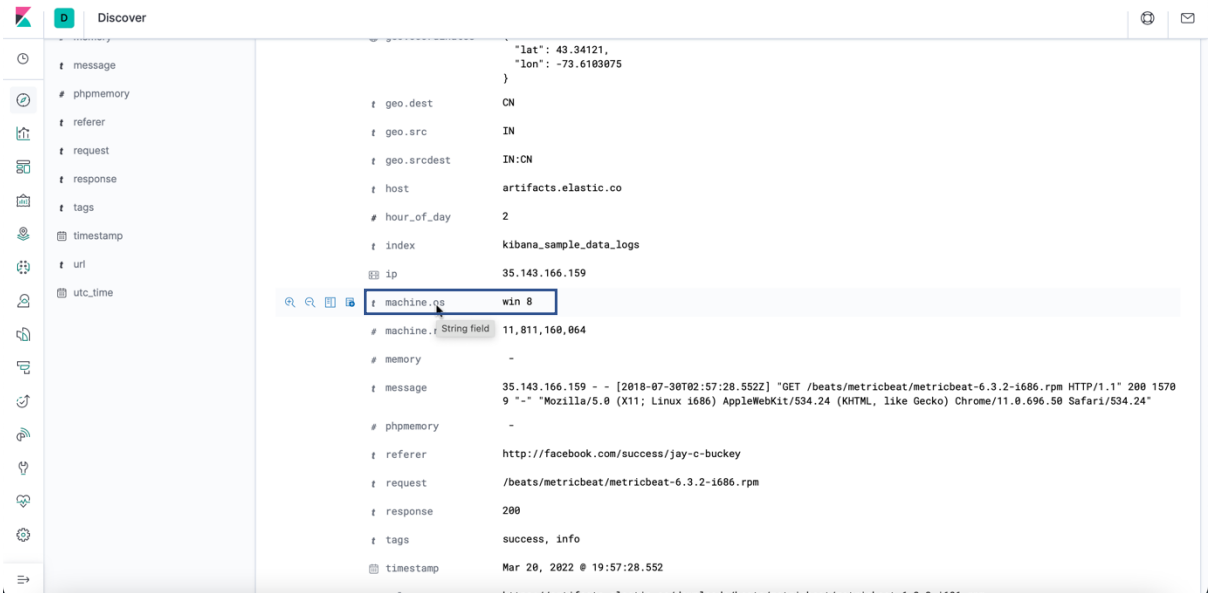
- What are the geo coordinates of this activity?

  Answer: { "lat": 43.34121, "lon": -73.6103075 }



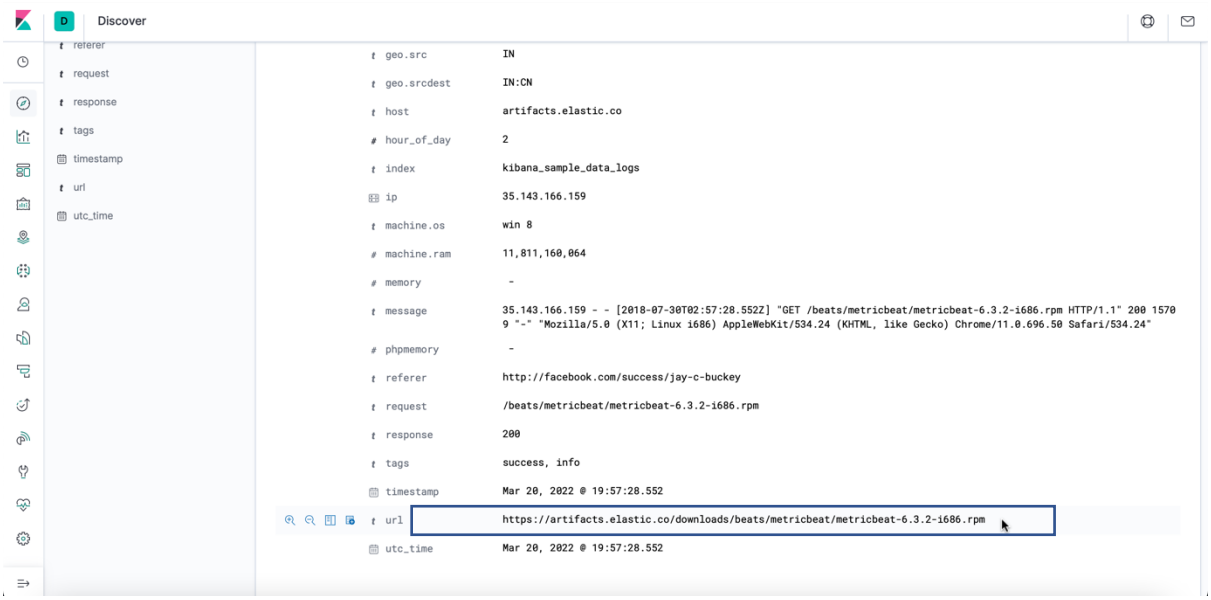
- What OS was the source machine running?

  Answer: Windows 8



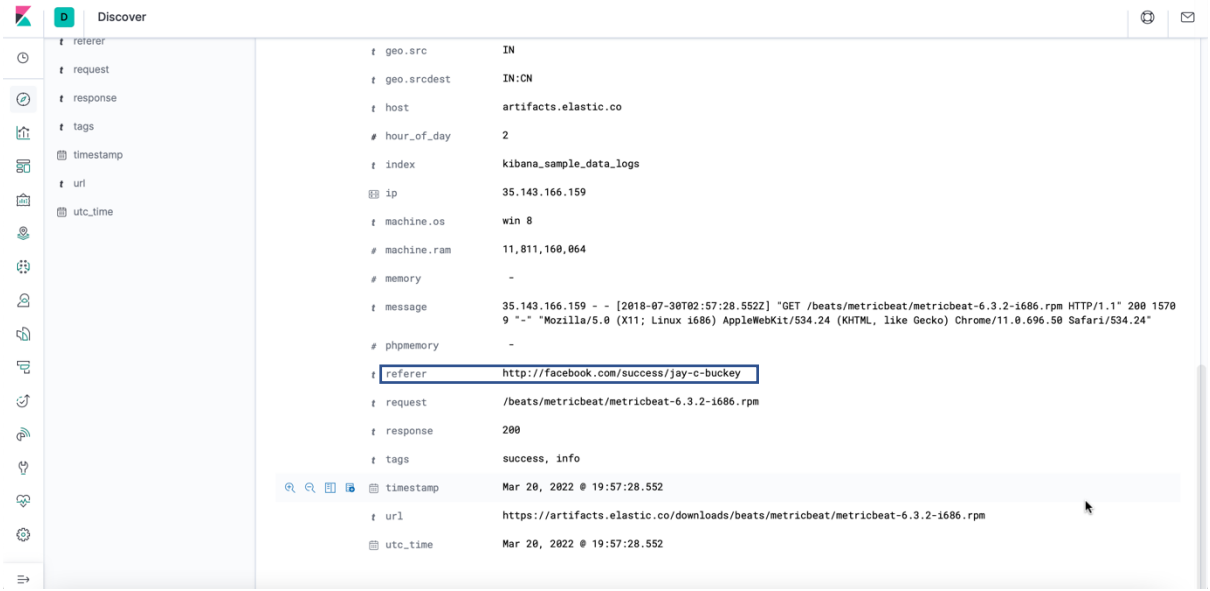
- What is the full URL that was accessed?

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



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

  Answer: Facebook



- What do you think the user was doing?

  Answer: I think the user was trying to download an installation package (Metricbeat) for Linux from the website.

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

  Answer: The installation does not seem malicious but could be. The file is usually used to download or update Metricbeat.

- Is there anything that seems suspicious about this activity?

Answer: Yes, the referrer for the download website was Facebook.

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

  Answer: Since the download link was posted on Facebook, it might be outside of compliance guidelines. Ideally speaking, it is not expected to have a download/update link posted to social media.