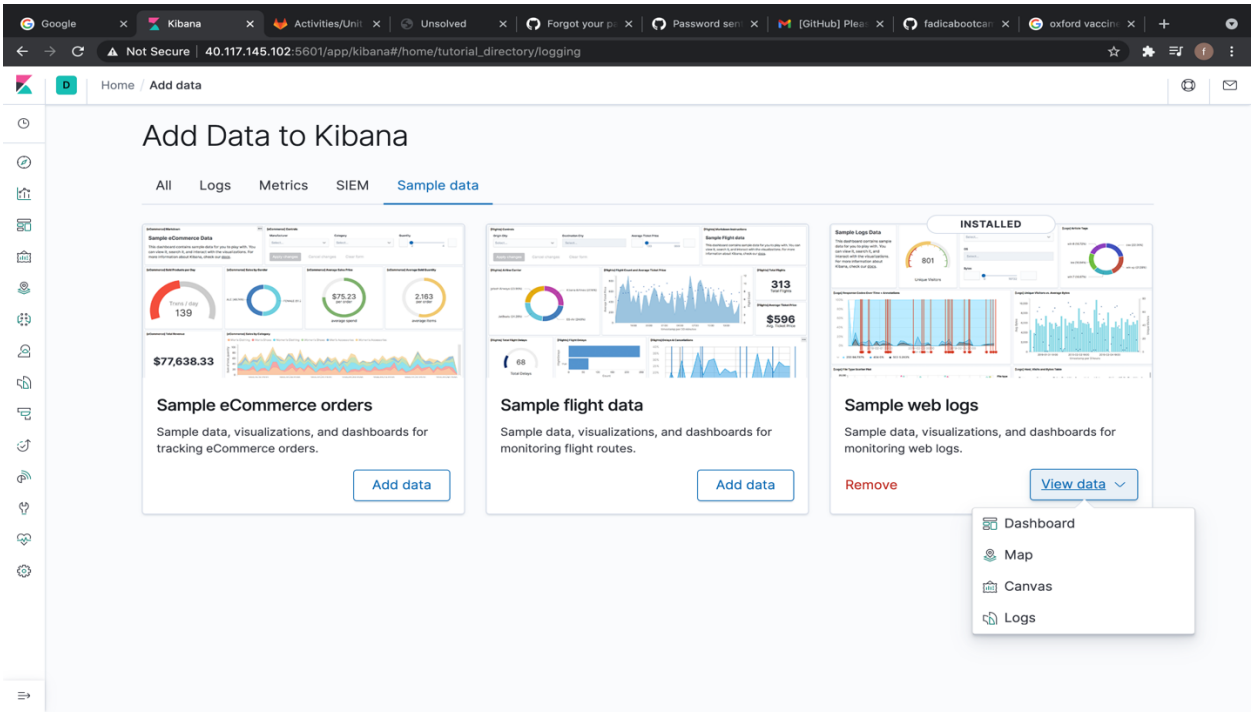
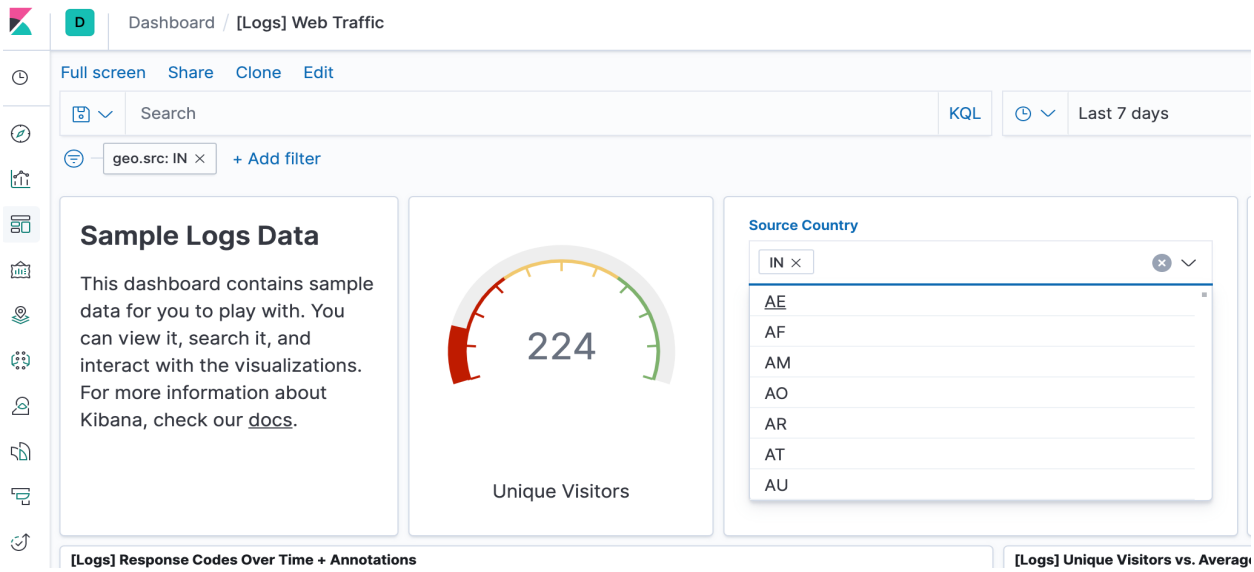
# Exploring Kibana

Add the sample web log data to Kibana.



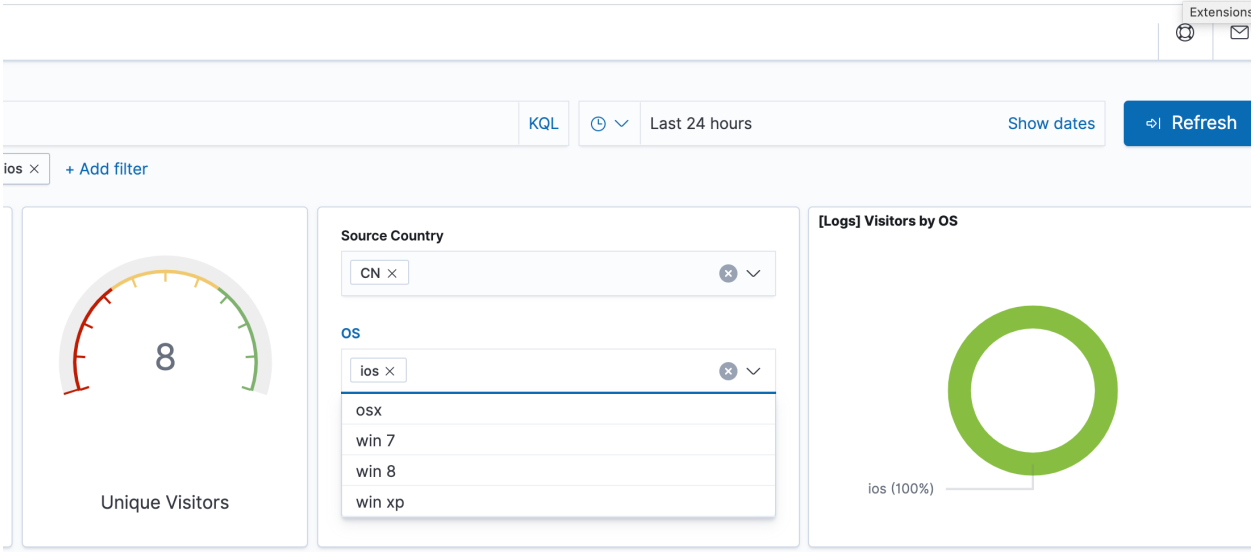

In the last 7 days, how many unique visitors were located in India?

224 unique visitors

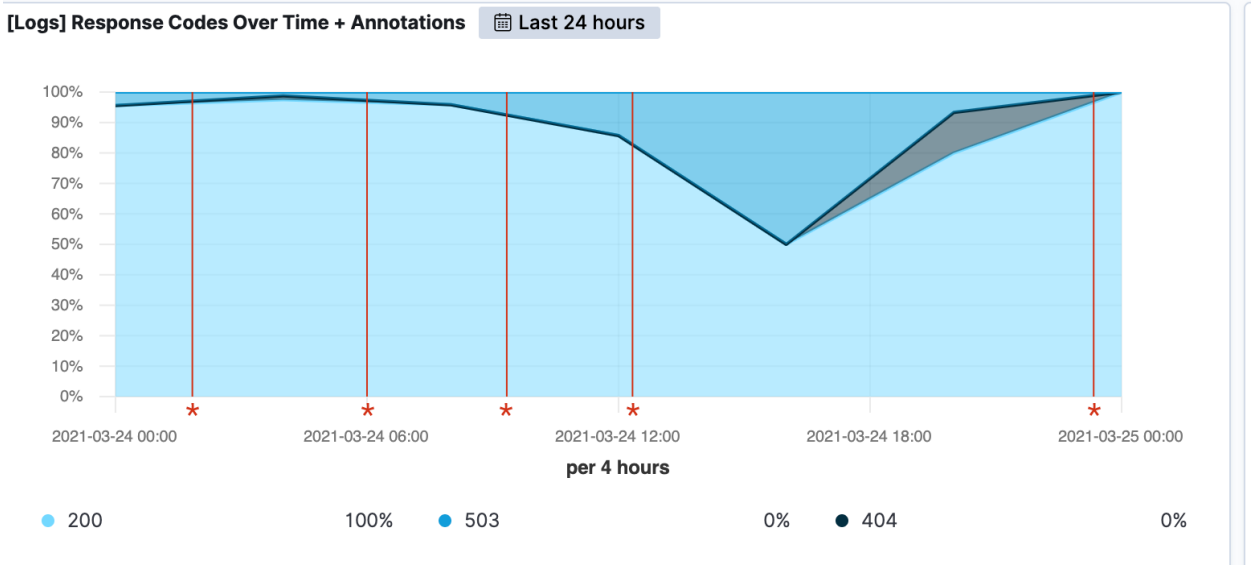


In the last 24 hours, of the visitors from China, how many were using Mac OSX?

8 users using OSX

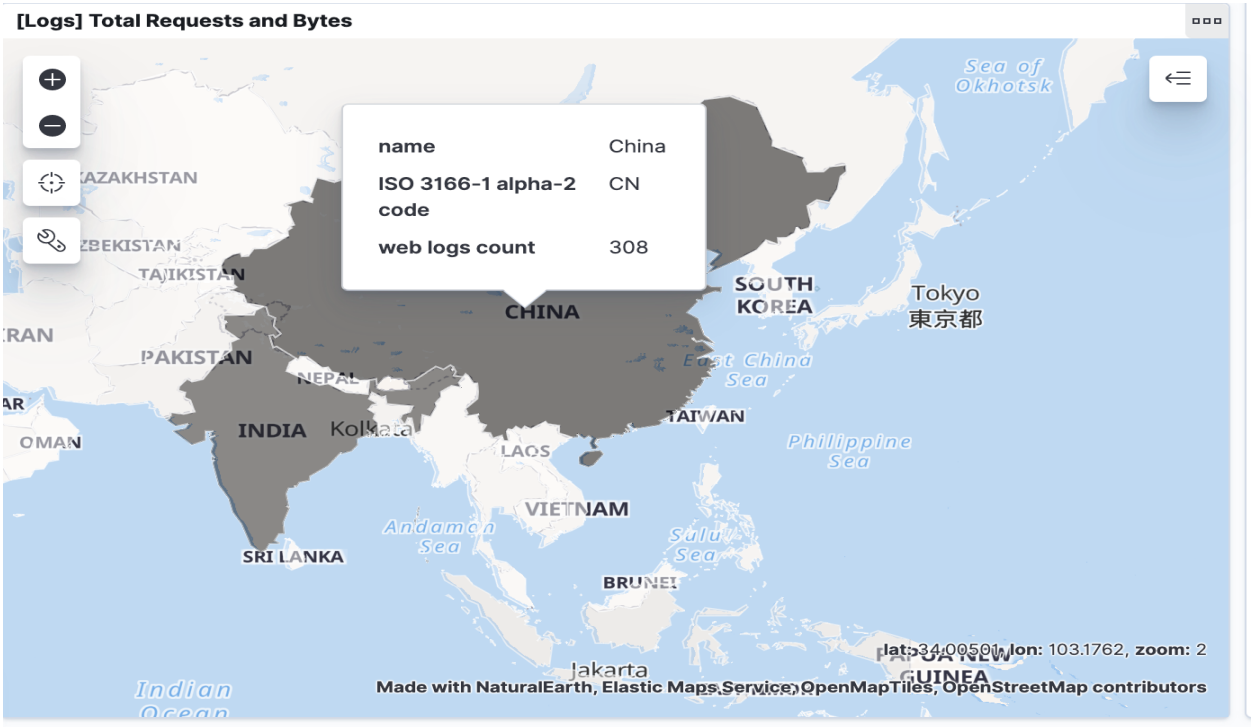



In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

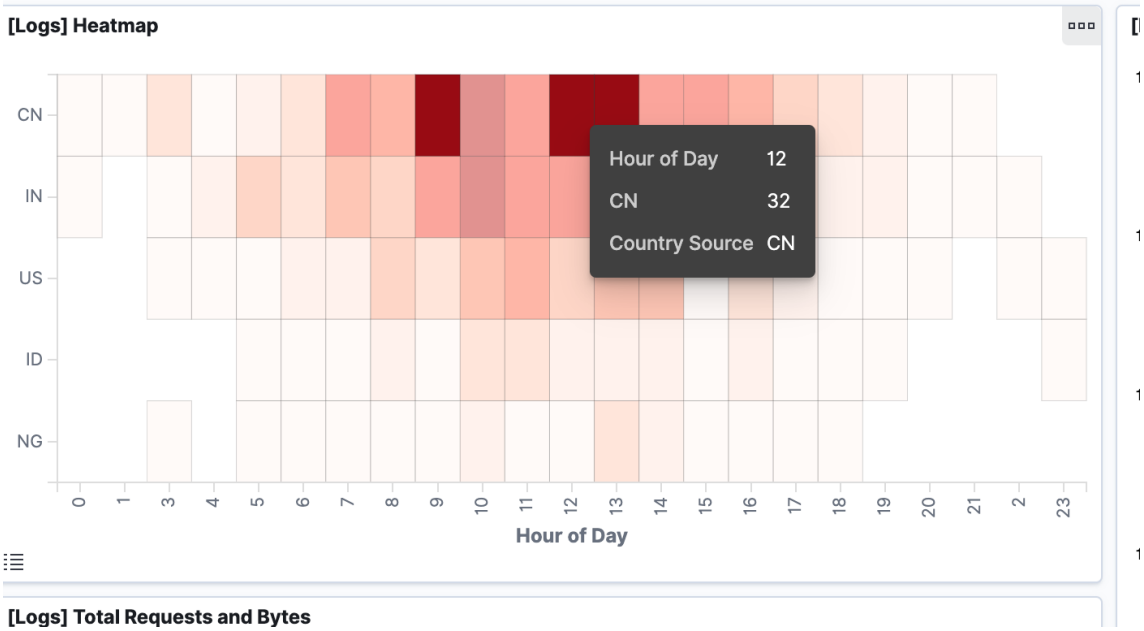


In the last 7 days, what country produced the majority of the traffic on the website?

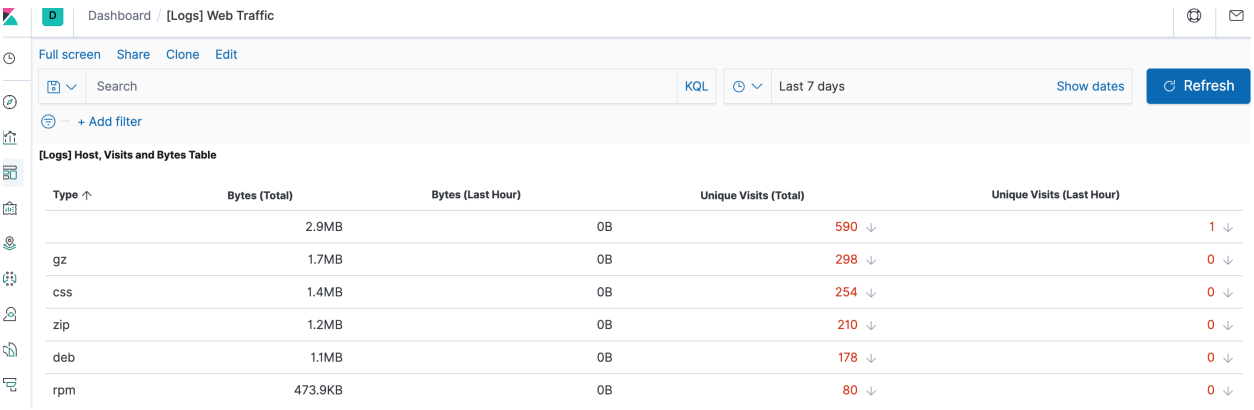
**China**




Of the traffic that's coming from that country, what time of day had the highest amount of activity? – **12PM- 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).




| Type | Bytes (Total) | Bytes (Last Hour) | Unique Visits (Total) | Unique Visits (Last Hour) |
|---|---|---|---|---|
| | 2.9MB | 0B | 590 | 1 |
| gz | 1.7MB | 0B | 298 | 0 |
| css | 1.4MB | 0B | 254 | 0 |
| zip | 1.2MB | 0B | 210 | 0 |
| deb | 1.1MB | 0B | 178 | 0 |
| rpm | 473.9KB | 0B | 80 | 0 |

**gz**: A GZ file is an archive file compressed by the standard GNU zip (gzip) compression algorithm

**css**: Stands for "Cascading Style Sheet." Cascading style sheets are used to format the layout of Web pages.

**Zip:** A Zip file is a single file containing one or more compressed files, offering an ideal way to make large files smaller and keep related files together

**deb**: deb is the format, as well as extension of the software package format for the Linux distribution Debian and its derivatives

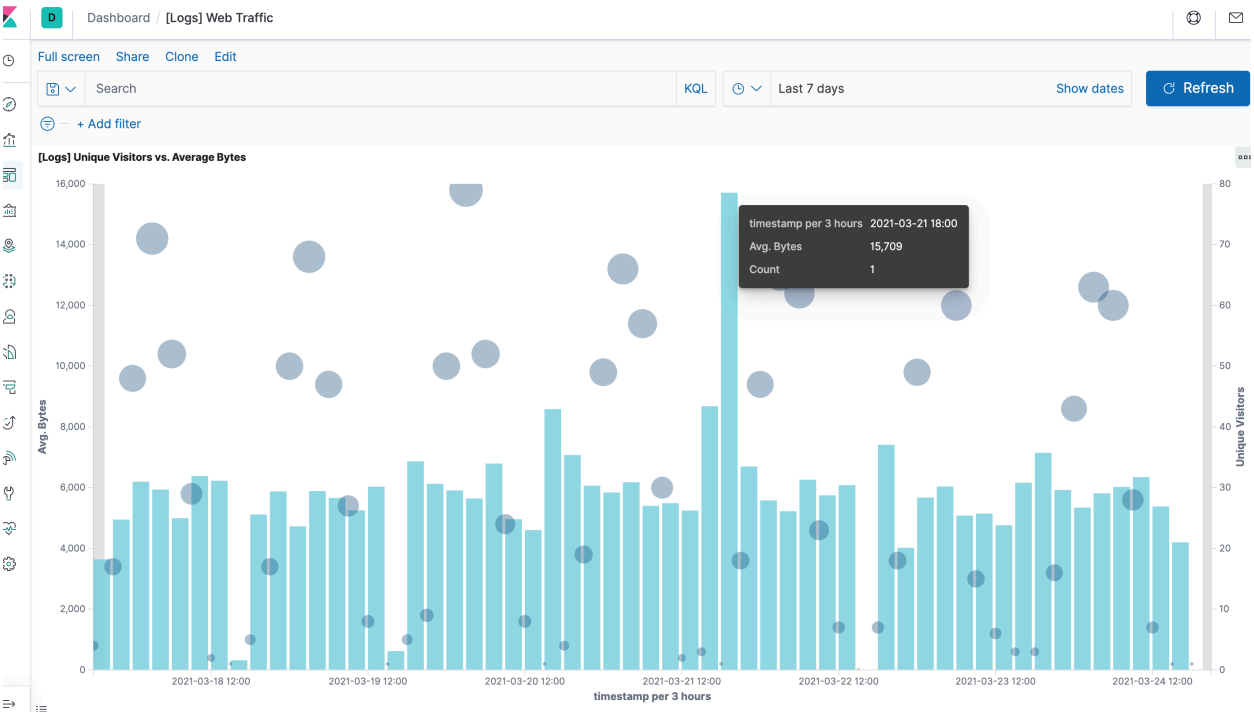
**rpm**:  file with the RPM file extension is a Red Hat Package Manager file that's used to store installation packages on Linux operating systems

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.

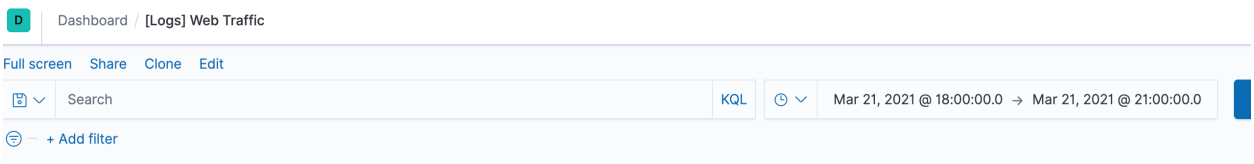

Locate the time frame in the last 7 days with the most amount of bytes (activity).
In your own words, is there anything that seems potentially strange about this activity?

> We need to investigate why one user is using considerably higher number of bytes (15709) than other users

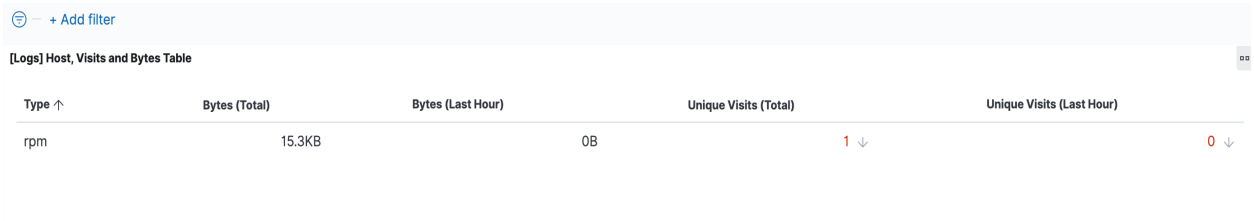



**Filter the data by this event**.

What is the timestamp for this event?




What kind of file was downloaded?

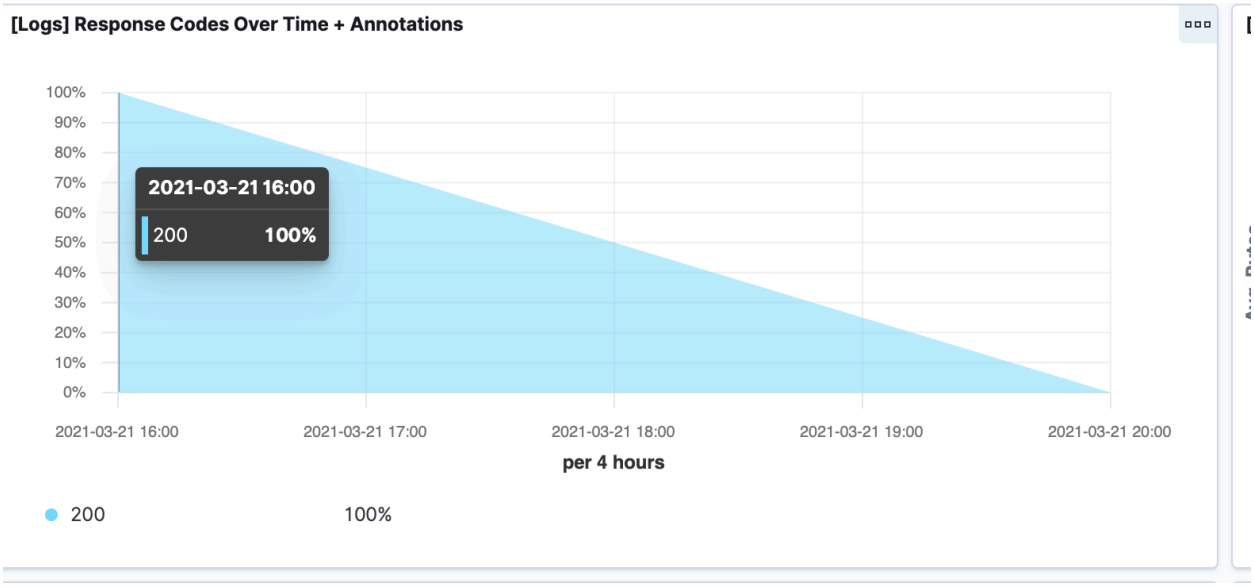



From what country did this activity originate?

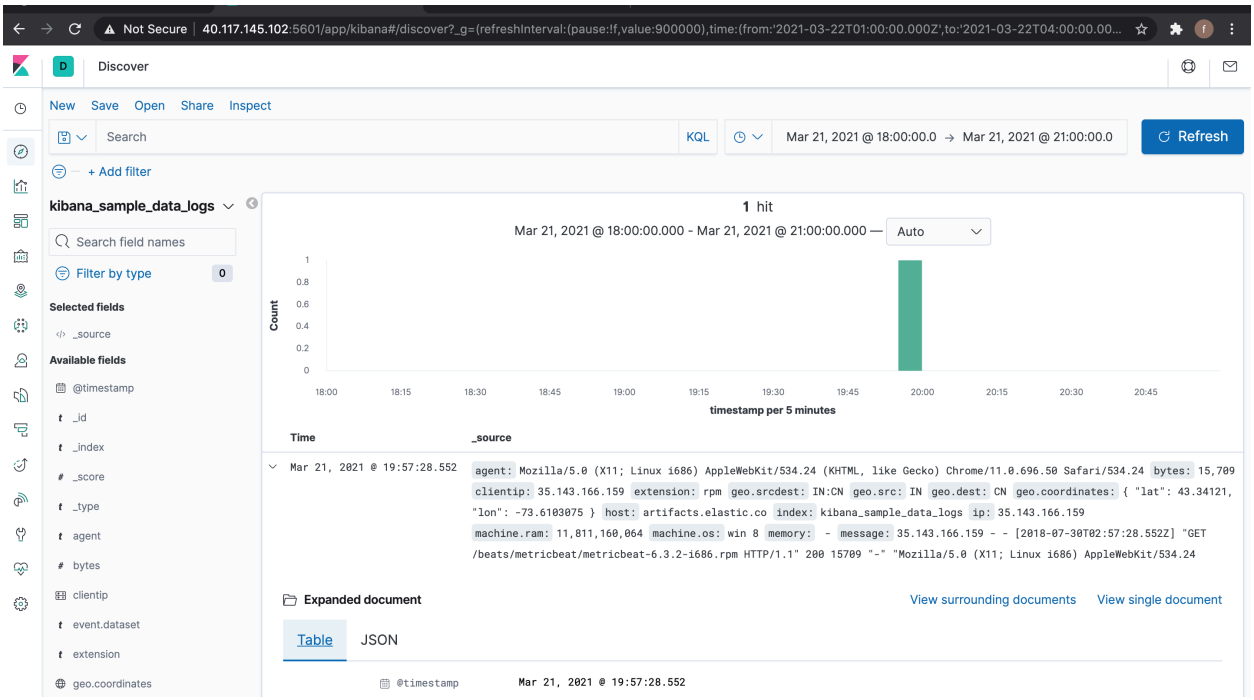
INDIA


What HTTP response codes were encountered by this visitor?

200 OK



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




What is the source IP address of this activity? What are the geo coordinates of this activity?

| | | |
|---|---|---|
| geo.coordinates | { "lat": 43.34121, "lon": -73.6103075 } |
| t geo.dest | CN |
| t geo.src | IN |
| t geo.srcdest | IN:CN |
| t host | artifacts.elastic.co |
| # hour_of_day | 2 |
| t index | kibana_sample_data_logs |
| ip | 35.143.166.159 |
| t machine.os | win 8 |

What OS was the source machine running?

| | |
|---|---|
| t machine.os | win 8 |

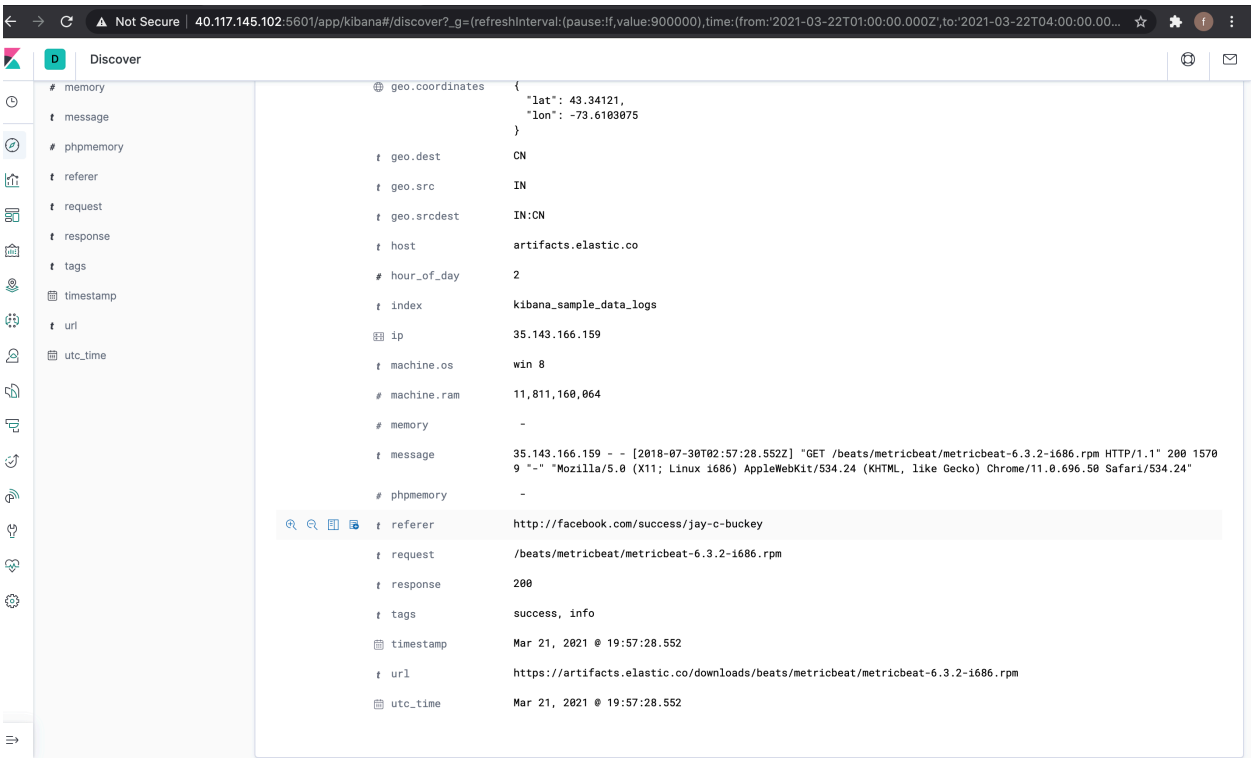
What is the full URL that was accessed?

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

From what website did the visitor's traffic originate?

Facebook

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




**Review**

What do you think user was doing?

User was downloading a RedHat linux package, which is used to store installation packages on Linux OS

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

Linux packages are generally harmless and vastly used by developers, sysadmins to install updates on system. Further analysis is needed to determine the download site

Is there anything that seems suspicious about this activity?

The only point of concern is traffic is originating from Facebook, which seems not right to post installation packages link on facebook

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

Posting packages updated on Facebook most likely not in compliance and this user's activity needs to be monitored and investigated