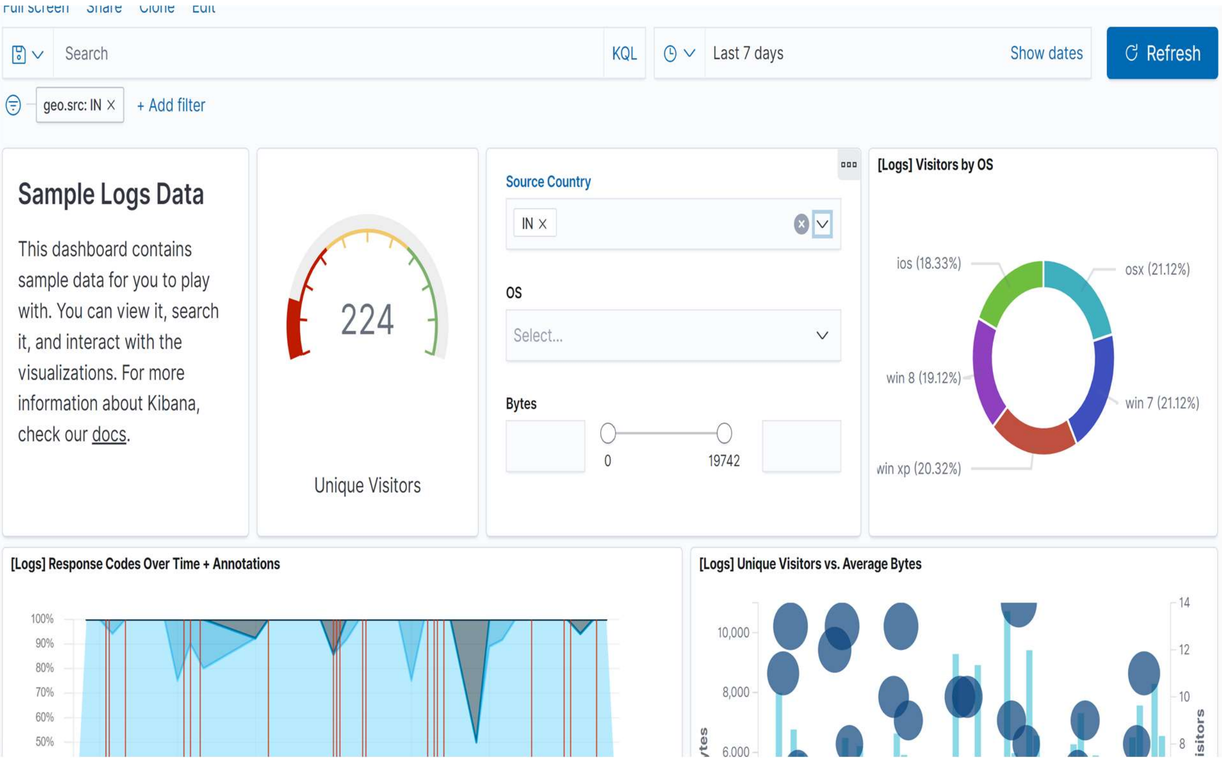
Day3 Activity 1

1. 224 unique visitors in India in last 7 days



Last 7 days

geo.src: IN

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

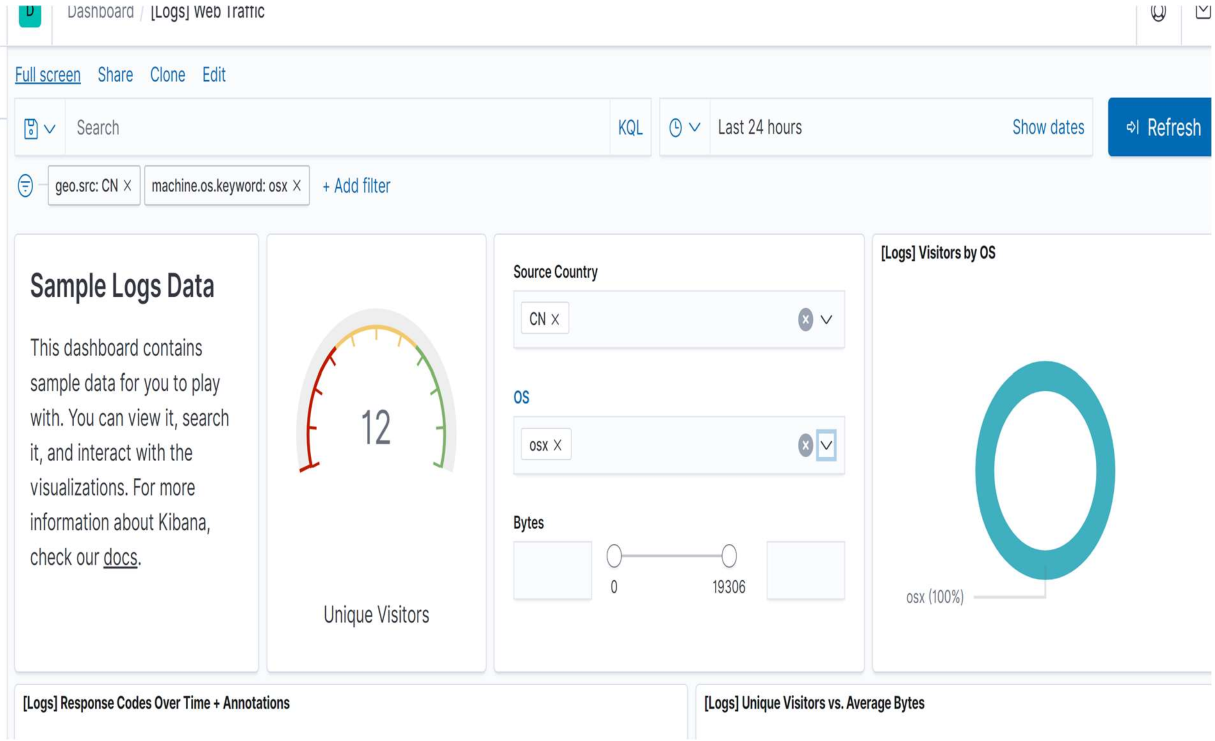
224

Source Country: IN

OS: Select...

Bytes: 0 – 19742

2. 12



Dashboard / [Logs] Web Traffic
Full screen Share Clone Edit
Search
KQL
Show dates
Refresh
+ Add filter
Unique Visitors
[Logs] Visitors by OS
osx (100%)
[Logs] Response Codes Over Time + Annotations
[Logs] Unique Visitors vs. Average Bytes

Last 24 hours

geo.src: CN machine.os.keyword: osx

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

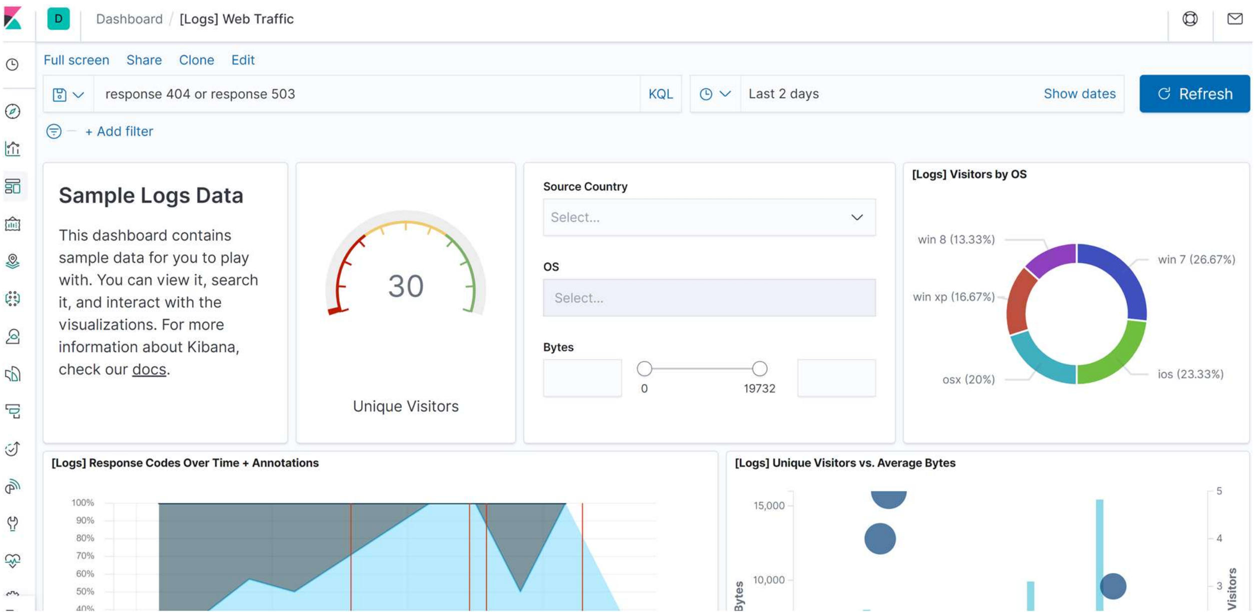
12

Source Country: CN

OS: osx

Bytes: 0 – 19306

3. Total 30 visitors with 404 or 503 response



response 404 or response 503

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

4. China produced majority of traffic
5. 10am had the highest amount of traffic
6. File types are:
   a. Css – cascading style sheets
   b. Deb – standard Unix archive containing two gzipped archive, one for installer information and another for installation data
   c. Gz – compressed file archive
   d. Rpm – redhat package manager file for linux installation packages
   e. Zip – archives that store multiple files
7. Time frame for most amount of bytes in 3/20 and 3/21 which is Saturday and Sunday. On both days, peak seems to be occurring around 15.00, with unique visitors 3-4 at that time. That means a few specific people are downloading vast amounts of data at that time.
8. Timestamp for this event is 2021-03-21 17.00
   a. Type of file downloaded for gz zip file
   b. Activity originated from India and China
   c. HTTP response codes were 200
9. Source:
   a. Source ip is 138.234.210.146
   b. { "lat": 62.06048639, "lon": -163.3021108 }
   c. Source OS was OSX (Mac os)

d. https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.3.2-linux-x86.tar.gz

e. Refer was http://www.elastic-elastic-elastic.com/success/robert-d-cabana

10. File seems to be a regular filebeat archived file for linux installation. It does not seem suspicious.