1. Sample data loaded…
2. Questions:
   * 228 Unique visitors from India

Graphical user interface, application

Description automatically generated

* + 0 unique users were using OSX from China in last 24 hours

Graphical user interface

Description automatically generated

* + 0% received 404 errors; 0% received 503 errors

Chart

Description automatically generated

* + The United States produced the majority of the traffic over the last 7 days

Map

Description automatically generated

* + 11 AM

Chart

Description automatically generated

* + gz files are compressed files that use gzip compression, css files define font, size, color and location of html information on a webpage, zip files are also compressed files and contain one or more files or directories that have been compressed into one package, deb files are a Debian Software Package file (Linux) and are installed when using the apt package manager, rpm files are Red Hat Software Package files.

1. Diving Deeper:
   * It looks like only a single user is using the largest amount of bytes

Chart, bubble chart

Description automatically generated

1. Event Questions:
   * March 27 at 19:55

Graphical user interface

Description automatically generated

* + An RPM file

Graphical user interface, application, website

Description automatically generated

* + North America.

Map

Description automatically generated

* + 200 codes

A picture containing chart

Description automatically generated

1. Kibana Discover Questions
   * Source IP: 35.143.166.159
   * Lat: 43:34121 Lon: -73.6103075
   * Windows 8
   * <https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm>
   * Facebook

Graphical user interface, text, application, email

Description automatically generated

1. Investigation Final Thoughts
   * This user is downloading an RPM (Linux) file from the website being monitored.
   * It is unclear whether the file is malicious or not. It could be but we need more information.
   * I find it strange that the user came from Facebook to this download link. Seems suspicious that this kind of file would be available on Facebook.
   * The fact that this link was from Facebook is likely not within compliance guidelines and would need to be investigated further.