Project Day 3

1. Add the sample web log data to Kibana.

Graphical user interface, application, Word

Description automatically generated

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

* 224 unique users

Graphical user interface, application

Description automatically generated

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

* 14 unique users

Graphical user interface, application

Description automatically generated

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

* 50% 404 and 50% 503

Chart

Description automatically generated

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?

* Seems that 10 am had the highest traffic.

Chart, treemap chart

Description automatically generated

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).

Table

Description automatically generated

Gz: A compressed file via the gzip compression utility.

CSS: Cascading style sheets are files that explain how HTML byproduct is displayed on the screen, they can either be embedded style or styles.

Zip:

Deb:

Rpm:

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).

* The largest number of Bytes was 8780 by one user

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

* After inspecting the chart, I noticed that one user used 8780 bytes which was the highest in usage in the last 7 days

Chart, bubble chart

Description automatically generated

Filter the data by this event. What is the timestamp for this event?

* The timestamp indicates 14:55

Chart, bar chart

Description automatically generated

What kind of file was downloaded?

* Gz @ 16.4KB

Graphical user interface

Description automatically generated with medium confidence

From what country did this activity originate?

* China

What HTTP response codes were encountered by this visitor?

* 200

A picture containing timeline

Description automatically generated

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

What is the source IP address of this activity?

* 172.71.191.193

Graphical user interface, text, application, email

Description automatically generated

What are the geo coordinates of this activity?

* Lat : 35.97636444, lon -115.1327708

Graphical user interface, text, application, email

Description automatically generated

What OS was the source machine running?

* Windows 8

Graphical user interface, text, application, email

Description automatically generated

What is the full URL that was accessed?

* <https://cdn.elastic-elastic-elastic.org/styles/ad-blocker.css>

Graphical user interface, text, application

Description automatically generated

From what website did the visitor's traffic originate?

* <http://twitter.com/success/yi-so-yeon>

Graphical user interface, text, application, email

Description automatically generated