EXPLORING KIBANA #3

`Activity File: Exploring Kibana`

•You are a DevOps professional and have set up monitoring for one of your web servers. You are collecting all sorts of web log data and it is your job to review the data regularly to make sure everything is running smoothly.

•Today, you notice something strange in the logs and you want to take a closer look.

•Your task: Explore the web server logs to see if there's anything unusual. Specifically, you will:

:warning: **Heads Up**: These sample logs are specific to the time you view them. As such, your answers will be different from the answers provided in the solution file.

Instructions

1.Add the sample web log data to Kibana.

2.Answer the following questions:

•In the last 7 days, how many unique visitors were located in India? **In the last 7 days there were 225 unique visitors from India.**

•In the last 24 hours, of the visitors from China, how many were using Mac OSX? **In the last 24 hours 7 visitors from China were Mac OSX.**

•In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? **In the last two days 100% of visitors had the 503 error and 0% had the 404 error.**

•In the last 7 days, what country produced the majority of the traffic on the website? **In the last 7 days the United States produced the majority of the traffic on the website.**

•Of the traffic that's coming from that country, what time of day had the highest amount of activity? **1Pm was the time of day that the highest activity coming from China.**

•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).

- **Ccs- cascading style sheet- it's used to format the contents of a webpage**
- **Deb- debian- it's a standard Unix archive that contains 2 biozipped archives, one for the installer and another for actual installable data.**
- **gz- gzip- archive file compressed by the standard GNU zip compression algorithm**
- **Rpm- Red Hat Package Manager- is a free and open-sourced package management system**

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? **The strange thing about this activity is that it seems there are only 3 users accessing this much data at this time of day.**

4.Filter the data by this event.

•What is the timestamp for this event? **This activity took place @ 9PM.**

•What kind of file was downloaded? **RPM files were downloaded.**
•From what country did this activity originate? **Country of origin is India.**
•What HTTP response codes were encountered by this visitor? **HTTP response code 200 was encountered by this visitor.**

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

•What is the source IP address of this activity? **IP address is 35.143.166.159**
•What are the geo coordinates of this activity? **Latitude 43.34121, Longitude -73.6103075**
•What OS was the source machine running? **The OS running was Windows 8.**
•What is the full URL that was accessed? **The full url is artifacts.elastic.com**
•From what website did the visitor's traffic originate? **http://facebook.com/success/jay-c-buckey**

6.Finish your investigation with a short overview of your insights.

•What do you think the user was doing? **I think the user was downloading sessions to utilize cookies.**
•Was the file they downloaded malicious? **Yes** If not, what is the file used for?
•Is there anything that seems suspicious about this activity? **Yes**
•Is any of the traffic you inspected potentially outside of compliance guidlines? **The traffic is non-compliant with post package update links on Facebook.**