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? `249`

   - In the last 24 hours, of the visitors from China, how many were using Mac OSX? `9`

   - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? `404 Errors = 25%` `503 Errors = 0%`

   - 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 and 1pm (Hour of Day 12 & 13)`

   - 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). `rpm - Red Hat Package Manager/ Software Package` `gz - gzip file` `zip - compressed archive` `deb - Debian/ Linux Software Package file` `css - Cascading Style Sheet file`

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?
  There is one bar showing a high average of bytes downloaded, but the data shows it is only from 1 user and not multiple users.

4. Filter the data by this event.

   - What is the timestamp for this event? 2022-03-13 from 16:00 to 20:00 with a timestamp of 19:55
   - What kind of file was downloaded? rpm file
   - From what country did this activity originate? India
   - What HTTP response codes were encountered by this visitor? HTTP 200 ok

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

   - What is the source IP address of this activity? 35.143.166.159
   - What are the geo coordinates of this activity? { "lat": 43.34121, "lon": -73.6103075 }
   - What OS was the source machine running? Windows 8
   - What is the full URL that was accessed? /beats/metricbeat/metricbeat-6.3.2-i686.rpm
   - 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? Downloading a large rpm file from the website
   - Was the file they downloaded malicious? If not, what is the file used for? See below
   - Is there anything that seems suspicious about this activity? See below
   - Is any of the traffic you inspected potentially outside of compliance guidlines? See below

The file looks to be a standard “Red Hat Package Manager” or software package file for RedHat based systems. It does not appear to be malicious and could be an install file or update file for Metricbeat v6.3.2.

The only thing that seems suspicious about this activity is that the source is originating from facebook.com from someone posting it or linking to it on facebook.

The traffic coming from facebook in a definitely outside compliance guidelines as it is definitely not guaranteed to be from a trusted source to the organization. Install and update files should come directly from the source servers to ensure data integrity of the files so that they have not been modified in malicious ways with malware or trojans to infect the system it gets installed or updated to.