## 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? **237 unique visitors from India**

- In the last 24 hours, of the visitors from China, how many were using Mac OSX? **7 Unique users from China**

- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? **404 errors were 4.3% (20 users). 503 errors were 3.9% (18 users)**

- 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? **10:00 and 12:00**

- 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).

**- GZ = GZIP, It is a compression file for easy transfer and mobility of data.**

**- CSS = cascading style sheet, file used to format the contents of a webpage.**

**- ZIP = ZIP, is a common file format that's used to compress one or more files together into a single location for easy transfer.**

**- DEB = Debian based distributions, is the installation package format used by all Linux machines.**

**- RPM = Red Hat Package Manager, is a free and open-source package management system for Red Hat software.**

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 only suspicious activity was a download of RPM extension on a Windows 8 machine.**

4. Filter the data by this event.

- What is the timestamp for this event? **Start time, Feb 6, 2022 @ 18:00:00.000 – End Time, Feb 6, 2022 @ 21:00:00.000.**

- 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? **200.**

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

- What is the source IP address of this activity? **clientip:**

**35.143.166.159**

- What are the geo coordinates of this activity? **geo.coordinates:**

**{ "lat": 43.34121, "lon": -73.6103075 }**

- What OS was the source machine running? **machine.os:**

**win 8**

- What is the full URL that was accessed? **https://artifacts.elastic.co/downloads/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? **The user was trying to download Metricbeat.**

- Was the file they downloaded malicious? If not, what is the file used for? **No. Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics from the operating system.**

- Is there anything that seems suspicious about this activity? **Yes. The user was on a Facebook page and got redirected to the Metricbeat page for the download.**

- Is any of the traffic you inspected potentially outside of compliance guidelines? **Yes, the traffic could be from a potential bad source which could compromise the integrity of the data.**

---

Â© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.