Exploring Kibana with Sample Data

Add the sample web log data to Kibana. Answer the following questions:

- In the last 7 days, how many unique visitors were located in India?
  224

- In the last 24 hours, of the visitors from China, how many were using Mac OSX?
  72

- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?
  404 error: up to 20%
  503 errors: up to 9.091%

- 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

- 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).
  Css – Cascading Style Sheet, to format contents of a web page
  Deb – Debian Software Package file, used in Unix-based OS, such as iOS, Linux
  Gz – gzip-compressed archive
  Rpm – Red Hat Package Manager file, to store installation packages on Linux
  Zip – zip-compressed archive

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).
  June 26, 2021 18:00 to June 26, 2021 21:00, specifically at 20:00 UTC

- In your own words, is there anything that seems potentially strange about this activity?
  A very high amount of activity (6586 bytes) , within very short time (5 min), with just 1 unique visitor.

Filter the data by this event.

- What is the timestamp for this event?
  June 26, 2021 18:00 to June 26, 2021 21:00, specifically at 20:00 UTC

- What kind of file was downloaded?
  zip

- From what country did this activity originate?
  Brazil

- What HTTP response codes were encountered by this visitor?
  200 OK (Request Success)

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

- What is the source IP address of this activity?
  17.111.163.53

- What are the geo coordinates of this activity?
  “latitude” : 42.59157139
  “longitude” : -114.7967178

- What OS was the source machine running?
  Win 7

- What is the full URL that was accessed?
  https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-windows-x86_64.zip

- From what website did the visitor's traffic originate?
  http://twitter.com/success/mark-kelly

Finish your investigation with a short overview of your insights.

- What do you think the user was doing?
  The user was downloading a zip-compressed file.

- Was the file they downloaded malicious? If not, what is the file used for?
  Not malicious. It’s the file for installing Kibana, specifically for a Windows OS.

- Is there anything that seems suspicious about this activity?
  Not at first. But the geo source is Brazil, and the geo destination is Malaysia, which is strange for someone trying to get a Kibana download from elastic.co. Also, why did this come the twitter.com website? And the geo coordinates do not

match. The latitude and longitude is in the United States. Something doesn’t add up.

- Is any of the traffic you inspected potentially outside of compliance guidelines? Not generally. But there might be some corporate regulations governing the usage of company website by employees when accessing websites to download and install software. Also, there might be laws governing accessing websites across political and national boundaries and use of VPN.