Exploring Kibana

2. 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 - is a compression file used to archive one or more files on Unix operatin systems by GNU zip compression algorithm.
* css file – formats the contents of a webpage. Displays HTML elements.
* zip – is a single file that contains one or more compressed files in Windows (Microsoft)
* deb – is a Unix archive that contains two bzipped or gzipped archives. Deb files are usually used to install packages in Debian based Linux versions.
* rpm – an installation package originally developed for Red Hat Linux operating systems.

1. 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 amounts of bytes (activity). The time frame with the most amounts of bytes took place between Sunday 5/16/21 and Monday 5/17/21.
* In your own words, is there anything that seems potentially strange about this activity? This is potentially strange because even though high amounts of bytes were used, the number of unique visitors was relatively low as compared to other time frames.

1. Filter the data by this event.
   * What is the timestamp for this event? 5/16/21 at 22:57:28.5 or 10:57 pm.
   * 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?

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

* + What is the source IP address of this activity? The source IP is 10.2.0.4
  + What are the geo coordinates of this activity?
  + What OS was the source machine running? Windows 8
  + What is the full URL that was accessed? http://10.2.0.4:9200
  + From what website did the visitor's traffic originate? elasticsearch

1. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing? The user was monitoring all three Web VMs looking for an open port. The attempt was through port 9200.