**2. Answer the following questions:**

- In the last 7 days, how many unique visitors were located in India? 238

- In the last 24 hours, of the visitors from China, how many were using Mac OSX? 78

- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

404 - 6.098% 503 - 3.571%

- In the last 7 days, what country produced the majority of the traffic on the website? Chine

- Of the traffic that's coming from that country, what time of day had the highest amount of activity? 12 pm and 3 pm (hours 12 and 15)

- 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:** GZ files are compressed files created using the gzip compression utility.

**css:** A CSS file is a cascading style sheet (CSS) file used to format the contents of a webpage.

**zip:** ZIP is an archive file format that supports lossless data compression.

**deb:** deb is the format, as well as extension of the software package format for the Linux distribution Debian and its derivatives.

**rpm:** A file with the RPM file extension is a Red Hat Package Manager file that's used to store installation packages on Linux operating systems.

**3. Look at the chart that shows Unique Visitors Vs. Average Bytes.**

- In your own words, is there anything that seems potentially strange about this activity? There is one single user that averages 12,961 bytes, which is a lot higher than the others.

**4. Filter the data by this event.**

- What is the timestamp for this event?

Feb 17, 2021 @ 15:00:00.00 -> Feb 17, 2021 @ 18:00:00.00

- What kind of file was downloaded? deb file

- From what country did this activity originate? India

- What HTTP response codes were encountered by this visitor? 200 OK

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

- What is the source IP address of this activity? 197.207.29.94

- What are the geo coordinates of this activity? "lat": 48.78388139, "lon": -97.62981028

- What OS was the source machine running? Windows 7

- What is the full URL that was accessed? <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.3.2.deb>

- From what website did the visitor's traffic originate? Twitter

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

- What do you think the user was doing? The user downloaded MSIE 6.0, which is a version of Microsoft Internet Explorer.

- Was the file they downloaded malicious? If not, what is the file used for? No it is not malicious. With MSIE downloaded they can now use the MSIE JavaScript Engine correctly.

- Was there anything that seems suspicious about this activity? Yes, if the user intends to use JavaScript with what they downloaded.

- Is any of the traffic you inspected potentially outside of compliance guidelines? No, but their activity could be further monitored to see what they do with it.