**Exploring Kibana**

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

244

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

7

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

**404 Errors:** 18.182%

**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?**

11AM

**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 – This is a language used for creating web pages.

DEB – A distro package used by linux freesource software.

GZ – A compressed format using gzip.

RPM -These are compressed linux software packages used in Red Hat Distros.

ZIP – Another compression format similar to GZIP.

**Locate the time frame in the last 7 days with the most amount of bytes (activity).**

**Avg Bytes:** 9000B

**Unique Visitors:** 2

**In your own words, is there anything that seems potentially strange about this activity?**

This seems strange because the amount of unique visitors was very low in comparison to other times. It would need more research, but this could indicate a user exfiltrating data.

**What is the timestamp for this event?**

**Timestamp:** 2021-01-07 15:16:40

**What kind of file was downloaded?**

CSS

**From what country did this activity originate?**

Poland

**What HTTP response codes were encountered by this visitor?**

200 Degrees

**What is the source IP address of this activity?**

159.148.160.139

**What are the geo coordinates of this activity?**

lat: 32.83422028

lon: -115.5787456

**What OS was the source machine running?**

Windows XP

**What is the full URL that was accessed?**

**From what website did the visitor's traffic originate?**

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

**What do you think the user was doing?**

**Was the file they downloaded malicious? If not, what is the file used for?**

**Is there anything that seems suspicious about this activity?**

**Is any of the traffic you inspected potentially outside of compliance guidlines?**