## 

## Activity File: Exploring Kibana

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

251 Unique Visitors

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

66 Unique Visitors

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

1.266% where 404 errors and 2.532% 503

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?

12pm and 1pm

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: .css files can help define font, size, color, spacing, border and location of HTML information on a webpage. They are downloaded with their .html counterparts and rendered by the browser.

zip**:** A lossless compression format. A .zip file may contain one or more files or directories that have been compressed.

deb: A file with the .deb file extension is a Debian (Linux) Software Package file. These files are installed when using the apt package manager.

rpm**:** .rpm file formats are a Red Hat Software Package file. RPM stands for Red Hat Package Manager.

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).

15,709 Avg. Bytes Cout 1 this was March 21st @ 9:56 P.M.

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

That its only one person using such a high amount of bytes at this time and its not showing anyone else using any Bytes at this time.

Filter the data by this event.

What is the timestamp for this event?

March 21st @ 21:56 -> March 22nd @ 00:00. The time stamp is 21:56

What kind of file was downloaded?

rmp file

From what country did this activity originate?

India

What HTTP response codes were encountered by this visitor?

200

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

What is the source IP address of this activity?

132.186.182.124

What are the geo coordinates of this activity?

"lat": 57.04713806, "lon": -135.3615983

What OS was the source machine running?

ios

What is the full URL that was accessed?

https://elastic-elastic-elastic.org/people/type:astronauts/name:william-s-mcarthur/profile

From what website did the visitor's traffic originate?

http://www.elastic-elastic-elastic.com/success/daniel-brandenstein

Finish your investigation with a short overview of your insights.

What do you think the user was doing?

There downloading package linux from a website.

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

Generally when it comes to downloading packages from Linux they aren't malicious and it should be watched to be on the safe side.

Is there anything that seems suspicious about this activity? Yes there coming form <http://www.elastic-elastic-elastic.com/success/daniel-brandenstein> trying to get into <https://elastic-elastic-elastic.org/people/type:astronauts/name:william-s-mcarthur/profile>

Is any of the traffic you inspected potentially outside of compliance guidelines

This should be watched because it seems like they are trying to add a package into this profile so when someone goes to look it up they will have a hidden payload that has been embedded into this person profile page.