1. Answer the following questions:

    - In the last 7 days, how many unique visitors were located in India? **250**

    - In the last 24 hours, of the visitors from China, how many were using Mac OSX? **66**
    - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 404 errors--100% and 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? **12 pm and 1 pm**
    - 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=** files are compressed files created using gzip compression utility
    - **.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 may 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=** These file formats are a hat software package file. RPM stands for Red Hat Package manager
2. 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).
    - In your own words, is there anything that seems potentially strange about this activity?

    At approximately 2300 hours, there were over 15,000 bytes coming from one user, which is suspicious.

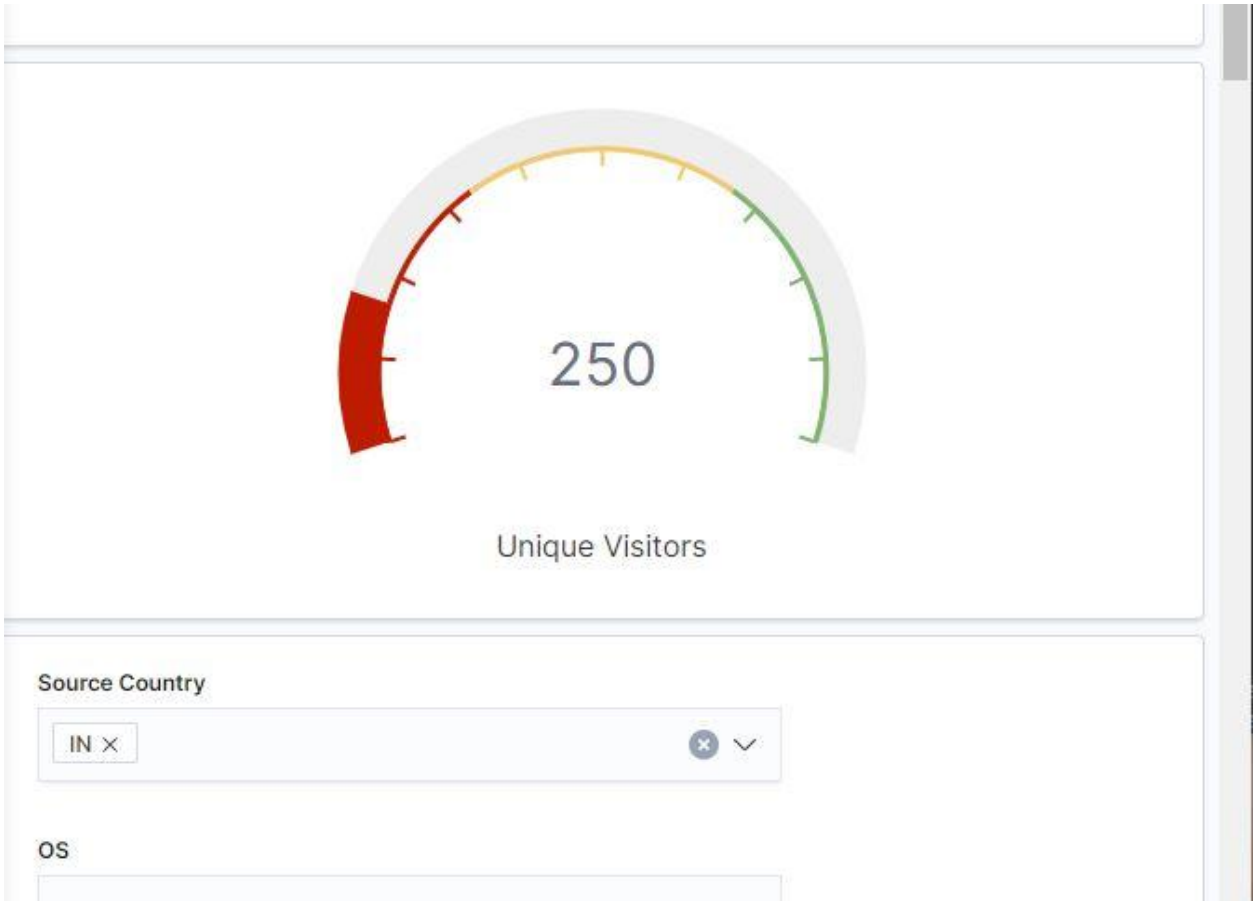
3. Filter the data by this event.

    - What is the timestamp for this event? **22:55:00-23:55:00**
    - What kind of file was downloaded? **.rmp**
    - From what country did this activity originate? **India**
    - What HTTP response codes were encountered by this visitor? **200 ok**
4. Switch to the Kibana Discover page to see more details about this activity.

- What is the source IP address of this activity? **35.143.166.159**
- What are the geo coordinates of this activity? **{ "lat": 43.34121, "lon": -73.6103075 }**
- What OS was the source machine running? **Windows 8**
- What is the full URL that was accessed? **https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm**
- From what website did the visitor's traffic originate? http://facebook.com/success/jay-c-buckey

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

    - What do you think the user was doing? **It appears this user was downloading some type of Linux file.**
    - Was the file they downloaded malicious? If not, what is the file used for? **Linux files tend not to be malicious however being open souce, they could be altered to become malicious.**
    - Is any of the traffic you inspected potentially outside of compliance guidlines?
    - **Yes because the traffic indicates there was a referral link to Facebook. Posting software packages like this on Facebook could be against guidelines.**



Unique Visitors

Source Country

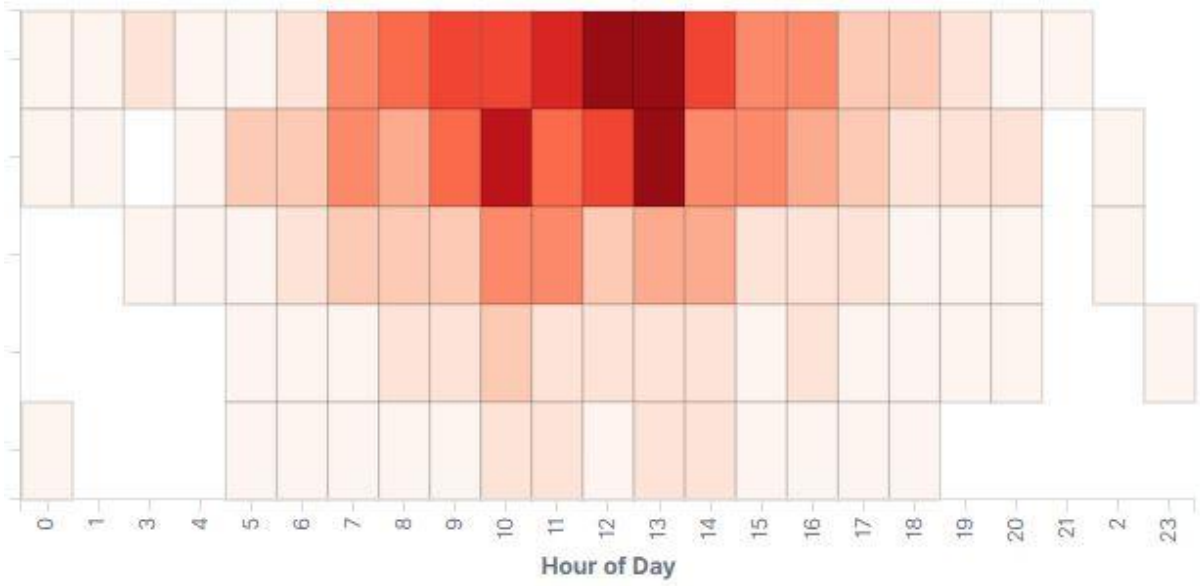
CN ×

OS

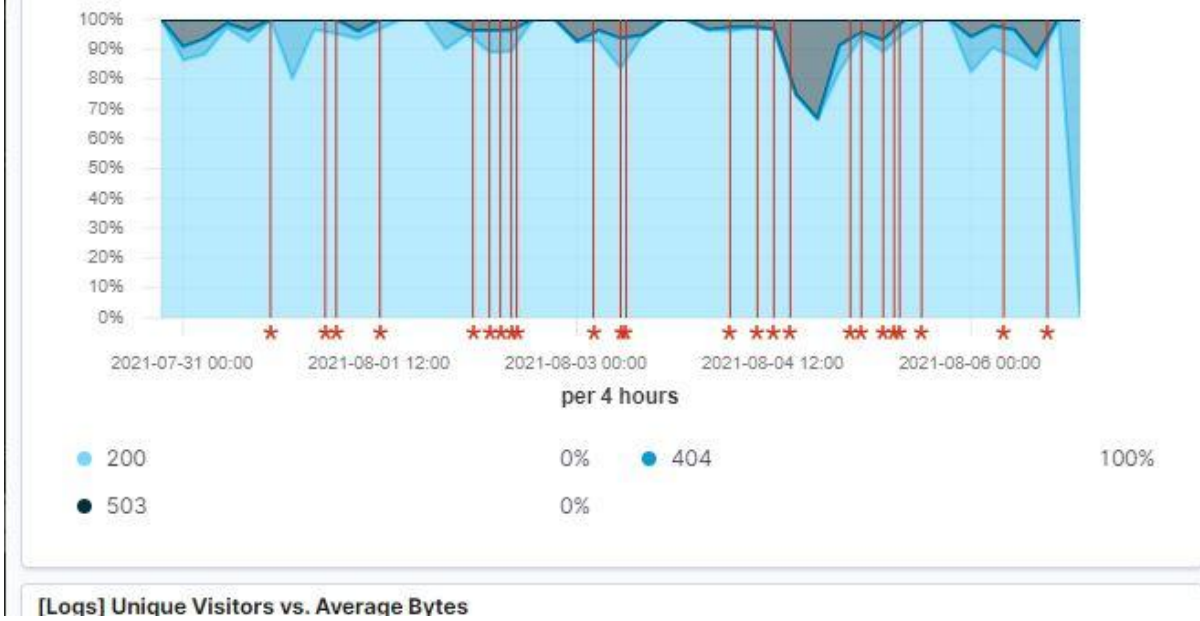
[Logs] Host, Visits and Bytes Table

Type	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	3.1MB	0B	615	0
gz	1.6MB	0B	283	0
css	1.4MB	0B	264	0
zip	1.2MB	0B	205	0
deb	1.1MB	0B	172	0
rpm	460.8KB	0B	71	0

gs] Heatmap

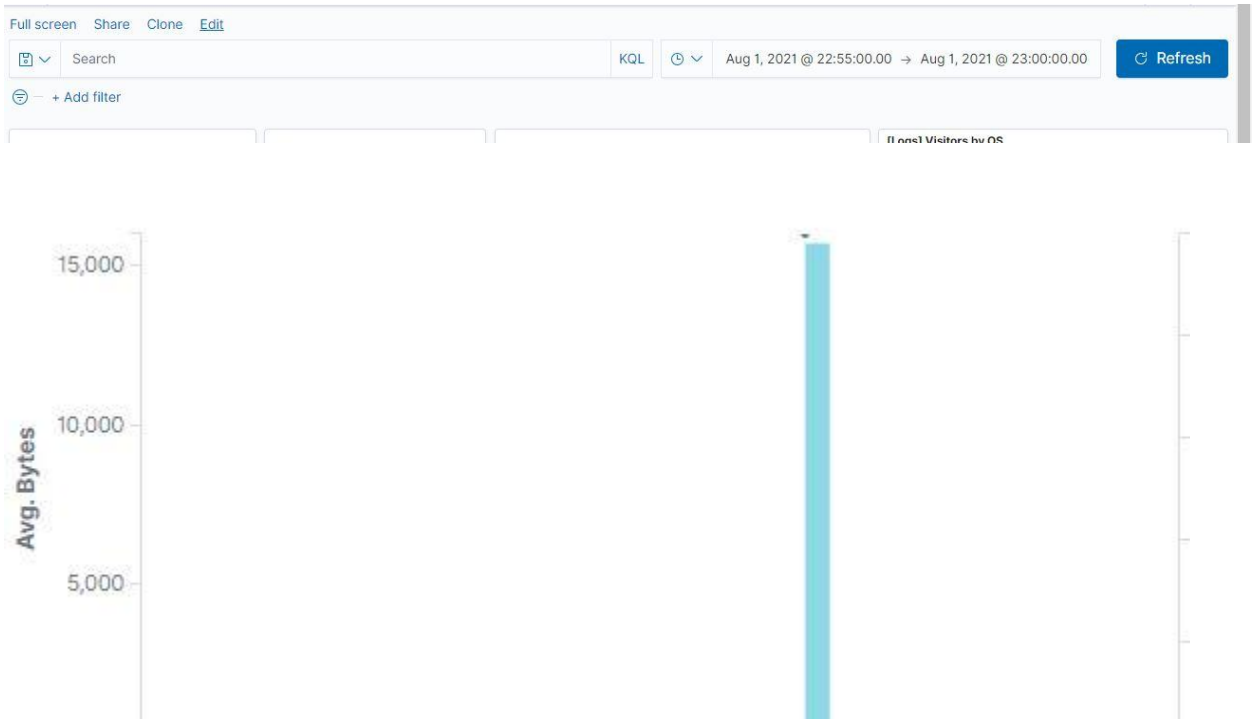


[Logs] Response Codes Over Time + Annotations



[Logs] Unique Visitors vs. Average Bytes


Source
Destination
Logs] Total Requests and Bytes
KAZAKHSTAN
MONGOLIA
KYRGYZSTAN
TURKMENISTAN
CHINA
SOUTH KOREA
IRAN
AFGHANISTAN
PAKISTAN
NEPAL
SAUDI ARABIA
UNITED ARAB EMIRATES
INDIA
TAIWAN
LAOS
Philippine Sea
YEMEN
VIETNAM
SRI LANKA


Full screen
Share
Clone
Edit
Search
KQL
Aug 1, 2021 @ 22:55:00.00 → Aug 1, 2021 @ 23:00:00.00
Refresh
+ Add filter
15,000
10,000
5,000
Avg. Bytes

timestamp per 100 milliseconds

me	_source
ıg 1, 2021 @ 22:57:28.552	agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534. bytes: 15,709 clientip: 35.143.166.159 extension: rpm geo.srcdest: IN:CN geo.src: IN geo.dest: CN geo.coordinates: { "lat": 43.34121, "lon": -73.6103075 } host: artifacts.elastic.co index: kibana_sample_data_logs ip: 35.143.166.159 machine.ram: 11,811,160,064 machine.os: win 8 memory: message: 35.143.166.159 - - [2018-07-30T02:57:28.552Z] "GET /beats/metricbeat/metricbeat-6.3.2-i686.rpm HT

#	phpmemory	-
t	referer	http://facebook.com/success/jay-c-buckey
t	request	/beats/metricbeat/metricbeat-6.3.2-i686.rpm
t	response	200

Aug 1, 2021 @ 22:57:28.552 https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm

Expanded document View surrounding documents View single doc

Table JSON

@timestamp	Aug 1, 2021 @ 22:57:28.552
t	_id	BZERHnsBmHpyCNNxPmrq
t	_index	kibana_sample_data_logs