UR-VIRT-RICH-CYBER-PT-062021-U-C

ELK Stack Project

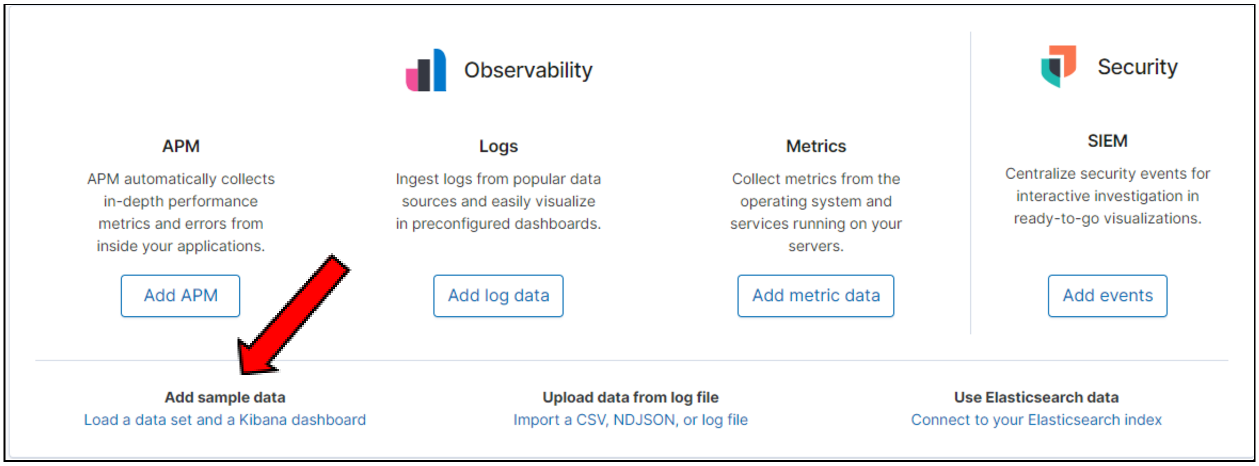
Josh Black

Laura Pratt

Courtney Templeton

Kibana Exploration Activity

To start, I added a sample data set. See below.



APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics

Collect metrics from the operating system and services running on your servers.

SIEM

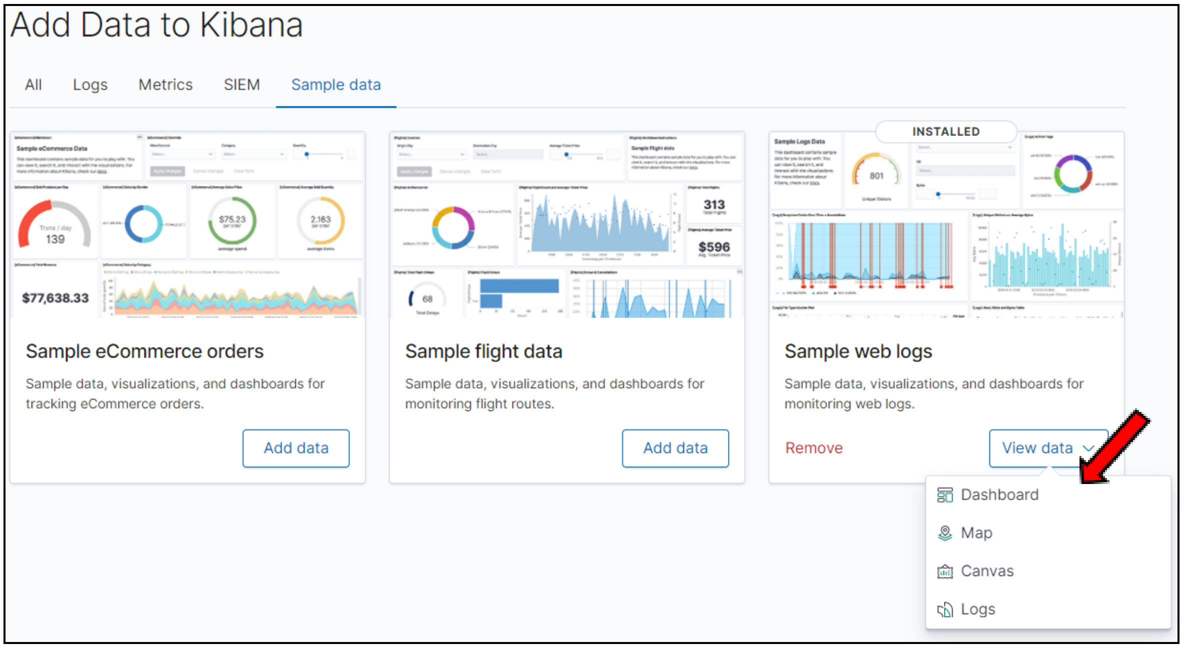
Centralize security events for interactive investigation in ready-to-go visualizations.

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Next, I selected to view the data on my dashboard.



Add Data to Kibana

Sample eCommerce orders

Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data

Sample data, visualizations, and dashboards for monitoring flight routes.

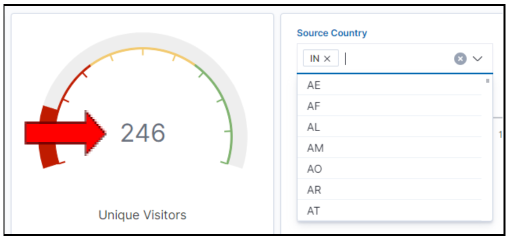
Sample web logs

Sample data, visualizations, and dashboards for monitoring web logs.

The next step is to answer the following questions:

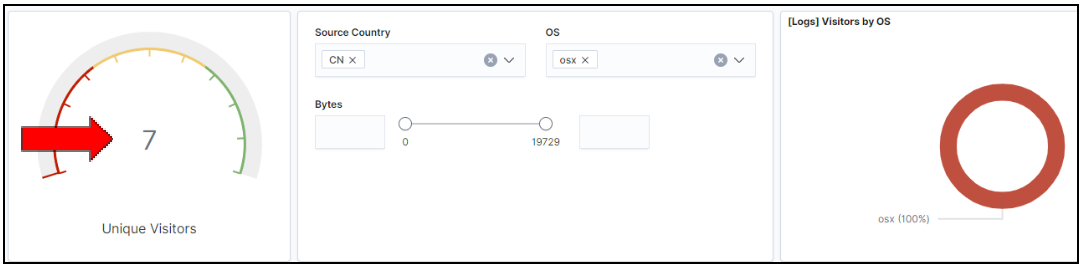
Answer the following questions:

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

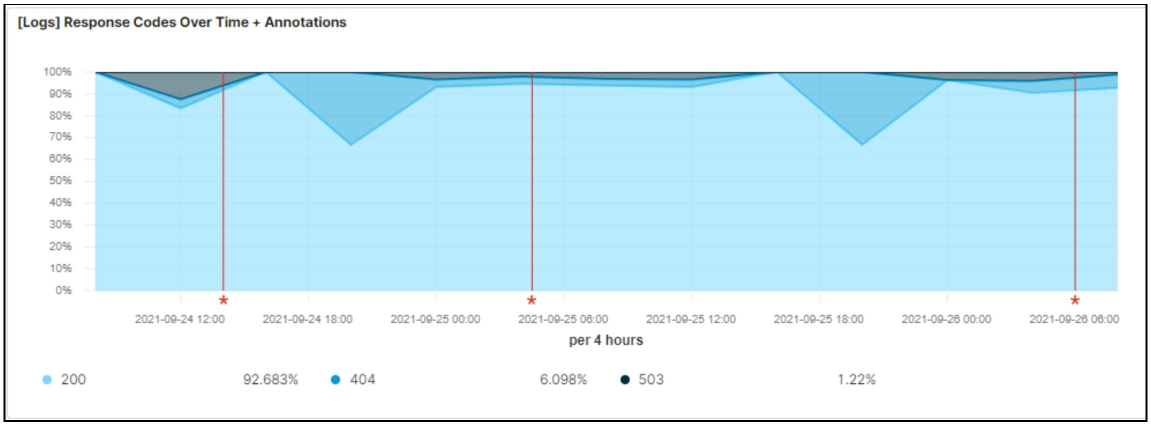


There were 246 unique visitors from India.

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



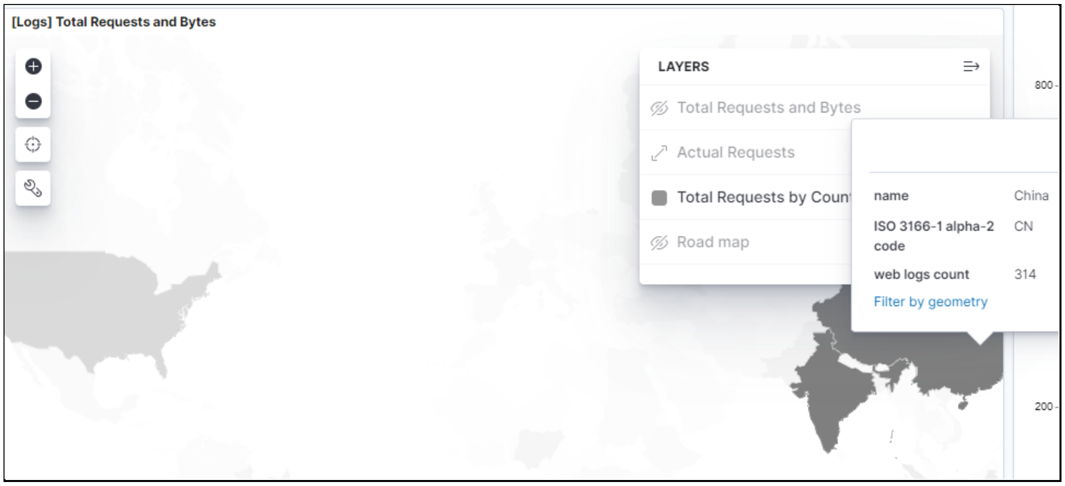
- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?



404 code= 6.098%

503 code= 1.22%

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


[Logs] Total Requests and Bytes

LAYERS

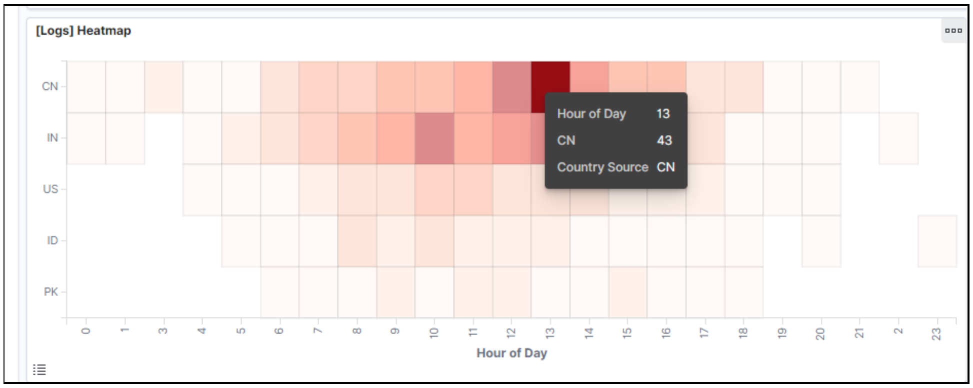
- Total Requests and Bytes
- Actual Requests
- Total Requests by Coun
- Road map

name	China
ISO 3166-1 alpha-2 code	CN
web logs count	314

Filter by geometry

I was able to hide the other layers and just isolate the total requests per country and then based on the heat map, determined that China had the highest total number of requests producing the most traffic.

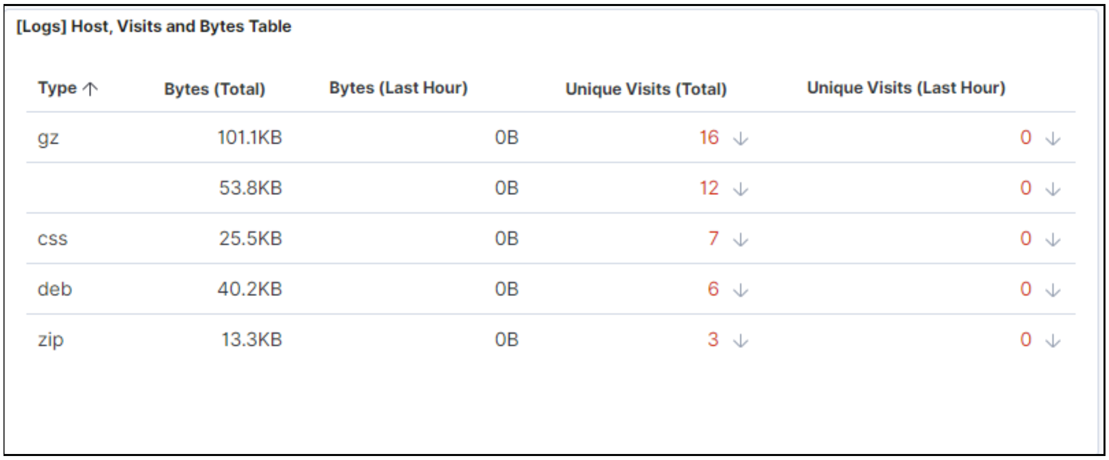
- Of the traffic that's coming from that country, what time of day had the highest amount of activity?


[Logs] Heatmap

Hour of Day	13
CN	43
Country Source	CN

According to this heat map, the time of day was 1300 that had the highest amount of activity.

- 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).



[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
gz	101.1KB	0B	16 ↓	0 ↓
	53.8KB	0B	12 ↓	0 ↓
css	25.5KB	0B	7 ↓	0 ↓
deb	40.2KB	0B	6 ↓	0 ↓
zip	13.3KB	0B	3 ↓	0 ↓

File types:

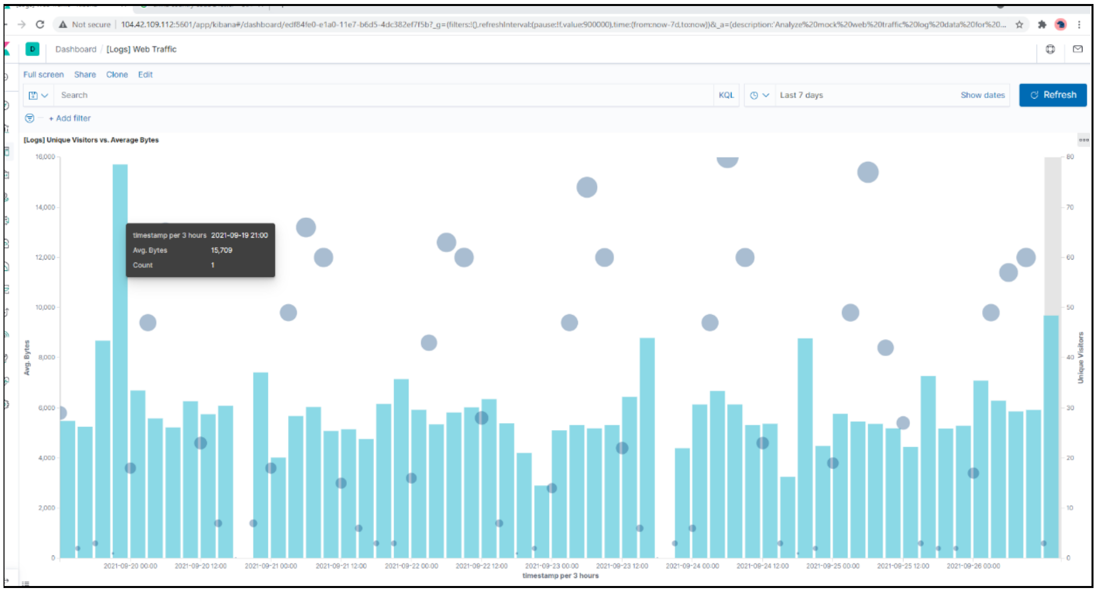
gz-compressed files created using the gzip compression utility

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

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.

Zip-a lossless compression format. A .zip file may contain one or more files or directories that have been compressed.

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 amount of bytes (activity).



Not secure | 104.42.109.112:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:900000),time:(from:now-7d,to:now))&_a=(description:'Analyze%20mock%20web%20traffic%20log%20data%20for%20...

Dashboard / [Logs] Web Traffic

Search | KQL | Last 7 days | Show dates

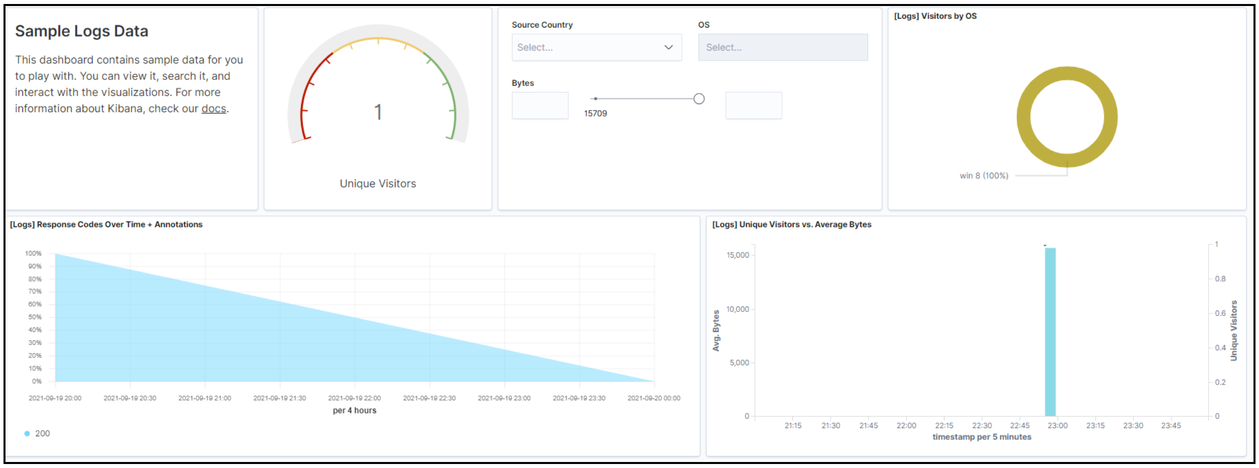
[Logs] Unique Visitors vs. Average Bytes

timestamp per 3 hours	2021-09-19 21:00
Avg. Bytes	15,709
Count	1

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

  It appears that one particular user is using almost double the amount of bytes as multiple users at one time.

2. Filter the data by this event.



Sample Logs Data

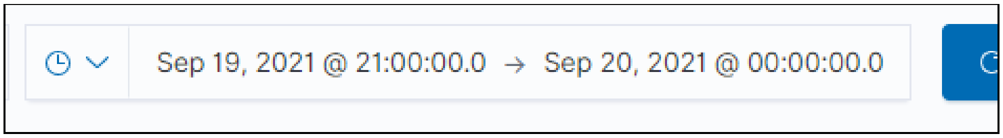
This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

Source Country: Select...

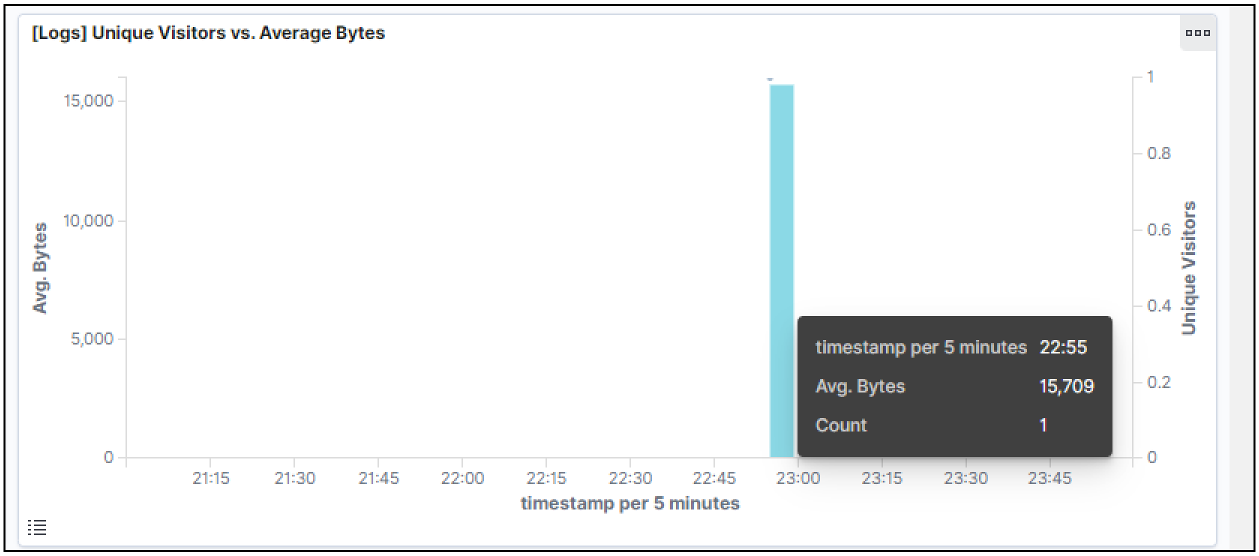
OS: Select...

Bytes: 15709

3. What is the timestamp for this event?



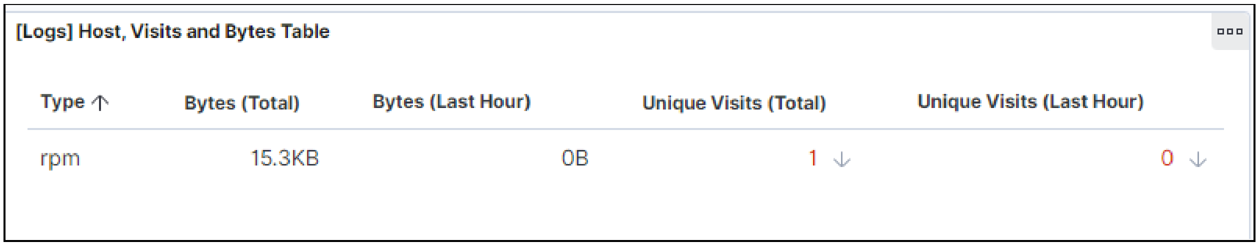
Sep 19, 2021 @ 21:00:00.0 → Sep 20, 2021 @ 00:00:00.0



[Logs] Unique Visitors vs. Average Bytes

timestamp per 5 minutes	22:55
Avg. Bytes	15,709
Count	1

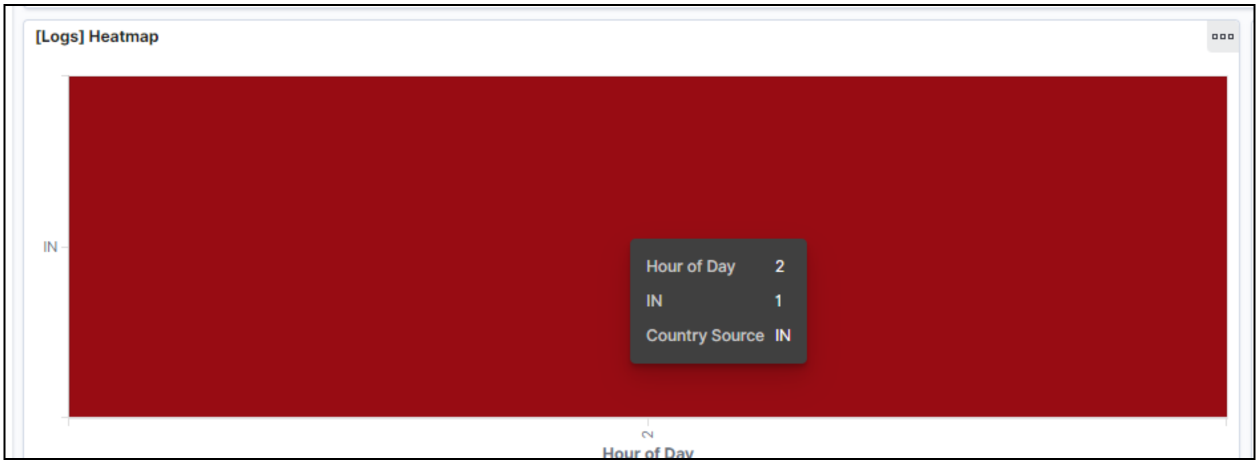
4. What kind of file was downloaded?



[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
rpm	15.3KB	0B	1 ↓	0 ↓

- From what country did this activity originate?

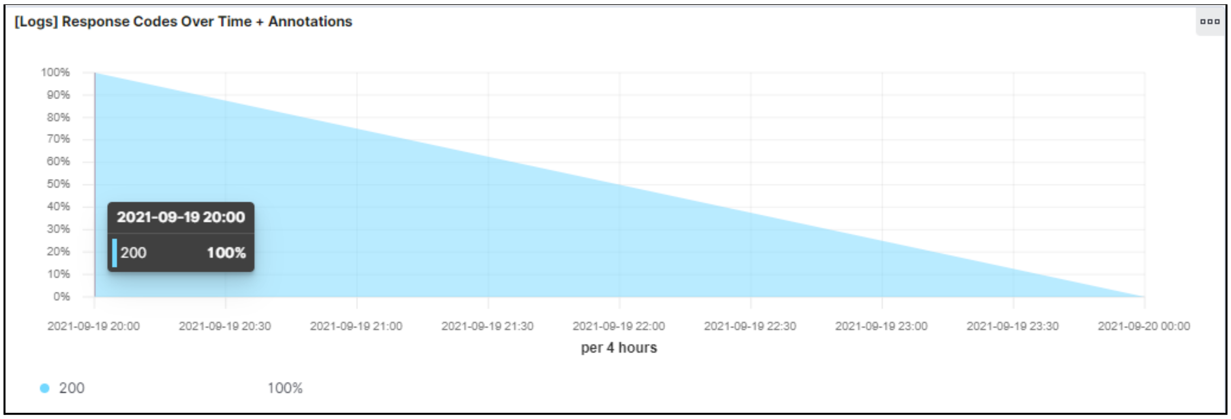


[Logs] Heatmap

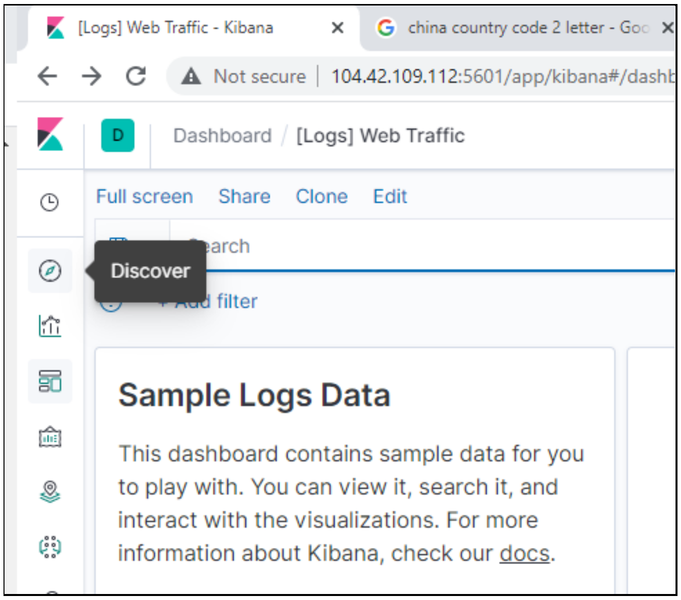
Hour of Day	2
IN	1
Country Source	IN

- What HTTP response codes were encountered by this visitor?

The response code was 200.



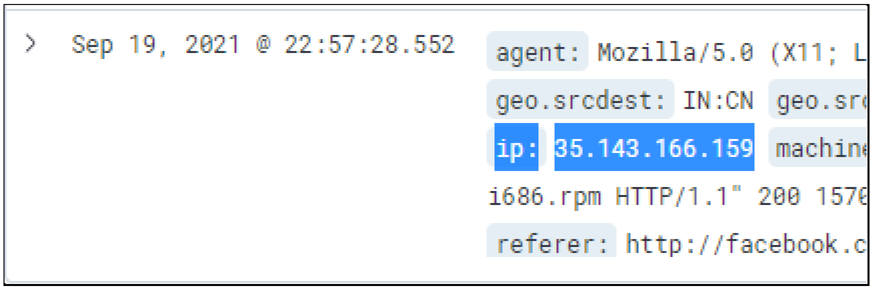
5. Switch to the Kibana Discover page to see more details about this activity.


[Logs] Web Traffic - Kibana
china country code 2 letter - Goo
Not secure
104.42.109.112:5601/app/kibana#/dashb
D
Dashboard / [Logs] Web Traffic
Full screen
Share
Clone
Edit
Search
Discover
+ Add filter

Sample Logs Data

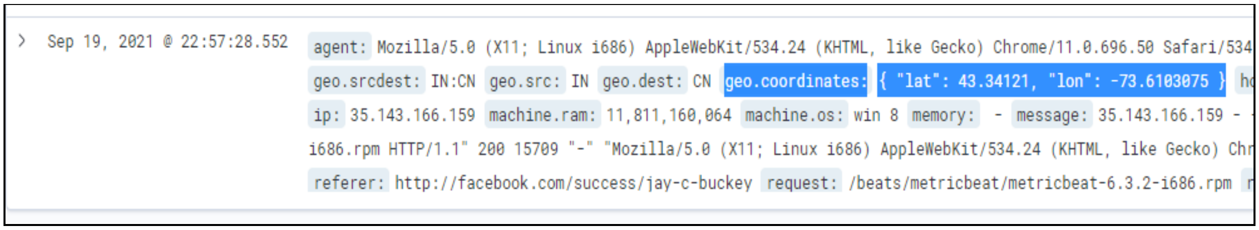
This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

- What is the source IP address of this activity?



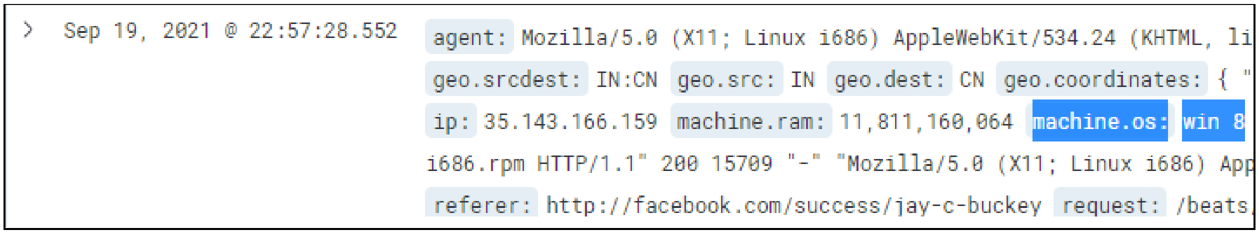
```
>  Sep 19, 2021 @ 22:57:28.552   agent: Mozilla/5.0 (X11; L
                                 geo.srcdest: IN:CN  geo.src
                                 ip: 35.143.166.159  machine
                                 i686.rpm HTTP/1.1" 200 1570
                                 referer: http://facebook.c
```

- What are the geo coordinates of this activity?



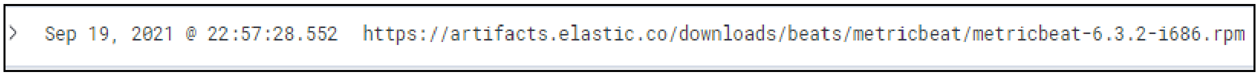
```
> Sep 19, 2021 @ 22:57:28.552   agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534
                                geo.srcdest: IN:CN geo.src: IN geo.dest: CN geo.coordinates: { "lat": 43.34121, "lon": -73.6103075 } hc
                                ip: 35.143.166.159 machine.ram: 11,811,160,064 machine.os: win 8 memory: - message: 35.143.166.159 -
                                i686.rpm HTTP/1.1" 200 15709 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chr
                                referer: http://facebook.com/success/jay-c-buckey request: /beats/metricbeat/metricbeat-6.3.2-i686.rpm r
```

- o What OS was the source machine running?



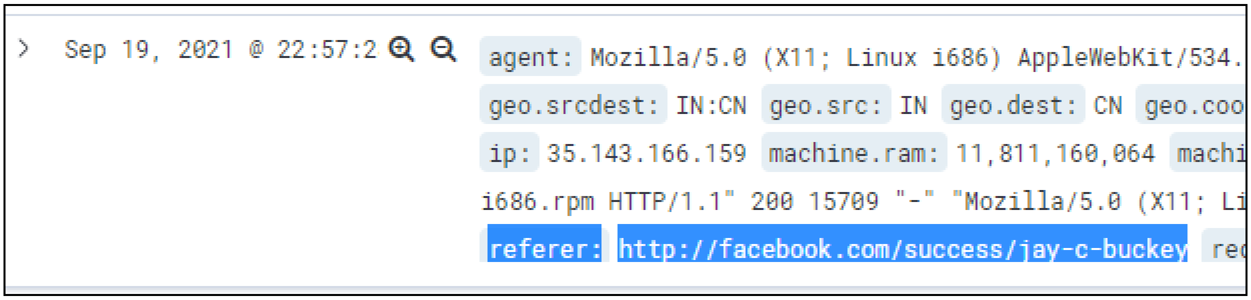
```
> Sep 19, 2021 @ 22:57:28.552   agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, li
                                geo.srcdest: IN:CN geo.src: IN geo.dest: CN geo.coordinates: { "
                                ip: 35.143.166.159 machine.ram: 11,811,160,064 machine.os: win 8
                                i686.rpm HTTP/1.1" 200 15709 "-" "Mozilla/5.0 (X11; Linux i686) App
                                referer: http://facebook.com/success/jay-c-buckey request: /beats
```

- o What is the full URL that was accessed?



```
> Sep 19, 2021 @ 22:57:28.552   https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm
```

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



```
> Sep 19, 2021 @ 22:57:2   agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.
                           geo.srcdest: IN:CN geo.src: IN geo.dest: CN geo.coo
                           ip: 35.143.166.159 machine.ram: 11,811,160,064 machi
                           i686.rpm HTTP/1.1" 200 15709 "-" "Mozilla/5.0 (X11; Li
                           referer: http://facebook.com/success/jay-c-buckey rec
```

6. Finish your investigation with a short overview of your insights.
   - o What do you think the user was doing?
     It looks like the user is trying to get the metricbeat package via Facebook.
   - o Was the file they downloaded malicious? If not, what is the file used for?
     It does not appear malicious based on the data provided. It just appears that they were trying to get the program for data collection through Facebook.
   - o Is there anything that seems suspicious about this activity?
     It is somewhat suspicious just because of the user trying to navigate data collection via Facebook.
   - o Is any of the traffic you inspected potentially outside of compliance guidelines?

     Not with the packet information that I saw.