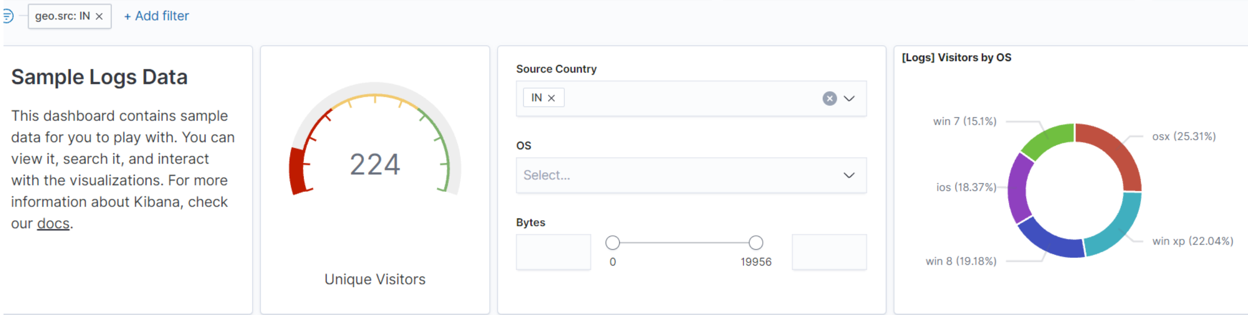
1. Add the sample web log data to Kibana.

2. Answer the following questions:

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

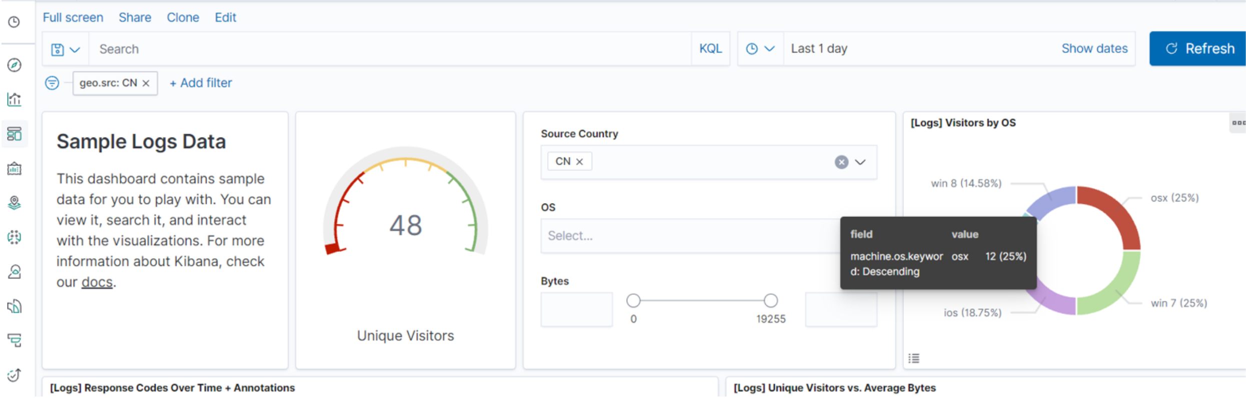


Sample Logs Data

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.

○

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

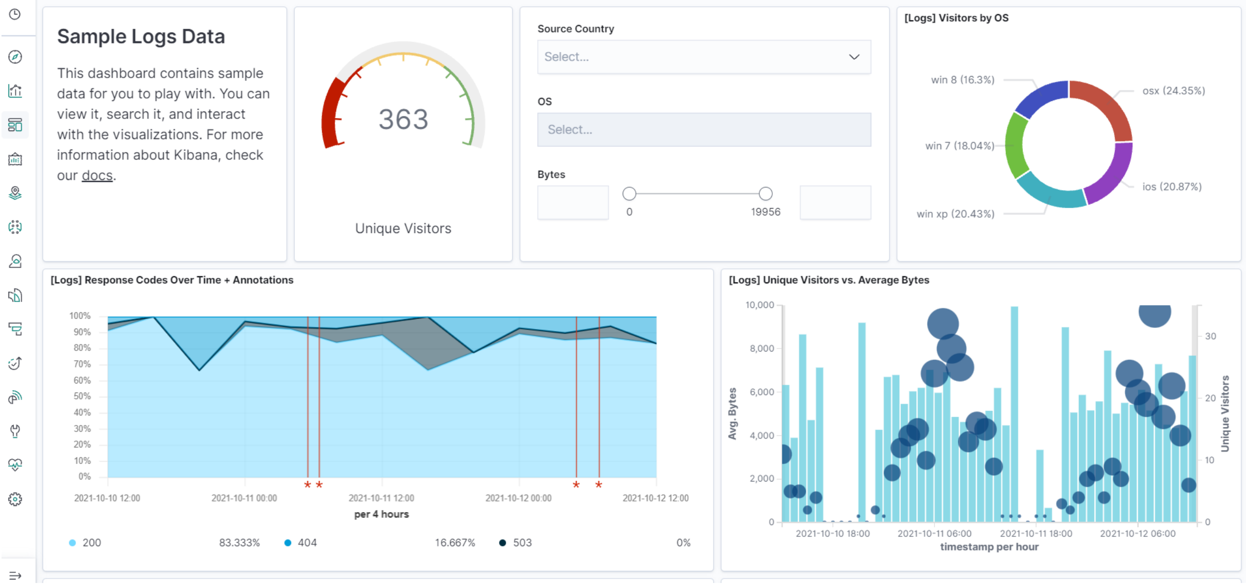


Sample Logs Data

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.

field	value
machine.os.keyword: Descending	osx 12 (25%)

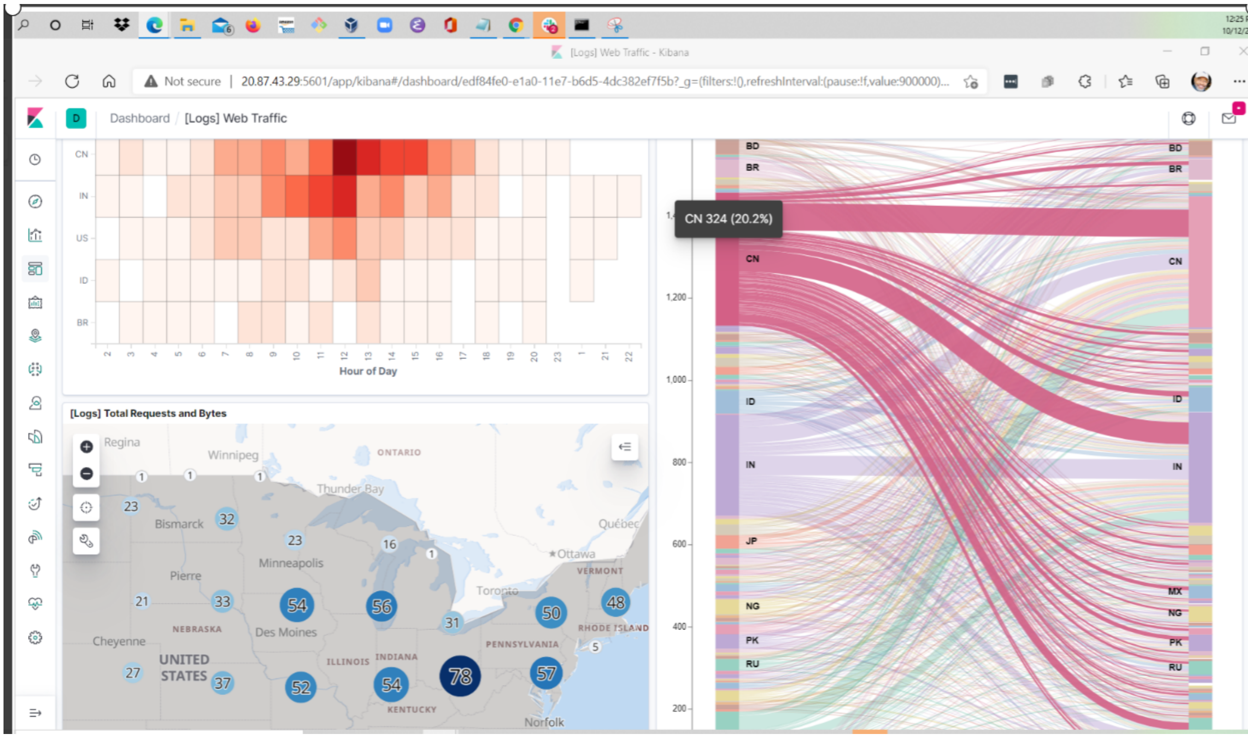
    - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?



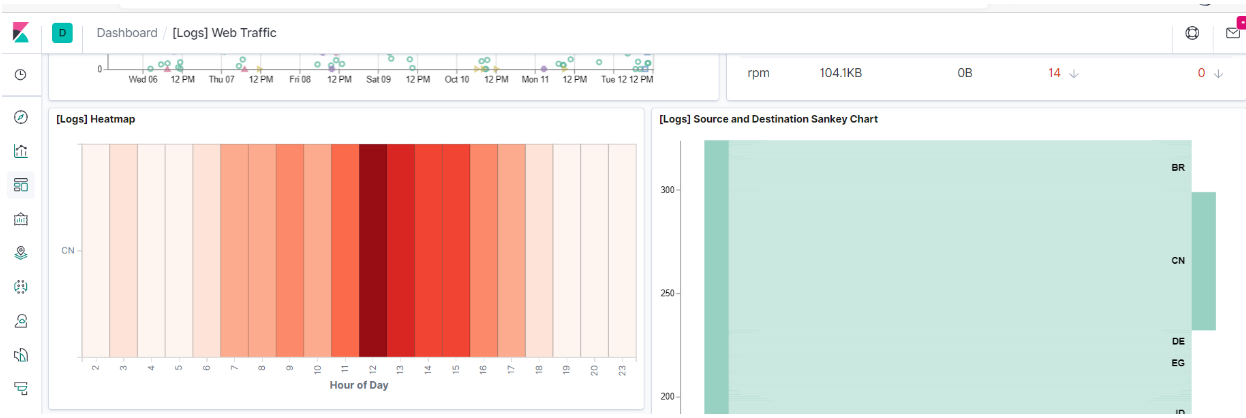
Sample Logs Data

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.

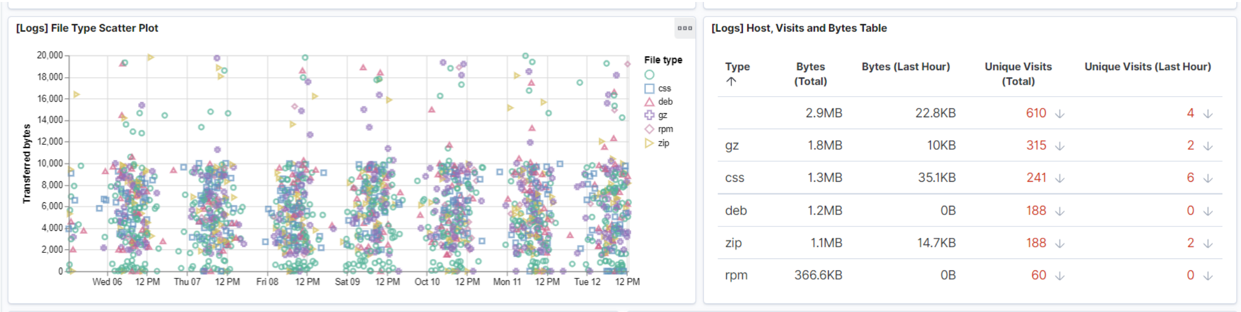
- In the last 7 days, what country produced the majority of the traffic on the website?china



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


D
Dashboard / [Logs] Web Traffic
0
Wed 06 12 PM Thu 07 12 PM Fri 08 12 PM Sat 09 12 PM Oct 10 12 PM Mon 11 12 PM Tue 12 12 PM
rpm 104.1KB 0B 14 0
[Logs] Heatmap
CN
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 23
Hour of Day
[Logs] Source and Destination Sankey Chart
300
250
200
BR
CN
DE
EG
ID

- 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)
	2.9MB	22.8KB	610 ↓	4 ↓
gz	1.8MB	10KB	315 ↓	2 ↓
css	1.3MB	35.1KB	241 ↓	6 ↓
deb	1.2MB	0B	188 ↓	0 ↓
zip	1.1MB	14.7KB	188 ↓	2 ↓
rpm	366.6KB	0B	60 ↓	0 ↓

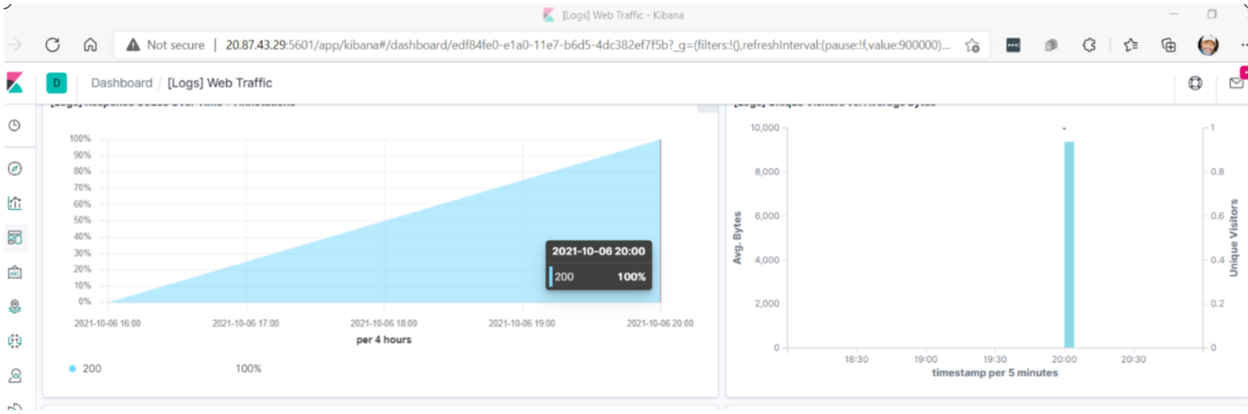
3. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.

   ○ 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?

4. Filter the data by this event.

   ○ What is the timestamp for this event?2000 8pm

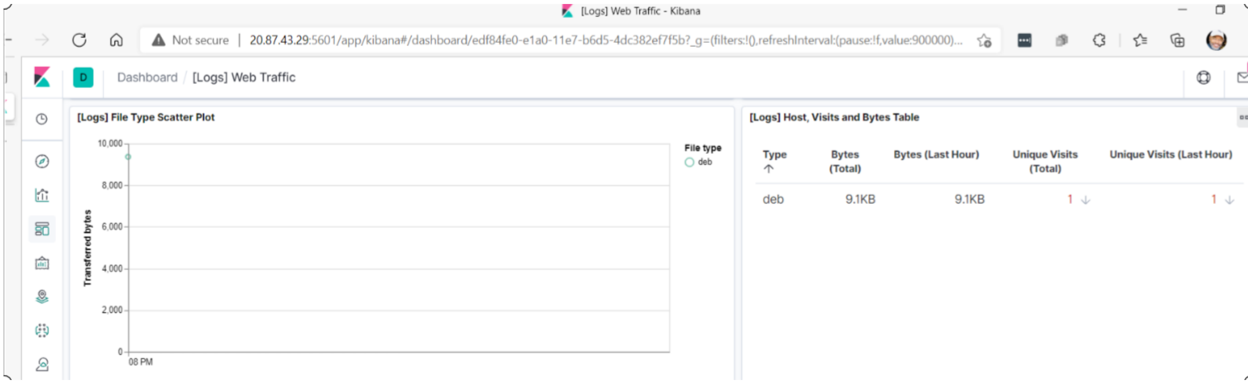


[Logs] Web Traffic - Kibana

Not secure | 20.87.43.29:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:900000)...

Dashboard / [Logs] Web Traffic

   ○ What kind of file was downloaded?deb



[Logs] Web Traffic - Kibana

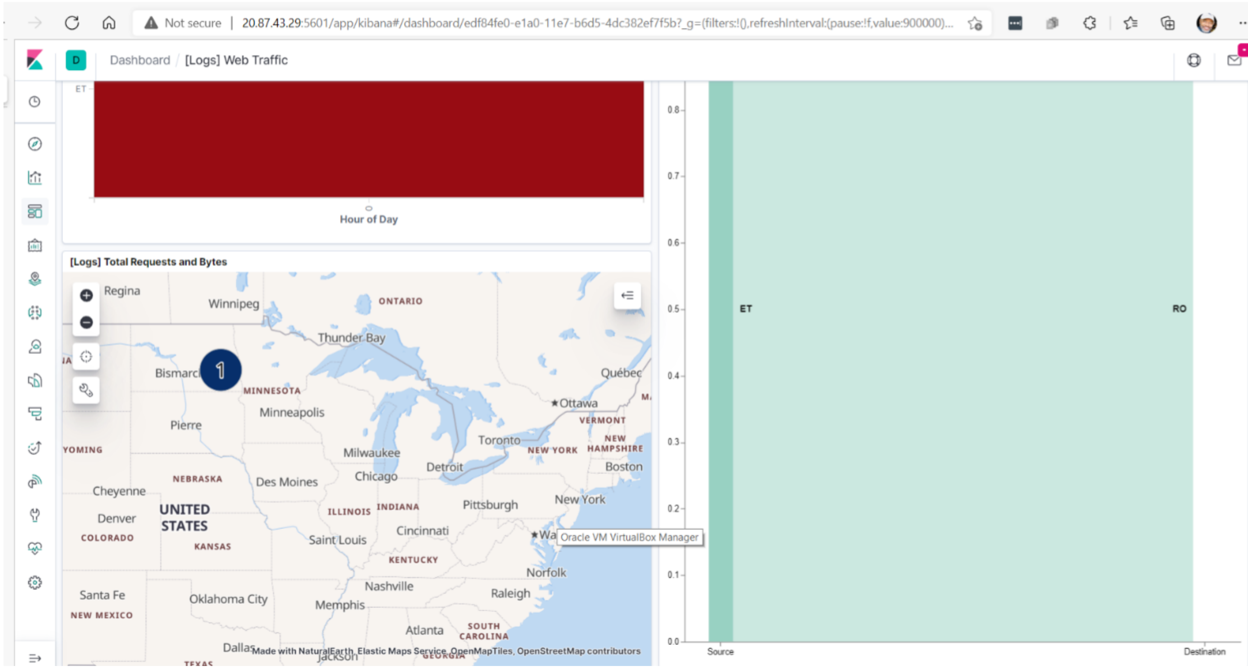
Not secure | 20.87.43.29:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:900000)...

Dashboard / [Logs] Web Traffic

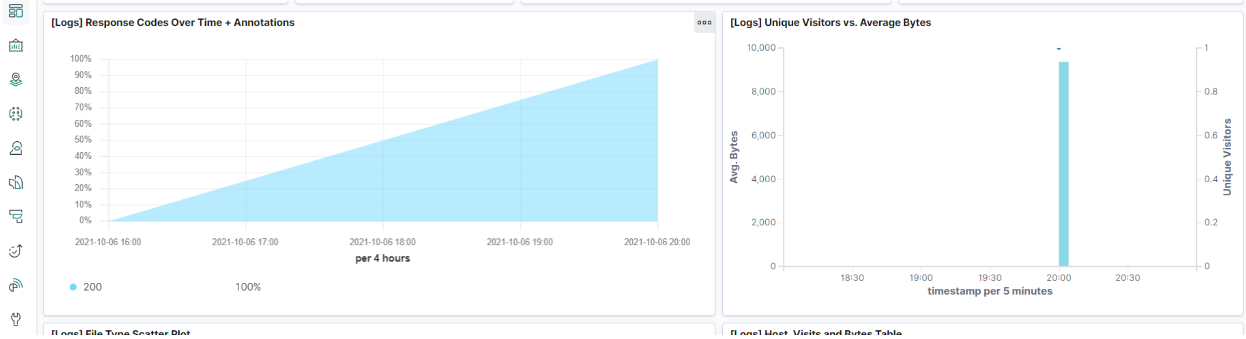
[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
deb	9.1KB	9.1KB	1 ↓	1 ↓

- From what country did this activity originate?Bismarck ND

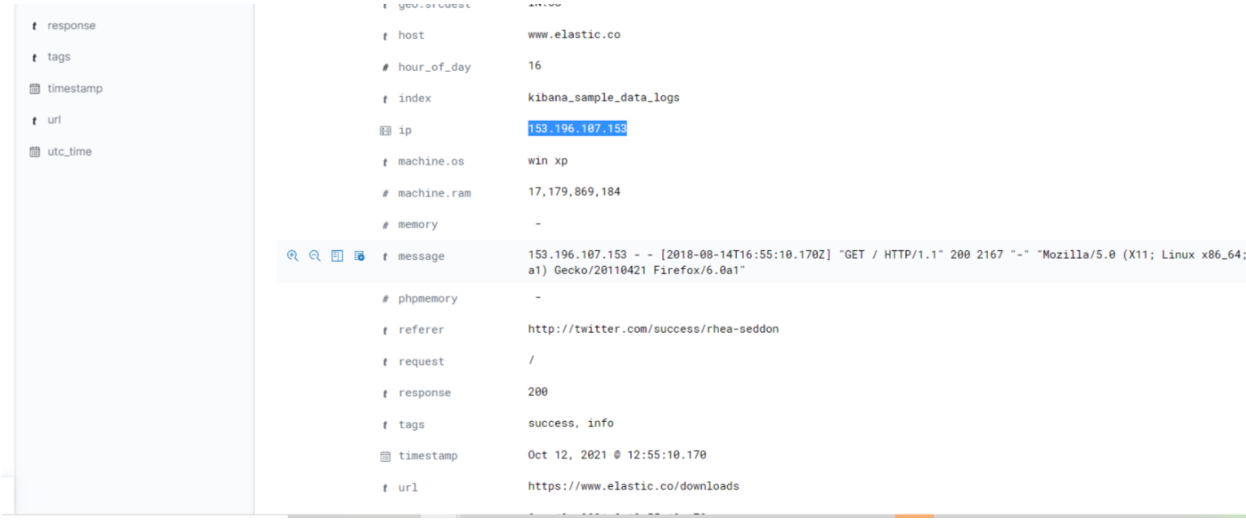


- What HTTP response codes were encountered by this visitor?200



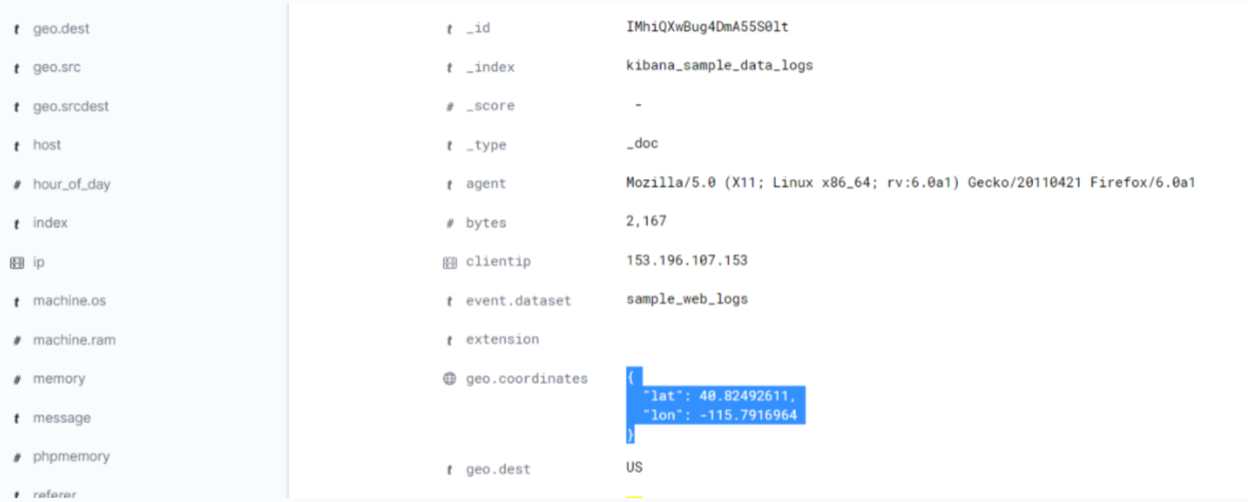
5. Switch to the Kibana Discover page to see more details about this activity.

- What is the source IP address of this activity?153.196.107.153



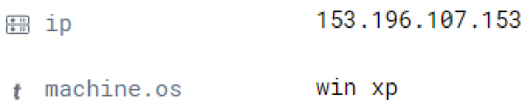
```
host             www.elastic.co
hour_of_day      16
index            kibana_sample_data_logs
ip               153.196.107.153
machine.os       win xp
machine.ram      17,179,869,184
memory           -
message          153.196.107.153 - - [2018-08-14T16:55:10.170Z] "GET / HTTP/1.1" 200 2167 "-" "Mozilla/5.0 (X11; Linux x86_64;
                 a1) Gecko/20110421 Firefox/6.0a1"
phpmemory        -
referer          http://twitter.com/success/rhea-seddon
request          /
response         200
tags             success, info
timestamp        Oct 12, 2021 @ 12:55:10.170
url              https://www.elastic.co/downloads
```

- What are the geo coordinates of this activity?{
- "lat": 40.82492611,
- "lon": -115.7916964
- }



```
_id              IMhiQXwBug4DmA55S0lt
_index           kibana_sample_data_logs
_score           -
_type            _doc
agent            Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1
bytes            2,167
clientip         153.196.107.153
event.dataset    sample_web_logs
extension
geo.coordinates  {
                   "lat": 40.82492611,
                   "lon": -115.7916964
                 }
geo.dest         US
```

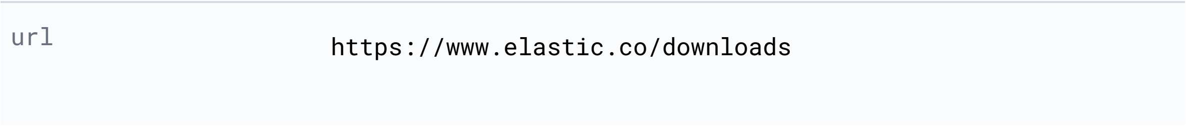
- What OS was the source machine running?win xp



```
ip            153.196.107.153

machine.os    win xp
```

- What is the full URL that was accessed?



```
url              https://www.elastic.co/downloads
```

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

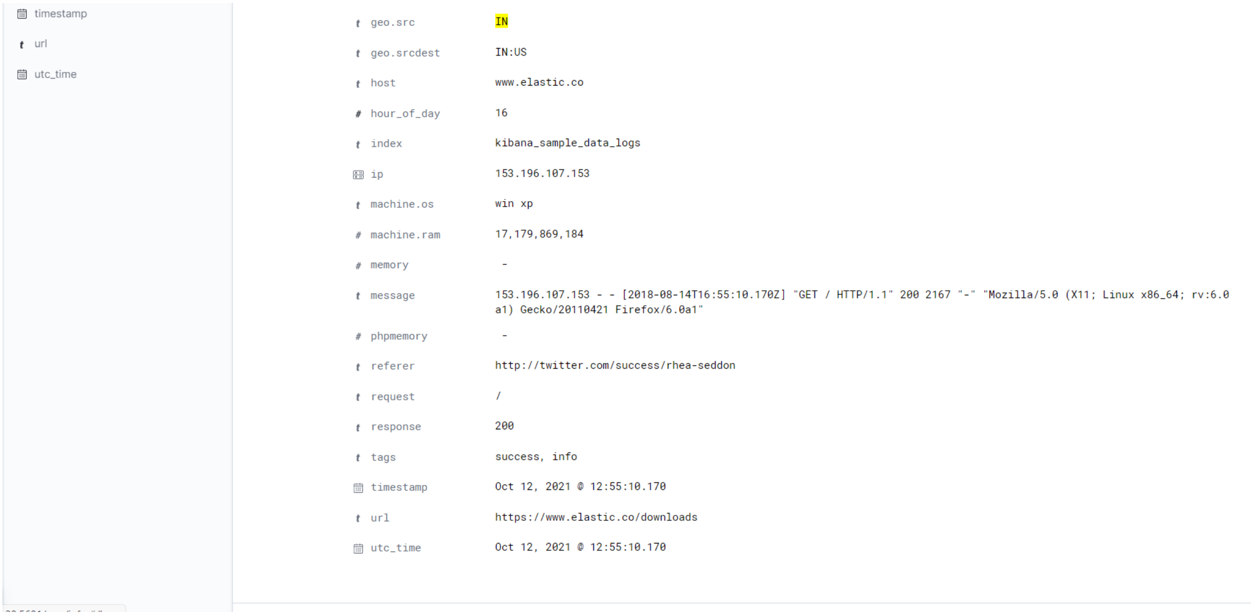
```
http://twitter.com/success/rhea-seddon
```

   -

6. 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 guidelines?

7.



geo.src	IN
geo.srcdest	IN:US
host	www.elastic.co
hour_of_day	16
index	kibana_sample_data_logs
ip	153.196.107.153
machine.os	win xp
machine.ram	17,179,869,184
memory	-
message	153.196.107.153 - - [2018-08-14T16:55:10.170Z] "GET / HTTP/1.1" 200 2167 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1"
phpmemory	-
referer	http://twitter.com/success/rhea-seddon
request	/
response	200
tags	success, info
timestamp	Oct 12, 2021 @ 12:55:10.170
url	https://www.elastic.co/downloads
utc_time	Oct 12, 2021 @ 12:55:10.170