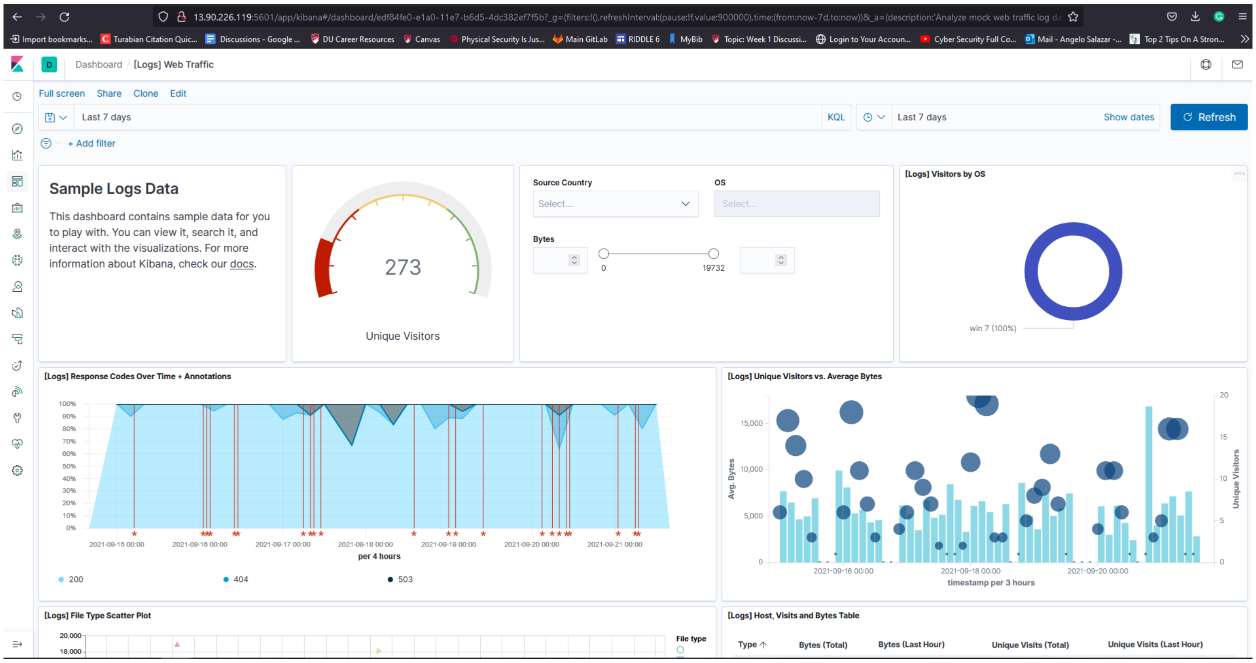
1. Source data is loaded.



13.90.226.119:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:900000),time:(from:now-7d,to:now))&_a=(description:'Analyze mock web traffic log da

Dashboard / [Logs] Web Traffic

Last 7 days

KQL | Last 7 days | Show dates | Refresh

+ Add filter

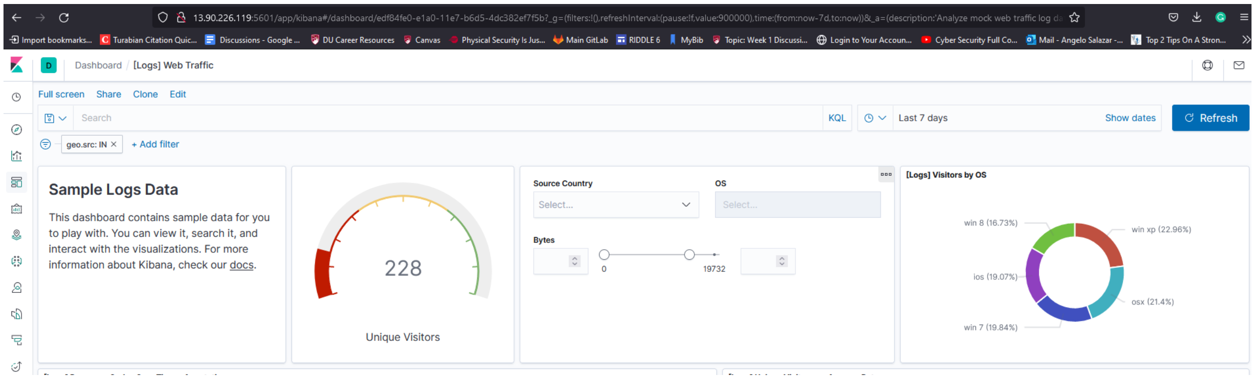
Sample Logs Data

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.

273

Unique Visitors

2. In the last 7 days, 228 unique visitors were located in India.



13.90.226.119:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:900000),time:(from:now-7d,to:now))&_a=(description:'Analyze mock web traffic log da

Dashboard / [Logs] Web Traffic

Search

KQL | Last 7 days | Show dates | Refresh

geo.src: IN ✕ | + Add filter

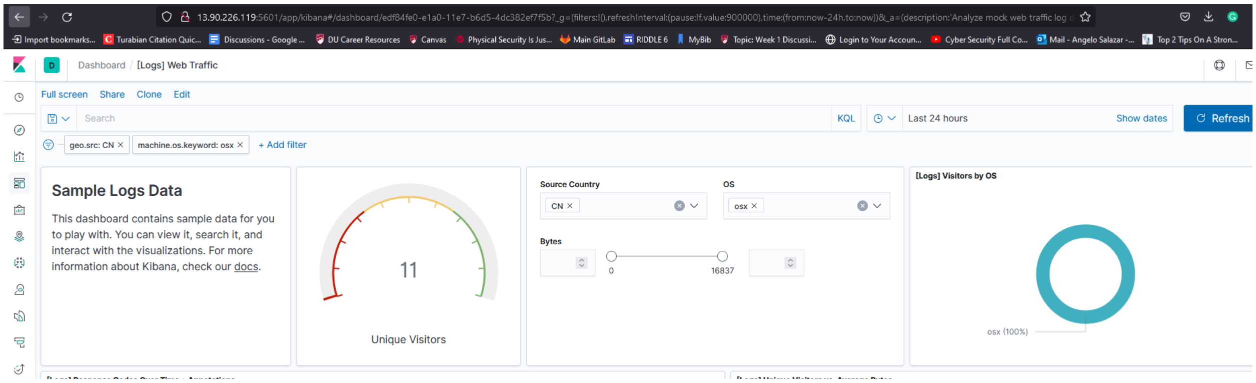
Sample Logs Data

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.

228

Unique Visitors

In the last 24 hours, 11 visitors from China were using Mac OSX.



13.90.226.119:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:900000),time:(from:now-24h,to:now))&_a=(description:'Analyze mock web traffic log d

Dashboard / [Logs] Web Traffic

Search

KQL | Last 24 hours | Show dates | Refresh

geo.src: CN ✕ | machine.os.keyword: osx ✕ | + 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.

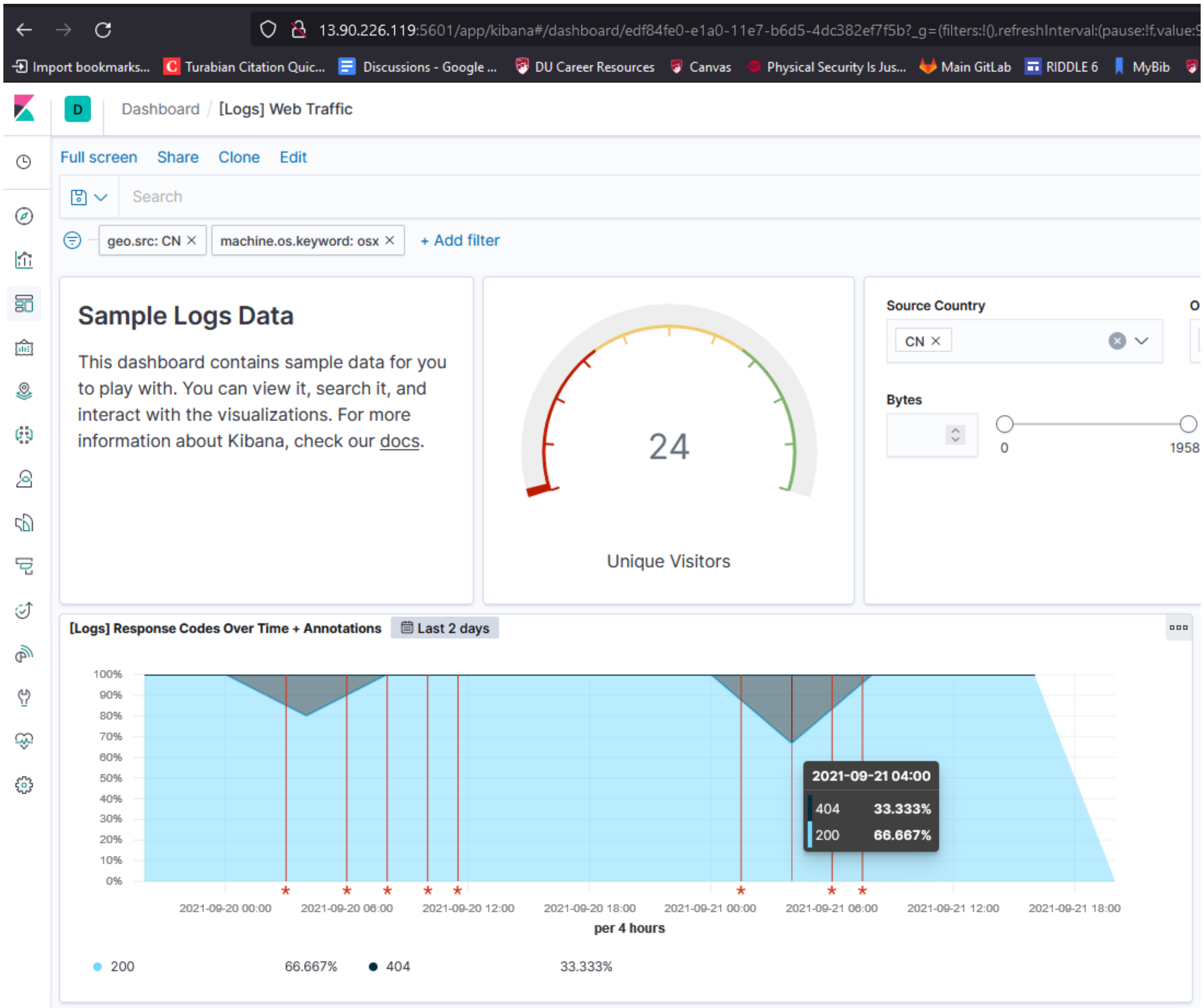
11

Unique Visitors

Source Country: CN ✕

OS: osx ✕

In the last two days, days, 33.33% of people got a 404 error and 0% of people got a 503 error.



13.90.226.119:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:!f,value:9

Dashboard / [Logs] Web Traffic

geo.src: CN ✕ machine.os.keyword: osx ✕ + 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.

24

Unique Visitors

Source Country: CN ✕

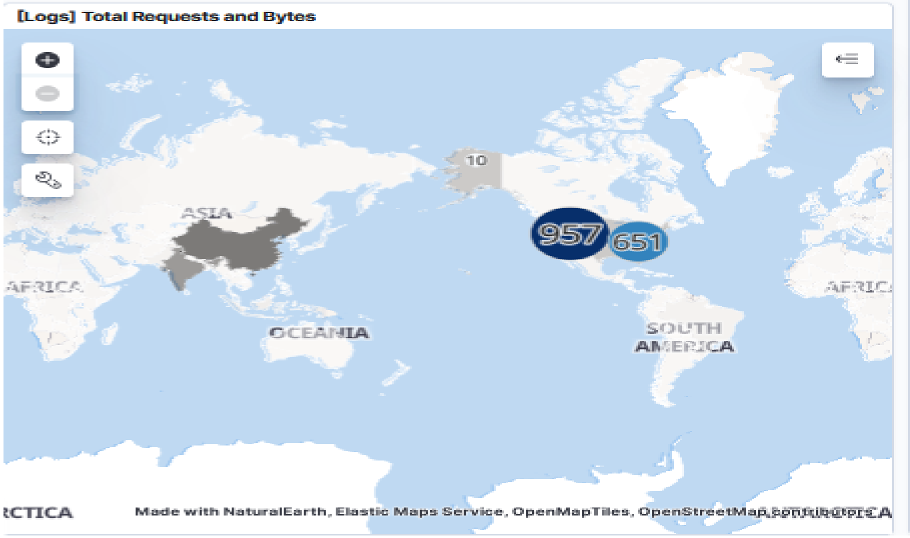
Bytes: 0 – 1958

[Logs] Response Codes Over Time + Annotations Last 2 days

2021-09-21 04:00
404 33.333%
200 66.667%

● 200 66.667% ● 404 33.333%

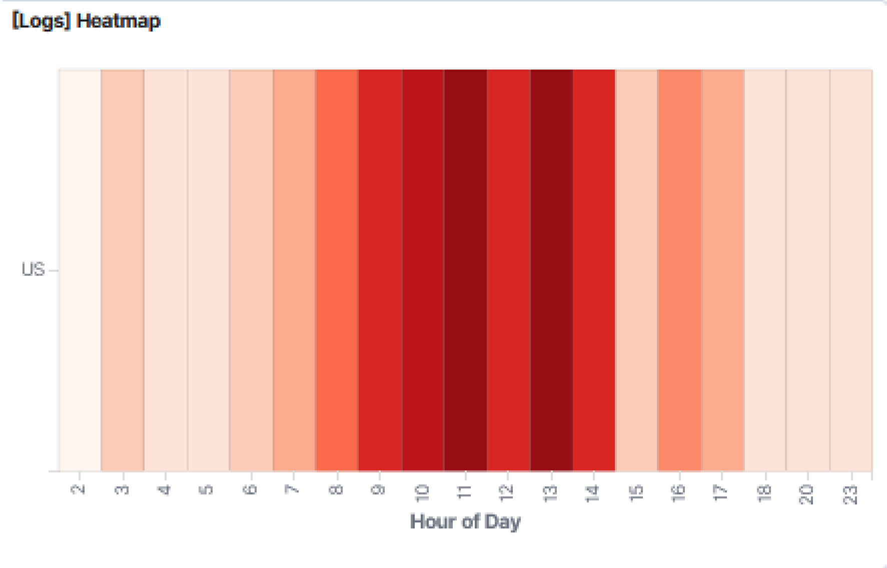
In the last 7 days, the country that produced a majority of the traffic was the U.S.



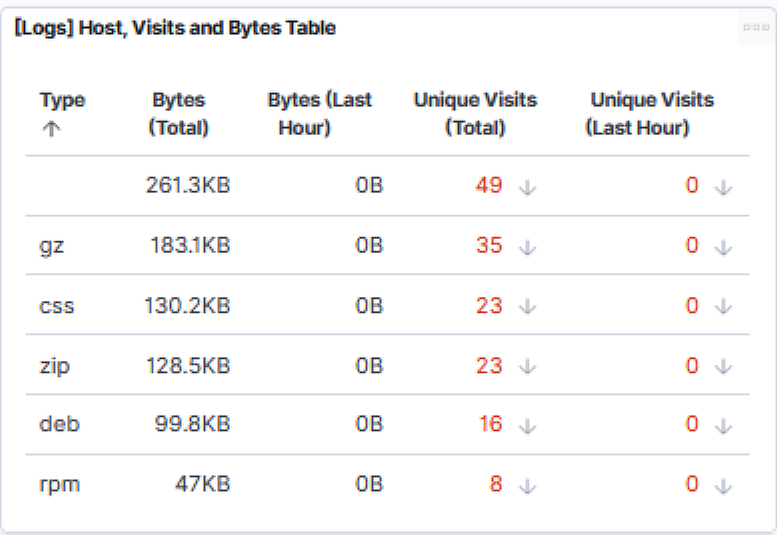
[Logs] Total Requests and Bytes

10
957
651
ASIA
AFRICA
OCEANIA
SOUTH AMERICA
AFRIC
ɹCTICA
Made with NaturalEarth, Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

From the U.S. the time of day with the most traffic was the 11th hou



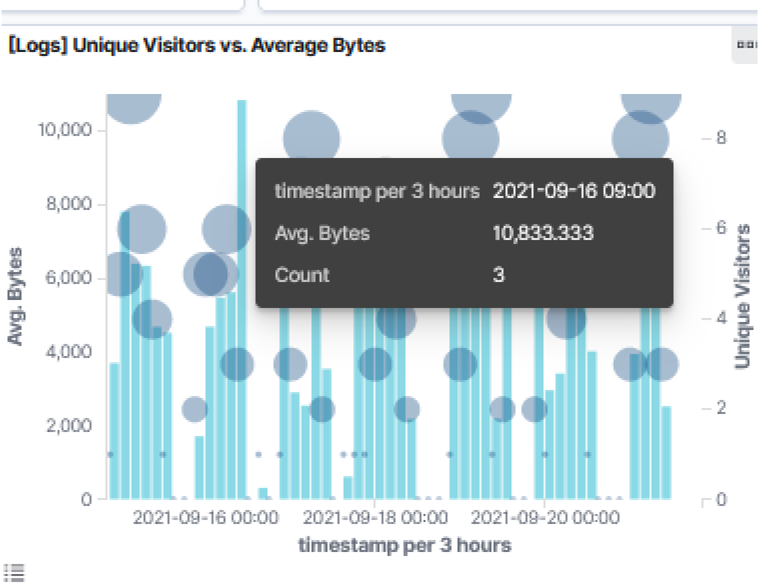
The file types are in the screenshot below.


[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	261.3KB	0B	49	0
gz	183.1KB	0B	35	0
css	130.2KB	0B	23	0
zip	128.5KB	0B	23	0
deb	99.8KB	0B	16	0
rpm	47KB	0B	8	0

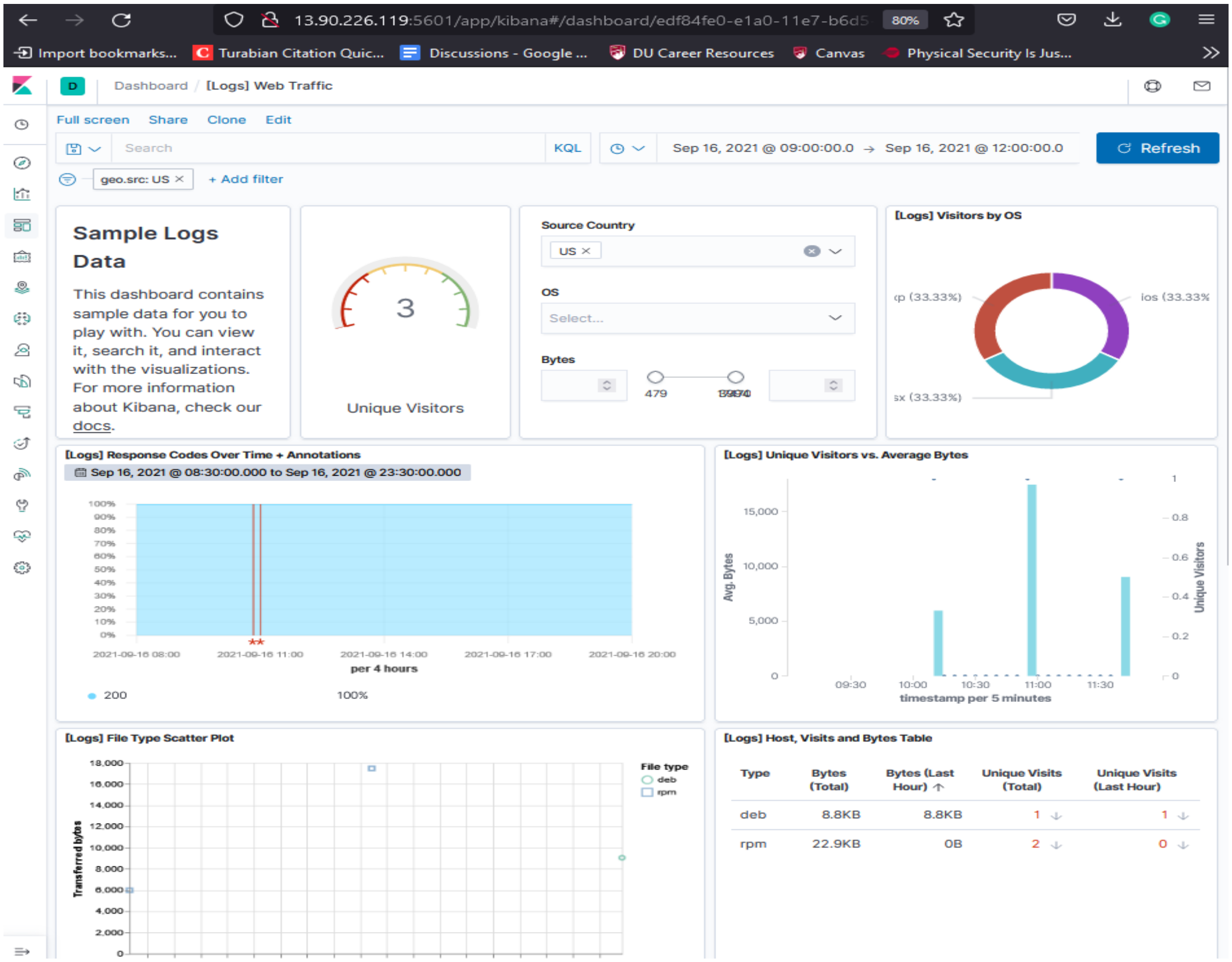
- gz file is
- css file is
- zip file is
- deb file is
- rpm file is

3. The time frame with the most amount of bytes was the 16th of September, 2021 at 9:00 p.m. with average bytes of 10,833.333. This is strange because the next closes average bytes was 8,795, while the average laid around 6,000.



[Logs] Unique Visitors vs. Average Bytes

4. The timestamp for this event was at 11:00 p.m. and was an rpm file. The average bytes for the event was 17,470 and happened in the U.S. The response code for this event was an HTTP 200 response code.



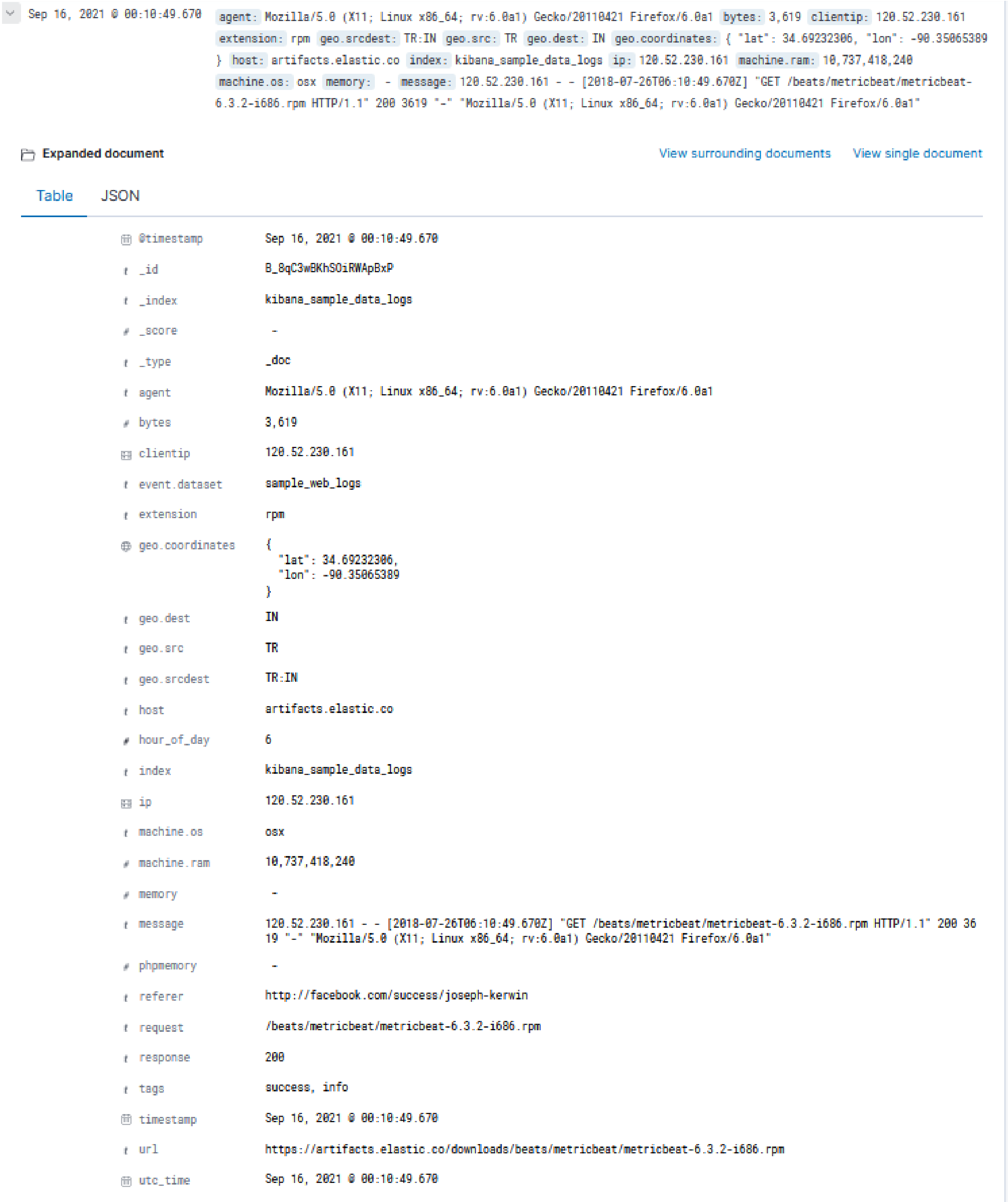
13.90.226.119:5601/app/kibana#/dashboard/edf84fe0-e1a0-11e7-b6d5
80%
Import bookmarks...
Turabian Citation Quic...
Discussions - Google ...
DU Career Resources
Canvas
Physical Security Is Jus...
D
Dashboard / [Logs] Web Traffic
Full screen
Share
Clone
Edit
Search
KQL
Sep 16, 2021 @ 09:00:00.0 → Sep 16, 2021 @ 12:00:00.0
Refresh
geo.src: US ×
+ 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.

Type	Bytes (Total)	Bytes (Last Hour) ↑	Unique Visits (Total)	Unique Visits (Last Hour)
deb	8.8KB	8.8KB	1 ↓	1 ↓
rpm	22.9KB	0B	2 ↓	0 ↓

5. The source IP is 120.52.230.161. The GEO coordinates are "lat": 34.69232306, "lon": -90.35065389. The OS on the source machine was Max OSX. The URL requested was https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm. The website that the traffic originated from was http://facebook.com/success/joseph-kerwin.



Sep 16, 2021 @ 00:10:49.670 agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 bytes: 3,619 clientip: 120.52.230.161 extension: rpm geo.srcdest: TR:IN geo.src: TR geo.dest: IN geo.coordinates: { "lat": 34.69232306, "lon": -90.35065389 } host: artifacts.elastic.co index: kibana_sample_data_logs ip: 120.52.230.161 machine.ram: 10,737,418,240 machine.os: osx memory: - message: 120.52.230.161 - - [2018-07-26T06:10:49.670Z] "GET /beats/metricbeat/metricbeat-6.3.2-i686.rpm HTTP/1.1" 200 3619 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1"

Expanded document

@timestamp	Sep 16, 2021 @ 00:10:49.670
_id	B_8qC3wBKhSOiRWApBxP
_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	3,619
clientip	120.52.230.161
event.dataset	sample_web_logs
extension	rpm

geo.coordinates	{
	"lat": 34.69232306,
	"lon": -90.35065389
	}

geo.dest	IN
geo.src	TR
geo.srcdest	TR:IN
host	artifacts.elastic.co
hour_of_day	6
index	kibana_sample_data_logs
ip	120.52.230.161
machine.os	osx
machine.ram	10,737,418,240
memory	-
message	120.52.230.161 - - [2018-07-26T06:10:49.670Z] "GET /beats/metricbeat/metricbeat-6.3.2-i686.rpm HTTP/1.1" 200 3619 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1"
phpmemory	-
referer	http://facebook.com/success/joseph-kerwin
request	/beats/metricbeat/metricbeat-6.3.2-i686.rpm
response	200
tags	success, info
timestamp	Sep 16, 2021 @ 00:10:49.670
url	https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm
utc_time	Sep 16, 2021 @ 00:10:49.670

6. At the time, the user was trying to authenticate to the social media platform Facebook. But, he fell victim to a URL hijacking scheme because it was http://facebook.com instead of https://facebook.com.The file, filebeat can be used to forward logs to the attacker’s computer. The thing that seemed suspicious was the malicious redirect from the social media platform, Facebook to install metricbeat.