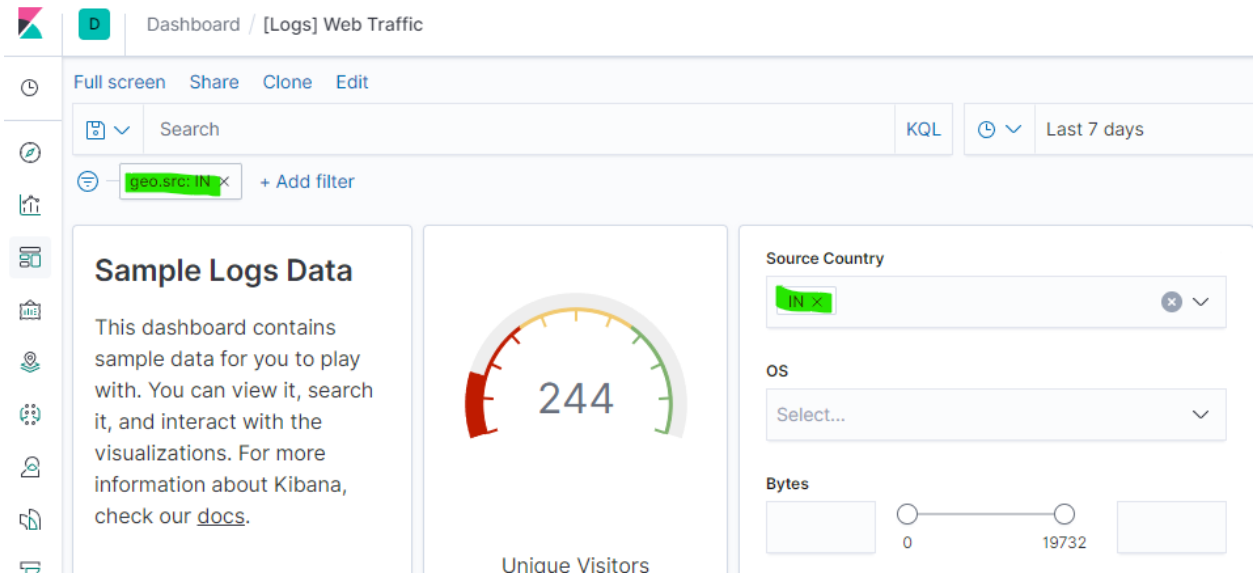
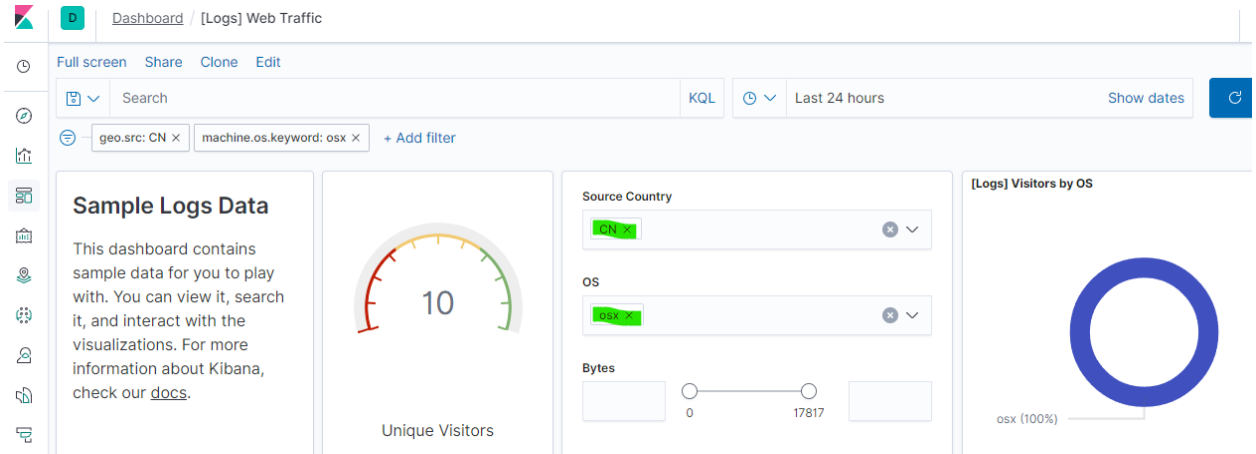
Sample Weblog Data

Once I Installed the Kibana I started to explore and investigate some of the data. I Add the sample web log data to Kibana. Here we are providing visualization in the form of a heat map, breaking down the hours of a day, geo-IP addressing for the total number of requests and bytes, and finally geo-IP source and destination. Below some of the data analyzed

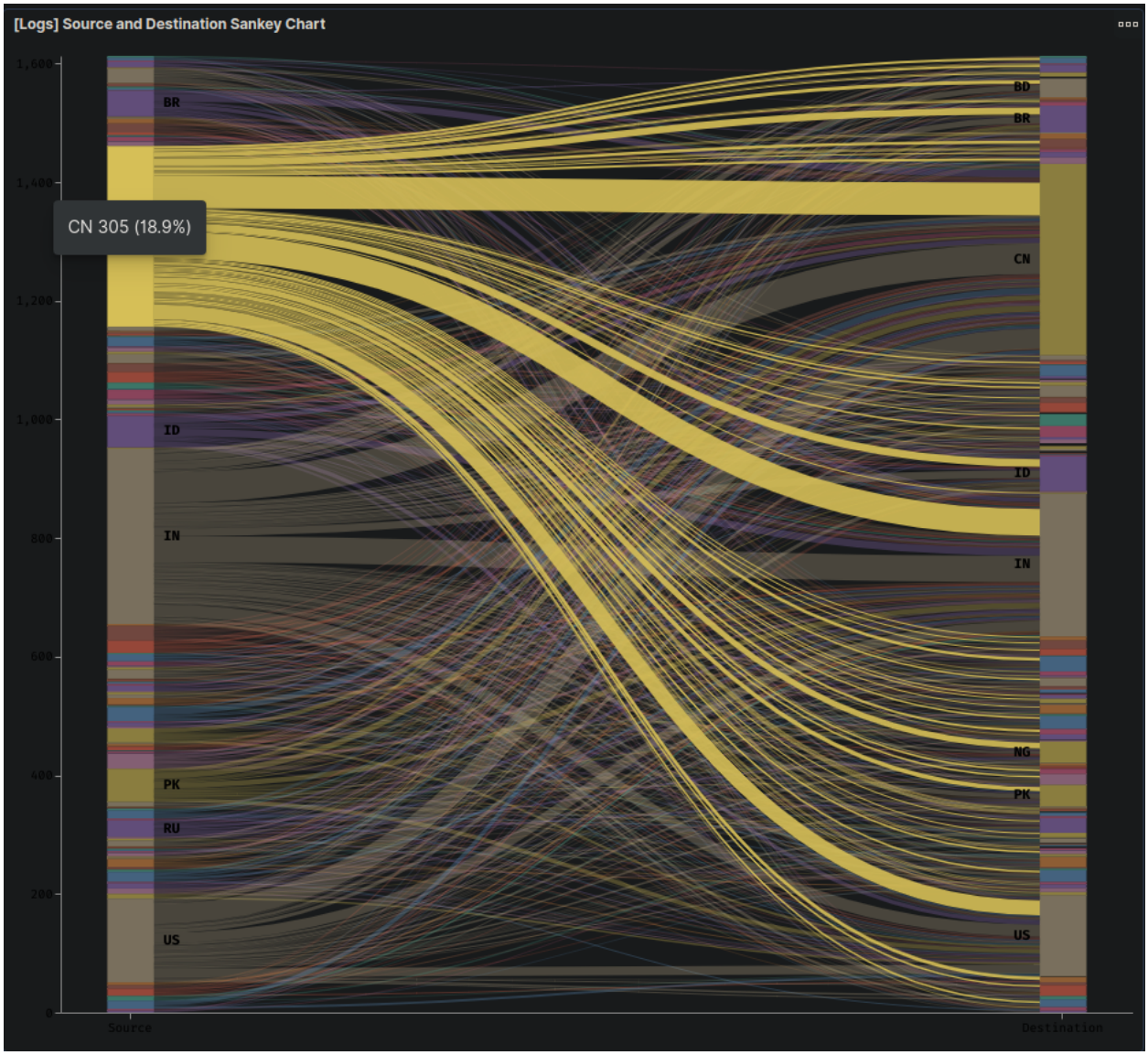
- Sample data I query about last 7 days, how many unique visitors were located in India so it os 244



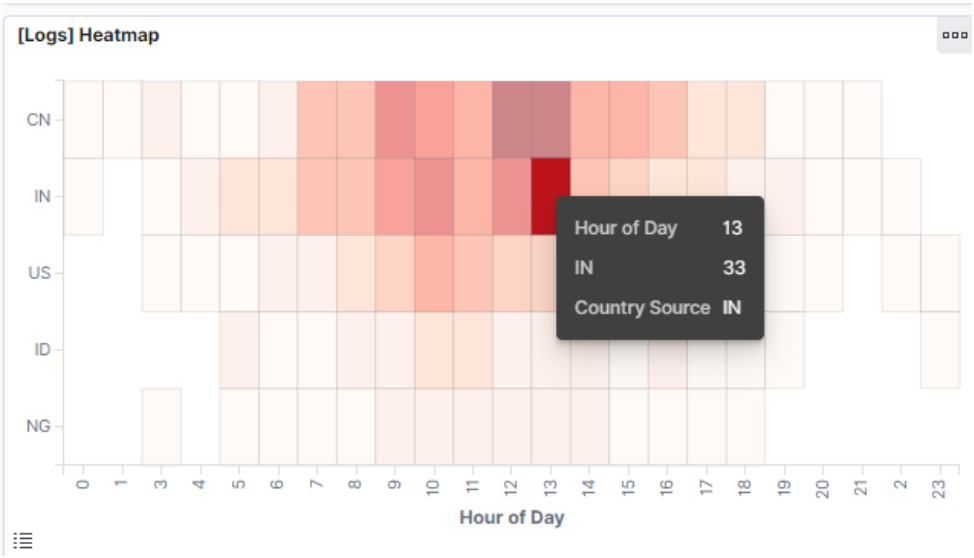
- In the last 24 hours, the visitors from China is 10



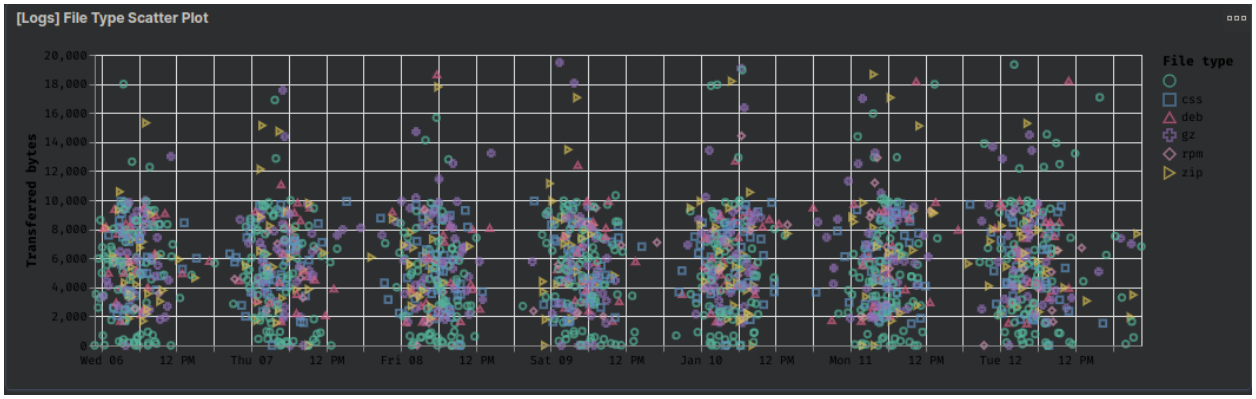
- In the last 7 days, China produced the majority of the traffic on the website



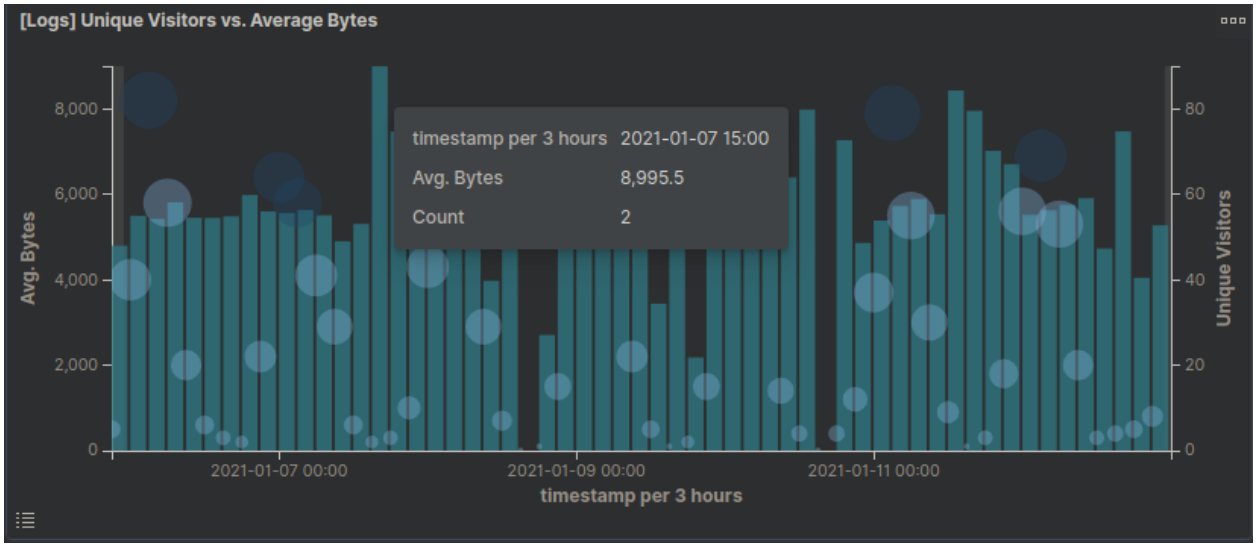
- Of the traffic that's coming from that country, what time of day had the highest amount of activity? It is 1 PM



- 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).
  - `css` - this is a programming language usually used for writing webpage elements and design
  - `deb` - compressed Linux software package, used by debian-based distros like ubuntu
  - `gz` - compressed archive using the gzip compression algorithm
  - `rpm` - similar to `deb` files, these are compressed linux software packages used in Red Hat Enterprise based distributions
  - `zip` - compressed archive similar to tarball or `gz` archive



- 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).
    - Avg Bytes: ~9,000B
    - Unique Visitors: 2

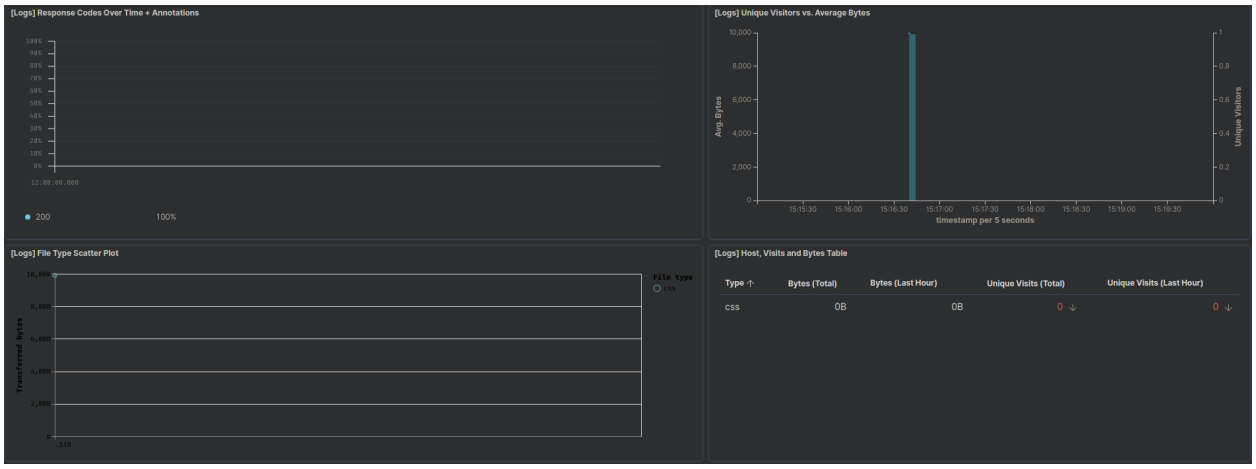


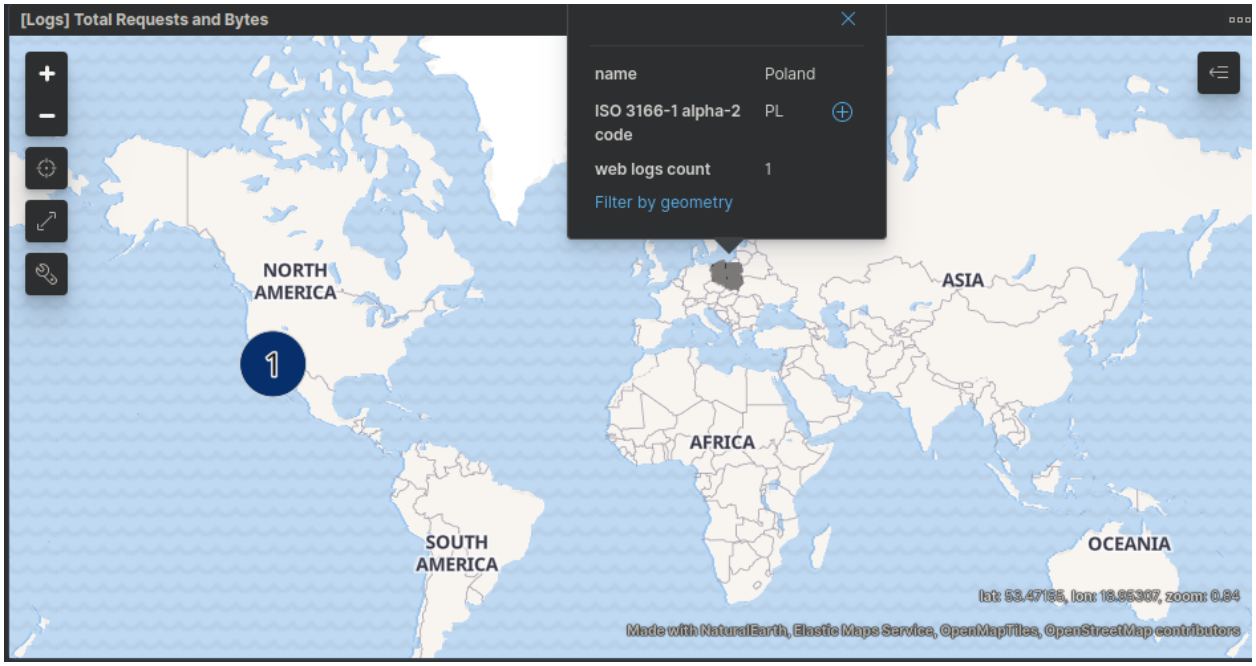
❖ Filter the data by this event.

- What is the timestamp for this event?
  - Timestamp: 2021-01-07 15:16:40

- What kind of file was downloaded?
  - css
  -
- From what country did this activity originate?
  - Poland

- 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?
  - 159.148.160.139

- What are the geo-coordinates of this activity?
  - lat: 32.83422028
  - lon: -115.5787456

- What OS was the source machine running?
  - Windows XP

- What is the full URL that was accessed?
  - https://cdn.elastic-elastic-elastic.org/styles/pretty-layout.css

- From what website did the visitor's traffic originate?
  - http://www.elastic-elastic-elastic.com/warning/alexander-poleshchuk

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

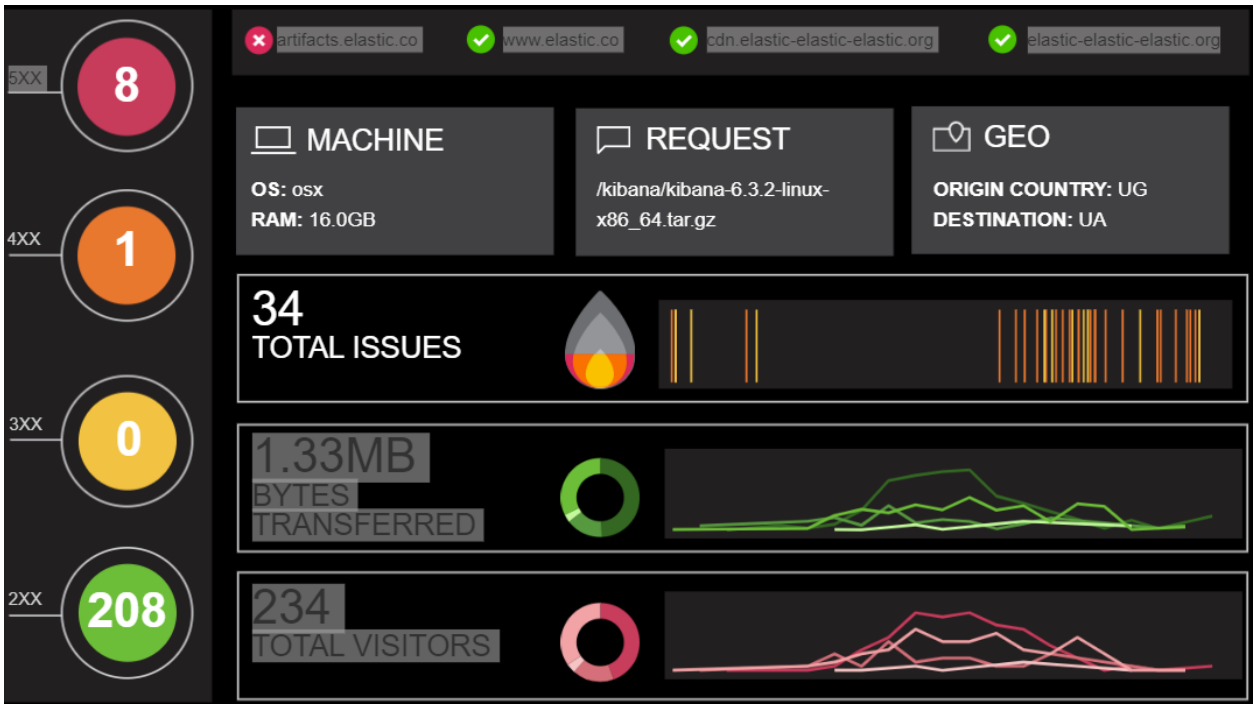
- What do you think the user was doing?
  - Downloading a CSS layout, specifically a "pretty" one.

- Was the file they downloaded malicious? If not, what is the file used for?
  - Likely it is not malicious, it is a stylesheet or layout for a webpage element. This is used for aesthetics and themes.

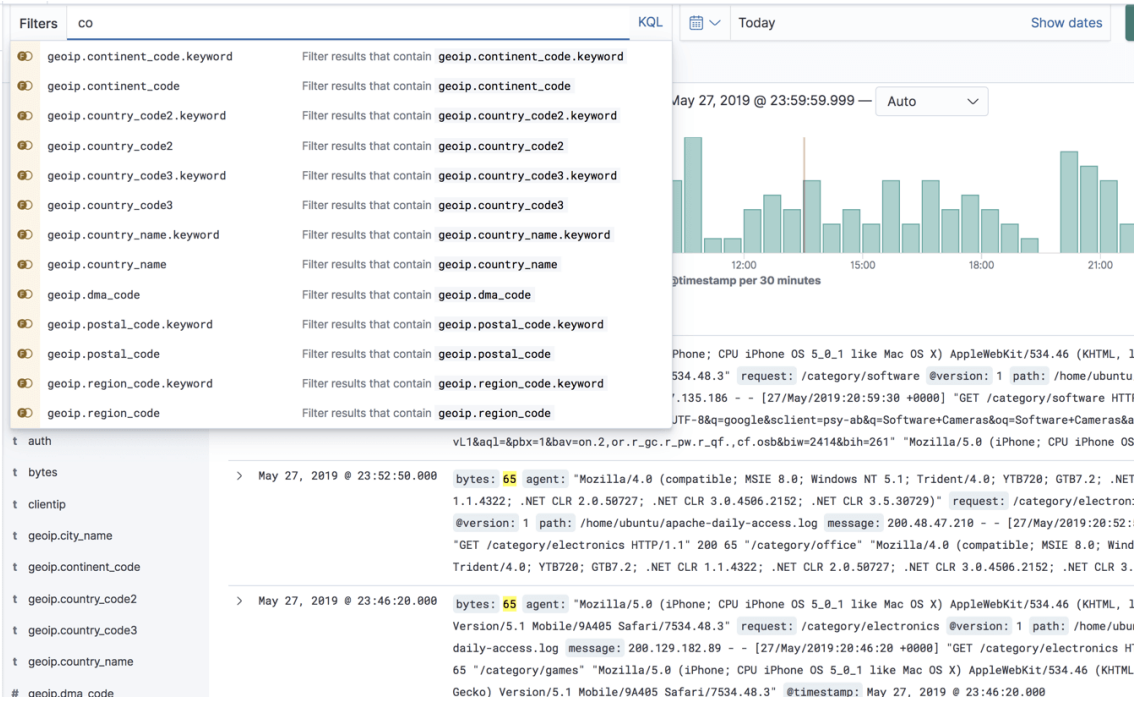
- Is there anything that seems suspicious about this activity?
  - Not particularly without seeing the actual file itself. This would be considered a normal action when visiting a webpage.

- Is any of the traffic you inspected potentially outside of compliance guidelines?
  - Unless there is a data download or bandwidth cap of some sort, this looks like it falls within normal user behavior.

Testing some of the Web Log data in canvas mode December 15 to December 17



To improve the search experience in Kibana, the autocomplete feature suggests search syntax as enter the query. As a type, relevant fields are displayed. It will speed up the process in a simple method .


Filters
co
KQL
Today
Show dates
geoip.continent_code.keyword Filter results that contain geoip.continent_code.keyword
geoip.continent_code Filter results that contain geoip.continent_code
geoip.country_code2.keyword Filter results that contain geoip.country_code2.keyword
geoip.country_code2 Filter results that contain geoip.country_code2
geoip.country_code3.keyword Filter results that contain geoip.country_code3.keyword
geoip.country_code3 Filter results that contain geoip.country_code3
geoip.country_name.keyword Filter results that contain geoip.country_name.keyword
geoip.country_name Filter results that contain geoip.country_name
geoip.dma_code Filter results that contain geoip.dma_code
geoip.postal_code.keyword Filter results that contain geoip.postal_code.keyword
geoip.postal_code Filter results that contain geoip.postal_code
geoip.region_code.keyword Filter results that contain geoip.region_code.keyword
geoip.region_code Filter results that contain geoip.region_code
May 27, 2019 @ 23:59:59.999 —
Auto
12:00
15:00
18:00
21:00
@timestamp per 30 minutes
t auth
t bytes
t clientip
t geoip.city_name
t geoip.continent_code
t geoip.country_code2
t geoip.country_code3
t geoip.country_name
geoip.dma_code
May 27, 2019 @ 23:52:50.000
May 27, 2019 @ 23:46:20.000

Sample eCommerce orders

I add the sample e-commerce data and investigate some of the function

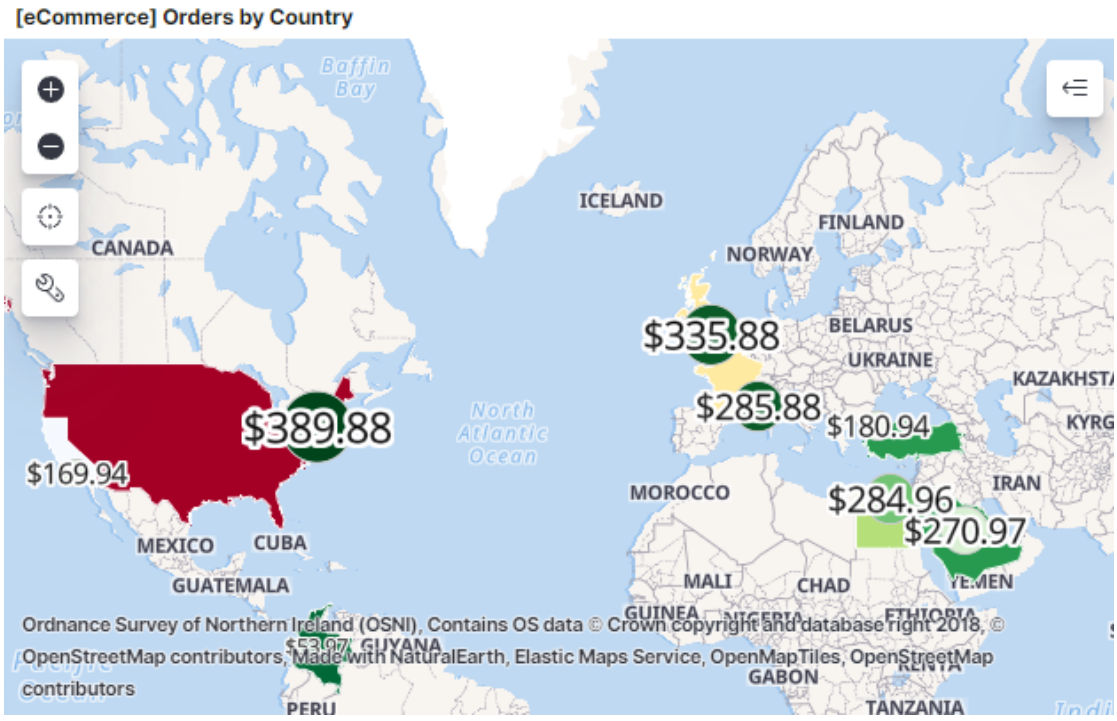
This is just showing the complete order details.

[eCommerce] Orders

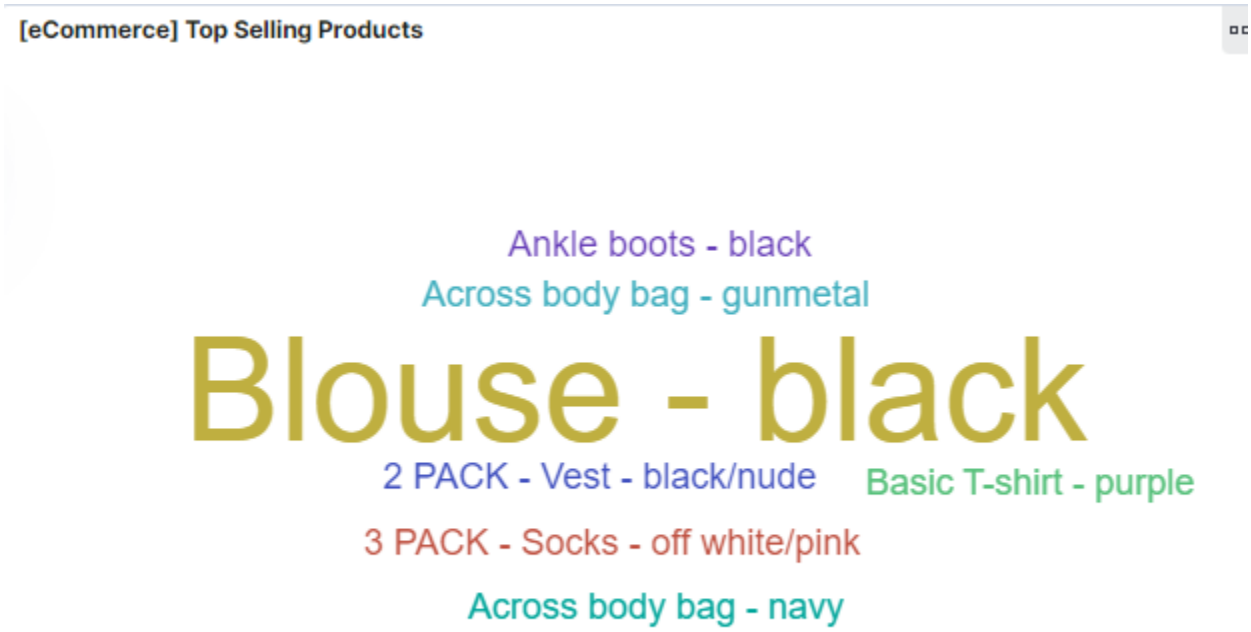
1–31 of 31

Time	category	sku	taxful_total_price	total_quantity
Dec 13, 2021 @ 05:19:12.000	Women's Clothing	ZO0266102661, ZO0169701697	$50.98	2
Dec 13, 2021 @ 05:17:46.000	Men's Clothing, Women's Accessories	ZO0423004230, ZO0292702927, ZO0320003200, ZO0318303183	$90.96	4
Dec 13, 2021 @ 05:14:53.000	Women's Accessories, Men's Clothing	ZO0466104661, ZO0444104441	$60.98	2
Dec 13, 2021 @ 04:56:10.000	Men's Clothing	ZO0125401254, ZO0123701237	$61.98	2
Dec 13, 2021 @ 04:27:22.000	Men's Clothing	ZO0417504175, ZO0535205352	$45.98	2
Dec 13, 2021 @ 04:05:46.000	Women's Clothing, Women's Accessories	ZO0343703437, ZO0207102071	$53.98	2
Dec 13, 2021 @ 03:51:22.000	Women's Clothing	ZO0215702157, ZO0638806388	$15.98	2
Dec 13, 2021 @ 03:39:50.000	Women's Shoes, Women's Clothing	ZO0031700317, ZO0157701577	$26.98	2
Dec 13, 2021 @ 03:32:38.000	Men's Clothing, Men's Shoes	ZO0557905579, ZO0513705137	$33.98	2
Dec 13, 2021 @ 03:28:19.000	Women's Accessories, Women's Clothing	ZO0306803068, ZO0174601746	$74.98	2

This shows the country based money value that people ordered



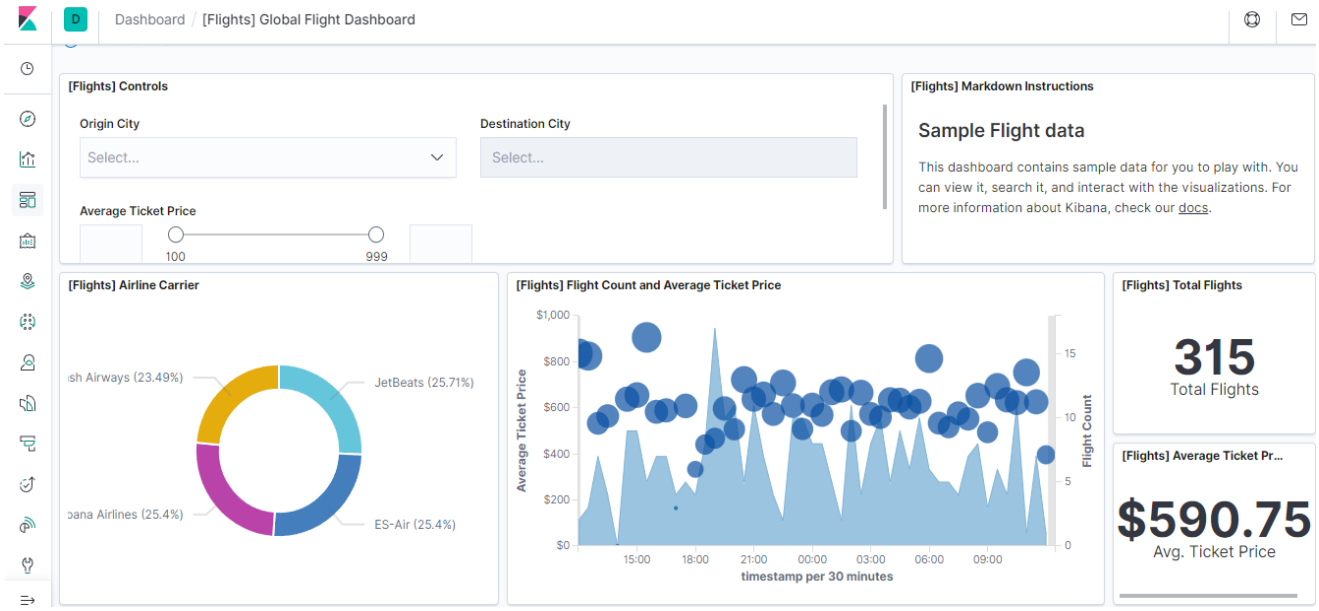
Analyse Data of top-selling products worldwide



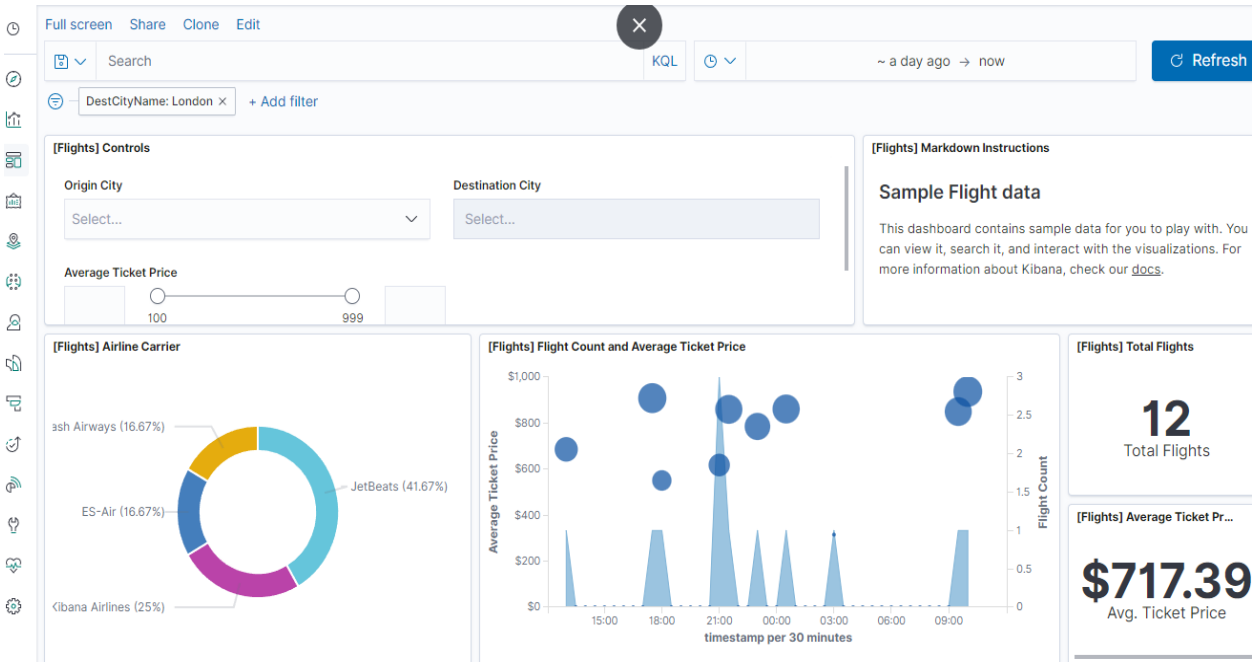
Through this data, we can get the eCommerce Total revenue and the Sales Category

Sample Flight Data

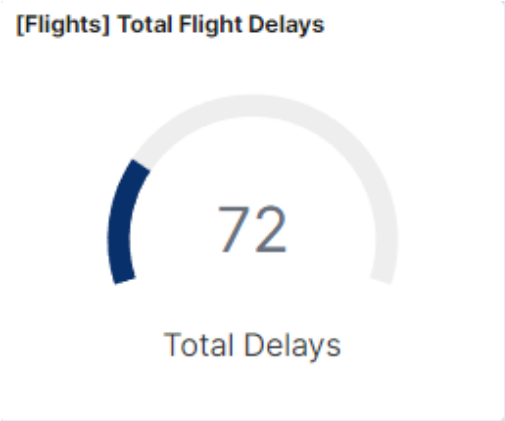
This Sample flight Data shows clearly what are airline carriers and how many total flights etc.

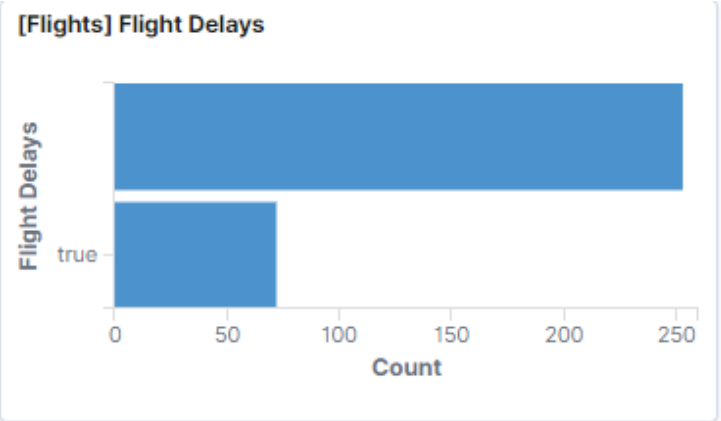


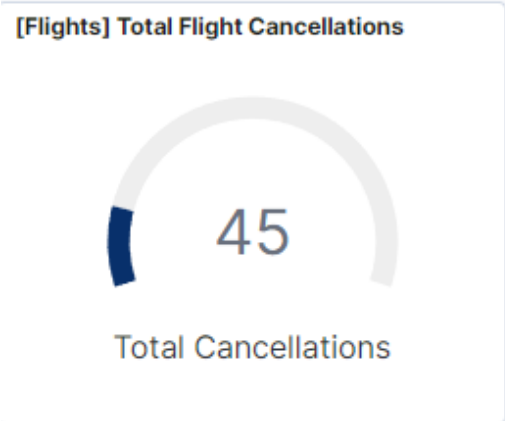
To pull data about London Dashboard display the data with total flight, Average cost, etc.

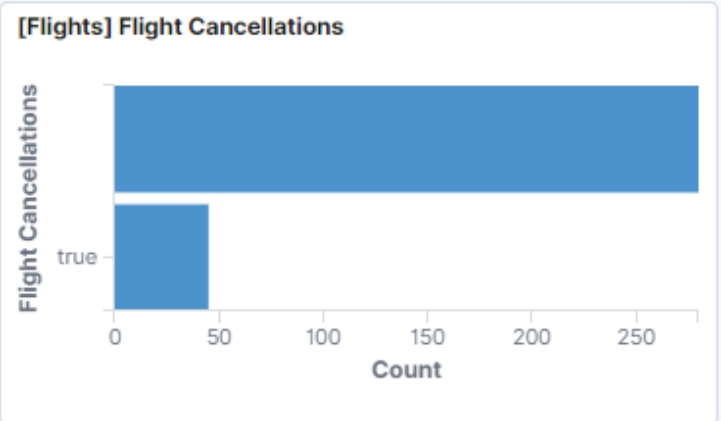


This Data in 24 Hours how many flight delays and canceled



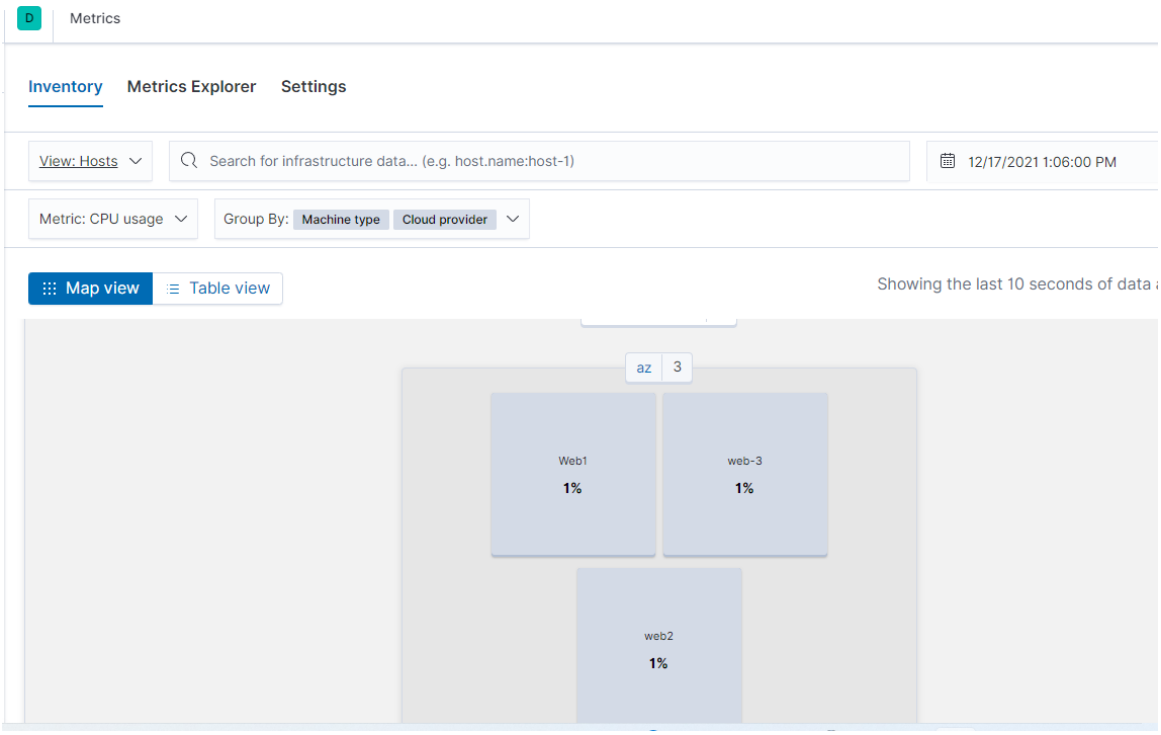




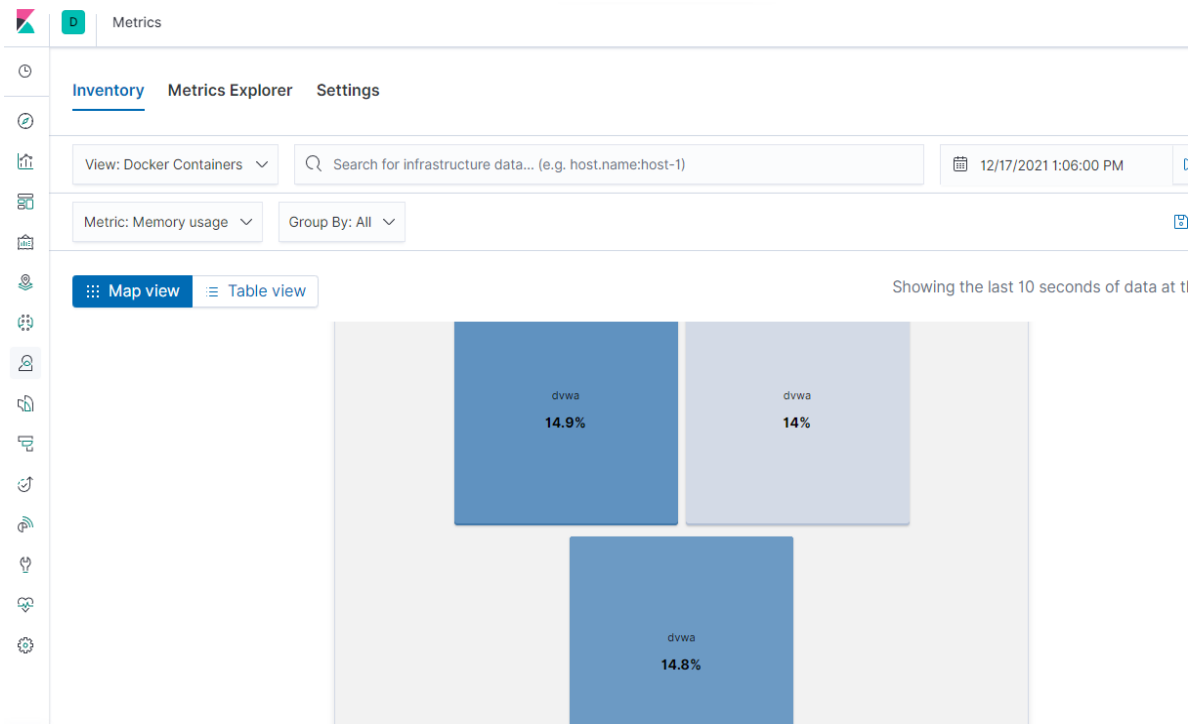


Metric beat

The web servers CPU usage



This shows the dvwa containers memory usage


Metrics
Inventory
Metrics Explorer
Settings
View: Docker Containers
Search for infrastructure data... (e.g. host.name:host-1)
12/17/2021 1:06:00 PM
Metric: Memory usage
Group By: All
Map view
Table view
Showing the last 10 seconds of data at t
dvwa
14.9%
dvwa
14%
dvwa
14.8%