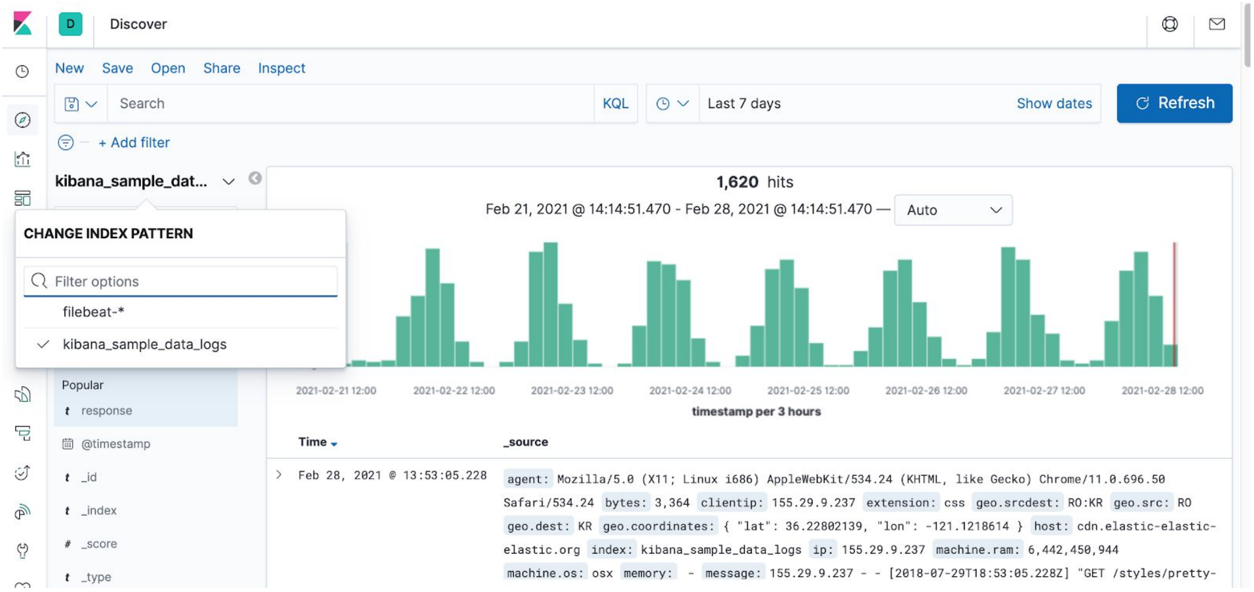
Instructions

1. **Add the sample web log data to Kibana.**

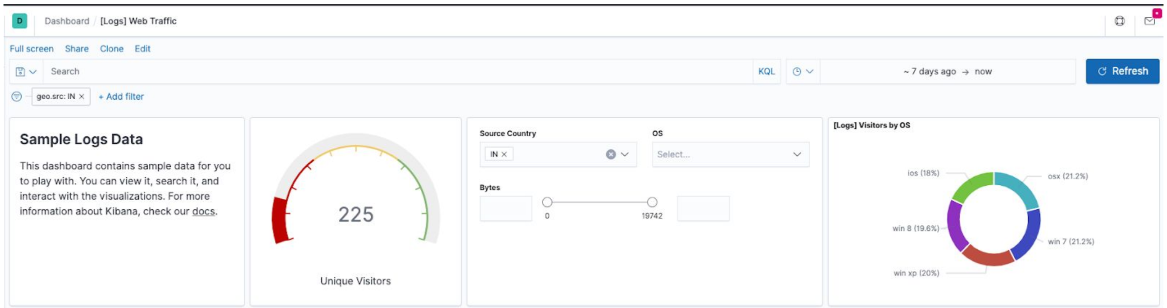


```
Feb 28, 2021 @ 13:53:05.228   agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50
                              Safari/534.24 bytes: 3,364 clientip: 155.29.9.237 extension: css geo.srcdest: RO:KR geo.src: RO
                              geo.dest: KR geo.coordinates: { "lat": 36.22802139, "lon": -121.1218614 } host: cdn.elastic-elastic-
                              elastic.org index: kibana_sample_data_logs ip: 155.29.9.237 machine.ram: 6,442,450,944
                              machine.os: osx memory:  - message: 155.29.9.237 - - [2018-07-29T18:53:05.228Z] "GET /styles/pretty-
```

2. **Answer the following questions:**

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

     225 uniques visitors

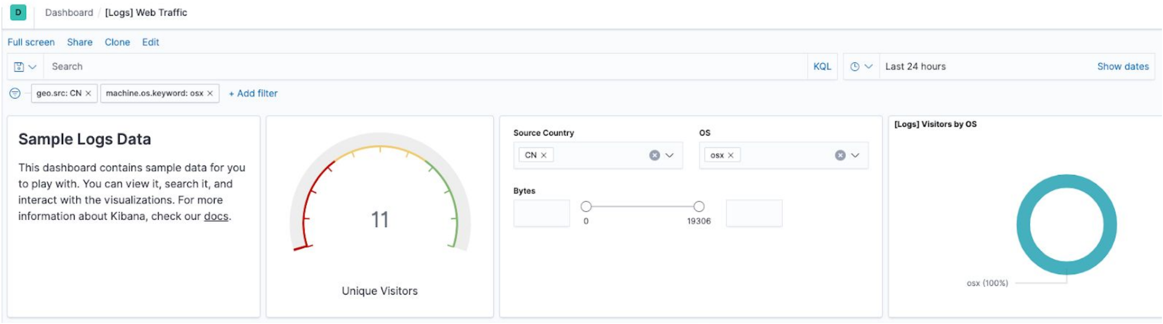


Sample Logs Data

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?**

11 visitors were using Mac OSX

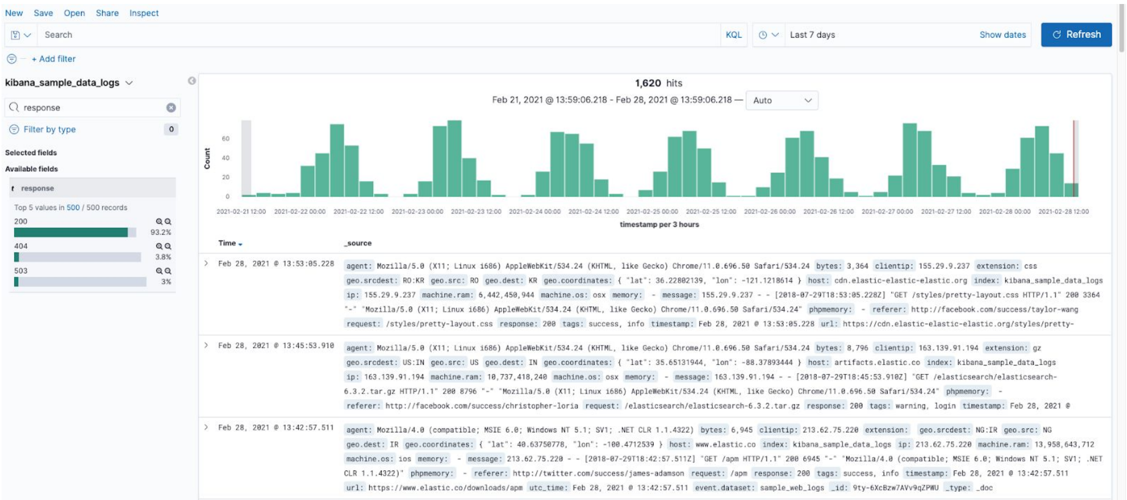


Sample Logs Data

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.

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

  Percentage of visitors who received 404 errors = 3.8%
  Percentage of visitors who received 503 errors = 3%

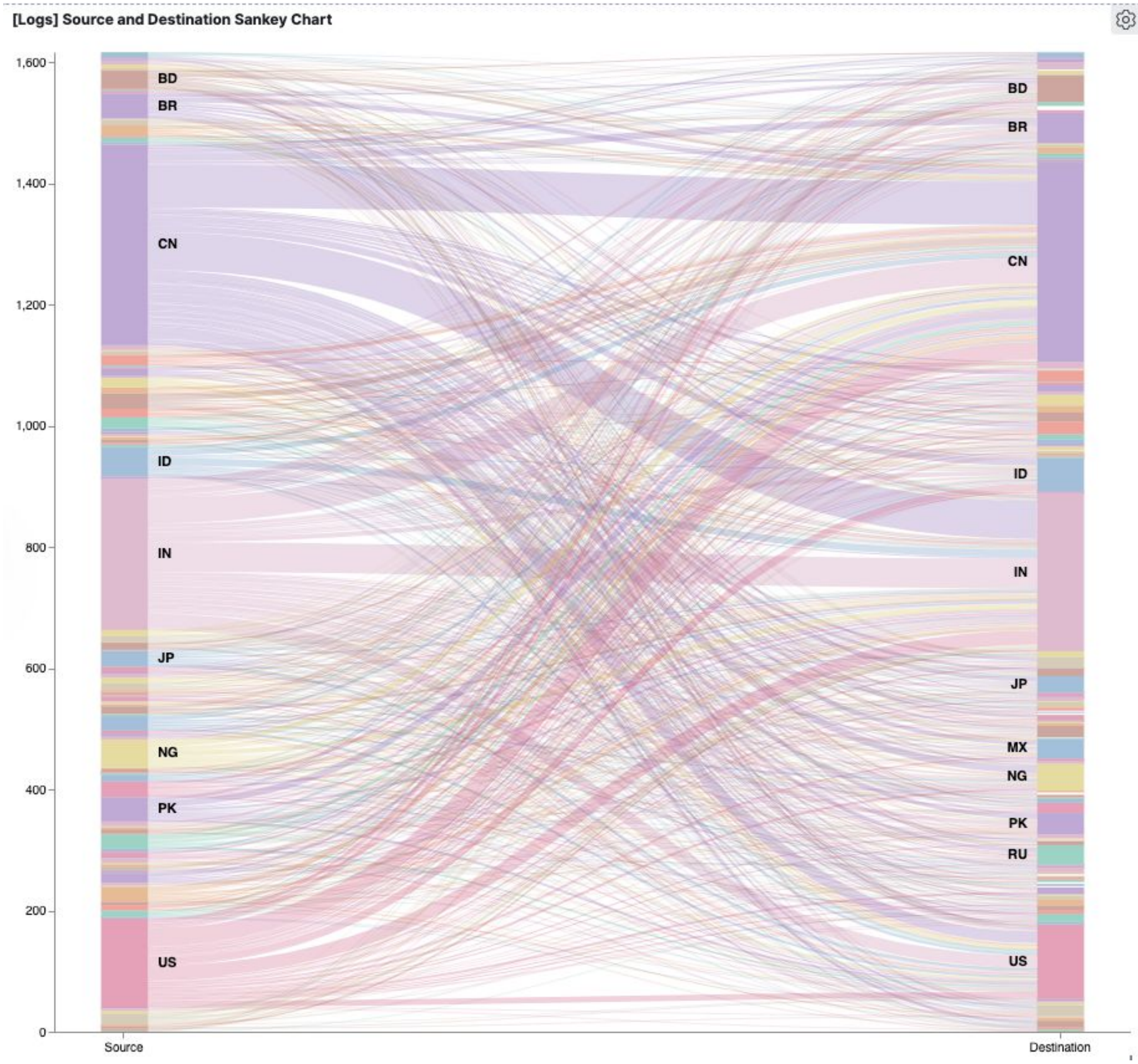


Top 5 values in 500 / 500 records

200	93.2%
404	3.8%
503	3%

```
> Feb 28, 2021 @ 13:53:05.228  agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 bytes: 3,364 clientip: 155.29.9.237 extension: css
    geo.srcdest: RO:KR geo.src: RO geo.dest: KR geo.coordinates: { "lat": 36.22802139, "lon": -121.1218614 } host: cdn.elastic-elastic-elastic.org index: kibana_sample_data_logs
    ip: 155.29.9.237 machine.ram: 6,442,450,944 machine.os: osx memory: - message: 155.29.9.237 - - [2018-07-29T18:53:05.228Z] "GET /styles/pretty-layout.css HTTP/1.1" 200 3364
    "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24" phpmemory: - referer: http://facebook.com/success/taylor-wang
    request: /styles/pretty-layout.css response: 200 tags: success, info timestamp: Feb 28, 2021 @ 13:53:05.228 url: https://cdn.elastic-elastic-elastic.org/styles/pretty-

> Feb 28, 2021 @ 13:45:53.910  agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 bytes: 8,796 clientip: 163.139.91.194 extension: gz
    geo.srcdest: US:IN geo.src: US geo.dest: IN geo.coordinates: { "lat": 35.65131944, "lon": -88.37893444 } host: artifacts.elastic.co index: kibana_sample_data_logs
    ip: 163.139.91.194 machine.ram: 10,737,418,240 machine.os: osx memory: - message: 163.139.91.194 - - [2018-07-29T18:45:53.910Z] "GET /elasticsearch/elasticsearch-
    6.3.2.tar.gz HTTP/1.1" 200 8796 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24" phpmemory: -
    referer: http://facebook.com/success/christopher-loria request: /elasticsearch/elasticsearch-6.3.2.tar.gz response: 200 tags: warning, login timestamp: Feb 28, 2021 @

> Feb 28, 2021 @ 13:42:57.511  agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) bytes: 6,945 clientip: 213.62.75.220 extension:  geo.srcdest: NG:IR geo.src: NG
    geo.dest: IR geo.coordinates: { "lat": 40.63750778, "lon": -100.4712539 } host: www.elastic.co index: kibana_sample_data_logs ip: 213.62.75.220 machine.ram: 13,958,643,712
    machine.os: ios memory: - message: 213.62.75.220 - - [2018-07-29T18:42:57.511Z] "GET /apm HTTP/1.1" 200 6945 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET
    CLR 1.1.4322)" phpmemory: - referer: http://twitter.com/success/james-adamson request: /apm response: 200 tags: success, info timestamp: Feb 28, 2021 @ 13:42:57.511
    url: https://www.elastic.co/downloads/apm utc_time: Feb 28, 2021 @ 13:42:57.511 event.dataset: sample_web_logs _id: 9ty-6XcBzw7AVv9qZPWU _type: _doc
```

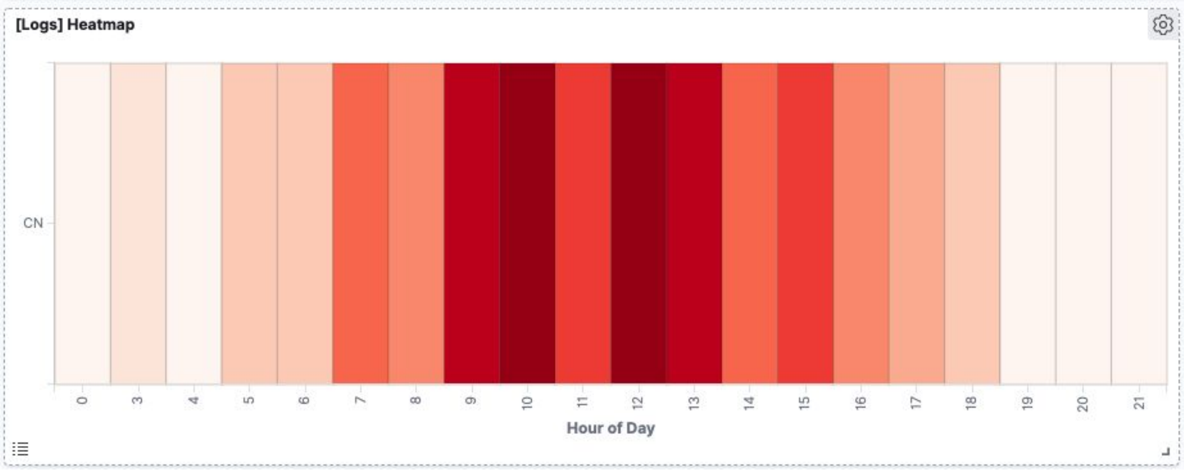
- **In the last 7 days, what country produced the majority of the traffic on the website?**
  China (CN) - 20.4



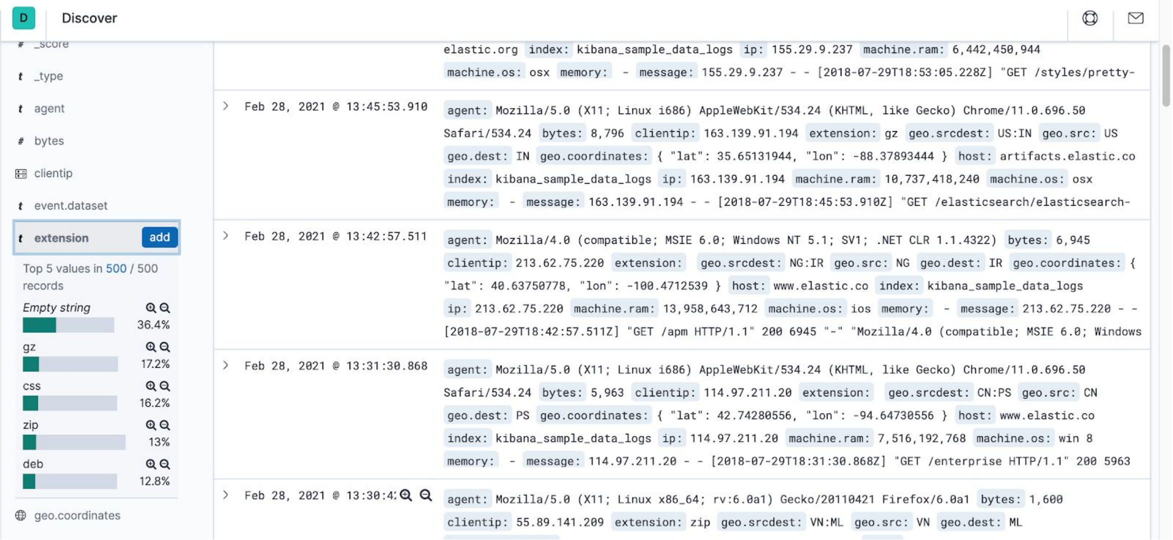
[Logs] Source and Destination Sankey Chart

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

At 10 and 12 hour of the day.



- **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).**
    1. gz - compressed archive file with standard GNU zip (gzip) algorithm
    2. css - file used to format the contents of a webpage. ... CSS files can define the size, color, font, line spacing, indentation, borders, and location of HTML elements
    3. zip - archive file format that's used to compress one or more files together into a single location, reducing the overall size, and making it easier to transport the files
    4. deb - deb is the format, as well as extension of the software package format for the Linux distribution Debian and its derivatives.



Top 5 values in 500 / 500 records

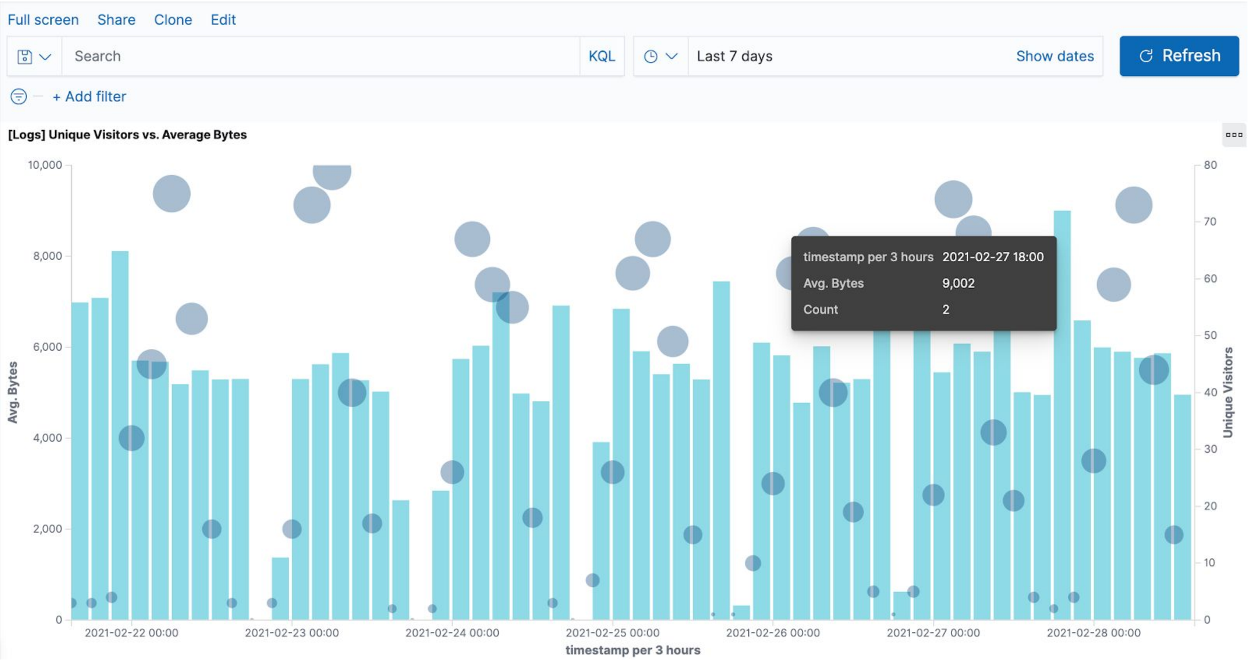
Empty string	36.4%
gz	17.2%
css	16.2%
zip	13%
deb	12.8%

```
elastic.org index: kibana_sample_data_logs ip: 155.29.9.237 machine.ram: 6,442,450,944
machine.os: osx memory: - message: 155.29.9.237 - - [2018-07-29T18:53:05.228Z] "GET /styles/pretty-

> Feb 28, 2021 @ 13:45:53.910  agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50
Safari/534.24 bytes: 8,796 clientip: 163.139.91.194 extension: gz geo.srcdest: US:IN geo.src: US
geo.dest: IN geo.coordinates: { "lat": 35.65131944, "lon": -88.37893444 } host: artifacts.elastic.co
index: kibana_sample_data_logs ip: 163.139.91.194 machine.ram: 10,737,418,240 machine.os: osx
memory: - message: 163.139.91.194 - - [2018-07-29T18:45:53.910Z] "GET /elasticsearch/elasticsearch-

> Feb 28, 2021 @ 13:42:57.511  agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) bytes: 6,945
clientip: 213.62.75.220 extension:  geo.srcdest: NG:IR geo.src: NG geo.dest: IR geo.coordinates: {
"lat": 40.63750778, "lon": -100.4712539 } host: www.elastic.co index: kibana_sample_data_logs
ip: 213.62.75.220 machine.ram: 13,958,643,712 machine.os: ios memory: - message: 213.62.75.220 - -
[2018-07-29T18:42:57.511Z] "GET /apm HTTP/1.1" 200 6945 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows

> Feb 28, 2021 @ 13:31:30.868  agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50
Safari/534.24 bytes: 5,963 clientip: 114.97.211.20 extension:  geo.srcdest: CN:PS geo.src: CN
geo.dest: PS geo.coordinates: { "lat": 42.74280556, "lon": -94.64730556 } host: www.elastic.co
index: kibana_sample_data_logs ip: 114.97.211.20 machine.ram: 7,516,192,768 machine.os: win 8
memory: - message: 114.97.211.20 - - [2018-07-29T18:31:30.868Z] "GET /enterprise HTTP/1.1" 200 5963

> Feb 28, 2021 @ 13:30:4  agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 bytes: 1,600
clientip: 55.89.141.209 extension: zip geo.srcdest: VN:ML geo.src: VN geo.dest: ML
```

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).**

      2021-2-27 18:00 - 9002 bytes



timestamp per 3 hours 2021-02-27 18:00
Avg. Bytes 9,002
Count 2

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

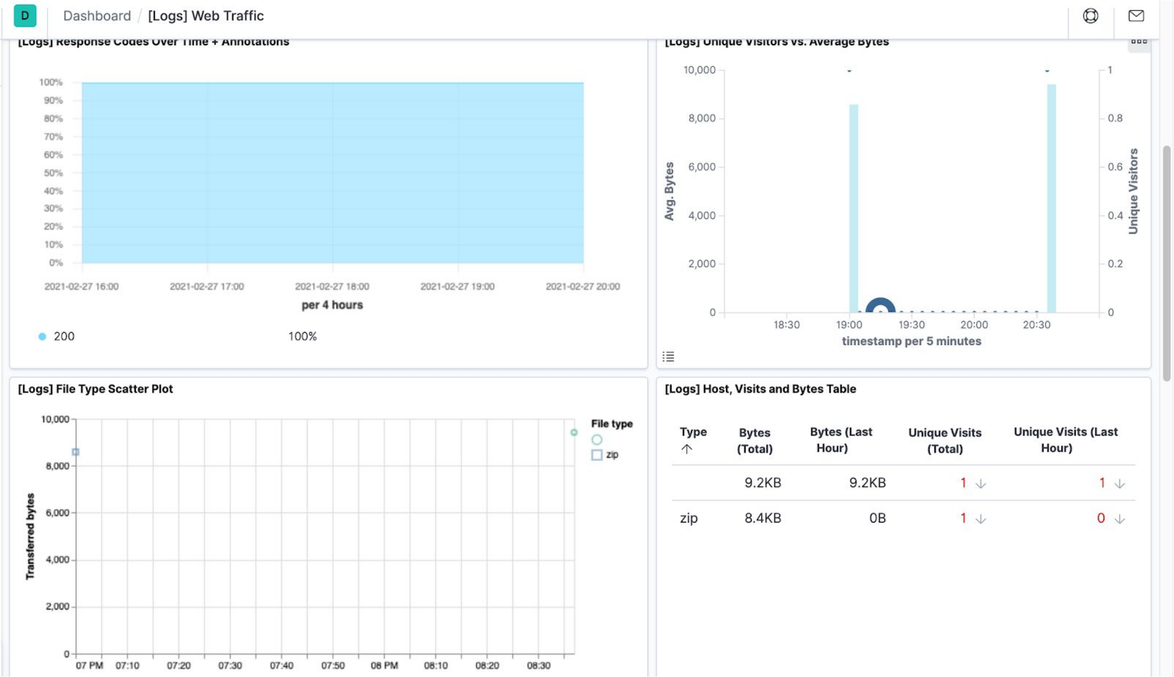
      2 unique visitors generated 9002 bytes at 2021-2-27 18:00, which is strange looking at the overall dataset because in other instances it is taking 30 - 50 unique visitors to generate such a huge amount of bytes.

4. **Filter the data by this event.**

    - **What is the timestamp for this event?**

      2021-2-27 19:00 - 8586 bytes
      2021-2-27 20:00 - 9418 bytes

- **What kind of file was downloaded?**
  zip and css file were downloaded



Dashboard / [Logs] Web Traffic

[Logs] Response Codes Over Time + Annotations

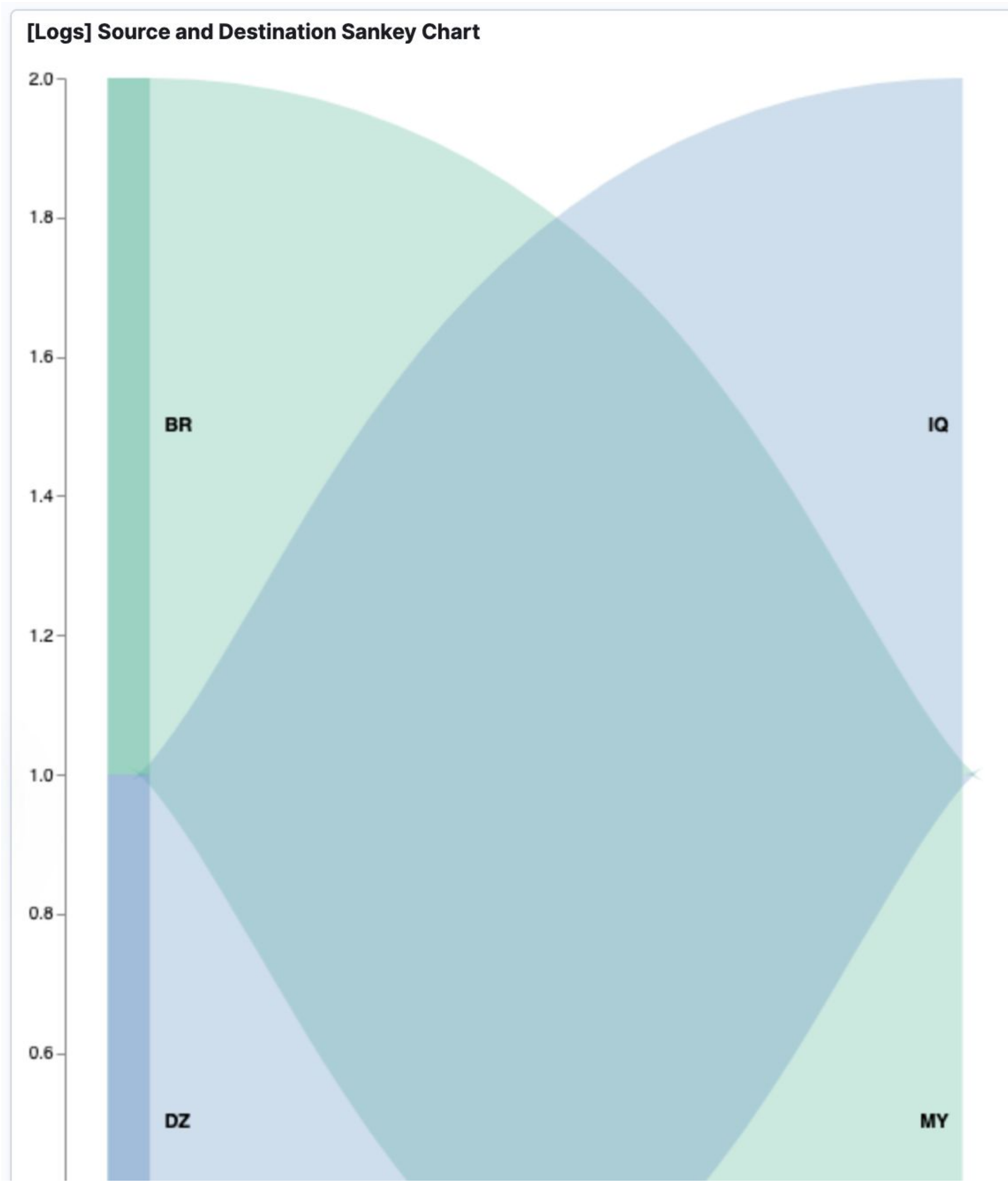
[Logs] Unique Visitors vs. Average Bytes

[Logs] File Type Scatter Plot

[Logs] Host, Visits and Bytes Table

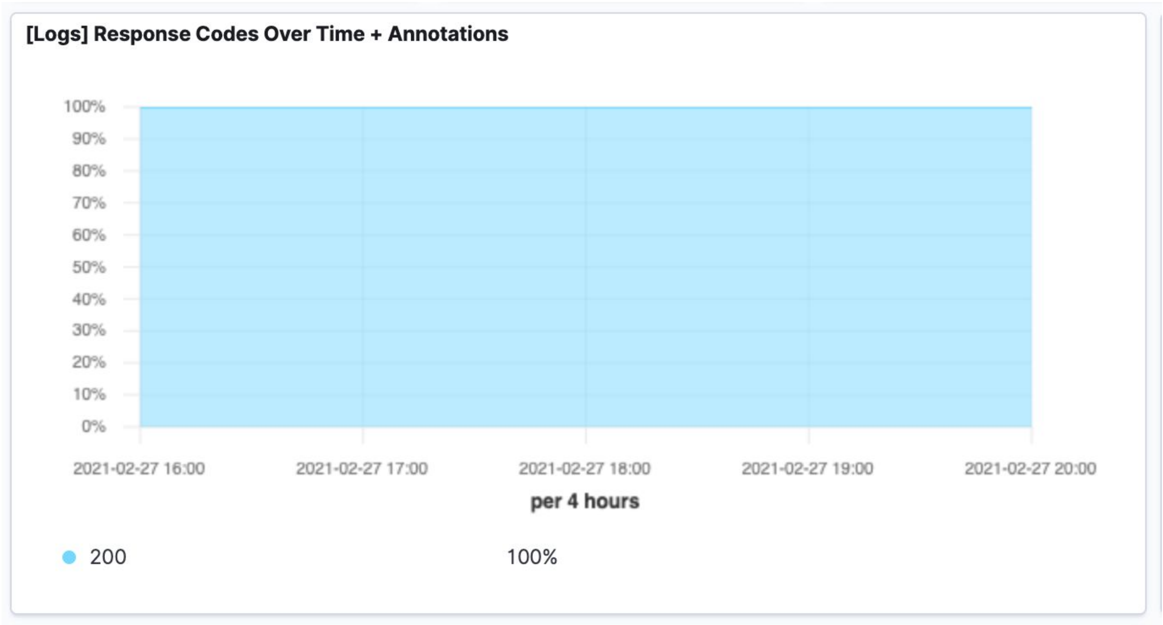
Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	9.2KB	9.2KB	1 ↓	1 ↓
zip	8.4KB	0B	1 ↓	0 ↓

- **From what country did this activity originate?**
  Brazil (BR) and Algeria (DZ)



[Logs] Source and Destination Sankey Chart

- **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?**
     DZ - 19.112.90.54
     BR - 17.111.163.53

   - **What are the geo coordinates of this activity?**
     BR - {

       "lat": 42.59157139,

       "lon": -114.7967178

     }

     DZ - {

       "lat": 40.88544444,

       "lon": -83.86863889

     }

   - **What OS was the source machine running?**

     DZ - ios
     BR - win 7

- **What is the full URL that was accessed?**

  DZ - https://www.elastic.co/downloads/apm
  BR -
  https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-windows-x86_64.zip

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

  DZ - elastic.co
  BR - artifacts.elastic.co

6. **Finish your investigation with a short overview of your insights.**

   - **What do you think the user was doing?**
     One user from DZ was accessing a elastic.co/download/apm page to download an apm server. The other user from BR was trying to download kibana-6.3.2 zip file applicable to windows machine

   - **Was the file they downloaded malicious? If not, what is the file used for?**
     No, the file they downloaded was not malicious.

     DZ - APM is an application performance monitoring system built on the Elastic Stack. It uses Elasticsearch as its data store and allows you to monitor performance of thousands of services in real time.

     BR - Kibana 6.3.2 is a data visualization dashboard for Elasticsearch.

   - **Is there anything that seems suspicious about this activity?**
     No

   - **Is any of the traffic you inspected potentially outside of compliance guidelines?**
     No