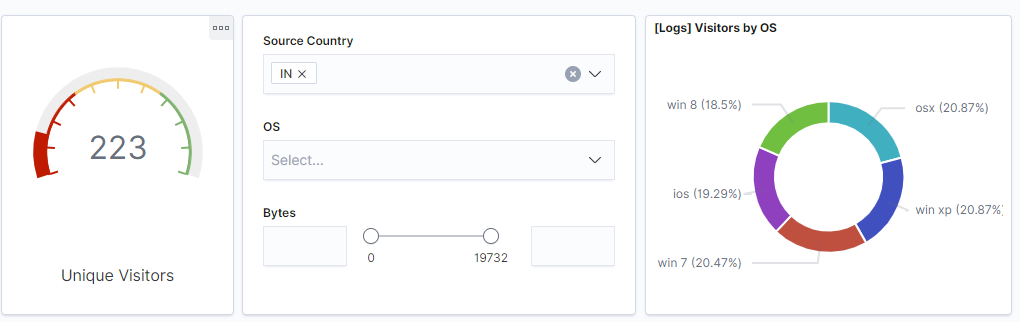
* You are a DevOps professional and have set up monitoring for one of your web servers. You are collecting all sorts of web log data and it is your job to review the data regularly to make sure everything is running smoothly.
* Today, you notice something strange in the logs and you want to take a closer look.
* Your task: Explore the web server logs to see if there's anything unusual.
* Your task: Explore the web server logs to see if there's anything unusual.

1. Add the sample web log data to Kibana
2. Answer the following questions:

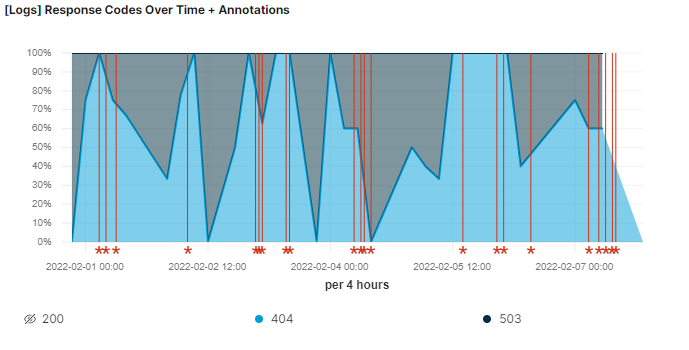
* In the last 7 days, how many unique visitors were located in India?  
  223



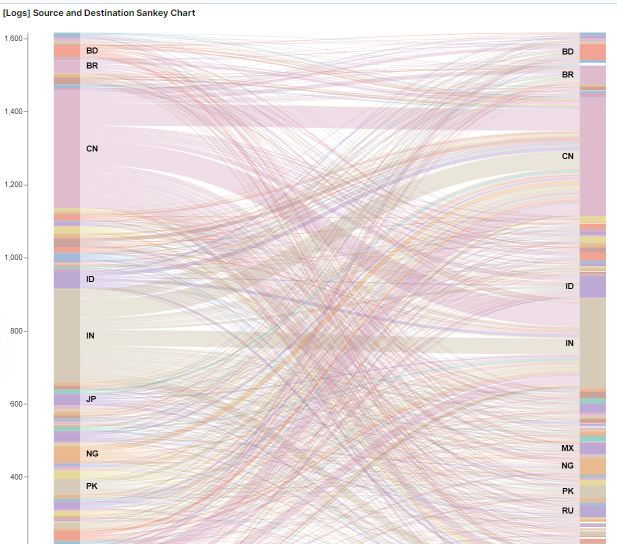
* In the last 24 hours, of the visitors from China, how many were using Mac OSX?  
  1



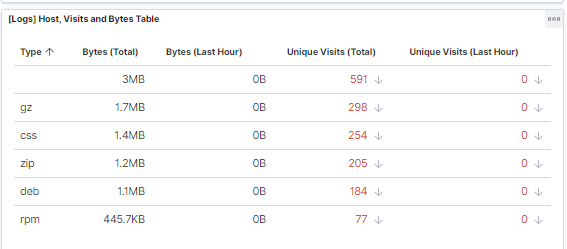
* In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?  
  404 = 100%  
  503 = 100%



* In the last 7 days, what country produced the majority of the traffic on the website?  
  China, 20%



* Of the traffic that's coming from that country, what time of day had the highest amount of activity?  
  1800
* 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).



\*\*gz: gzip, compressed archive using an algorithm\*\*

\*\*css: programming language used for web pages\*\*

\*\*zip: compressed archive\*\*

\*\*deb: debian, linux compressed package\*\*

\*\*rpm: like deb, but used for red hat enterprises\*\*

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).  
  10,735 bytes
* In your own words, is there anything that seems potentially strange about this activity?  
  There appears to be 3 suspicious visitors

1. Filter the data by this event.

* What is the timestamp for this event?  
  Feb 7, 2022 @ 20:22 & 23:05 & 23:20
* What kind of file was downloaded?  
  Zip file
* From what country did this activity originate?  
  India, US, China
* What HTTP response codes were encountered by this visitor?  
  200

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

* What is the source IP address of this activity?  
  223.112.248.233 & 223.112.248.233 & 35.143.166.159
* What are the geo coordinates of this activity?  
  { "lat": 37.85008167, "lon": -83.84575194 } & { "lat": 42.99821222, "lon": -74.32955111 }& { "lat": 43.34121, "lon": -73.6103075 }
* What OS was the source machine running?  
  Linux
* What is the full URL that was accessed?  
  <https://www.elastic.co/downloads/apm> & /kibana/kibana-6.3.2-windows-x86\_64.zip & /beats/metricbeat/metricbeat-6.3.2-i686.rpm
* From what website did the visitor's traffic originate?  
  http://nytimes.com/warning/georgi-beregovoi & http://twitter.com/success/maksim-surayev & http://facebook.com/success/jay-c-buckey

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

* What do you think the user was doing?  
  One was downloading a apm file and the other was downloading a deb file and the last was downloading an rpm
* Was the file they downloaded malicious? If not, what is the file used for?  
  Probably not, the apm file is a performance application and the other a debian application.
* Is there anything that seems suspicious about this activity?  
  Unless you can see the actual file then there’s no real way of telling unless it's from a legitimate and trusted source.
* Is any of the traffic you inspected potentially outside of compliance guidelines?  
  Nothing in particular stands out to me. Looks like normal use.