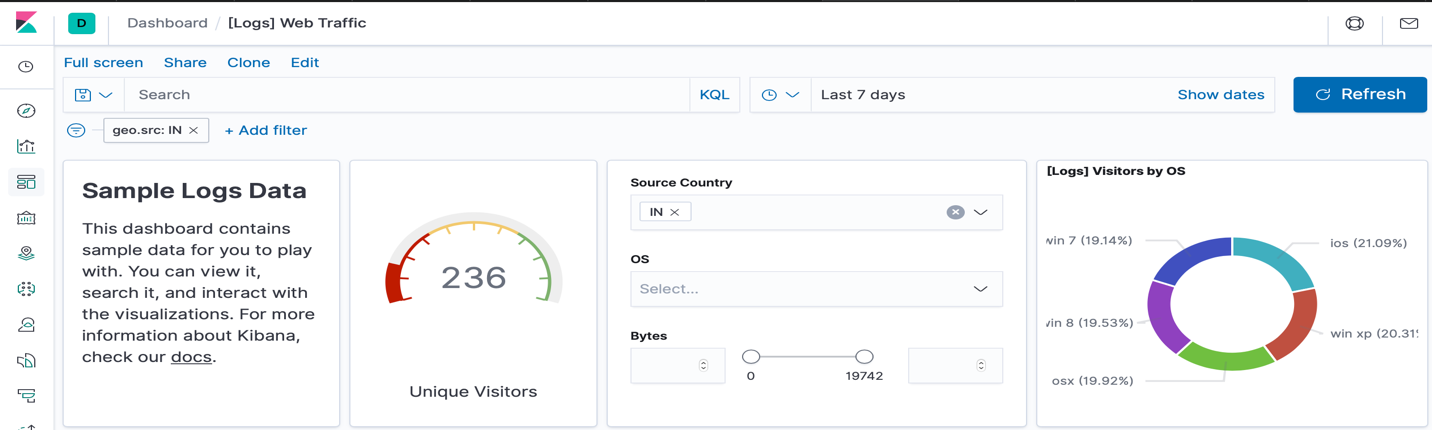
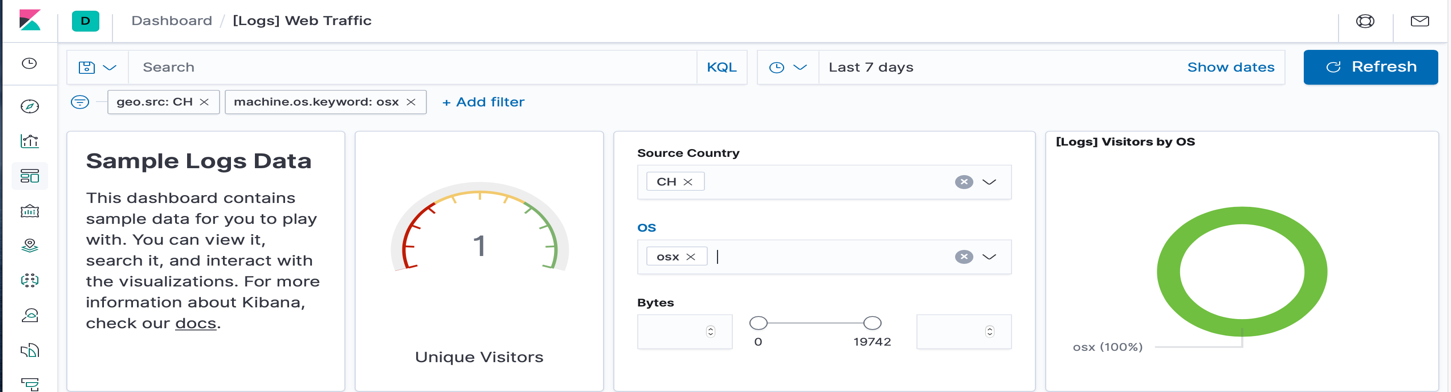
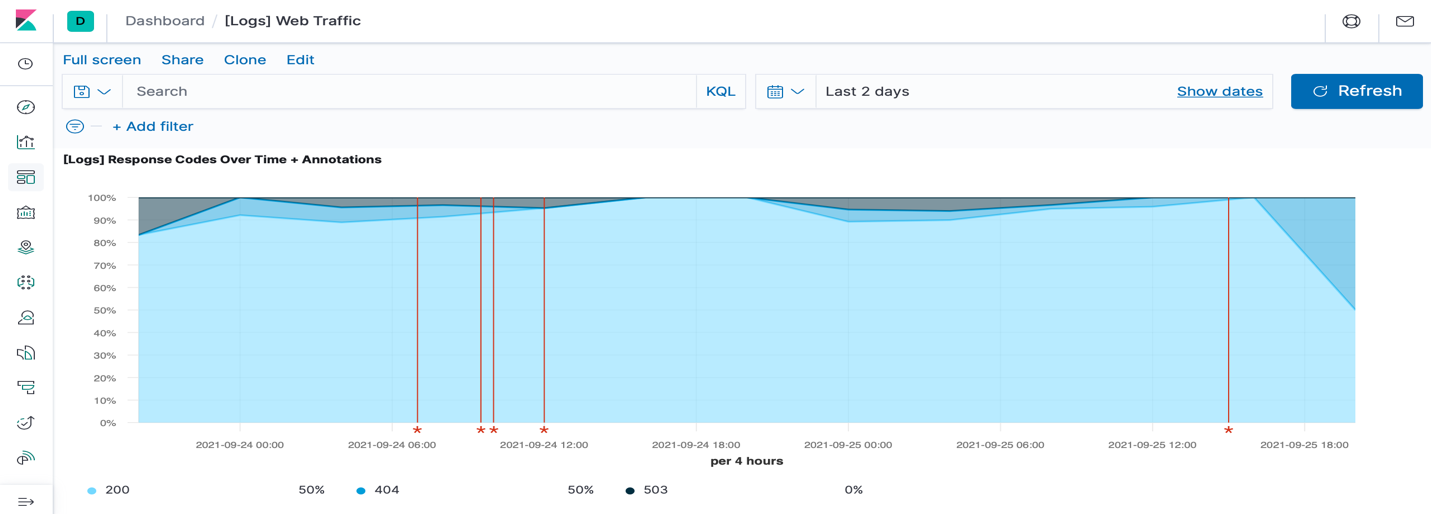
1. In the last 7 days, how many unique visitors were located in India? (236)



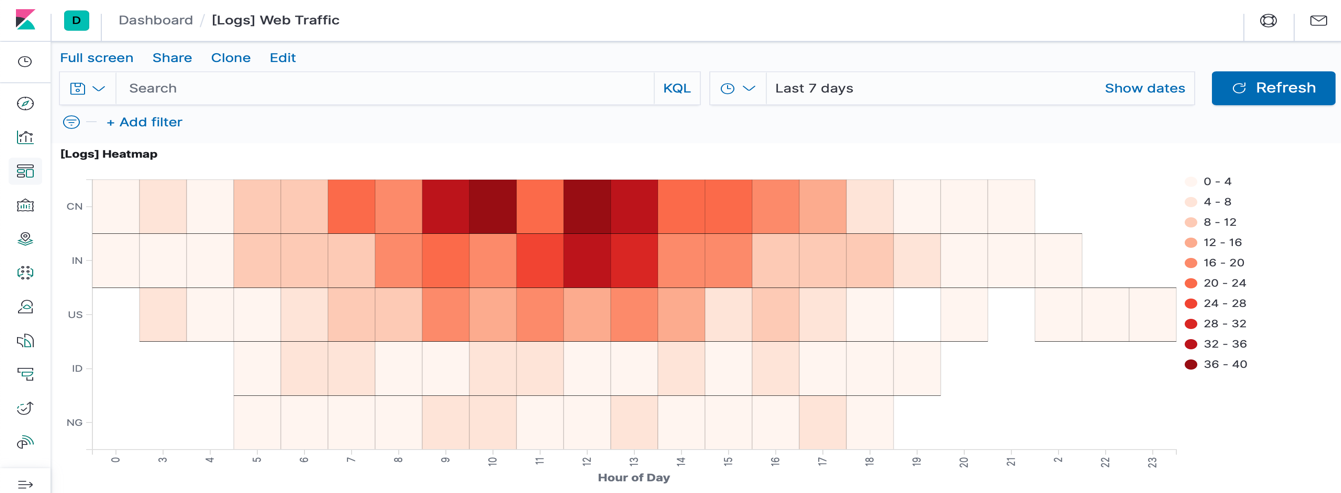
1. In the last 24 hours, of the visitors from China, how many were using Mac OSX? (1)



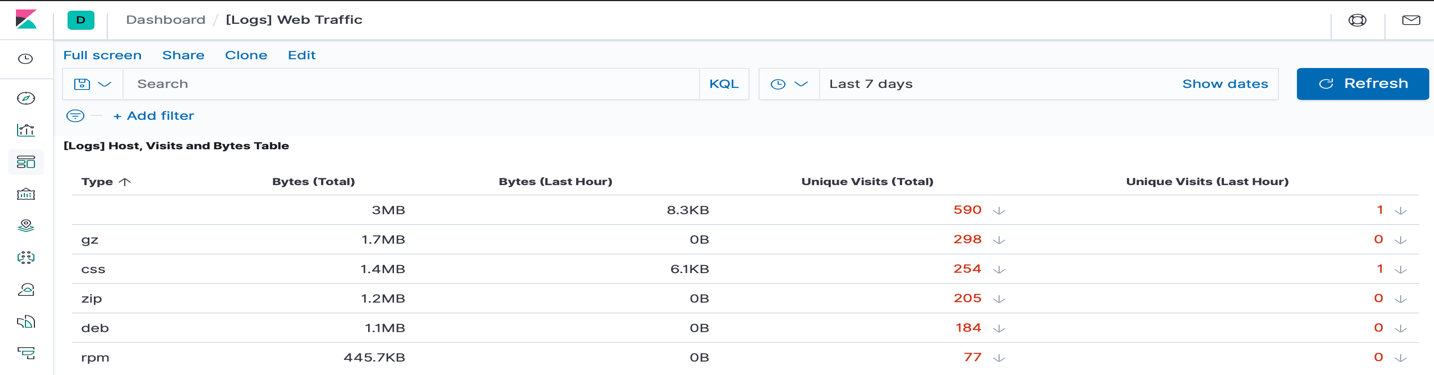
1. In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 404: 50% and 503: 0%



1. In the last 7 days, what country produced the majority of the traffic on the website?
2. Of the traffic that's coming from that country, what time of day had the highest amount of activity? China between 10 a.m. and 12 p.m.



1. 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:** .gz files are compressed files created using the gzip compression utility.

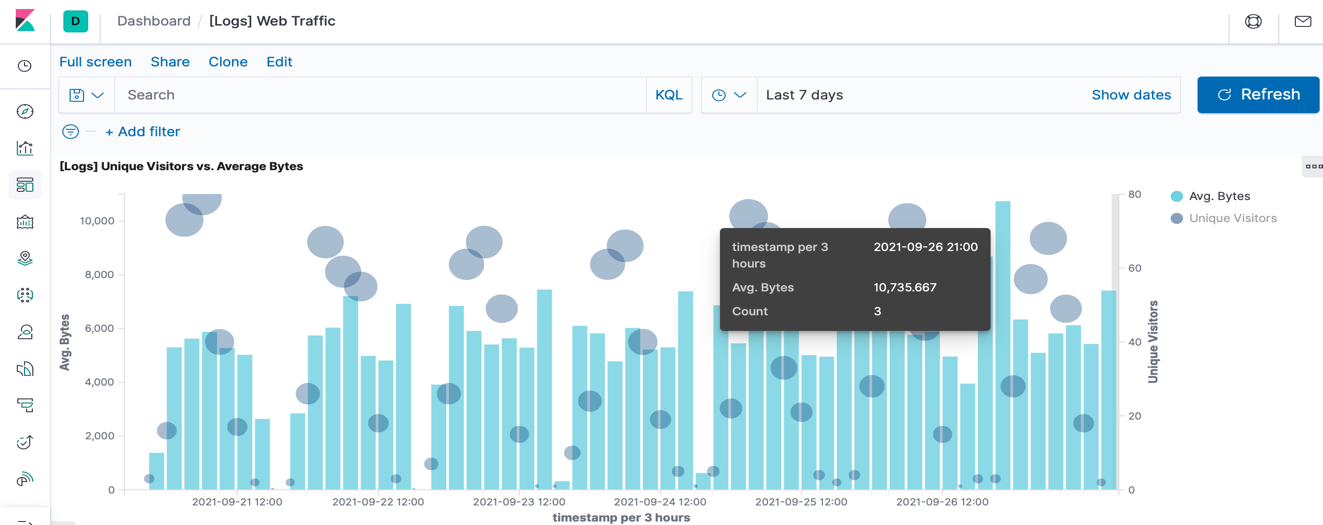
 **css:** .css files can help define font, size, color, spacing, border and location of HTML information on a webpage. They are downloaded with their .html counterparts and rendered by the browser.

 **zip:** A lossless compression format. A .zip file may contain one or more files or directories that have been compressed.

 **deb:** A file with the .deb file extension is a Debian (Linux) Software Package file. These files are installed when using the apt package manager.

 **rpm:** .rpm file formats are a Red Hat Software Package file. RPM stands for Red Hat Package Manager.

1. Look at the chart that shows Unique Visitors Vs. Average Bytes.

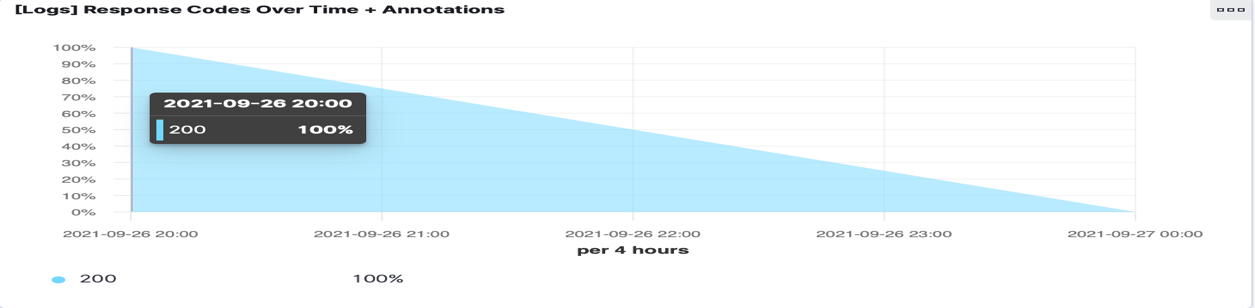


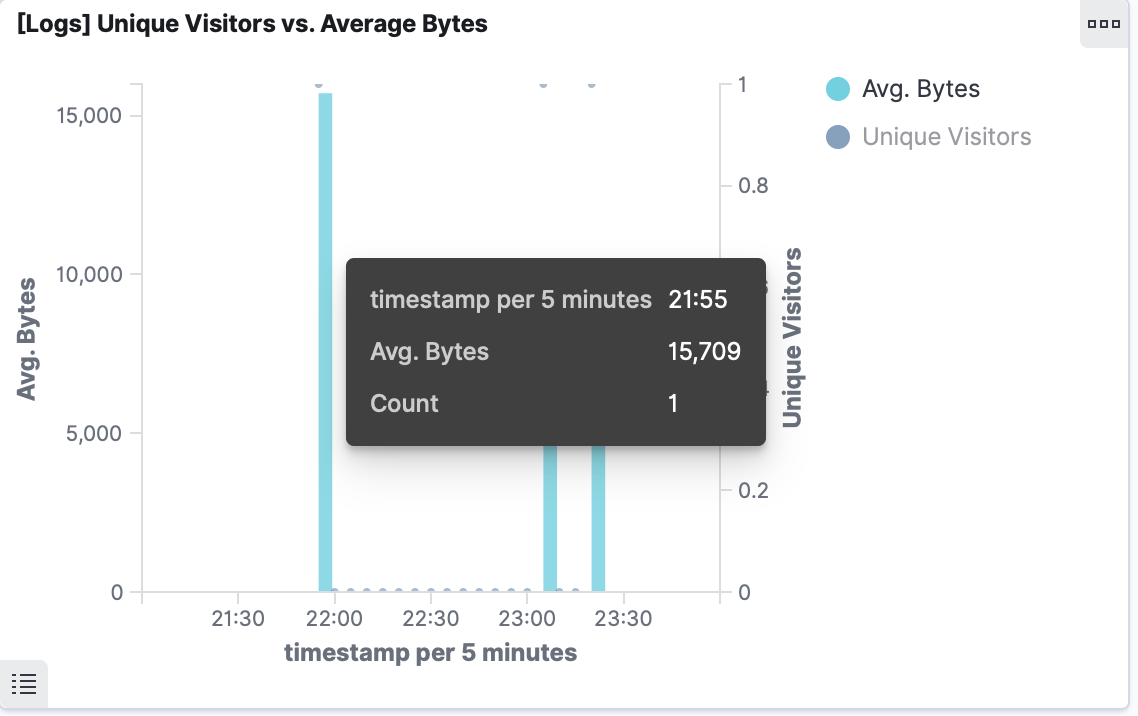
 Locate the time frame in the last 7 days with the most amount of bytes (activity).

 In your own words, is there anything that seems potentially strange about this activity? In the graph above, it appears that  *one* visitor is using 10,735.667 bytes, which is considerably higher than all other usage.

1. Filter the data by this event.







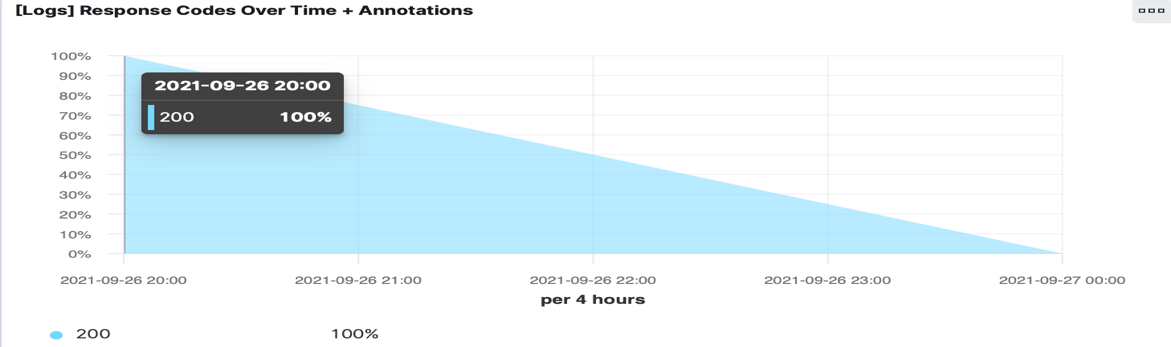
What is the timestamp for this event?

* **Example Answer:** The time filter shows Sep 26, 2020 @ 21:00 -> Sep 27, 2020 @ 00:00. The time stamp is 21:55.

What kind of file was downloaded? RPM and Zip files



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



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

 What is the source IP address of this activity? 125.46.156.2

 What are the geo coordinates of this activity? { "lat": 30.7313, "lon": -86.15160833 }

 What OS was the source machine running? Windows 8

 What is the full URL that was accessed?

<https://artifacts.elastic.co/downloads/kibana/kibana-6.3.2-darwin-x86_64.tar.gz>

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

<http://www.elastic-elastic-elastic.com/success/ronald-mcnair>

Finish your investigation with a short overview of your insights.

* What do you think the user was doing?
  + This event appears to be a user downloading a Kibana from the website being monitored.
* Was the file they downloaded malicious? If not, what is the file used for?
  + The file does not appear to be malicious, as Kibana is an free and open frontend application that sits on top of the Elastic Stack, providing search and data visualization capabilities for data indexed in Elasticsearch
* Was there anything that seems suspicious about this activity?
  + Nothing appears to be suspicious.
* Is any of the traffic you inspected potentially outside of compliance guidelines?
  + Nothing appears to be out of compliance guidelines.