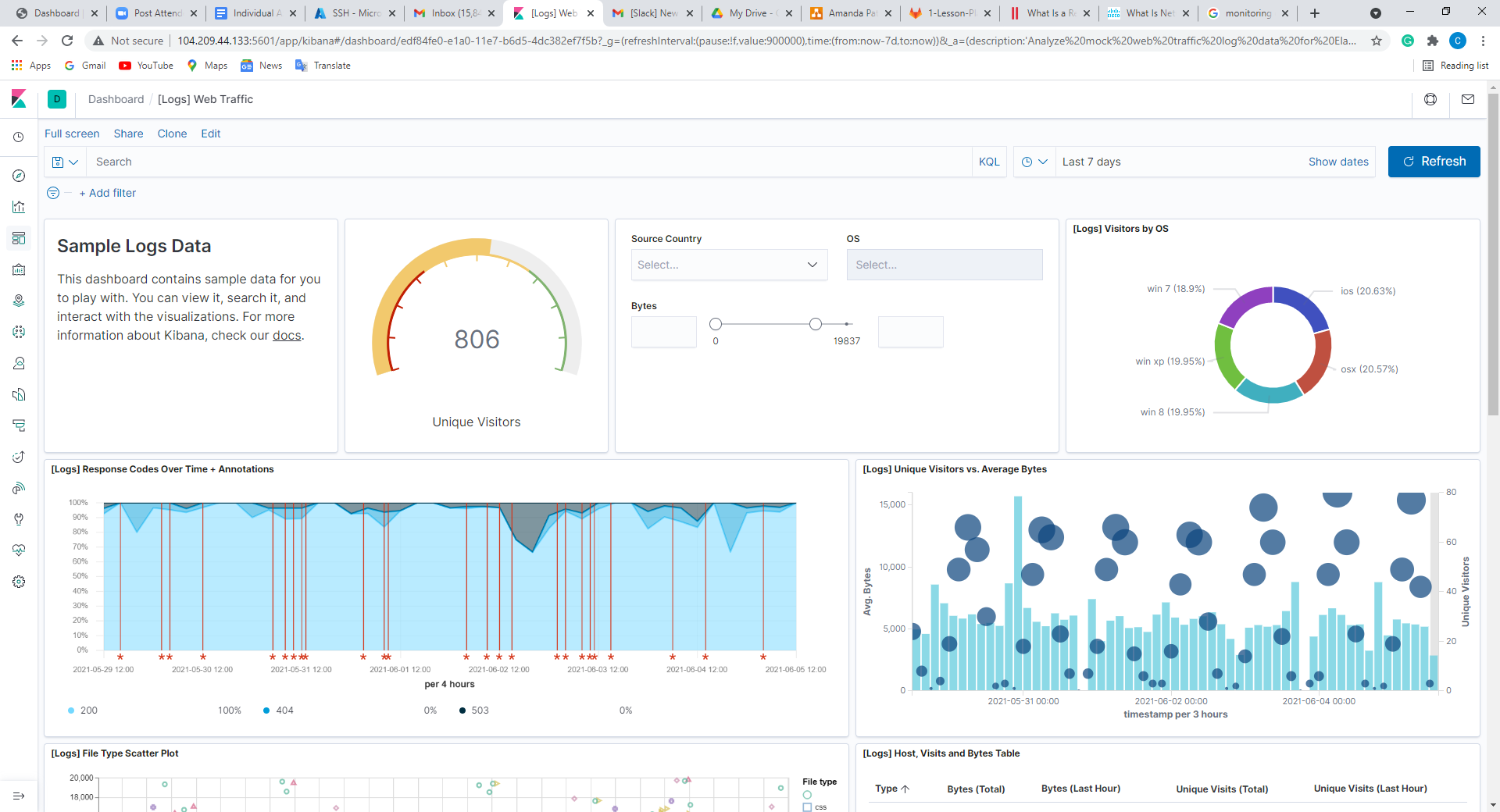
Amanda Patterson

6/5/2021

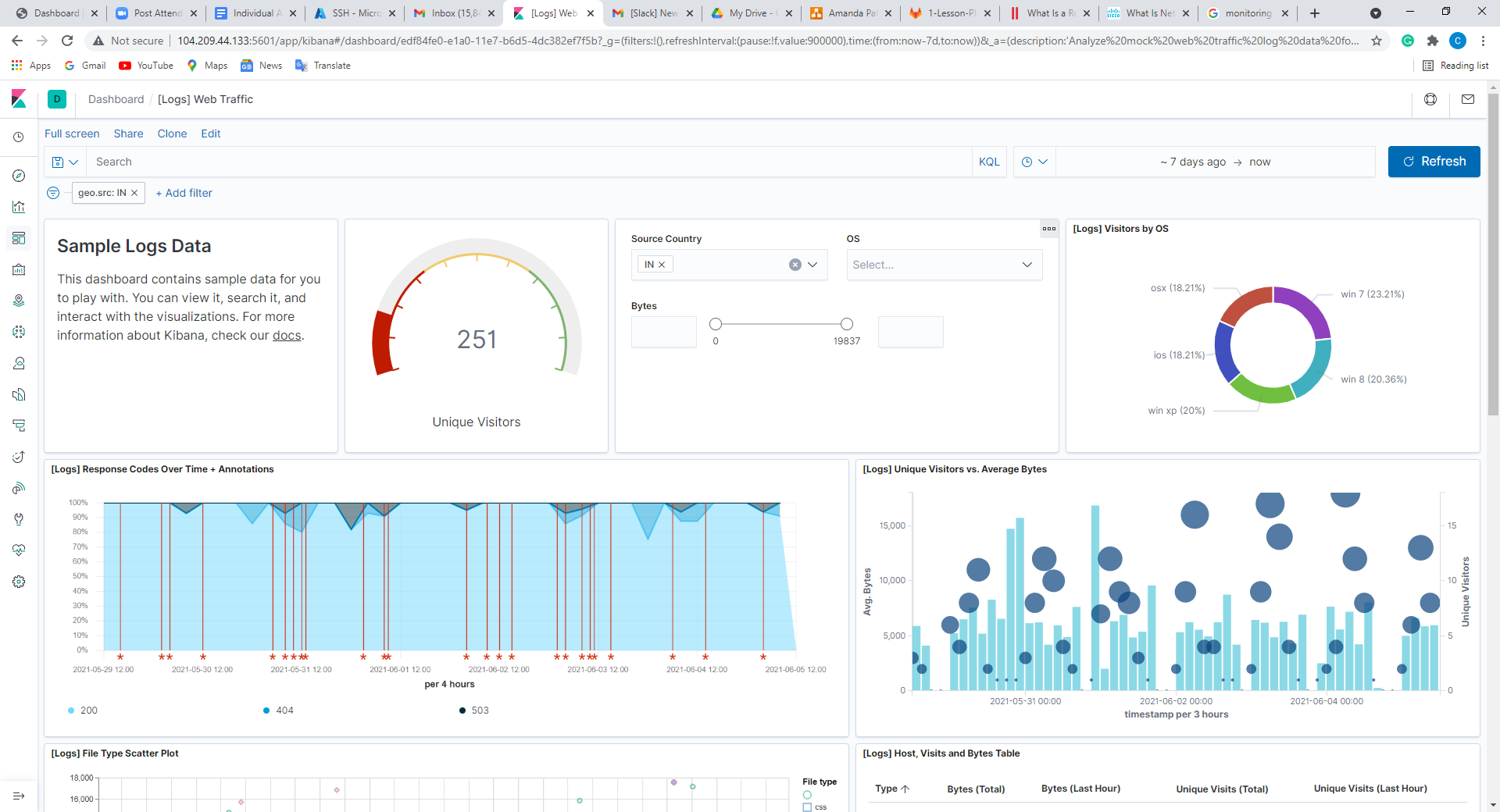
Project 13 Part

Exploring Kibana / Kibana Continued

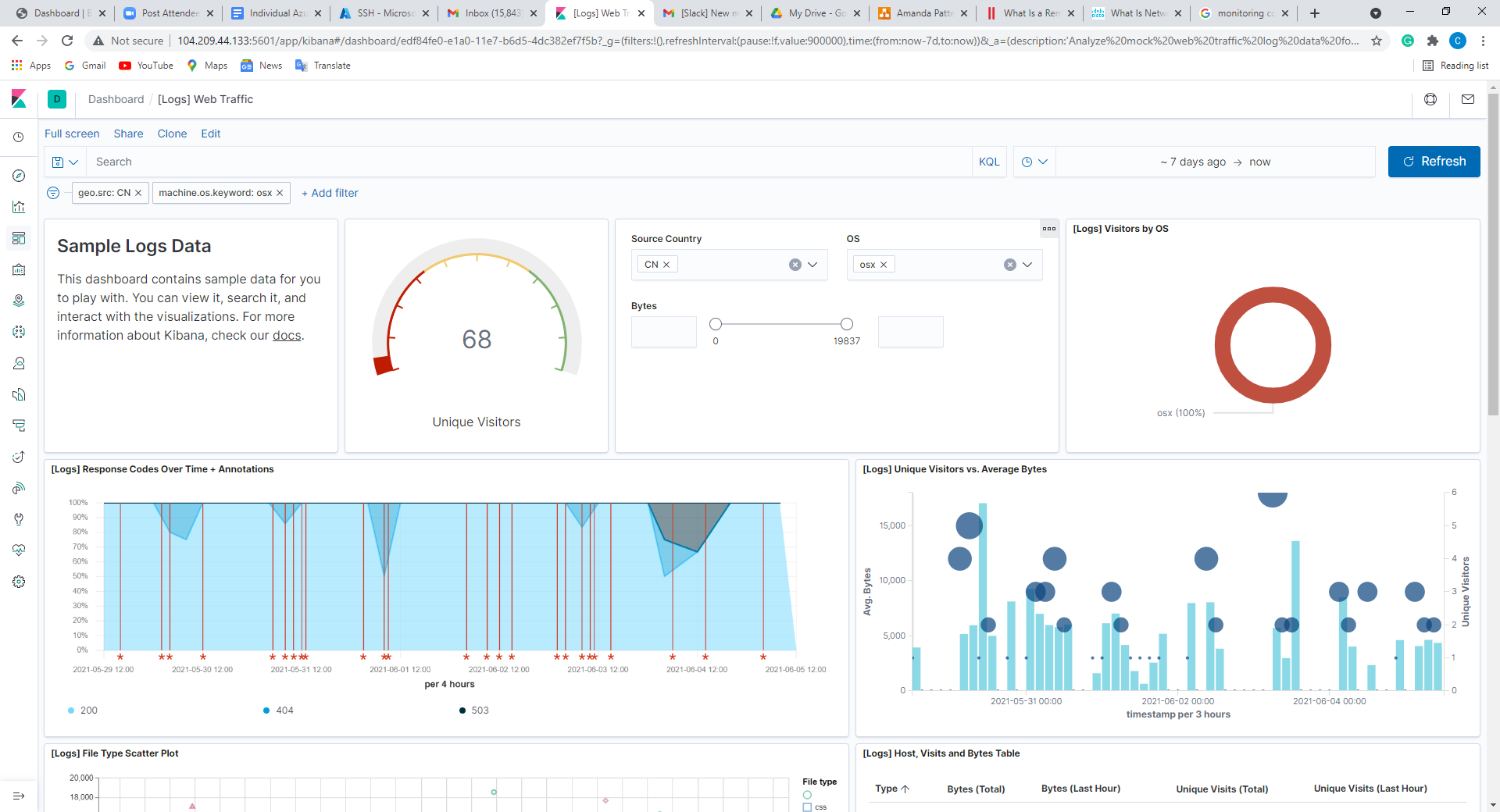
Launch Sample Data



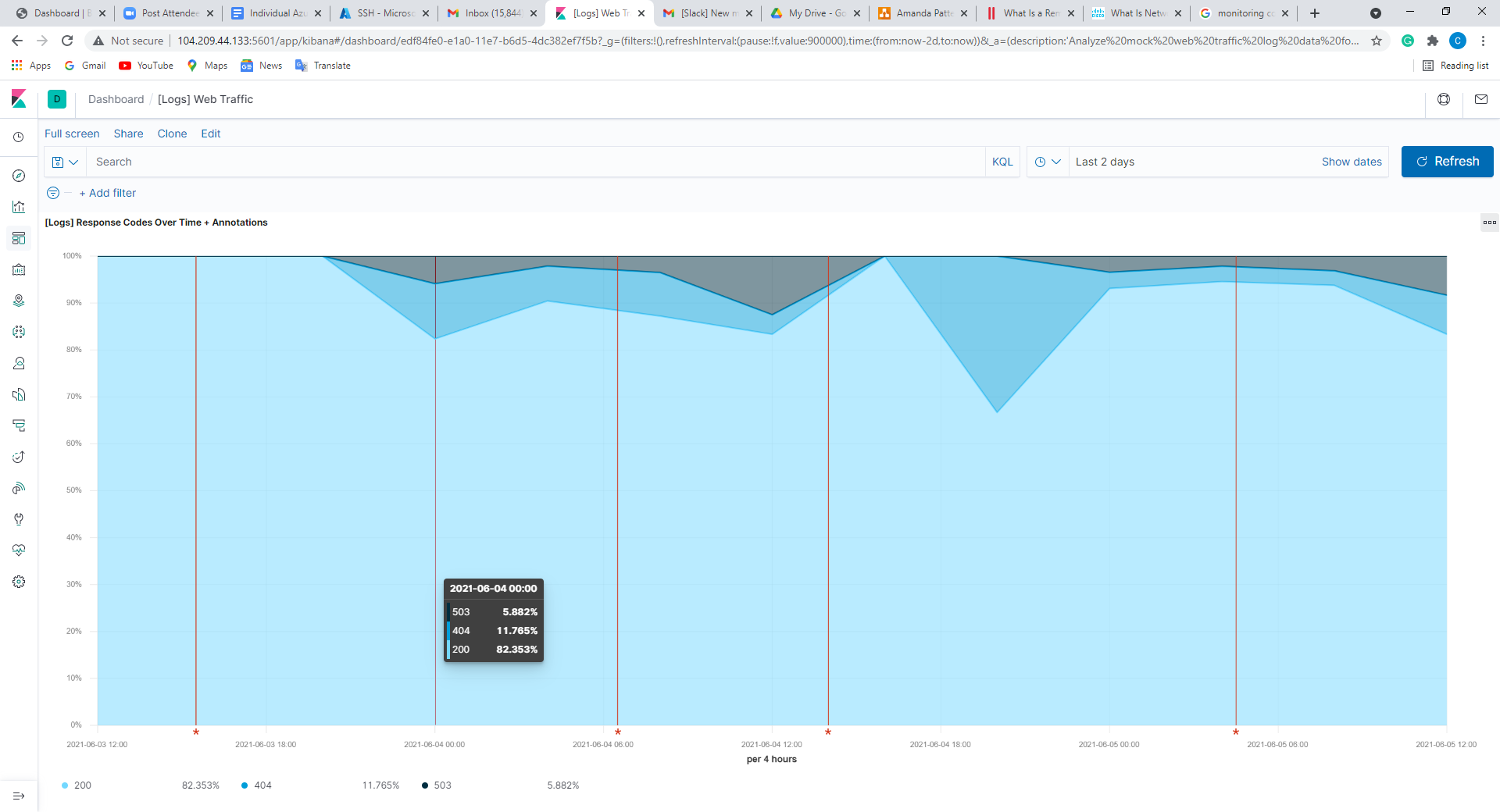
India unique users: (251)

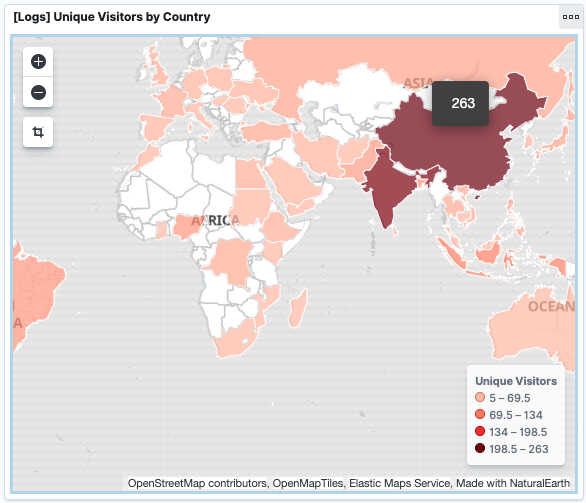


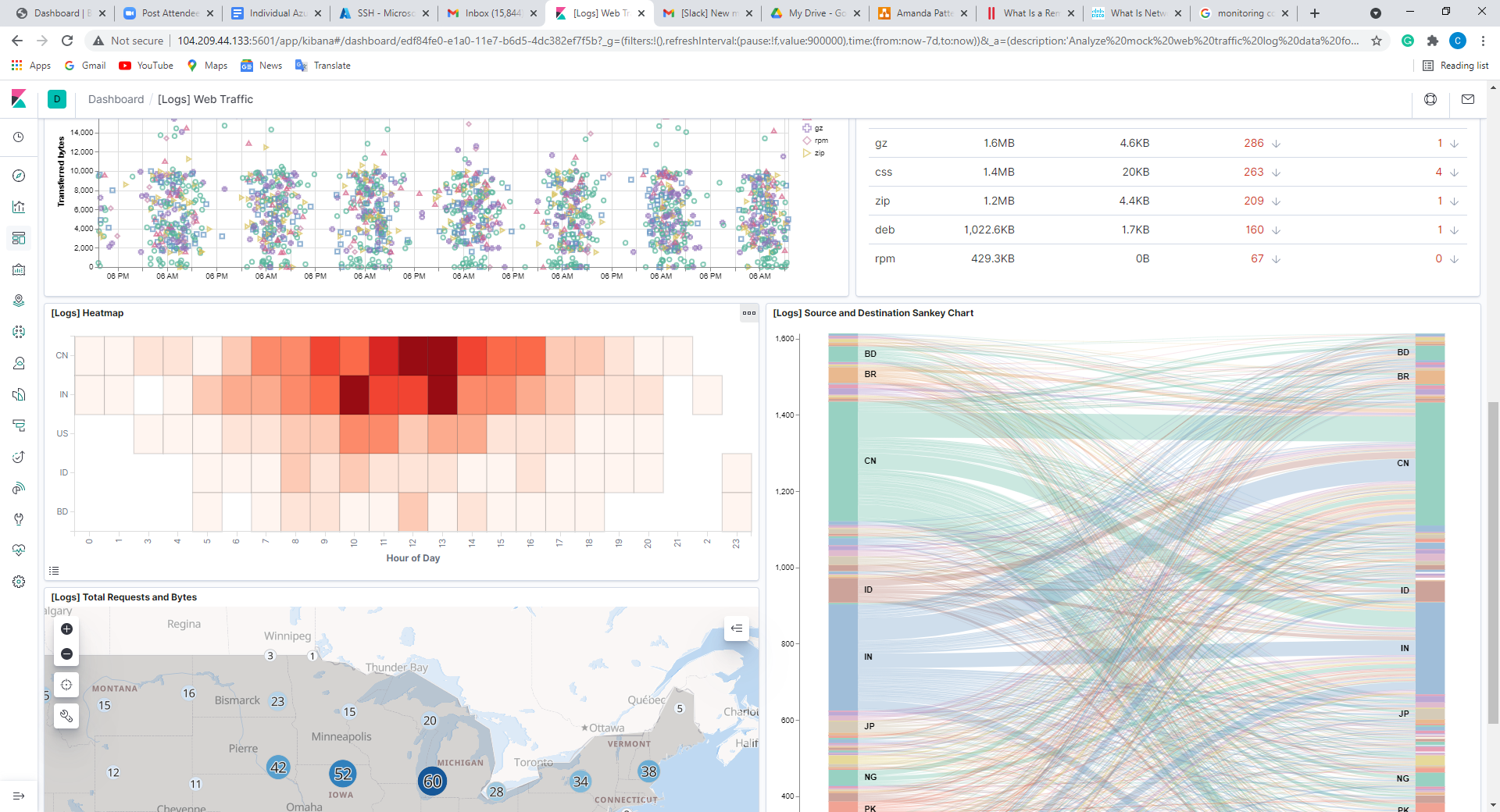
In the last 24 hours of the visitors from China, how many were using Mac OSX? (68)

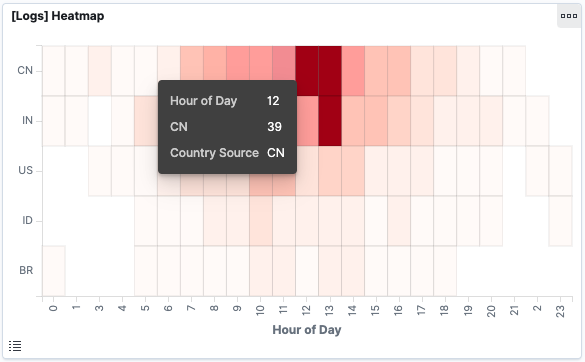


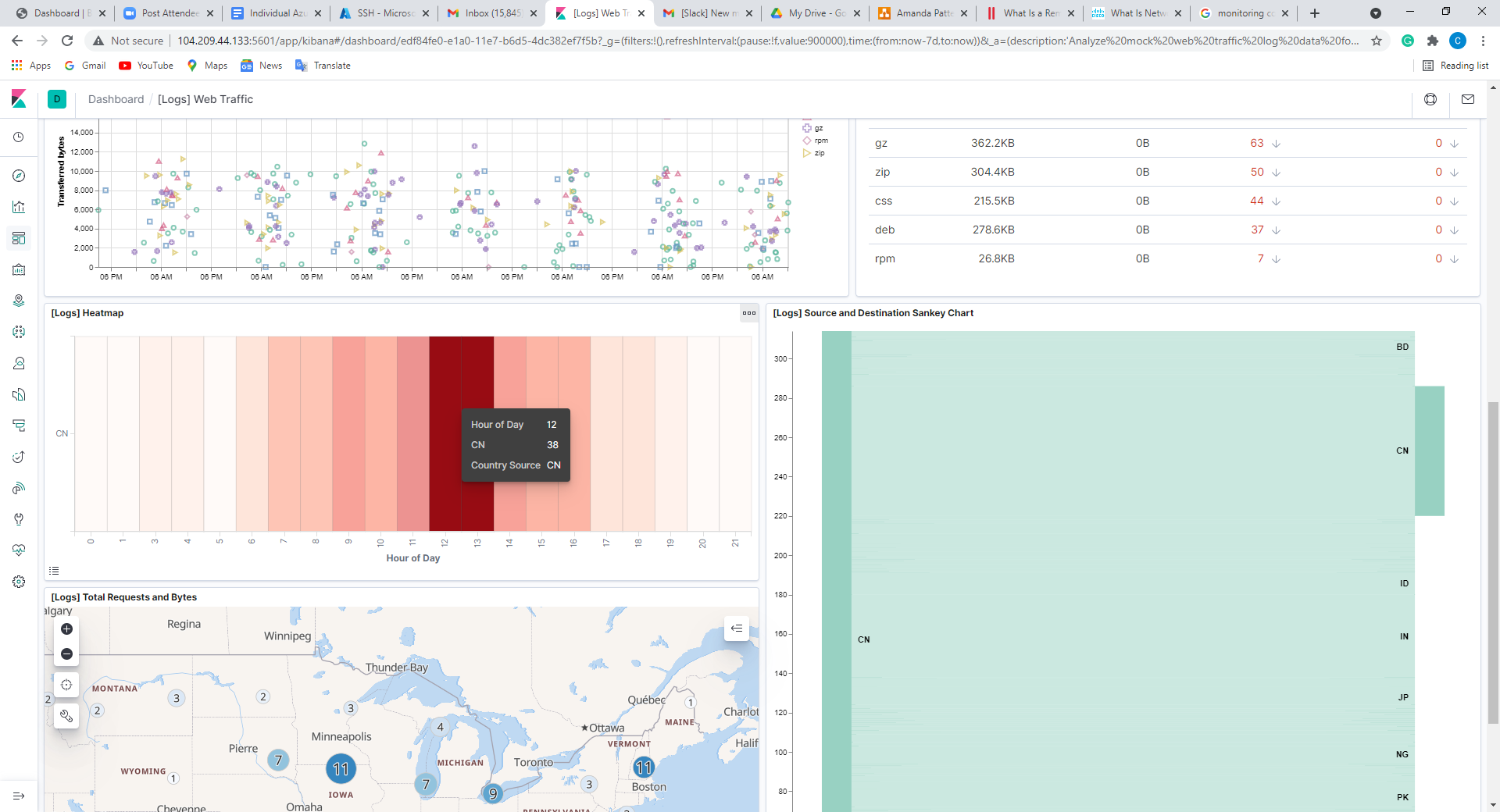
In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? : 404: 11.765% and 503: 5.882 %

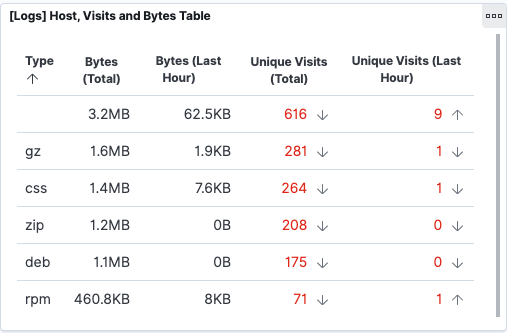


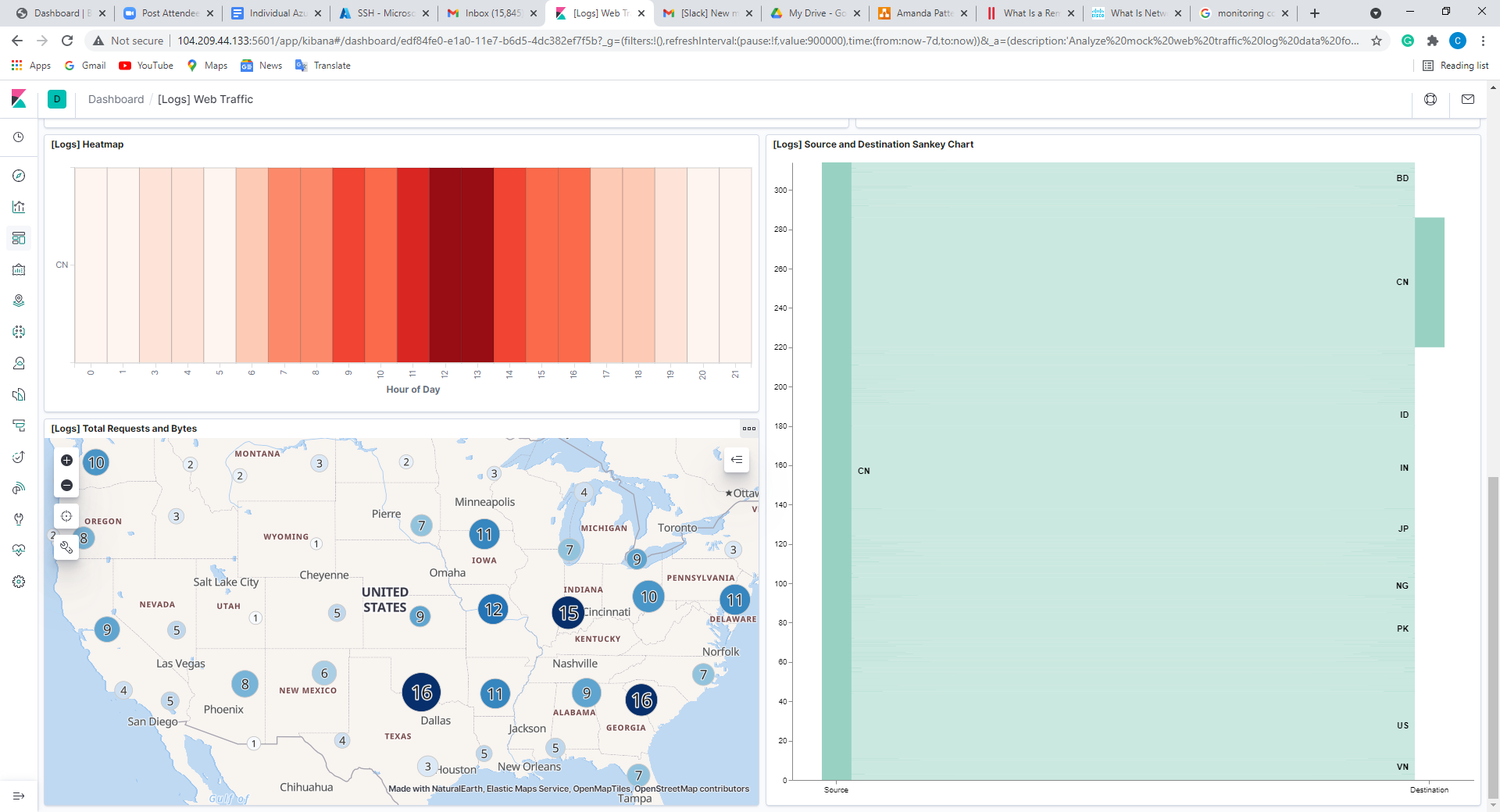










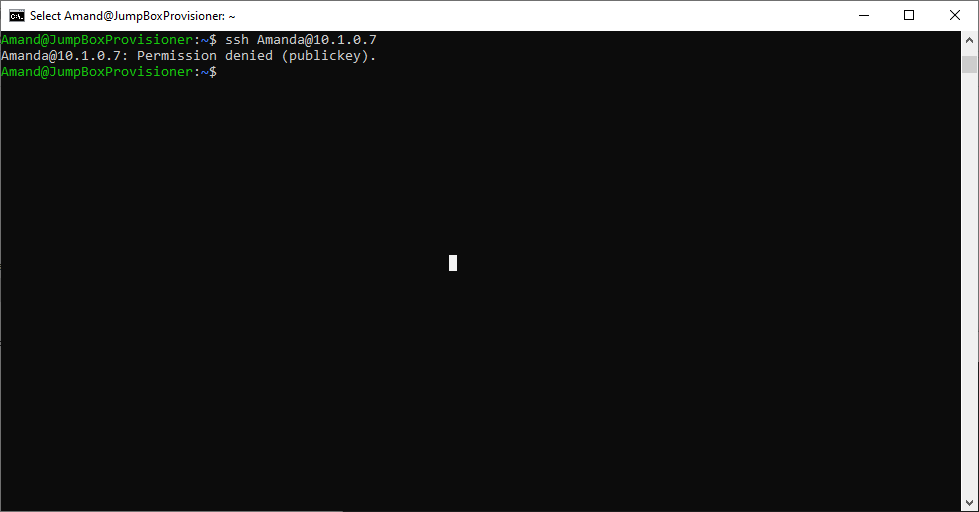


**SSH Barrage Solutions**

1. Start by logging into your jump-box.
   * Run: ssh username@ip.of.web.vm
   * You should receive an error:
   * sysadmin@Jump-Box-Provisioner:~$ ssh sysadmin@10.0.0.5

sysadmin@10.0.0.5: Permission denied (publickey).

* + This error was also logged and sent to Kibana.



Run the failed SSH command in a loop to generate failed login log entries.

# Creates 1000 login attempts on the 10.0.0.5 server.

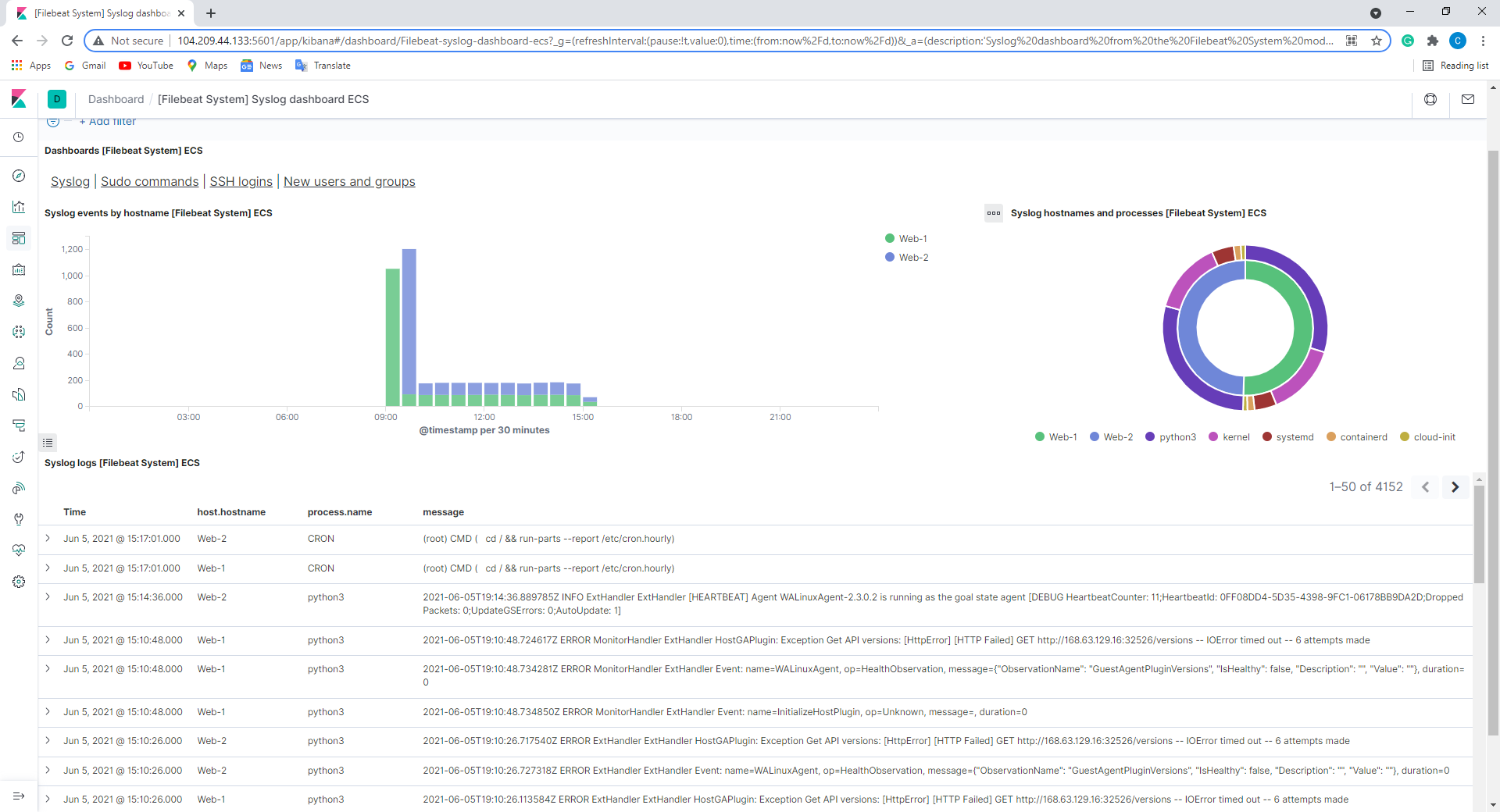
sysadmin@Jump-Box-Provisioner:~$ for i in {1..1000}; do ssh sysadmin@10.0.0.5; done

Search through the logs in Kibana to locate your generated failed login attempts.

# IMPORTANT: This loop will continue to run until you stop it using `CTRL + C`

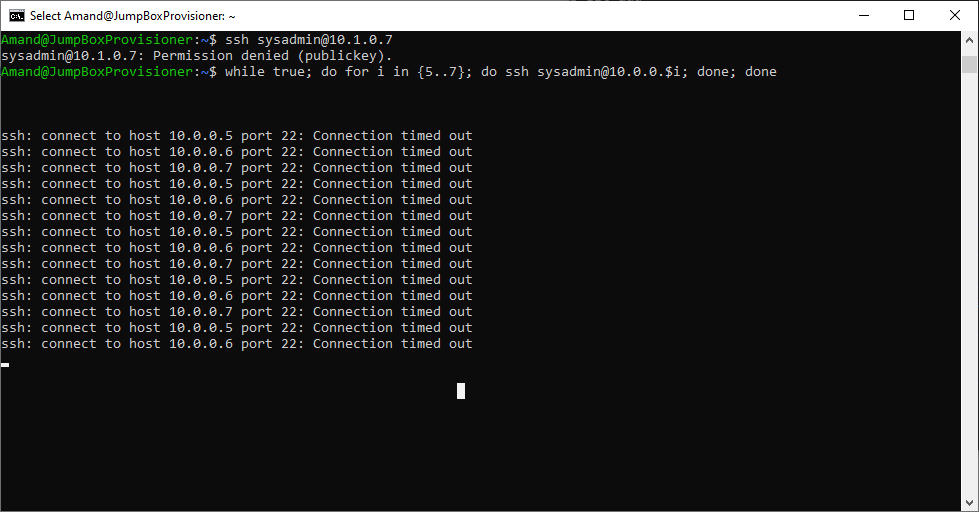
# It will create thousands of login attempts on the 10.0.0.5 server.

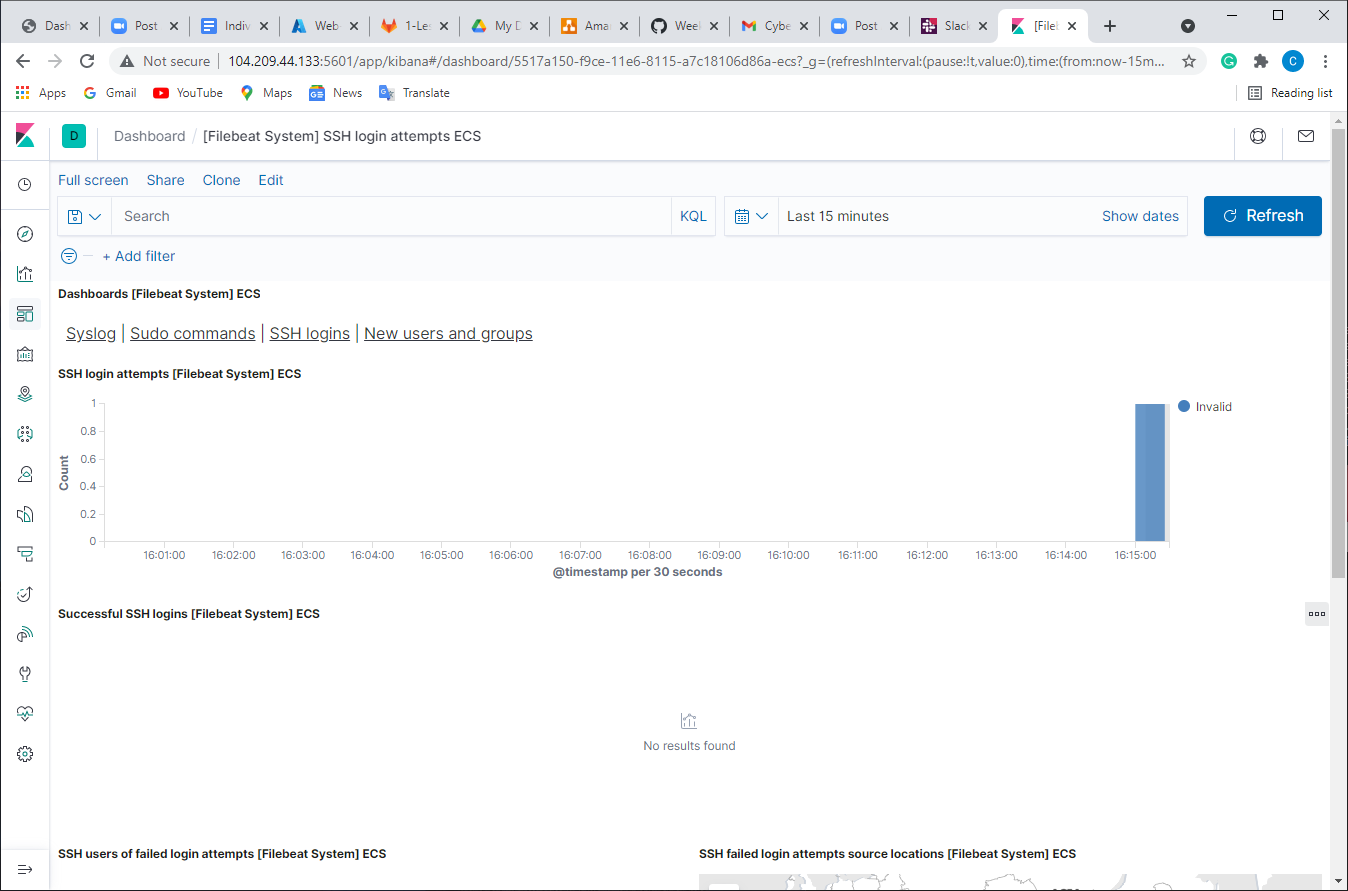
sysadmin@Jump-Box-Provisioner:~$ while true; do ssh sysadmin@10.0.0.5; done



Create a nested loop that generates SSH login attempts across all 3 of your VM's.

sysadmin@Jump-Box-Provisioner:~$ while true; do for i in {5..7}; do ssh sysadmin@10.0.0.$i; done; done





for i in {1..1000}; do ssh sysadmin@10.0.0.5; done

