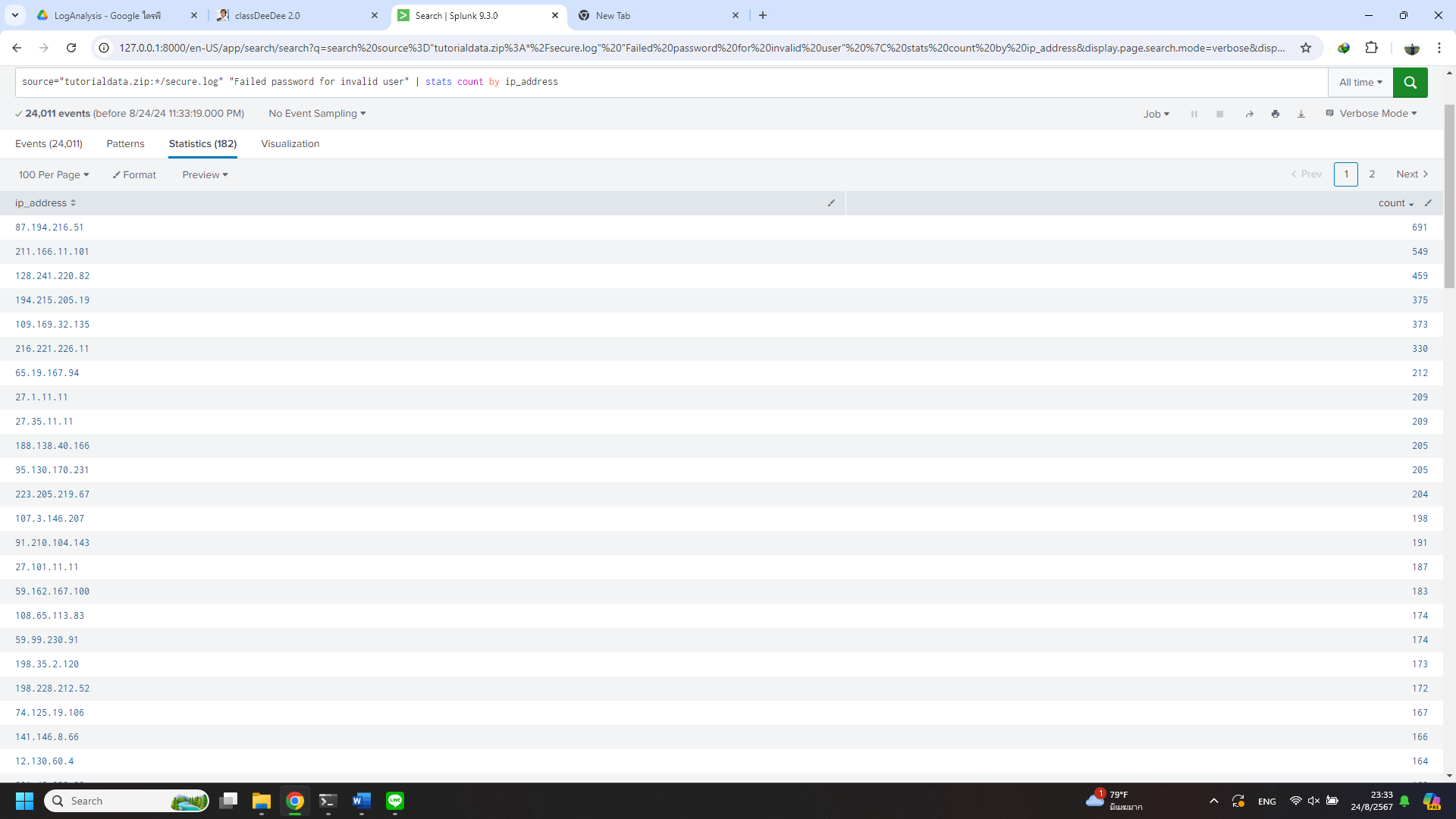
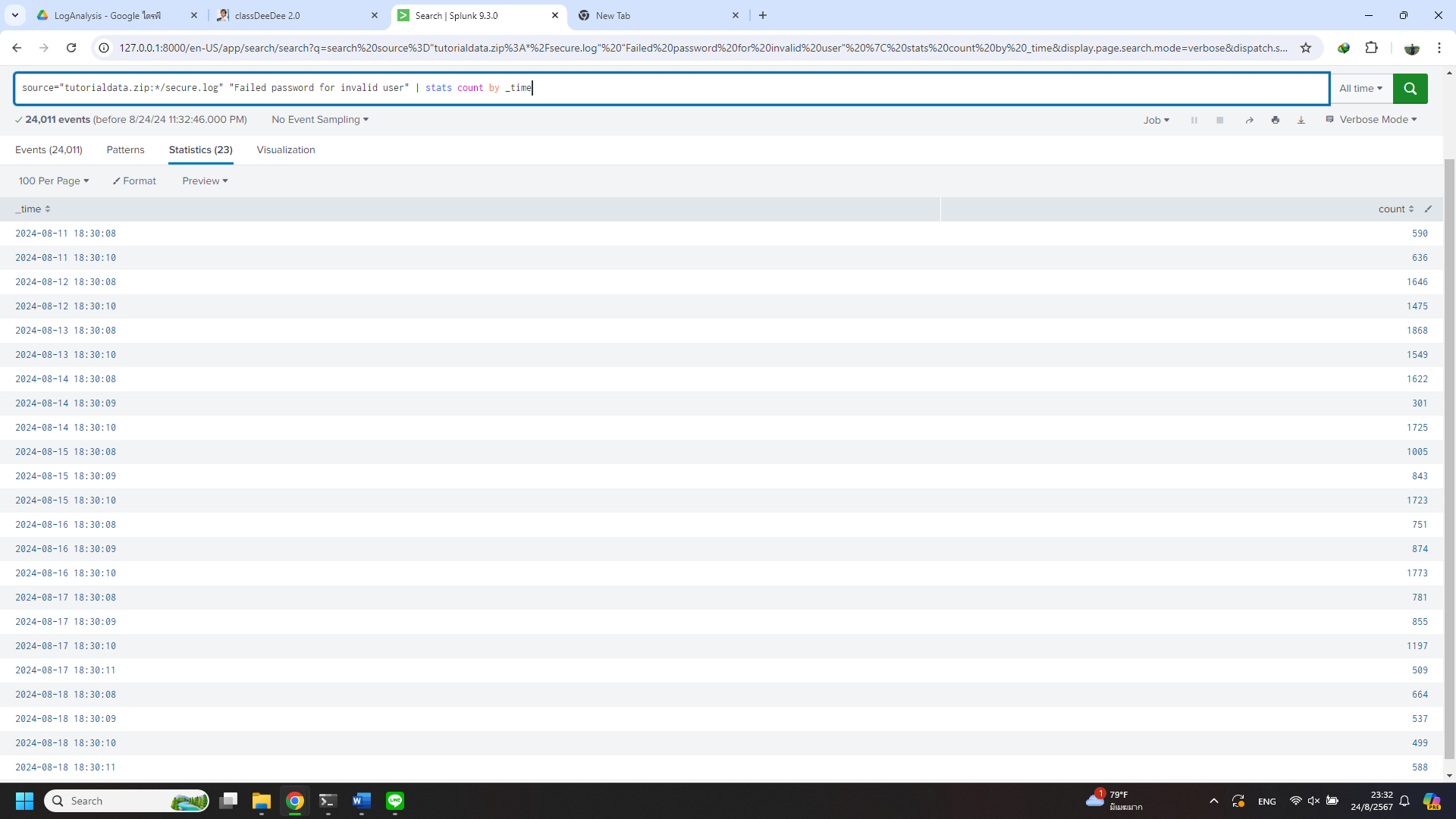
Q1. How many hackers are trying to get access to our servers? And how many attempts are there? Explain/define how you count distinct hackers.



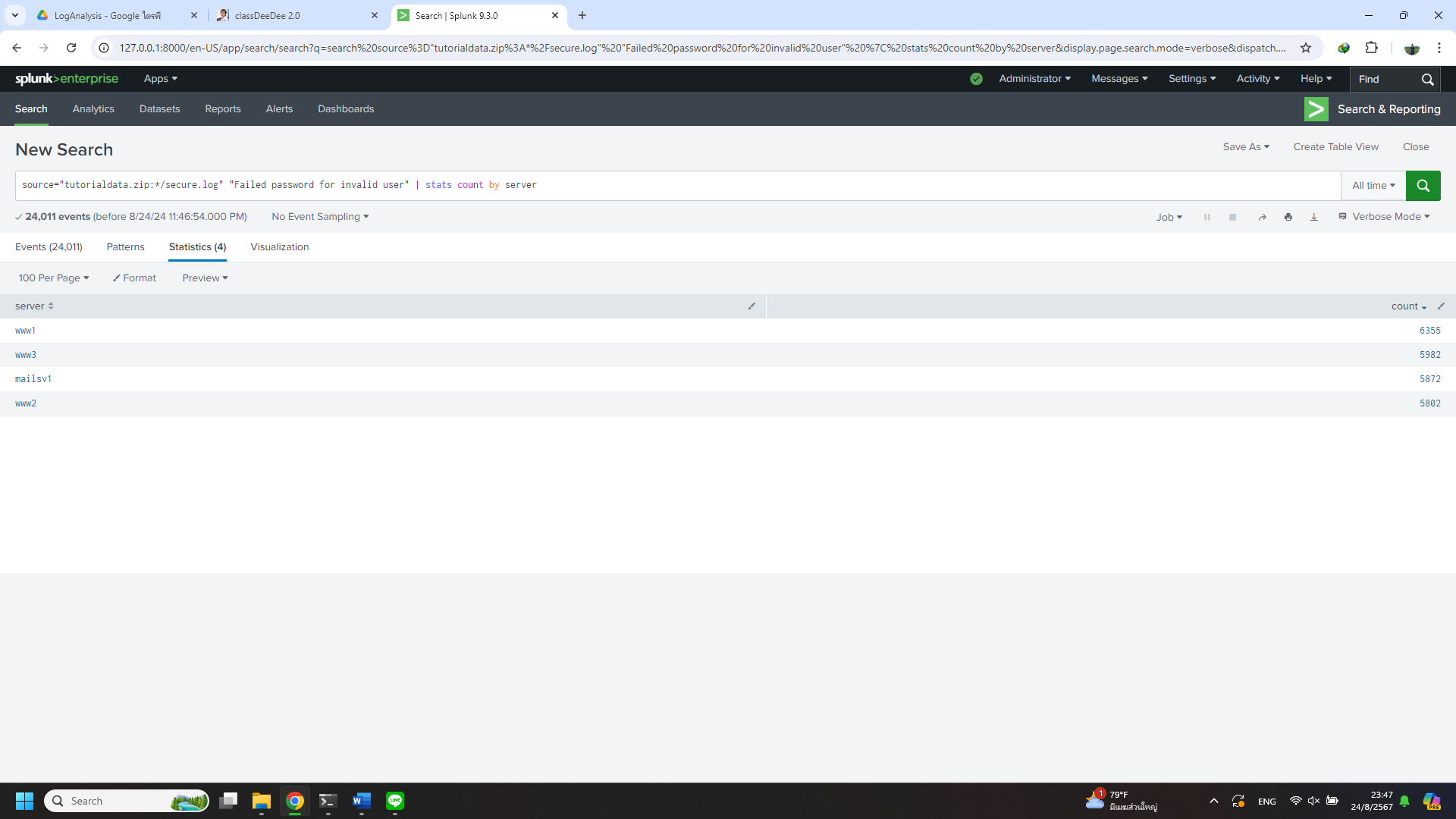
Ans. I assume that each hacker uses their own ip-address. So, I make new field via regular expression from (?<ip\_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}) and search in secure.log then pipe to count  
source="tutorialdata.zip:\*/secure.log" "Failed password for invalid user" | stats count by ip\_address As the result of 182 hackers and 24011 attempts.

Q2. What time do hackers appear to try to hack our servers?



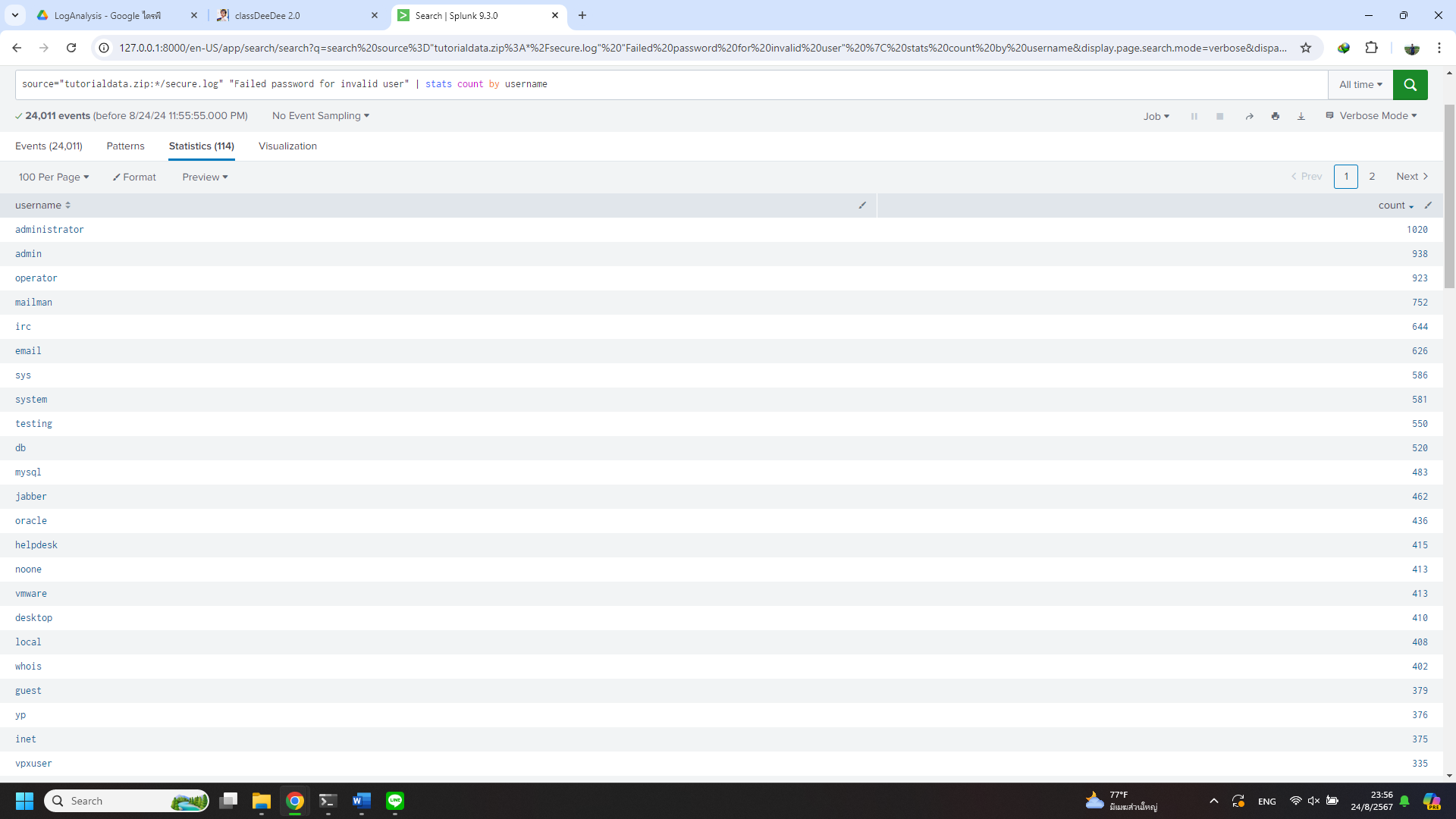
Ans. From 11/08/2024 to 18/08/2024 during 18:30:08 to 18:30:11 for all attempts.

Q3. Which server (mailsv, www1, www2, www3) had the most attempts?



Ans. This time regular expression for extract field generated by splunk working fine. So, this time I just count by newly extracted field name “server”. As the result of Server www1 with 6355 attempts.

Q4. What is the most popular account that hackers use to try to break in?

Ans. Extract username and result of user administrator 1020 attempts.