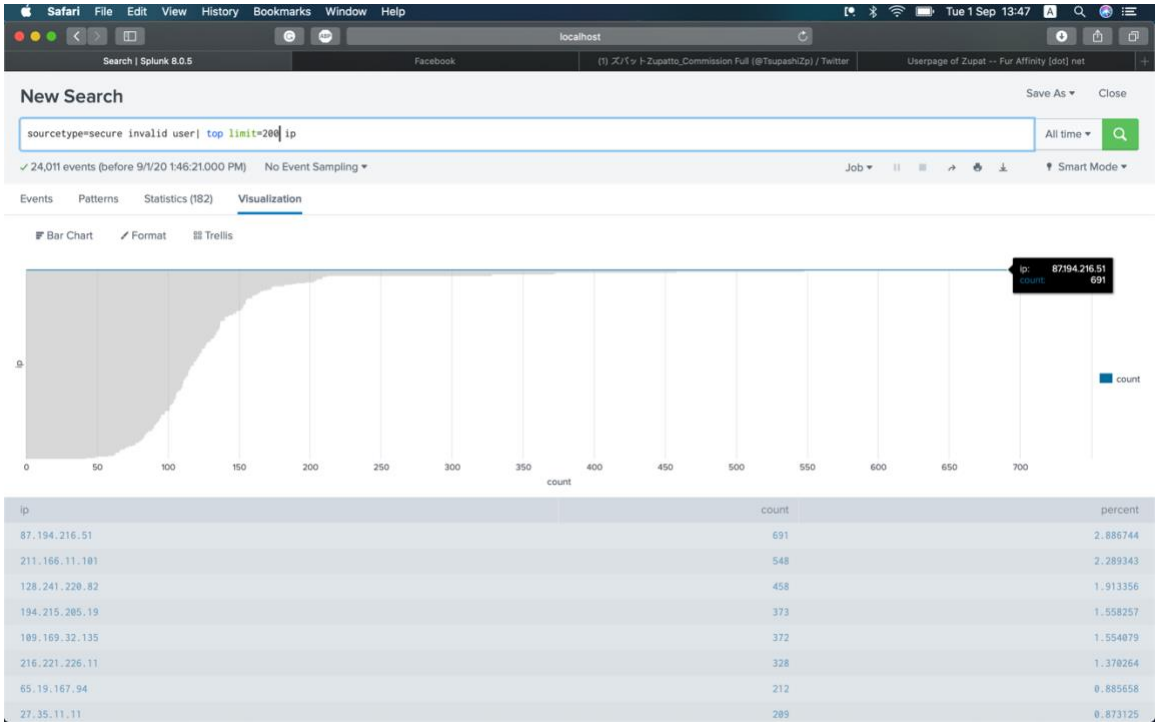
Phatcharapon Jumruspun 6031040921

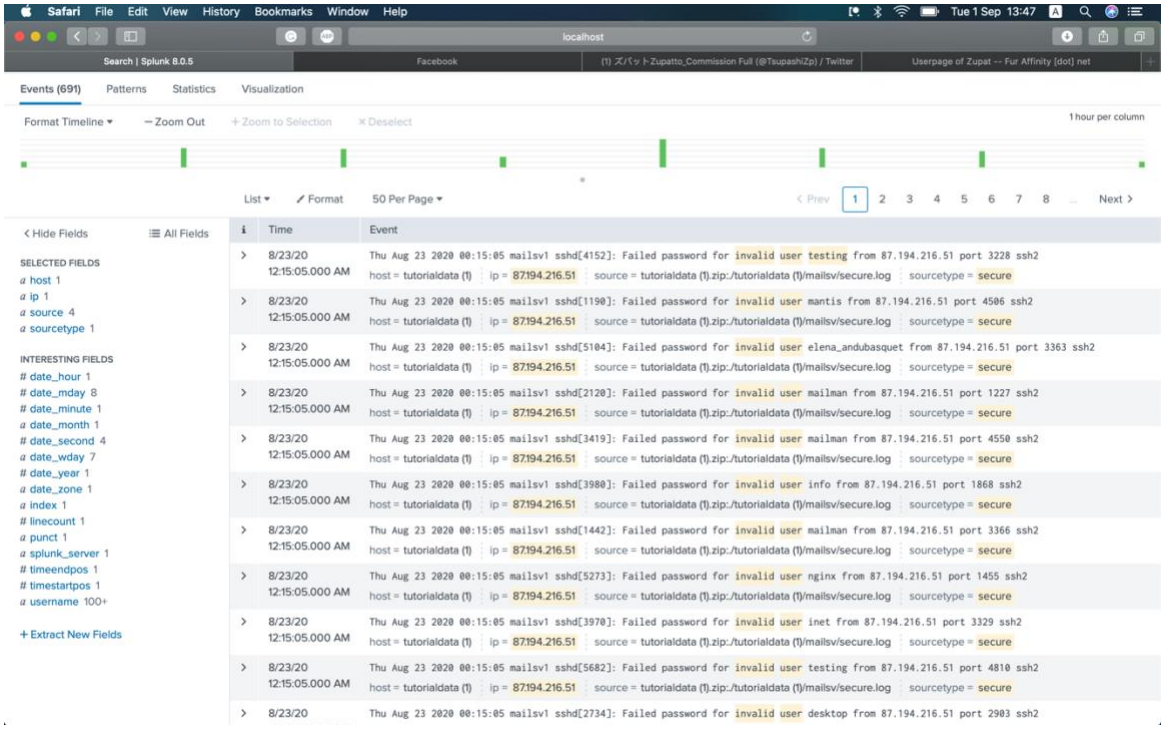
Activity-IV Log Analysis

Q1 - How many hackers are trying to get access to our servers? And how many attempts are there?

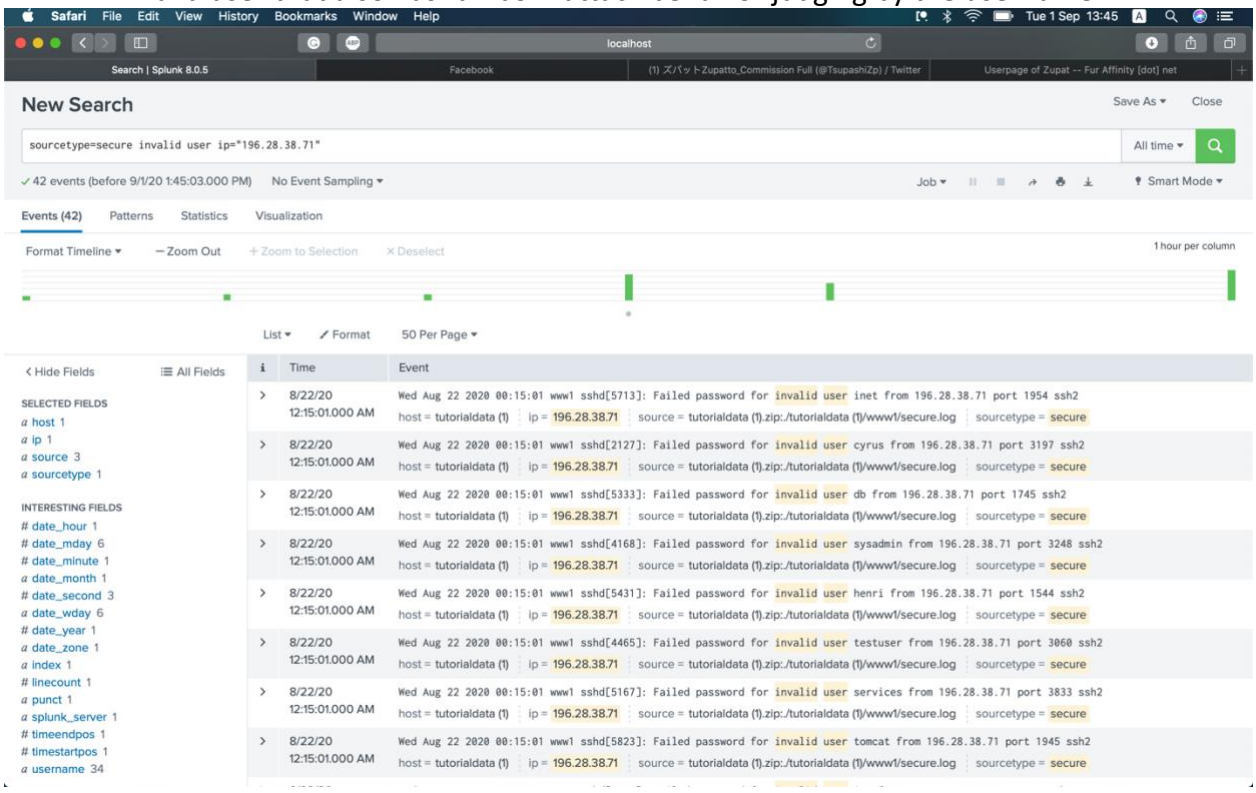
Query for “invalid user” attempts showed a lot of IP that is trying to rainbow-attack the servers. There are total of 182 different ips with 24011 attempts trying to log in with rainbow-attack behavior.



The picture below shows attempts from 87.194.216.51 which has the most attempt with invalid user, also has rainbow-attack behavior judging by the username



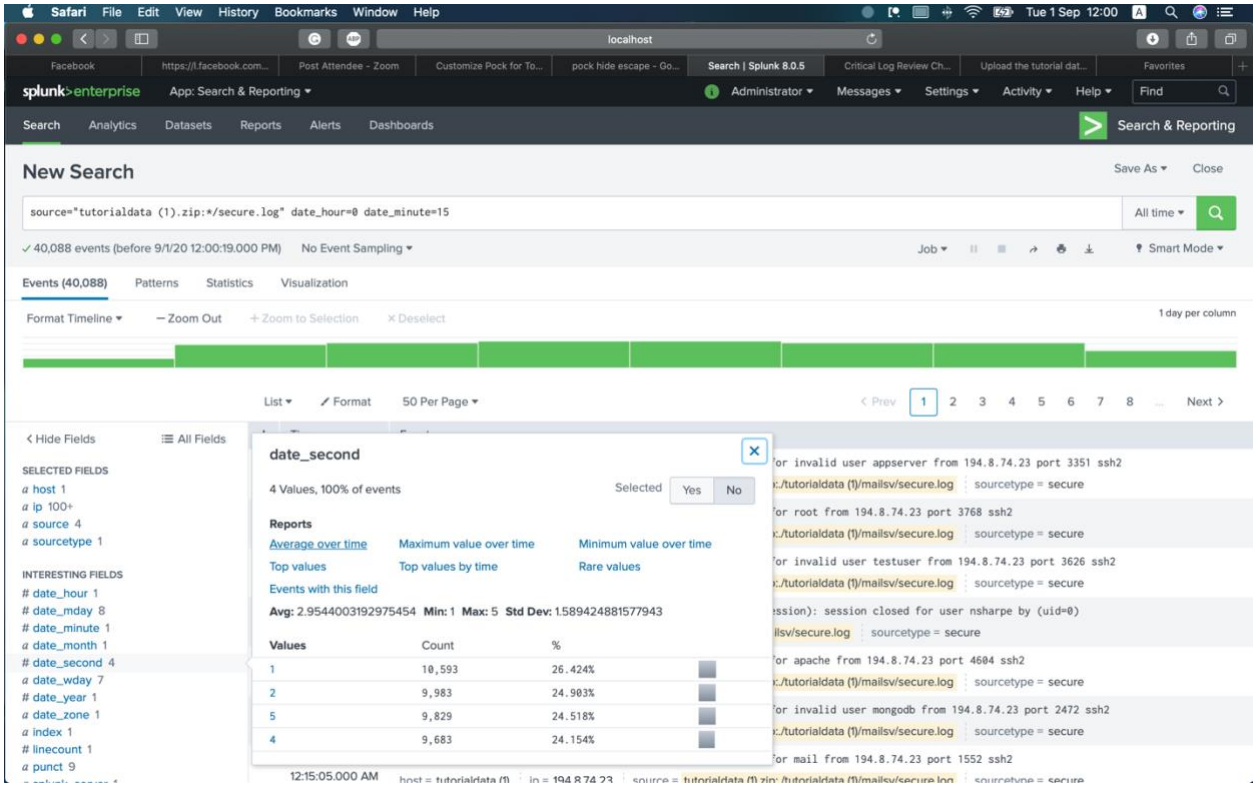
The picture below shows attempts from 196.28.38.71 which has the least attempt with invalid user that also has rainbow-attack behavior judging by the username



So it is safe to conclude that there are total of 182 hackers and 24011 attempts

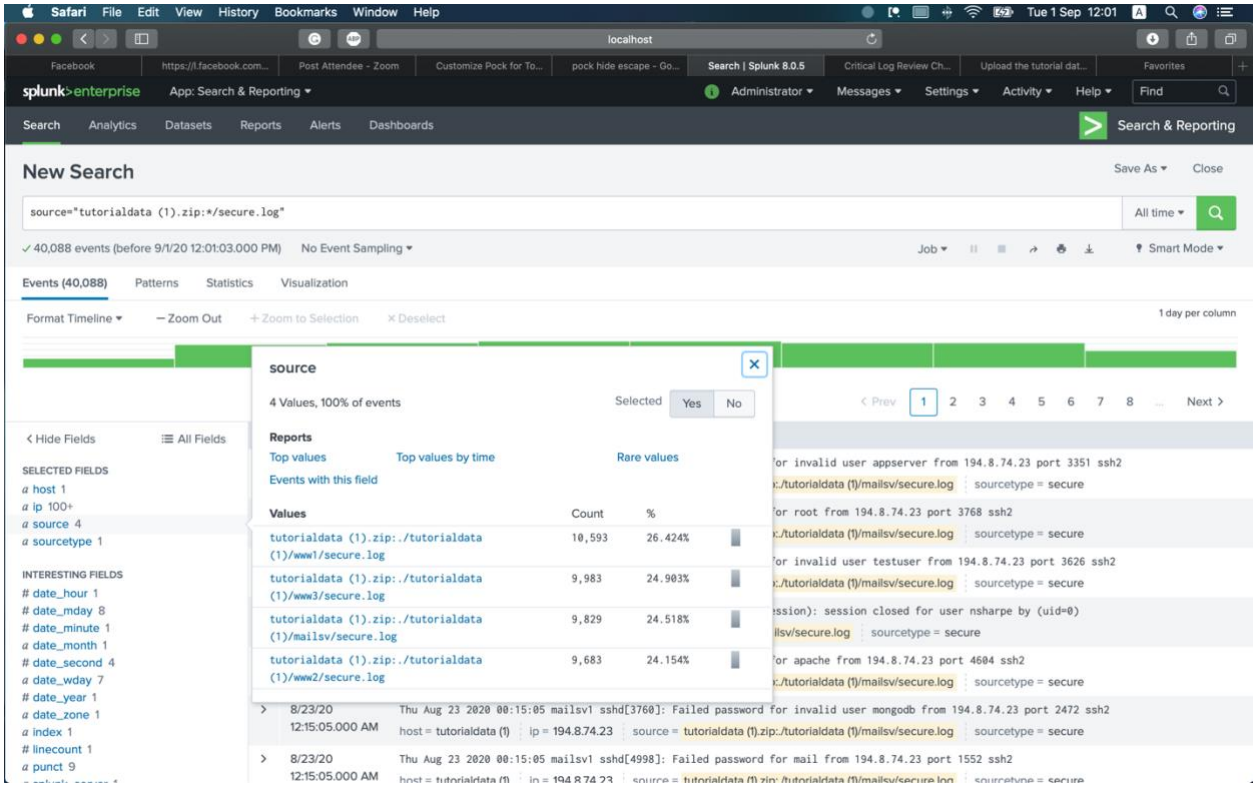
Q2

12:15 AM seems to be the most favorable time (almost the only time) that the hackers favor the most



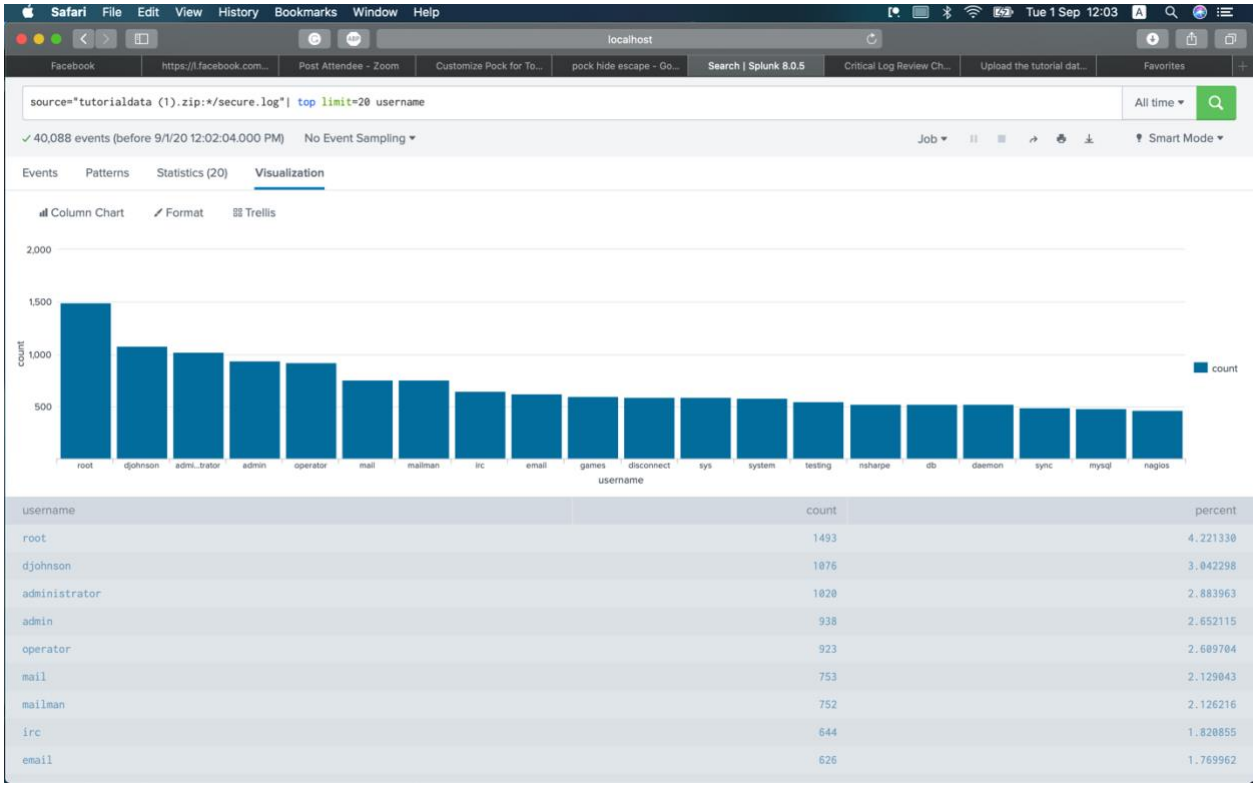
Q3

www1 seems to have most attempts (10593 attempts).



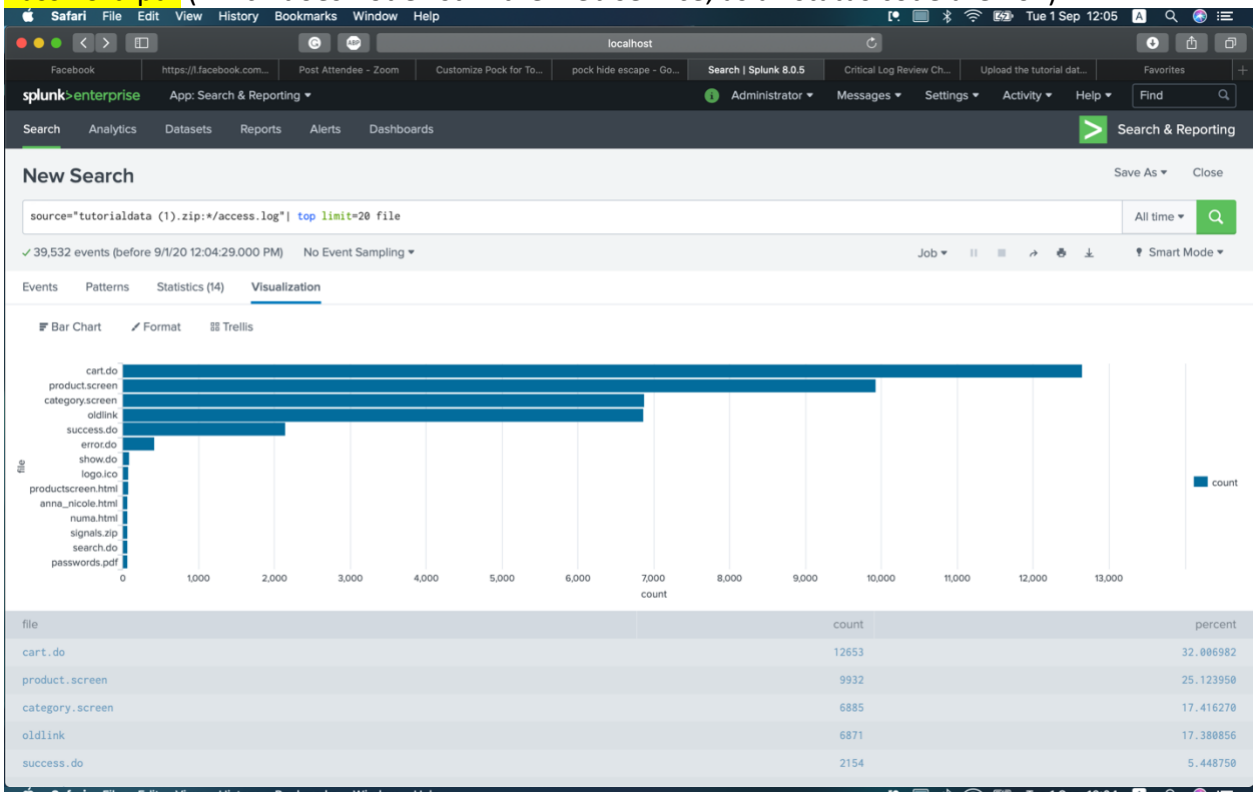
Q4

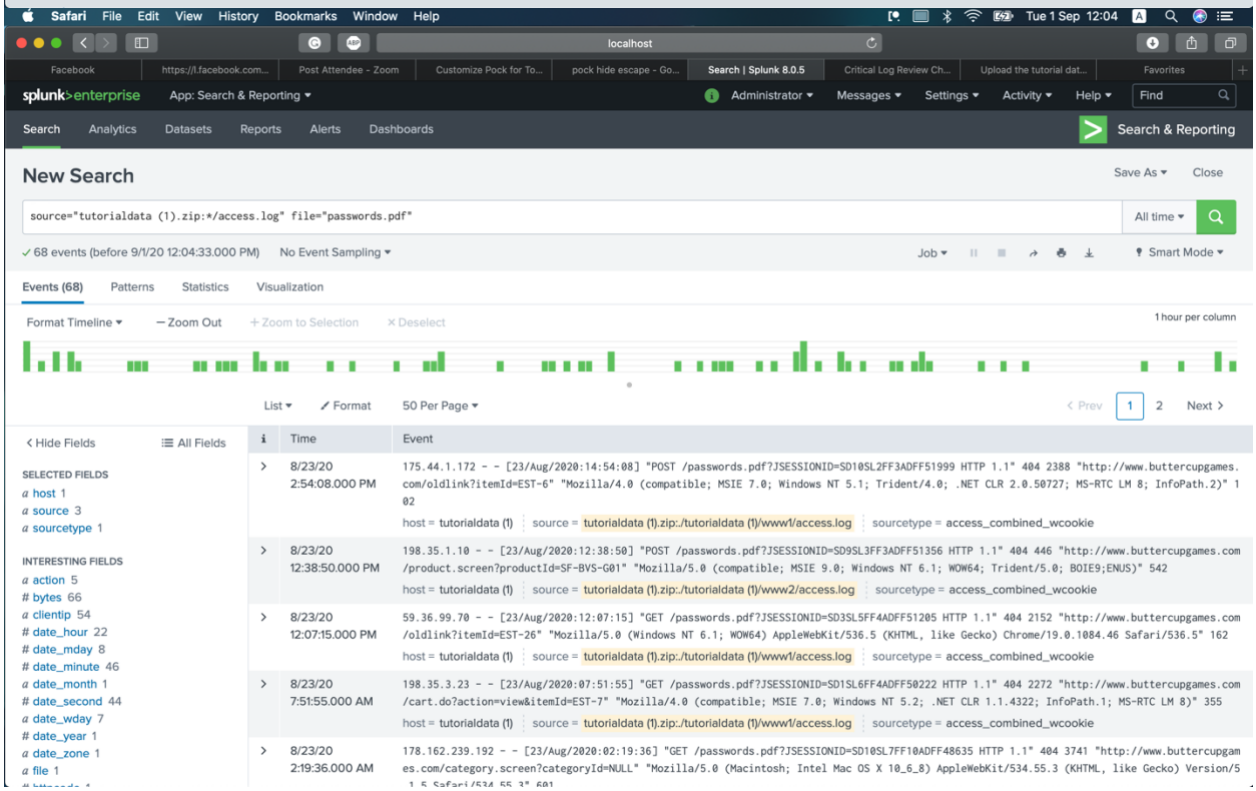
Most popular account would be root (1493 attempts).

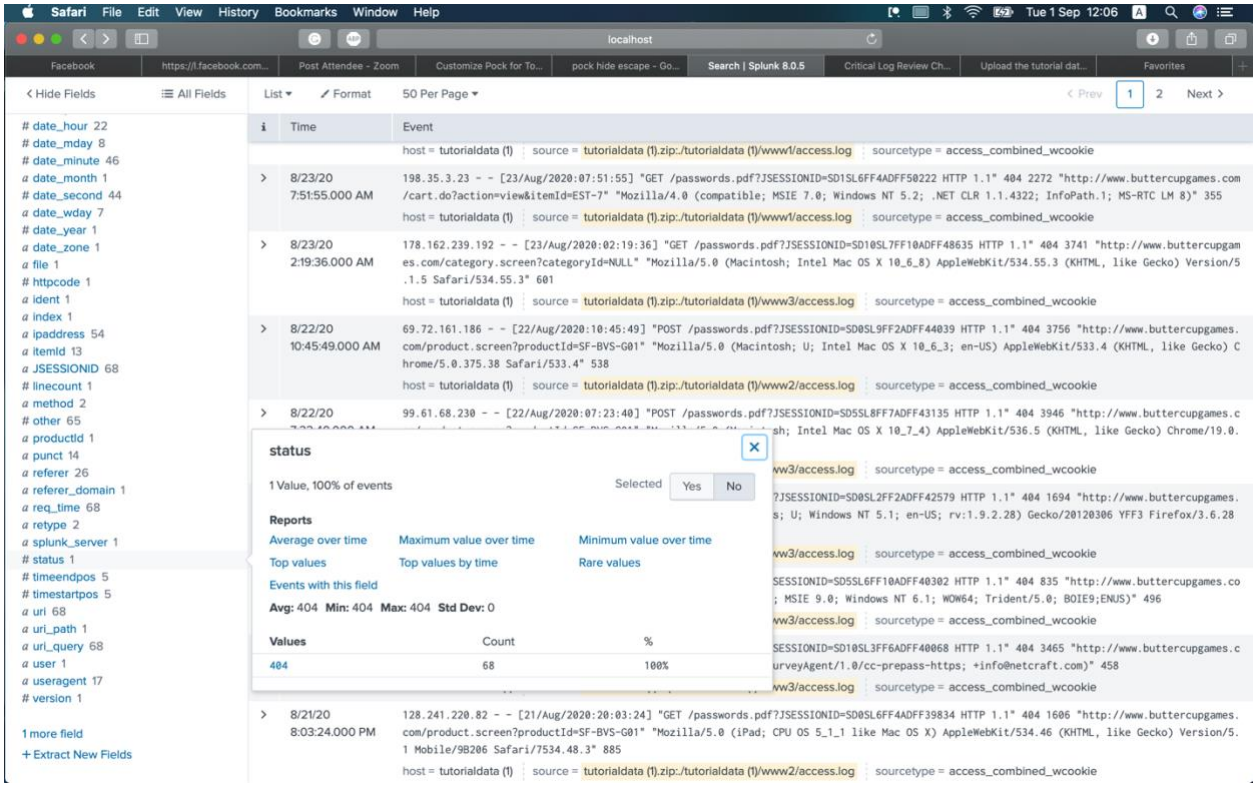


Q5

Password.pdf (which does not exist in the web service, as all status code are 404)







Q6

Password.pdf (reasoning in Q5 above)