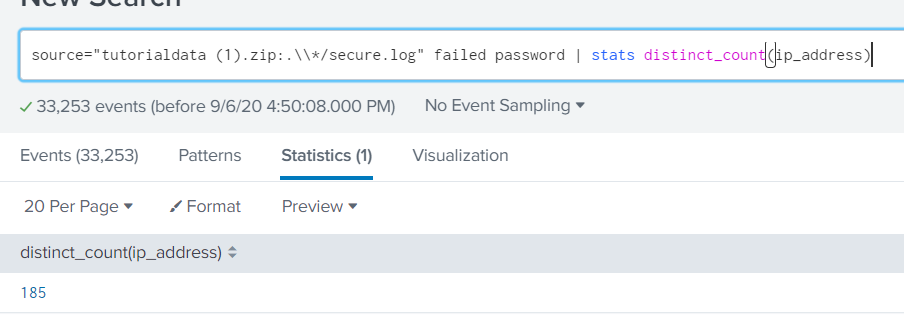
Part I. Can you find people trying to break into the servers?

Q1. How many hackers are trying to get access to our servers? And how many

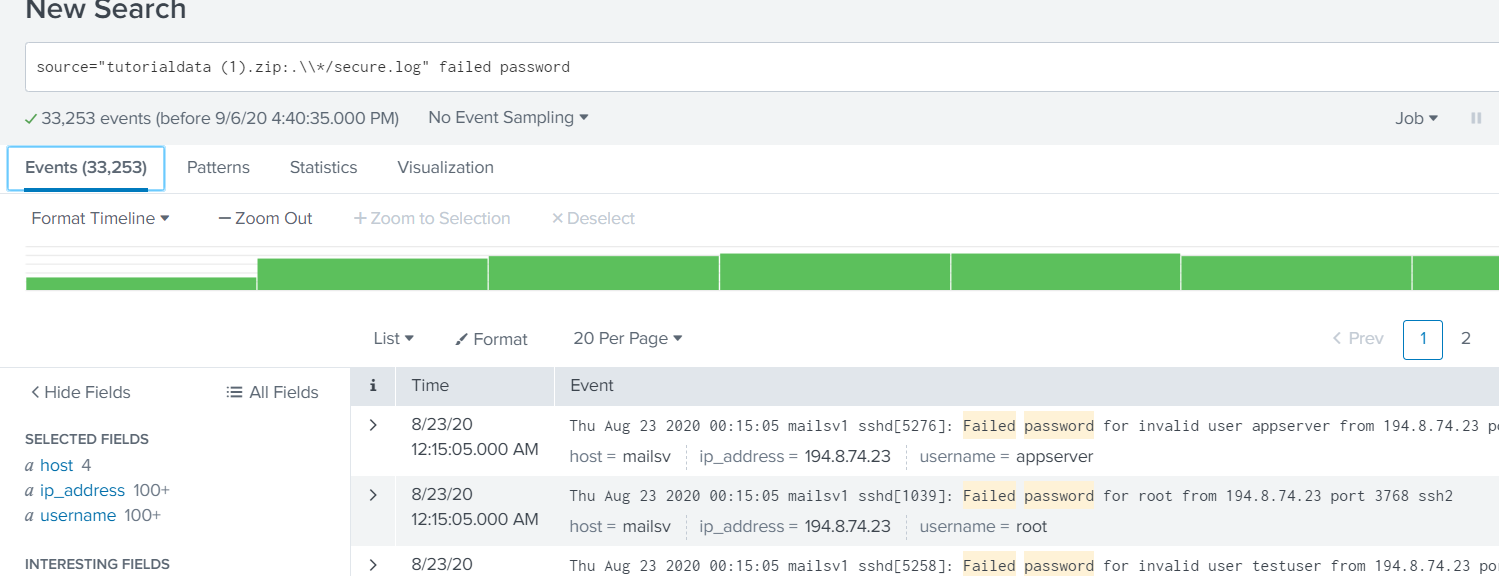
attempts are there?

Hackers: 185, Attempts: 33253

Command for counting hacker

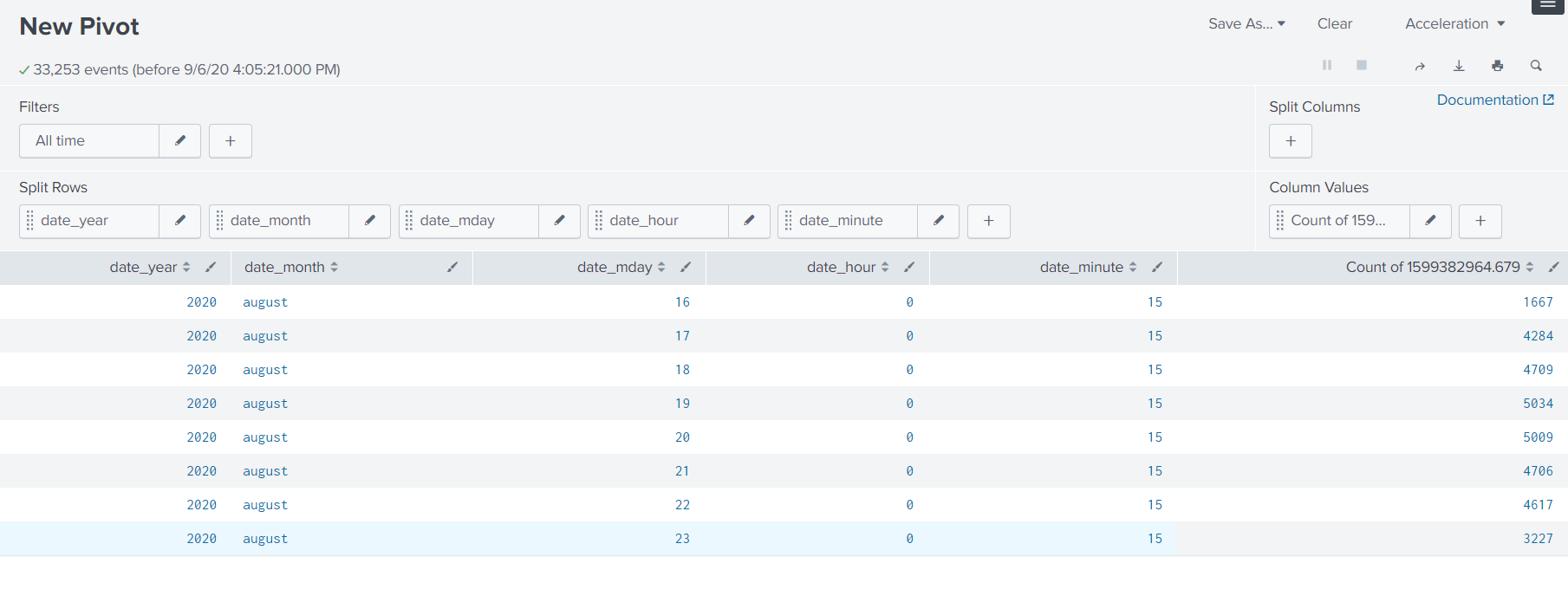


Command for counting attempts



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

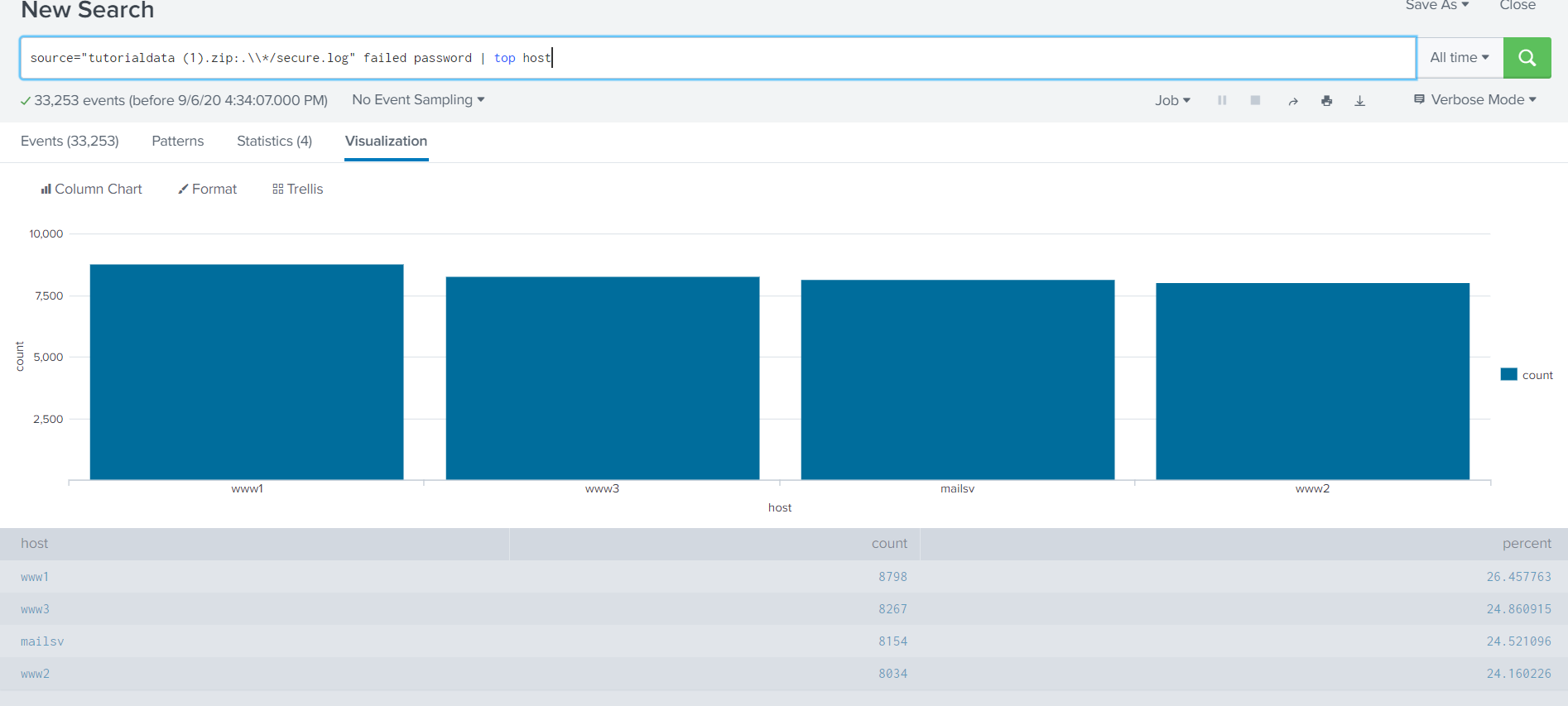
16-23 Aug 2020 00:15:01



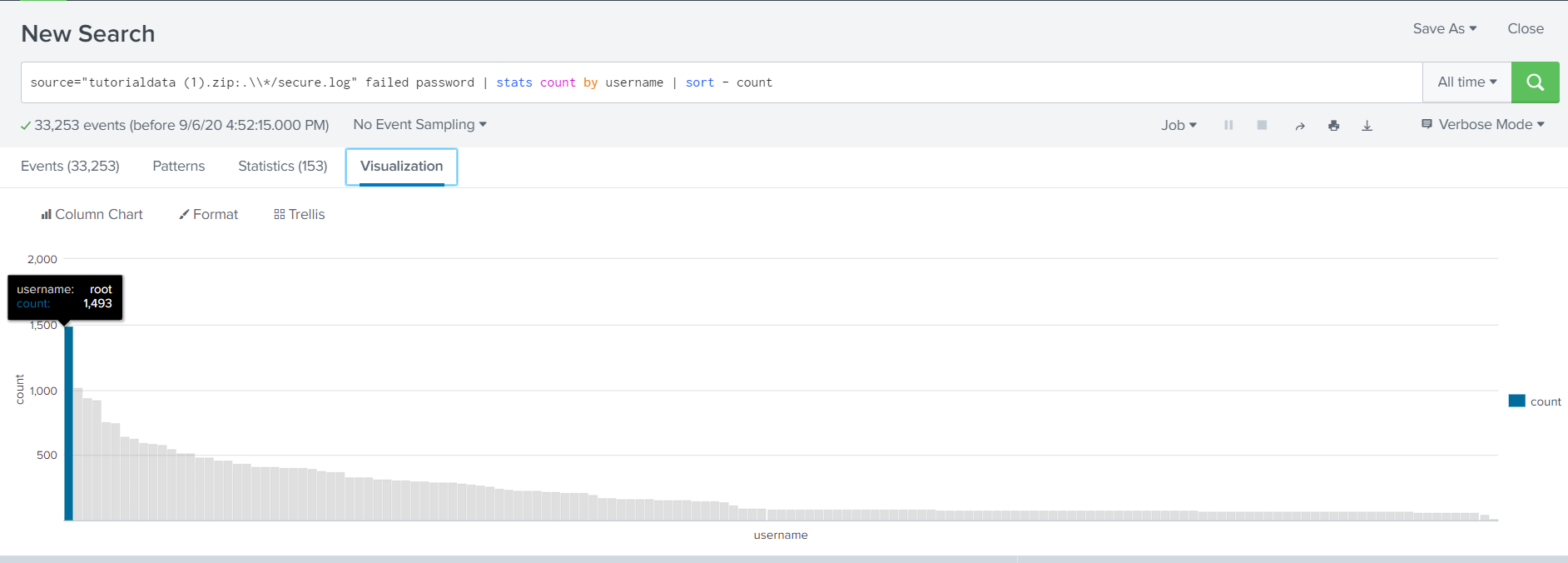
This result is visualized from search keyword “failed password”

Q3. Which server (mailsv, www1, www2, www3) seem to see the most attempts?

It’s equally distribute but www1 hold get most attempts



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

root

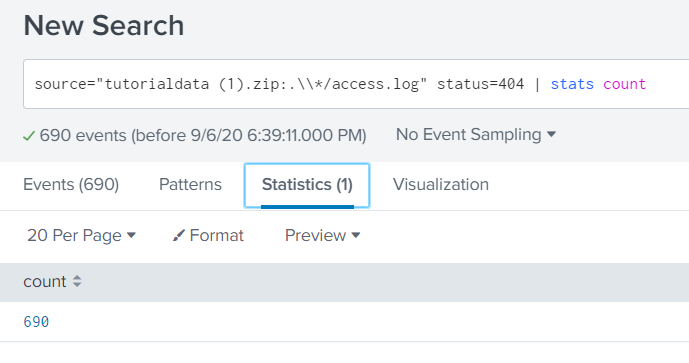
Part II. Sensitive Files on Web Servers

Q5. Can you find attempts to get access to sensitive information from our web

servers? How many attempts were there?

I guess that request not found (404) can infer hacker try to access to sensitive information without knowing endpoint.

Then there are 690 attempts.



Q6. What resource/file are hackers looking for?

List below are resources that they are looking for.

