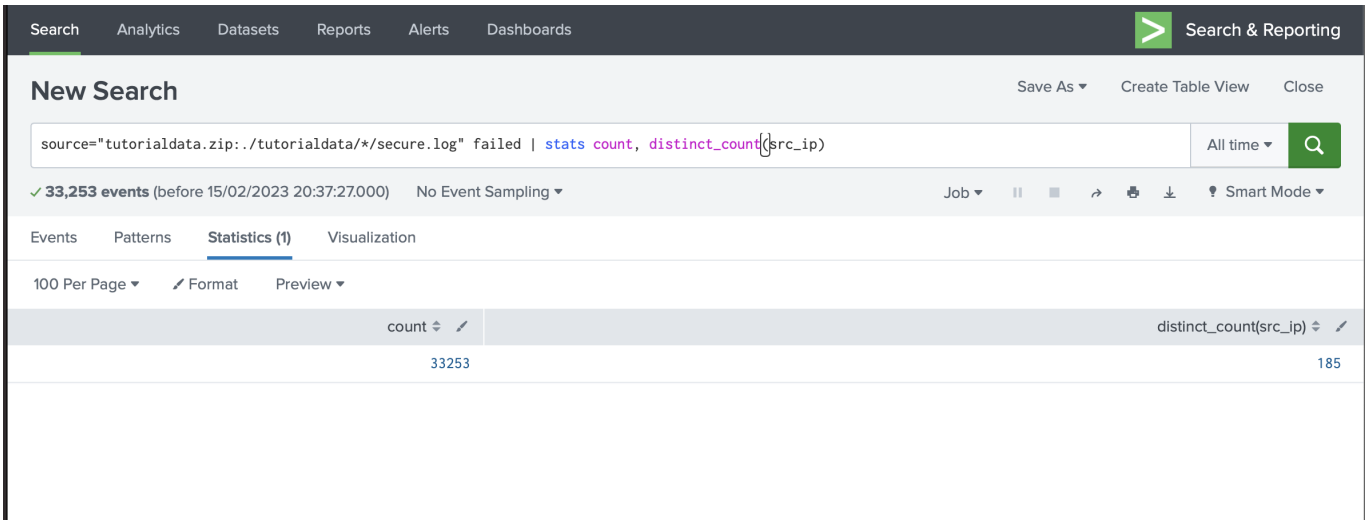
Activity 1: Can you find people trying to break into the servers?

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

Ans.

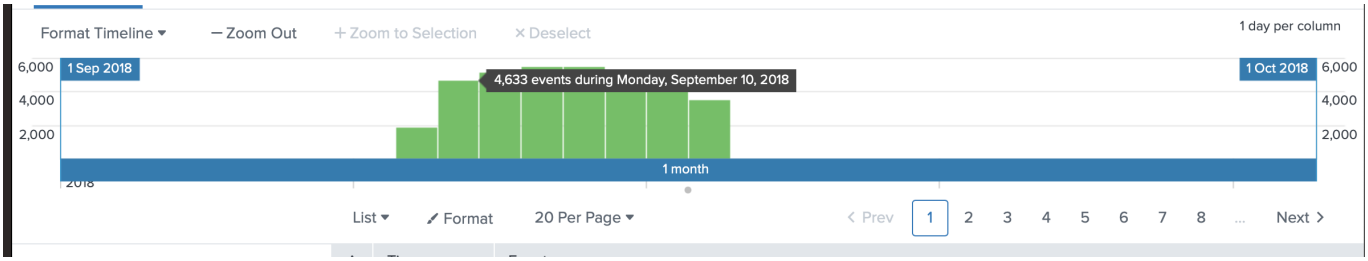
There is 185 hackers and 33253 times. using extra field by using regex (?P<src_ip>[^]+) port (?P<src_port>\d+)



1.2 What time do hackers appear to try to hack our servers?

Ans.

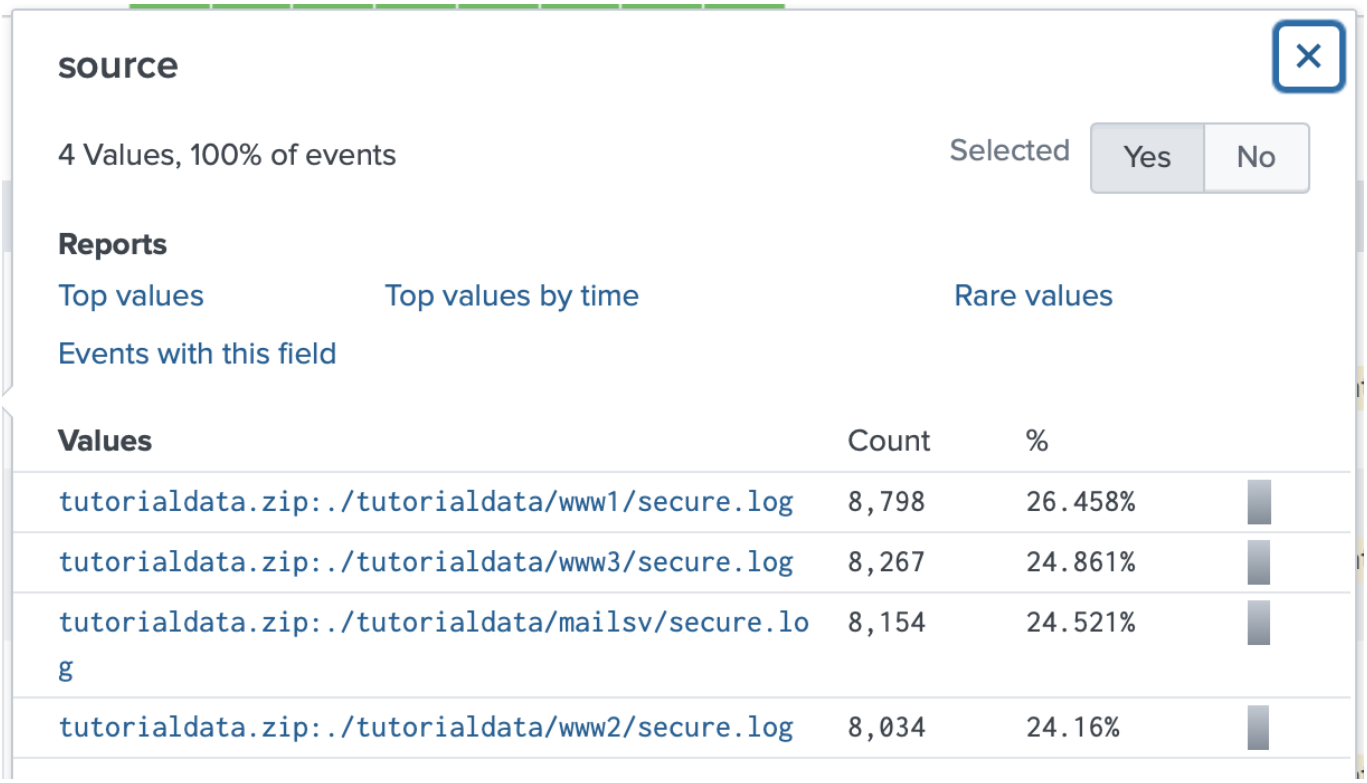
The hacking starts from 9 September to 17 September on every 12.15.05



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

Ans.

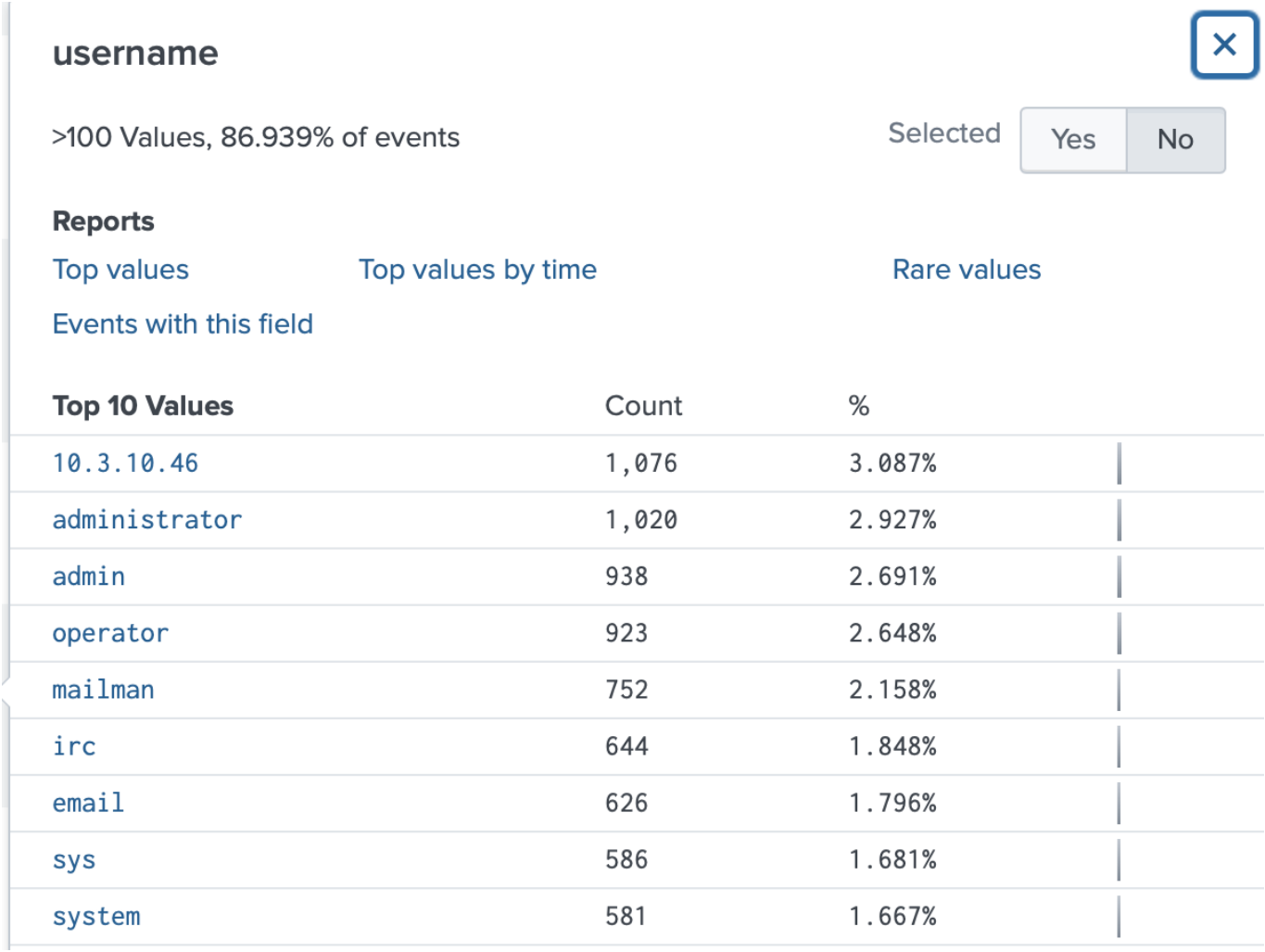
www1 has the most attempts with 8798 attemps



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

Ans.

The most popular account is 10.3.10.46

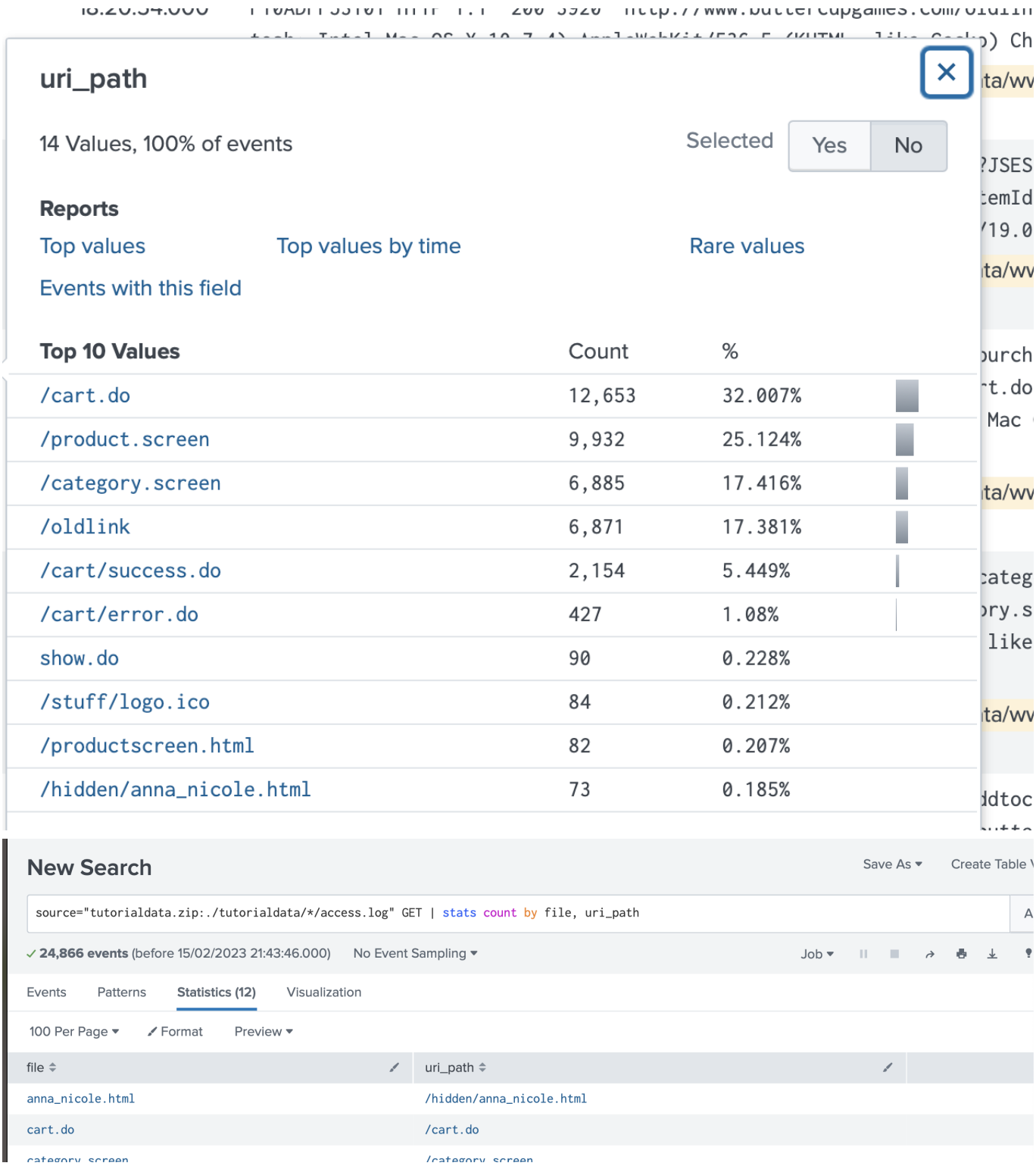


Top 10 Values	Count	%
10.3.10.46	1,076	3.087%
administrator	1,020	2.927%
admin	938	2.691%
operator	923	2.648%
mailman	752	2.158%
irc	644	1.848%
email	626	1.796%
sys	586	1.681%
system	581	1.667%

Activity 2: Sensitive Files on Web Servers

2.1 Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?

Ans. There are 2 files that are sensitive which are password.pdf (51 times for GET method) and anna_nicole.html (62 times for GET method)



2.2 What resource/file are hackers looking for?

Ans.

password.pdf and anna_nicole.html which is located in hidden folder.

Activity 3: (Optional)

Are there bots crawling our websites?

Ans.

Yes

3.2 Can you find any bots crawling our websites?

Yes, there are 2 bots which are YandexBot and GoogleBot