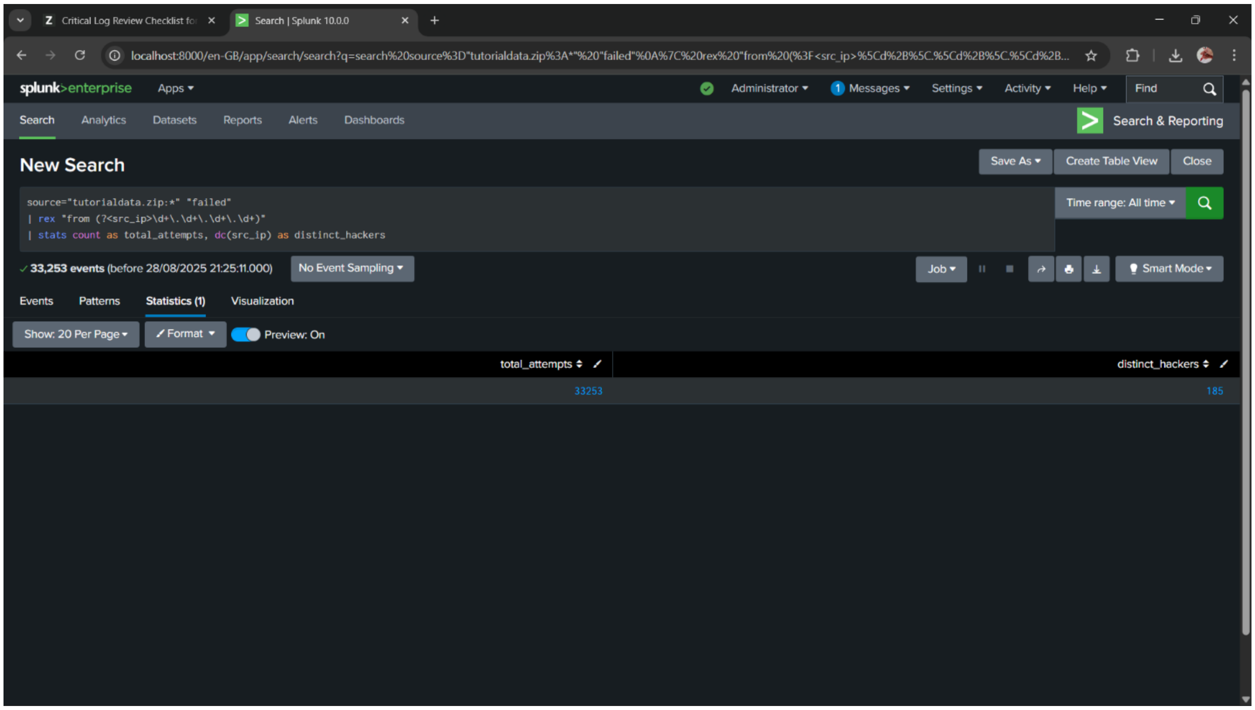
Com Sec Act 2 Splunk

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: #hacker=185, #attempt=33253



New Search

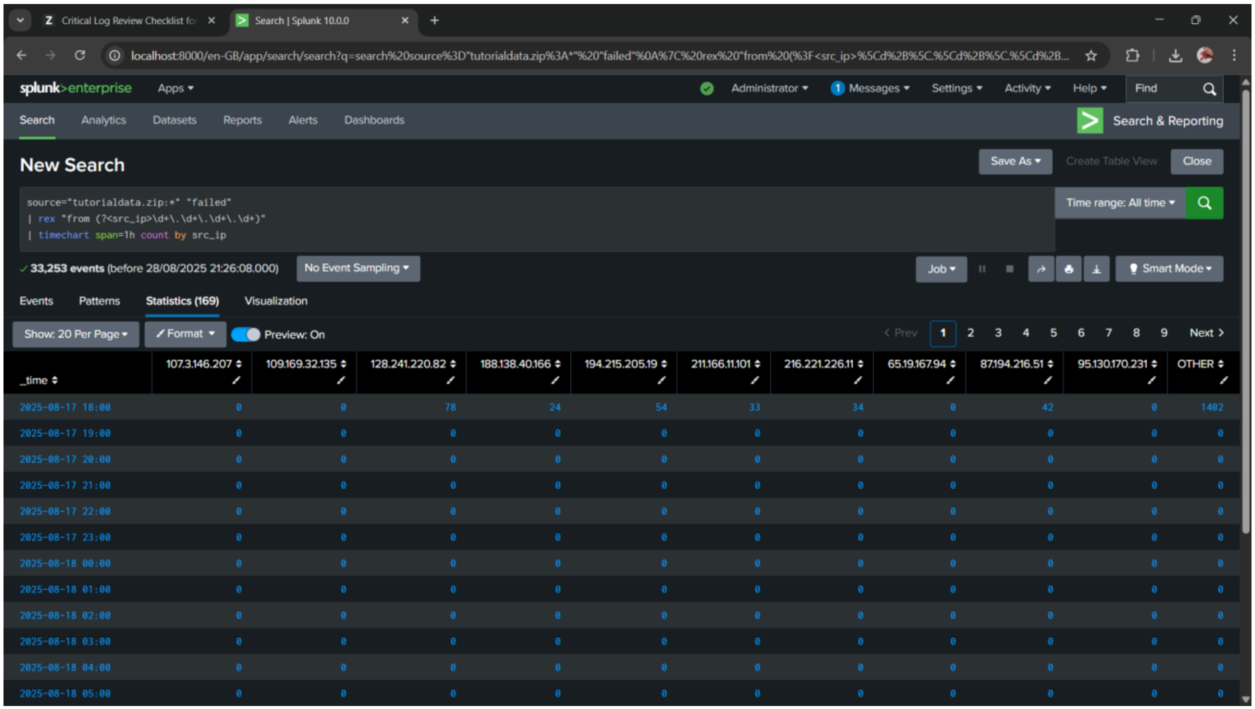
```
source="tutorialdata.zip:*" "failed"
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count as total_attempts, dc(src_ip) as distinct_hackers
```

✓ 33,253 events (before 28/08/2025 21:25:11.000)

total_attempts	distinct_hackers
33253	185

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

ANS: 2025-08-17 18:00, 2025-08-18 18:00, 2025-08-19 18:00,
2025-08-20 18:00, 2025-08-21 18:00, 2025-08-22 18:00,
2025-08-23 18:00, 2025-08-24 18:00

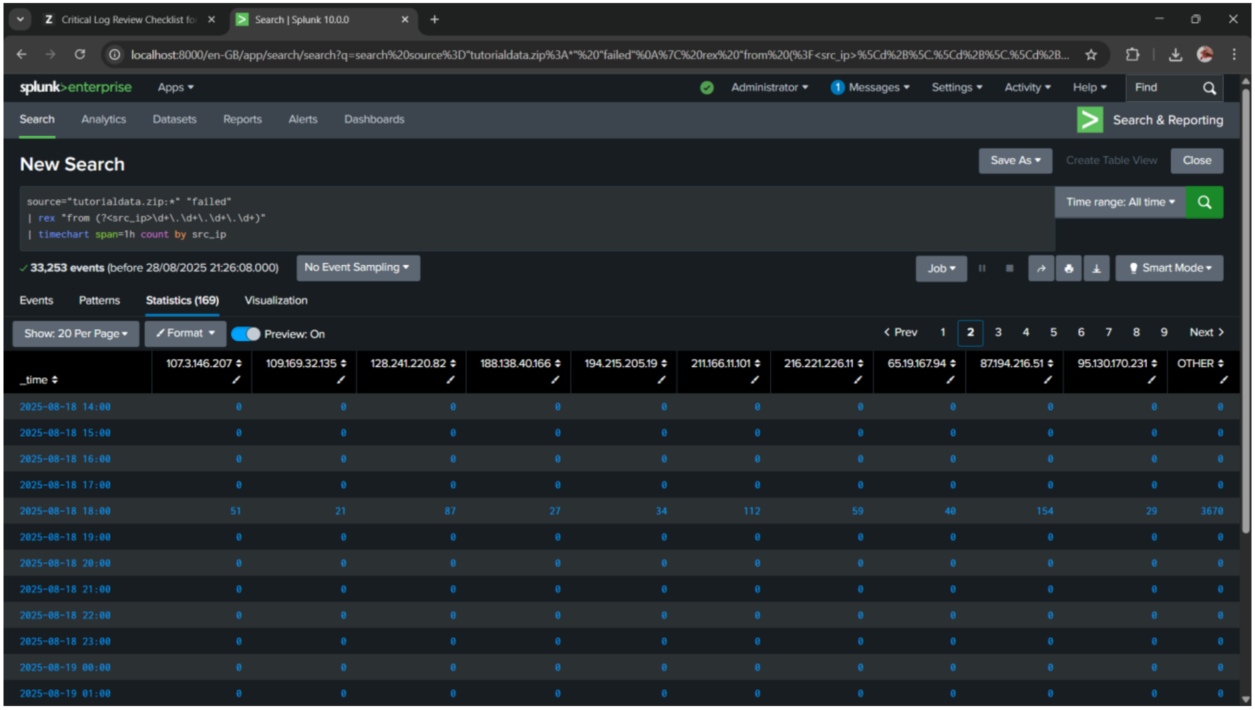


New Search

```
source="tutorialdata.zip:*" "failed"
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| timechart span=1h count by src_ip
```

✓ 33,253 events (before 28/08/2025 21:26:08.000)

_time	107.3.146.207	109.169.32.135	128.241.220.82	188.138.40.166	194.215.205.19	211.166.11.101	216.221.226.11	65.19.167.94	87.194.216.51	95.130.170.231	OTHER
2025-08-17 18:00	0	0	78	24	54	33	34	0	42	0	1402
2025-08-17 19:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-17 20:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-17 21:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-17 22:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-17 23:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 00:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 01:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 02:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 03:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 04:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 05:00	0	0	0	0	0	0	0	0	0	0	0



New Search

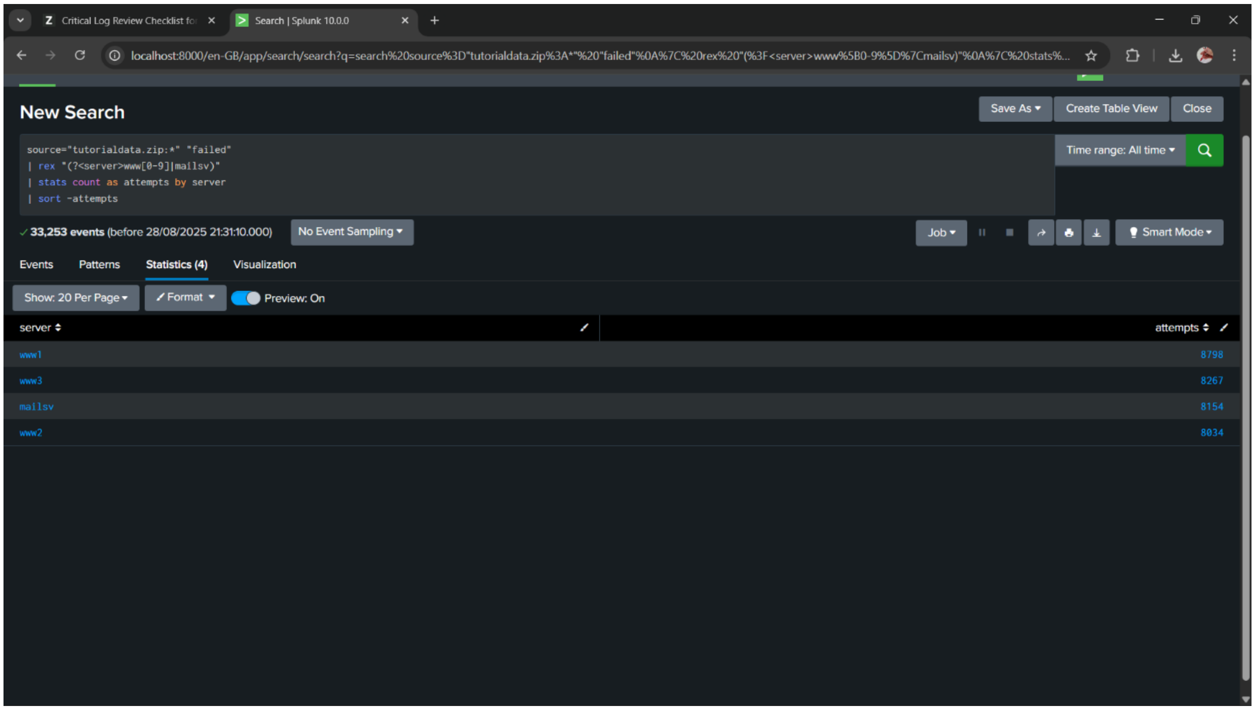
```
source="tutorialdata.zip:*" "failed"
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| timechart span=1h count by src_ip
```

✓ 33,253 events (before 28/08/2025 21:26:08.000)

_time	107.3.146.207	109.169.32.135	128.241.220.82	188.138.40.166	194.215.205.19	211.166.11.101	216.221.226.11	65.19.167.94	87.194.216.51	95.130.170.231	OTHER
2025-08-18 14:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 15:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 16:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 17:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 18:00	51	21	87	27	34	112	59	40	154	29	3670
2025-08-18 19:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 20:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 21:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 22:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-18 23:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-19 00:00	0	0	0	0	0	0	0	0	0	0	0
2025-08-19 01:00	0	0	0	0	0	0	0	0	0	0	0

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

ANS: www1



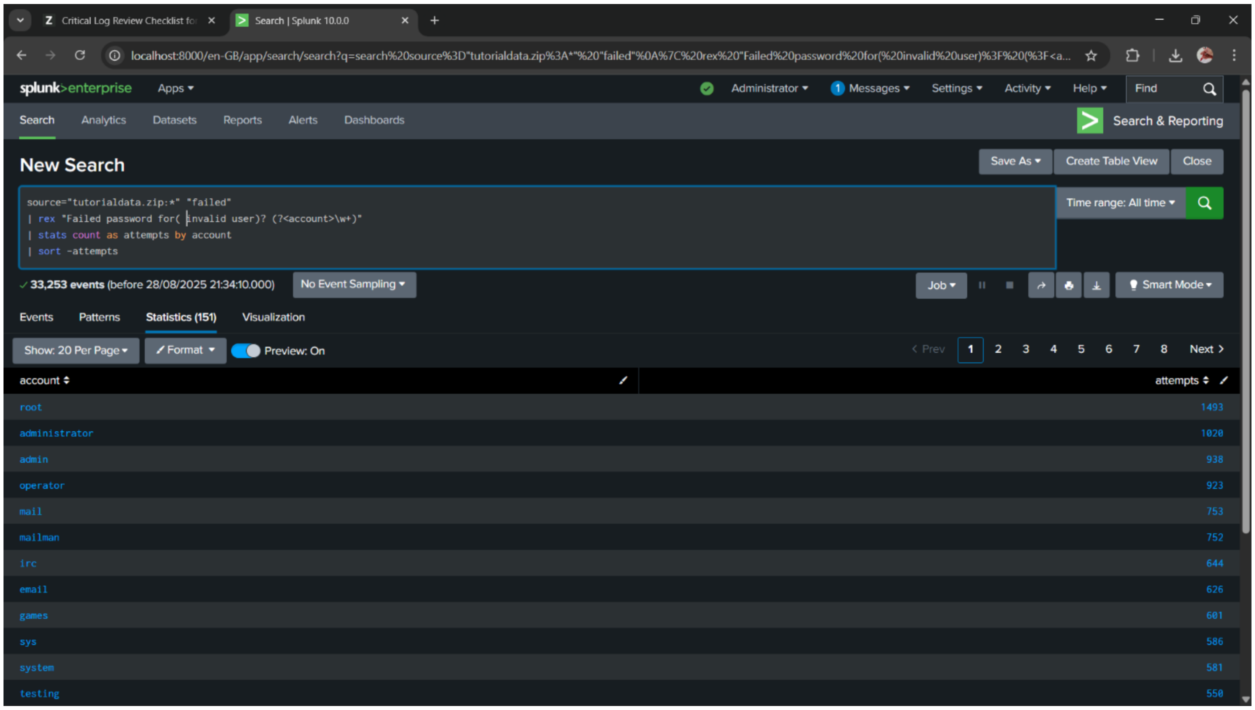
```
source="tutorialdata.zip:*" "failed"
| rex "(?<server>www[0-9]|mailsv)"
| stats count as attempts by server
| sort -attempts
```

✓ 33,253 events (before 28/08/2025 21:31:10.000)

server	attempts
www1	8798
www3	8267
mailsv	8154
www2	8034

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

ANS: root



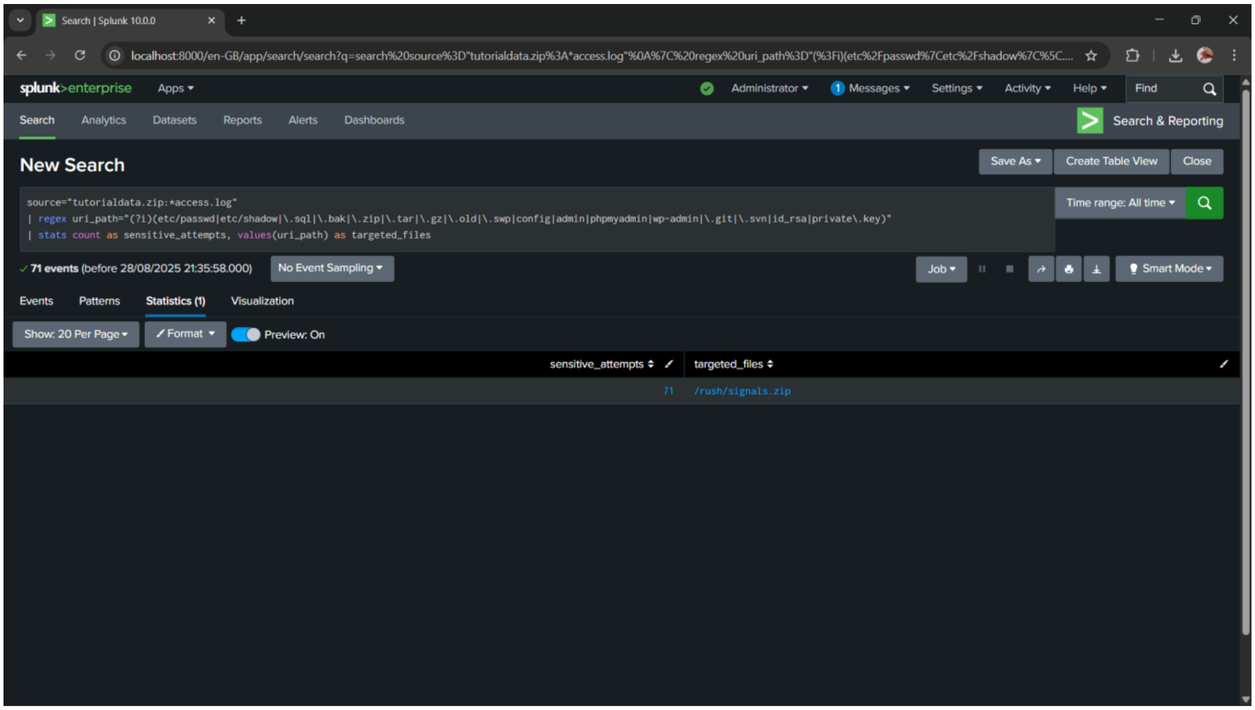
```
source="tutorialdata.zip:*" "failed"
| rex "Failed password for( invalid user)? (?<account>\w+)"
| stats count as attempts by account
| sort -attempts
```

✓ 33,253 events (before 28/08/2025 21:34:10.000)

account	attempts
root	1493
administrator	1020
admin	938
operator	923
mail	753
mailman	752
irc	644
email	626
games	601
sys	586
system	581
testing	550

Q5. Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?

ANS: 71 times



```
source="tutorialdata.zip:*access.log"
| regex uri_path="(?i)(etc/passwd|etc/shadow|\.sql|\.bak|\.zip|\.tar|\.gz|\.old|\.swp|config|admin|phpmyadmin|wp-admin|\.git|\.svn|id_rsa|private\.key)"
| stats count as sensitive_attempts, values(uri_path) as targeted_files
```

✓ 71 events (before 28/08/2025 21:35:58.000) No Event Sampling

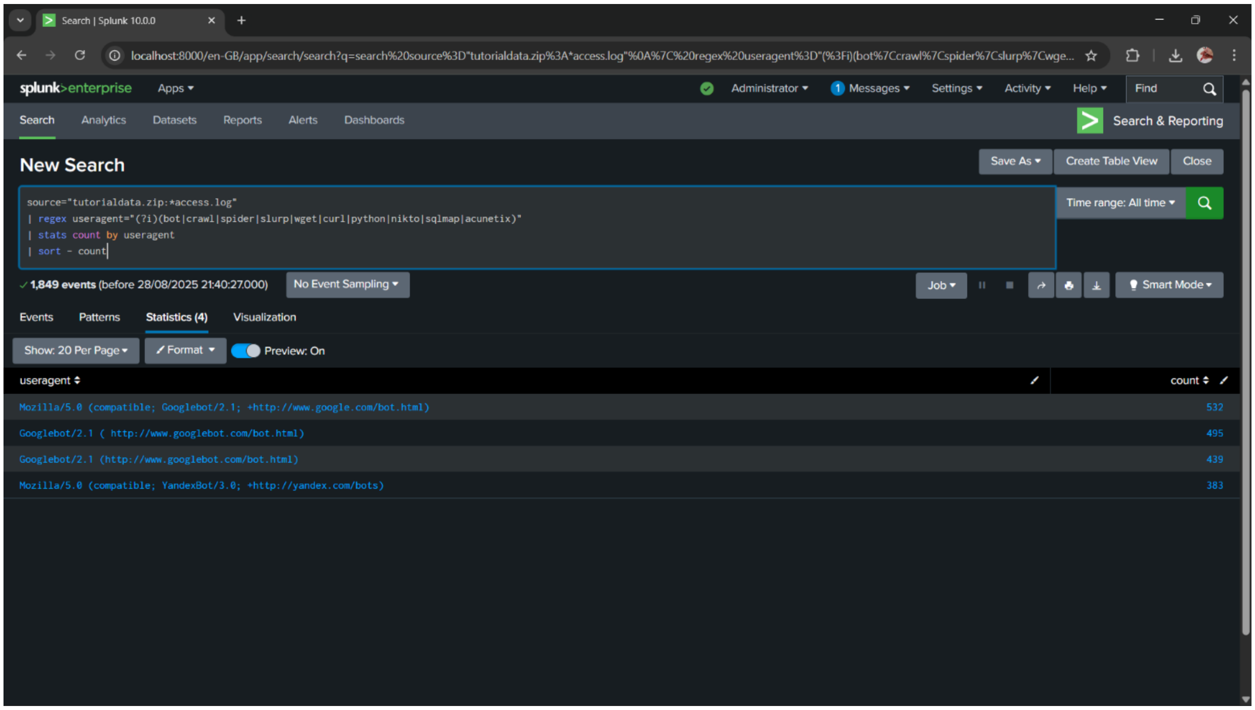
sensitive_attempts	targeted_files
71	/rush/signals.zip

Q6. What resource/file are hackers looking for?

ANS: /rush/signals.zip

Q7. Can you find any bots crawling our websites?

ANS: YES



New Search

```
source="tutorialdata.zip:*access.log"
| regex useragent="(?i)(bot|crawl|spider|slurp|wget|curl|python|nikto|sqlmap|acunetix)"
| stats count by useragent
| sort - count
```

✓ 1,849 events (before 28/08/2025 21:40:27.000)

useragent	count
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	532
Googlebot/2.1 (http://www.googlebot.com/bot.html)	495
Googlebot/2.1 (http://www.googlebot.com/bot.html)	439
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	383

Q8. What are they doing on the site? (Hint: Look for User-Agent in the web access.logs.)

ANS: Bots are crawling the site to index pages for search engines.