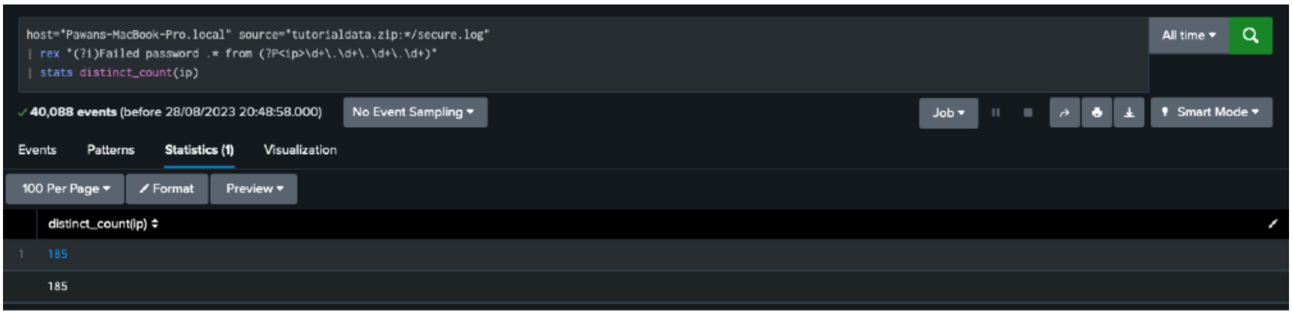
Activity 2

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.

There’re 185 distinct hackers

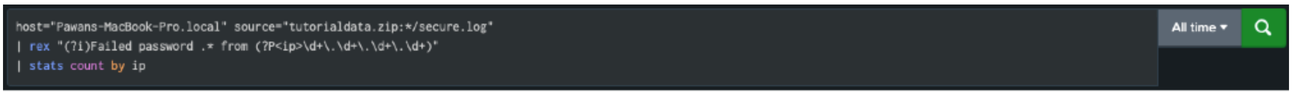


```
host="Pawans-MacBook-Pro.local" source="tutorialdata.zip:*/secure.log"
| rex "(?i)Failed password .* from (?P<ip>\d+\.\d+\.\d+\.\d+)"
| stats distinct_count(ip)
```

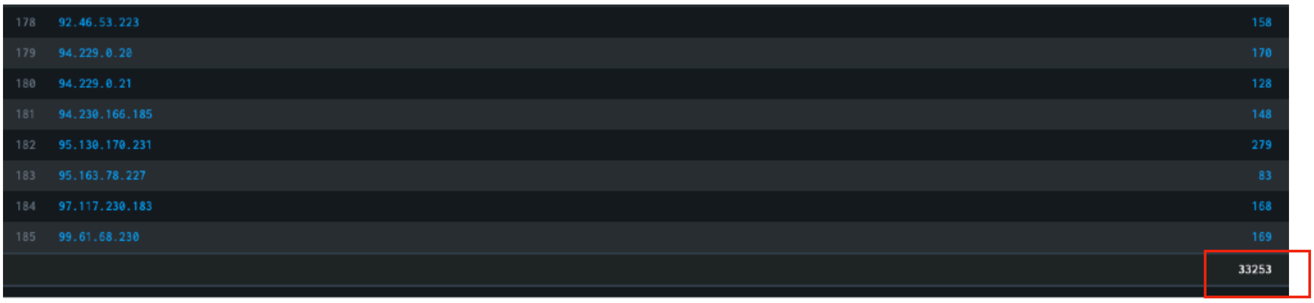
✓ **40,088 events** (before 28/08/2023 20:48:58.000) No Event Sampling ▾

	distinct_count(ip)
1	185
	185

There’re 33,253 attempts



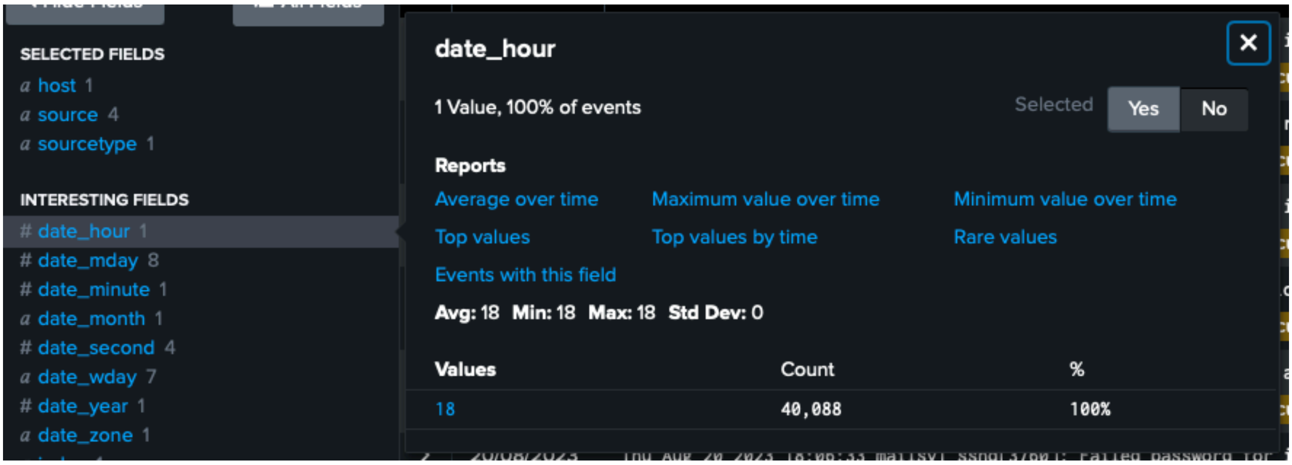
```
host="Pawans-MacBook-Pro.local" source="tutorialdata.zip:*/secure.log"
| rex "(?i)Failed password .* from (?P<ip>\d+\.\d+\.\d+\.\d+)"
| stats count by ip
```



178	92.46.53.223	158
179	94.229.0.20	170
180	94.229.0.21	128
181	94.230.166.185	148
182	95.130.170.231	279
183	95.163.78.227	83
184	97.117.230.183	168
185	99.61.68.230	169
		33253

Solution : Query in every secure.log file and look for distinct ip with many attempts

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



SELECTED FIELDS

- *a* host 1
- *a* source 4
- *a* sourcetype 1

INTERESTING FIELDS

- # date_hour 1
- # date_mday 8
- # date_minute 1
- *a* date_month 1
- # date_second 4
- *a* date_wday 7
- # date_year 1
- *a* date_zone 1

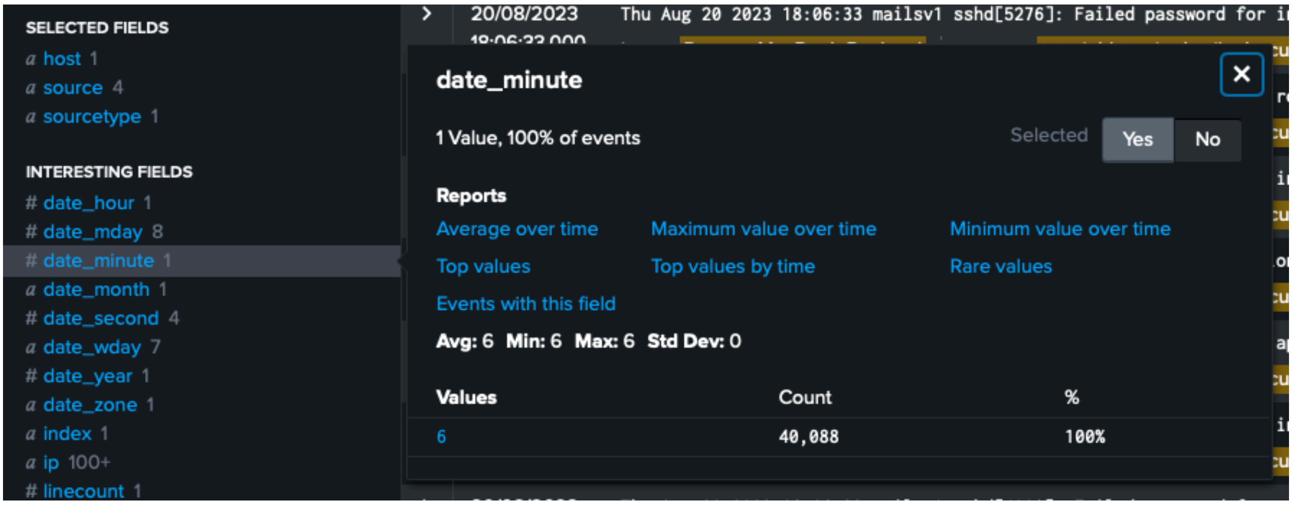
date_hour

1 Value, 100% of events

Reports

Avg: 18 **Min:** 18 **Max:** 18 **Std Dev:** 0

Values	Count	%
18	40,088	100%



```
20/08/2023    Thu Aug 20 2023 18:06:33 mailsv1 sshd[5276]: Failed password for i
18:06:33.000
```

SELECTED FIELDS

- *a* host 1
- *a* source 4
- *a* sourcetype 1

INTERESTING FIELDS

- # date_hour 1
- # date_mday 8
- # date_minute 1
- *a* date_month 1
- # date_second 4
- *a* date_wday 7
- # date_year 1
- *a* date_zone 1
- *a* index 1
- *a* ip 100+
- # linecount 1

date_minute

1 Value, 100% of events

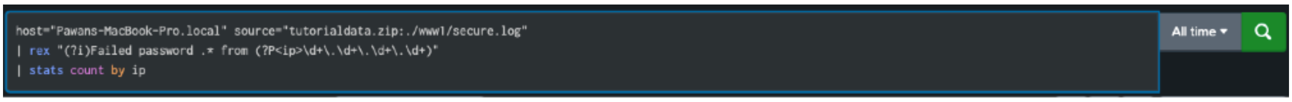
Reports

Avg: 6 **Min:** 6 **Max:** 6 **Std Dev:** 0

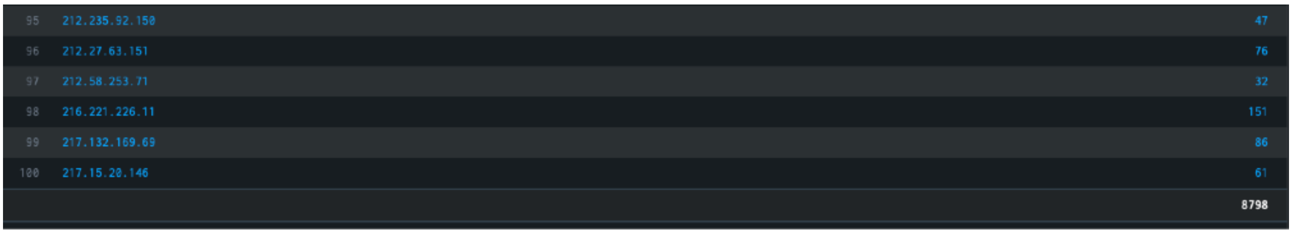
Values	Count	%
6	40,088	100%

Every attempts is 18 hours and 6 minutes or at 18.06

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



```
host="Pawans-MacBook-Pro.local" source="tutorialdata.zip:./www1/secure.log"
| rex "(?i)Failed password .* from (?P<ip>\d+\.\d+\.\d+\.\d+)"
| stats count by ip
```

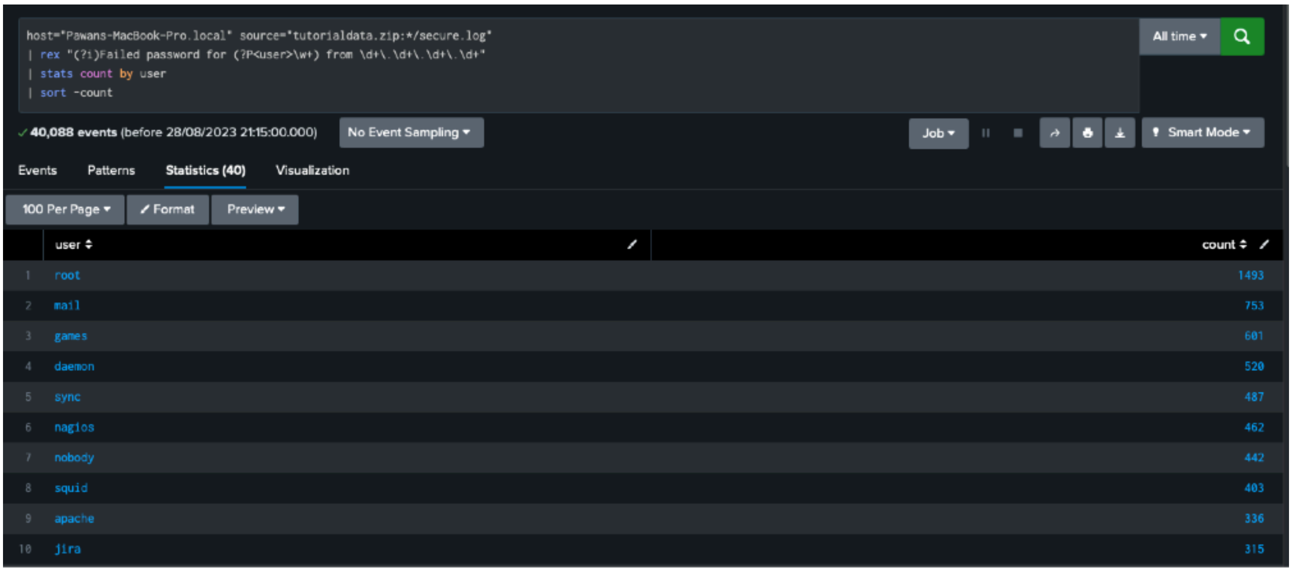


95	212.235.92.150	47
96	212.27.63.151	76
97	212.58.253.71	32
98	216.221.226.11	151
99	217.132.169.69	86
100	217.15.20.146	61
		8798

mailsv = 8154, www1 = 8798, www2 = 8034, www3 = 8267

www1 has the most attempts

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



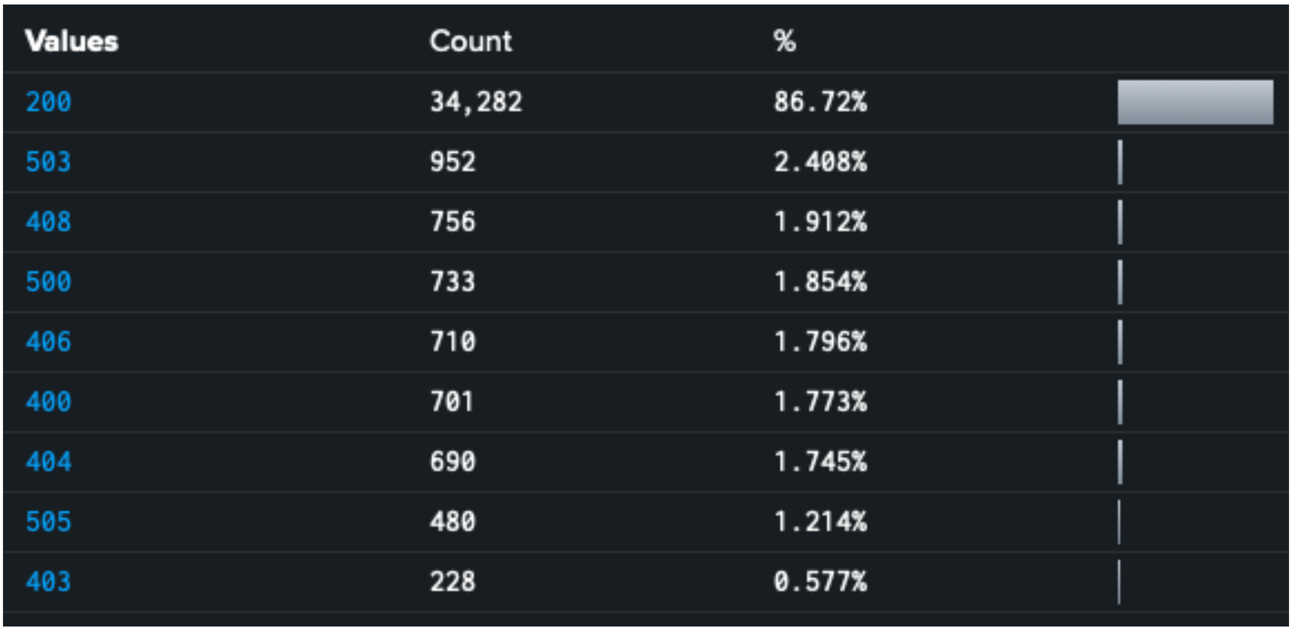
```
host="Pawans-MacBook-Pro.local" source="tutorialdata.zip:*/secure.log"
| rex "(?i)Failed password for (?P<user>\w+) from \d+\.\d+\.\d+\.\d+"
| stats count by user
| sort -count
```

✓ 40,088 events (before 28/08/2023 21:15:00.000)

	user	count
1	root	1493
2	mail	753
3	games	601
4	daemon	520
5	sync	487
6	nagios	462
7	nobody	442
8	squid	403
9	apache	336
10	jira	315

The most popular is "root"

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

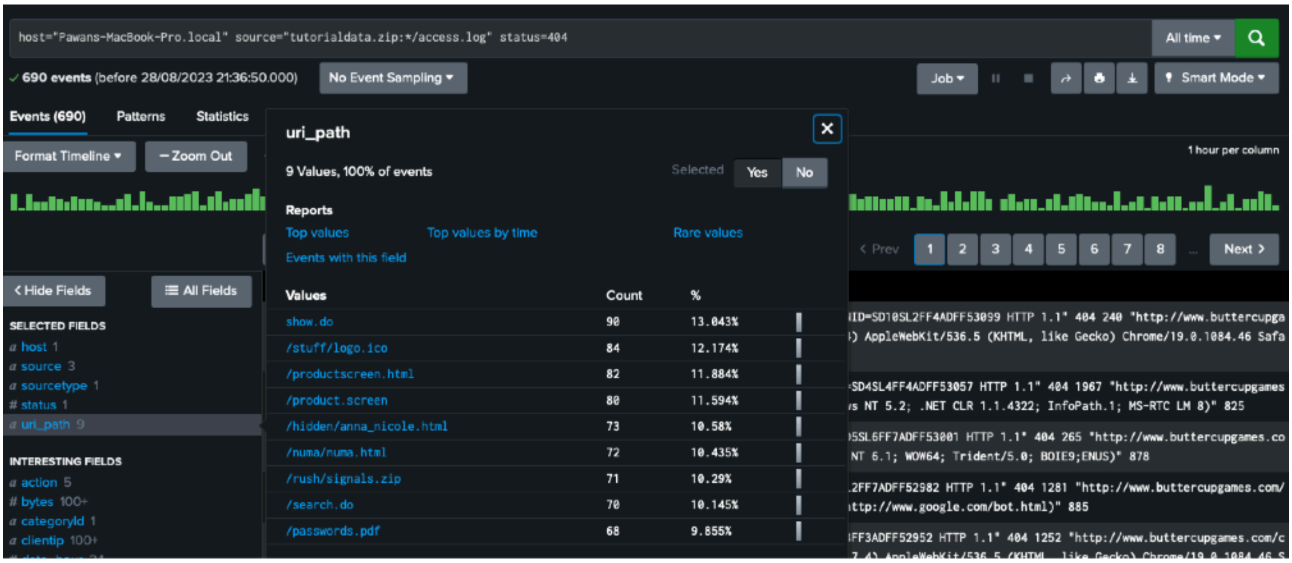


Values	Count	%
200	34,282	86.72%
503	952	2.408%
408	756	1.912%
500	733	1.854%
406	710	1.796%
400	701	1.773%
404	690	1.745%
505	480	1.214%
403	228	0.577%

Yes, in my opinion, status 401 and 403 is trying to access the information that is not allow. So, the attempt is 228

(We might include 404 since someone could guess the path to access to sensitive info) So, in this case the attempt is 918

Q6. What resource/file are hackers looking for?



```
host="Pawans-MacBook-Pro.local" source="tutorialdata.zip:*/access.log" status=404
```

✓ 690 events (before 28/08/2023 21:36:50.000)

SELECTED FIELDS

- a host 1
- a source 3
- a sourcetype 1
- # status 1
- a uri_path 9

INTERESTING FIELDS

- a action 5
- # bytes 100+
- a categoryId 1
- a clientip 100+

uri_path

9 Values, 100% of events

Selected: Yes **No**

Reports

Top values · Top values by time · Rare values

Events with this field

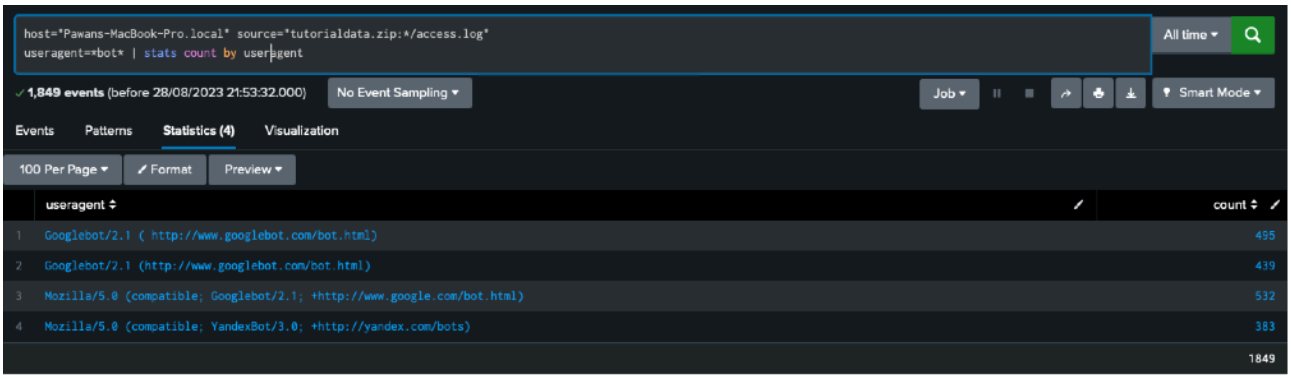
Values	Count	%
show.do	90	13.043%
/stuff/logo.ico	84	12.174%
/productscreen.html	82	11.884%
/product.screen	80	11.594%
/hidden/anna_nicole.html	73	10.58%
/numa/numa.html	72	10.435%
/rush/signals.zip	71	10.29%
/search.do	70	10.145%
/passwords.pdf	68	9.855%

```
ID=SD10SL2FF4ADFF53099 HTTP 1.1" 404 240 "http://www.buttercupga
) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safa

SD4SL4FF4ADFF53057 HTTP 1.1" 404 1967 "http://www.buttercupgames
s NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 825

5SL6FF7ADFF53001 HTTP 1.1" 404 265 "http://www.buttercupgames.co
NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 878

2FF7ADFF52982 HTTP 1.1" 404 1281 "http://www.buttercupgames.com/
ttp://www.google.com/bot.html)" 885

FF3ADFF52952 HTTP 1.1" 404 1252 "http://www.buttercupgames.com/c
```

In this case we should filter response 404 and see the path
The most resource is show.do

Q7. Can you find any bots crawling our websites?

Yes

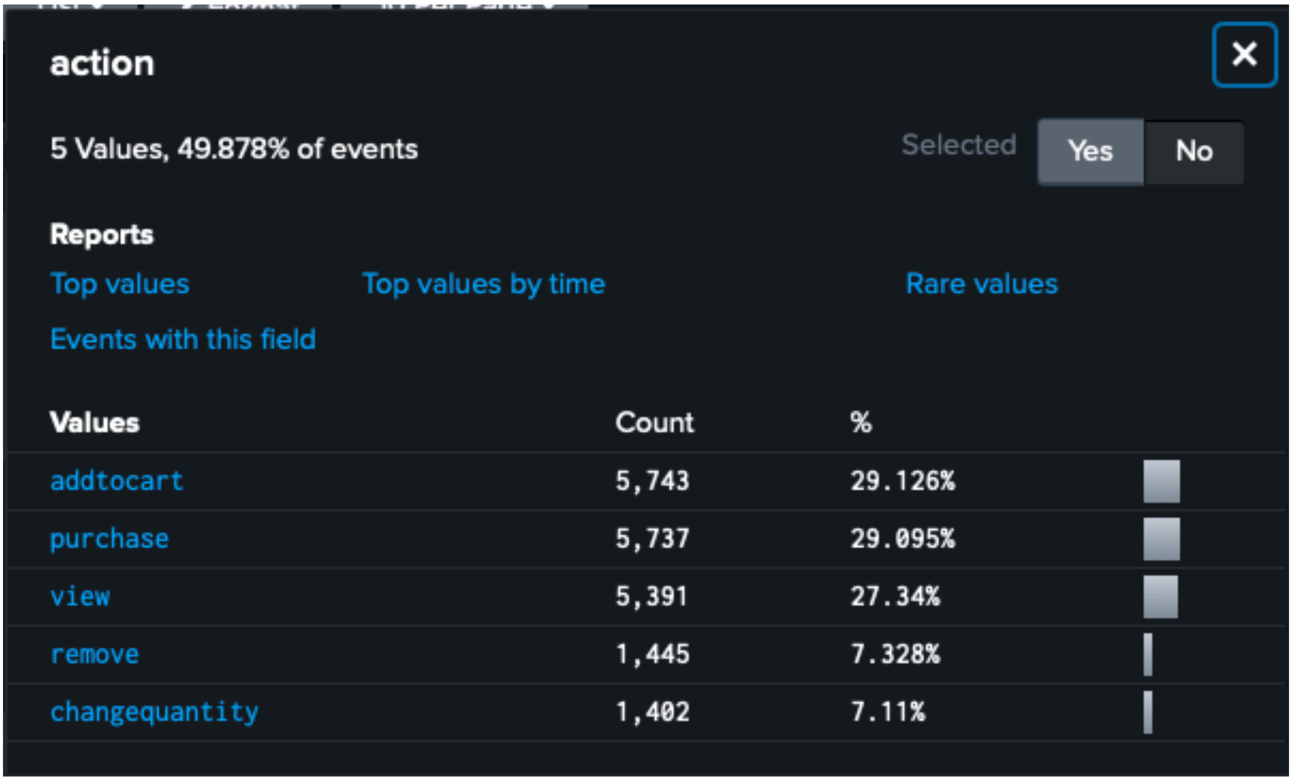


```
host="Pawans-MacBook-Pro.local" source="tutorialdata.zip:*/access.log"
useragent=*bot* | stats count by useragent
```

✓ 1,849 events (before 28/08/2023 21:53:32.000)

	useragent	count
1	Googlebot/2.1 (http://www.googlebot.com/bot.html)	495
2	Googlebot/2.1 (http://www.googlebot.com/bot.html)	439
3	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	532
4	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	383
		1849

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



action

5 Values, 49.878% of events

Selected [✓ Yes] No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
addtocart	5,743	29.126%
purchase	5,737	29.095%
view	5,391	27.34%
remove	1,445	7.328%
changequantity	1,402	7.11%