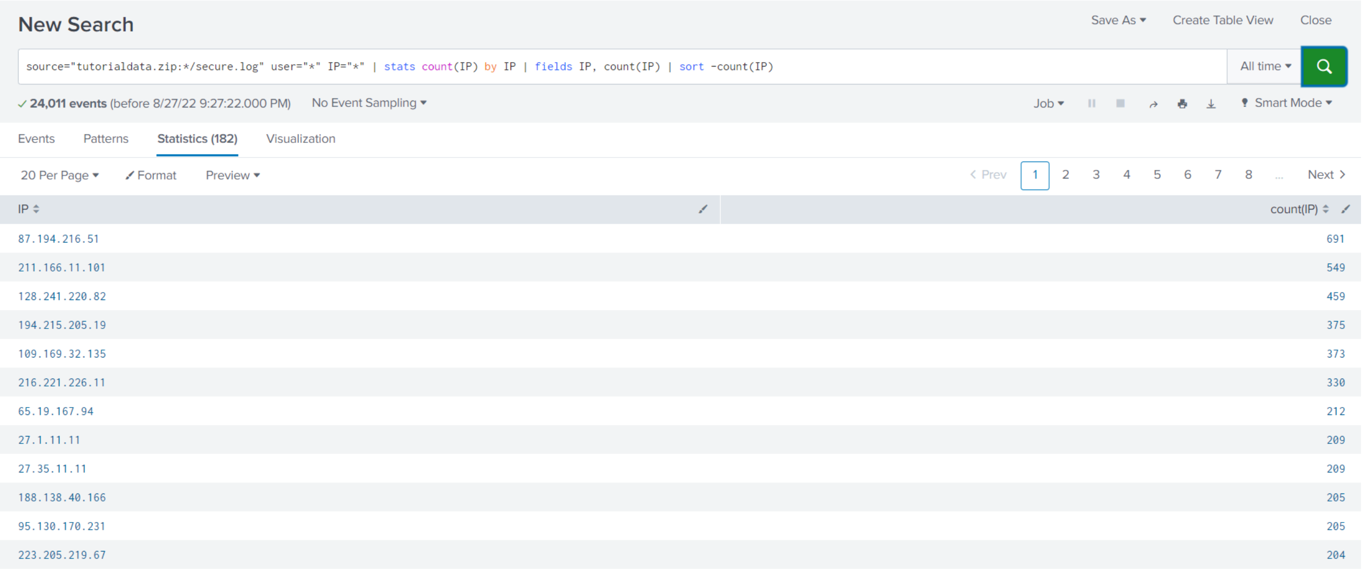
Activity 3 : Log Analysis

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

1. How many hackers are trying to get access to our servers? And how many attempts are there? Explain/define how you count distinct hackers.

We will define the hackers as the people who are trying to get into the servers with invalid usernames. Distinct hackers are recognized by distict IP addresses.

From this search query, there are 182 hackers and 24,011 attempts.

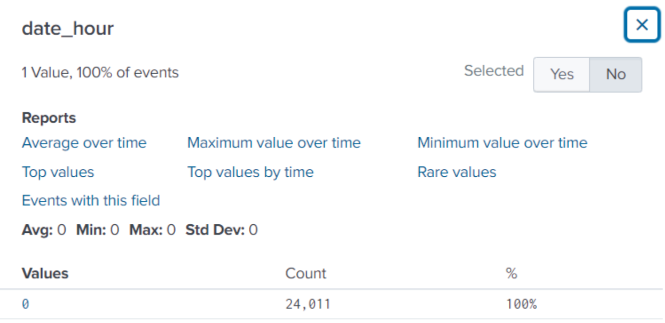


```
source="tutorialdata.zip:*/secure.log" user="*" IP="*" | stats count(IP) by IP | fields IP, count(IP) | sort -count(IP)
```

IP	count(IP)
87.194.216.51	691
211.166.11.101	549
128.241.220.82	459
194.215.205.19	375
109.169.32.135	373
216.221.226.11	330
65.19.167.94	212
27.1.11.11	209
27.35.11.11	209
188.138.40.166	205
95.130.170.231	205
223.205.219.67	204

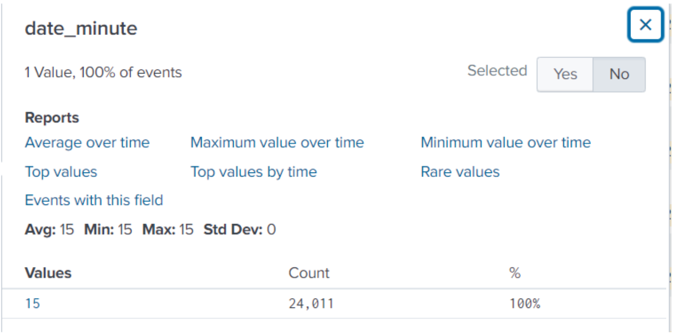
2. What time do hackers appear to try to hack our servers?

00.15 AM of every day available in the data.



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

Values	Count	%
0	24,011	100%

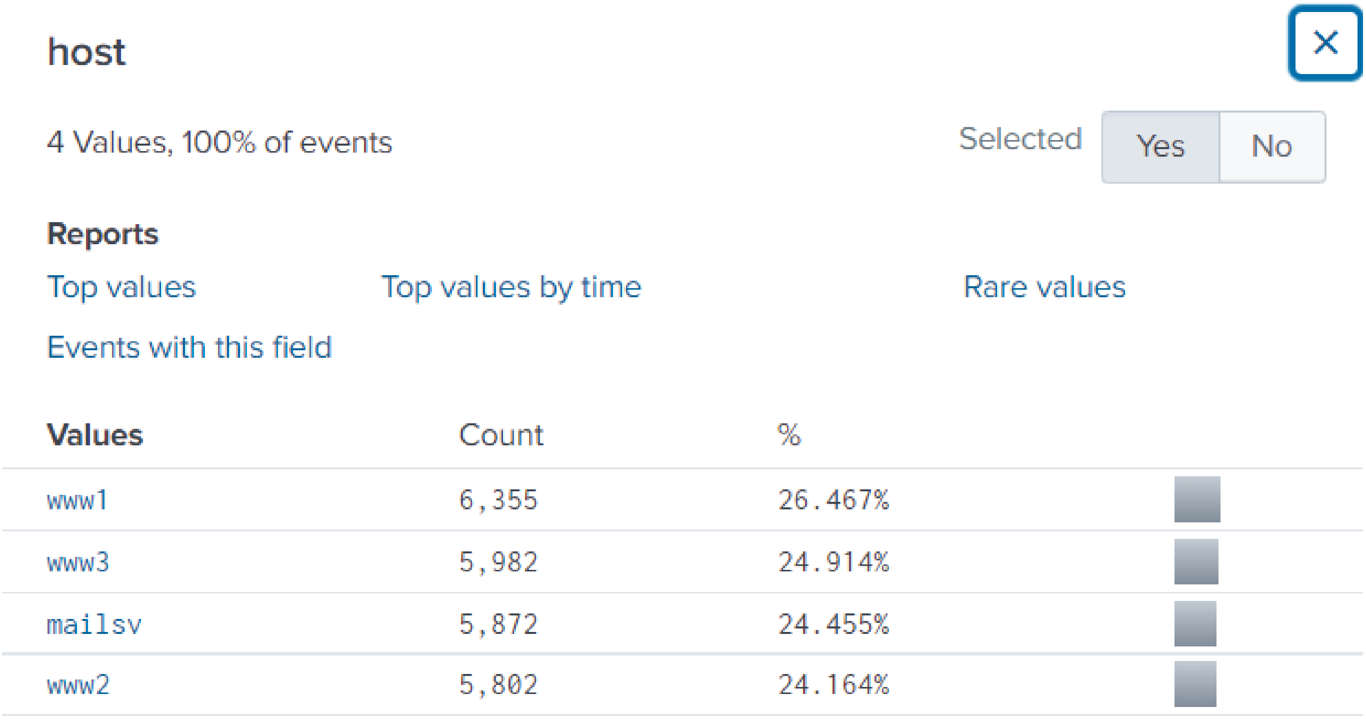


Avg: 15 **Min:** 15 **Max:** 15 **Std Dev:** 0

Values	Count	%
15	24,011	100%

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

www1. However, the percentage of attacks on each server is roughly the same.



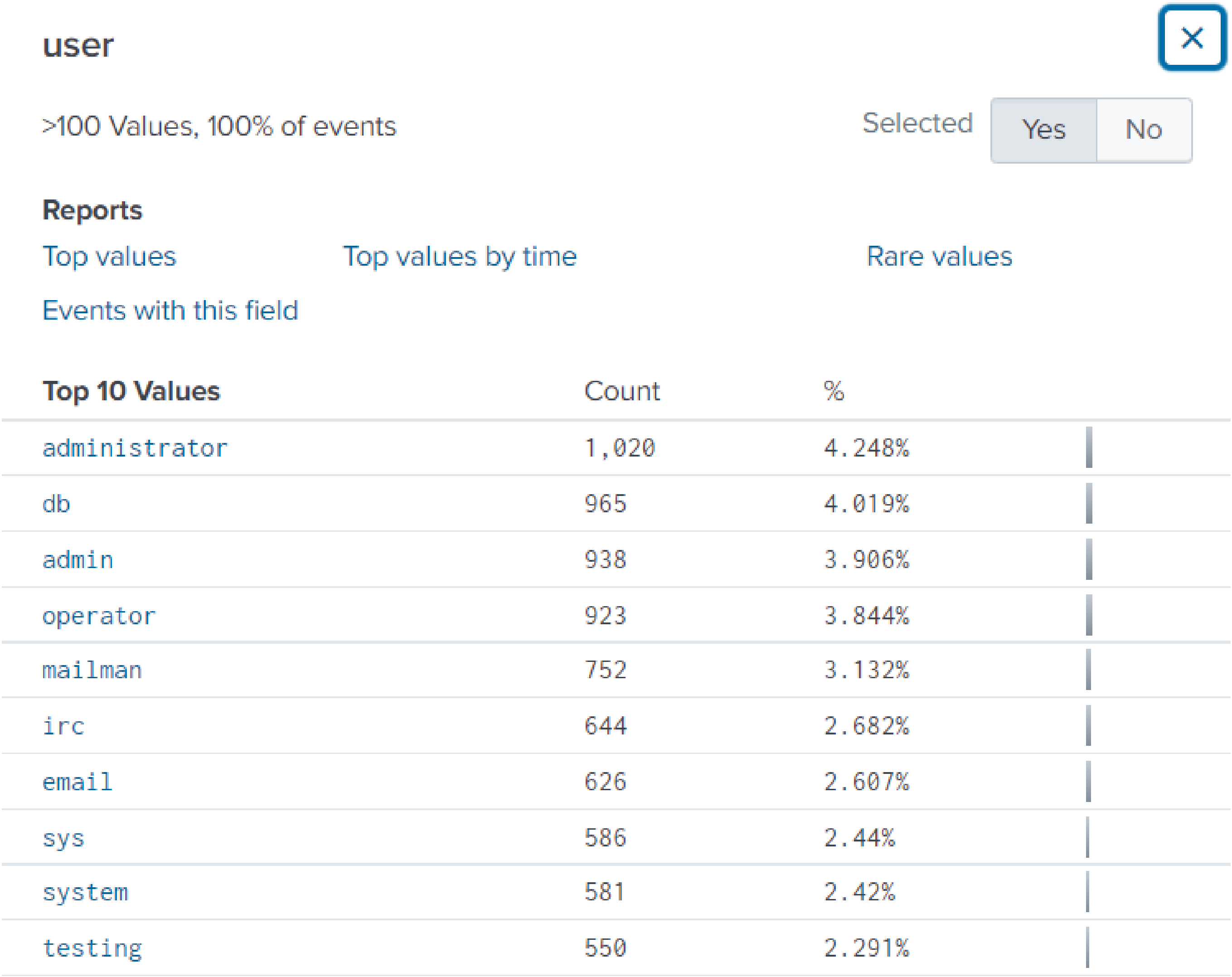
host

4 Values, 100% of events

Values	Count	%
www1	6,355	26.467%
www3	5,982	24.914%
mailsv	5,872	24.455%
www2	5,802	24.164%

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

administrator.



user

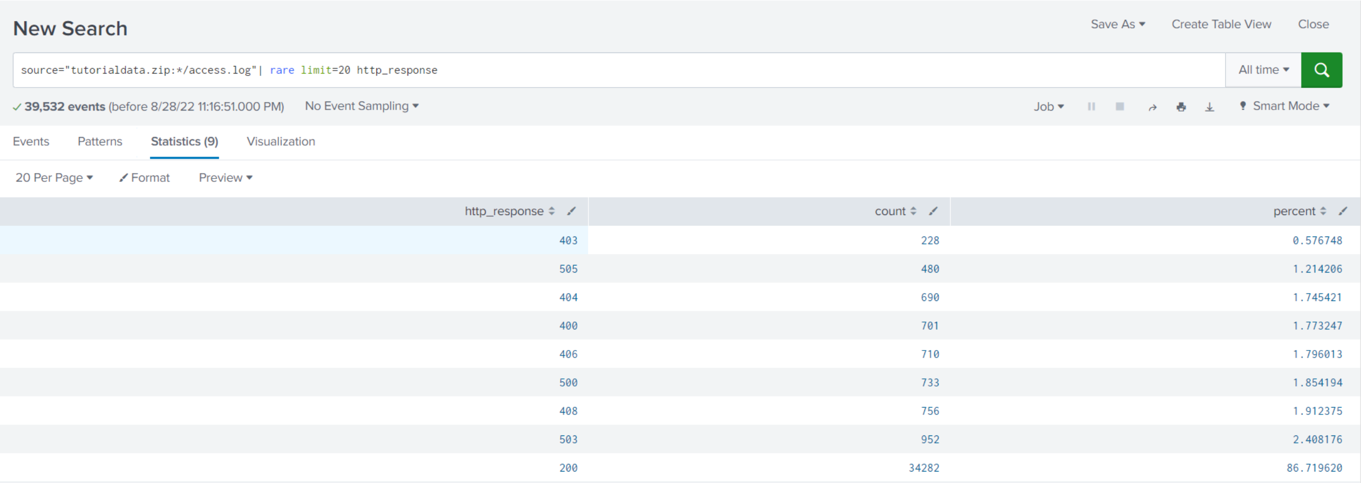
>100 Values, 100% of events

Top 10 Values	Count	%
administrator	1,020	4.248%
db	965	4.019%
admin	938	3.906%
operator	923	3.844%
mailman	752	3.132%
irc	644	2.682%
email	626	2.607%
sys	586	2.44%
system	581	2.42%
testing	550	2.291%

Part II. Sensitive Files on Web Servers

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

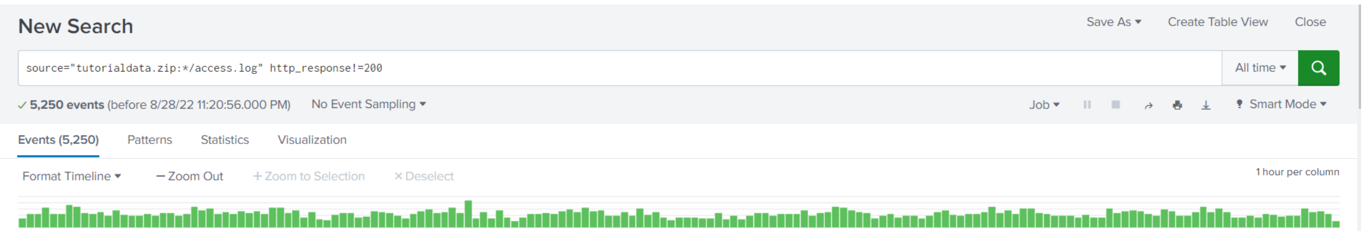
We consider requests that return http responses in the 400-500 range to be an attempt. From the data, there are 5,250 attempts.



```
source="tutorialdata.zip:*/access.log"| rare limit=20 http_response
```

✓ 39,532 events (before 8/28/22 11:16:51.000 PM)

http_response	count	percent
403	228	0.576748
505	480	1.214206
404	690	1.745421
400	701	1.773247
406	710	1.796013
500	733	1.854194
408	756	1.912375
503	952	2.408176
200	34282	86.719620

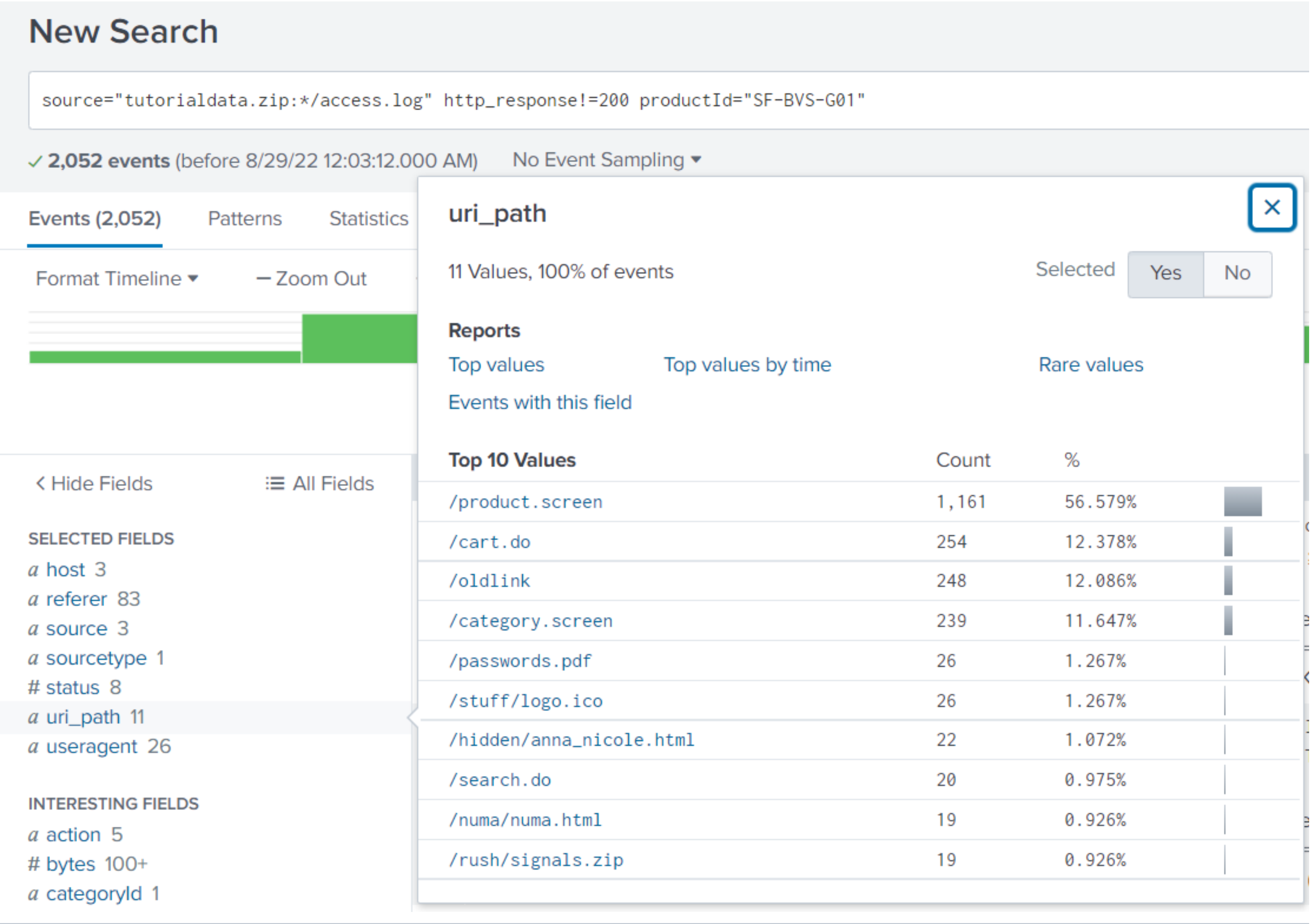


```
source="tutorialdata.zip:*/access.log" http_response!=200
```

✓ 5,250 events (before 8/28/22 11:20:56.000 PM)

6. What resource/file are hackers looking for?

They are mainly looking for productId SF-BVS-G01 and SF-BVS-01, using these URI paths.



New Search

```
source="tutorialdata.zip:*/access.log" http_response!=200 productId="SF-BVS-G01"
```

✓ 2,052 events (before 8/29/22 12:03:12.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 3
a referer 83
a source 3
a sourcetype 1
# status 8
a uri_path 11
a useragent 26

INTERESTING FIELDS
a action 5
# bytes 100+
a categoryId 1

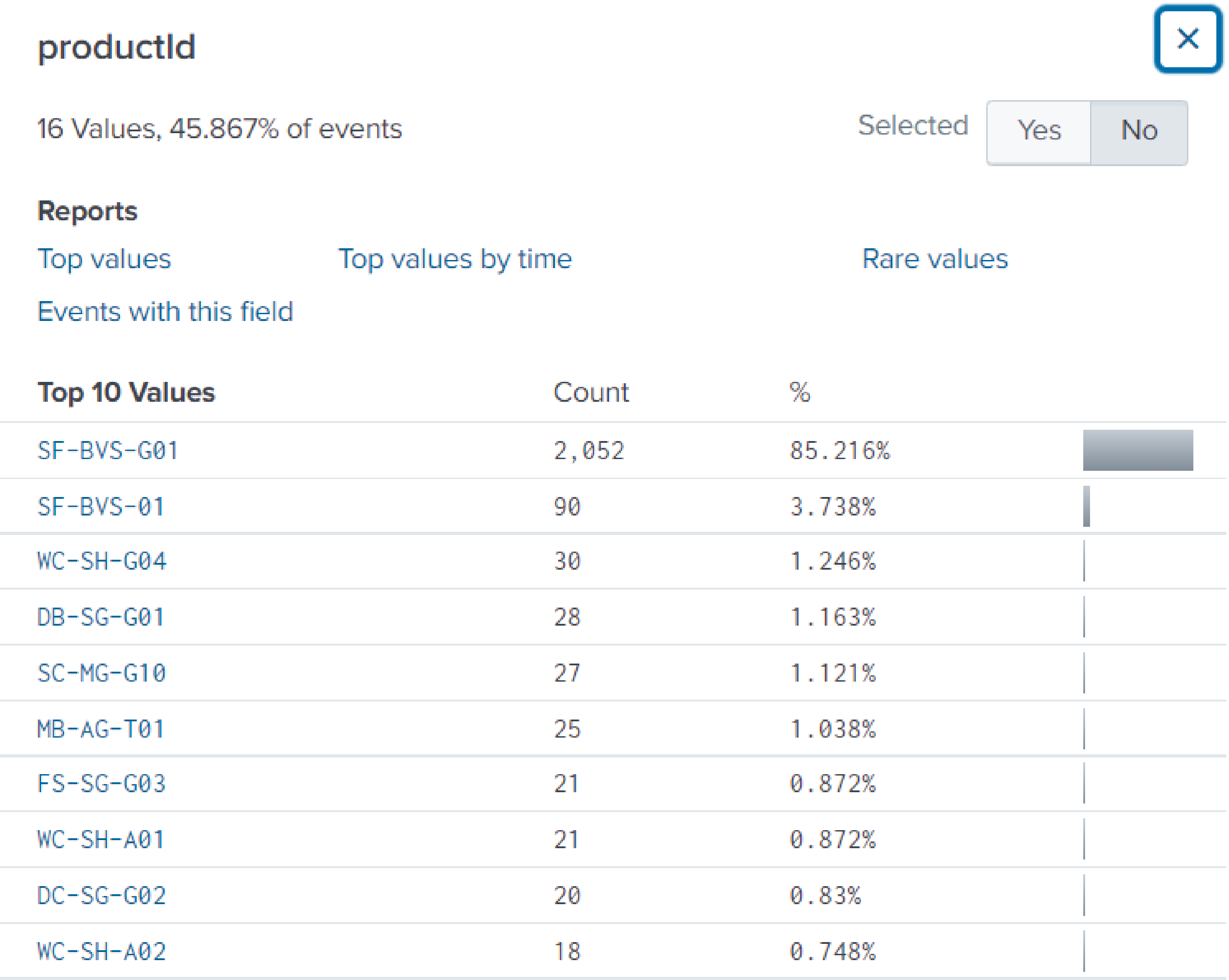
uri_path

11 Values, 100% of events

Selected Yes No

Reports
Top values Top values by time Rare values
Events with this field

Top 10 Values	Count	%
/product.screen	1,161	56.579%
/cart.do	254	12.378%
/oldlink	248	12.086%
/category.screen	239	11.647%
/passwords.pdf	26	1.267%
/stuff/logo.ico	26	1.267%
/hidden/anna_nicole.html	22	1.072%
/search.do	20	0.975%
/numa/numa.html	19	0.926%
/rush/signals.zip	19	0.926%



productId

16 Values, 45.867% of events

Selected Yes No

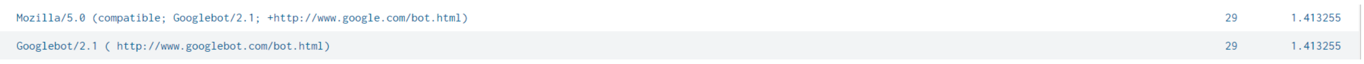
Reports
Top values Top values by time Rare values
Events with this field

Top 10 Values	Count	%
SF-BVS-G01	2,052	85.216%
SF-BVS-01	90	3.738%
WC-SH-G04	30	1.246%
DB-SG-G01	28	1.163%
SC-MG-G10	27	1.121%
MB-AG-T01	25	1.038%
FS-SG-G03	21	0.872%
WC-SH-A01	21	0.872%
DC-SG-G02	20	0.83%
WC-SH-A02	18	0.748%

Part III. Are there bots crawling our websites?

7. Can you find any bots crawling our websites?

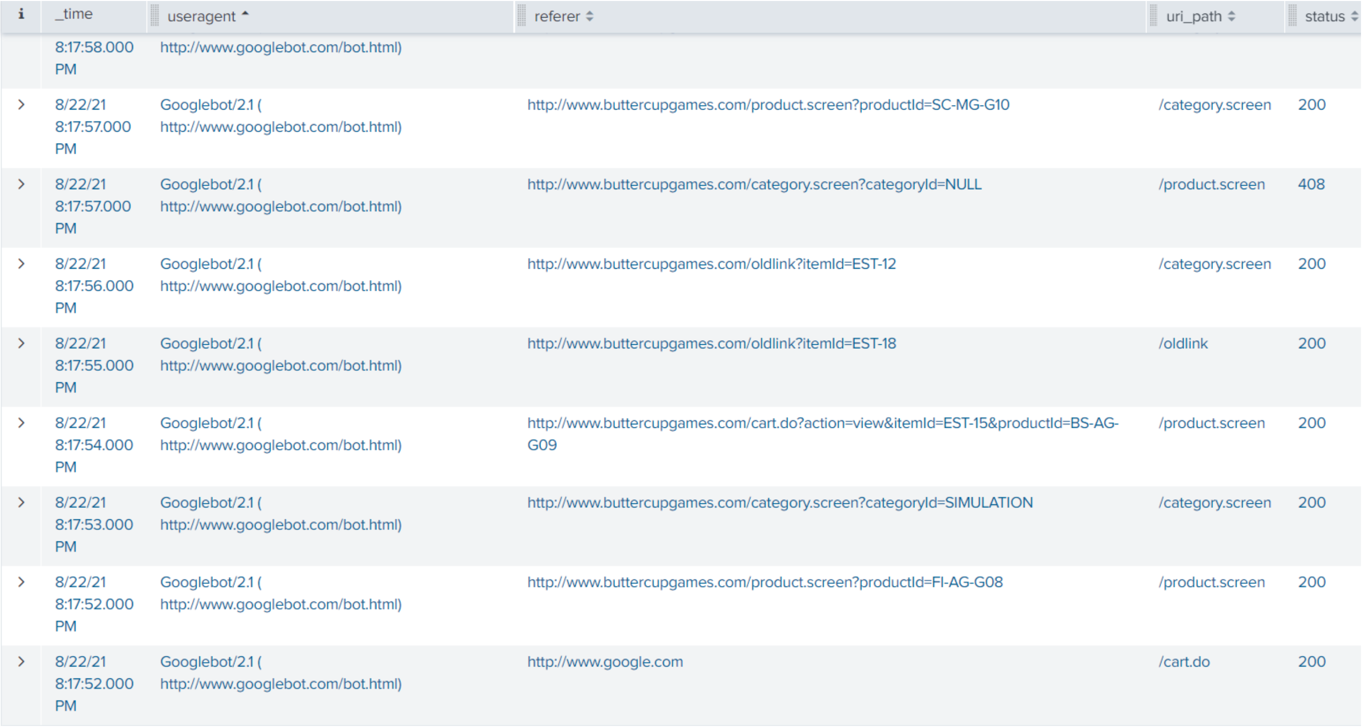
Yes, 2 googlebots



Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	29	1.413255
Googlebot/2.1 (http://www.googlebot.com/bot.html)	29	1.413255

8. What are they doing on the site?

The bots are browsing the products and adding them to cart. This image is an example of the events.



i	_time	useragent	referer	uri_path	status
	8:17:58.000 PM	http://www.googlebot.com/bot.html)			
>	8/22/21 8:17:57.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/product.screen?productId=SC-MG-G10	/category.screen	200
>	8/22/21 8:17:57.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/category.screen?categoryId=NULL	/product.screen	408
>	8/22/21 8:17:56.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/oldlink?itemId=EST-12	/category.screen	200
>	8/22/21 8:17:55.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/oldlink?itemId=EST-18	/oldlink	200
>	8/22/21 8:17:54.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/cart.do?action=view&itemId=EST-15&productId=BS-AG-G09	/product.screen	200
>	8/22/21 8:17:53.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/category.screen?categoryId=SIMULATION	/category.screen	200
>	8/22/21 8:17:52.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.buttercupgames.com/product.screen?productId=FI-AG-G08	/product.screen	200
>	8/22/21 8:17:52.000 PM	Googlebot/2.1 (http://www.googlebot.com/bot.html)	http://www.google.com	/cart.do	200