

The Search Pipeline >

- Relies heavily on the Unix pipe operator |

splunk> Put that in your | and Splunk it.

The Search Pipeline >

Broad search
host=myhost
sourcetype=csv

```
11010101
00001001
11011101
01111010
```

Keywords/booleans/fields
fail OR failure
locked
user=b123

```
11010101
00001001
11011101
```

Commands
count
sum
eval

```
1101
0101
1111
```

Table / Viz
Table
timechart

```
1101
0101
```

A lot of data



The data we want
The format we want

The Search Pipeline >

```
sourcetype=WinEventLog:Security EventCode=4625 user=* | timechart span=1h  
count(EventCode) by user
```

Let's break this down

```
sourcetype=WinEventLog:Security EventCode=4625 user=*
```

- I am searching for a specific source type. This source type was created by a Splunk App for Windows.
- The source type I am searching for is the `Security` portion of the `WinEventLog`.
- I am also narrowing my search to one specific event code: `4625`, which is a failed log on.
- Finally, I want to include all the user names because I know I am going to use this field later to build a table or visualization.

The Search Pipeline >

```
sourcetype=WinEventLog:Security EventCode=4625 user=* | timechart span=1h  
count(EventCode) by user
```

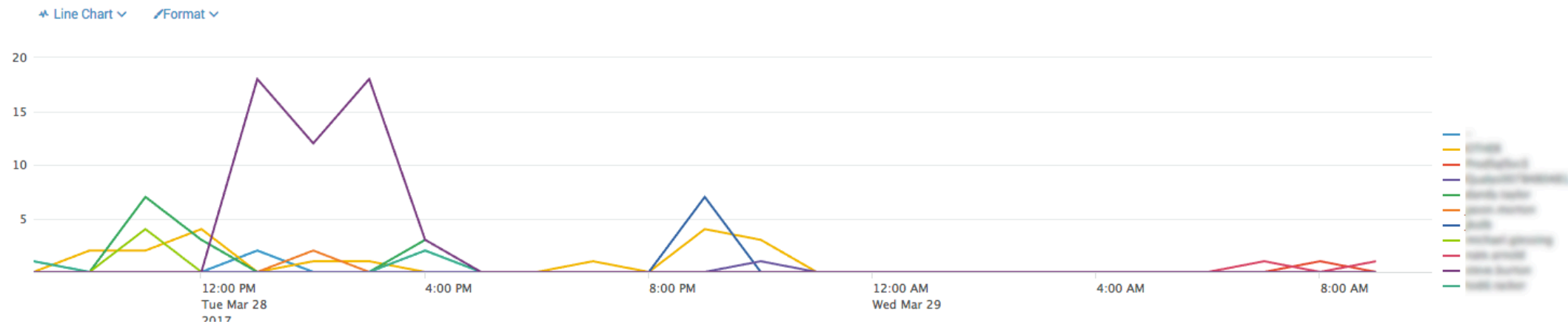
Let's break this down

```
| timechart span=1h count(EventCode) by user
```

- I am "piping" the previous data into a `timechart` command.
- By using the `span=1hr` statement, I am forcing the chart to have one hour increments.
- Next, I am counting the `EventCode` (which is what I searched for before the pipe).
- Finally, I want the data analyzed by `user`.

The Search Pipeline >

```
sourcetype=WinEventLog:Security EventCode=4625 user=* | timechart span=1h  
count(EventCode) by user
```



The Search Pipeline >

```
sourcetype=WinEventLog:Security EventCode=4625 user=* | stats  
count(EventCode) by user
```

user	count(EventCode)
NT AUTHORITY\SYSTEM	2
NT AUTHORITY\LOCAL SERVICE	1
NT AUTHORITY\NETWORK SERVICE	13
NT AUTHORITY\SYSTEM	2
NT AUTHORITY\SYSTEM	7
NT AUTHORITY\SYSTEM	1
NT AUTHORITY\SYSTEM	1
NT AUTHORITY\SYSTEM	1
NT AUTHORITY\SYSTEM	4
NT AUTHORITY\SYSTEM	2
NT AUTHORITY\SYSTEM	1
NT AUTHORITY\SYSTEM	51
NT AUTHORITY\SYSTEM	1
NT AUTHORITY\SYSTEM	3

The Search Pipeline >

```
sourcetype=WinEventLog:Security EventCode=4625 user=* | stats  
count(EventCode) by user _time | table _time user count(EventCode) | sort  
-_time
```

_time	user	count(EventCode)
2017-03-29 09:09:48	NT AUTHORITY\SYSTEM	1
2017-03-29 07:12:41	NT AUTHORITY\SYSTEM	1
2017-03-29 07:10:07	NT AUTHORITY\SYSTEM	1
2017-03-28 21:40:13	NT AUTHORITY\SYSTEM	1
2017-03-28 21:40:00	NT AUTHORITY\SYSTEM	1
2017-03-28 21:39:52	NT AUTHORITY\SYSTEM	1
2017-03-28 21:39:32	NT AUTHORITY\SYSTEM	1
2017-03-28 21:39:17	NT AUTHORITY\SYSTEM	1
2017-03-28 21:39:07	NT AUTHORITY\SYSTEM	1
2017-03-28 21:39:01	NT AUTHORITY\SYSTEM	1
2017-03-28 19:57:27	NT AUTHORITY\SYSTEM	1
2017-03-28 16:40:07	NT AUTHORITY\SYSTEM	3
2017-03-28 16:32:46	NT AUTHORITY\SYSTEM	3
2017-03-28 16:13:44	NT AUTHORITY\SYSTEM	1

The Search Pipeline >

```
sourcetype=WinEventLog:Security EventCode=4625 user=* | stats count(EventCode) by user _time | table _time  
user count(EventCode) | sort -_time
```

11010101
00001001
11011101
01111010

11010101
00001001
11011101

1101
0101
1111

1101
0101

A lot of data



The data we want
The format we want

Thanks, Splunkers!

