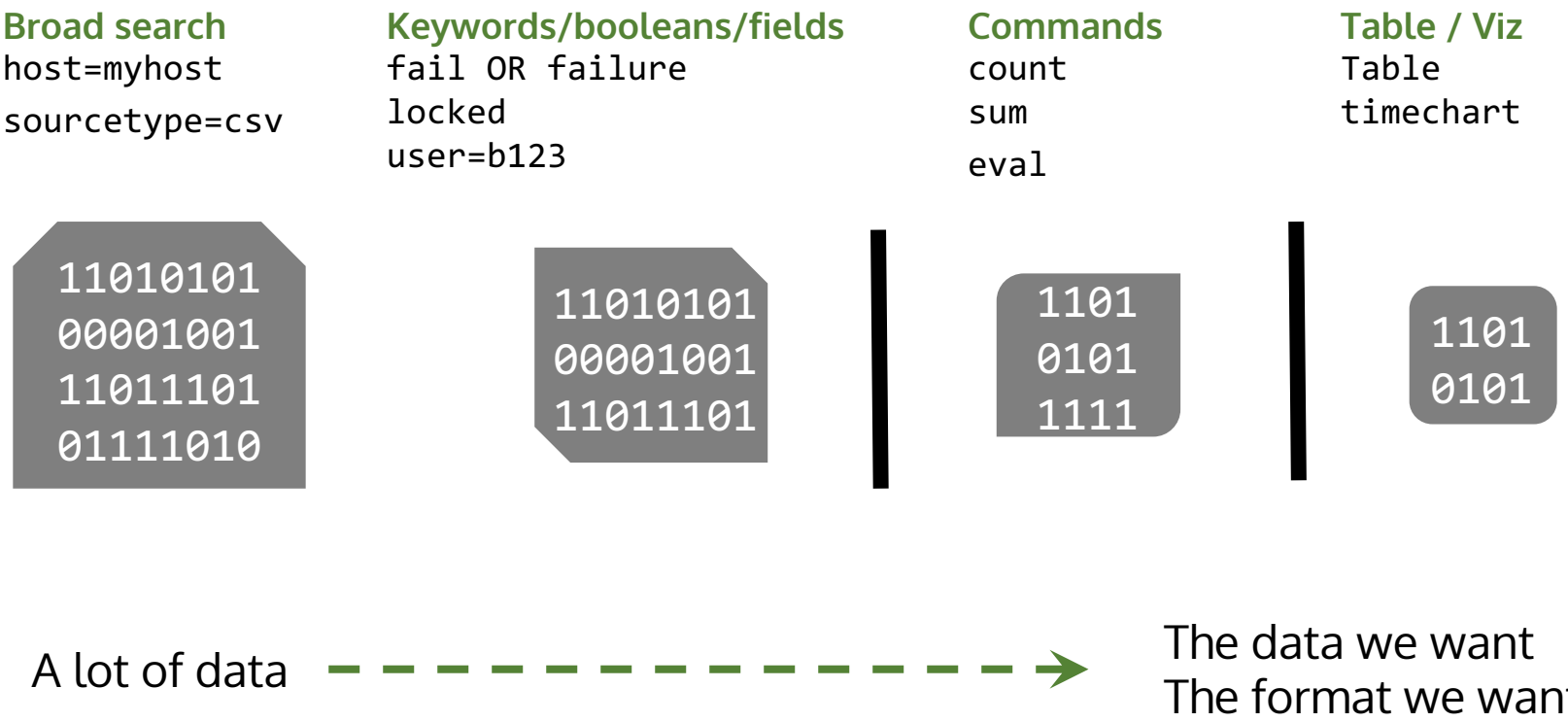
The Search Pipeline >

- Relies heavily on the Unix pipe operator |

The Search Pipeline >



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
```

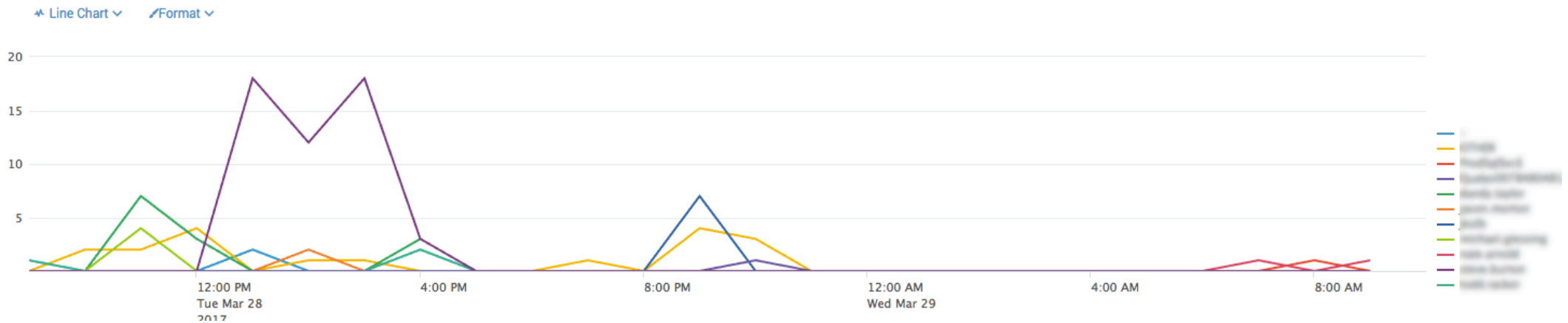
Let's break this down

```
| 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
```



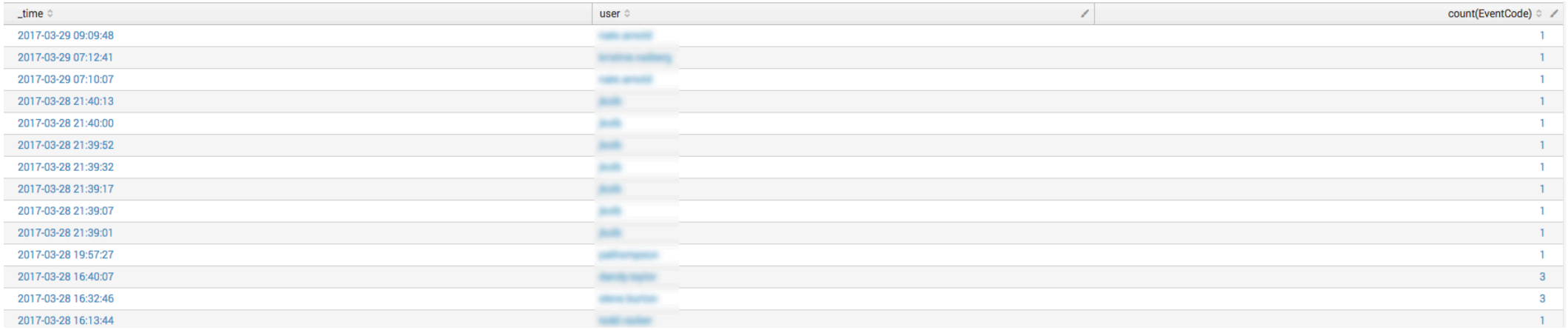
The Search Pipeline >

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

user	count(EventCode)
	2
	1
	13
	2
	7
	1
	1
	1
	4
	2
	1
	51
	1
	3

The Search Pipeline >

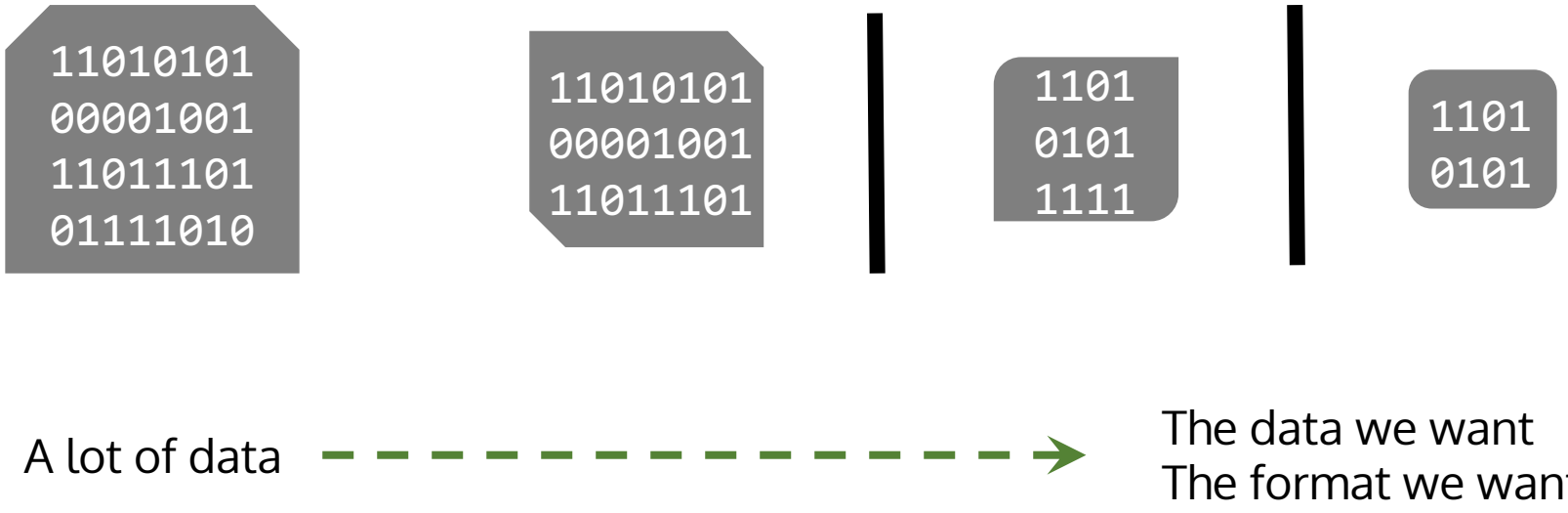
```
sourcetype=WinEventLog:Security EventCode=4625 user=* | stats
count(EventCode) by user _time | table _time user count(EventCode) | sort
-_time
```



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

The Search Pipeline >

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



Thanks, Splunkers!