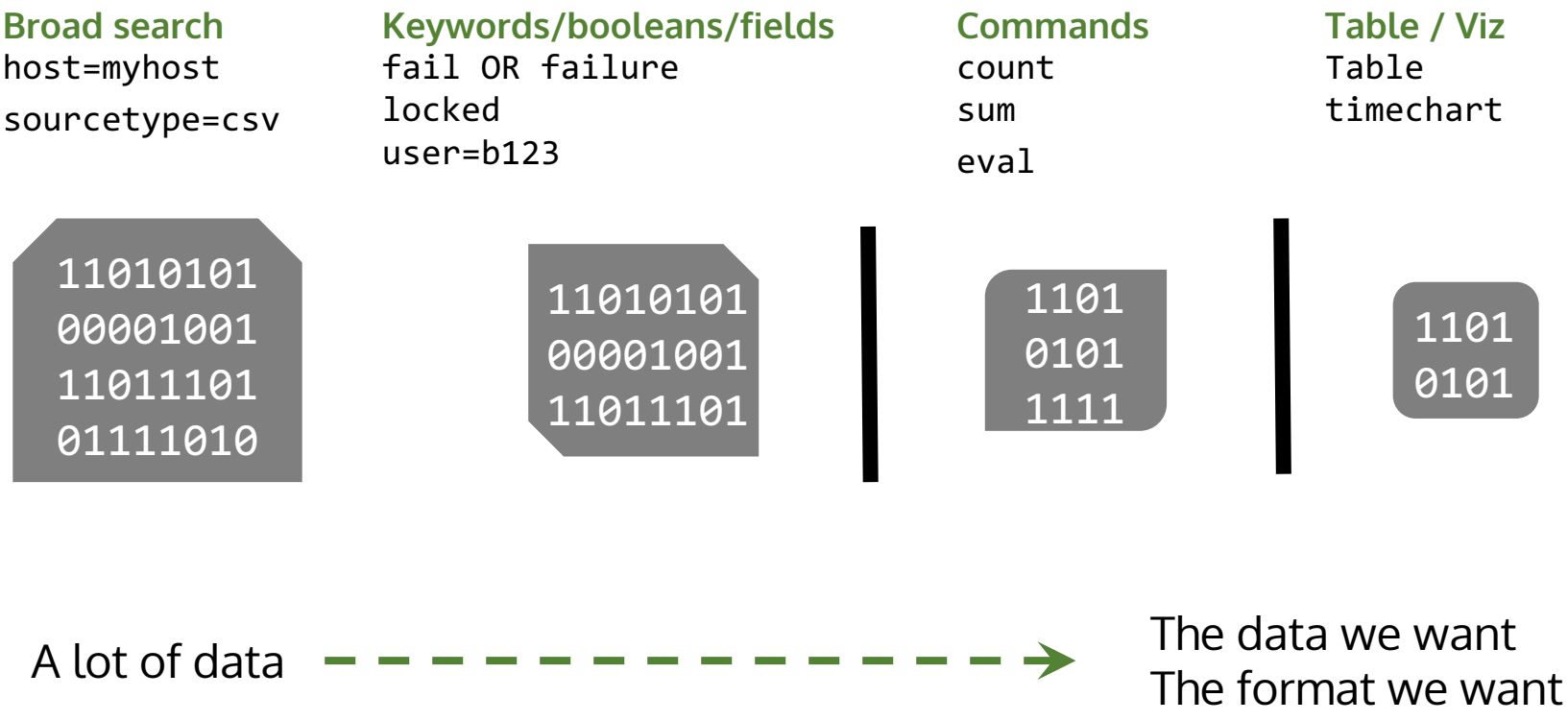
Intermediate Searching >

Recall the search pipeline



Intermediate Searching >

Let's look at some transforming commands

- `top`
- `rare`
- `stats`

Intermediate Searching >

Top

- `top <field>`
- Returns the most common values of a given field
- Defaults to 10 fields
- Can be combined with `limit=<number>`
- Automatically builds a table with `count` and `percent` columns
- Can be used with multiple fields
  - "return the top value for a field organized by another field"

Intermediate Searching >

```
| top user
```

user	count	percent
gholmes0	43	21%
jruiz1	30	15%
hdean	24	12%
pbishop	23	11.5%
lmendez	23	11.5%
kpuroo14	20	1%
dlamd5t	12	0.06%
wgreene87	9	0.04%
jbruss	9	0.04%
anolowitz2	7	0.03%

Intermediate Searching >

Rare

- `rare <field>`
- Opposite of `top`
- Returns the least common values of a field
- Options are identical to `top`

Intermediate Searching >

Stats

- `stats <function(field)> BY <field(s)>`

- Some common functions
  - `count, avg, max, mean, median, sum, stdev, values, list`

Intermediate Searching >

```
| stats avg(kbps) BY host
```

Avg(kbps)	host
654.78	host1.domain.com
852.66	host2.domain.com

```
| stats count(failed_logins) BY user
```

Failed_logins	user
42	jwebber
16	asloken3

Demo: `top`, `rare`, & `stats`

Thanks, Splunkers!