The Pipe Operator

- Output of one command is fed into the input of the next
- Can thinking of it as a filtering and aggregation pipeline
- In most cases here the first command will be reading from a Bro log file

```
sudo dmesg | less
```

grep

- Search for a string in the input
- -v inverts the search, printing things that don't contain the string

```
cat conn.log | grep dns
```

bro-cut

- Specify a subset of a bro log
- Can reorder fields
- -d converts timestamps to human-readable (but timestamp field must be included)

```
cat conn.log | bro-cut uid missed_bytes
```

sort

- Sort the rows of the input
- -r for reverse, -n for numbers

```
cat conn.log | bro-cut missed_bytes uid | sort –n
```

uniq

- Remove *adjacent* duplicated lines
- -c counts the number of occurrences

```
cat dns.log | bro-cut query | sort | uniq -c
```