ngrep

like grep for your network

```
$ sudo ngrep GET
```

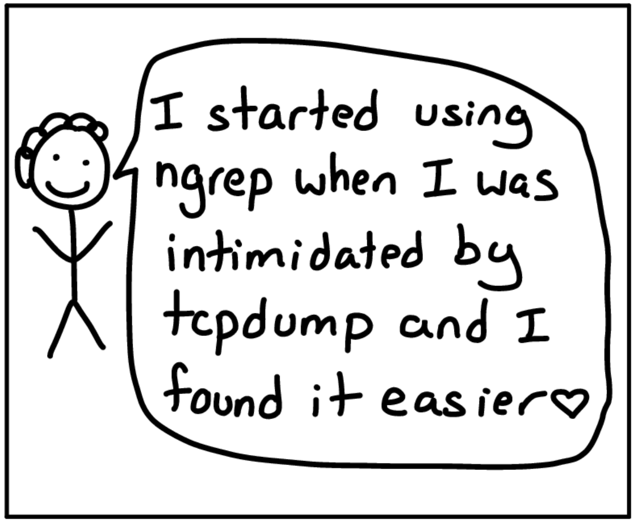
will find every plaintext HTTP GET request

ngrep syntax

```
$ ngrep
  [options]
  [regular expression]
  [BPF filter]
```

what to search packets for

same format as tcpdump uses!


I started using ngrep when I was intimidated by tcpdump and I found it easier ♡

-d

is for device

which network interface to use. same as tcpdump's -i (try '-d any'!)

-W byline

prints line breaks as line breaks, not "\n". Nice when looking at HTTP requests

-I file.pcap
-O file.pcap

read/write packets from/to a pcap file