



# Grepcidr in 30 minutes or less

- <http://www.av8.net/dist/grepcidr/>
- Get grepcidr-2.1.tar.gz
- ./configure; make; make install
- grepcidr -h is hopefully self explanatory



# Grepcidr -h

Usage: grepcidr [OPTIONS]... [[PATTERN] [FILES]]...

-h, --help	Print help and exit
-V, --version	Print version and exit
-c, --count	Count Lines
-b, --blocks	Output Matching blocks
-n, --numblocks	Number of matching blocks
-v, --invert	Invert match
-e, --pattern=STRING	Pattern
-f, --file=STRING	Pattern file
-i, --ipaddr	Output matching IP
-l, --no-filename	Suppress prefixing filename for multiple files
-s, --sb	Square brackets around IP to matched
--cb	Curly braces around IP to be matched
-p, --pb	Parentheses around IP to be matched
--vb	Vertical Bars around IP to be matched
--lb=STRING	custom left bracket
--rb=STRING	custom right bracket



# Pattern Formats

CIDR format:	a.b.c.d/n
IP range:	a.b.c.d-e.f.g.h
IP range :	a.b.c.d+size
Single IP:	a.b.c.d

Just like grep:

- one pattern on command line or
- multiple `-e <pattern>` options
- multiple `-f` file options



# Uses

- Log analysis

- Technique: get bad login worst offenders

- grep badlogin logfile | grepcidr -i 0.0.0.0/0 | sort -u > xx

- grepcidr -bf xx logfile #count of badlogins per ip

- Traffic analysis

- Blacklist management

- Technique: expire rehabilitated abusers

- grepcidr -vbf blacklist maillogs > notseenrecently

- Technique: make sure we aren't in blacklist

- grepcidr -f ourblocks blacklist

- Spam filtering

- Now from Ronco...



# Where to get allocation info

`ftp.arin.net://pub/stats/{RIR} /delegated- {RIR} -latest`

RIR = afrinic apnic arin lacnic ripencc

Currently allocated blocks:

- afrinic 1513
- apnic 16616
- arin 40841
- lacnic 2384
- ripencc 37482

- Total 98836

TODO:

Don't have LIR data