DEVOPSSAAR

Unix tips and tricks from the “moth box” - The Unix / Linux / BSD command line

Andreas Koch / Jürgen Kammer

Meeting No. 3

31. Jan 2019

Sponsored by

OVH Innovation is Freedom

>eurodata

INFOSERVE >eurodata-Gruppe

Agenda

- Introduction
- History
- Tools with tips and tricks
- big round: “what do you know”

Introduction

Why commandline? (Is not the command line oldshool?)

YES, but very fast!

Introduction - philosophy

The UNIX philosophy is documented by Doug McIlroy in the Bell System Technical Journal from 1978

1. Make each program do one thing well. To do a new job, build afresh rather than complicate old programs by adding new "features".
2. Expect the output of every program to become the input to another, as yet unknown, program. Don't clutter output with extraneous information. Avoid stringently columnar or binary input formats. Don't insist on interactive input.
3. Use tools in preference to unskilled help to lighten a programming task, even if you have to detour to build the tools and expect to throw some of them out after you've finished using them.

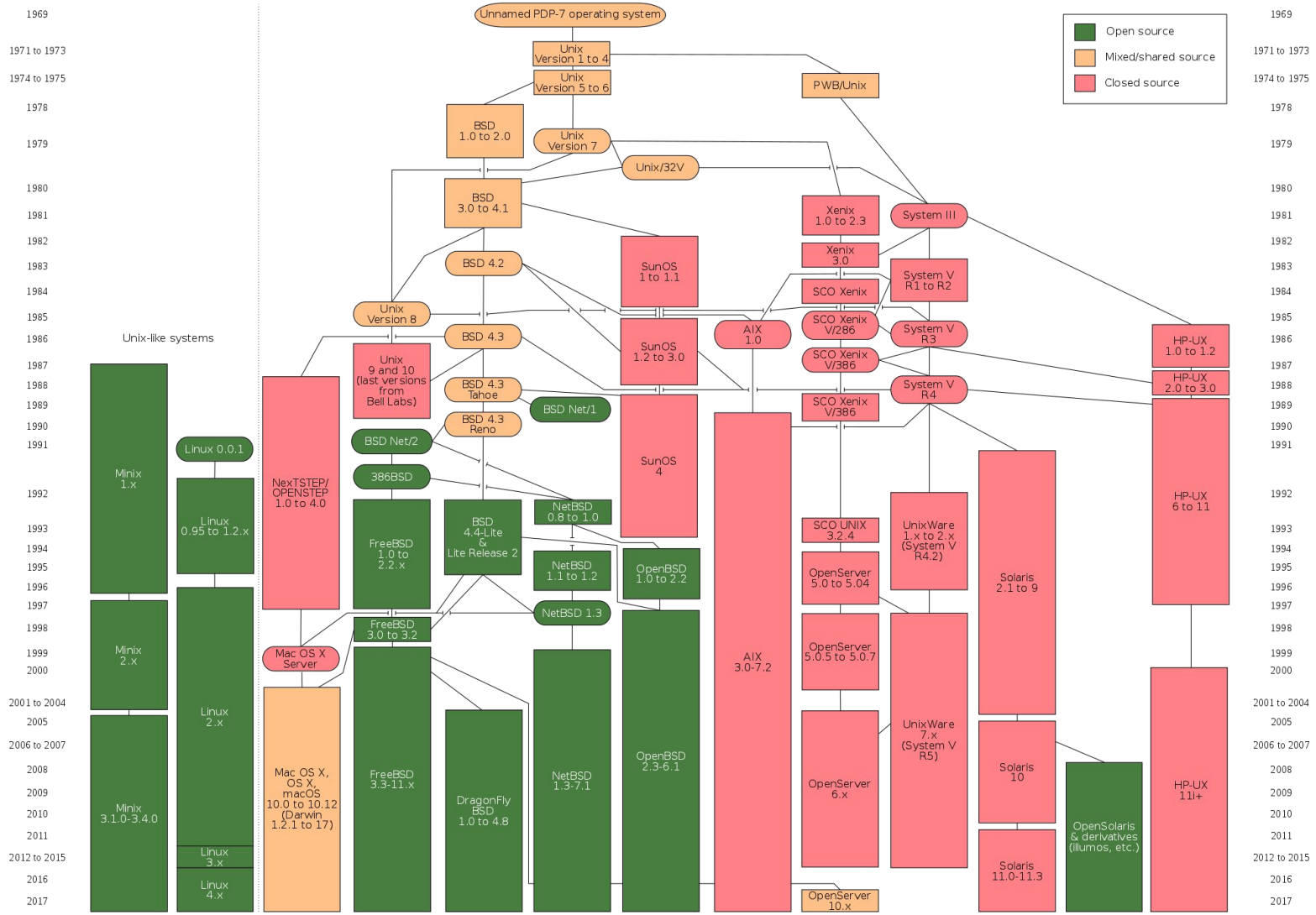
Introduction - motivation

Unix is a toolbox

Introduction - motivation

1. Conserving resources
2. interactive
3. fast
4. Needs little bandwidth
5. The learning curve is only once steep

History


Open source
Mixed/shared source
Closed source
Unix-like systems
1969
1971 to 1973
1974 to 1975
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001 to 2004
2005
2006 to 2007
2008
2009
2010
2011
2012 to 2015
2016
2017
Unnamed PDP-7 operating system
Unix Version 1 to 4
Unix Version 5 to 6
Unix Version 7
PWB/Unix
BSD 1.0 to 2.0
Unix/32V
BSD 3.0 to 4.1
Xenix 1.0 to 2.3
System III
Xenix 3.0
BSD 4.2
SunOS 1 to 1.1
System V R1 to R2
SCO Xenix
Unix Version 8
SCO Xenix V/286
AIX 1.0
System V R3
BSD 4.3
SunOS 1.2 to 3.0
SCO Xenix V/386
HP-UX 1.0 to 1.2
Unix 9 and 10 (last versions from Bell Labs)
BSD 4.3 Tahoe
BSD Net/1
System V R4
HP-UX 2.0 to 3.0
BSD 4.3 Reno
BSD Net/2
SunOS 4
386BSD
NetBSD 0.8 to 1.0
NetBSD 1.1 to 1.2
NetBSD 1.3
OpenBSD 1.0 to 2.2
FreeBSD 3.0 to 3.2
SCO UNIX 3.2.4
OpenServer 5.0 to 5.04
OpenServer 5.0.5 to 5.0.7
OpenServer 6.x
OpenServer 10.x
UnixWare 1.x to 2.x (System V R4.2)
UnixWare 7.x (System V R5)
Solaris 2.1 to 9
Solaris 10
Solaris 11.0-11.3
OpenSolaris & derivatives (illumos, etc.)
HP-UX 6 to 11
HP-UX 11i+
Minix 1.x
Minix 2.x
Minix 3.1.0-3.4.0
Linux 0.0.1
Linux 0.95 to 1.2.x
Linux 2.x
Linux 3.x
Linux 4.x
NexTSTEP/ OPENSTEP 1.0 to 4.0
Mac OS X Server
Mac OS X, OS X, macOS 10.0 to 10.12 (Darwin 1.2.1 to 17)
FreeBSD 1.0 to 2.2.x
FreeBSD 3.3-11.x
BSD 4.4-Lite & Lite Release 2
DragonFly BSD 1.0 to 4.8
NetBSD 1.3-7.1
OpenBSD 2.3-6.1
AIX 3.0-7.2

History - IEEE Std 1003.1-2008 utilities

admin, alias, ar, asa, at, awk, basename, batch, bc, bg, break, c99, cal, cat, cd, cflow, chgrp, chmod, chown, cksum, cmp, colon, comm, command, compress, continue, cp, crontab, csplit, ctags, cut, cxref, date, dd, delta, df, diff, dirname, dot, du, echo, ed, env, eval, ex, exec, exit, expand, export, expr, false, fc, fg, file, find, fold, fort77, fuser, gencat, get, getconf, getopts, grep, hash, head, iconv, id, ipcrm, ipcs, jobs, join, kill, lex, link, ln, locale, localedef, logger, logname, lp, ls, m4, mailx, make, man, mesg, mkdir, mkfifo, more, mv, newgrp, nice, nl, nm, nohup, od, paste, patch, pathchk, pax, pr, printf, prs, ps, pwd, qalter, qdel, qhold, qmove, qmsg, qrerun, qrls, qselect, qsig, qstat, qsub, read, readonly, renice, return, rm, rmdel, rmdir, sact, sccs, sed, set, sh, shift, sleep, sort, split, strings, strip, stty, tabs, tail, talk, tee, test, time, times, touch, tput, tr, trap, true, tsort, tty, type, ulimit, umask, unalias, uname, uncompress, unexpand, unget, uniq, unlink, unset, uucp, uudecode, uuencode, uustat, uux, val, vi, wait, wc, what, who, write, xargs, yacc, zcat

History - Linux Standard Base (LSB)

[, ar, at, awk, basename, batch, bc, cat, cd, chfn, chgrp, chmod, chown, chsh, cksum, cmp, col, comm, cp, cpio, crontab, csplit, cut, date, dd, df, diff, dirname, dmesg, du, echo, ed, egrep, env, expand, expr, false, fgrep, file, find, fold, fuser, gencat, getconf, getopts, gettext, grep, groupadd, groupdel, groupmod, groups, gunzip, gzip, head, hostname, iconv, id, install, install_initd, ipcrm, ipcs, join, kill, killall, ln, locale, localedef, logger, logname, lp, lpr, ls, lsbinstall, lsb_release, m4, mailx, make, man, md5sum, mkdir, mkfifo, mknod, mktemp, more, mount, msgfmt, mv, newgrp, nice, nl, nohup, od, passwd, paste, patch, pathchk, pax, pidof, pr, printf, ps, pwd, read, remove_initd, renice, rm, rmdir, sed, sendmail, sh, shutdown, sleep, sort, split, strip, stty, su, sync, tail, tar, tee, test, time, touch, tr, true, tsort, tty, umask, umount, uname, unexpand, uniq, useradd, userdel, usermod, wait, wc, xargs

Tools with tips and tricks

Documentation

man “tool”

Example: man man

Tools with tips and tricks

copy

```
cp -r /disk1/.* /disk2/
```

faster copy

```
(cd /disk1/ ; tar -cplf - . ) | ( cd /disk2/; tar -xplf - )
```

Use more then 1 CPU
All permissions are the same

Tools with tips and tricks

awk (Aho-Weinberger-Kernighan)

- beloved script language for your unix shell.
- strings / arrays, "calculator", regular expressions
- devides STDIN lines into words, and you work with them
  default separator: whitespace, you can change it with “-F”, i.e. -F: (for /etc/password)
  $0 - whole line, $1 first word (or “field”), NF number of fields, $NF last field.

Example1: File "Werte.txt"

```
<snip>
Alpha 23
Berta 53
Charly      66
Delta 11
<snap>
$ awk '{print $2,$1}' < Werte.txt                  # swap columns
$ awk '{x+=$2}END{print "Summe: ",x}' < Werte.txt  # Summe of the numbers
$ awk '/ha/' < Werte.txt                           # all lines with "ha"
```

Tools with tips and tricks

awk (Aho-Weinberger-Kernighan)

- beloved script language for your unix shell.
- strings / arrays, "calculator", regular expressions
- devides STDIN lines into words, and you work with them
  default separator: whitespace, you can change it with “-F”, i.e. -F: (for /etc/password)
  $0 - whole line, $1 first word (or “field”), NF number of fields, $NF last field.

Example2: read out iptables counters
- put ipv6 trafic through a dedicated ip6tables-Chains.
- add up all lines you want

```
Chain V6Out (3 references)
    pkts      bytes target     prot opt in   out    source  destination
  971992 138447246 RETURN       all      *       bond1  ::/0     ::/0

$ ip6tables  -L V6Out -v -x | awk '/RETURN/{opacks+=$1;obytes+=$2}END{print
"OPACKS="opacks";OBYTES="obytes}'
  OPACKS=971992;OBYTES=138447246
```

- grep and add up what you want....

Tools with tips and tricks

awk (Aho-Weinberger-Kernighan)

- beloved script language for your unix shell.
- strings / arrays, "calculator", regular expressions
- devides STDIN lines into words, and you work with them
  default separator: whitespace, you can change it with “-F”, i.e. -F: (for /etc/password)
  $0 - whole line, $1 first word (or “field”), NF number of fields, $NF last field.

awk, here there be dragons!

- add something up (often needed)...

```
$ awk 'END{print 30*10+555+3}' < /dev/null     # awk-Freak, bc hater
858
$ awk 'END{print 2147483647+3}' < /dev/null
2.14748e+09                    # in decimal?
$ awk 'END{printf("%d\n", 2147483647+3)}' < /dev/null
2147483647                     # wait, what?
```

Tools with tips and tricks

awk (Aho-Weinberger-Kernighan)

- beloved script language for your unix shell.
- strings / arrays, "calculator", regular expressions
- devides STDIN lines into words, and you work with them
  default separator: whitespace, you can change it with “-F”, i.e. -F: (for /etc/password)
  $0 - whole line, $1 first word (or “field”), NF number of fields, $NF last field.

- awk != awk. Ganz böse Falle. Hier: mawk <-> gawk.

```
$ mawk 'END{print 2147483647+2147483647}' < /dev/null
4.29497e+09
$ gawk 'END{print 2147483647+2147483647}' < /dev/null
4294967294
$ gawk 'END{printf("%d\n", 2147483647+2147483647)}' < /dev/null
4294967294
$ mawk 'END{printf("%d\n", 2147483647+2147483647)}' < /dev/null
2147483647
```

Tools with tips and tricks

alternative: cut (be faster since it is a smaller)

cut -d ‘“delimiter” -f “fields”

Example 1: File "Werte.txt"

<snip>
Alpha,11
Berta,12
Charly,13
Delta,14
<snap>
> cut -d \, -f 2 → <snip> 11 12 13 14 <snap>
> cut -d 1 -f 2 → <snip> 1 2 3 4 <snap>
> cut -d 1 -f 1 → <snip> Alpha, Berta, Charly, Delta, <snap>

Tools with tips and tricks

alternative: cut (be faster since it is a smaller)

Example:

awk '/WORD/ { print $2 }' filename

grep WORD filename| cut -f 2 -d ' '

File with 500.000 lines:

awk ~ 0,5s
grep + cut ~ 0,05s

Tools with tips and tricks

example

1. Which http requests have requested more than 1 MB within one hour or uploaded more than 1 MB?

   zcat /var/log/squid/access.log.7.gz | tailocal | grep '2018-04-28 09' | awk '{if ($6 > 1048576) {print $6/1048576 " von " $8 }}'

2. How many MB were retrieved from or uploaded to a particular URL?

   zcat /var/log/squid/access.log.7.gz | tailocal | grep '2018-04-28 09' | grep -e ‘URL\.com’ | awk '{summe = summe +$6} END {print summe/1048576 }'

3. How many MBs were retrieved from or uploaded to a specific URL on which day?

   for i in $(seq 62 92);do zgrep eurodata.de /var/log/squid/access.log.$i.gz | awk '{summe=summe +$6} END {print summe/1048576 " MB" }';echo "Accesslog=/var/log/squid3/access.log.$i.gz"; done

Tools with tips and tricks

Write image/Zip to disk

dd if=/tmp/image.img of=/dev/disk bs=1M

- of= -> target
- if= -> source
- bs= -> Size of the data blocks (Use 4096 in new systems)

unzip -p /path/image.zip | dd of=/dev/disk1 bs=4M

Tools with tips and tricks

Write image/Zip to disk - Status?

dd if=/tmp/image.img of=/dev/disk bs=1M

unzip -p /path/image.zip | dd of=/dev/disk1 bs=4M

- dd with option “status=progress”
- other shell: watch -n10 killall -USR1 dd
  (watch: execute a program periodically, showing output fullscreen)

Tools with tips and tricks

/bin/ls: Argument list too long

ls *.txt | wc -l

-bash: /bin/ls: Argument list too long

find -type f -name '*.txt' | wc -l

Option find: -maxdepth

Tools with tips and tricks

shell tricks

sudo

```
user@localhost: find /var/log -type f -mtime +1
find: ‘/var/log/xyz’ : Permission denied
user@localhost: sudo !!
sudo find /var/log -type f -mtime +1
[sudo] password for user:
/var/log/syslog
/var/log/dmesg
user@localhost:
```

Tools with tips and tricks

shell tricks

Killing and yanking text

user@localhost: find /var/log -type f _ -mtime +1
Ctrl K (cut to end of the line)
user@localhost: find /var/log -type f
Ctrl Y (way back)
user@localhost: find /var/log -type f _ -mtime +1
Ctrl U (cut to beginning of the line)
user@localhost: -mtime +1
user@localhost: find /var/log -type f _ -mtime +1
Ctrl W (cut word backward)
user@localhost: find /var/log -type _ -mtime +1
user@localhost: find /var/log _ -mtime +1

Tools with tips and tricks

shell tricks

example kill/yank flow

user@localhost: find /var/log -type f -mtime +1_
Ctrl U
sudo
Ctrl Y
user@localhost: sudo find /var/log -type f -mtime +1_

Tools with tips and tricks

shell tricks

replace ‘tail’ with ‘less’

user@localhost: tail -f /var/log/syslog
user@localhost: less +F /var/log/syslog (starts of the end)
Ctrl C (pause and read the file)

Shift F (restart follow mode)

Tools with tips and tricks

shell tricks

paste the argument of the previous command

user@localhost: ping 8.8.8.8

user@localhost: dig -x
Alt .
user@localhost: dig -x 8.8.8.8

Tools with tips and tricks

shell tricks

change the previous...

user@localhost: cat /var/log/* | grep WORDfine | sort

user@localhost: ^fine^poor
cat /var/log/* | grep WORDpoor | sort

Tools with tips and tricks

alias

Make life easier

1. alias sl=’ls’
2. alias mdkir=’mkdir’
3. alias g=’git’
4. alias d=’docker’
5. alias gpom=’git push origin master’
6. alias grom=’git reset --hard origin/master’

Tools with tips and tricks

alias

Make life easier … or not???

alias ls=’ls -l’

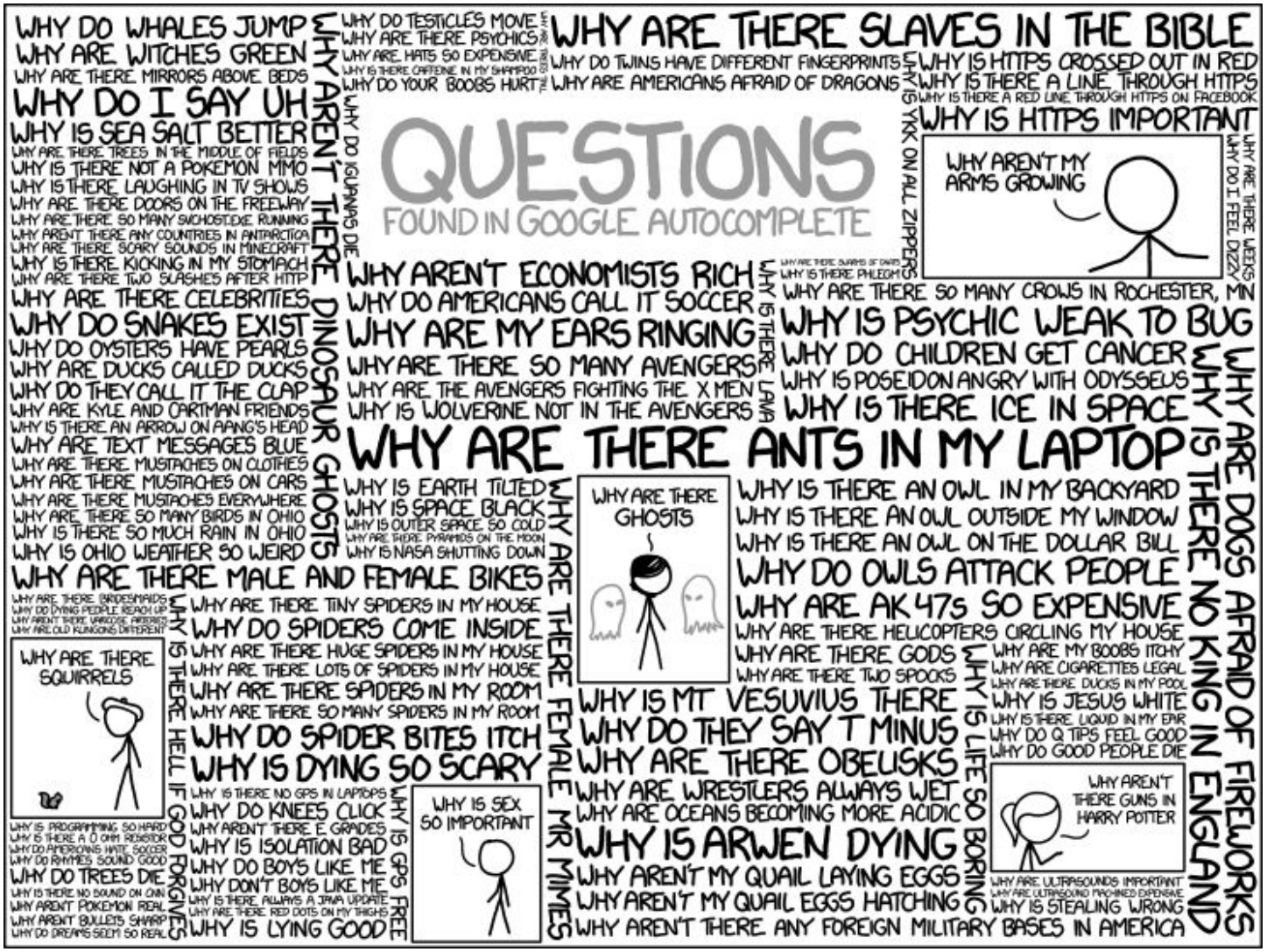
(How can I execute the original command?)

\ls /tmp/

Tools with tips and tricks

big round:
“what do you know”

Thanks


QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SWOOSHES RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE AMBERS
WHY ARE OLD KLINGONS DIFFERENT
WHY ARE THERE SQUIRRELS
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY DO IGUANAS DIE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY AREN'T MY ARMS GROWING
WHY IS YKK ON ALL ZIPPERS
WHY ARE THERE DINOSAUR GHOSTS
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY ARE THERE SWARMS OF DAVID
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY IS THERE LAVA
WHY ARE THERE ANTS IN MY LAPTOP
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOOKS
WHY ARE THERE FIREWORKS
WHY ARE DOGS AFRAID OF
WHY IS THERE NO KING IN ENGLAND
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY ARE THERE FEMALE MR MIMES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY IS THERE HELL IF GOD FORGIVES
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS SEX SO IMPORTANT
WHY IS GPS FREE
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY IS LIFE SO BORING
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY