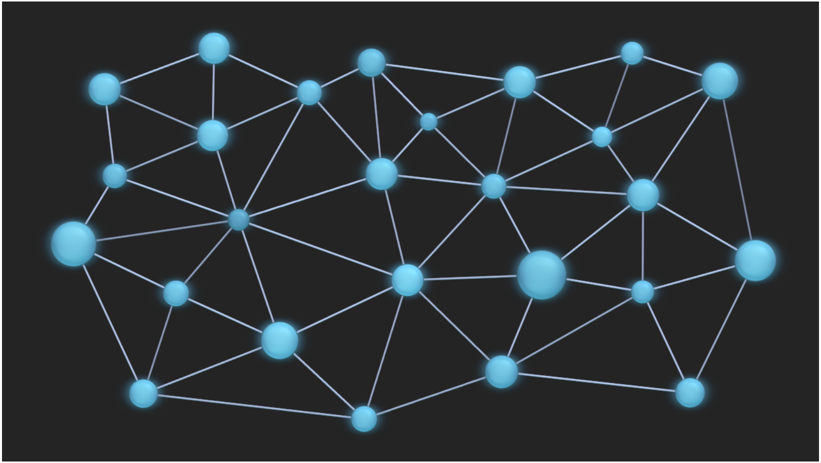
Fearless deployments with Guix

Christopher Allan Webber

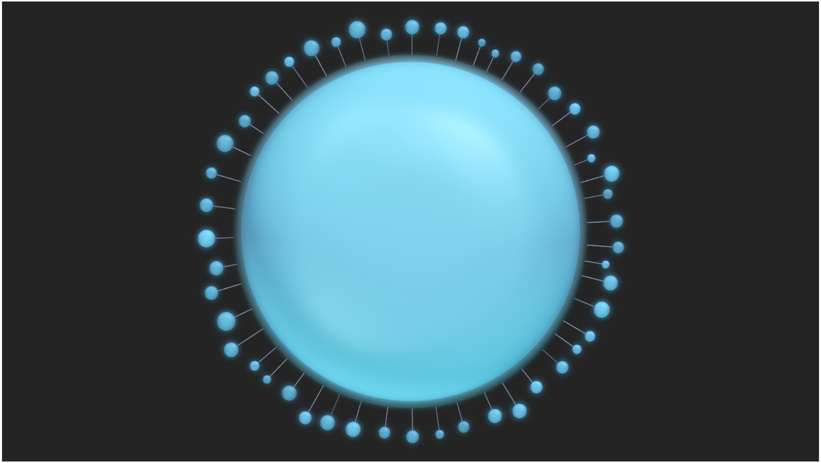
2016-03-04 Fri

Who am I?

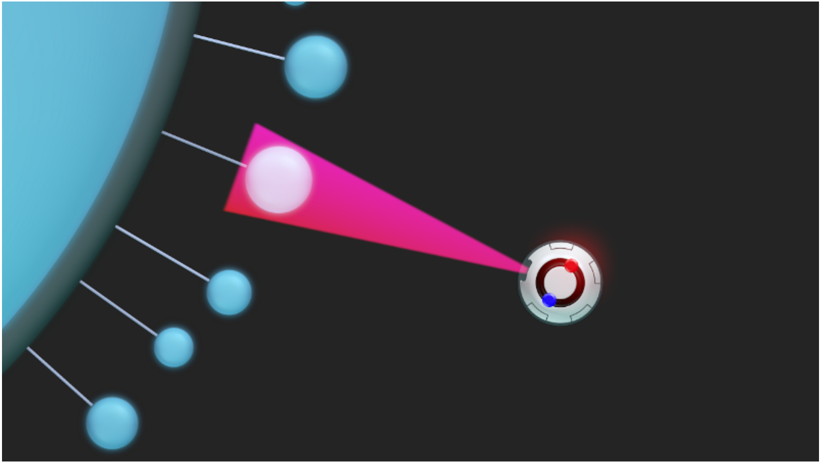
The web we want



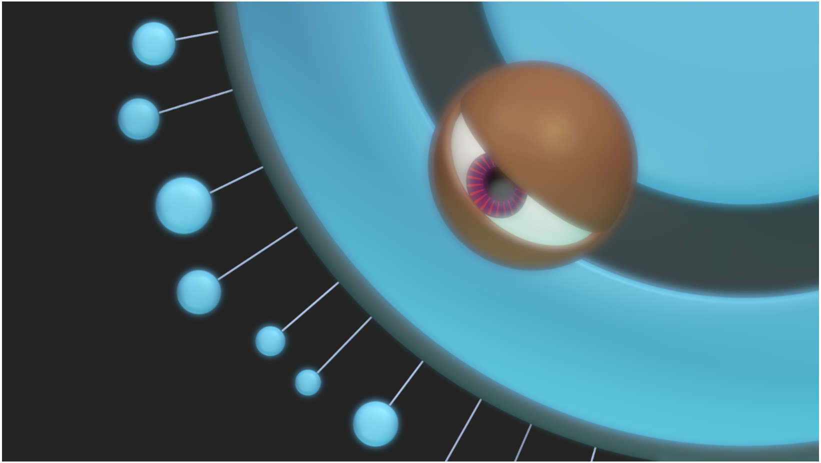
The sad reality (centralization)



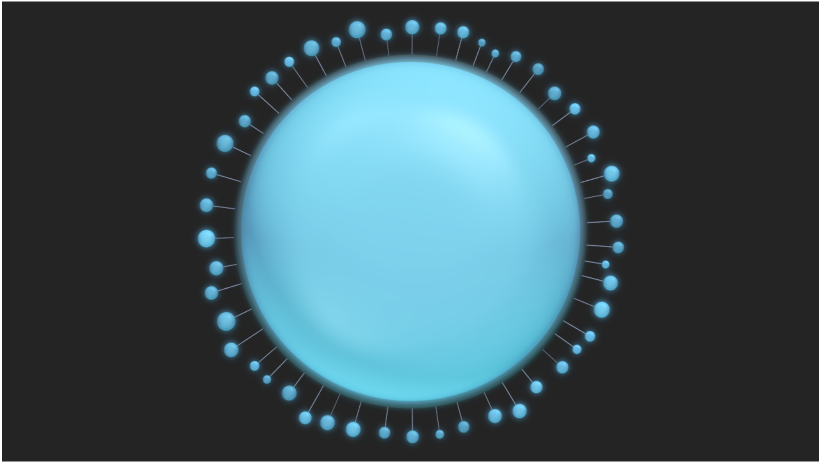
The sad reality (censorship)



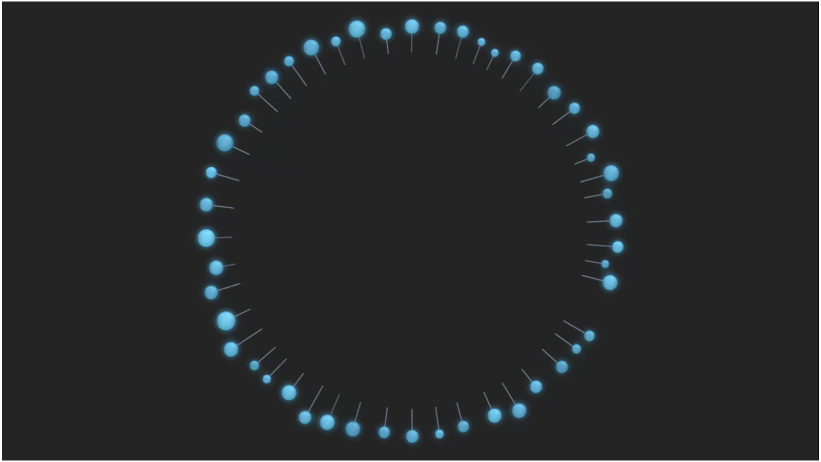
The sad reality (surveillance)



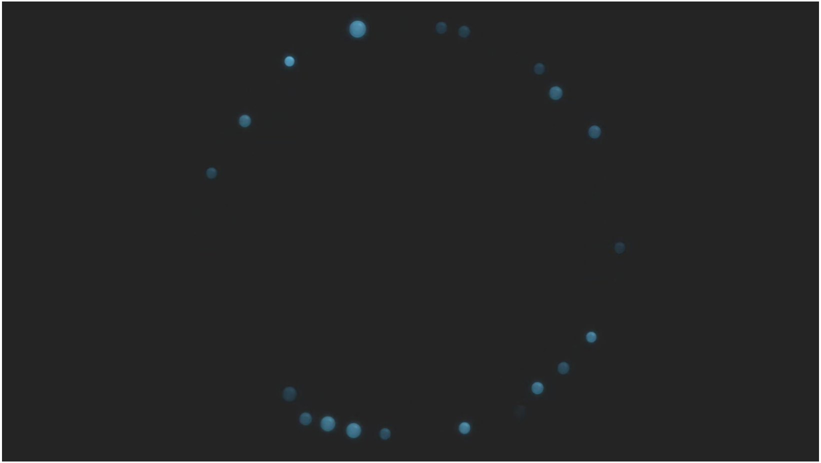
The sad reality (fragility)



The sad reality (fragility)



The sad reality (fragility)



The sad reality (fragility)

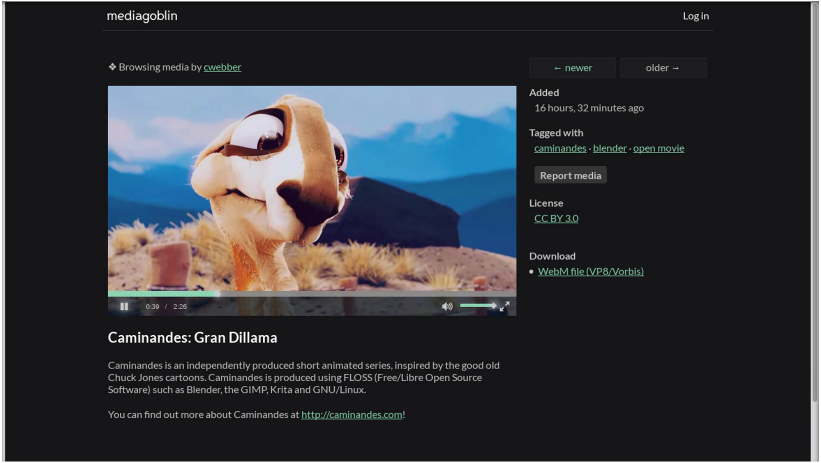
So I work on MediaGoblin...

Cupcake!

Uploaded on 2011-10-26 by main

We got these treats over at Sally's Cupcakes. They were SOOO good!

Decentralized media publishing



❖ Browsing media by cwebber

Added
16 hours, 32 minutes ago

Tagged with
caminandes · blender · open movie

License
CC BY 3.0

Download
- WebM file (VP8/Vorbis)

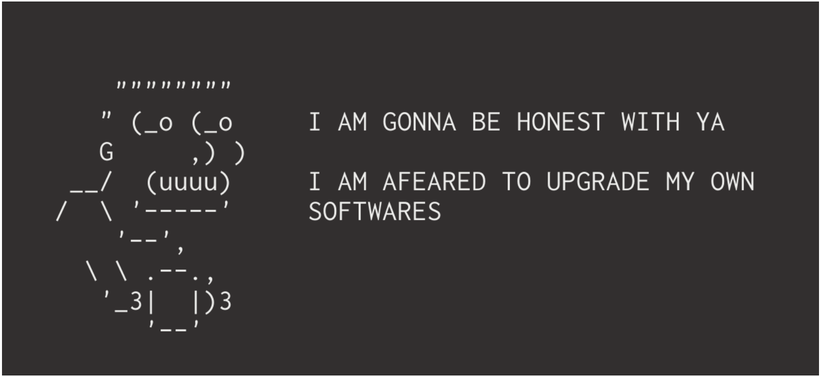
Caminandes: Gran Dillama

Caminandes is an independently produced short animated series, inspired by the good old Chuck Jones cartoons. Caminandes is produced using FLOSS (Free/Libre Open Source Software) such as Blender, the GIMP, Krita and GNU/Linux.

You can find out more about Caminandes at http://caminandes.com!

Sounds great! But???

Stuff is complex to run



```
    """"""""
   " (_o (_o        I AM GONNA BE HONEST WITH YA
   G      ,) )
 __/  (uuuu)        I AM AFEARED TO UPGRADE MY OWN
/  \ '-----'        SOFTWARES
    '__',
  \ \ .--.,
   '_3|  |)3
      '__'
```

Dependent on phase of the moon

One Language Package Manager Per Child

Have fun managing configuration

So... docker??? (Or something like it?)

```
                       __
                    __|II|      ,.
                 __|II|II|__   (  \_,/\
-.-'-.-'-.-'- __|II|II|II|II|___/   __/ -'-.-'-.-'-
------------ |      [Docker]       / ---------------
------------ :                    / ----------------
------------- \____, o          ,' -----------------
-------------- '--,___________,'  ------------------
```

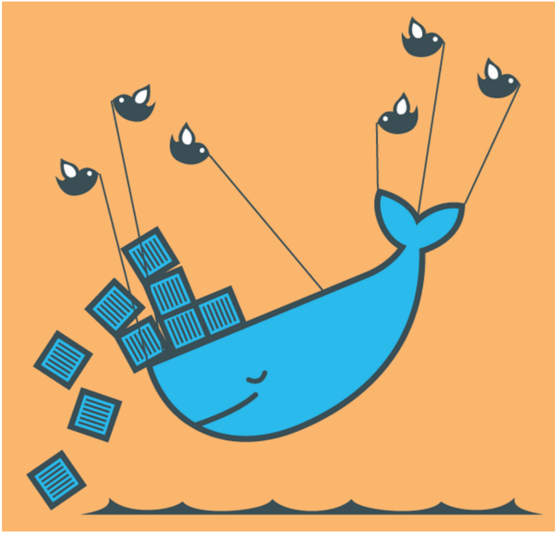
Easy for users! "I already built this for you, just pull it down and use it!"

Maybe not :(

Distro-sized static compiling considered hazardous

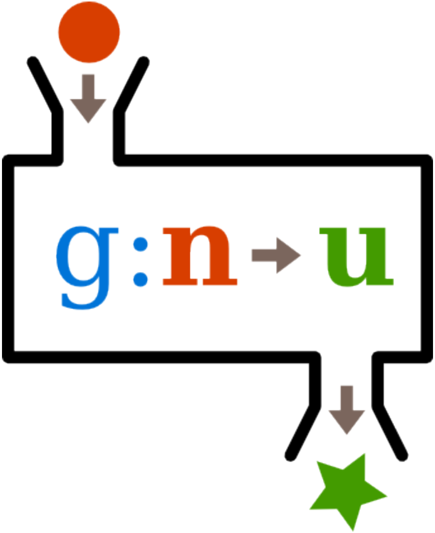
- Extremely heavy: throws away dynamic linking
- Hard to introspect, rebuild
- Analysis of Docker Hub: over 70% have medium vulnerabilities, 30-40% high (shellshock, heartbleed) vulnerabilities `http://www.banyanops.com/blog/analyzing-docker-hub/`
- Reproducible? Only kinda... Docker's DSL is not expressive, and..
- Still dependent on "phase of the moon" of distributions!

And so here we are

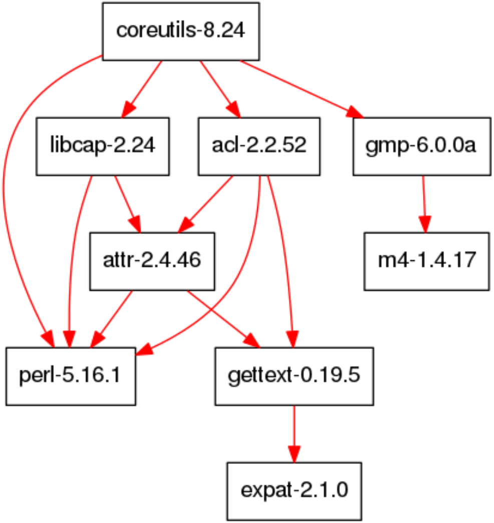


Enter Guix! Enter GuixSD!

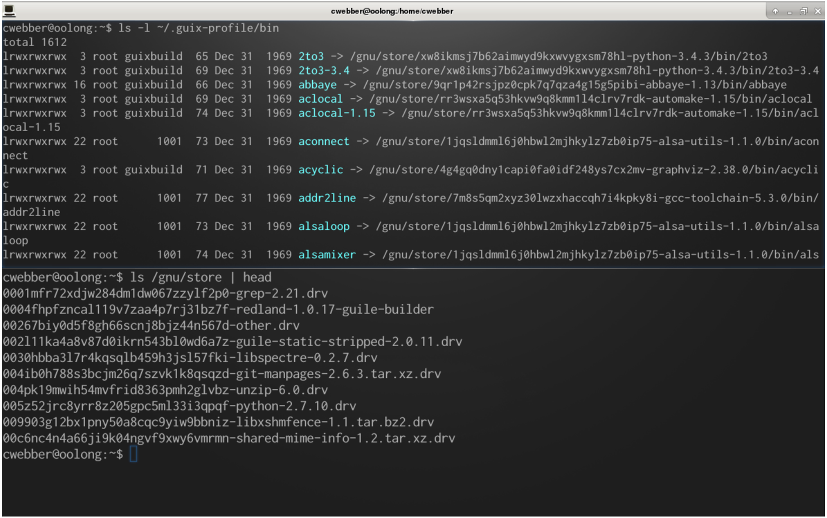
Functional packaging (hold the monads!)



All the way down!



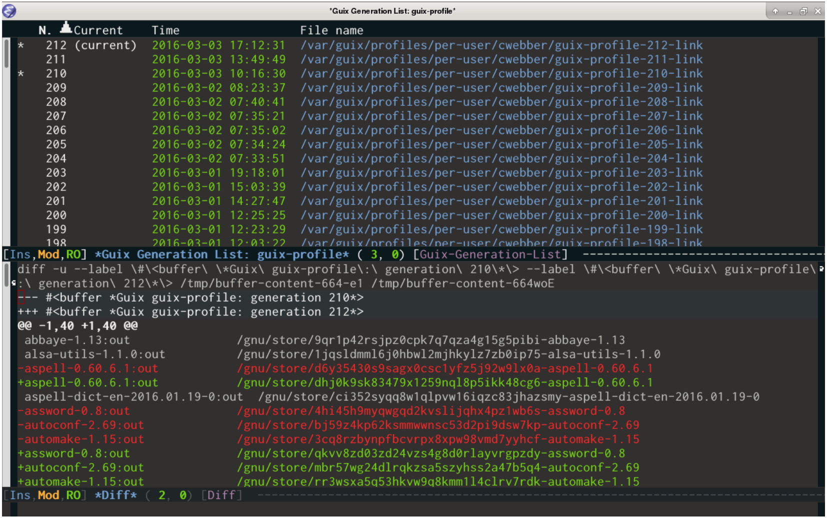
Like git, for your operating system!



```
cwebber@oolong:~$ ls -l ~/.guix-profile/bin
total 1612
lrwxrwxrwx  3 root guixbuild  65 Dec 31  1969 2to3 -> /gnu/store/xw8ikmsj7b62aimwyd9kxwvygxsm78hl-python-3.4.3/bin/2to3
lrwxrwxrwx  3 root guixbuild  69 Dec 31  1969 2to3-3.4 -> /gnu/store/xw8ikmsj7b62aimwyd9kxwvygxsm78hl-python-3.4.3/bin/2to3-3.4
lrwxrwxrwx 16 root guixbuild  66 Dec 31  1969 abbaye -> /gnu/store/9qr1p42rsjpz0cpk7q7qza4g15g5pibi-abbaye-1.13/bin/abbaye
lrwxrwxrwx  3 root guixbuild  69 Dec 31  1969 aclocal -> /gnu/store/rr3wsxa5q53hkvw9q8kmm1l4clrv7rdk-automake-1.15/bin/aclocal
lrwxrwxrwx  3 root guixbuild  74 Dec 31  1969 aclocal-1.15 -> /gnu/store/rr3wsxa5q53hkvw9q8kmm1l4clrv7rdk-automake-1.15/bin/acl
ocal-1.15
lrwxrwxrwx 22 root      1001  73 Dec 31  1969 aconnect -> /gnu/store/1jqsldmml6j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/acon
nect
lrwxrwxrwx  3 root guixbuild  71 Dec 31  1969 acyclic -> /gnu/store/4g4gq0dny1capi0fa0idf248ys7cx2mv-graphviz-2.38.0/bin/acycli
c
lrwxrwxrwx 22 root      1001  77 Dec 31  1969 addr2line -> /gnu/store/7m8s5qm2xyz30lwzxhaccqh7i4kpky8i-gcc-toolchain-5.3.0/bin/
addr2line
lrwxrwxrwx 22 root      1001  73 Dec 31  1969 alsaloop -> /gnu/store/1jqsldmml6j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/alsa
loop
lrwxrwxrwx 22 root      1001  74 Dec 31  1969 alsamixer -> /gnu/store/1jqsldmml6j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/als
```

```
cwebber@oolong:~$ ls /gnu/store | head
0001mfr72xdjw284dm1dw067zzylf2p0-grep-2.21.drv
0004fhpfzncal119v7zaa4p7rj31bz7f-redland-1.0.17-guile-builder
00267biy0d5f8gh66scnj8bjz44n567d-other.drv
002l11ka4a8v87d0ikrn543bl0wd6a7z-guile-static-stripped-2.0.11.drv
0030hbba3l7r4kqsqlb459h3jsl57fki-libspectre-0.2.7.drv
004ib0h788s3bcjm26q7szvk1k8qsqzd-git-manpages-2.6.3.tar.xz.drv
004pk19mwih54mvfrid8363pmh2glvbz-unzip-6.0.drv
005z52jrc8yrr8z205gpc5ml33i3qpqf-python-2.7.10.drv
009903g12bx1pny50a8cqc9yiw9bbniz-libxshmfence-1.1.tar.bz2.drv
00c6nc4n4a66ji9k04ngvf9xwy6vmrmn-shared-mime-info-1.2.tar.xz.drv
cwebber@oolong:~$ 
```

Keep the history until you don’t need it



Guix Generation List: guix-profile

```
     N.  Current    Time                 File name
 *   212 (current)  2016-03-03 17:12:31  /var/guix/profiles/per-user/cwebber/guix-profile-212-link
     211            2016-03-03 13:49:49  /var/guix/profiles/per-user/cwebber/guix-profile-211-link
 *   210            2016-03-03 10:16:30  /var/guix/profiles/per-user/cwebber/guix-profile-210-link
     209            2016-03-02 08:23:37  /var/guix/profiles/per-user/cwebber/guix-profile-209-link
     208            2016-03-02 07:40:41  /var/guix/profiles/per-user/cwebber/guix-profile-208-link
     207            2016-03-02 07:35:21  /var/guix/profiles/per-user/cwebber/guix-profile-207-link
     206            2016-03-02 07:35:02  /var/guix/profiles/per-user/cwebber/guix-profile-206-link
     205            2016-03-02 07:34:24  /var/guix/profiles/per-user/cwebber/guix-profile-205-link
     204            2016-03-02 07:33:51  /var/guix/profiles/per-user/cwebber/guix-profile-204-link
     203            2016-03-01 19:18:01  /var/guix/profiles/per-user/cwebber/guix-profile-203-link
     202            2016-03-01 15:03:39  /var/guix/profiles/per-user/cwebber/guix-profile-202-link
     201            2016-03-01 14:27:47  /var/guix/profiles/per-user/cwebber/guix-profile-201-link
     200            2016-03-01 12:25:25  /var/guix/profiles/per-user/cwebber/guix-profile-200-link
     199            2016-03-01 12:23:29  /var/guix/profiles/per-user/cwebber/guix-profile-199-link
     198            2016-03-01 12:03:22  /var/guix/profiles/per-user/cwebber/guix-profile-198-link
[Ins,Mod,RO] *Guix Generation List: guix-profile* ( 3, 0) [Guix-Generation-List] ----------------------------------
diff -u --label \#\<buffer\ \*Guix\ guix-profile\:\ generation\ 210\*\> --label \#\<buffer\ \*Guix\ guix-profile\
:\ generation\ 212\*\> /tmp/buffer-content-664-e1 /tmp/buffer-content-664woE
--- #<buffer *Guix guix-profile: generation 210*>
+++ #<buffer *Guix guix-profile: generation 212*>
@@ -1,40 +1,40 @@
 abbaye-1.13:out              /gnu/store/9qr1p42rsjpz0cpk7q7qza4g15g5pibi-abbaye-1.13
 alsa-utils-1.1.0:out         /gnu/store/1jqsldmml6j0hbwl2mjhkylz7zb0ip75-alsa-utils-1.1.0
-aspell-0.60.6.1:out          /gnu/store/d6y35430s9sagx0csc1yfz5j92w9lx0a-aspell-0.60.6.1
+aspell-0.60.6.1:out          /gnu/store/dhj0k9sk83479x1259nql8p5ikk48cg6-aspell-0.60.6.1
 aspell-dict-en-2016.01.19-0:out  /gnu/store/ci352syqq8w1qlpvw16iqzc83jhazsmy-aspell-dict-en-2016.01.19-0
-assword-0.8:out              /gnu/store/4hi45h9myqwgqd2kvslijqhx4pz1wb6s-assword-0.8
-autoconf-2.69:out            /gnu/store/bj59z4kp62ksmmwwnsc53d2pi9dsw7kp-autoconf-2.69
-automake-1.15:out            /gnu/store/3cq8rzbynpfbcvrpx8xpw98vmd7yyhcf-automake-1.15
+assword-0.8:out              /gnu/store/qkvv8zd03zd24vzs4g8d0rlayvrgpzdy-assword-0.8
+autoconf-2.69:out            /gnu/store/mbr57wg24dlrqkzsa5szyhss2a47b5q4-autoconf-2.69
+automake-1.15:out            /gnu/store/rr3wsxa5q53hkvw9q8kmm1l4clrv7rdk-automake-1.15
[Ins,Mod,RO] *Diff* ( 2, 0) [Diff] -------------------------------------------------------------------------------
```

You are now a time wizard.

```
# Bad upgrade?  No problem!
guix package --roll-back
```

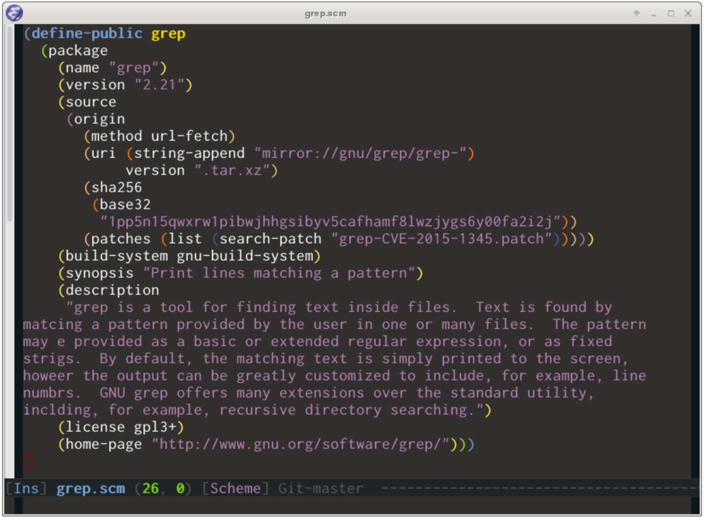
Your profile, my profile

- User profiles don't conflict with system profiles
- Local development environments with `guix environment`
- Need a different glibc or gcc or whatever? No problem!
- As many profiles as you want

Wait, why not Nix?

Guix is based on Nix's ideas! And Nix is super cool!
But it's hard to write tooling...

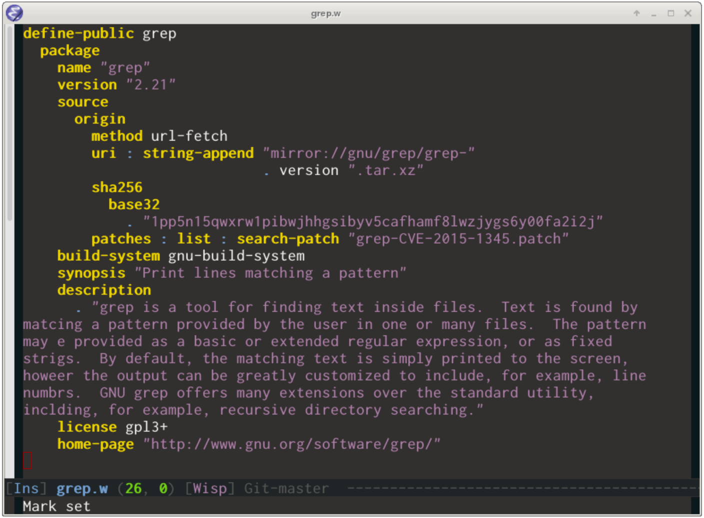
Guix is just scheme, yo



```
(define-public grep
  (package
    (name "grep")
    (version "2.21")
    (source
     (origin
       (method url-fetch)
       (uri (string-append "mirror://gnu/grep/grep-"
            version ".tar.xz"))
       (sha256
        (base32
         "1pp5n15qwxrw1pibwjhhgsibyv5cafhamf8lwzjygs6y00fa2i2j"))
       (patches (list (search-patch "grep-CVE-2015-1345.patch")))))
    (build-system gnu-build-system)
    (synopsis "Print lines matching a pattern")
    (description
     "grep is a tool for finding text inside files.  Text is found by
matcing a pattern provided by the user in one or many files.  The pattern
may e provided as a basic or extended regular expression, or as fixed
strigs.  By default, the matching text is simply printed to the screen,
howeer the output can be greatly customized to include, for example, line
numbrs.  GNU grep offers many extensions over the standard utility,
inclding, for example, recursive directory searching.")
    (license gpl3+)
    (home-page "http://www.gnu.org/software/grep/")))

[Ins] grep.scm (26, 0) [Scheme] Git-master ------------------------------------
```

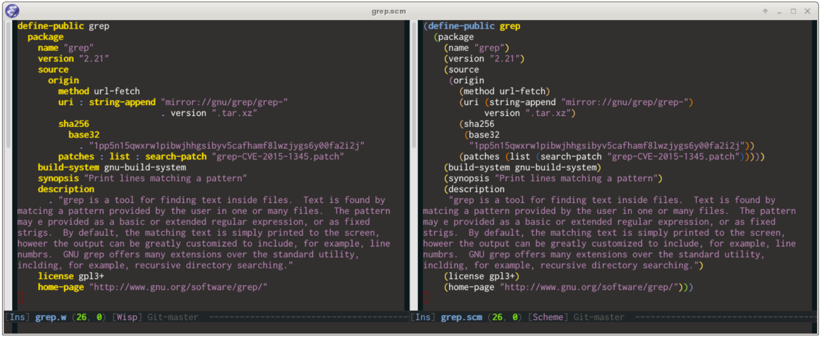
Oh no parentheses!?



```
define-public grep
  package
    name "grep"
    version "2.21"
    source
      origin
        method url-fetch
        uri : string-append "mirror://gnu/grep/grep-"
                            . version ".tar.xz"
        sha256
          base32
            . "1pp5n15qwxrw1pibwjhhgsibyv5cafhamf8lwzjygs6y00fa2i2j"
        patches : list : search-patch "grep-CVE-2015-1345.patch"
    build-system gnu-build-system
    synopsis "Print lines matching a pattern"
    description
      . "grep is a tool for finding text inside files.  Text is found by
matcing a pattern provided by the user in one or many files.  The pattern
may e provided as a basic or extended regular expression, or as fixed
strigs.  By default, the matching text is simply printed to the screen,
howeer the output can be greatly customized to include, for example, line
numbrs.  GNU grep offers many extensions over the standard utility,
inclding, for example, recursive directory searching."
    license gpl3+
    home-page "http://www.gnu.org/software/grep/"

[Ins] grep.w (26, 0) [Wisp] Git-master ------------------------------------------
Mark set
```

Parentheses: Not so foreign after all!



```
define-public grep
  package
    name "grep"
    version "2.21"
    source
      origin
        method url-fetch
        uri : string-append "mirror://gnu/grep/grep-"
                          . version ".tar.xz"
        sha256
          base32
            . "1pp5n15qwxrw1pibwjhhgsibyv5cafhamf8lwzjygs6y00fa2i2j"
        patches : list : search-patch "grep-CVE-2015-1345.patch"
    build-system gnu-build-system
    synopsis "Print lines matching a pattern"
    description
      . "grep is a tool for finding text inside files.  Text is found by
matcing a pattern provided by the user in one or many files.  The pattern
may e provided as a basic or extended regular expression, or as fixed
strigs.  By default, the matching text is simply printed to the screen,
howeer the output can be greatly customized to include, for example, line
numbrs.  GNU grep offers many extensions over the standard utility,
incldiing, for example, recursive directory searching."
    license gpl3+
    home-page "http://www.gnu.org/software/grep/"

[Ins] grep.w (26, 0) [Wisp] Git-master ------------------------------------
```

```
(define-public grep
  (package
    (name "grep")
    (version "2.21")
    (source
     (origin
       (method url-fetch)
       (uri (string-append "mirror://gnu/grep/grep-"
                  version ".tar.xz"))
       (sha256
        (base32
         "1pp5n15qwxrw1pibwjhhgsibyv5cafhamf8lwzjygs6y00fa2i2j"))
       (patches (list (search-patch "grep-CVE-2015-1345.patch")))))
    (build-system gnu-build-system)
    (synopsis "Print lines matching a pattern")
    (description
     "grep is a tool for finding text inside files.  Text is found by
matcing a pattern provided by the user in one or many files.  The pattern
may e provided as a basic or extended regular expression, or as fixed
strigs.  By default, the matching text is simply printed to the screen,
howeer the output can be greatly customized to include, for example, line
numbrs.  GNU grep offers many extensions over the standard utility,
incldiing, for example, recursive directory searching.")
    (license gpl3+)
    (home-page "http://www.gnu.org/software/grep/")))

[Ins] grep.scm (26, 0) [Scheme] Git-master ------------------------------------
```

Guix is a library, too

All datastructures, functions, etc exposed. Hack away!
With very little additional code, Guix(SD) has:

- Declarative config management (like Puppet, Chef, Salt, Ansible)
- Universal language packaging (apt, yum, pip/eggs, gems...)
- Local dev environments (virtualenv, rvm, rbenv...)
- Local VM tooling (Vagrant...)
- Container support (Docker, Rocket...)

Add your own tools here!

This just in: grafts!

State of Guix

- "It's still beta!"
- But probably more stable than most devops stuff
- A delight to run (I use it!)
- Easy to develop and get involved in

What's next?

- More packages! (~3350 at time of writing)
- Deployment tools (GuixOps!)
- Good UI tools needed! (Not just emacs and command line :))
- Some day soon we'll have to tackle the nightmare of npm
- Sandboxed containers!

A short story

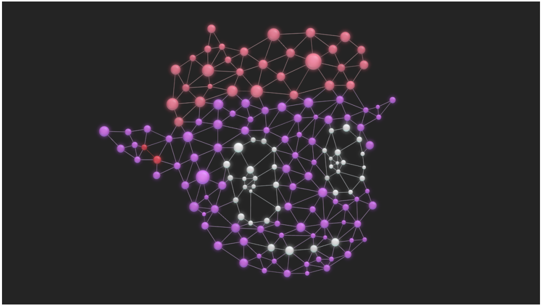
Credits (p.1)

- Moon image from *Le Voyage dans la lune* (A Trip to the Moon), public domain. Retrieved from: `https://en.wikipedia.org/wiki/A_Trip_to_the_Moon#/media/File:Le_Voyage_dans_la_lune.jpg`
- Tar pit image by Ray Bouknight, CC BY 2.0: `https://www.flickr.com/photos/raybouk/8341369957`
- Snowflake from zfootage, CC BY 4.0: `https://www.youtube.com/watch?v=Arw269x4duQ` `https://i.ytimg.com/vi/Arw269x4duQ/maxresdefault.jpg`
- Rena runs aground (container fail image), CC BY 2.0 `https://www.flickr.com/photos/nzdefenceforce/6386334175/`
- Tree grafting image, CC BY-SA 2.0 `https://www.flickr.com/photos/51691575@N00/2540483417`

Credits (p.2)

- Caminandes video screenshot by Blender Institute, CC BY 4.0 `http://www.caminandes.com/`
- Chemical warehouse image from Pixabay, CC0 `https://pixabay.com/en/warehouse-chemistry-industry-629641/`
- GuixSD logos by Luis Felipe López Acevedo, CC BY-SA 4.0 `http://www.gnu.org/software/guix/graphics/`
- Docker + Twitter image by Karen Rustad
- NixOS logo by NixOS team
- Some parts borrowed from David Tompson's presentation
- Slight snippet from Guix (grep package), GPLv3 or later
- Everything else by me (I think???)

Thanks! Questions? (Demonstrations?)



More on Guix: `https://gnu.org/software/guix`
More on MediaGoblin: `http://mediagoblin.org/`