Bootstrapping Intro – Current status
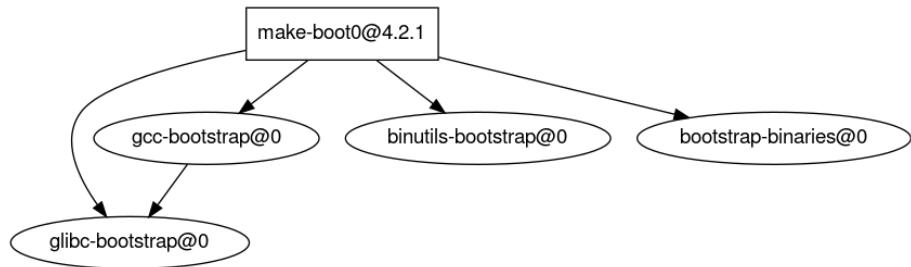
janneke@gnu.org

GNU Guix Days @FOSDEM'20

2020-01-30

Outline

1 Bootstrapping Guix v1.0

2 Aim for the Stars: Full Source Bootstrap

Guix v1.0: The First Package

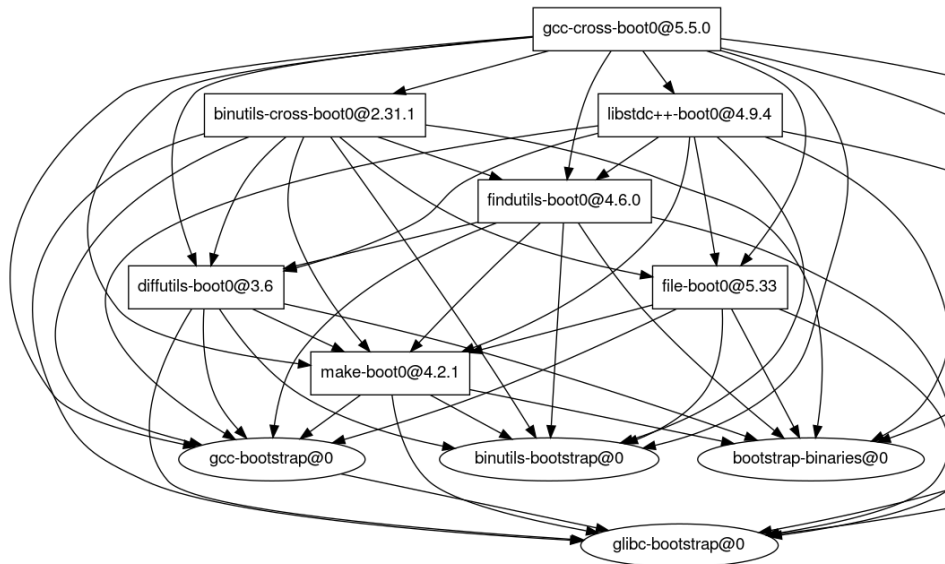# Guix Graph

```
$ guix graph make
$ guix graph make | dot -T png > make.png
$ guix graph -e '(@@ (gnu packages commencement) gnu-make-boot0
```

Guix v1.0: The First GCC

Guix bootstrap tarballs

```
$ guix build bootstrap-tarballs
```

Guix v1.0 bootstrap binary seed

```
$ du -schx $(readlink $(guix build bootstrap-tarballs)/*)
2.1M    /gnu/store/9623n4bq6iq5c8cwwdq99qb7d0xj93ym-binutils-st
18M     /gnu/store/437xwygmmwwpkddcyy1qvjcv4hak89pb-gcc-strippe
1.8M    /gnu/store/55ccx18a0d1x5y6a575jf1yr0ywizvdg-glibc-strip
5.7M    /gnu/store/bqf0ajclbvnbm0a46819f30804y3ilx0-guile-stati
5.8M    /gnu/store/j8yzjmh9sy4gbdfwjrhw46zca43aah6x-static-bina
33M     total
$ for i in $(readlink $(guix build bootstrap-tarballs)/*);\
  do sudo tar xf $i; done
$ du -schx *
130M    bin
13M     include
54M     lib
51M     libexec
5.2M    share
252M    total
```

Reduce binary seeds to bare minimum

These big chunks of binary code are practically non-auditable which breaks the source to binary transparency that we get in the rest of the package dependency graph.

Every unauditable binary leaves us vulnerable to compiler backdoors as described by Ken Thompson in the 1984 paper Reflections on Trusting Trust.

Thus, our goal is to reduce the set of bootstrap binaries to the bare minimum. – Ludovic Courtès (GNU Guix documentation, December 2017)

Guix Reduced Binary Seed

```
$ du -schx $(readlink $(guix build bootstrap-tarballs)/*)
5.7M    /gnu/store/9f8gi8raqfx9j3l9d00qrrc0jg3r1kyj-guile-stati
80K     /gnu/store/b6rjl52hibhmvyw4dg8678pwryhla0h2-linux-libre
12K     /gnu/store/d7zlxsjcnqilmvqwx7scija9x9bjw8cw-mescc-tools
428K    /gnu/store/n7zc4kpi8ny6jlfaikkzxlwhc5fvr1vr-mes-minimal
6.0M    /gnu/store/nv4djwlrljfqmynqr2cqvfwz0ydx7kxb-static-bina
13M     total
$ for i in $(readlink $(guix build bootstrap-tarballs)/*);\
  do sudo tar xf $i; done
Password:
$ du -schx *
93M     bin
700K    include
38M     lib
14M     share
145M    total
```

Guix Scheme-only bootstrap

```
$ du -schx $(readlink $(~/src/guix/wip-bootstrap/pre-inst-env g
5.7M    /gnu/store/1mq2pcd2h7g54xpi2jrgj6ibbi4lgi3c-guile-stati
80K     /gnu/store/bl1r2bpk6fam8r2gjvr5mvr48i3dm2hn-linux-libre
12K     /gnu/store/w0dlz486dhb8aiq8pxm5akllz628fqin-mescc-tools
428K    /gnu/store/15j6l18q44ymlrh1cfp4s4hc9835xic5-mes-minimal
6.2M    total
$ for i in $(readlink $(~/src/guix/wip-bootstrap/pre-inst-env g
  do sudo tar xf $i; done
$ du -schx *
4.9M    bin
700K    include
38M     lib
14M     share
57M     total
```
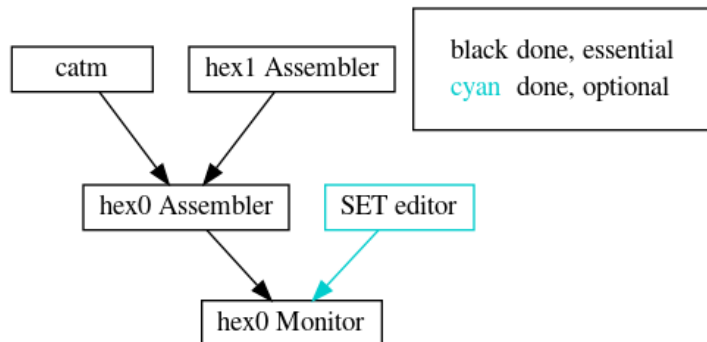
Scheme-only bootstrap: Gash Core Utils

```
awk        cp        gash    mv      sleep  uname
basename   cut       grep    pwd     sort   uniq
bash       diff      gzip    reboot  tar    wc
cat        dirname   head    rm      test   which
chmod      expr      ln      rmdir   touch
cmp        false     ls      sed     tr
compress   find      mkdir   sh      true
```
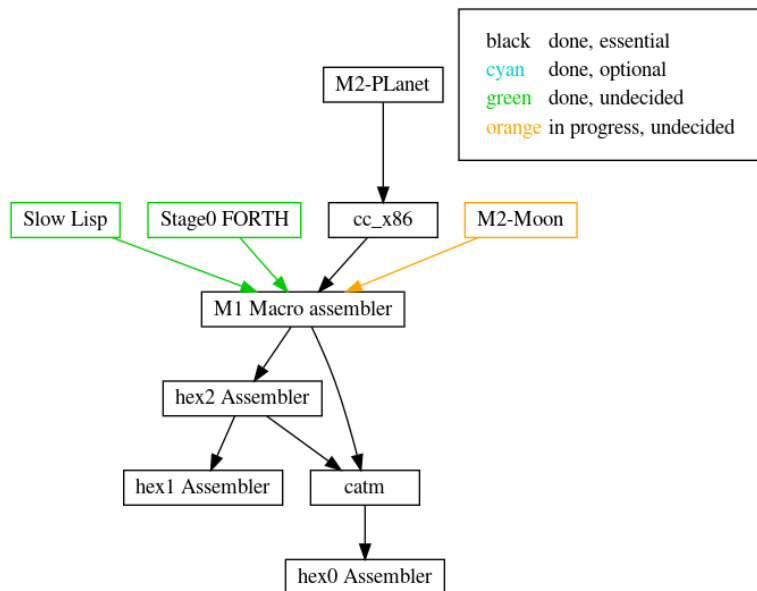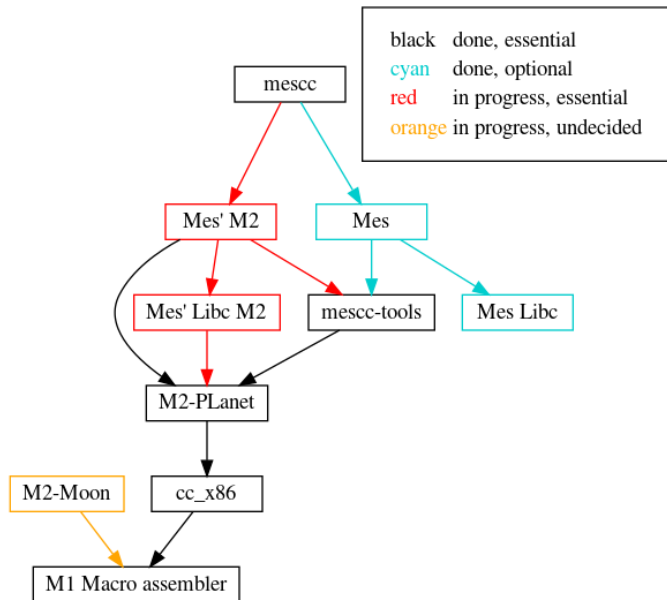
Full Source Bootstrap

Full Source Bootstrap: Stage 0

Full Source Bootstrap: Stage 1

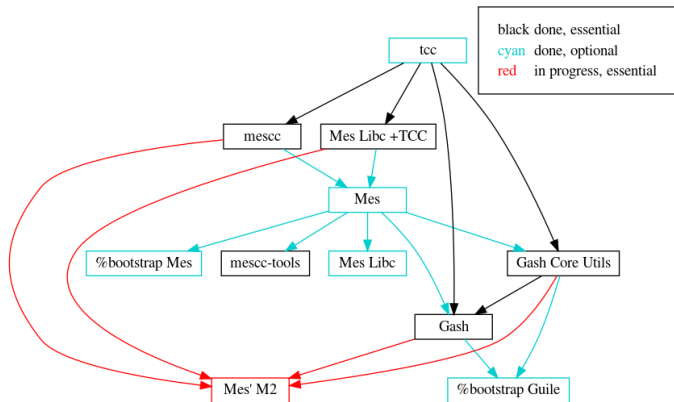# Full Source Bootstrap: Stage 2

Full Source Bootstrap: Stage mes

Full Source Bootstrap: Stage mesboot