Arch Linux Reproducible Builds

Are we reproducible yet?!

Jelle van der Waa jelle@archlinux.org
Overview

1. About me
2. Reproducible builds
3. Arch Reproducible
4. Questions
$ whoami

- Joined Arch Linux in 2010
- Developer @ Arch Linux (since 2017)
- Involved in the security/devops team
Reproducible Builds

“reproducible” builds enable anyone to reproduce the exact same binary packages from a given source
Why

- Verification of repository packages
Benefits

- Repo packages can be verified by users
- (Secure) automation
- Deterministic builds
Issues

- Timestamps
- private keys!
- timezones
- hashes
- python2
Diffoscope

Awesome tool to diff arbitrary files

- Supports tons of file formats
- `pacman -S diffoscope`
Diffoscope example

$ diffoscope awesome-4.2-1-x86_64.pkg.tar.xz /tmp/awesome-4.2-1-

-  <li><a href="/classes/tag.html#beautiful.master_width_
-  <li><a href="/classes/tag.html#tag.master_fill_p
+  <li><a href="/classes/tag.html#tag.master_width_
+  <li><a href="/classes/tag.html#beautiful.master_

See also:

https://tests.reproducible-builds.org/archlinux/community/awesome/awesome-4.2-1-x86_64.pkg.tar.xz.html
Arch Reproducible

- Reproducing packages continuously
- Multiple variations

https://tests.reproducible-builds.org/archlinux/archlinux.html
Pacman changes

- BUILDINFO support
- SOURCE_DATE_EPOCH support
- Removing timestamp from PKGINFO/MTREE
BUILDINFO

Describes the build env where a package was build

$ tar xvf glibc-2.28-4-x86_64.pkg.tar.xz .BUILDINFO
$ cat .BUILDINFO
format = 1
pkgname = glibc
pkgbase = glibc
pkgver = 2.28-4
pkgarch = x86_64
pkgbuild_sha256sum = af410234b2184...
... 
installed = acl-2.2.53-1-x86_64
installed = archlinux-keyring-20180808-1-any

man BUILDINFO
Goal

- User verifiable builds
- Arch official rebuild infra
Work In Progress

- Devtools-repro
- Tool to reproduce/check repo packages
- still unofficial

https://github.com/Foxboron/devtools-repro
Repro build

- Build a package twice for reproducibility

```bash
$ repro build
  ==> Using SOURCE_DATE_EPOCH: 1535055076
  ==> Starting build1...
  ...
  ==> Starting build2...
    - Create snapshot for build2...
  ==> Settings build environment...
  export TZ=/usr/share/zoneinfo/Etc/GMT-14
  export LANG=fr_CH.UTF-8
  ==> Comparing hashes...
    - acl-2.2.53-1-x86_64.pkg.tar.xz from build2 is reproducible
  ==> Package is reproducible!
```
Repro check

- Verify a repo package

repro check filesystem-2018.8-1-x86_64.pkg.tar.xz

... 

  --> Preparing packages
  Downloading acl-2.2.53-1-x86_64.pkg.tar.xz
  Downloading archlinux-keyring-20180808-1-any.pkg.tar.xz

  --> Package is not reproducible!
Help out

- #reproducible-builds
- #archlinux-reproducible
- work on repro issues
Questions