You think you're not a target?
A tale of 3 developers…

Chris Lamb
@lolamby
Debian Project Leader

FLOSSUK 2018
26th April 2018
Edinburgh, Scotland

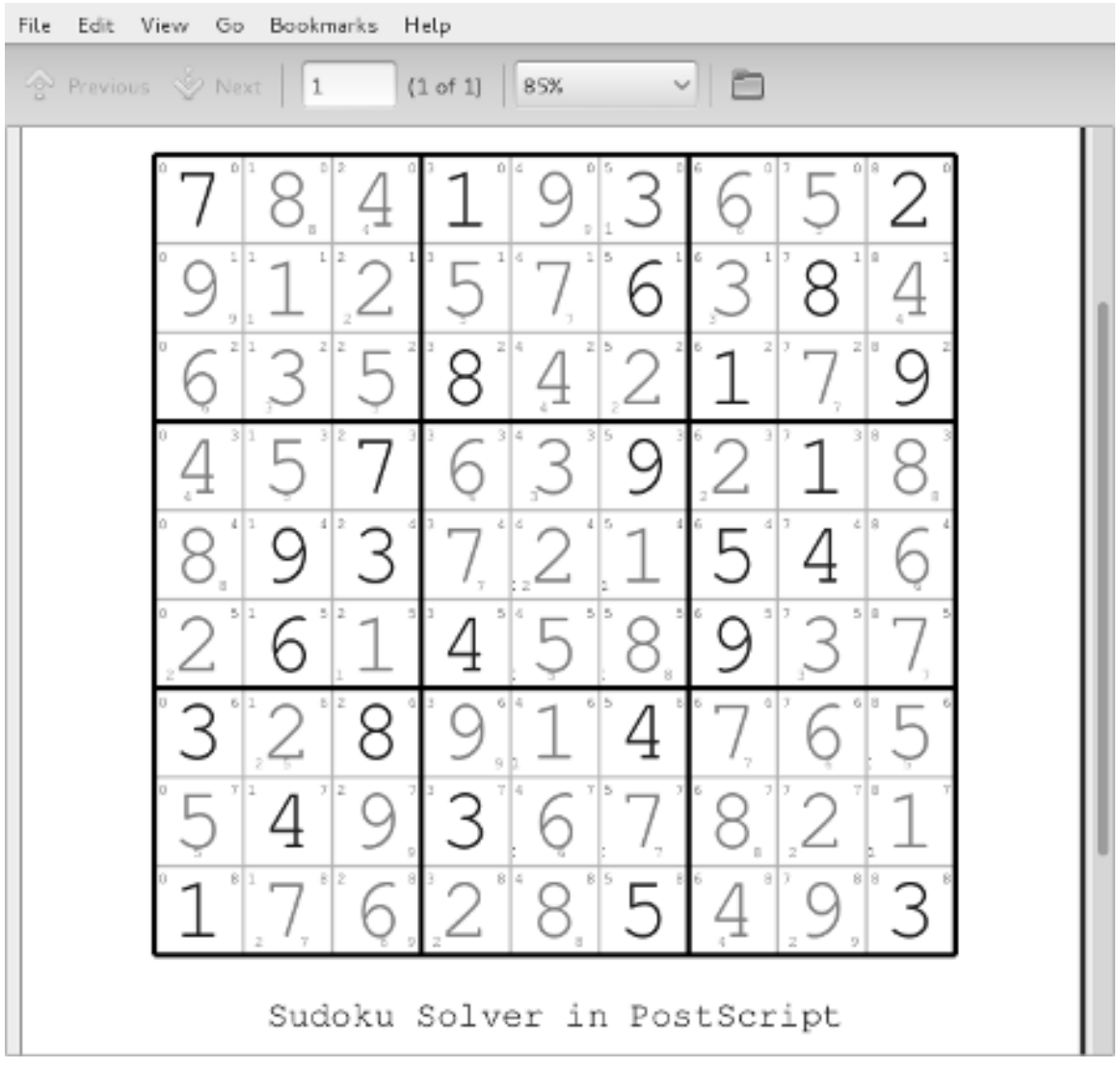
Cambridge
Analytica

Debian Project Leader

OpenSource.org Board Member

Free software developer for 10+ years

Freelance software developer


File Edit View Go Bookmarks Help
Previous
Next
1
(1 of 1)
85%
7 8 4 1 9 3 6 5 2
9 1 2 5 7 6 3 8 4
6 3 5 8 4 2 1 7 9
4 5 7 6 3 9 2 1 8
8 9 3 7 2 1 5 4 6
2 6 1 4 5 8 9 3 7
3 2 8 9 1 4 7 6 5
5 4 9 3 6 7 8 2 1
1 7 6 2 8 5 4 9 3
Sudoku Solver in PostScript

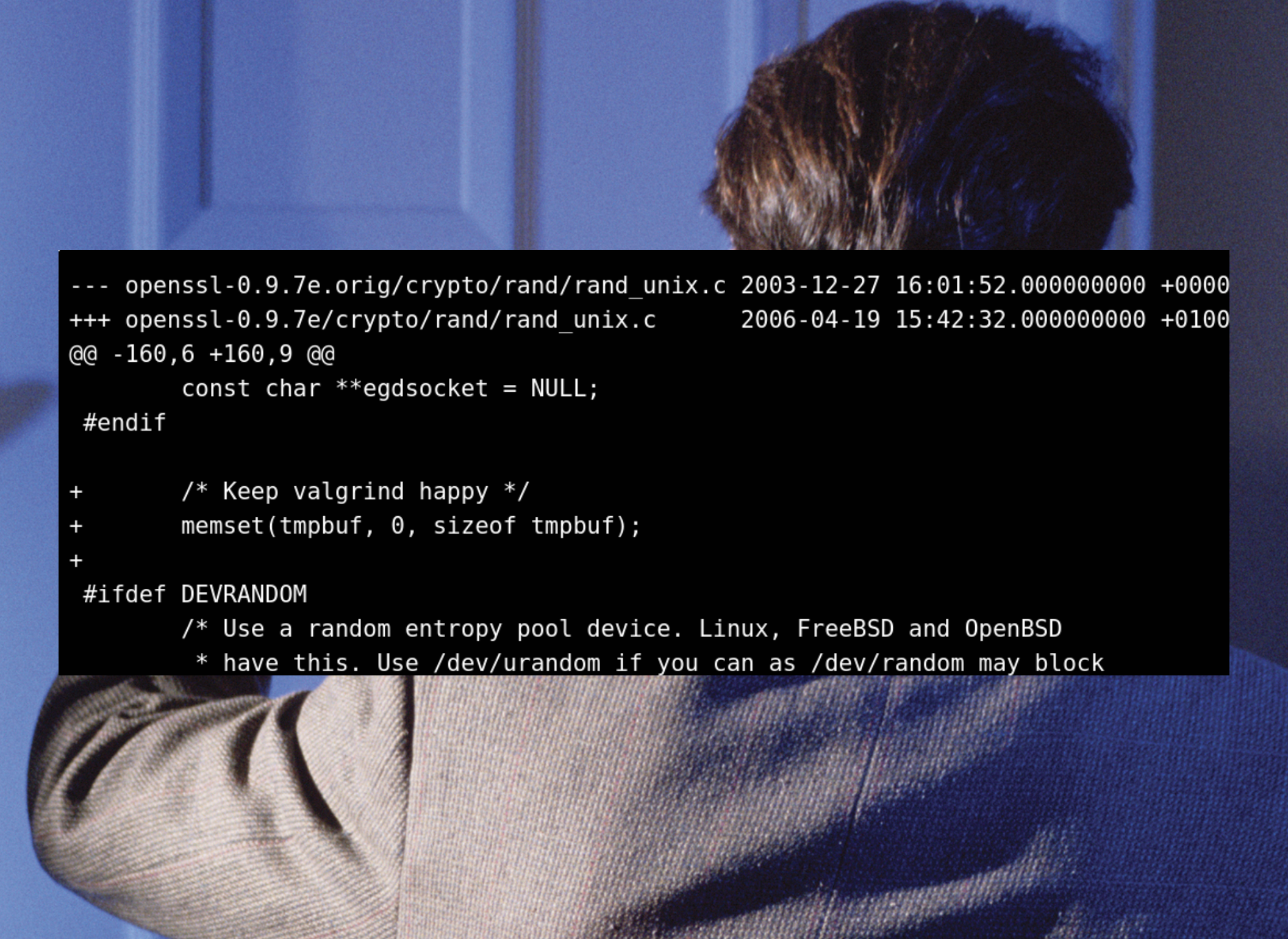
Three developers…


Alice


e lists... Done
dency tree... Done
extra packages will be installed:
apache2-data apache2-utils file libalgorithm-c3-perl libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
xtract-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libbareword-filehandles-perl libcgi-fast-perl li
perl libclass-c3-xs-perl libclass-method-modifiers-perl libclass-xsaccessor-perl libcpan-changes-perl libcpan-me
ist-perl libdata-perl-perl libdata-section-perl libdevel-caller-perl libdevel-globaldestruction-perl libdevel-le
cale-perl libexpat1 libexporter-tiny-perl libfcgi-perl libffi6 libfile-slurp-perl libgdbm3 libgetopt-long-descri
gnutls-deb0-28 libhogweed4 libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libicu
to-perl libindirect-perl libio-html-perl libio-stringy-perl libldap-2.4-2 liblexical-sealrequirehints-perl
utils-perl liblog-message-perl liblog-message-simple-perl liblua5.1-0 liblwp-mediatypes-perl libmagic1 libmodule
plementation-perl libmodule-pluggable-perl libmodule-runtime-perl libmodule-signature-perl libmoo-perl libmoox-
t-perl libmultidimensional-perl libnamespace-autoclean-perl libnamespace-clean-perl libnettle6 libnghttp2-14 li
onstants-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparam
lidate-perl libpath-tiny-perl libpod-latex-perl libpod-markdown-perl libpod-readme-perl librole-tiny-perl libsa
ules libsasl2-modules-db libsoftware-license-perl libsqlite3-0 libssl1.0.2 libstrictures-perl libsub-exporter-pe
ter-progressive-perl libsub-identify-perl libsub-install-perl libsub-name-perl libtasn1-6 libterm-ui-perl libte
late-perl libtimedate-perl libtry-tiny-perl libtype-tiny-perl libtype-tiny-xs-perl libunicode-utf8-perl liburi-p
magic-perl libxml2 mime-support openssl perl perl-modules rename sgml-base ssl-cert xml-core
ages:
apache2-doc apache2-suexec-pristine apache2-suexec-custom gnutls-bin libdata-dump-perl libscalar-number-perl
ules-otp libsasl2-modules-ldap libsasl2-modules-sql libsasl2-modules-gssapi-mit libsasl2-modules-gssapi-heimdal
cktrace-perl libwww-perl ca-certificates perl-doc libterm-readline-gnu-perl libterm-readline-perl-perl make libl
dist-build-perl libcpanplus-perl libfile-checktree-perl libobject-accessor-perl sgml-base-doc openssl-blacklist
NEW packages will be installed:
he2-bin apache2-data apache2-utils file libalgorithm-c3-perl libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libapru
xtract-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libbareword-filehandles-perl libcgi-fast-perl li
perl libclass-c3-xs-perl libclass-method-modifiers-perl libclass-xsaccessor-perl libcpan-changes-perl libcpan-me
ist-perl libdata-perl-perl libdata-section-perl libdevel-caller-perl libdevel-globaldestruction-perl libdevel-le
cale-perl libexpat1 libexporter-tiny-perl libfcgi-perl libffi6 libfile-slurp-perl libgdbm3 libgetopt-long-descri
gnutls-deb0-28 libhogweed4 libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libicu
to-perl libindirect-perl libio-html-perl libio-stringy-perl libldap-2.4-2 liblexical-sealrequirehints-perl
utils-perl liblog-message-perl liblog-message-simple-perl liblua5.1-0 liblwp-mediatypes-perl libmagic1 libmodule
plementation-perl libmodule-pluggable-perl libmodule-runtime-perl libmodule-signature-perl libmoo-perl libmoox-
t-perl libmultidimensional-perl libnamespace-autoclean-perl libnamespace-clean-perl libnettle6 libnghttp2-14 li
onstants-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparam
lidate-perl libpath-tiny-perl libpod-latex-perl libpod-markdown-perl libpod-readme-perl librole-tiny-perl libsa
ules libsasl2-modules-db libsoftware-license-perl libsqlite3-0 libssl1.0.2 libstrictures-perl libsub-exporter-pe
ter-progressive-perl libsub-identify-perl libsub-install-perl libsub-name-perl libtasn1-6 libterm-ui-perl libte
late-perl libtimedate-perl libtry-tiny-perl libtype-tiny-perl libtype-tiny-xs-perl libunicode-utf8-perl liburi-p
magic-perl libxml2 mime-support openssl perl perl-modules rename sgml-base ssl-cert xml-core
4 newly installed, 0 to remove and 1 not upgraded.
.8 MB of archives.
ration, 97.9 MB of additional disk space will be used.
continue? [Y/n]


Bob
AR-15
RAIDMAX


Bob's Privacy Browser
Download Source
or
Download .exe / .deb / .rpm


--- openssl-0.9.7e.orig/crypto/rand/rand_unix.c 2003-12-27 16:01:52.000000000 +0000
+++ openssl-0.9.7e/crypto/rand/rand_unix.c 2006-04-19 15:42:32.000000000 +0100
@@ -160,6 +160,9 @@
const char **egdsocket = NULL;
#endif
+ /* Keep valgrind happy */
+ memset(tmpbuf, 0, sizeof tmpbuf);
+
#ifdef DEVRANDOM
/* Use a random entropy pool device. Linux, FreeBSD and OpenBSD
* have this. Use /dev/urandom if you can as /dev/random may block


Bob's Privacy Browser
Download Source
Download .zip / .deb / .rpm


← Caro


Eve

The four essential freedoms

A program is free software if the program's users have the four essential freedoms:

- The freedom to run the program as you wish, for any purpose (freedom 0).
- The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

Alice

Servers attacked

Bob

Blackmailed

Carol

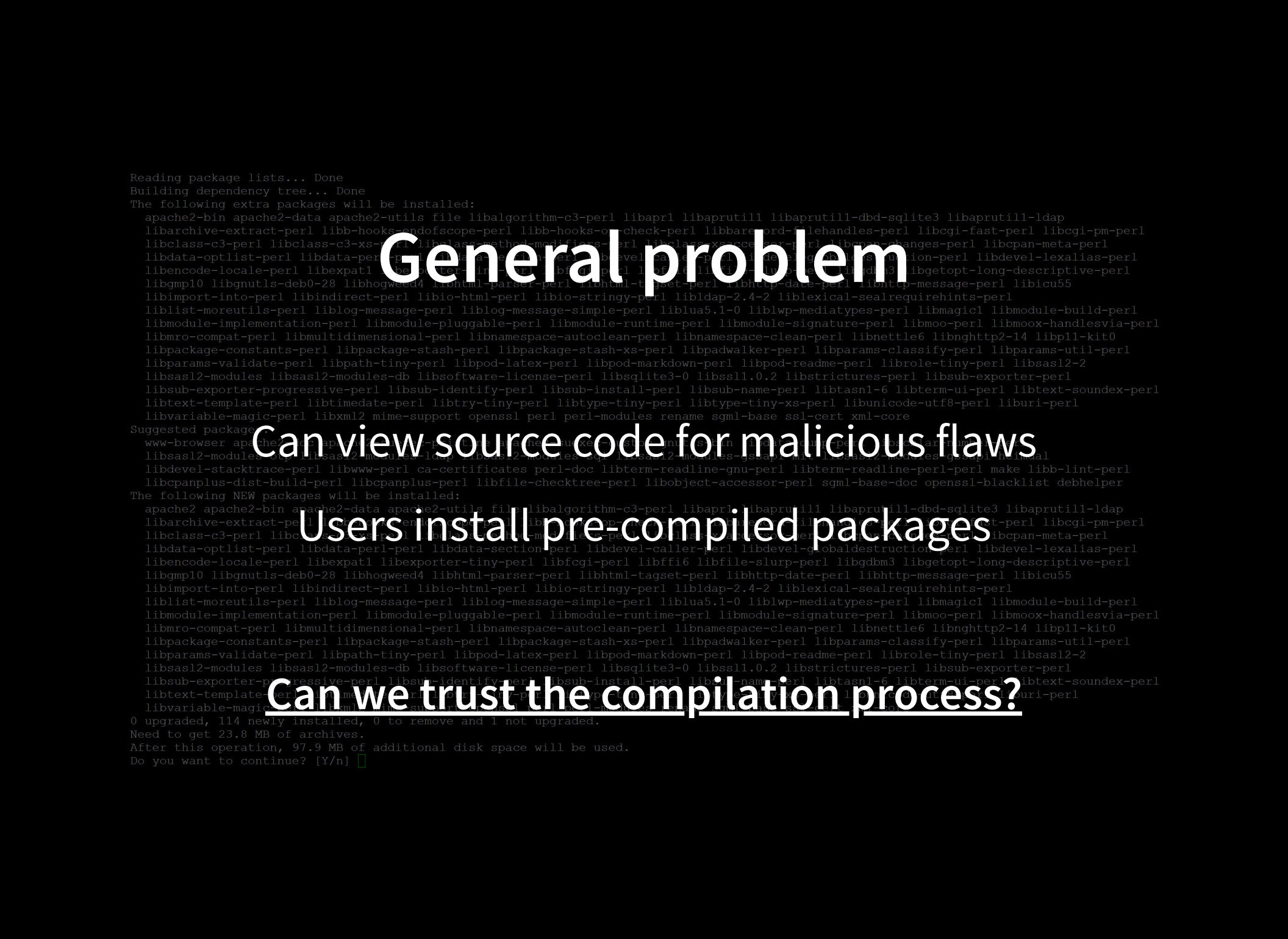
Compromised laptop

All are "good guys"

My good guys are your…

Disincentives to share

Cannot trust their binaries



General problem

Can view source code for malicious flaws

Users install pre-compiled packages

Can we trust the compilation process?

cker explains how he put "backdoor" in hundreds of Linux Mi wnloads

hacker said their prime motivation for the backdoor was to build a botnet.

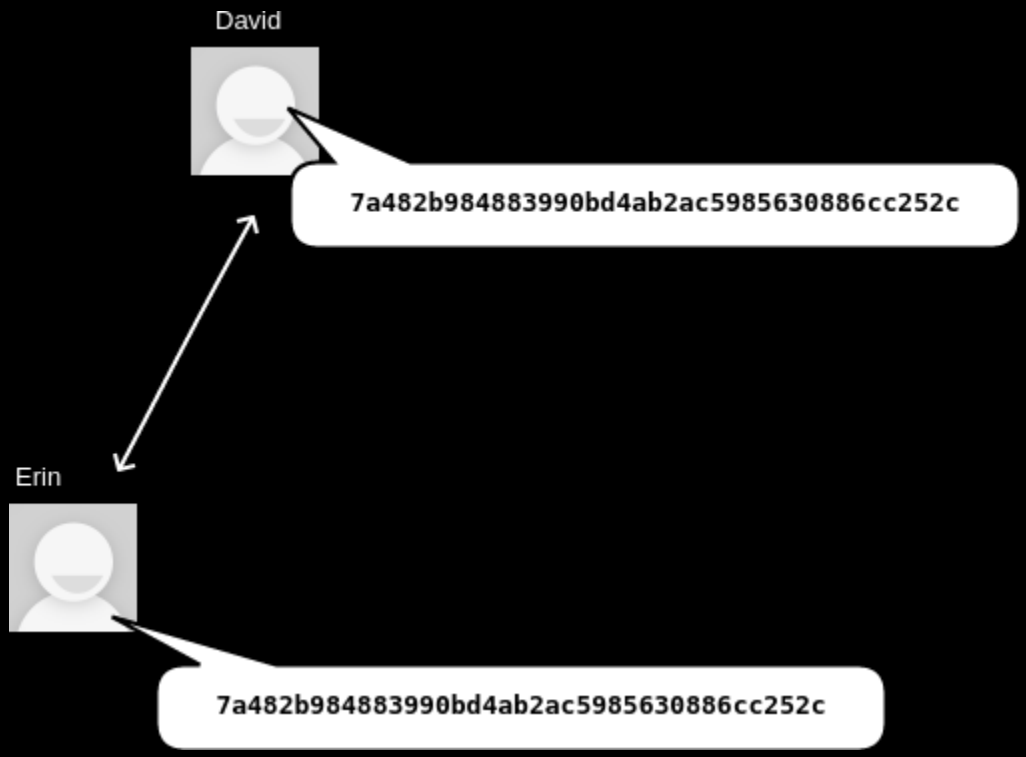
Solution?

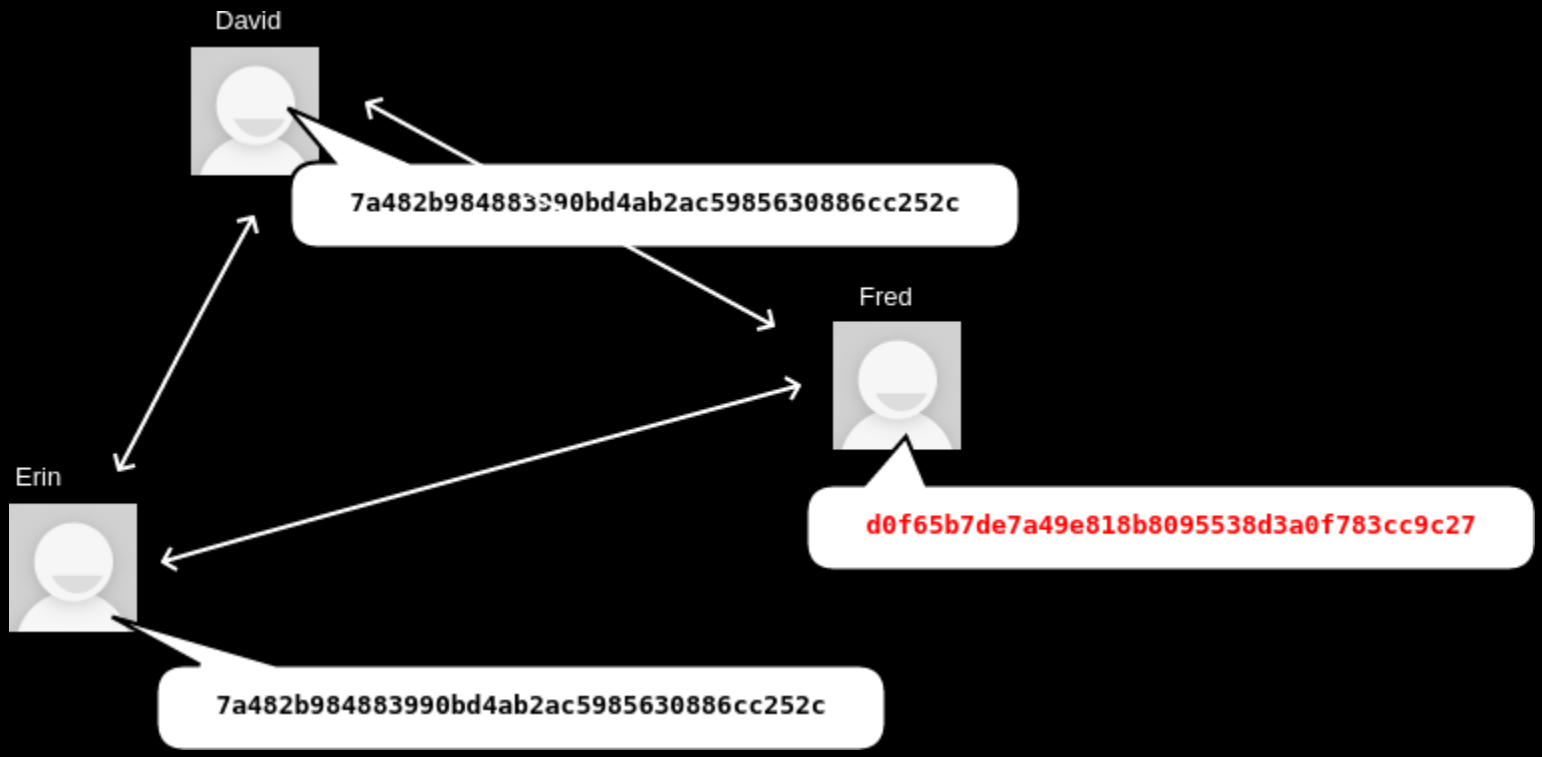
By Zack Whittaker for Zero Day | February 22, 2016 -- 01:28 GMT (01:28 GMT) | Topic: Security

2. Ensure builds always

3. Compare results


David
7a482b984883990bd4ab2ac5985630886cc252c


David
7a482b984883990bd4ab2ac5985630886cc252c
Erin
7a482b984883990bd4ab2ac5985630886cc252c


David
7a482b984883990bd4ab2ac5985630886cc252c
Fred
Erin
d0f65b7de7a49e818b8095538d3a0f783cc9c27
7a482b984883990bd4ab2ac5985630886cc252c

How does this help?

Alice → Attack detected

Bob → Blackmail uncovered

Carol → Compromised laptop detected

Reduces incentive to attack in the first place

"Builds with the same dependencies"... ✖

"Reliable" builds... ✖

Identical build results

Wait…

Timestamps

Users, groups, `umask`, environment variables, etc.

Build paths

File ordering

Dictionary key ordering

Parallelism in build output

Other advantages?

Minimal diffs on "deliberate" changes

Find unnecessary build-dependencies

Cache ratio — save time, money & CO_2

Finds bugs ahead of time

Predictable OpenID secret

```
# Build.PL
$build->config_data(OpenIDConsumerSecret=>int(1e15*rand()));


# /usr/share/perl5/GBrowse/ConfigData.pm
{
 'OpenIDConsumerSecret' => '639098210478536',
 'cgibin' => '/usr/lib/cgi-bin/gbrowse',
 'conf' => '/etc/gbrowse',
 [..]
},
```

Every installation of this build shared the same secret

Debian & reproducible builds

Torture test

Time & date

Hostname & domain name

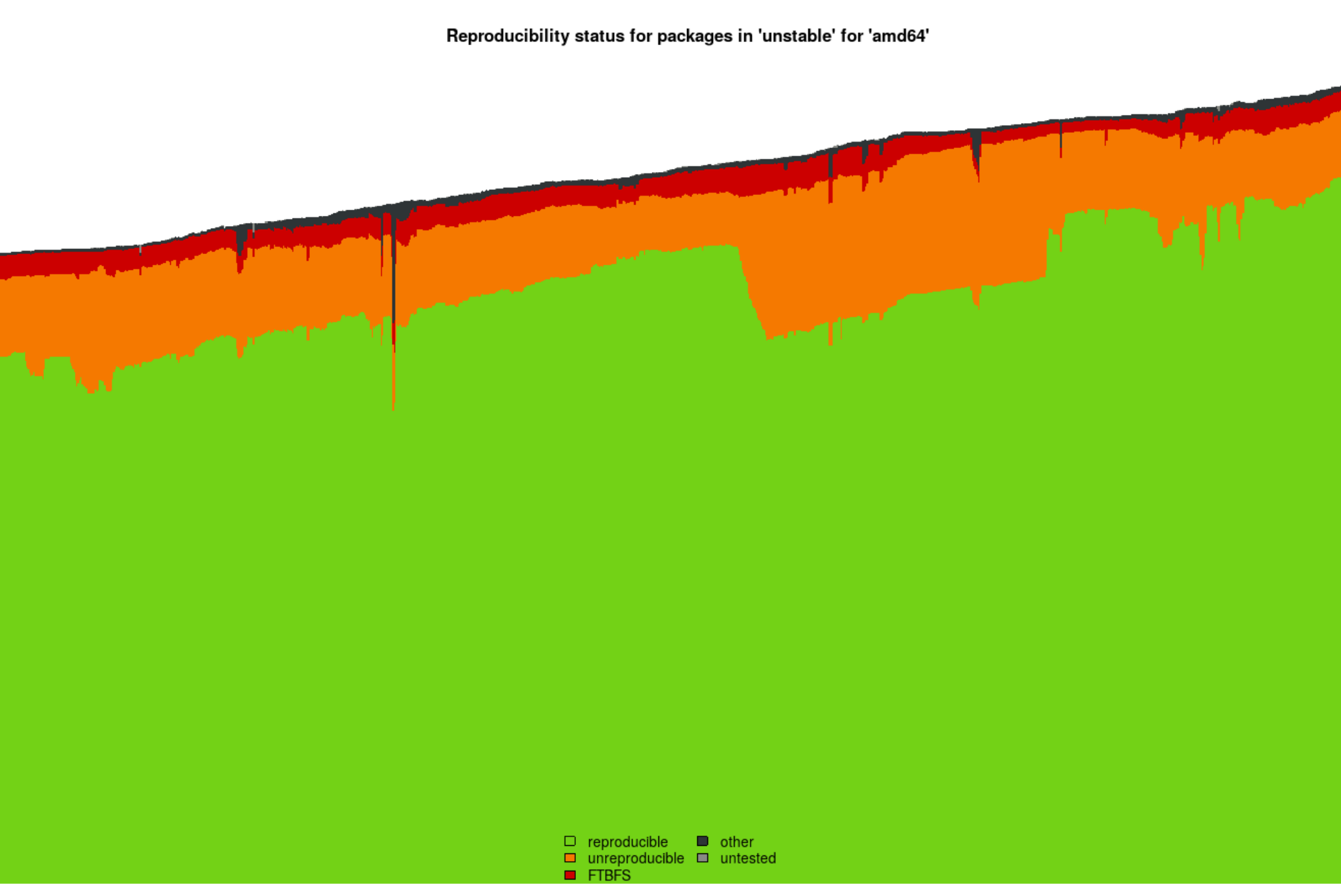
Filesystem (`disorderfs`)

Timezone & locale

`uid` & `gid`

Kernel & CPU type

First rebuild in 2013	24% packages reproducible
March 2018	93% packages reproducible


Reproducibility status for packages in 'unstable' for 'amd64'
reproducible
unreproducible
FTBFS
other
untested
-02-12
2015-04-20
2015-06-26
2015-09-01
2015-11-07
2016-01-13
2016-03-20
2016-05-26
2016-08-01
2016-10-07
2016-12-13
2017-02-18
2017-04-26
2017-07-02
2017-09-07

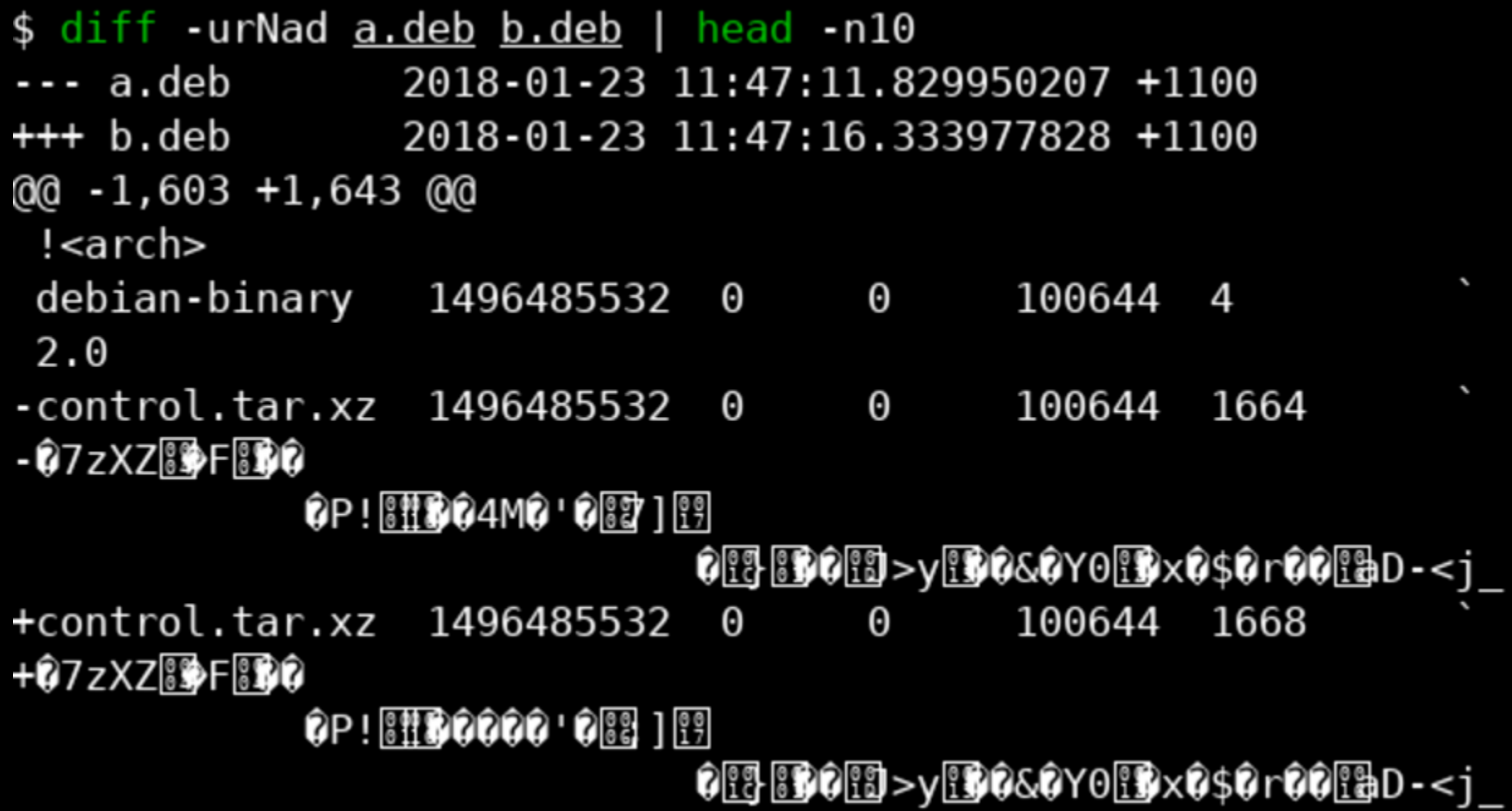
isdebianreproducibleyet.com

Beyond Debian…

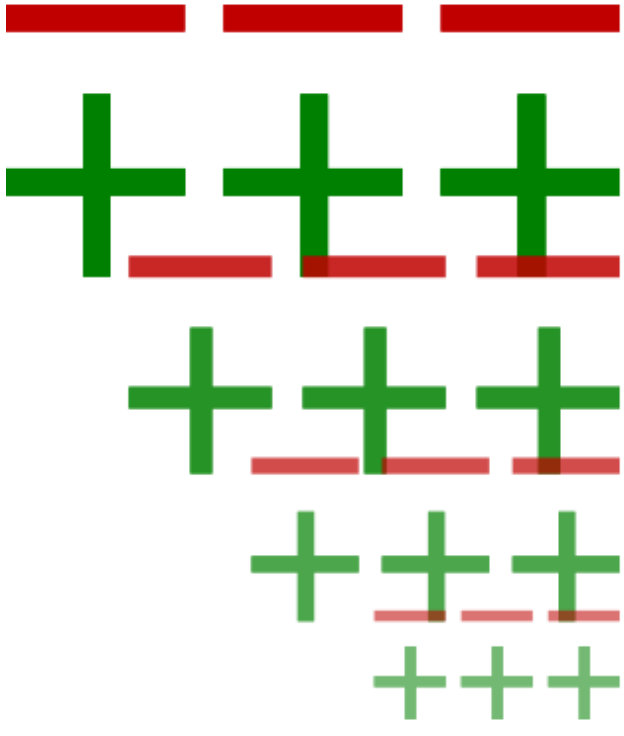
coreboot, Fedora, LEDE, OpenWRT, NetBSD, FreeBSD, Archlinux, Qubes, F-Droid, NixOS, Guix, Meson, etc.

Reproducible Builds summits (Athens, Berlin)

```
# diff -urNad file1 file2
--- file1  2017-06-18 12:37:03.179186661 +0800
+++ file2  2017-06-18 12:37:04.811193648 +0800
@@ -1 +1 @@
-This is the first file.
+This is the second file.
```


$ diff -urNad a.deb b.deb | head -n10
--- a.deb 2018-01-23 11:47:11.829950207 +1100
+++ b.deb 2018-01-23 11:47:16.333977828 +1100
@@ -1,603 +1,643 @@
!<arch>
debian-binary 1496485532 0 0 100644 4 `
2.0
-control.tar.xz 1496485532 0 0 100644 1664 `
-7zXZ F
P! 4M']
>y &Y0 x $ r aD-<j_
+control.tar.xz 1496485532 0 0 100644 1668 `
+7zXZ F
P! ']
>y &Y0 x $ r aD-<j_

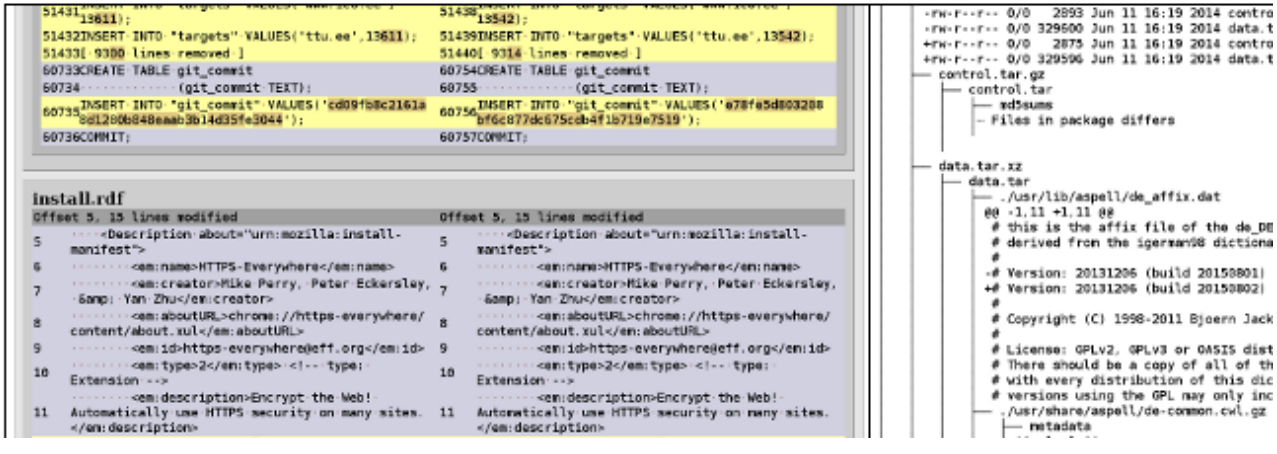

I SHOULD BUILD A BETTER DIFF



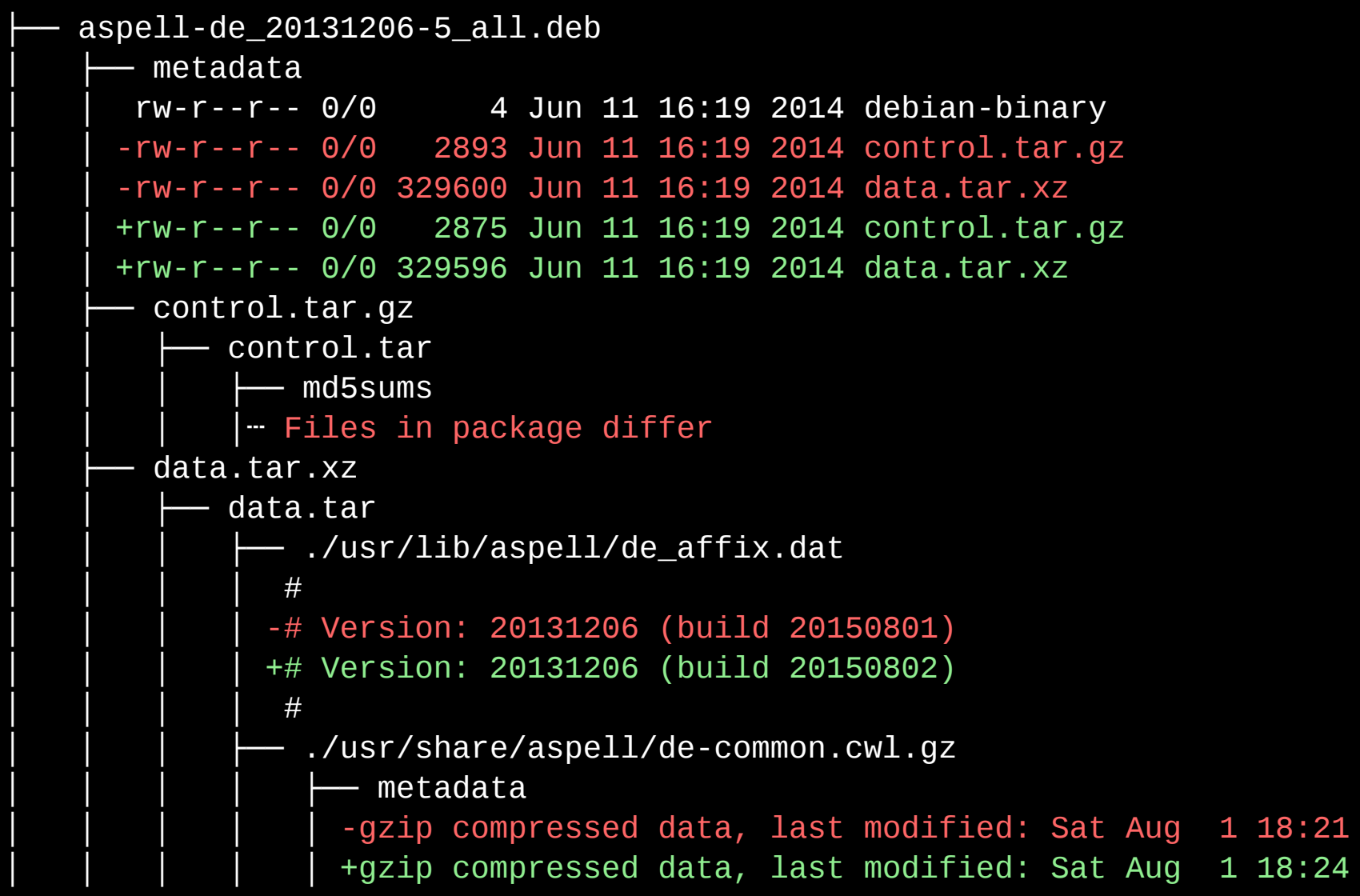
diffoscope

in-depth comparison of files, archives, and directories

> *diffoscope* will try to get to the bottom of what makes files or directories different. It will recursively unpack archives of many kinds and transform various binary formats into more human readable form to compare them. It can compare two tarballs, ISO images, or PDF just as easily.



https://diffoscope.org/

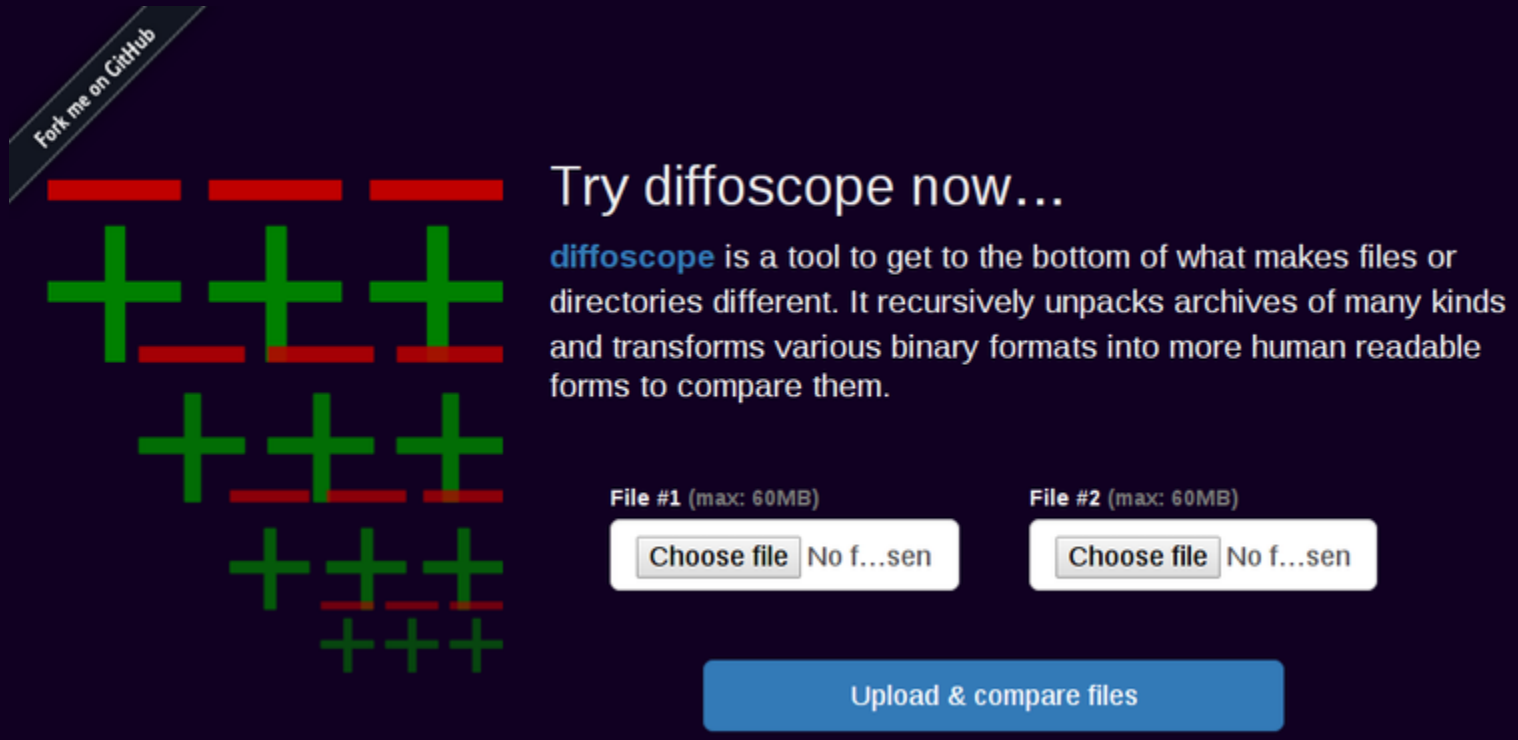

├── aspell-de_20131206-5_all.deb
│ ├── metadata
│ │ rw-r--r-- 0/0 4 Jun 11 16:19 2014 debian-binary
│ │ -rw-r--r-- 0/0 2893 Jun 11 16:19 2014 control.tar.gz
│ │ -rw-r--r-- 0/0 329600 Jun 11 16:19 2014 data.tar.xz
│ │ +rw-r--r-- 0/0 2875 Jun 11 16:19 2014 control.tar.gz
│ │ +rw-r--r-- 0/0 329596 Jun 11 16:19 2014 data.tar.xz
│ ├── control.tar.gz
│ │ ├── control.tar
│ │ │ ├── md5sums
│ │ │ │┄ Files in package differ
│ ├── data.tar.xz
│ │ ├── data.tar
│ │ │ ├── ./usr/lib/aspell/de_affix.dat
│ │ │ │ #
│ │ │ │ -# Version: 20131206 (build 20150801)
│ │ │ │ +# Version: 20131206 (build 20150802)
│ │ │ │ #
│ │ │ ├── ./usr/share/aspell/de-common.cwl.gz
│ │ │ │ ├── metadata
│ │ │ │ │ -gzip compressed data, last modified: Sat Aug 1 18:21
│ │ │ │ │ +gzip compressed data, last modified: Sat Aug 1 18:24

Android APK files, Android boot images, Ar(1) archives, Berkeley DB database files, Bzip2 archives, Character/block devices, ColorSync colour profiles (.icc), Coreboot CBFS filesystem images, Cpio archives, Dalvik .dex files, Debian .buildinfo files, Debian .changes files, Debian source packages (.dsc), Device Tree Compiler blob files, Directories, ELF binaries, Ext2/ext3/ext4/btrfs filesystems, FreeDesktop Fontconfig cache files, FreePascal files (.ppu), Gettext message catalogues, GHC Haskell .hi files, GIF image files, Git repositories, GNU R database files (.rdb), GNU R Rscript files (.rds), Gnumeric spreadsheets, Gzipped files, ISO 9660 CD images, Java .class files, JavaScript files, JPEG images, JSON files, LLVM IR bitcode files, MacOS binaries, Microsoft Windows icon files, Microsoft Word .docx files, Mono 'Portable Executable' files, Ogg Vorbis audio files, OpenOffice .odt files, OpenSSH public keys, OpenWRT package archives (.ipk), PDF documents, PGP signed/encrypted messages, PNG images, PostScript documents, RPM archives, Rust object files (.deflate), SQLite databases, SquashFS filesystems, Statically-linked binaries, Symlinks, Tape archives (.tar), Tcpdump capture files (.pcap), Text files, TrueType font files, XML binary schemas (.xsb), XML files, XZ compressed files, etc.

Security uploads

Binary blobs (eg. router images)

`diffoscope` ≠ definition of reproducible



try.diffoscope.org

What's left to do?

Source code

Backdoors

Programming errors

Weak algorithms

Code with "testing" modes

```
$ apt install python-pywt-doc
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  python-pywt-doc
0 upgraded, 1 newly installed, 0 to remove and 4 not upgrad
Need to get 102 kB of archives.
After this operation, 978 kB of additional disk space will
WARNING: The following packages are not reproducible!
  python-pywt-doc
Install these packages anyway? [y/N]
```

Toolchain fixes (GCC, OCaml, R, etc.)

Improving developer tools

Distribution policy changes

Defeating *Trusting Trust*…?

Get involved!

Visit:	`reproducible-builds.org`
Follow:	**@ReproBuilds** on Twitter
Join:	`#reproducible-builds` on `irc.oftc.net`

Thank you!

@lolamby
lamby@debian.org

chris-lamb.co.uk
reproducible-builds.org