



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

Holger Levsen  
h01ger  
based on Chris Lamb's slides

MiniDebConf Brasil  
Curitiba  
13th April 2018

**My name is...**



**Holger Levsen**

...e eu nao falo Português, desculpa!!

**My nick is...**

**h01ger**



went to CCA Congress before Linux / IPv4

Debian user since 1995

Free software contributor for 15+ years

Freelancer



**more about Debian and me**



Debian contributor since 2001, DD since 2007  
ex-debconf organizer 2004-2014 and dc-committee member

[video.debian.net](http://video.debian.net)

Debian Edu

[piuparts.debian.org](http://piuparts.debian.org)

[jenkins.debian.net](http://jenkins.debian.net)

[qubes-os.org](http://qubes-os.org) user

coreboot user



# Ask me anything!

feel free to interrupt

or ask me later



This talk is about

# Reproducible Builds

in Debian started at DebConf13 by Lunar

I've been working on it since 2014





Slides taken from Chris 'lamby' Lamb

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



***My Awesome Software***

**Download Source**

or

**Download .exe / .deb / .rpm**



## ***My Awesome Software***

**Download Source**

or

**Download ~~.exe~~ / .deb / .rpm**



Bob







← 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.

Reading package lists... Done

Building dependency tree... Done

The following extra packages will be installed:

apache2-bin apache2-data apache2-utils file libalgorithm-c3-perl libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
libarchive-extract-perl libb-hooks-endofscope-perl libb-hooks-on-check-perl libbareword-filehandles-perl libbcgi-fast-perl libbcgi-pm-perl  
libclass-c3-perl libclass-c3-xs-perl libclass-method-modifiers-perl libclass-xs-accessor-perl libcpan-changes-perl libcpan-meta-perl  
libdata-optlist-perl libdata-perl-perl libdata-section-perl libdevel-caller-perl libdevel-global-destroy-perl libdevel-lexalias-perl  
libencode-locale-perl libexpat1 libexporter-tiny-perl libfcgi-perl libffi6 libfile-slurp-perl libgdbm3 libgetopt-long-descriptive-perl  
libgmp10 libgnutls-deb0-28 libhogweed4 libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libicu55  
libimport-into-perl libindirect-perl libio-html-perl libio-stringy-perl libldap-2.4-2 liblexical-sealrequirehints-perl  
liblist-moreutils-perl liblog-message-perl liblog-message-simple-perl liblua5.1-0 liblwp-mediatypes-perl libmagic1 libmodule-build-perl  
libmodule-implementation-perl libmodule-pluggable-perl libmodule-runtime-perl libmodule-signature-perl libmoo-perl libmoox-handlesvia-perl  
libmro-compat-perl libmultidimensional-perl libnamespace-autoclean-perl libnamespace-clean-perl libnettle6 libnghttp2-14 libp11-kit0  
libpackage-constants-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparams-util-perl  
libparams-validate-perl libpath-tiny-perl libpod-latex-perl libpod-markdown-perl libpod-readme-perl librole-tiny-perl libsasl2-2  
libsasl2-modules libsasl2-modules-db libsoftware-license-perl libsqlite3-0 libssl1.0.2 libstrictures-perl libsub-exporter-perl  
libsub-exporter-progressive-perl libsub-identify-perl libsub-install-perl libsub-name-perl libtasn1-6 libterm-ui-perl libtext-soundex-perl  
libtext-template-perl libtimedate-perl libtry-tiny-perl libtype-tiny-perl libtype-tiny-xs-perl libunicode-utf8-perl liburi-perl  
libvariable-magic-perl libxml2 mime-support openssl perl perl-modules rename sgml-base ssl-cert xml-core

Suggested packages:

www-browser apache2-doc apache2-mpm-itk apache2-suexec-minimal libapache2-mod-authn-sasl libapache2-mod-authn-xmldsig perl-modules-5.28  
libsasl2-modules-gssapi-mit libsasl2-modules-ldap libsasl2-modules-otp libsasl2-modules-sql libtasn1-doc libxml2-utils libzstd-dev  
libdevel-stacktrace-perl libwww-perl ca-certificates perl-doc libterm-readline-gnu-perl libterm-readline-perl-perl make libb-lint-perl  
libcpanplus-dist-build-perl libcpanplus-perl libfile-checktree-perl libobject-accessor-perl sgml-base-doc openssl-blacklist debhelper

The following NEW packages will be installed:

apache2 apache2-bin apache2-data apache2-utils file libalgorithm-c3-perl libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
libarchive-extract-perl libb-hooks-endofscope-perl libb-hooks-on-check-perl libbareword-filehandles-perl libbcgi-fast-perl libbcgi-pm-perl  
libclass-c3-perl libclass-c3-xs-perl libclass-method-modifiers-perl libclass-xs-accessor-perl libcpan-changes-perl libcpan-meta-perl  
libdata-optlist-perl libdata-perl-perl libdata-section-perl libdevel-caller-perl libdevel-global-destroy-perl libdevel-lexalias-perl  
libencode-locale-perl libexpat1 libexporter-tiny-perl libfcgi-perl libffi6 libfile-slurp-perl libgdbm3 libgetopt-long-descriptive-perl  
libgmp10 libgnutls-deb0-28 libhogweed4 libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libicu55  
libimport-into-perl libindirect-perl libio-html-perl libio-stringy-perl libldap-2.4-2 liblexical-sealrequirehints-perl  
liblist-moreutils-perl liblog-message-perl liblog-message-simple-perl liblua5.1-0 liblwp-mediatypes-perl libmagic1 libmodule-build-perl  
libmodule-implementation-perl libmodule-pluggable-perl libmodule-runtime-perl libmodule-signature-perl libmoo-perl libmoox-handlesvia-perl  
libmro-compat-perl libmultidimensional-perl libnamespace-autoclean-perl libnamespace-clean-perl libnettle6 libnghttp2-14 libp11-kit0  
libpackage-constants-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparams-util-perl  
libparams-validate-perl libpath-tiny-perl libpod-latex-perl libpod-markdown-perl libpod-readme-perl librole-tiny-perl libsasl2-2  
libsasl2-modules libsasl2-modules-db libsoftware-license-perl libsqlite3-0 libssl1.0.2 libstrictures-perl libsub-exporter-perl  
libsub-exporter-progressive-perl libsub-identify-perl libsub-install-perl libsub-name-perl libtasn1-6 libterm-ui-perl libtext-soundex-perl  
libtext-template-perl libtimedate-perl libtry-tiny-perl libtype-tiny-perl libtype-tiny-xs-perl libunicode-utf8-perl liburi-perl  
libvariable-magic-perl libxml2 mime-support openssl perl perl-modules rename sgml-base ssl-cert xml-core

0 upgraded, 114 newly installed, 0 to remove and 1 not upgraded.

Need to get 23.8 MB of archives.

After this operation, 97.9 MB of additional disk space will be used.

Do you want to continue? [Y/n]

# General problem

## Can view source code for malicious flaws

## But users install pre-compiled packages

## Can we trust the compilation process?

# Hacker explains how he put "backdoor" in hundreds of Linux Mi Downloads

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](#)



Cloud Solutions & Processes

2. Ensure builds always

3. Compare results

Webinar  
7 | 5:00 pm CEST

[REGISTER NOW](#)

Agnes Valkova  
Marketing Manager

## Free Resco Cloud Webinar

Get run through all the solutions Resco Cloud has to offer and who benefits from which.

David



7a482b984883990bd4ab2ac5985630886cc252c



David



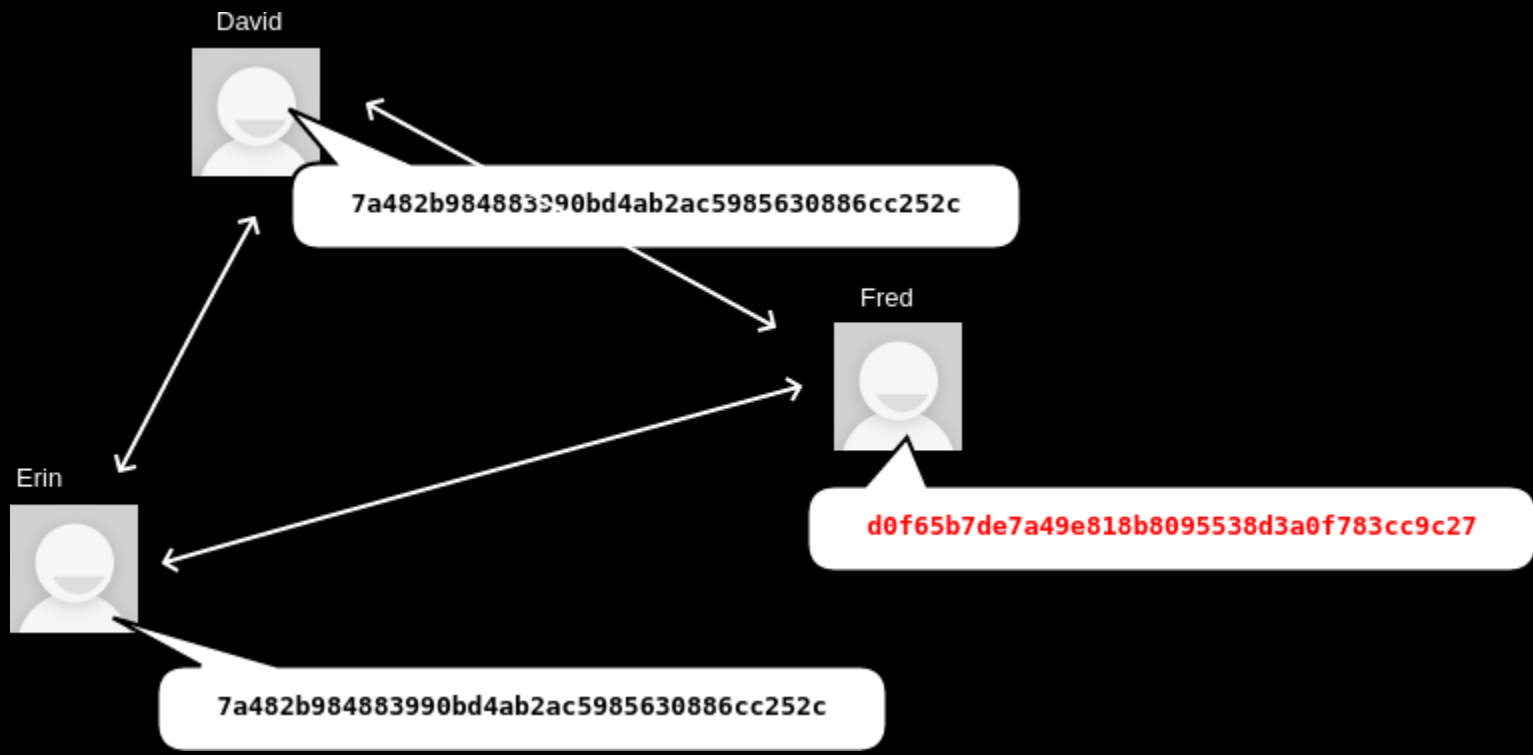
7a482b984883990bd4ab2ac5985630886cc252c

Erin



7a482b984883990bd4ab2ac5985630886cc252c





# How does this help?

Alice → Blackmail will be uncovered

Bob → Compromise detected

Carol → Tampered laptop will be discovered

**Reduces incentive to attack in the first place**



**“Reproducible” builds allows verification  
that no flaws have been introduced during  
the compilation process**

"Reliable" builds... ✘

"Builds with the same dependencies"... ✘

**Identical build results**

**Wait...**

Dictionary/hash/database ordering

Parallelism in builds

Timestamps

Build paths

Non-deterministic file ordering

Users, groups, umask, environment variables, etc.

**Other advantages**

Minimal diffs on "deliberate" changes

Cache ratio — save time, money & CO<sub>2</sub>

Detect corrupted build environments

Remove build-dependencies

Finds bugs!

# 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 shares the same secret.

# Random characters in manpages?

```
-This manual page documents the usage of WikipediaFS.  
+This manual page documents the usage of WikipediaFS.
```

```
memcpy(&buf[1], &buf[2], strlen(buf)-1);
```

```
memcpy(3): The memory areas must not overlap
```

```
- memcpy(&buf[1], &buf[2], strlen(buf)-1);  
+ memmove(&buf[1], &buf[2], strlen(buf)-1);
```



# Fails to build 0.46% of the time?

```
x = f(u('abc'), 16)
y = f(u('abc'), 16)
self.assertEqual(sorted(set(x)), [u('a'), u('b'), u('c')])
```

```
AssertionError: Lists differ: [u'a', u'b'] != [u'a', u'b', u'c']
```

$$({}_3C_2) * (2/3)^{16} - ({}_3C_1) * (1/3)^{16} \approx 0.46\%$$

The Debian logo, a red spiral, is positioned behind the text.

# Debian & reproducible builds

# "Torture test"

Time & date

Hostname & domain name

Filesystem (disorderfs)

Timezone & locale

uid & gid

Kernel & CPU type

First rebuild in 2013

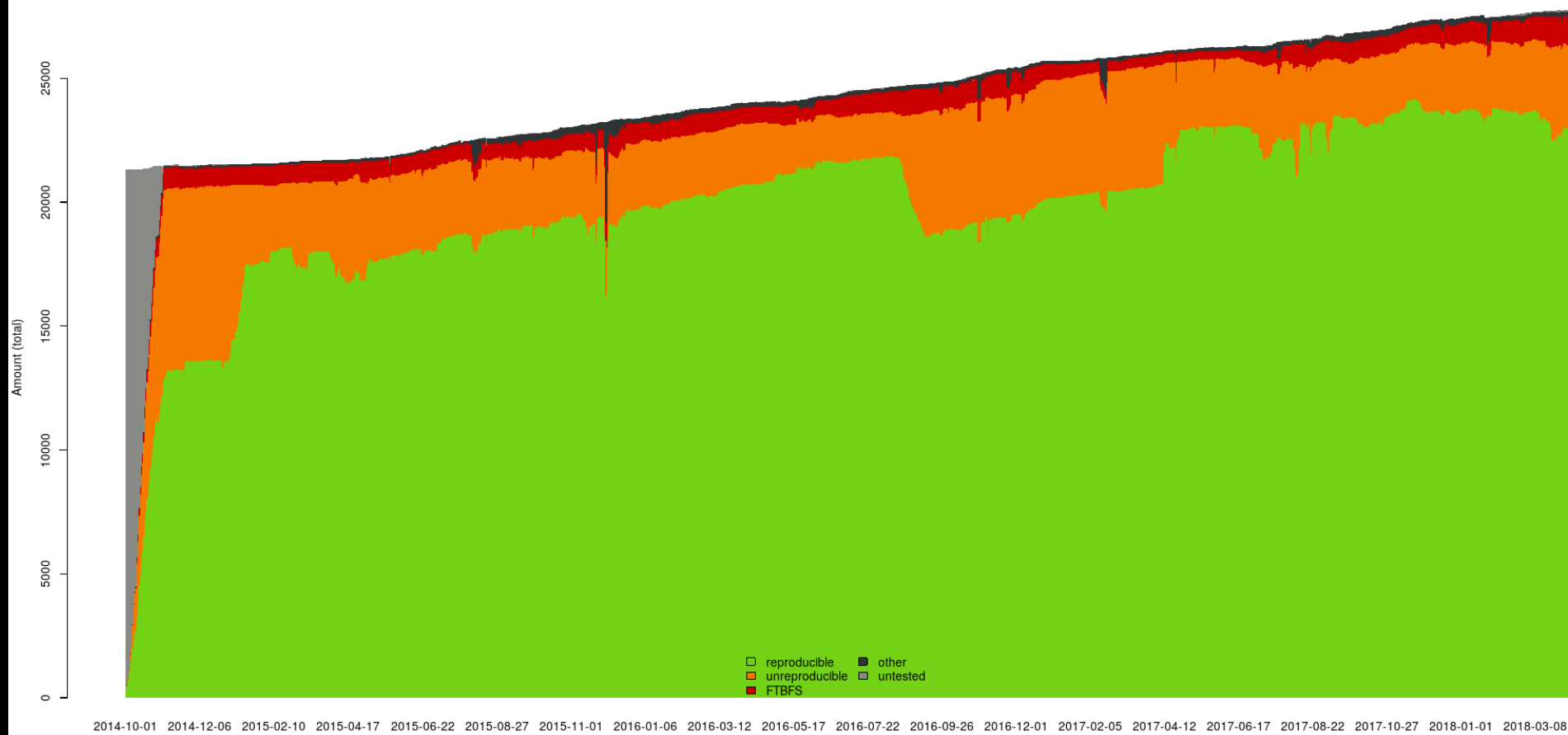
24% packages reproducible

---

April 2018

93% packages reproducible

Reproducibility status for packages in 'unstable' for 'amd64'



A red spiral graphic, resembling a stylized 'e' or a similar character, is positioned behind the text. It starts from a central point and winds outwards in a clockwise direction, with a slight 3D effect and a dark red color.

**[isdebianreproducible.net.com](http://isdebianreproducible.net.com)**

# Beyond Debian...

coreboot, OpenSUSE, OpenWRT, NetBSD, FreeBSD, Archlinux, Tails, Qubes, F-Droid, NixOS, Guix, Basel, Meson, etc.

Other projects using "Debian"'s testing framework

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.
```



```

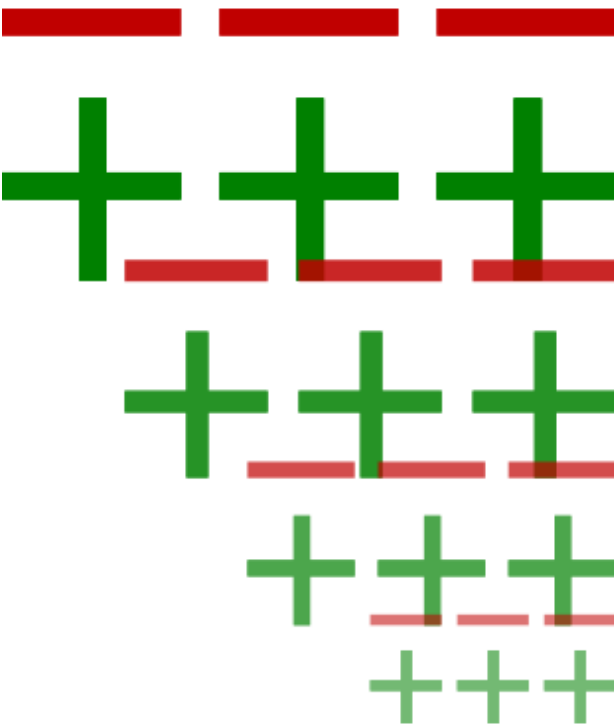
$ diff -urNad a.deb b.deb | head -n10
--- a.deb          2018-01-23 11:47:11.829950207 +1100
+++ b.deb          2018-01-23 11:47:16.333977828 +1100
@@ -1,603 +1,643 @@
 !<arch>
 debian-binary    1496485532  0      0      100644  4
 2.0
-control.tar.xz  1496485532  0      0      100644  1664
-7zXZF
      P! 4M' ]
      >y&Y0x$rD-<j_
+control.tar.xz  1496485532  0      0      100644  1668
+7zXZF
      P! 00000' ]
      >y&Y0x$rD-<j_

```

# 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.



```
51431INSERT INTO "targets" VALUES('ttu.ee',13611); 51438INSERT INTO "targets" VALUES('ttu.ee',13542);
51432INSERT INTO "targets" VALUES('ttu.ee',13611); 51439INSERT INTO "targets" VALUES('ttu.ee',13542);
51433[ 9300 lines removed ] 51440[ 9314 lines removed ]
60733CREATE TABLE git_commit
60734..... (git_commit TEXT); 60754CREATE TABLE git_commit
60755..... (git_commit TEXT);
60735INSERT INTO "git_commit" VALUES('cd09f0bc2161a
6073681206b848eaab3b14d35f43044'); 60756INSERT INTO "git_commit" VALUES('e78fe5d803208
60757bf6c877dc675c0b4f15719e7519');
60736COMMIT; 60757COMMIT;
```

```
install.rdf
Offset 5, 15 lines modified
5.....<Description about="urn:mozilla:install-
manifest">
6.....<em:name>HTTPS-Everywhere</em:name>
7.....<em:creator>Mike Perry, Peter Eckersley,
&amp; Yan Zhu</em:creator>
8.....<em:aboutURL>chrome://https-everywhere/
content/about.xul</em:aboutURL>
9.....<em:id>https-everywhere@eff.org</em:id>
10.....<em:type>2</em:type><!-- type:
Extension -->
11.....<em:description>Encrypt the Web!
Automatically use HTTPS security on many sites.
</em:description>
```

```
51438INSERT INTO "targets" VALUES('ttu.ee',13542);
51439INSERT INTO "targets" VALUES('ttu.ee',13542);
51440[ 9314 lines removed ]
60754CREATE TABLE git_commit
60755..... (git_commit TEXT);
60756INSERT INTO "git_commit" VALUES('e78fe5d803208
60757bf6c877dc675c0b4f15719e7519');
60757COMMIT;
```

```
control.tar.gz
- edSignatures
- Files in package differs

data.tar.xz
./usr/lib/aspell/de_affix.dat
@ -1.11 +1.11 @@
# this is the affix file of the de_DE
# derived from the Igerman08 dictionary
#
-# Version: 20131206 (build 20150801)
+# Version: 20131206 (build 20150802)
#
# Copyright (C) 1998-2011 Bjoern Jack
#
# License: GPLV2, GPLv3 or OASIS dist
# There should be a copy of all of th
# with every distribution of this dic
# versions using the GPL may only inc
./usr/share/aspell/de-common.cwl.gz
- metadata
```

<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.

Fork me on GitHub



## Try diffoscope now...

**diffoscope** is a tool to get to the bottom of what makes files or directories different. It recursively unpacks archives of many kinds and transforms various binary formats into more human readable forms to compare them.

File #1 (max: 60MB)

Choose file No f...sen

File #2 (max: 60MB)

Choose file No f...sen

Upload & compare files

# try.diffoscope.org

Show differences in security uploads

diffoscope != definition of reproducible!

Binary blobs (eg. router images)

**What's left to do?**

# Source code

Programming errors

Backdoors / obfuscated code

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 upgraded
Need to get 102 kB of archives.
After this operation, 978 kB of additional disk space will be used.
WARNING: The following packages are not reproducible!
  python-pywt-doc
Install these packages anyway? [y/N]
```

Toolchain fixes (GCC!)

Improving developer tools

Mandating Debian packages be reproducible?

Defeating *Trusting Trust*...?

# Get involved!

Visit: [reproducible-builds.org](https://reproducible-builds.org)

Follow: [@ReproBuilds](https://twitter.com/ReproBuilds) on Twitter

Join: [#reproducible-builds](https://reproducible-builds.irc.oftc.net)  
on [irc.oftc.net](https://irc.oftc.net)

Fix: Bugs and toolchain issues!

*Obrigado!*



**h01ger**  
**holger@debian.org**

**reproducible-builds.org**  
**tests.reproducible-builds.org**