

Stretching out for trustworthy reproducible builds

Holger Levsen
holger@debian.org

Lunar
lunar@debian.org

FOSDEM'15
2015-01-31





What?



What are reproducible builds?

“reproducible builds”
enable anyone to reproduce
identical binary packages
from a given source



“I want to believe”

source $\xrightarrow{\text{build}}$ binary



“I want to believe”

free software

freedom
to study

freedom
to run

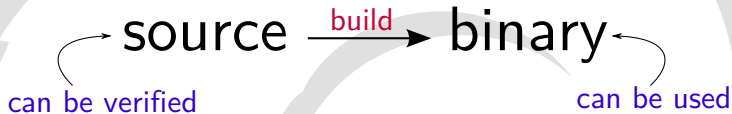
source

build

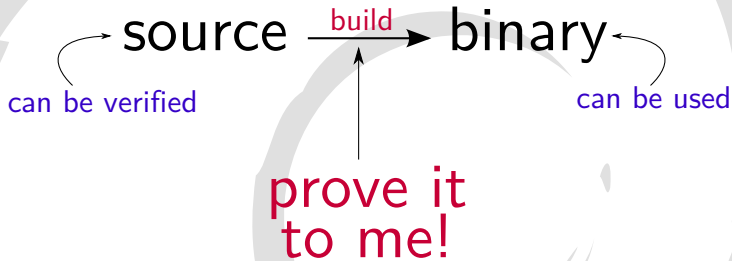
binary



“I want to believe”



“I want to believe”





Why?



Why?

Reproducible builds allow for **independent verifications** that a binary matches what the source intended to produce.

... and other nice things.



But I'm the developer!

"I know what's in the binary because I compiled it myself!"

"I'm an upstanding, careful, and responsible individual!"

"Why should I have to worry about hypothetical risks about the contents of my binaries?"



But the build machines are secure

- How can you be sure?



Unpleasant thoughts

- We think of software development as a fundamentally benign activity.
 - ▶ *“I’m not that interesting.”*
- Users can be targeted through developers
- Known successful attacks against infrastructure used by Linux (2003), FreeBSD (2013)



Strong motivations

- Compromise one computer to get:
 - ▶ Hundreds of millions of other computers?
 - ▶ Every bank account in the world?
 - ▶ Every Windows computer in the world?
 - ▶ Every Linux server in the world?
- Compromise one computer is worth:
 - ▶ \$100k USD? (Market price of remote 0day)
 - ▶ \$100M USD? (Censorship budget of Iran per year)
 - ▶ \$4B USD? (Bitcoin market cap)



How small can a backdoor be?

OpenSSH 3.0.2 (CVE-2002-0083) – exploitable security bug (privilege escalation: user can get root)

```
{  
    Channel *c;  
-   if (id < 0 || id > channels_alloc) {  
+   if (id < 0 || id >= channels_alloc) {  
        log("channel_lookup: %d: bad id", id);  
        return;  
    }  
}
```



Result of fixing the bug (asm)

```
cmpl $0x0,0x8(%ebp)
js 16
mov 0x4,%eax
cmp %eax,0x8(%ebp)
jle 30
mov 0x8(%ebp),%eax
mov %eax,0x4(%esp)
movl $0x4c,(%esp)
call 25
```

```
cmpl $0x0,0x8(%ebp)
js 16
mov 0x4,%eax
cmp %eax,0x8(%ebp)
jl 30
mov 0x8(%ebp),%eax
mov %eax,0x4(%esp)
movl $0x4c,(%esp)
call 25
```



Result of fixing the bug (asm)

```
cmp1 $0x0,0x8(%ebp)
js 16
mov 0x4,%eax
cmp %eax,0x8(%ebp)
jle 30
mov 0x8(%ebp),%eax
mov %eax,0x4(%esp)
movl $0x4c, (%esp)
call 25
```

```
cmp1 $0x0,0x8(%ebp)
js 16
mov 0x4,%eax
cmp %eax,0x8(%ebp)
jl 30
mov 0x8(%ebp),%eax
mov %eax,0x4(%esp)
movl $0x4c, (%esp)
call 25
```



Resulting difference in the binary

What's the difference between `if (a > b)`
and `if (a >= b)` in x86 assembly?

assembly:	JLE	JL
opcode:	0x7E	0x7C
binary:	01111110	01111100

A single bit!

Other corresponding opcode pairs also differ by just a single bit (JGE=0x7D, JG=0x7F)



Result of fixing the bug (hex)

Vulnerable	Fixed
55 89 e5 83 ec	55 89 e5 83 ec
28 83 7d 08 00	28 83 7d 08 00
78 0a a1 04 00	78 0a a1 04 00
00 00 39 45 08	00 00 39 45 08
7e 1a 8b 45 08	7c 1a 8b 45 08
89 44 24 04 c7	89 44 24 04 c7
04 24 4c 00 00	04 24 4c 00 00
00 e8 fc ff ff	00 e8 fc ff ff
ff b8 00 00 00	ff b8 00 00 00
00 eb 35	00 eb 35

Overall file size: approx. 500 kB

Result of fixing the bug (hex)

Vulnerable	Fixed
55 89 e5 83 ec	55 89 e5 83 ec
28 83 7d 08 00	28 83 7d 08 00
78 0a a1 04 00	78 0a a1 04 00
00 00 39 45 08	00 00 39 45 08
7e 1a 8b 45 08	7c 1a 8b 45 08
89 44 24 04 c7	89 44 24 04 c7
04 24 4c 00 00	04 24 4c 00 00
00 e8 fc ff ff	00 e8 fc ff ff
ff b8 00 00 00	ff b8 00 00 00
00 eb 35	00 eb 35

Overall file size: approx. 500 kB

How did this start?

https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise

Startpage



HOME ARCHIVES ABOUT TOR

Deterministic Builds Part One: Cyberwar and Global Compromise

View Edit

Posted August 20th, 2013 by mikeperry in [cyberpeace](#), [dangerous toys](#), [decentralization](#), [deterministic builds](#), [ghia](#), [lack of foresight](#), [National Insecurity Agency](#), [security](#)

I've spent the past few months developing a new build system for the [3.0 series](#) of the Tor Browser Bundle that produces what are called "deterministic builds" -- packages which are byte-for-byte identical no matter who actually builds them, or what hardware they use. This effort was extraordinarily involved, consuming all of my development time for over two months (including several nights and weekends), babysitting builds and fixing differences and issues that arose.

When describing my recent efforts to others, by far the two most common questions I've heard are "Why did you do that?" and "How did you do that?". I've decided to answer each question at length in a separate blog post. This blog post attempts to answer the first question: "Why would anyone want a deterministic build process?"

The short answer is: to protect against targeted attacks. Current popular software development practices simply cannot survive targeted attacks of the scale and scope that we are seeing today. In fact, I believe we're just about to witness the first examples of large scale "watering hole" attacks. This would be malware that attacks the software development and build processes themselves to distribute copies of itself to tens or even hundreds of millions of machines in a single, officially signed, instantaneous update. Deterministic, distributed builds are perhaps the only way we can reliably prevent these types of targeted attacks in the face of the endless stockpiling of weaponized exploits and other "cyberweapons".

- Add a New Blog Post
- Manage Blog
- Admin Comments
- Manage Users
- Add an Event
- Manage Events
- Manage Forums

Search

Bitcoin's motivation

- Malicious modifications to binaries could result in irrevocable unwanted transfers of bitcoins
- Individual developers could be blamed for such modifications
- Users might not believe that a developer's machine was hacked
- Reproducible builds therefore protect developers



Nothing new though

From: Martin Uecker <muecker@gmx.de>

Cc: debian-devel@lists.debian.org

Date: Sun, 23 Sep 2007 23:32:59 +0200

I think it would be really cool if the Debian policy required that packages could be rebuild bit-identical from source. At the moment, it is impossible to independly verify the integricity of binary packages.

<https://lists.debian.org/debian-devel/2007/09/msg00746.html>



Wouldn't it be cool?

- Debian is the largest collection of free software
- More than 21,000 source packages
- “Our priorities are our **users** and **free software**”





How?



How?

- Record the build environment
- Reproduce the build environment
- Eliminate unneeded variations





How:

Record the build environment



*.buildinfo

New control file *.buildinfo which records:

- Versions of build dependencies
 - ▶ ... and their dependencies
- Checksum of the source package.
- Checksums of the binary packages.



Example *.buildinfo

```
Format: 1.9
Build-Architecture: amd64
Source: ttorcon
Binary: python-ttorcon
Architecture: all
Version: 0.11.0-1
Build-Path: /usr/src/debian/ttorcon-0.11.0-1
Checksums-Sha256:
  a26549d9...7b 125910 python-ttorcon_0.11.0-1_all.deb
  28f6bcbe...69 2039 ttorcon_0.11.0-1.dsc
Build-Environment:
  base-files (= 8),
  base-passwd (= 3.5.37),
  bash (= 4.3-11+b1),
  ...
```





How:

Reproduce the build environment



- `snapshot.debian.org` archives every state of the Debian archive.
- 2015-01-29: 28 terabytes of data in almost 17 million files.



srebuild

- Thin wrapper around sbuild
- Find the right archive snapshot
- Install packages listed in the *.buildinfo file
- Start the build

Status: work in progress





How:

Eliminate unneeded variations



General approach

- Gitian (Bitcoin, Tor Browser):
 - ▶ Use a VM: same kernel, same user, same build path
 - ▶ `libfaketime`
- Debian:
 - ▶ Fix the tools
 - ▶ Fix the build systems
 - ▶ Work-arounds as last resort



strip-nondeterminism

- Normalize various file formats
- Currently handle:
 - ▶ ar archives (.a)
 - ▶ gzip
 - ▶ Java jar
 - ▶ Javadoc HTML
 - ▶ ZIP archives
- Written in Perl (like dpkg-dev)



Investigating packages

debindiff :

- Two files → HTML
- Recursively unpack archives
- Seeks human readability:
 - ▶ uncompress PDF
 - ▶ disassemble binaries,
 - ▶ unpack Gettext files,
 - ▶ ... *easy to extend to new file formats*
- Falls back to binary comparison



Test

(and test again)



reproducible.debian.net: idea

- Build the package
- *Rebuild* the package
- Compare the results

Initially a 10 lines shell script...



reproducible.debian.net: today

- Driven by jenkins.debian.net
 - ▶ announced 2014-09-26
- 14 jobs defined in 263 LOC of YAML
 - ▶ 3 build jobs, rescheduled every 2 minutes
 - ▶ Job for auto-scheduling
 - ▶ Jobs to recreate pbuilder base.tgz and debbindiff schroot
 - ▶ Job to update notes and issues from Git
 - ▶ JSON output
 - ▶ Remaining jobs mostly to create HTML and graphs
- 13 Shell scripts with 2049 LOC
- 4 Python scripts with 948 LOC



reproducible.debian.net: variations

The second build is different in:

- time
- file ordering
- CPU ordering and availability
- hostname
- user & group
- locale



reproducible.debian.net: more goodies

- `https://reproducible.debian.net/$PACKAGE`
- Reproducibility status in `tracker.debian.org`
- Package sets:
 - ▶ `Essential:yes, build-essential`
 - ▶ 1337 most frequently installed packages (popcon)
 - ▶ Packages installed on Debian machines
 - ▶ All packages in Tails and their build dependencies
 - ▶ All packages in Grml and their build dependencies
- List of unreproducible packages per maintainer



reproducible.debian.net: not reproducible

Overview of packages which failed to build reproducibly

21557 packages have been attempted to be build so far, that's 100.0% of 21557 source packages in Debian sid currently. Out of these, 17632 packages (81.7%) [could be built reproducibly!](#)

Have a look at:



[issues](#)

[packages with notes](#)

[currently scheduled](#)

[packages tested in the last 24h](#)


[packages tested in the last 48h](#)

[all tested packages \(sorted alphabetically\)](#)

[maintainers of unreproducible packages](#)

[stats](#)

[package sets stats](#)

 3058 (14.1%) packages which failed to build reproducibly: [java-xmlbuilder](#) [gfpoken](#) [freehep-graphicsio-tests](#) [munge-maven-plugin](#) [maven](#) [nvidia-settings](#) [camping](#) [libmodule-build-perl](#) [octave-secsld](#) [alienblaster](#) [primrose](#) [gpgme1.0](#) [webassets](#) [vmm](#) [ubuntu-packaging-guide](#) [txtorcon](#) [tsung](#) [taurus](#) [statsmodels](#) [spykeviewer](#) [skimage](#) [shinken](#) [sardana](#) [salt](#) [rdflib](#) [quodlibet](#) [qiime](#) [pythondialog](#) [python-tidylib](#) [python-shapely](#) [python-sfml](#) [python-secretstorage](#) [python-repoze.who](#) [python-reconfigure](#) [python-qt4](#) [python-pyaudio](#) [python-mzml](#) [python-fitbit](#) [python-expyriment](#) [python-django-mptt](#) [python-cogent](#) [pytables](#) [pyqt5](#) [pyotherside](#) [pyopencl](#) [pymvpa2](#) [pymvpa](#) [pycurl](#) [pycairo](#) [py-postgresql](#) [py3cairo](#) [psi4](#) [powerline](#) [plainbox](#) [pbatch](#) [php-guzzle](#) [pebl](#) [paramiko](#) [owncloud-doc](#) [owncloud-client](#) [opencolorio](#)

reproducible.debian.net: package

gdb 7.7.1+dfsg-5  at 2015-01-24 15:50 UTC: [notes](#) [debbindiff](#) [buildinfo](#) [rbuild](#) (4MB) [PTS](#) [BTS](#) [sources](#) [debian/rules](#) reproducible builds

Version annotated: 7.7.1+dfsg-5

Identified issues:

Identifier: [timestamps_in_jar](#)

URL <https://wiki.debian.org/ReproducibleBuilds/TimestampsInJarFiles>

Description jar (Java Archive) file stores mtimes. Most often of files generated during the build.

Identifier: [timestamps_in_dvi_generated_by_latex](#)

URL <https://wiki.debian.org/ReproducibleBuilds/TimestampsInDviGeneratedByLaTeX>

Description The creation date of the DVI file is the current time.

Comments: Capture build time and hostname in
`/usr/share/doc/gdb/check.log.gz`

reproducible.debian.net: package

gdb 7.7.1+dfsg-5 at 2015-01-24 15:50 UTC: notes [debbindiff](#) buildinfo rbuild (4MB) PTS BTS sources debian/rules reproducible builds

**/srv/reproducible-results/tmp.7nCU6iQ1Qp/b1/gdb_7.7.1+dfsg-5_amd64.changes vs.
/srv/reproducible-results/tmp.7nCU6iQ1Qp/b2/gdb_7.7.1+dfsg-5_amd64.changes**
List of files does not match

1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9

```
1 b50f3b2295bb9326dc9f0aca00fe62f9_23964520_devel_optio
2 1938d3870b5e8630678a197371895db9_2290974_devel_optional
3 68dd51ae5e93497a222899a7394d8b33_1921986_devel_optional
4 ef05db34e2230f40a29456844c7f66be_2778614_devel_optional
5 467e677816443aa17f76a332c3059bd7_243784_devel_optional
6 19d1d1454ad62a1872683b174b4dbd28_18135504_debug_extra_c
7 33b38adc35ff40ef6404a6a4ebcb5_8691_devel_optional_g
8 dfe3b37639e8666ce714849e41218bf0_23963628_devel_optiona
9 05ade3469adba2eb21bfe65f25d9f1c9_2290898_devel_optional
10 2be2566270f0b1175a9738bf400eecd_1921982_devel_optional
11 ef05db34e2230f40a29456844c7f66be_2778614_devel_optional
12 467e677816443aa17f76a332c3059bd7_243784_devel_optional
13 19d1d1454ad62a1872683b174b4dbd28_18135504_debug_extra_c
14 51ef6cf7f7302ea4e27fcf02632fc99f_8691_devel_optional_g
```

gdb-minimal_7.7.1+dfsg-5_amd64.deb

control.tar.gz

reproducible.debian.net: package

`gdb 7.7.1+dfsg-5` at 2015-01-24 15:50 UTC: [notes](#) [debbindiff](#) [buildinfo](#) [build \(4MB\)](#) [PTS](#) [BTS](#) [sources](#) [debian/rules](#) reproducible builds

```
Starting to build gdb on 2015-01-24 15:50
The jenkins build log is/was available at https://jenkins.debian.net/job/reproducible_builder_alpha/26194//console
Reading package lists...
Building dependency tree...
Reading state information...
NOTICE: 'gdb' packaging is maintained in the 'Git' version control system at:
git://anonscm.debian.org/pkg-gdb/gdb.git
Need to get 17.7 MB of source archives.
Get:1 http://ftp.de.debian.org/debian/ sid/main gdb 7.7.1+dfsg-5 (dsc) [2783 B]
Get:2 http://ftp.de.debian.org/debian/ sid/main gdb 7.7.1+dfsg-5 (tar) [17.7 MB]
Get:3 http://ftp.de.debian.org/debian/ sid/main gdb 7.7.1+dfsg-5 (diff) [71.0 kB]
Fetched 17.7 MB in 0s (21.5 MB/s)
Download complete and in download only mode
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

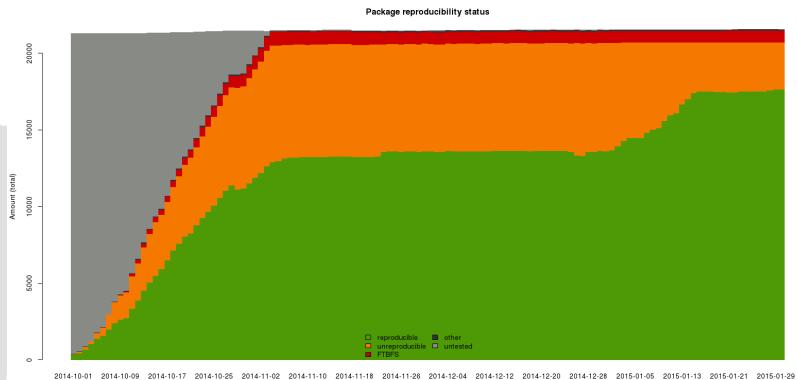
Format: 3.0 (quilt)
Source: gdb
Binary: gdb, gdb-minimal, gdb64, gdb-multiarch, gdbserver, gdb-source, gdb-dbg
Architecture: any all
-----BEGIN PGP SIGNED MESSAGE-----
```

Experimental “reproducible” toolchain

- Test and refine changes to tools used by build systems
- Currently 20 source packages
- Examples : `dpkg`, `debhelper`, `cdb`s, `libxslt`, `r-base`, `gtk-doc`, `fontforge`, ...
- Most patches already submitted
- `git://git.debian.org/reproducible/$pkg.git`
in branch `pu/reproducible_builds`



reproducible.debian.net overall stats



For those in the back

81.7%

More than 17,600 source packages!



For those in the back

81.7%

More than 17,600 source packages!
(in our test environment!)



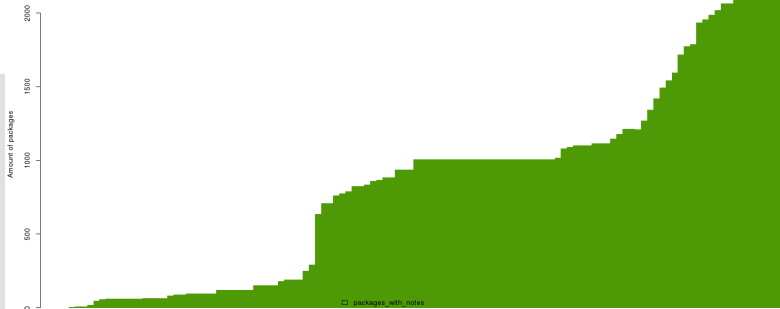
What is not tested (yet)

- `uname` output
- `Day/month/year`
- `/proc/cpuinfo`
- *More?*

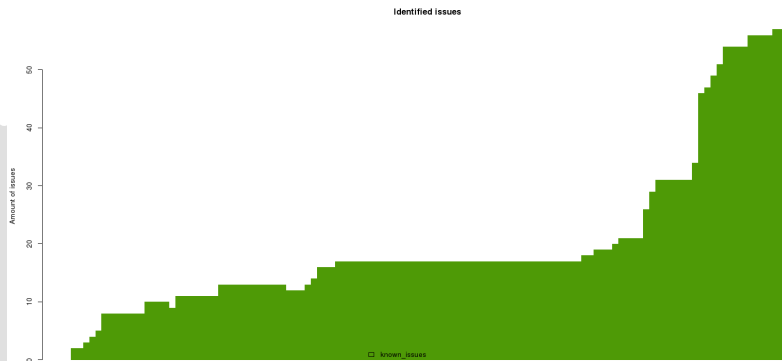


Investigated packages

Packages which have notes



Identified issues



Findings



Identified issues

- Timestamps (recording current time)
- File order
- (Pseudo-)randomness:
 - ▶ Temporary file paths
 - ▶ UUID
 - ▶ Protection against complexity attacks



Identified issues (cont.)

- CPU and memory related:
 - ▶ Code optimizations for current CPU class
 - ▶ Recording of memory addresses
- Build-path
- Others, eg. locale settings



Examples

Timestamps added by build systems



Timestamps in static libraries

data.tar

./usr/lib/libform_g.a

metadata

234	14112	Jan	2	06:04	2015	f_trace.o	234	14112	Jan	2	06:22	2015	f_trace.o
234	14336	Jan	2	06:04	2015	fld_arg.o	234	14336	Jan	2	06:22	2015	fld_arg.o
234	16112	Jan	2	06:04	2015	fld_attr.o	234	16112	Jan	2	06:22	2015	fld_attr.o
234	16368	Jan	2	06:04	2015	fld_current.o	234	16368	Jan	2	06:22	2015	fld_current.o
234	23592	Jan	2	06:04	2015	fld_def.o	234	23592	Jan	2	06:22	2015	fld_def.o
234	14920	Jan	2	06:04	2015	fld_dup.o	234	14920	Jan	2	06:22	2015	fld_dup.o
234	13064	Jan	2	06:04	2015	fld_ftchoice.o	234	13064	Jan	2	06:22	2015	fld_ftchoice.o
234	13992	Jan	2	06:04	2015	fld_ftlink.o	234	13992	Jan	2	06:22	2015	fld_ftlink.o
234	13992	Jan	2	06:04	2015	fld_info.o	234	13992	Jan	2	06:22	2015	fld_info.o
234	13616	Jan	2	06:04	2015	fld_just.o	234	13616	Jan	2	06:22	2015	fld_just.o
234	14688	Jan	2	06:04	2015	fld_link.o	234	14688	Jan	2	06:22	2015	fld_link.o
234	13472	Jan	2	06:04	2015	fld_max.o	234	13472	Jan	2	06:22	2015	fld_max.o
234	13208	Jan	2	06:04	2015	fld_move.o	234	13208	Jan	2	06:22	2015	fld_move.o
234	16296	Jan	2	06:04	2015	fld_newtyp.o	234	16296	Jan	2	06:22	2015	fld_newtyp.o
234	16232	Jan	2	06:04	2015	fld_opts.o	234	16232	Jan	2	06:22	2015	fld_opts.o
234	14312	Jan	2	06:04	2015	fld_pad.o	234	14312	Jan	2	06:22	2015	fld_pad.o
234	13616	Jan	2	06:04	2015	fld_page.o	234	13616	Jan	2	06:22	2015	fld_page.o
234	13504	Jan	2	06:04	2015	fld_stat.o	234	13504	Jan	2	06:22	2015	fld_stat.o
234	14912	Jan	2	06:04	2015	fld_type.o	234	14912	Jan	2	06:22	2015	fld_type.o
234	13488	Jan	2	06:04	2015	fld_user.o	234	13488	Jan	2	06:22	2015	fld_user.o

Timestamps in static libraries (cont.)

data.tar

./usr/lib/libuninum.a

No differences found inside, yet data differs

a 2f20 2020 2020 2020 !<arch>./	a 2f20 2020 2020 2020 !<arch>./
0 3134 3231 3837 3334 14218734	0 3134 3231 3837 3334 14218734
0 2020 3020 2020 2020 06 0 0	0 2020 3020 2020 2020 51 0 0
0 3239 3634 2020 2020 0 2964	0 3239 3634 2020 2020 0 2964
a 0000 0bd8 0000 0bd8	a 0000 0bd8 0000 0bd8
0 0000 0bd8 0000 0bd8	0 0000 0bd8 0000 0bd8
0 0000 0bd8 0000 0bd8	0 0000 0bd8 0000 0bd8
0 0000 0bd8 0000 0bd8	0 0000 0bd8 0000 0bd8
0 0000 0bd8 0000 0bd8	0 0000 0bd8 0000 0bd8
0bd8 0000 0bd8 0000 0bd8 0000 0bd8	0bd8 0000 0bd8 0000 0bd8 0000 0bd8
5 6e67 6433 0074 656e engd2.tengd3.ten	5 6e67 6433 0074 656e engd2.tengd3.ten
7 6435 0074 656e 6764 gd4.tengd5.tengd	7 6435 0074 656e 6764 gd4.tengd5.tengd
7 0074 656e 6764 3800 6.tengd7.tengd8.	7 0074 656e 6764 3800 6.tengd7.tengd8.
4 656e 6764 3130 0074 tengd9.tengd10.t	4 656e 6764 3130 0074 tengd9.tengd10.t
0 756e 696e 756d 2e6f engd11..uninum.o	0 756e 696e 756d 2e6f engd11..uninum.o
0 3134 3231 3837 3334 / 14218734	0 3134 3231 3837 3334 / 14218734
0 2020 3132 3334 2020 05 1234 1234	0 2020 3132 3334 2020 50 1234 1234
0 3336 3636 3038 2020 100644 366608	0 3336 3636 3038 2020 100644 366608

Timestamps written by Maven

data.tar.xz

data.tar

annotation-indexer.jar

META-INF/maven/org.jenkins-ci/annotation-indexer/pom.properties

```
1 #Generated by Maven
2 #Tue Dec 16 21:03:56 UTC 2014
3 version=1.9
4 groupId=org.jenkins-ci
5 artifactId=annotation-indexer
```

```
1 #Generated by Maven
2 #Tue Dec 16 21:03:28 UTC 2014
3 version=1.9
4 groupId=org.jenkins-ci
5 artifactId=annotation-indexer
```



Timestamps written by PyQt4

data.tar.xz

data.tar

./usr/lib/armory/qrc_img_resources.py

```
# -*- coding: utf-8 -*-
```

```
# Resource object code
```

```
#
```

```
# Created: Thu Jan 1 01:13:33 2015
```

```
# by: The Resource Compiler for PyQt4
```

```
#
```

```
# WARNING! All changes made in this file
```

```
from PyQt4 import QtCore
```

```
+-87477 lines: qt_resource_data = "\-----
```

```
# -*- coding: utf-8 -*-
```

```
# Resource object code
```

```
#
```

```
# Created: Thu Jan 1 01:17:12 2015
```

```
# by: The Resource Compiler for PyQt4
```

```
#
```

```
# WARNING! All changes made in this file
```

```
from PyQt4 import QtCore
```

```
+-87477 lines: qt_resource_data = "\-----
```



Timestamps written by Erlang compiler

data.tar.xz

data.tar

./usr/lib/x86_64-linux-gnu/ejabberd/ebin/mod_admin_extra.beam

4f 5231 0000 733c 4245 414d 4174 6f6d FO	64f 5231 0000 733c 4245 414d 4174 6f6d Fi
68 0264 0006 6f75 7464 summaryh.d..outd	968 0264 0006 6f75 7464 summaryh.d..outd
69 6e68 0264 0001 696b irk..ebin.h.d..lik	269 6e68 0264 0001 696b irk..ebin.h.d..lik
61 6262 6572 642d 6465 .../ejabberd-de	a61 6262 6572 642d 6465 .../ejabberd-de
64 656a 6802 6400 0776 v/includejh.d..v	564 656a 6802 6400 0776 v/includejh.d..v
00 0535 2e30 2e32 6802 ersionk..5.0.2h.	b00 0535 2e30 2e32 6802 ersionk..5.0.2h.
68 0662 0000 07de 610c d..timeh.b....a.	568 0662 0000 07de 610c d..timeh.b....a.
26 6802 6400 0673 6f75 a.a.a.a&h.d..sou	120 6802 6400 0673 6f75 a.a.a.a h.d..sou
74 6d70 2f62 7569 6c64 rcek.Q/tmp/build	f74 6d70 2f62 7569 6c64 rcek.Q/tmp/build
65 7264 2d63 6f6e 7472 d/ejabberd-contr	265 7264 2d63 6f6e 7472 d/ejabberd-contr
31 342e 3039 2e32 322f ib-0.2014.09.22/	031 342e 3039 2e32 322f ib-0.2014.09.22/
69 6e5f 6578 7472 612f mod_admin_extra/	d69 6e5f 6578 7472 612f mod_admin_extra/
5f 6164 6d69 6e5f 6578 src/mod_admin_ex	45f 6164 6d69 6e5f 6578 src/mod_admin_ex
6a 4162 7374 0000 0000 tra.erljAbst....	c6a 4162 7374 0000 0000 tra.erljAbst....
9 6e65 0000 037c 0000 0000 0000 0000 Lin	69 6e65 0000 037c 0000 0000 0000 0000 Lin

< ||| > < ||| >



Timestamps in PE binaries

Windows, UEFI, Mono...

data.tar.xz

data.tar

./usr/lib/mono-cecil/Mono.Cecil.Mdb.dll

9000 0300 0000 0400 0000 ffff 0000 MZ...	9000 0300 0000 0400 0000 ffff 0000 MZ...
0000 0000 0000 0000	0000 0000 0000 0000
0000 0000 8000 0000	0000 0000 8000 0000
21b8 014c cd21 5468!.L.!Th	21b8 014c cd21 5468!.L.!Th
616d 2063 616e 6e6f is program canno	616d 2063 616e 6e6f is program canno
2069 6e20 444f 5320 t be run in DOS	2069 6e20 444f 5320 t be run in DOS
2400 0000 0000 0000 mode....\$......	2400 0000 0000 0000 mode....\$......
5df1 9154 0000 0000 PE..L...].T....	9ef1 9154 0000 0000 PE..L...].T....
0b01 0800 00a2 0000!......	0b01 0800 00a2 0000!......
6ec1 0000 0020 0000n.....	6ec1 0000 0020 0000n.....
0020 0000 0002 0000@.....	0020 0000 0002 0000@.....
0400 0000 0000 0000	0400 0000 0000 0000
30fb 0000 0300 40850.....e.	3552 0100 0300 40855R.....e.
0000 1000 0010 0000	0000 1000 0010 0000
0000 0000 0000 0000	0000 0000 0000 0000
00e0 0000 6003 0000 ...K.....	00e0 0000 6003 0000 ...K.....
0000 0000 0000 0000	0000 0000 0000 0000
0000 0000 0000 0000	0000 0000 0000 0000



Timestamps in Java jar

data.tar

./usr/share/java/flute-1.1-SNAPSHOT.jar

metadata

l.1-SNAPSHOT.jar	l.1-SNAPSHOT.jar
1568 bytes, number of entries: 45	1568 bytes, number of entries: 45
inx 0 bx stor 15-Jan-07 20:23 META	inx 0 bx stor 15-Jan-07 20:25 META
inx 259 b- defN 15-Jan-07 20:23 META	inx 259 b- defN 15-Jan-07 20:25 META
inx 0 b- stor 15-Jan-07 20:23 org/	inx 0 b- stor 15-Jan-07 20:25 org/
inx 0 b- stor 15-Jan-07 20:23 org/	inx 0 b- stor 15-Jan-07 20:25 org/
inx 0 b- stor 15-Jan-07 20:23 org/	inx 0 b- stor 15-Jan-07 20:25 org/
inx 0 b- stor 15-Jan-07 20:23 org/	inx 0 b- stor 15-Jan-07 20:25 org/
inx 0 b- stor 15-Jan-07 20:23 org/	inx 0 b- stor 15-Jan-07 20:25 org/
inx 0 b- stor 15-Jan-07 20:23 org/	inx 0 b- stor 15-Jan-07 20:25 org/
inx 585 b- defN 15-Jan-07 20:23 org/	inx 585 b- defN 15-Jan-07 20:25 org/
inx 5744 b- defN 15-Jan-07 20:23 org/	inx 5744 b- defN 15-Jan-07 20:25 org/
inx 320 b- defN 15-Jan-07 20:23 org/	inx 320 b- defN 15-Jan-07 20:25 org/

They are ZIP archives, really.

Timestamps in PHP registry

data.tar.xz

data.tar

./usr/share/php/.registry/channel.pecl.php.net/oauth.reg

```
"2.0";s:13:"_lastmodified";i:1419537766;} "2.0";s:13:"_lastmodified";i:1419537812;}
```



Timestamps by a template engine

data.tar

./usr/lib/python2.7/dist-packages/spectacle/dsc/__init__.py

```
1 +-- 28 lines: #!/usr/bin/env python-----usr/bin/env python-----
29 VFSL=valueFromFrameOrSearchList         ameOrSearchList
30 VFSL=valueFromSearchList                 rchList
31 VFN=valueForName
32 currentTime=time.time                    time
33 __CHEETAH_version__ = '2.4.4'             __ = '2.4.4'
34 __CHEETAH_versionTuple__ = (2, 4, 4,     Tuple__ = (2, 4, 4, 'development', 0)
35 __CHEETAH_genTime__ = 1421397870.77925   __ = 1421397902.668939
36 __CHEETAH_genTimestamp__ = 'Fri Jan 16  stamp__ = 'Fri Jan 16 08:45:02 2015'
37 __CHEETAH_src__ = 'dsc.templ'           'dsc.templ'
38 __CHEETAH_srcLastModified__ = 'Fri Feb Modified__ = 'Fri Feb 25 06:40:15 2011'
39 __CHEETAH_docstring__ = 'Autogenerated ng__ = 'Autogenerated by Cheetah: The Pyth
40
41 if __CHEETAH_versionTuple__ < Required ionTuple__ < RequiredCheetahVersionTuple:
42     raise AssertionError(                 onError(
43 +--127 lines: 'This template was compo is this template was compiled with Cheetah vers
```



Identified issues (cont.)

Examples

Archives



Timestamps in gzip headers

data.tar.xz

data.tar

./usr/share/ispell/brasileiro.mwl.gz

metadata

```
1 gzip compressed data, was "br.ispell", last modified: Sat Jan 3 22:47:40 2015
```



Timestamps in ZIP archives

data.tar.xz

data.tar

./usr/share/boa-constructor/Docs/boa.apphelp.htb

metadata

```
+--249 lines: Archive:  boa.apphelp.htb-----
minimum file system compatibility required:  MS-DOS, OS/2 or NT FAT
minimum software version required to extract:  2.0
compression method:                          deflated
compression sub-type (deflation):             normal
file security status:                        not encrypted
extended local header:                       no
file last modified on (DOS date/time):       2015 Jan 16 09:55:52
file last modified on (UT extra field modtime): 2015 Jan 16 09:55:52 local
file last modified on (UT extra field modtime): 2015 Jan 16 09:55:52 UTC
32-bit CRC value (hex):                      5bb8662c
compressed size:                             1660 bytes
uncompressed size:                          5682 bytes
length of filename:                         19 characters
length of extra field:                      24 bytes
length of file comment:                     0 characters
```



Timestamps in tarballs

data.tar.xz

data.tar

./usr/share/doc/allegro4-doc/examples/source.tar.gz

source.tar

metadata

64	2015-01-09	22:29:44	CMakeLists.txt	64	2015-01-09	22:32:29	CMakeLists.txt
08	2015-01-09	22:29:44	afinfo.c	08	2015-01-09	22:32:29	afinfo.c
19	2015-01-09	22:29:44	akaitest.c	19	2015-01-09	22:32:29	akaitest.c
32	2015-01-09	22:29:44	allegro.pcx	32	2015-01-09	22:32:29	allegro.pcx
70	2015-01-09	22:29:44	digitest.c	70	2015-01-09	22:32:29	digitest.c
10	2015-01-09	22:29:44	ex12bit.c	10	2015-01-09	22:32:29	ex12bit.c
46	2015-01-09	22:29:44	ex3buf.c	46	2015-01-09	22:32:29	ex3buf.c
57	2015-01-09	22:29:44	ex3d.c	57	2015-01-09	22:32:29	ex3d.c
34	2015-01-09	22:29:44	exaccel.c	34	2015-01-09	22:32:29	exaccel.c
06	2015-01-09	22:29:44	exalpha.c	06	2015-01-09	22:32:29	exalpha.c
62	2015-01-09	22:29:44	example.dat	62	2015-01-09	22:32:29	example.dat
65	2015-01-09	22:29:44	example.h	65	2015-01-09	22:32:29	example.h
30	2015-01-09	22:29:44	examples.txt	30	2015-01-09	22:32:29	examples.txt



Users and groups in tarballs

data.tar.xz

data.tar

./usr/share/doc/raster3d/diffs.tar.gz

diffs.tar

metadata

1	-rw-r--r--	pbuilder1/pbuilder1	1	-rw-r--r--	pbuilder2/pbuilder2
2	-rw-r--r--	pbuilder1/pbuilder1	2	-rw-r--r--	pbuilder2/pbuilder2
3	-rw-r--r--	pbuilder1/pbuilder1	3	-rw-r--r--	pbuilder2/pbuilder2
4	-rw-r--r--	pbuilder1/pbuilder1	4	-rw-r--r--	pbuilder2/pbuilder2
5	-rw-r--r--	pbuilder1/pbuilder1	5	-rw-r--r--	pbuilder2/pbuilder2
6	-rw-r--r--	pbuilder1/pbuilder1	6	-rw-r--r--	pbuilder2/pbuilder2
7	-rw-r--r--	pbuilder1/pbuilder1	7	-rw-r--r--	pbuilder2/pbuilder2
8	-rw-r--r--	pbuilder1/pbuilder1	8	-rw-r--r--	pbuilder2/pbuilder2
9	-rw-r--r--	pbuilder1/pbuilder1	9	-rw-r--r--	pbuilder2/pbuilder2
10	-rw-r--r--	pbuilder1/pbuilder1	10	-rw-r--r--	pbuilder2/pbuilder2
11	-rw-r--r--	pbuilder1/pbuilder1	11	-rw-r--r--	pbuilder2/pbuilder2
12	-rw-r--r--	pbuilder1/pbuilder1	12	-rw-r--r--	pbuilder2/pbuilder2

Examples

Timestamps in documentation



Timestamps written by Doxygen

data.tar.xz

data.tar

./usr/share/doc/libnfo-doc/html
/dir_68267d1309a1af8e8297ef4c3efbcdba.html

<pre>: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html> <head> <meta charset="utf-8" /> <title>libnfo documentation</title> </head> <body> <div class="memItemLeft" align="center"> <small> Mon Dec 15 2014 04:03:26 for libnfo by &#1 </small> </div> <div class="memSeparator" colspan="2"></div> <div class="memItemLeft" align="center"> <small> Mon Dec 15 2014 04:04:03 for libnfo by &#1 </small> </div> </body> </html></pre>	<pre>: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html> <head> <meta charset="utf-8" /> <title>libnfo documentation</title> </head> <body> <div class="memItemLeft" align="center"> <small> Mon Dec 15 2014 04:04:03 for libnfo by &#1 </small> </div> <div class="memSeparator" colspan="2"></div> <div class="memItemLeft" align="center"> <small> Mon Dec 15 2014 04:03:26 for libnfo by &#1 </small> </div> </body> </html></pre>
---	---

< | >



Timestamps written by docbook-to-man

data.tar.xz

data.tar

ace_netsvcs.1.gz

ace_netsvcs.1

ETSVCS" "1" -----	ETSVCS" "1" -----
vc.conf, /usr/share/doc/ace-netsvcs/ACE-r	vc.conf, /usr/share/doc/ace-netsvcs/ACE-r
dt@cs.wustl.edu>	dt@cs.wustl.edu>
docbook-to-man, Thu 25 Dec 2014, 01:10	docbook-to-man, Thu 25 Dec 2014, 01:23



Timestamps written by Ghostscript

data.tar.xz

data.tar

./usr/share/doc/c++-annotations/cplusplus.pdf

pdftk cplusplus.pdf output - uncompress

```
-----  
d='W5M0MpCehiHzreSzNTczkc9d' ?>  
a/' x:xmptk='XMP toolkit 2.9.1-13, fram  
3.org/1999/02/22-rdf-syntax-ns#' xmlns:  
er>dvips + GPL Ghostscript 9.06</pdf:Pr :2b7e66bf-d448-11ef-0000-a06d27758a43'  
Date>2015-01-14T20:23:14Z</xmp:ModifyDa :2b7e66bf-d448-11ef-0000-a06d27758a43'  
:29Z</xmp:CreateDate>  
rref package</xmp:CreatorTool></rdf:Des  
DocumentID='uuid:b743c33d-d447-11ef-000 :2b7e66bf-d448-11ef-0000-a06d27758a43'  
t='application/pdf'><dc:title><rdf:Alt> :2b7e66bf-d448-11ef-0000-a06d27758a43'
```

Timestamps written by Ghostscript (cont.)

```
431320 9159 0 obj
431321 <<
431322 /ModDate (D:20150114202314Z00'00)
431323 /Subject ()
431324 /CreationDate (D:20150114202314Z
431325 /Author ()
431326 /Title ()
431327 /Keywords ()
431328 /Creator (LaTeX with hyperref pa
431329 /Producer (dvips + GPL Ghostscri
431330 >>
431331 +--9160 lines: endobj xref-----
440491 0027736476 00000 n
440492 0027841270 00000 n
440493 trailer
440494
440495 <<
440496 /Info 9159 0 R
440497 /ID [ece9748e11c19361dc941039bb]
440498 /Root 1 0 R
440499 /Size 9160
440500 >>

431320 9159 0 obj
431321 <<
431322 /ModDate (D:20150114202629Z00'00)
431323 /Subject ()
431324 /CreationDate (D:20150114202629Z
431325 /Author ()
431326 /Title ()
431327 /Keywords ()
431328 /Creator (LaTeX with hyperref pa
431329 /Producer (dvips + GPL Ghostscri
431330 >>
431331 +--9160 lines: endobj xref-----
440491 0027736476 00000 n
440492 0027841270 00000 n
440493 trailer
440494
440495 <<
440496 /Info 9159 0 R
440497 /ID [54f331d30af99447035b87a9bb]
440498 /Root 1 0 R
440499 /Size 9160
440500 >>
```

Timestamps written by GNU groff

data.tar.xz

data.tar

./usr/share/doc/corosync/html/confdb_context_get.3.html

<pre><!-- Creator : groff version 1.22.3 - <!-- CreationDate: Thu Jan 8 04:06:53 20 <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4 "http://www.w3.org/TR/html4/loose.dtd"> <html> <head> <meta name="generator" content="groff -Tr <meta http-equiv="Content-Type" content=" +-- 95 lines: <meta name="Content-Style"</pre>	<pre><!-- Creator : groff version 1.22.3 - <!-- CreationDate: Thu Jan 8 04:09:52 20 <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4 "http://www.w3.org/TR/html4/loose.dtd"> <html> <head> <meta name="generator" content="groff -Th <meta http-equiv="Content-Type" content=" +-- 95 lines: <meta name="Content-Style"</pre>
---	---

./usr/share/doc/corosync/html/confdb_context_set.3.html

<pre>1 <!-- Creator : groff version 1.22 2 <!-- CreationDate: Thu Jan 8 04:06:5 3 <!DOCTYPE html PUBLIC "-//W3C//DTD HT</pre>	<pre>1 <!-- Creator : groff version 1.22 2 <!-- CreationDate: Thu Jan 8 04:09:5 3 <!DOCTYPE html PUBLIC "-//W3C//DTD HT</pre>
--	--

Timestamps written by Javadoc

data.tar.xz

data.tar

./usr/share/doc/libconstantine-java-doc/javadoc/allclasses-frame.html

```
DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/
-- NewPage -->
<html lang="en">
<head>
-- Generated by javadoc (version 1.7.0_65) on Wed Jan 07 12:39:34 UTC 2015 -->
<meta http-equiv="Content-Type" content="text/html" charset="UTF-8">
<title>All Classes</title>
<meta name="date" content="2015-01-07">
<link rel="stylesheet" type="text/css" href="stylesheet.css" title="Style">
</head>
<body>
-147 lines: <h1 class="bar">All Classes</h1>-----
```



Timestamps written by man2html

data.tar.xz

data.tar

./usr/share/doc/privoxy/man-page/privoxy-man-page.html

<pre>1 +--301 lines: <!DOCTYPE HTML PUBLIC " 302 </DL> 303 </DL> 304 <HR> 305 This document was created by 306 man2html, 307 using the manual pages.
 308 Time: 07:05:10 GMT, January 16, 2015 309 </BODY> 310 </HTML></pre>	<pre>1 +--301 lines: <!DOCTYPE HTML PUBLIC " 302 </DL> 303 </DL> 304 <HR> 305 This document was created by 306 man2html, 307 using the manual pages.
 308 Time: 07:06:29 GMT, January 16, 2015 309 </BODY> 310 </HTML></pre>
--	--



Timestamps in TeX output (.dvi)

data.tar.xz

data.tar

manual.dvi.gz

manual.dvi

b 0000 0000 04b0 1b20;.....	b 0000 0000 04b0 1b20;.....
0 7574 2032 3031 342e TeX output 2014.	0 7574 2032 3031 342e TeX output 2014.
6 3430 8b00 0000 0100 12.11:0640.....	6 3431 8b00 0000 0100 12.11:0641.....
0 0000 0000 0000 0000 0 0000 0000 0000 0000 d 9ff2 0000 8ea0 0218 b 8d91 63ba d4f3 327c .s....{.c...2 0 0800 0000 0463 6d72 {Y.....cmr 0 7490 871c 7970 9078 8.Go...t...yp.x 5 7365 7474 696e 6793 7573 696e 6793 .e:	0 0000 0000 0000 0000 0 0000 0000 0000 0000 d 9ff2 0000 8ea0 0218 b 8d91 63ba d4f3 327c .s....{.c...2 0 0800 0000 0463 6d72 {Y.....cmr 0 7490 871c 7970 9078 8.Go...t...yp.x 5 7365 7474 696e 6793 7573 696e 6793 .e:

< ||| > < ||| >



Identified issues (cont.)

Examples

“Compiled at/on/by”



Build time via C preprocessor macros

```
80     {"to",1,NULL,'t'},
81     {0,0,0,0}
82 };
83
84 #define MSGSIZE 512
85 #define INPUT_TEXT_SIZE_INIT 32
86
87 char *pgname = "numconv";
88 char compdate[]="Compiled " __DATE__ " " __TIME__ ;
89
90 void ShowNumberSystems(int which) {
```

package info (click to toggle)

libuninum 2.7-1.1

- links: [PTS](#)
- area: main
- in suites: jessie, sid, wheezy
- size: 1,972 kB
- SLOC: ansic: 9,968; sh: 8,715; tcl: 553; makefile: 78

Build time via C preprocessor macros

```
190 z_version(void)
191 {
192     printf("Zorp %s (%s)\n"
193           "Revision: %s\n"
194           "Compile-Date: %s %s\n"
195           "Config-Date: %s\n"
196           "Trace: %s\n"
197           "Debug: %s\n"
198           "IPOptions: %s\n"
199           "%s\n"
200           ,
201           BROCHURE_VERSION, VERSION,
202           ZORP_SOURCE_REVISION,
203           __DATE__, __TIME__,
204           ZORP_CONFIG_DATE,
205           ON_OFF_STR(ENABLE_TRACE),
206           ON_OFF_STR(ENABLE_DEBUG),
207           ON_OFF_STR(ENABLE_IPOPTIONS),
```

package info (click to toggle)

zorp 3.9.5-4

- links: [PTS](#)
- area: main
- in suites: jessie, sid, wheezy
- size: 5,412 kB
- ctags: 5,387

Build time recorded via Makefile

```
149 genversion.$(OBJEXT): $(genversion_SOURCES) genversion.h
150
151 genversion.h: $(top_builddir)/config.status
152     -rm -f $@ $@.new
153     echo '#define CC "$(CC)"' > $@.new
154     echo '#define BUILT_DATE "'`date`'" >> $@.new
155     echo '#define BUILT_MACH "$(target)"' >> $@.new
156     mv $@.new $@
157
158 version.c: genversion$(EXEEXT)
159     -rm -f version.c
160     ./genversion$(EXEEXT) > version.c
161
162 BUILT_SOURCES += genversion.h version.c
```

package info (click to toggle)

amanda 1:3.3.6-4

- links: [PTS](#), [VCS](#)
- area: main
- in suites: jessie, sid
- size: 25,248 kB
- ctags: 28,823
- SLOC: ansic: 225,464; perl:

Hostname recorded via ./configure

```
364     VERSION="$VERSION (svn$SVN_REV)"
365     fi
366     fi
367     HOSTNAME=`hostname`
368     DATE=`date +"%d.%m.%Y %H:%M:%S %Z"`
369
370     cat > version.h <<EOF
371     /*
372     * anytun version info
373     *
374     * this file was created automatically
375     * do not edit this file directly
376     * use ./configure instead
377     */
378
379     #ifndef ANYTUN_version_h_INCLUDED
380     #define ANYTUN_version_h_INCLUDED
381
382     #define VERSION_STRING_0 " version $VERSION"
383     #define VERSION_STRING_1 "built on $HOSTNAME, $DATE"
```

package info (click to toggle)

anytun 0.3.5-1

- links: [PTS](#), [VCS](#)
- area: main
- in suites: jessie, sid
- size: 1,424 kB
- ctags: 1,339
- SLOC: cpp: 9,126; sh: 618; makefile: 367

Build time recorded via ./configure

```
364     VERSION="$VERSION (svn$SVN_REV)"
365     fi
366 fi
367 HOSTNAME=`hostname`
368 DATE=`date +"%d.%m.%Y %H:%M:%S %Z"`
369
370 cat > version.h <<EOF
371 /*
372  * anytun version info
373  *
374  * this file was created automatically
375  * do not edit this file directly
376  * use ./configure instead
377  */
378
379 #ifndef ANYTUN_version_h_INCLUDED
380 #define ANYTUN_version_h_INCLUDED
381
382 #define VERSION_STRING_0 " version $VERSION"
383 #define VERSION_STRING 1 "built on $HOSTNAME, $DATE"
```

package info (click to toggle)

anytun 0.3.5-1

- links: [PTS](#), [VCS](#)
- area: main
- in suites: jessie, sid
- size: 1,424 kB
- ctags: 1,339
- SLOC: cpp: 9,126; sh: 618;
makefile: 367

m4 macros for autoconf (build time)

```
75 AC_FLDIGI_SH_DQ([echo $ac_configure_args])
76 AC_DEFINE_UNQUOTED([BUILD_CONFIGURE_ARGS], [$ac_sh_dq], [Configure arguments])
77
78 AC_FLDIGI_SH_DQ([date])
79 AC_DEFINE_UNQUOTED([BUILD_DATE], [$ac_sh_dq], [Build date])
80
81 AC_FLDIGI_SH_DQ([whoami])
82 AC_DEFINE_UNQUOTED([BUILD_USER], [$ac_sh_dq], [Build user])
83
84 AC_FLDIGI_SH_DQ([hostname])
85 AC_DEFINE_UNQUOTED([BUILD_HOST], [$ac_sh_dq], [Build host])
86
87 AC_FLDIGI_SH_DQ([$CXX -v 2>&1 | tail -1])
88 AC_DEFINE_UNQUOTED([BUILD_COMPILER], [$ac_sh_dq], [Compiler])
```

m4 macros for autoconf (username)

```
75 AC_FLDIGI_SH_DQ([echo $ac_configure_args])
76 AC_DEFINE_UNQUOTED([BUILD_CONFIGURE_ARGS], [$ac_sh_dq], [Configure arguments])
77
78 AC_FLDIGI_SH_DQ([date])
79 AC_DEFINE_UNQUOTED([BUILD_DATE], [$ac_sh_dq], [Build date])
80
81 AC_FLDIGI_SH_DQ([whoami])
82 AC_DEFINE_UNQUOTED([BUILD_USER], [$ac_sh_dq], [Build user])
83
84 AC_FLDIGI_SH_DQ([hostname])
85 AC_DEFINE_UNQUOTED([BUILD_HOST], [$ac_sh_dq], [Build host])
86
87 AC_FLDIGI_SH_DQ([$CXX -v 2>&1 | tail -1])
88 AC_DEFINE_UNQUOTED([BUILD_COMPILER], [$ac_sh_dq], [Compiler])
```

m4 macros for autoconf (hostname)

```
75 AC_FLDIGI_SH_DQ([echo $ac_configure_args])
76 AC_DEFINE_UNQUOTED([BUILD_CONFIGURE_ARGS], [$ac_sh_dq], [Configure arguments])
77
78 AC_FLDIGI_SH_DQ([date])
79 AC_DEFINE_UNQUOTED([BUILD_DATE], [$ac_sh_dq], [Build date])
80
81 AC_FLDIGI_SH_DQ([whoami])
82 AC_DEFINE_UNQUOTED([BUILD_USER], [$ac_sh_dq], [Build user])
83
84 AC_FLDIGI_SH_DQ([hostname])
85 AC_DEFINE_UNQUOTED([BUILD_HOST], [$ac_sh_dq], [Build host])
86
87 AC_FLDIGI_SH_DQ([$CXX -v 2>&1 | tail -1])
88 AC_DEFINE_UNQUOTED([BUILD_COMPILER], [$ac_sh_dq], [Compiler])
```

Identified issues (cont.)

Examples

File ordering



File ordering in python-support files

./usr/share/python-support/babiloo.private

```
1 +-- 16 lines: /usr/share/babiloo/run.py 1 +-- 16 lines: /usr/share/babiloo/run.py
17 /usr/share/babiloo/core/modules/utills.py 17 /usr/share/babiloo/core/modules/utills.py
18 /usr/share/babiloo/core/modules/_init_.py 18 /usr/share/babiloo/core/modules/_init_.py
19 /usr/share/babiloo/core/modules/compress.py 19 /usr/share/babiloo/core/modules/compress.py
20 /usr/share/babiloo/core/net/xmlrpc.py 20 /usr/share/babiloo/core/net/xmlrpc.py
21 /usr/share/babiloo/core/net/_init_.py 21 /usr/share/babiloo/core/net/_init_.py
22 /usr/share/babiloo/core/net/downloader.py 22 /usr/share/babiloo/core/net/downloader.py
-----
23 /usr/share/babiloo/qt/settings.py 23 /usr/share/babiloo/qt/main_ui.py
24 /usr/share/babiloo/qt/gui_widgets.py 24 /usr/share/babiloo/qt/settings.py
25 /usr/share/babiloo/qt/dictfilemanager.py 25 /usr/share/babiloo/qt/gui_widgets.py
26 /usr/share/babiloo/qt/contentSearchModel.py 26 /usr/share/babiloo/qt/dictfilemanager.py
27 /usr/share/babiloo/qt/historyListModel.py 27 /usr/share/babiloo/qt/contentSearchModel.py
28 /usr/share/babiloo/qt/main.py 28 /usr/share/babiloo/qt/historyListModel.py
29 +-- 4 lines: /usr/share/babiloo/qt/about.py 29 /usr/share/babiloo/qt/main.py
30 /usr/share/babiloo/qt/onlineDictionary.py 30 +-- 4 lines: /usr/share/babiloo/qt/about.py
31 /usr/share/babiloo/qt/definitionView.py 31 /usr/share/babiloo/qt/onlineDictionary.py
32 /usr/share/babiloo/qt/SplashScreen.py 32 /usr/share/babiloo/qt/definitionView.py
33 /usr/share/babiloo/qt/_init_.py 33 /usr/share/babiloo/qt/SplashScreen.py
34 /usr/share/babiloo/qt/Qt2Po.py 34 /usr/share/babiloo/qt/_init_.py
35 /usr/share/babiloo/qt/images_rc.py 35 /usr/share/babiloo/qt/Qt2Po.py
36 /usr/share/babiloo/qt/about_ui.py 36 /usr/share/babiloo/qt/images_rc.py
37 /usr/share/babiloo/qt/settings_ui.py 37 /usr/share/babiloo/qt/about_ui.py
38 /usr/share/babiloo/qt/chooseLanguage_ui.py 38 /usr/share/babiloo/qt/settings_ui.py
39 /usr/share/babiloo/qt/main_ui.py 39 /usr/share/babiloo/qt/chooseLanguage_ui.py
40 /usr/share/babiloo/qt/about_ui.py 40 /usr/share/babiloo/qt/main_ui.py
41 /usr/share/babiloo/qt/chooseLanguage_ui.py 41 /usr/share/babiloo/qt/about_ui.py
42 /usr/share/babiloo/qt/main_ui.py 42 /usr/share/babiloo/qt/chooseLanguage_ui.py
```



Identified issues (cont.)

Examples

Randomness



Random Perl hash order

See *Algorithmic complexity attacks in perlsec(1)*.

data.tar.xz

data.tar

./usr/lib/x86_64-linux-gnu/perl5/5.20/Gtk2/Spell/Install/Files.pm

```
1 package GtkSpell::Install::Files;
2
3 $self = {
4     'deps' => [
5         'Cairo',
6         'Pango',
7         'Gtk2',
8         'Glib'
9     ],
10    'inc' => '-pthread -I/usr/inc
11    'libs' => '-lgtkspell -lgtk-;
12    'typemaps' => [
13 ++ 30 lines: 'gtkspell.typemap'-----
```

```
1 package GtkSpell::Install::Files;
2
3 $self = {
4     'deps' => [
5         'Pango',
6         'Cairo',
7         'Gtk2',
8         'Glib'
9     ],
10    'inc' => '-pthread -I/usr/inc
11    'libs' => '-lgtkspell -lgtk-;
12    'typemaps' => [
13 ++ 30 lines: 'gtkspell.typemap'-----
```



Random serial numbers in Ogg streams

data.tar.xz

data.tar

./usr/share/games/kiki-the-nano-bot/sound/atom_digest.ogg

4f67 6753 0002 0000 0000 0000 0000 4c1c	4f67 6753 0002 0000 0000 0000 0000 b2dd
2106 0000 0000 693d d98c 011e 0176 6f72	920e 0000 0000 b90a bf35 011e 0176 6f72
6269 7300 0000 0001 112b 0000 0000 0000	6269 7300 0000 0001 112b 0000 0000 0000
4871 0000 0000 0000 9901 4f67 6753 0000	4871 0000 0000 0000 9901 4f67 6753 0000
0000 0000 0000 0000 4c1c 2106 0100 0000	0000 0000 0000 0000 b2dd 920e 0100 0000
7c12 0a7e 0b3f ffff ffff ffff ffb5	9927 b7d1 0b3f ffff ffff ffff ffb5
0376 6f72 6269 732f 0000 0058 6970 682e	0376 6f72 6269 732f 0000 0058 6970 682e
4f72 6720 6c69 6256 6f72 6269 7320 4920	4f72 6720 6c69 6256 6f72 6269 7320 4920
3230 3134 3031 3232 2028 5475 7270 616b	3230 3134 3031 3232 2028 5475 7270 616b
c3a4 72c3 a46a 6969 6e29 0000 0000 0105	c3a4 72c3 a46a 6969 6e29 0000 0000 0105
766f 7262 6973 1242 4356 0100 0001 000c	766f 7262 6973 1242 4356 0100 0001 000c
5214 2125 1953 4a63 0895 5252 2905 1d63	5214 2125 1953 4a63 0895 5252 2905 1d63
lines: 00000c0: 505b 471d 63d4 3946 2164 10	lines: 00000c0: 505b 471d 63d4 3946 2164 10
9452 4a29 a594 524a 29a5 0000 8003 0700	9452 4a29 a594 524a 29a5 0000 8003 0700
8000 23e8 24a3 ca22 6c34 e1c2 0310 0000	8000 23e8 24a3 ca22 6c34 e1c2 0310 0000
0002 0002 4c00 8101 8282 5108 0284 1108	0002 0002 4c00 8101 8282 5108 0284 1108
0000 0000 0008 00f8 0000 480a 8088 8868	0000 0000 0008 00f8 0000 480a 8088 8868
e60c 0e10 1214 1618 1a1c 1e20 2224 0000	e60c 0e10 1214 1618 1a1c 1e20 2224 0000
0000 0000 0000 0000 0000 044f 6767 5300	0000 0000 0000 0000 0000 044f 6767 5300
04af 1200 0000 0000 004c 1c21 0602 0000	04af 1200 0000 0000 00b2 dd92 0e02 0000
0086 dc69 8014 5e40 3b47 4c37 3a49 3f42	0026 c74f de14 5e40 3b47 4c37 3a49 3f42



Identified issues (cont.)

Examples

Even more timestamps!



Timestamps in PNG

Even images!

data.tar.xz

data.tar

./usr/share/icons/hicolor/128x128/apps/hedgewars.png

sng

```
1 +--104 lines: #SNG: from stdin-----
105   ( 64,141,230)   # rgb = (0x40,
106 }
107 bKGD {index: 12}
108 tRNS {
109 0}
110 tIME {
111   # 31 Dec 2014 05:46:02 GMT
112   year: 2014
113   month: 12
114   day: 31
115   hour: 5
116   minute: 46
117   second: 2
118 }
119 tEXt {
120   keyword: "date:create";
121   text: "2014-12-31T05:46:00+00:00"
122 }
```

```
1 +--104 lines: #SNG: from stdin-----
105   ( 64,141,230)   # rgb = (0x40,
106 }
107 bKGD {index: 12}
108 tRNS {
109 0}
110 tIME {
111   # 31 Dec 2014 05:52:27 GMT
112   year: 2014
113   month: 12
114   day: 31
115   hour: 5
116   minute: 52
117   second: 27
118 }
119 tEXt {
120   keyword: "date:create";
121   text: "2014-12-31T05:52:25+00:00"
122 }
```



Timestamps in TrueType font files

And fonts!

```
by FontForge 14:57 31-July-2012
Font created: Sun Feb 27 14:37:21 2011
Font modified: Fri Jan 2 00:02:36 2015
```

```
le (at 102048)
Version=1
fontRevision=2.32999
checksumAdj=cc520daa
magicNumber=5f0f3cf5 (0x5f0f3cf5, diff=0
flags=1f baseline_at_0 lsb_at_0 instrs_d
unitsPerEm=2048
create[0]=0
create[1]=c9901221
File created: Sun Feb 27 14:37:21 2011
modtime[0]=0
modtime[1]=d0cb909c
File modified: Fri Jan 2 00:02:36 2015
```

```
by FontForge 14:57 31-July-2012
Font created: Sun Feb 27 14:37:21 2011
Font modified: Fri Jan 2 00:06:50 2015
```

```
le (at 102048)
Version=1
fontRevision=2.32999
checksumAdj=cc5209b2
magicNumber=5f0f3cf5 (0x5f0f3cf5, diff=0
flags=1f baseline_at_0 lsb_at_0 instrs_d
unitsPerEm=2048
create[0]=0
create[1]=c9901221
File created: Sun Feb 27 14:37:21 2011
modtime[0]=0
modtime[1]=d0cb919a
File modified: Fri Jan 2 00:06:50 2015
```



Please help!



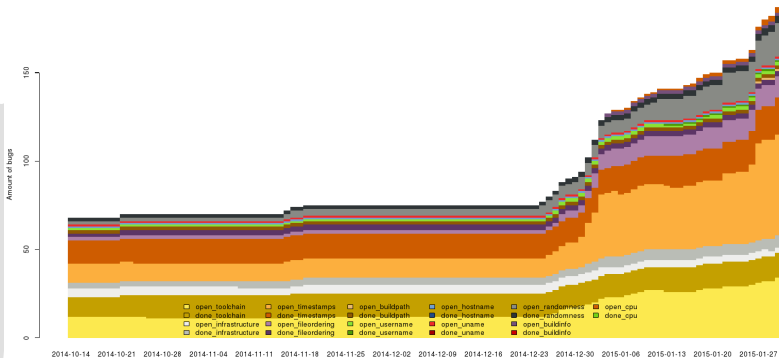
Please help!

- Do not record time, username, hostname, kernel version...
 - ▶ ... or make it optional.
- Sort file paths.
- Sort dictionary keys.
- Merge our patches!

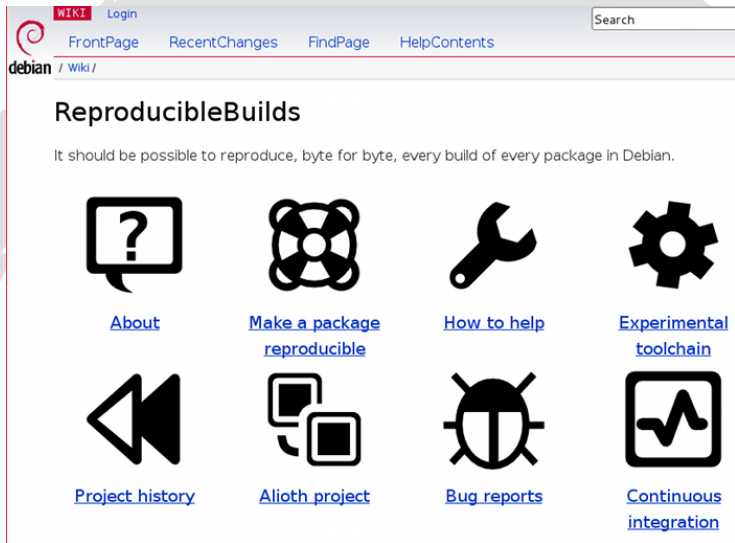


Bugs filed









Bugs with usertags for user reproducible-builds@lists.alioth.debian.org



Help Debian?



The screenshot shows the Debian Wiki page for 'Reproducible Builds'. At the top, there is a navigation bar with 'WIKI' in a red box, a 'Login' link, and a search box. Below this are links for 'FrontPage', 'RecentChanges', 'FindPage', and 'HelpContents'. The page title is 'ReproducibleBuilds'. A paragraph below the title states: 'It should be possible to reproduce, byte for byte, every build of every package in Debian.' Below this paragraph are eight icons arranged in a 2x4 grid, each with a corresponding link below it:

-  [About](#)
-  [Make a package reproducible](#)
-  [How to help](#)
-  [Experimental toolchain](#)
-  [Project history](#)
-  [Alioth project](#)
-  [Bug reports](#)
-  [Continuous integration](#)

Help Debian?

- Inventory issues
- Make packages build reproducibly
- Fix known common issues:
 - ▶ Get reproducible PE binaries;
 - ▶ Random filenames with GCC;
 - ▶ ...
- Hack Debian archive infrastructure
 - ▶ Store and distribute *.buildinfo files (#763822)
 - ▶ ...
- Hack tools to display local packages reproducibility status

Contributors

akira	Hans-Christoph Steiner	Peter De Wachter
Andrew Ayer	Helmut Grohne	Reiner Herrmann
Asheesh Laroia	Holger Levsen	Stefano Rivera
Chris Lamb (lamby)	josch	Stéphane Glondu
Chris West	Lunar	Steven Chamberlain
Daniel Kahn Gillmor	Mattia Rizzolo	Tom Fitzhenry
David Suarez	Niels Thykier	Tomasz Buchert
Drew Fisher	Niko Tyni	Wookey
Guillem Jover	Paul Wise	Ximin Luo

Stay in touch

- Subscribe to the ReproducibleBuilds wiki pages.
- Mailing lists:
 - ▶ `reproducible-builds@lists.alioth.debian.org`
 - ▶ `reproducible-commits@lists.alioth.debian.org`
- Join `#debian-reproducible` on `irc.oftc.net`



Other distributions

- Fedora
<http://securityblog.redhat.com/2013/09/18/reproducible-builds-for-fedora/>
- OpenSUSE build-compare
<https://build.opensuse.org/package/show/openSUSE:Factory/build-compare>
- NixOS
<http://lists.science.uu.nl/pipermail/nix-dev/2013-June/011357.html>



Reproducible Fedora?

- No known activity after the initial blog post.
- Fedora is leading developments for key components.
- Can we help **reproducible Fedora**?

fedora 



SLES? OpenBSD? Firefox? LibreOffice?

- We hope **reproducible builds** will become the norm.
- Our documentation should be helpful to others.
- Come talk to us!



Future

- Ready for the next Debian release (*stretch*)
- Reproducible installation media
- Reproducible live images (pure Debian, Grml, Tails)
- Reproducible cross-platform builds (“rebootstrap”)
- Binary transparency logs: public log of all software releases



Thanks

- Mike Perry and Seth Schoen for their 31C3 talk
- Profitbricks for sponsoring `jenkins.debian.net`
- Globalsign for sponsoring X.509 certificates
- Designers of Tango icons
- Everyone who helped!



Questions? Comments?



<https://wiki.debian.org/ReproducibleBuilds>
[https://reproducible.debian.net/
#debian-reproducible](https://reproducible.debian.net/#debian-reproducible) on OFTC

Holger B8BF 5413 7B09 D35C F026 FE9D 091A B856 069A AA1C
Lunar 0603 CCFD 9186 5C17 E88D 4C79 8382 C95C 2902 3DF9

