

Browsing the Web Securely with Tor

Alexander Færøy

March 5, 2020

Driving IT Aarhus



About Me

- Core Developer at The Tor Project since early 2017. Team Lead of the Network Team since late 2019.
- Free Software developer since 2006.
- Worked with distributed systems in the Erlang programming language, WebKit-based mobile browsers, embedded development, and software development consulting.



What is Tor?

- Online anonymity, and censorship circumvention.
 - Free software.
 - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.

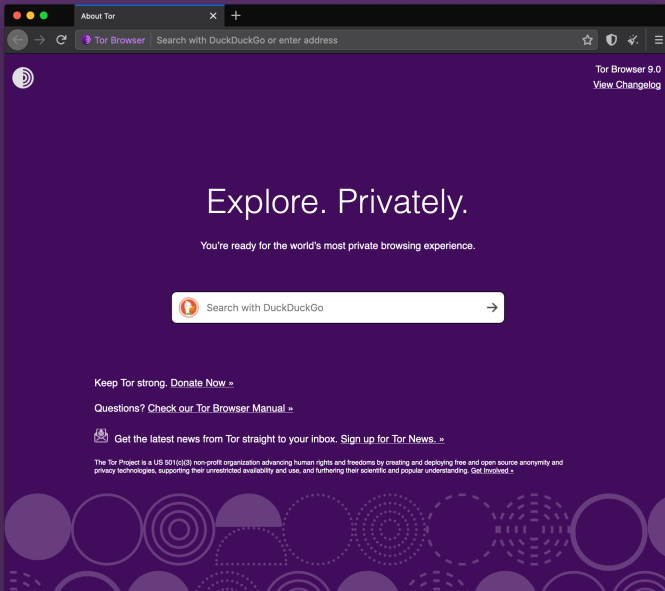


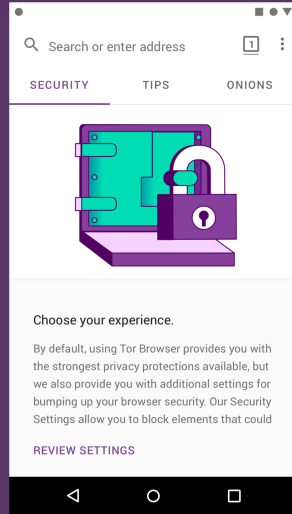
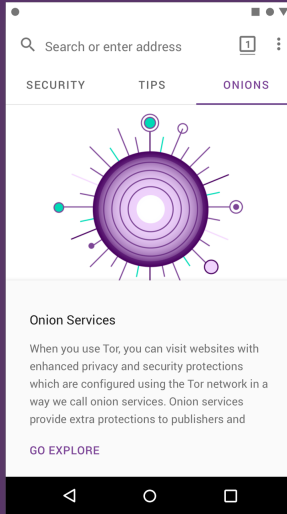
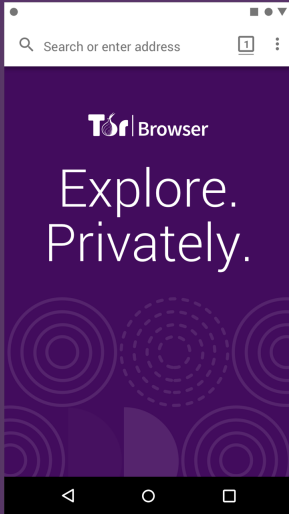
History

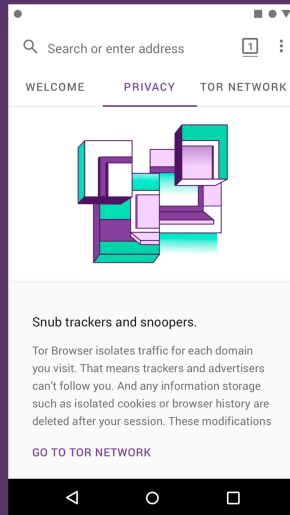
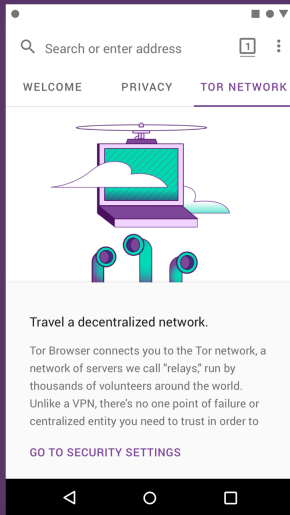
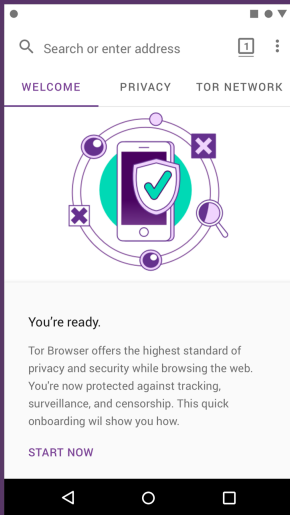
Early 2000s	Working with the U.S. Naval Research Laboratory.
2004	Sponsorship by the Electronic Frontier Foundation.
2006	The Tor Project, Inc. became a non-profit.
2007	Expansion to anti-censorship.
2008	Tor Browser development.
2010	The Arab spring.
2013	The summer of Snowden.
2018	Anti-censorship team created.
2019	Tor Browser for Android released.
2020	Network Health team created.

Somewhere between 2,000,000 and 8,000,000 daily users.





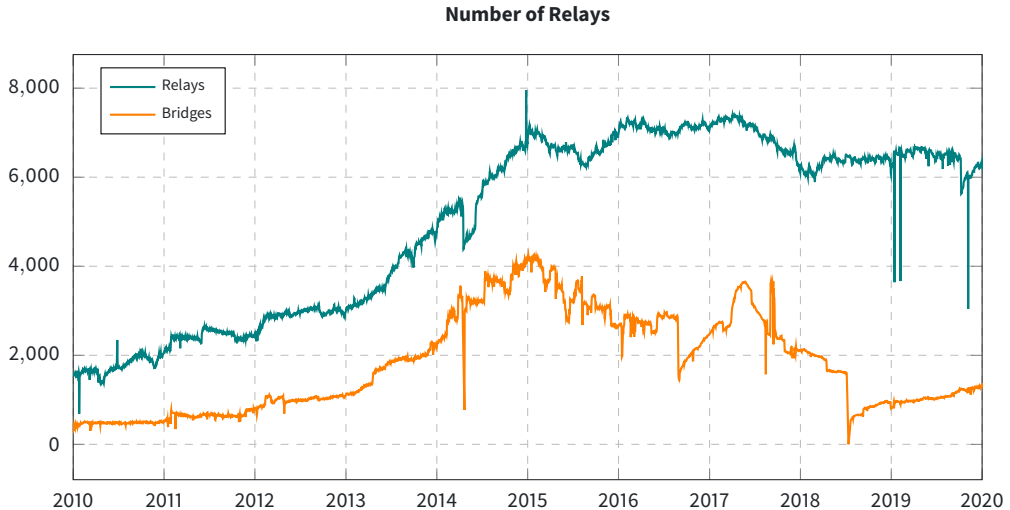




We also ship Tor to others:

- We have our own Debian mirror on deb.torproject.org.
- Other free software distributions. This is often where the relay operators get their Tor version from.
- Brave's "Private Tab" feature uses Tor.
- OnionShare, SecureDrop, etc.

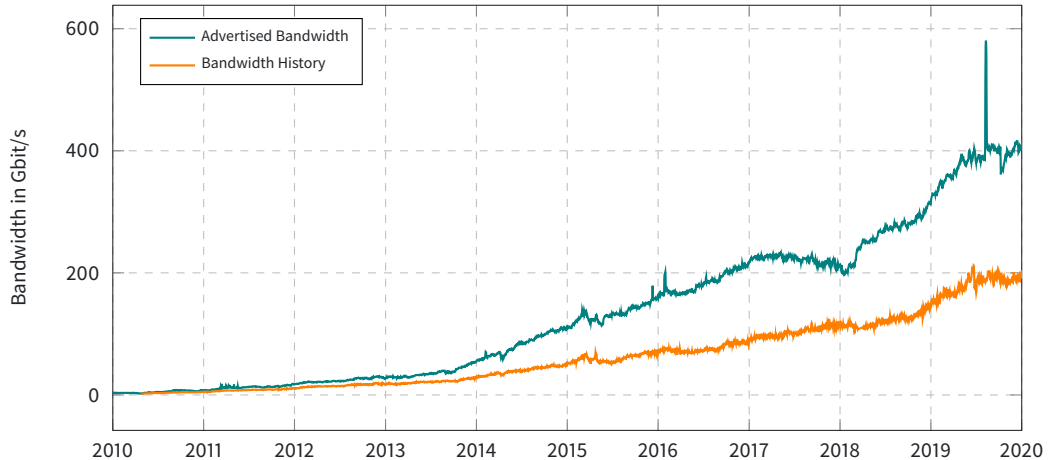
The Tor Network



Source: metrics.torproject.org

The Tor Network

Total Relay Bandwidth



Source: metrics.torproject.org

The Tor Network

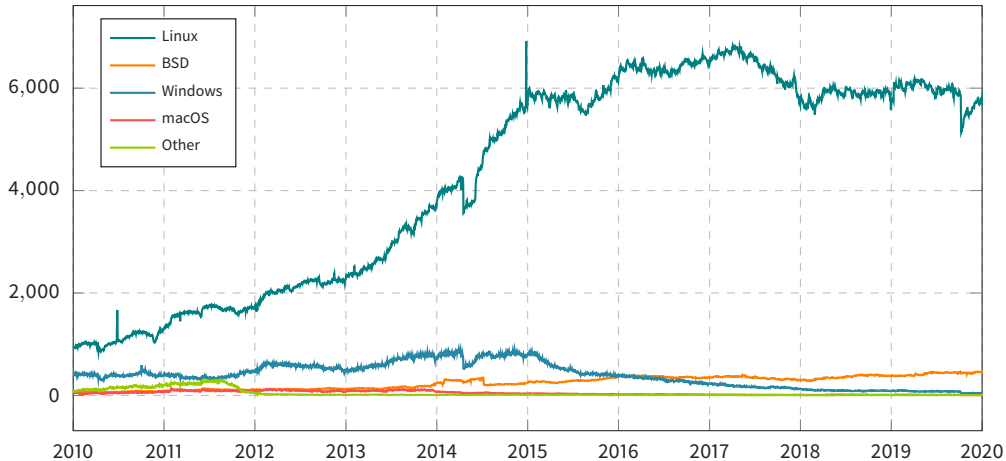
Tor's **safety** comes from **diversity**:

1. Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation.
2. Diversity of users and reasons to use it. 50,000 users in Iran means almost all of them are normal citizens.

Research problem: How do we measure diversity over time?

The Tor Network

Number of Relays per Platform

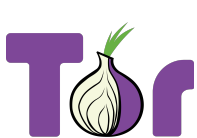


Source: metrics.torproject.org

Tor Releases

Version	Merge Window	Feature Freeze	Release	End of Life
0.3.5 (LTS)	15/6/2018	15/9/2018	7/1/2019	1/2/2022
0.4.0	15/10/2018	15/1/2019	2/5/2019	2/2/2020
0.4.1	15/2/2018	15/5/2019	20/8/2019	20/5/2020
0.4.2	10/6/2019	15/9/2019	9/12/2019	15/9/2022
0.4.3	11/10/2019	15/1/2020	15/4/2020	TBD
0.4.4	15/2/2020	15/5/2020	15/8/2020	TBD
0.4.5	15/6/2020	15/9/2020	15/12/2020	TBD

Tor Browser



=



Tor Project | Anonymity Online

https://www.torproject.org

Site Information for www.torproject.org

Connection

Secure Connection

Tor Circuit

This browser

Lithuania 195.189.96.148 Guard

Germany 131.188.40.188

Austria 109.70.100.7

torproject.org

New Circuit for this Site

Your Guard node may not change. Learn more

Permissions

You have not granted this site any special permissions.


rt Community Blog Donate English (En)

Download Tor Browser

Privately.
Freely.

and surveillance. Circumvent censorship.

Download Tor Browser



BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

Tor Browser

Anti-Censorship Team

- FTE.
- Meek.
- Obfs 3 and 4.
- Scramblesuit.

Applications Team

- Tor Launcher.
- Tor Button.

Network Team

- Tor ("little-t-tor")



Tor Browser

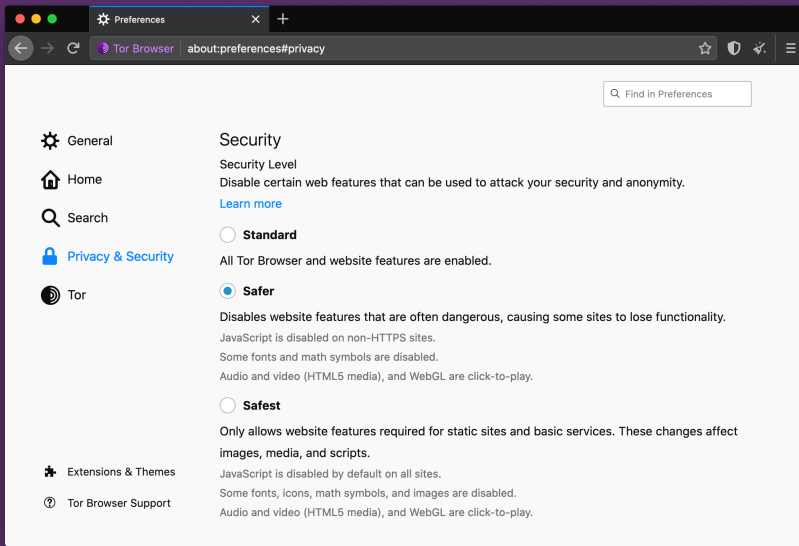
The philosophy behind the design choices in Tor Browser:

- Preserve existing user model.
- Favor changes that are least likely to break sites.
- Plugins must be restricted.
- Minimize Global Privacy Options.
- No filters.
- Stay current.

Tor Browser

The security requirements are primarily concerned with ensuring the safe use of Tor.

- Proxy Obedience.
- State Separation.
- Disk Avoidance.
- Application Data Isolation.



Focus on strong privacy protection:

- Cross-Origin Identifier Unlinkability.
- Cross-Origin Fingerprinting Unlinkability.
- Long-Term Unlinkability.

Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0

Tor Browser

Attribute	Value
User agent ⓘ	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept ⓘ	text/html,application/xhtml+xml,application/xml;q=0.9;/*;q=0.8
Content encoding ⓘ	gzip, deflate, br
Content language ⓘ	en-US,en;q=0.5
List of plugins ⓘ	
Platform ⓘ	Linux x86_64
Cookies enabled ⓘ	yes
Do Not Track ⓘ	yes
Timezone ⓘ	-120
Screen resolution ⓘ	1920x1080x24
Use of local storage ⓘ	yes
Use of session storage ⓘ	yes
Canvas ⓘ	Cwm fjordbank glyphs vext quiz, 🧐 Cwm fjordbank glyphs vext quiz, 😊
WebGL Vendor ⓘ	Intel Open Source Technology Center
WebGL Renderer ⓘ	Mesa DRI Intel(R) UHD Graphics 620 (Kabylake GT2)

Firefox 60

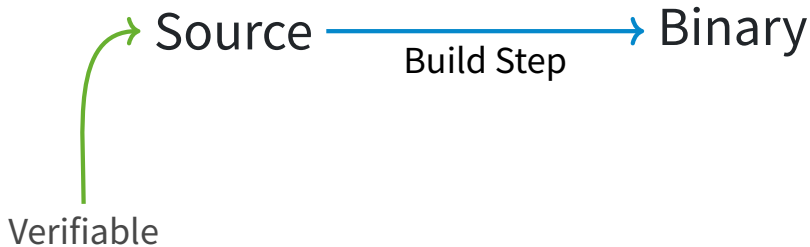
Attribute	Value
User agent ⓘ	Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
Accept ⓘ	text/html,application/xhtml+xml,application/xml;q=0.9;/*;q=0.8
Content encoding ⓘ	gzip, deflate
Content language ⓘ	en-US,en;q=0.5
List of plugins ⓘ	
Platform ⓘ	Linux x86_64
Cookies enabled ⓘ	yes
Do Not Track ⓘ	NC
Timezone ⓘ	0
Screen resolution ⓘ	1000x900x24
Use of local storage ⓘ	yes
Use of session storage ⓘ	yes
Canvas ⓘ	
WebGL Vendor ⓘ	Not supported
WebGL Renderer ⓘ	Not supported

Tor Browser

Reproducible Builds



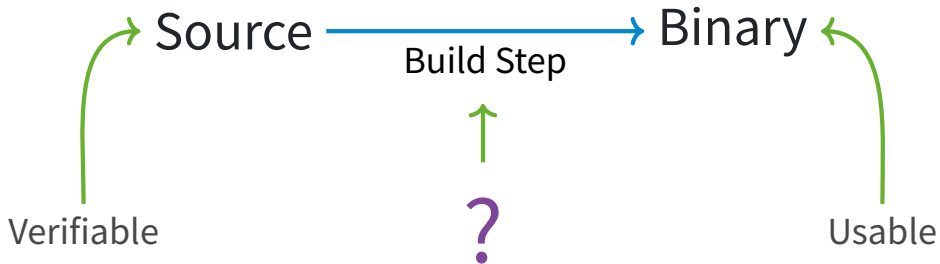
Reproducible Builds



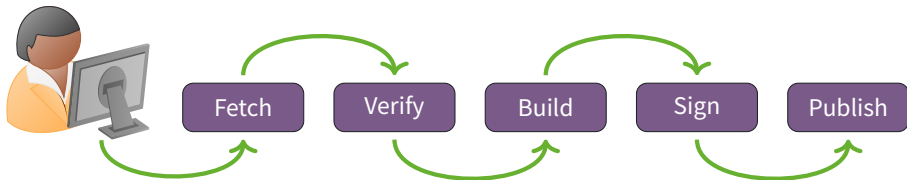
Reproducible Builds



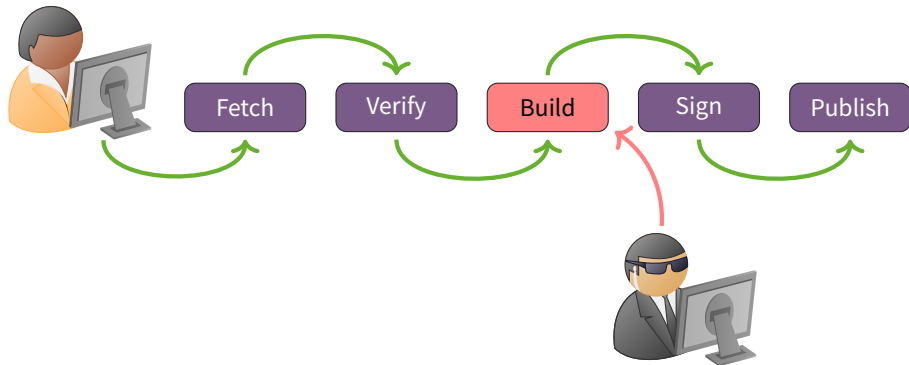
Reproducible Builds



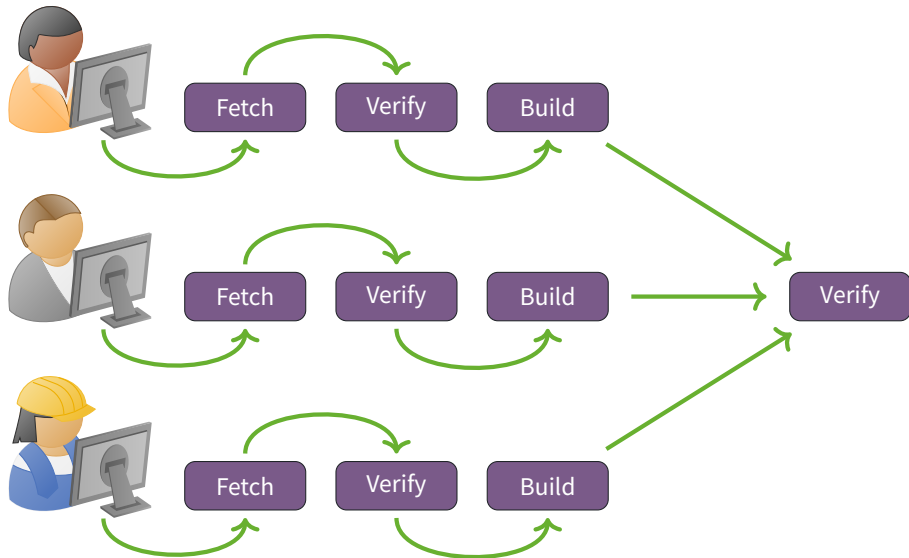
Build Process



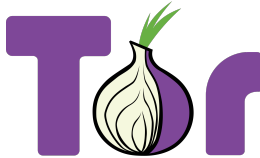
Build Process



Build Process



Reproducible Builds



Reproducible Builds Workflow

#29510 closed task (fixed)

Opened at 2019-02-15T11:18:49+01:00

Closed at 2019-02-23T10:05:18+01:00

Last modified at 2019-02-27T12:18:01+01:00

Check reproducibility of the build of 8.5a8

Reported by:	boklm	Owned by:	tbb-team
Priority:	Very High	Milestone:	
Component:	Applications/Tor Browser	Version:	
Severity:	Normal	Keywords:	
Cc:	pospeselr	Actual Points:	
Parent ID:		Points:	
Reviewer:		Sponsor:	

Description

I did the build of 8.5a8 that we are releasing:

[Reply](#) [Delete](#)

⇒ <https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.txt>

⇒ <https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.txt-boklm.asc>

⇒ <https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.incrementals.txt>

⇒ <https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.incrementals.txt-boklm.asc>

In order to verify that the build of this release is reproducible, we need a second person to do a build. We usually do that before publishing a release. However we are having some delay doing it this time, and because this release includes an important security fix, we will be doing this verification after the release is published.

Reproducible Builds Workflow

Changed at 2019-02-27T12:02:14+01:00 by boklm

comment:2 follow-up: ↓ 3

pospeselr mentioned his build was matching, except the `mar-tools-mac64.zip` file.

I uploaded there the `mar-tools-mac64.zip` he sent me:

➡ https://people.torproject.org/~boklm/bug_29510/mar-tools-mac64.zip

And the diff from diffoscope:

➡ https://people.torproject.org/~boklm/bug_29510/mar-tools.diff

Reproducible Builds Workflow

```
--- mar-tools-mac64.zip
+++ /home/boklm/tor-browser-build/alpha/unsigned/8.5a8/mar-tools-mac64.zip
  zipinfo {}
@@ -1,20 +1,20 @@
-Zip file size: 2049025 bytes, number of entries: 18
+Zip file size: 2049012 bytes, number of entries: 18
 drwx-----  3.0 unx          0 b- stor 19-Feb-12 08:50 mar-tools/

[...]

--rwx-----  3.0 unx    50216 b- defN 19-Feb-12 08:50 mar-tools/mar
--rwx-----  3.0 unx    27112 b- defN 19-Feb-12 08:50 mar-tools/mbsdiff
+-rwx-----  3.0 unx    50208 b- defN 19-Feb-12 08:50 mar-tools/mar
+-rwx-----  3.0 unx    27104 b- defN 19-Feb-12 08:50 mar-tools/mbsdiff

[...]

-18 files, 4637421 bytes uncompressed, 2046841 bytes compressed:  55.9%
+18 files, 4637405 bytes uncompressed, 2046828 bytes compressed:  55.9%
```

Reproducible Builds Workflow

```
readelf --wide --hex-dump=.strtab {}  
@@ -2,15 +2,15 @@  
Hex dump of section '.strtab':  
0x00000000 00637274 73747566 662e6300 5f5f4a43 .crtstuff.c.__JC  
0x00000010 525f4c49 53545f5f 00646572 65676973 R_LIST__.deregis  
0x00000020 7465725f 746d5f63 6c6f6e65 73007265 ter_tm_clones.re  
0x00000030 67697374 65725f74 6d5f636c 6f6e6573 gister_tm_clones  
0x00000040 005f5f64 6f5f676c 6f62616c 5f64746f .__do_global_dto  
0x00000050 72735f61 75780063 6f6d706c 65746564 rs_aux.completed  
- 0x00000060 2e363637 30005f5f 646f5f67 6c6f6261 .6670.__do_globa  
+ 0x00000060 2e363636 31005f5f 646f5f67 6c6f6261 .6661.__do_globa  
0x00000070 6c5f6474 6f72735f 6175785f 66696e69 l_dtors_aux_fini  
0x00000080 5f617272 61795f65 6e747279 00667261 _array_entry.fra  
0x00000090 6d655f64 756d6d79 005f5f66 72616d65 me_dummy.__frame  
0x000000a0 5f64756d 6d795f69 6e69745f 61727261 _dummy_init_arra  
0x000000b0 795f656e 74727900 2f766172 2f746d70 y_entry./var/tmp  
0x000000c0 2f627569 6c642f66 69726566 6f782d35 /build/firefox-5  
0x000000d0 38613433 39646434 6536662f 6d6f6475 8a439dd4e6f/modu
```

Reproducible Builds Workflow

```
readelf --wide --string-dump=.comment {}  
@@ -1,6 +1,6 @@
```

String dump of section '.comment':

```
- [ 0] GCC: (Debian 4.9.2-10+deb8u1) 4.9.2  
- [ 24] clang version 3.9.1 (tags/RELEASE_391/final)  
- [ 51] GCC: (Debian 4.8.4-1) 4.8.4  
+ [ 0] GCC: (Debian 4.9.2-10) 4.9.2  
+ [ 1d] clang version 3.9.1 (tags/RELEASE_391/final)  
+ [ 4a] GCC: (Debian 4.8.4-1) 4.8.4
```

Reproducible Builds Problems

Common problems includes:

- Timestamps as part of the build process.
- Usernames.
- Locale settings.
- Host settings (such as hostname and IP).

Tor is not foolproof

- Browser metadata fingerprinting.
- Browser exploits.
- Traffic analysis.
- Operational security mistakes.

How can you help?

Help test our Alpha releases



torproject.org/download/alpha/

How can you help?


- Run a Tor relay or a bridge!
- Teach others about Tor and privacy in general.
- Find, and maybe fix, bugs in Tor.
- Test Tor on your platform of choice.
- Work on some of the many open research projects.
- Donate at donate.torproject.org



Questions?

 @ahfaeroey

 ahf@torproject.org

 OpenPGP:
1C1B C007 A9F6 07AA 8152
C040 BEA7 B180 B149 1921



This work is licensed under a
Creative Commons
Attribution-ShareAlike 4.0 International License

