

HOW DO I TAILS?

A Beginner's Guide to Anonymous Computing

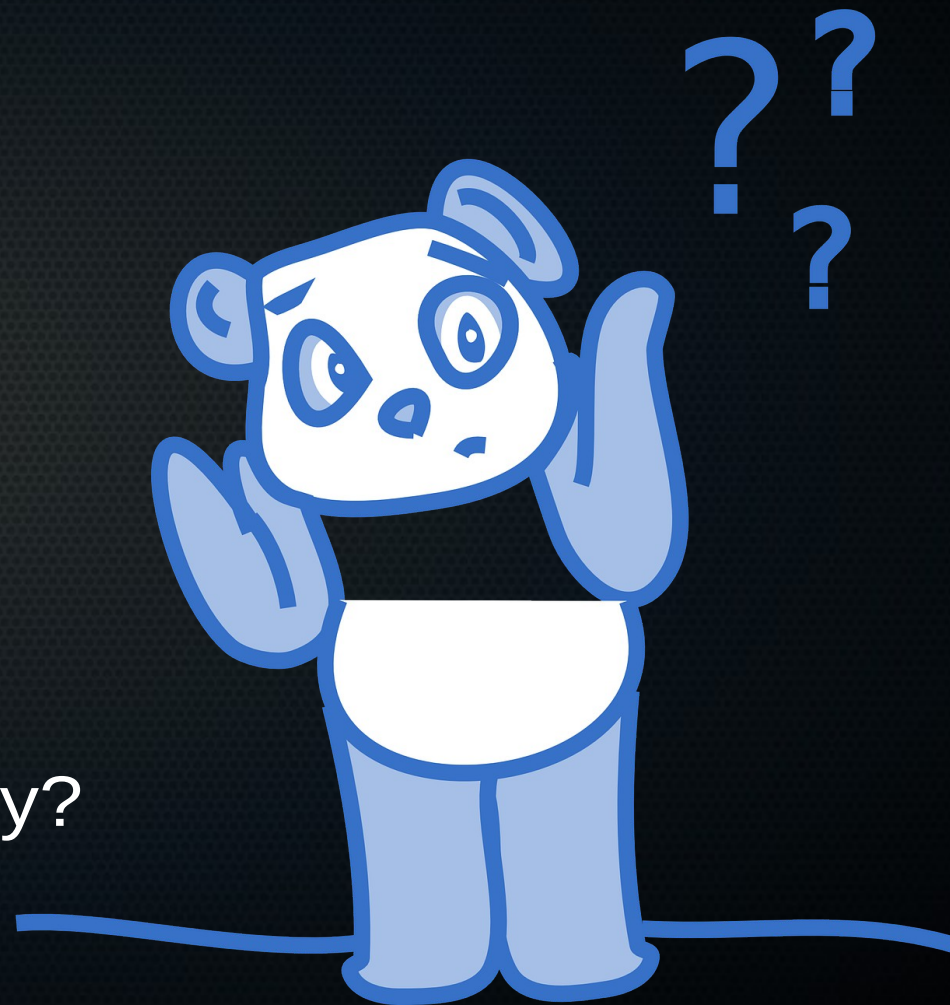


Who is this guy?

- Penetration Tester
- Former Network & Sysadmin
- Protester, Activist
- Privacy Advocate, EFF Volunteer

What is covered in this talk?

- What is Tails, who uses it, and why?
- How does it work?
- How do I start using it?
- Threat Modeling? Operational Security?



What is TAILS?

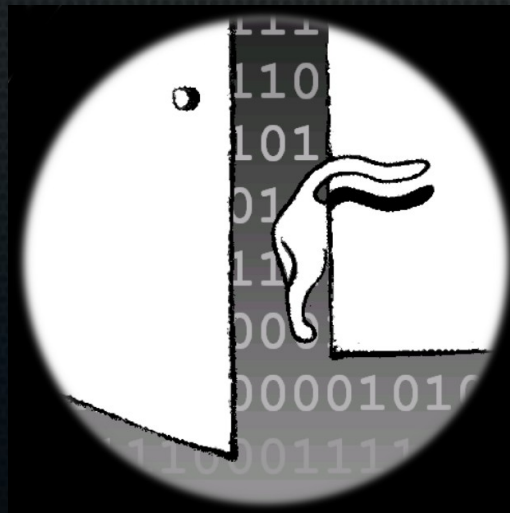
- "...a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity."
- GPL3 licensed.



Free as in Freedom

Where did it come from?

- Originally started as Incognito, a Gentoo-based distro.
- Tails first released June 2009.
- Funded primarily by The Tor Project.
- Developers are anonymous/pseudonymous.



Who uses Tails/Tor?

- Journalists & Their Sources
- Whistleblowers
- Political Activists & Protesters
- Military & Government Agents
- Librarians
- Victims of Stalking, Domestic Abuse
- Privacy Conscious Netizens

Why should I care about privacy?

- Chilling effects.
- Information can be edited, manipulated and misconstrued.
- Information collected won't be used to your benefit.
- Subject to the faults of human behavior.



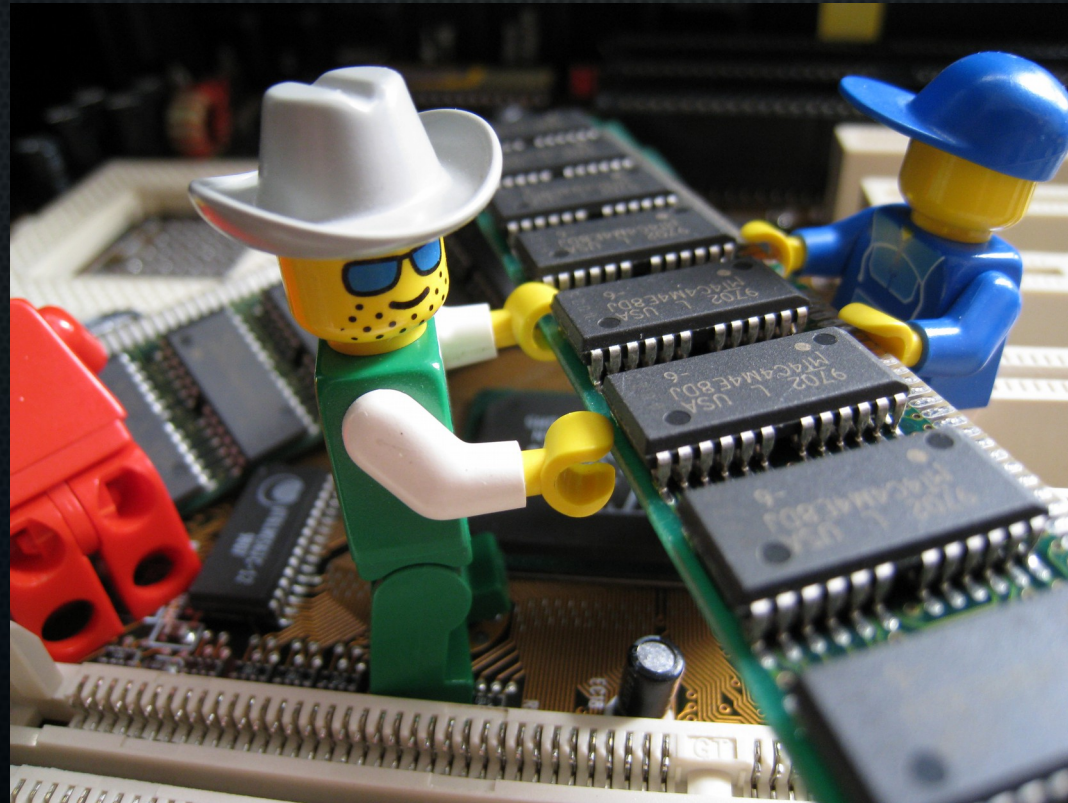
Is privacy really that important?

- Article 12, UN Universal Declaration of Human Rights
- <https://ihavesomethingtohi.de>



Amnesic

- Runs entirely in RAM (no swap).
- RAM is wiped on reboot/shutdown.

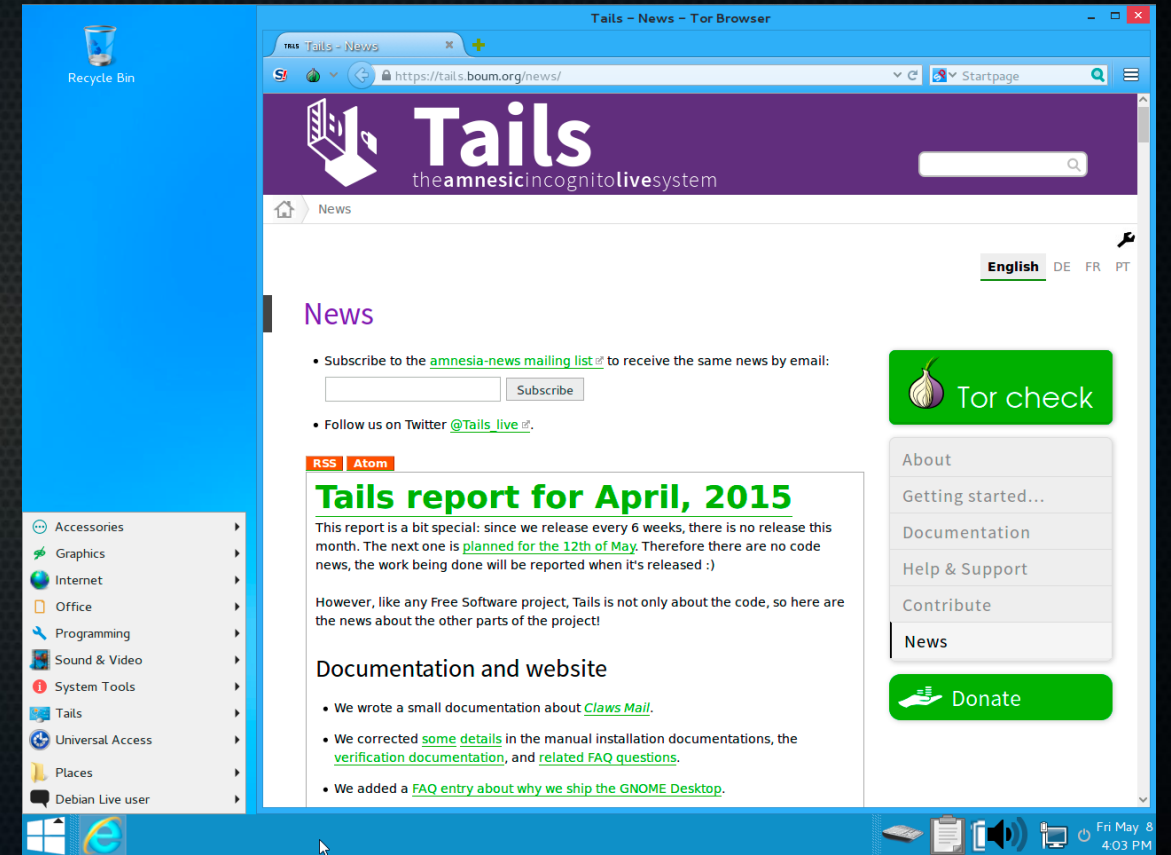
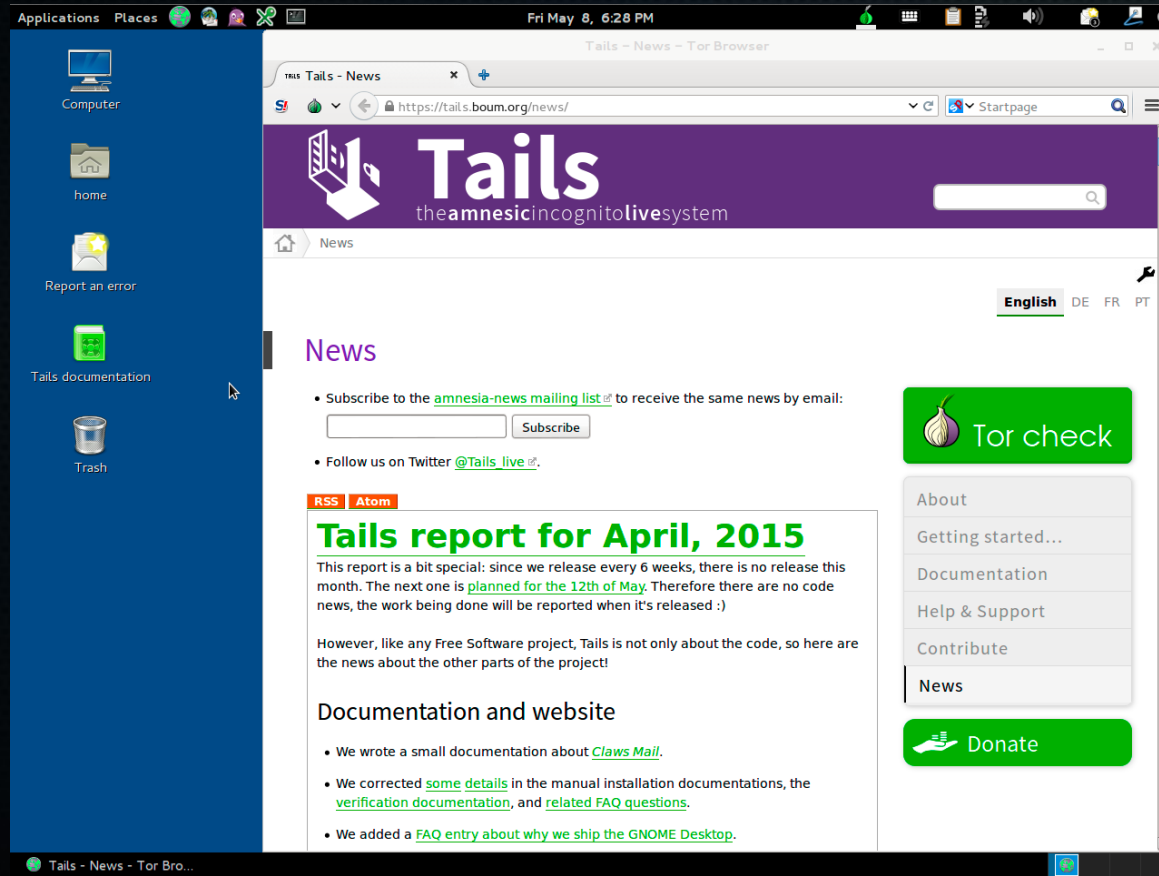


Incognito

- Uses MAC address spoofing.
- All traffic is routed through Tor.
- LAN Admin / ISP can see Tor traffic, but no contents.
- Destination can see that you're coming from Tor.



Camouflage



Portable

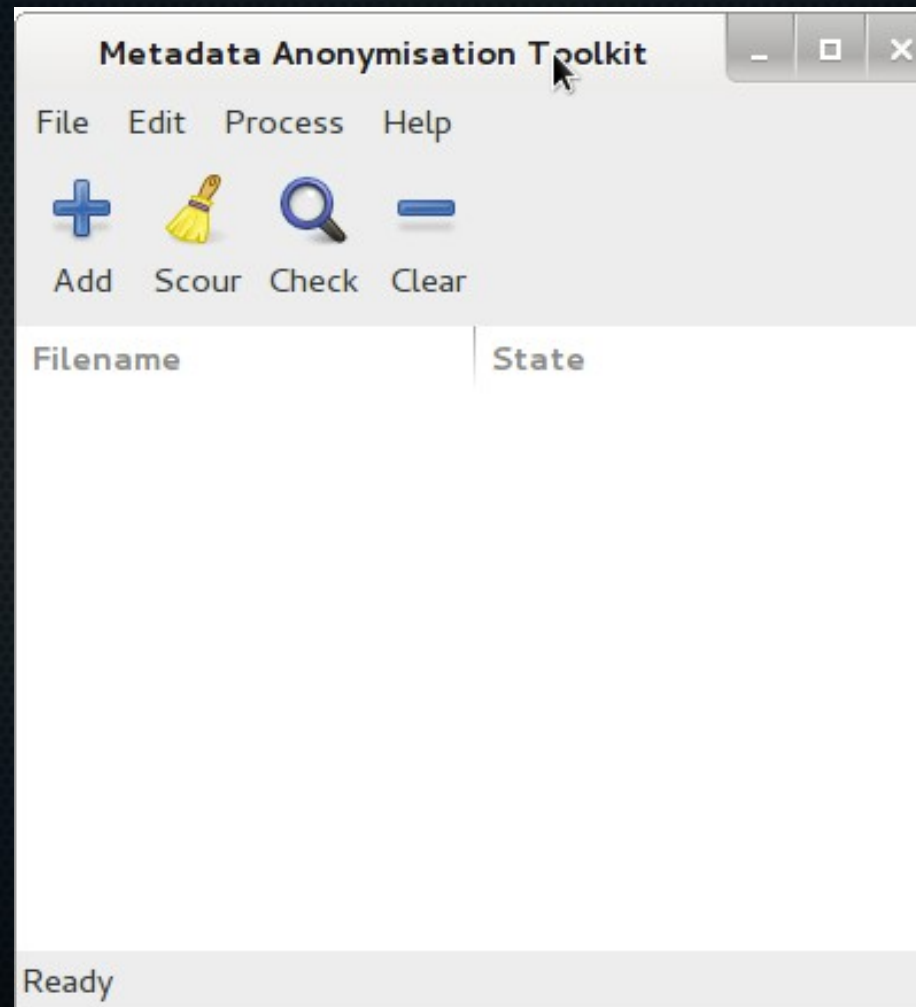
- (Almost) any machine, (almost) anywhere!



Live System

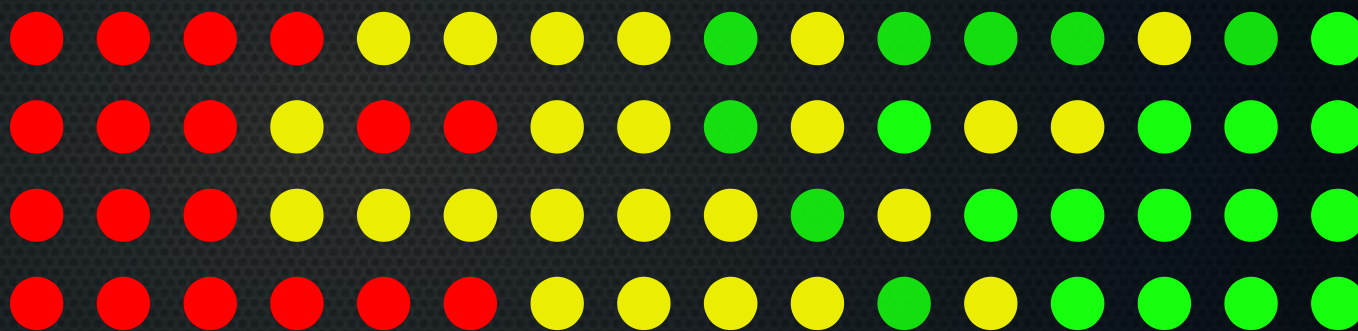
- Web Browser (Tor Browser w/ NoScript)
- Mail Client (CLAWS w/ GPG [Soon to be Icedove])
- Chat Client (Pidgin w/ OTR)
- Bitcoin Wallet (Electrum)
- Password Manager (KeePassX)
- Document Software (LibreOffice)
- Image Software (GIMP & Inkscape)
- Audio Software (Audacity)

Metadata Anonymisation Toolkit



I2P Integration

I2P



Threat Modeling

- Tier I – General privacy, passive tracking & profiling

The Acxiom logo features the word "acxiom" in a blue, lowercase, sans-serif font. The letter "i" is replaced by a green globe icon with white latitude and longitude lines. A small "TM" trademark symbol is located to the right of the word.

at&t



Threat Modeling

- Tier II – "Low level" active adversary.



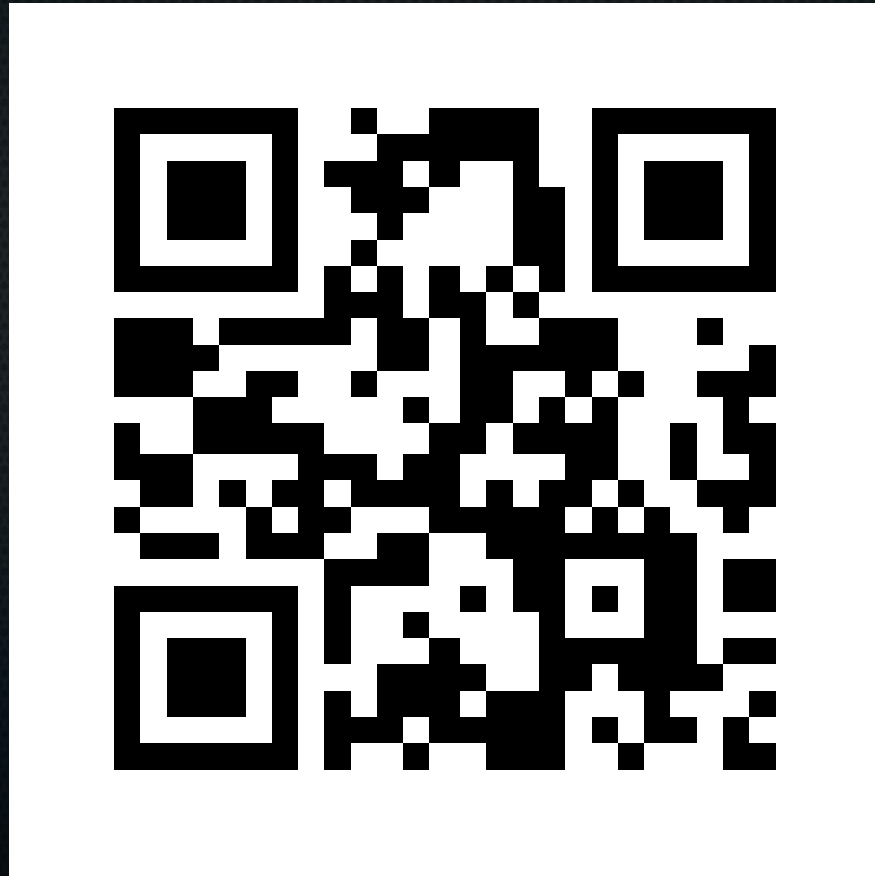
Threat Modeling

- Tier III – Nation States, "Three Letter Agencies"

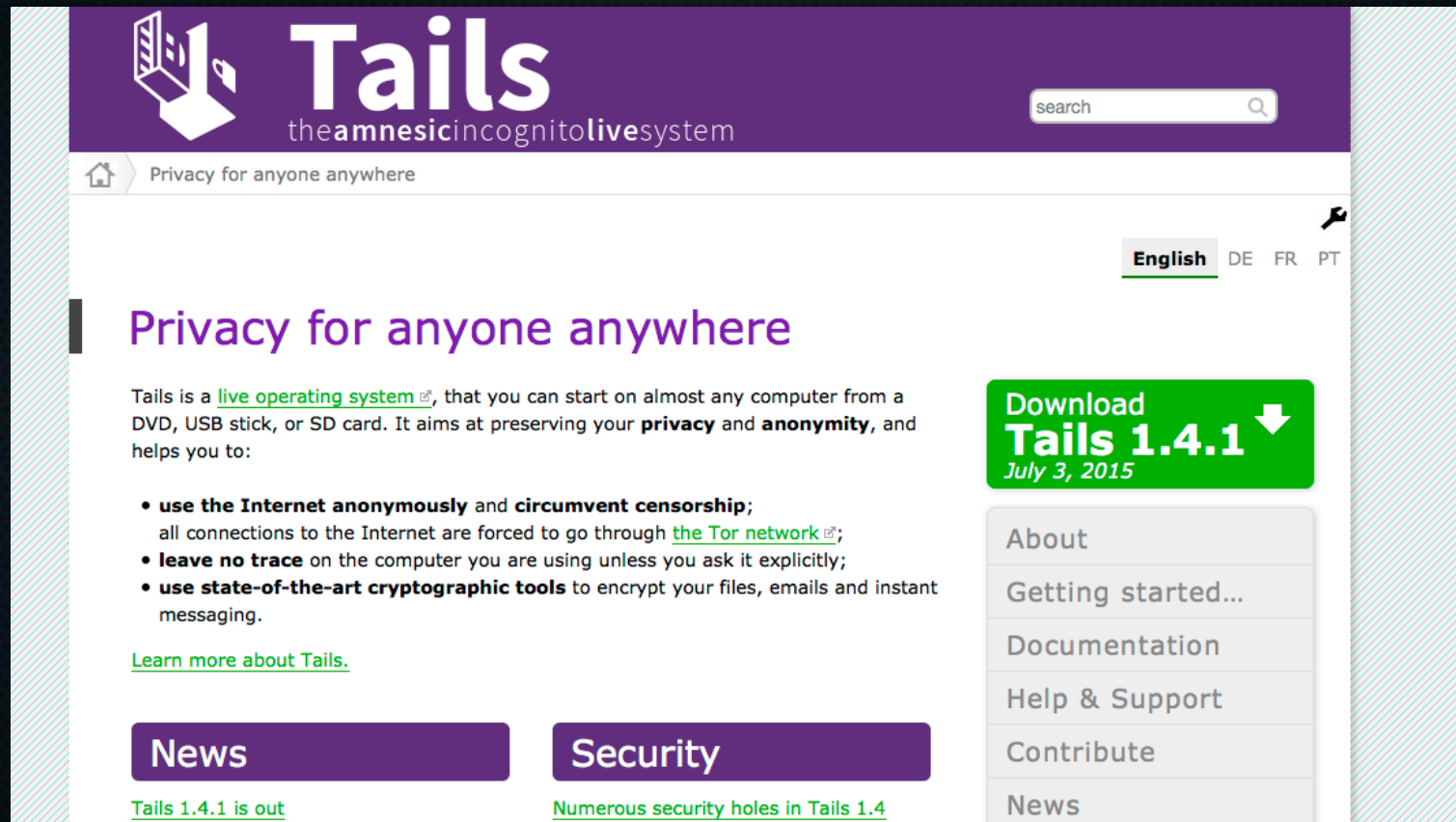


Simple Instructions

- <https://goo.gl/A6m2si>



Obtaining Image



The screenshot shows the homepage of the Tails operating system. The header is purple with the Tails logo (a laptop with a padlock) and the text "Tails the amnesic incognito livesystem". A search bar is on the right. Below the header, a navigation bar includes a home icon, the slogan "Privacy for anyone anywhere", and language options for English, DE, FR, and PT. The main content area features a large purple heading "Privacy for anyone anywhere" followed by a paragraph describing Tails as a live operating system. A list of three bullet points highlights its features: anonymous internet use, no trace left, and state-of-the-art cryptographic tools. A green button with a download arrow says "Download Tails 1.4.1 July 3, 2015". A sidebar on the right contains a menu with links for About, Getting started..., Documentation, Help & Support, Contribute, and News. At the bottom, two purple buttons labeled "News" and "Security" are shown, with links below them: "Tails 1.4.1 is out" and "Numerous security holes in Tails 1.4".

Tails
the amnesic incognito livesystem

search

Privacy for anyone anywhere


English DE FR PT

Privacy for anyone anywhere

Tails is a [live operating system](#), that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your **privacy** and **anonymity**, and helps you to:

- **use the Internet anonymously** and **circumvent censorship**; all connections to the Internet are forced to go through [the Tor network](#);
- **leave no trace** on the computer you are using unless you ask it explicitly;
- **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

[Learn more about Tails.](#)

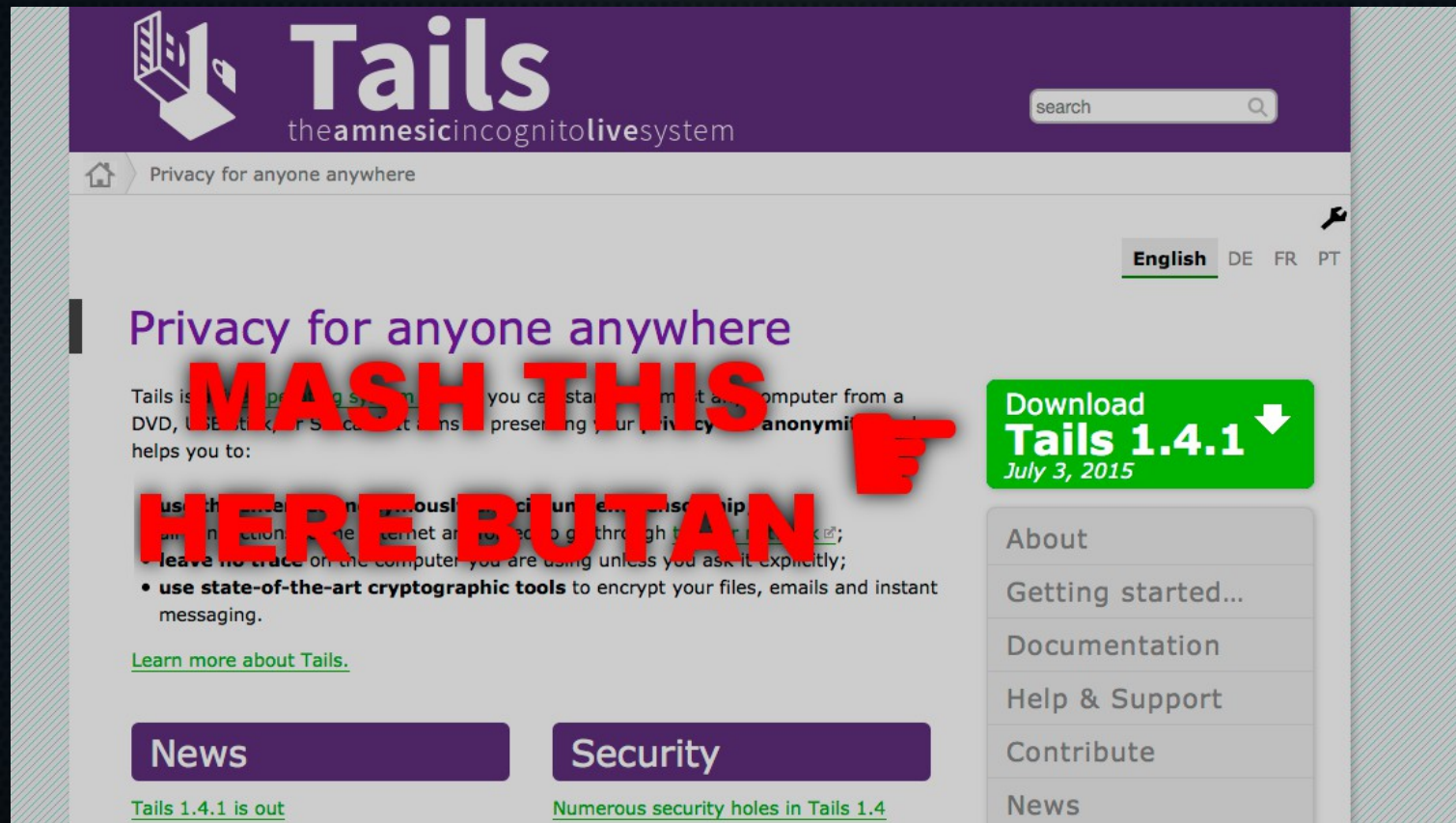
Download Tails 1.4.1 
July 3, 2015

About
Getting started...
Documentation
Help & Support
Contribute
News

News **Security**

[Tails 1.4.1 is out](#) [Numerous security holes in Tails 1.4](#)

Obtaining Image



The screenshot shows the Tails website homepage. The header features the Tails logo (a stylized laptop) and the text "Tails the amnesic incognito livesystem". A search bar is located in the top right. Below the header, there is a navigation bar with a home icon and the text "Privacy for anyone anywhere". The main content area includes a large heading "Privacy for anyone anywhere" and a paragraph of text. A prominent red annotation "MASH THIS" with a hand icon pointing to a green "Download Tails 1.4.1" button is overlaid on the page. Another red annotation "HERE BUT AN" is overlaid on the text below. The page also features a sidebar with links for "About", "Getting started...", "Documentation", "Help & Support", "Contribute", and "News". At the bottom, there are two purple buttons labeled "News" and "Security", each with a link below it.

MASH THIS

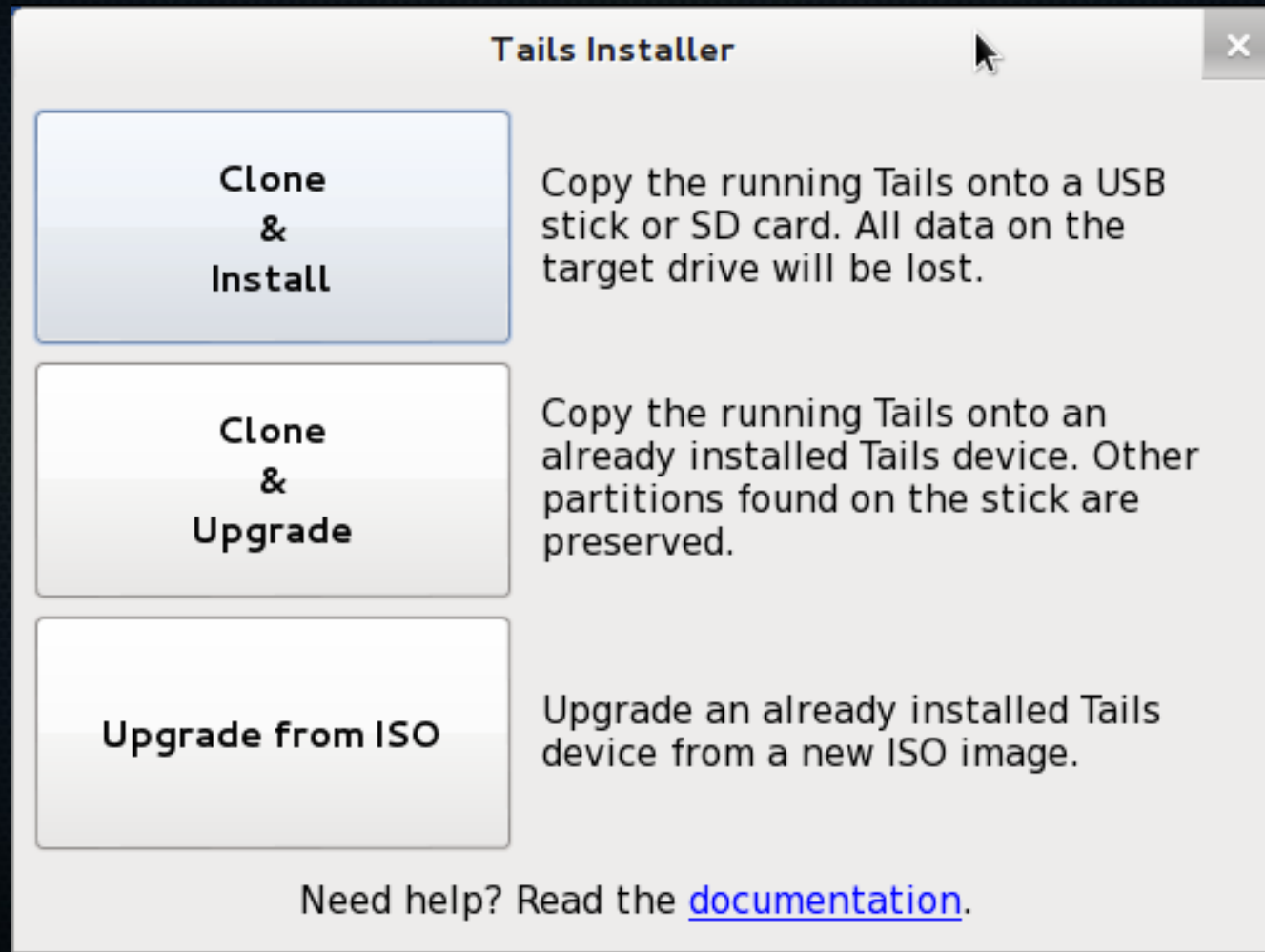
HERE BUT AN

Download Tails 1.4.1
July 3, 2015

News
[Tails 1.4.1 is out](#)

Security
[Numerous security holes in Tails 1.4](#)

Tails Installer



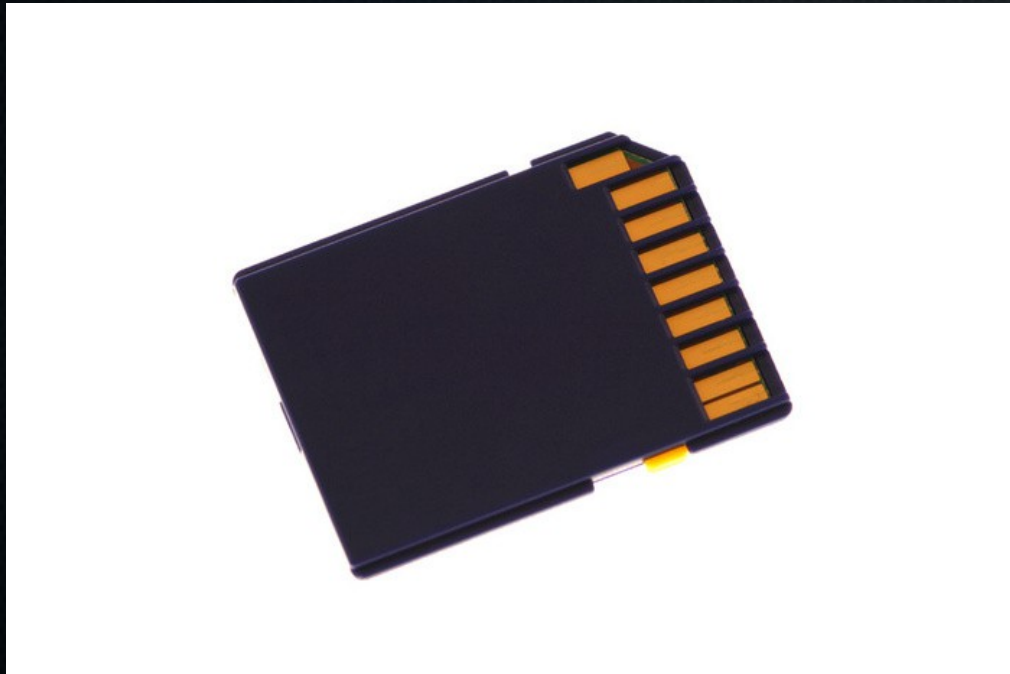
Persistent Storage

- Your Documents
- GPG Keychain
- KeePassX Keyring
- Bitcoin Wallet
- Additional Packages
- Config Files

Choose Your Installation Media

- What you install on matters!
- Base your decision off of your threat model.

SD Card



USB Drive



USB Drive

- Can you trust your USB drive?

Some of the recent enhancements of Kanguru Remote Management Console 6.0 include:

- **New FIPS 140-2 Validated Encryption**
- **Active Directory Integration to Allow Rapid Deployment of Configured Devices**
- **Deliver files to remote Defender USB drives securely over the internet**
- **User Experience Enhancements: Including More Granular Search, Audit and Reporting Functionality**
- **Intelligent Installer to Prevent Database Conflicts**
- **Built on the Backbone of Kanguru's Common Criteria-Evaluated KRMC Version 5 (in process)**

USB Drive

- Can you trust your USB drive?

Some of the recent enhancements of Kanguru Remote Management Console 6.0 include:

- **New FIPS 140-2 Validated Encryption**
- **Active Directory Integration to Allow Rapid Deployment of Configured Devices**
- **Deliver files to remote Defender □ USB drives securely over the internet**
- **User Experience Enhancements: Including More Granular Search, Audit and Reporting Functionality**
- **Intelligent Installer to Prevent Database Conflicts**
- **Built on the Backbone of Kanguru's Common Criteria-Evaluated KRMC Version 5 (in process)**

Approved

by U.S. Department of
Homeland Security



KANGURU

Defender Elite USB Devices
& Kanguru Remote Management

Forensic Write Blockers



DVD-ROM



Operational Security



OpSec Continued

- Everything must be new.
- No similarities/correlations with meatspace.
- GPG/OTR are your friends.
- Need to know - “three can keep a secret...”

Snail Mail

- Avoid if at all possible.
- If not, try to use abandoned address.
- Otherwise, burner mailboxes are best bet.
- If possible, test the pickup process beforehand.

Fighting Deanononymization Attacks

- Break files into sub-100MB chunks.
- Reboot when changing activities.

How do I help?

- Open source project (code, documentation, etc.)
- Donate!

