

# 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?

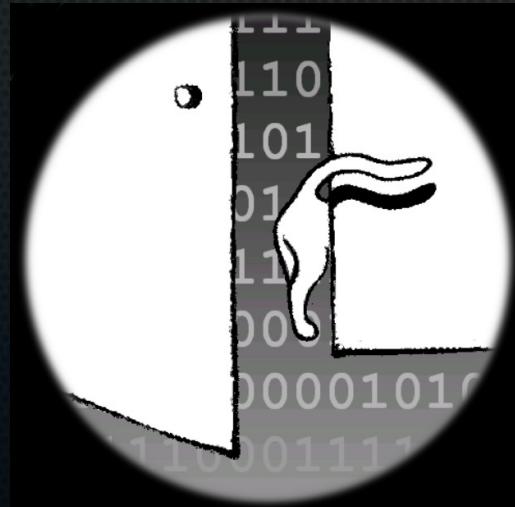
- "...a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity."
- GPL3 licensed.



*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.



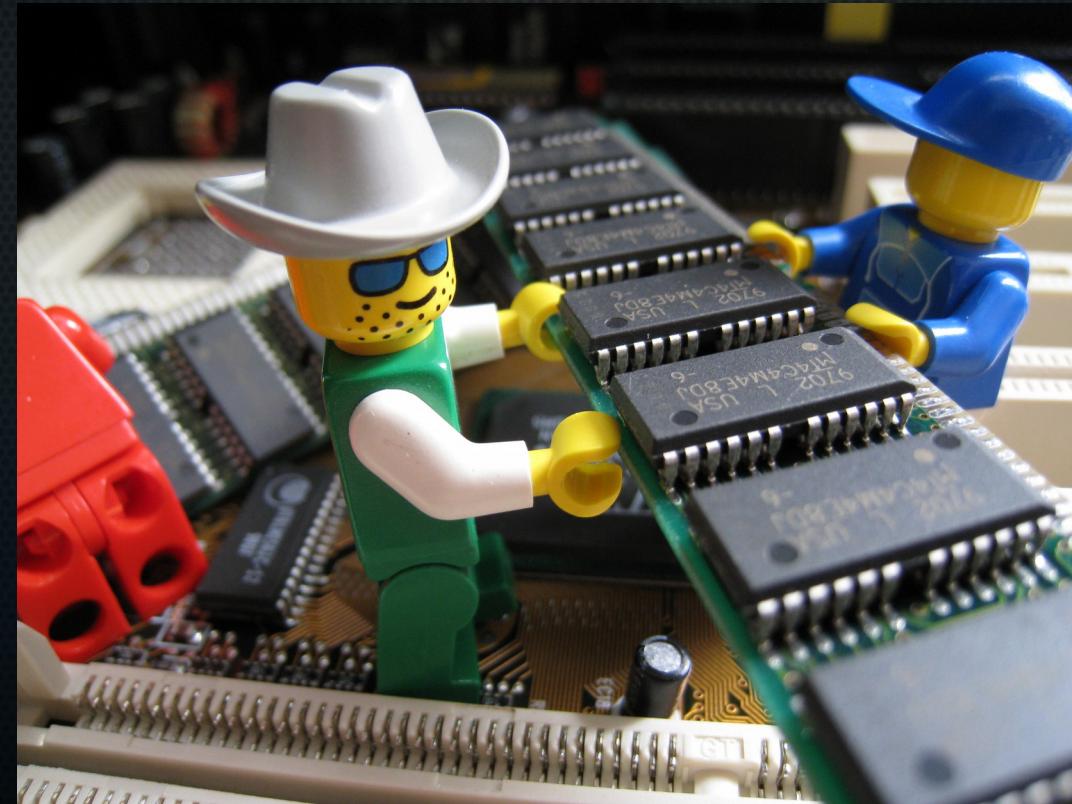
# Is privacy really that important?

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



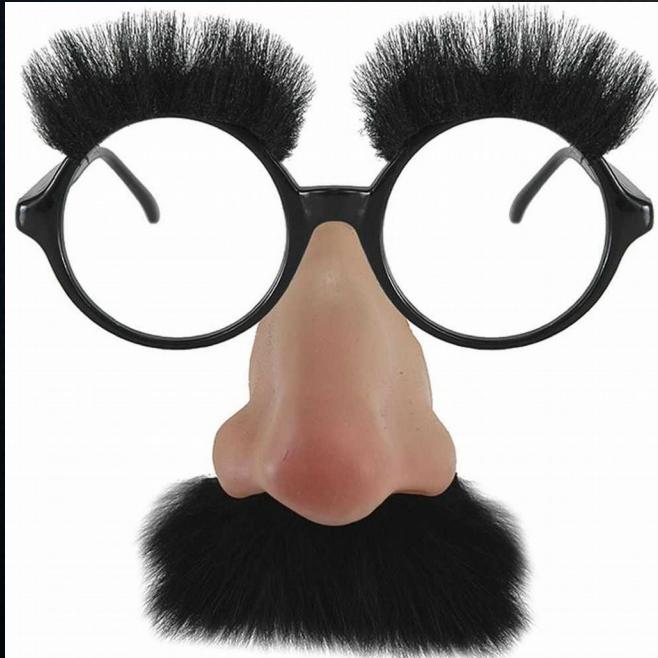
# Amnesic

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

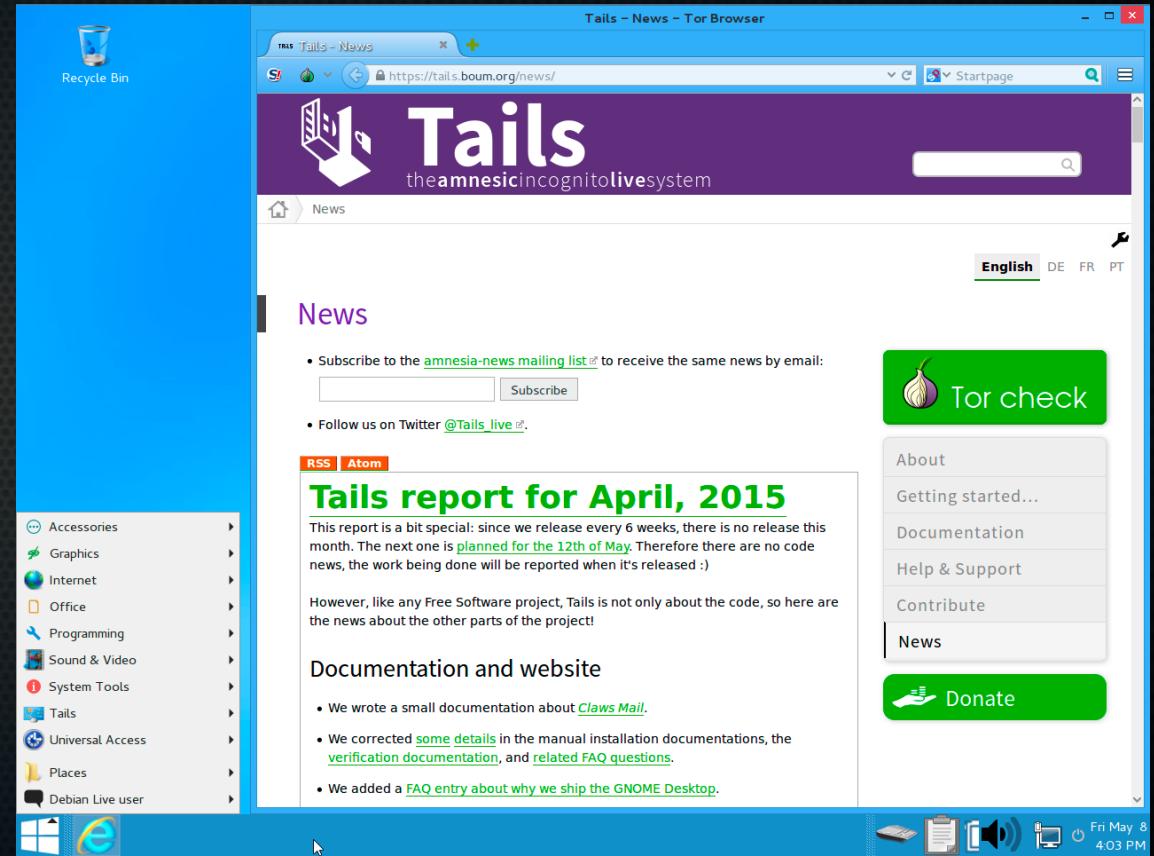
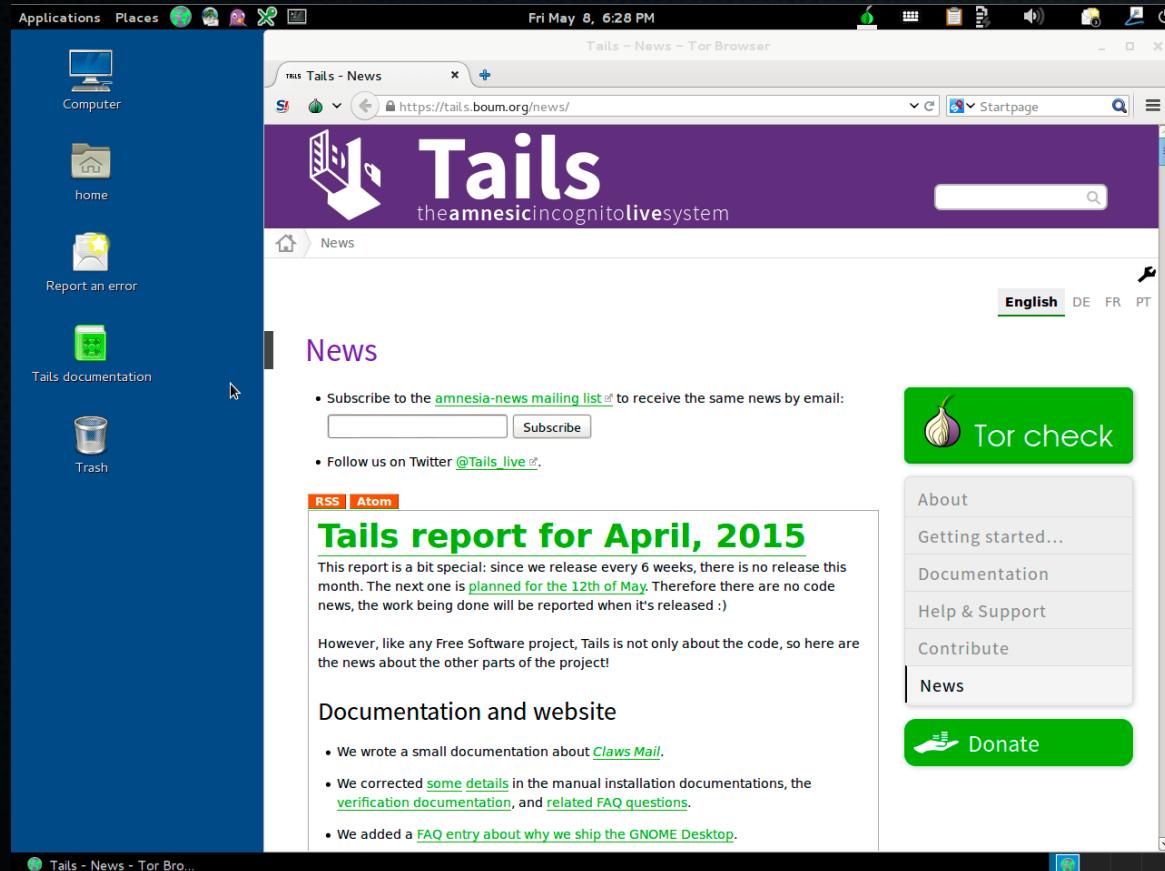


# Incognito

- 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

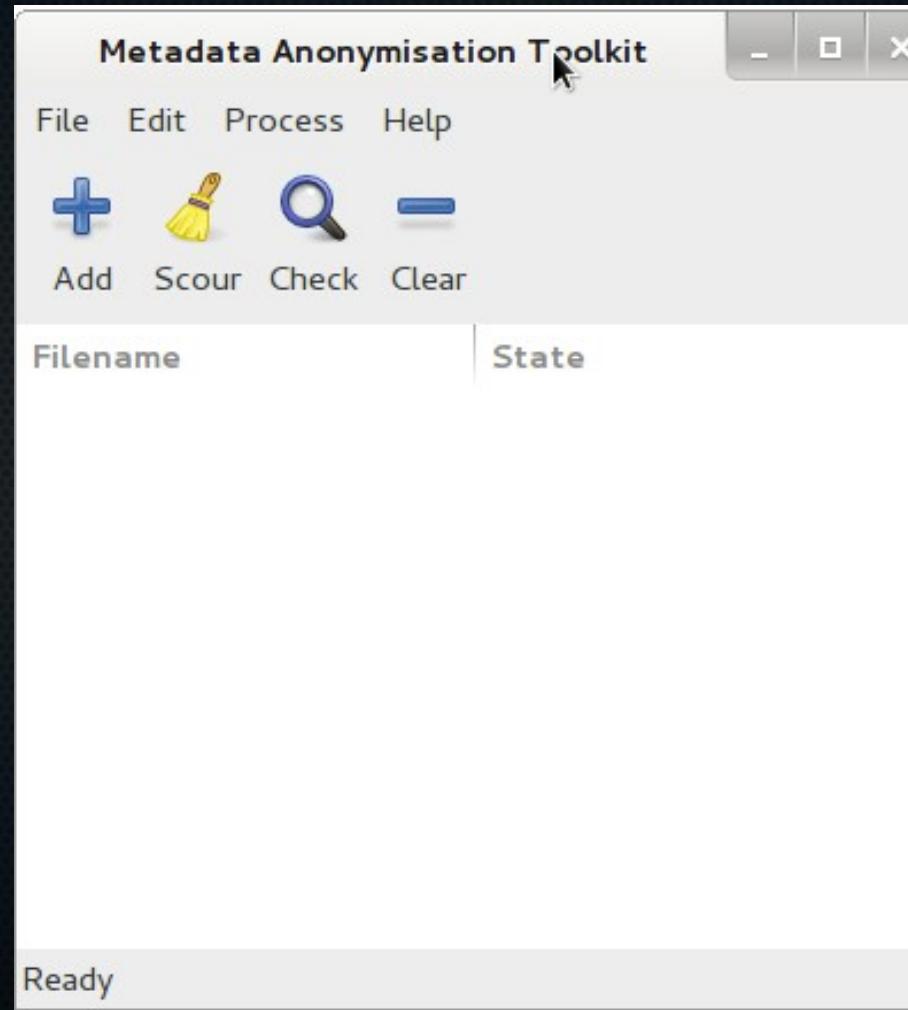
- (Almost) any machine, (almost) anywhere!



# Live System

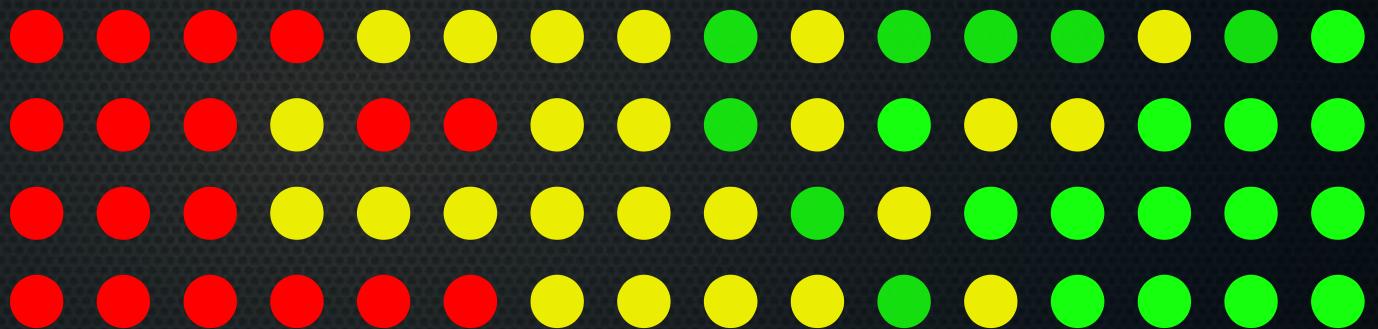
- Web Browser (Tor Browser w/ NoScript)
- Mail Client (CLAWS w/ GPG [Soon to be Icedove])
- Chat Client (Pidgin w/ OTR)
- Bitcoin Wallet (Electrum)
- Password Manager (KeePassX)
- Document Software (LibreOffice)
- Image Software (GIMP & Inkscape)
- Audio Software (Audacity)

# Metadata Anonymisation Toolkit



# I2P Integration

I2P



# Threat Modeling

- Tier I – General privacy, passive tracking & profiling



# Threat Modeling

- Tier II – "Low level" active adversary.



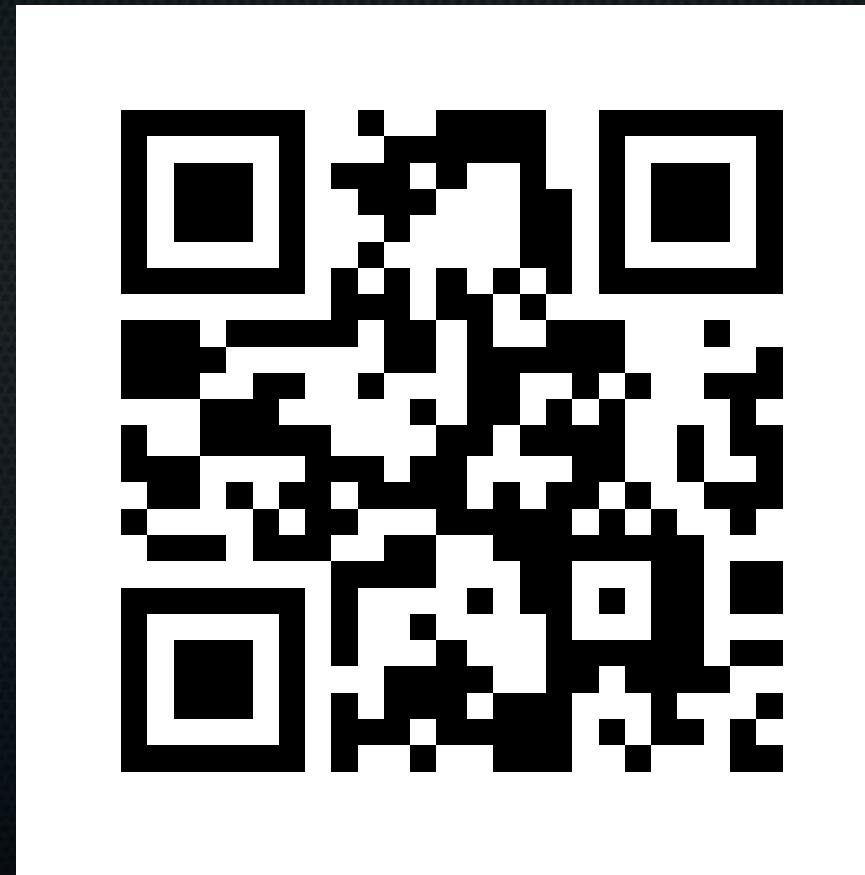
# Threat Modeling

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



# Simple Instructions

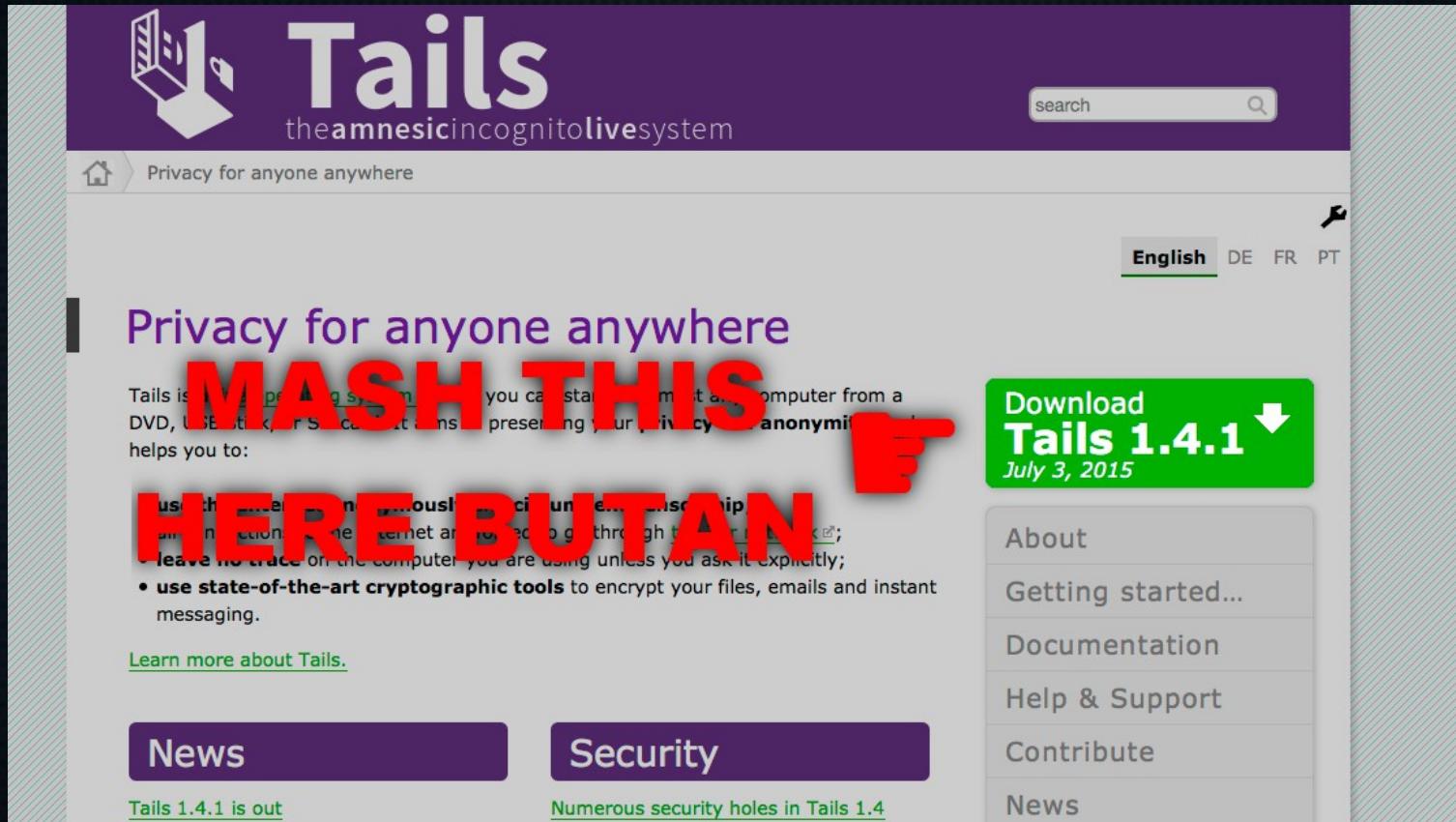
- <https://goo.gl/A6m2si>



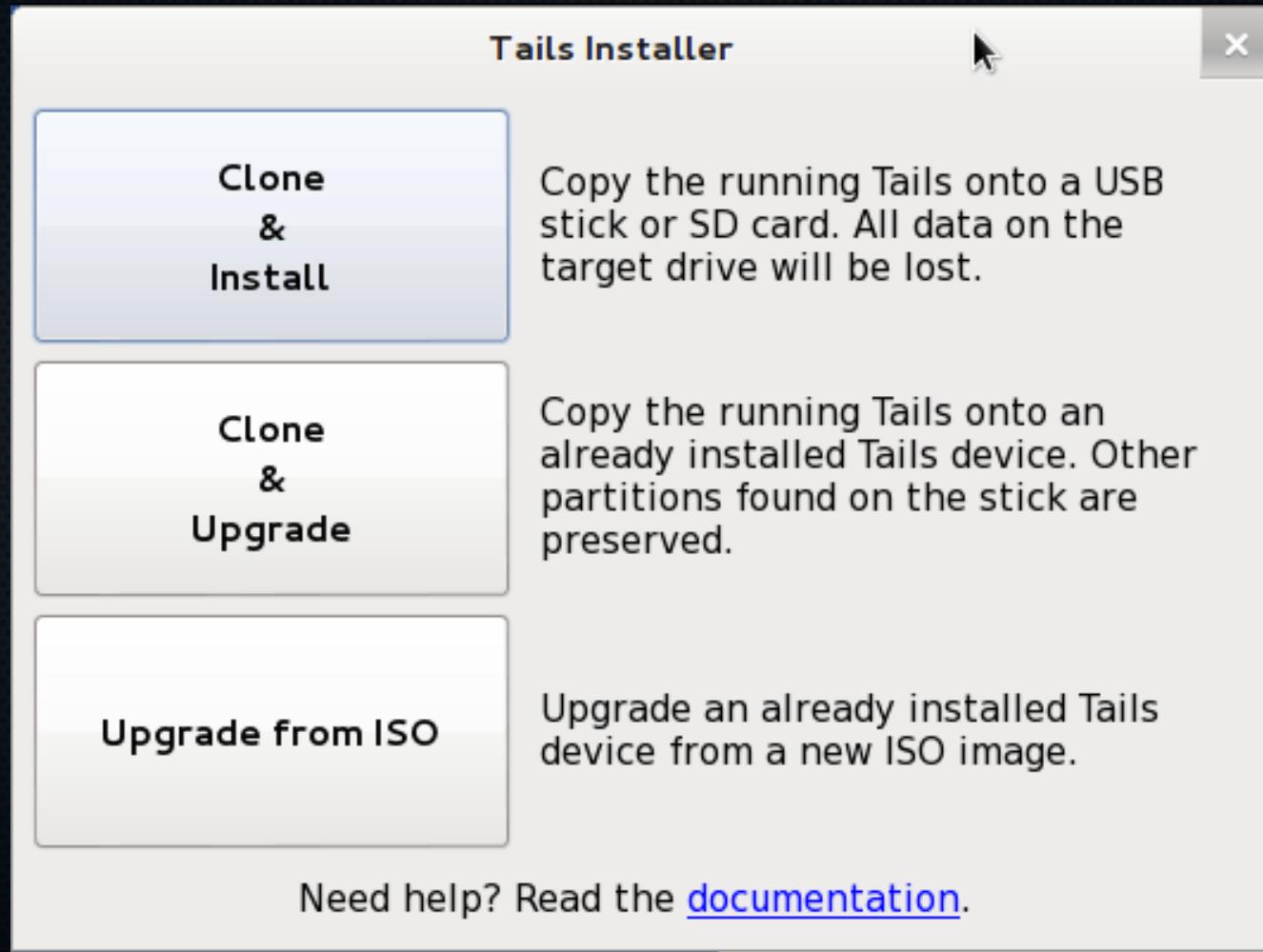
# Obtaining Image

The screenshot shows the official website for Tails, the Amnesic Incognito Live System. The header features the Tails logo (a stylized white figure) and the text "Tails" in large white letters, followed by "the amnesic incognitolive system". A search bar is located in the top right corner. Below the header, a breadcrumb navigation shows "Privacy for anyone anywhere". The main content area has a purple background and features the heading "Privacy for anyone anywhere" in a large, bold, purple font. Below this, a text block explains that Tails is a live operating system that preserves privacy and anonymity. It lists three key features: using the Internet anonymously, leaving no trace, and using cryptographic tools. A green button at the bottom left encourages users to "Download Tails 1.4.1" from July 3, 2015. At the bottom, there are two purple buttons for "News" and "Security", along with links to "Tails 1.4.1 is out" and "Numerous security holes in Tails 1.4". A sidebar on the right contains links for "About", "Getting started...", "Documentation", "Help & Support", "Contribute", and "News". Language selection buttons for English, DE, FR, and PT are also present.

# Obtaining Image



# Tails Installer



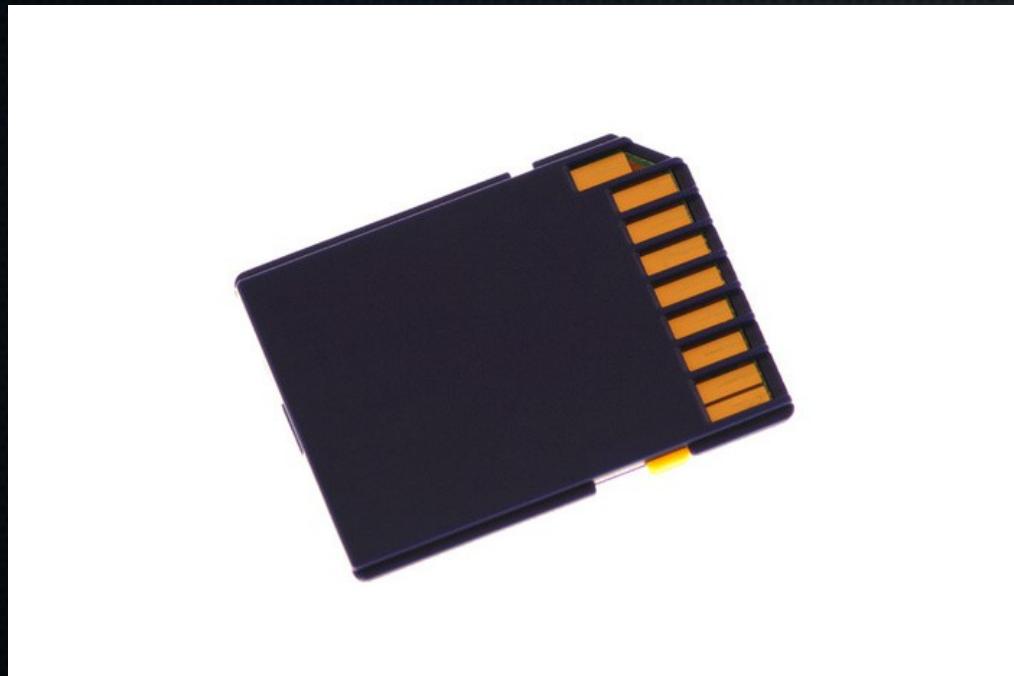
# Persistent Storage

- 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



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 Deanonymization Attacks

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

# How do I help?

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

