Tails
theamnesicincognitolivesystem

TAILS
The **A**mnesic **I**ncognito **L**ive **S**ystem

- Amnesie: Vergessen - hinterläßt keine Spuren auf dem Rechner
- Incognito: Unerkannt - bei Arbeiten am Computer und im Internet mit TOR
- Live System - Datenträger (USB-Stick, DVD) der ein startfähiges vollständiges Betriebssystem enthält.

Anonym surfen mit TOR

- WIKIPEDIA-Video

  u.a. gefördert von:
- ROSA LUXEMBURG-Stiftung
- HEINRICH-BÖLL-Stiftung
- https://de.wikipedia.org/wiki/Anonymität_im_Internet#Anonymizer

IP-ADRESSEN

- Die IP (Internet-Protokoll)-Adresse wird bei jeder Netzaktivität wie eine Briefadresse d.h. Absenderangabe standardmäßig mitgeschickt.

- Ohne TOR ist Surfen, Chatten oder Mailen mit der Identität und Lokalität des Routers nachvollziehbar verknüpft.

Im Jahr

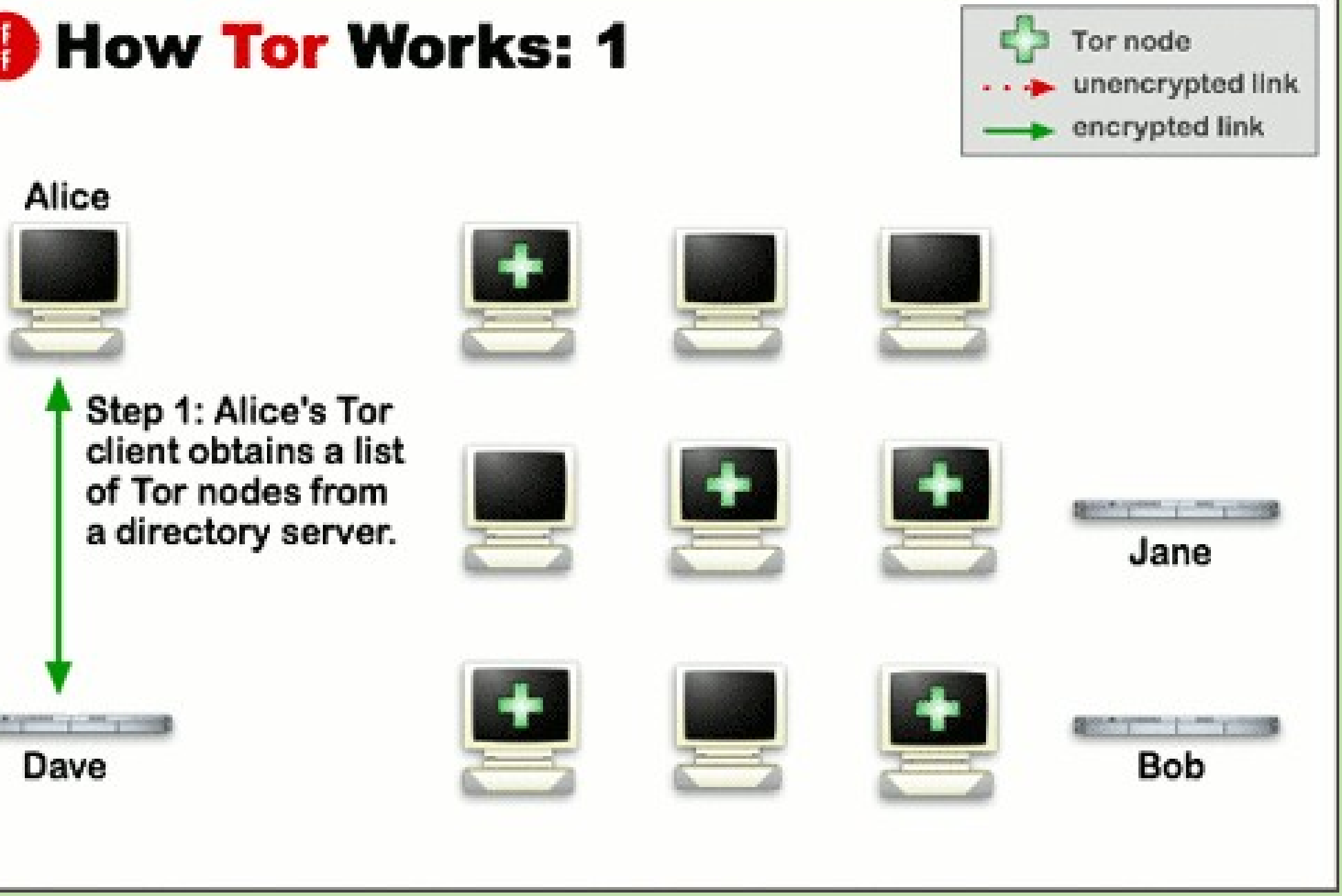
2023

verbanden sich täglich mehr als

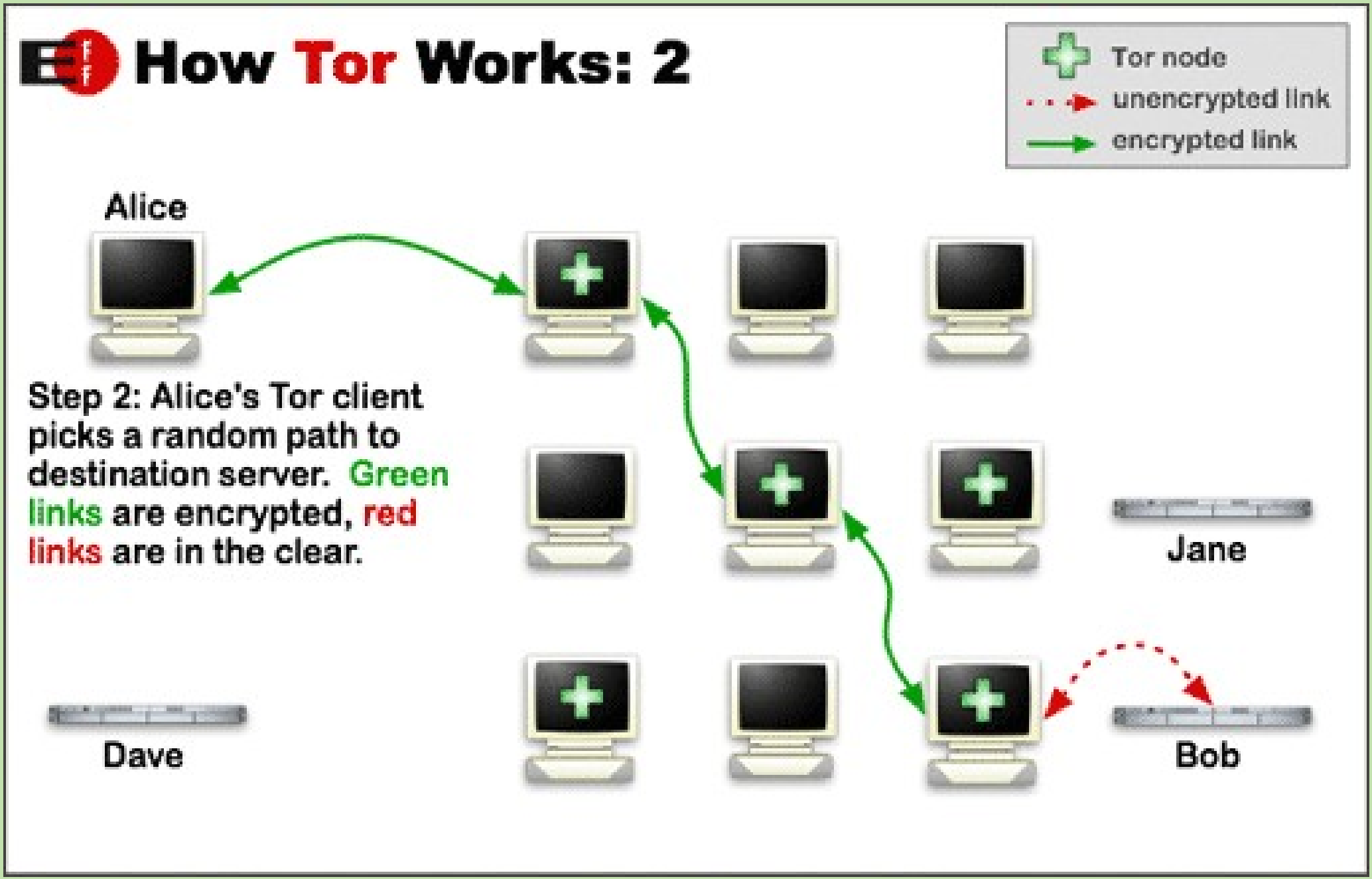
4 000 000

Nutzer mit Tor.

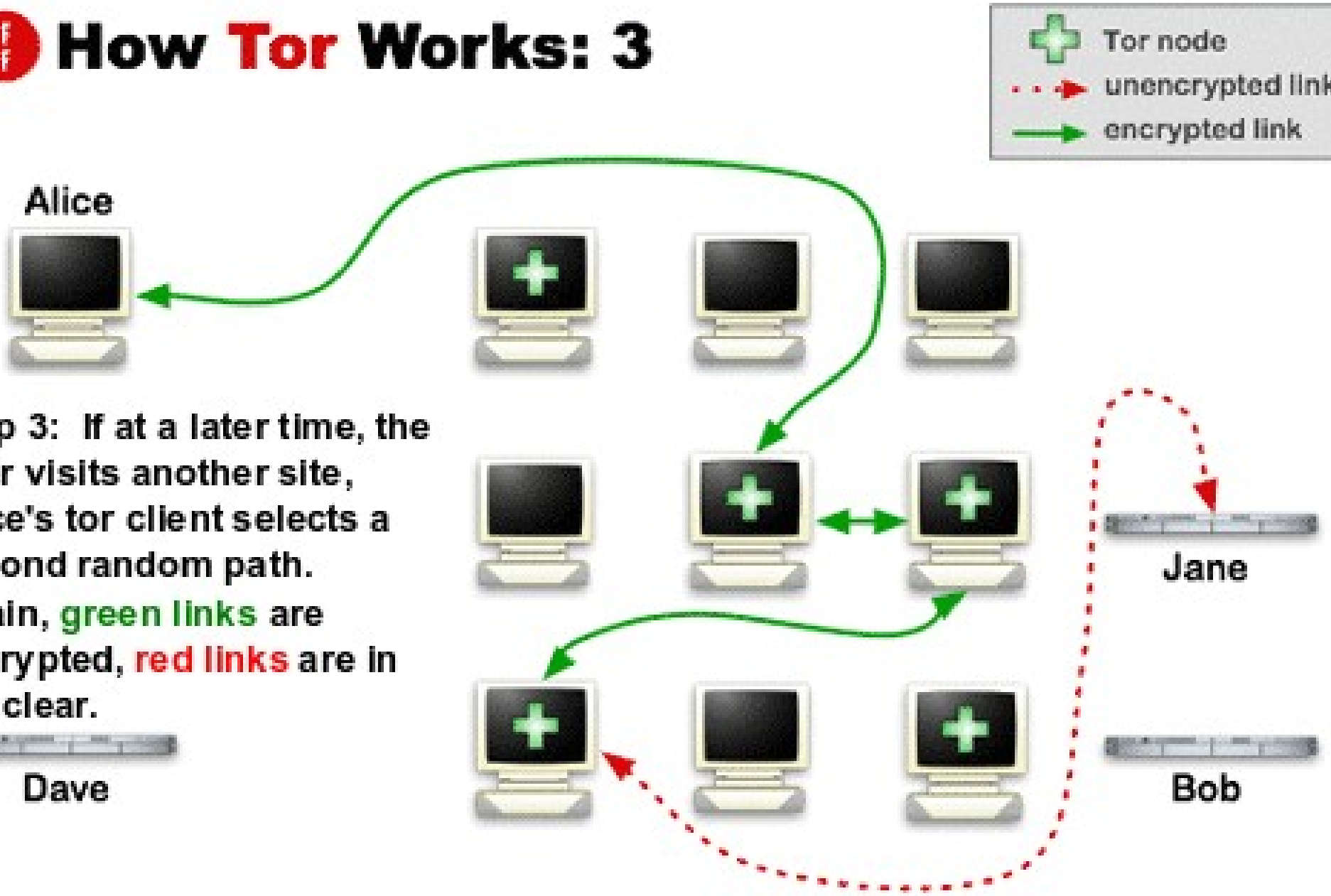
How Tor Works: 1



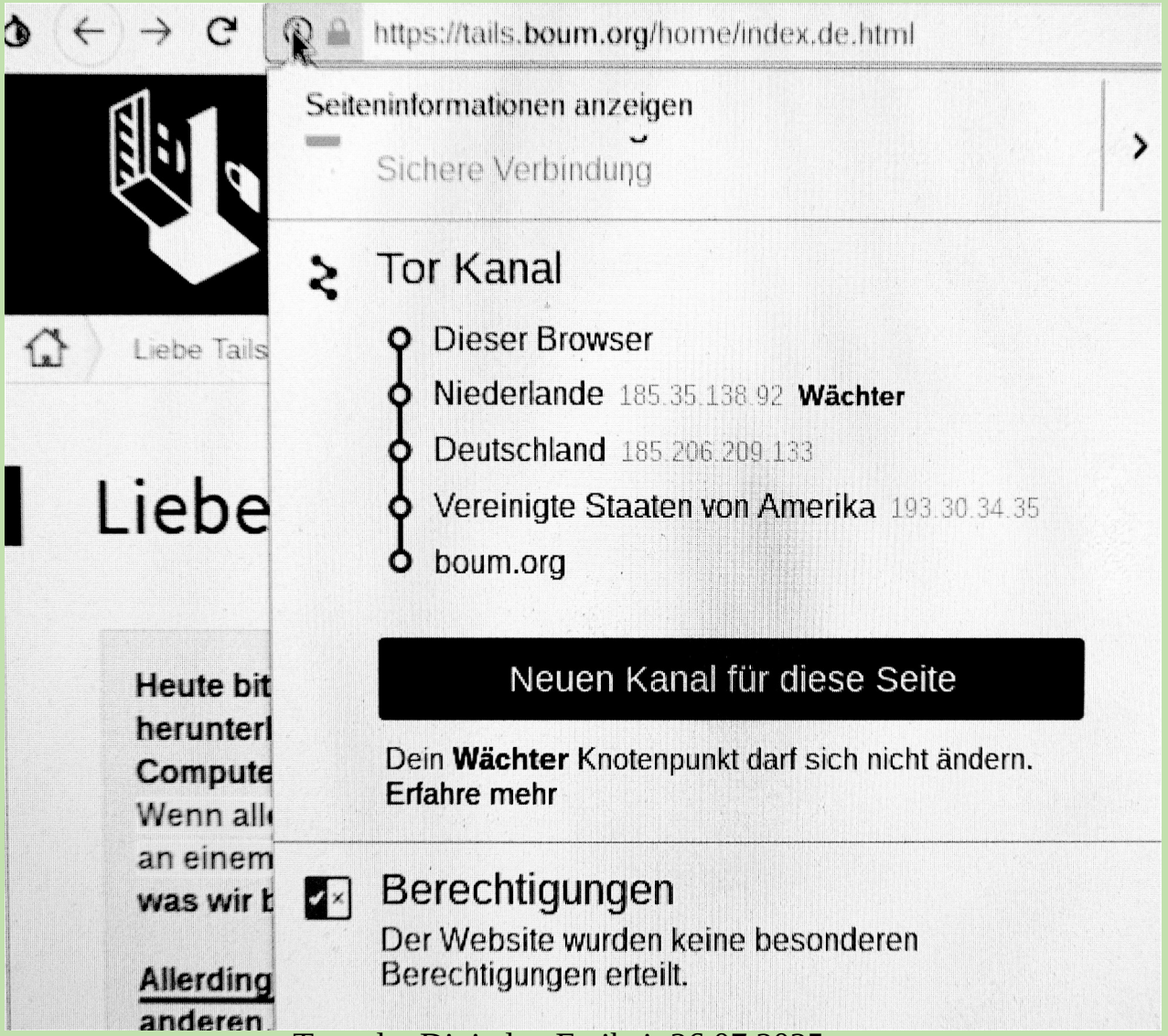
How Tor Works: 2



How Tor Works: 3



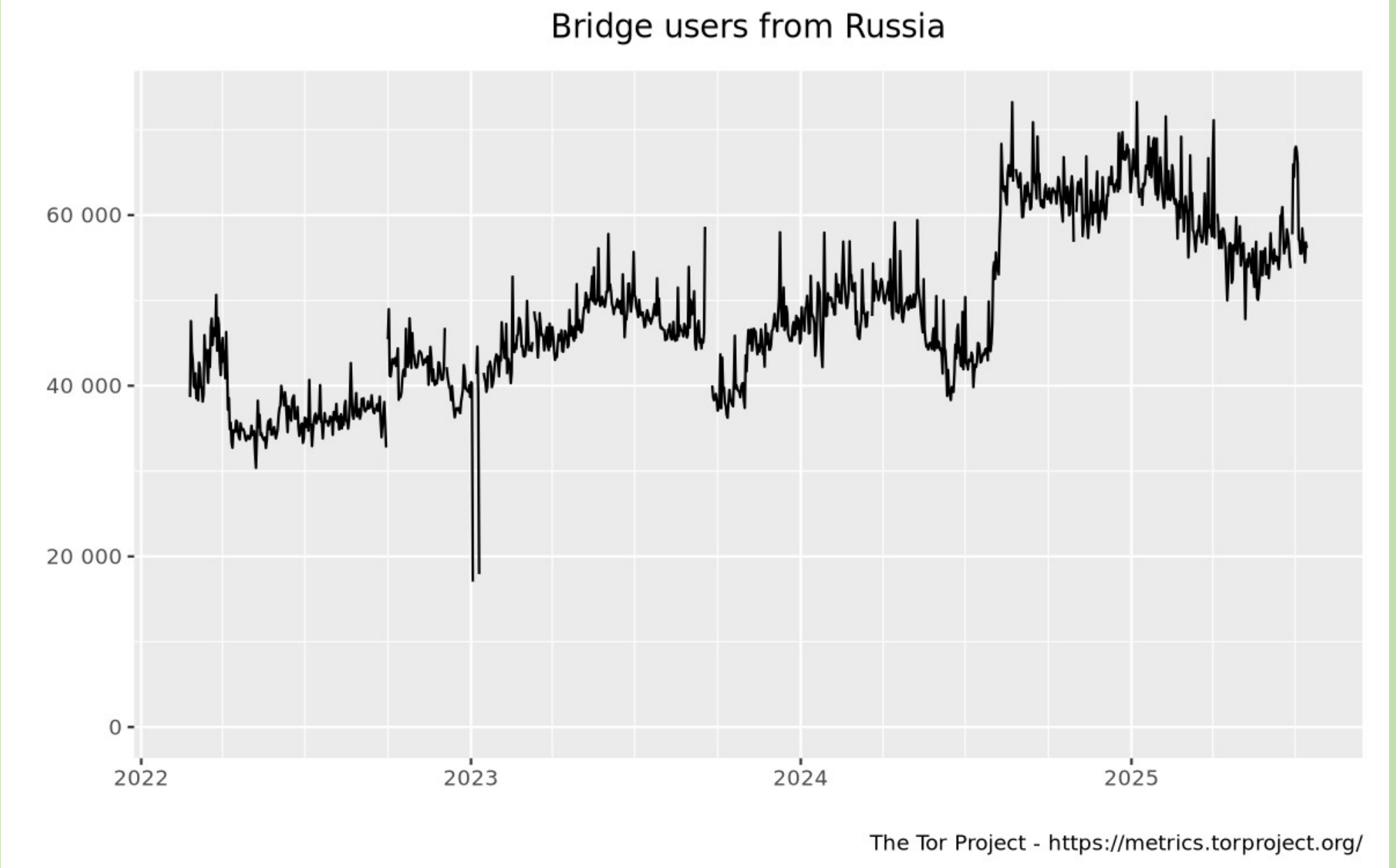
TOR-Kanal:
3 von 8700 TOR-Knoten



Ca.1800 Tor Bridges (nicht-öffentlich bekannte Entry-Nodes) sind gegen Zensurmaßnahmen bzw. Überwachung verfügbar

Country	Durchschnitt täglicher Brücken-Nutzer in den letzen 3 Monaten
Russia	55972 (43.91 %)
United States	11582 (9.09 %)
Iran	10882 (8.54 %)
Germany	4845 (3.80 %)
Turkmenistan	4321 (3.39 %)
Netherlands	3184 (2.50 %)
United Kingdom	2936 (2.30 %)
France	2111 (1.66 %)
China	1934 (1.52 %)
India	1542 (1.21 %)

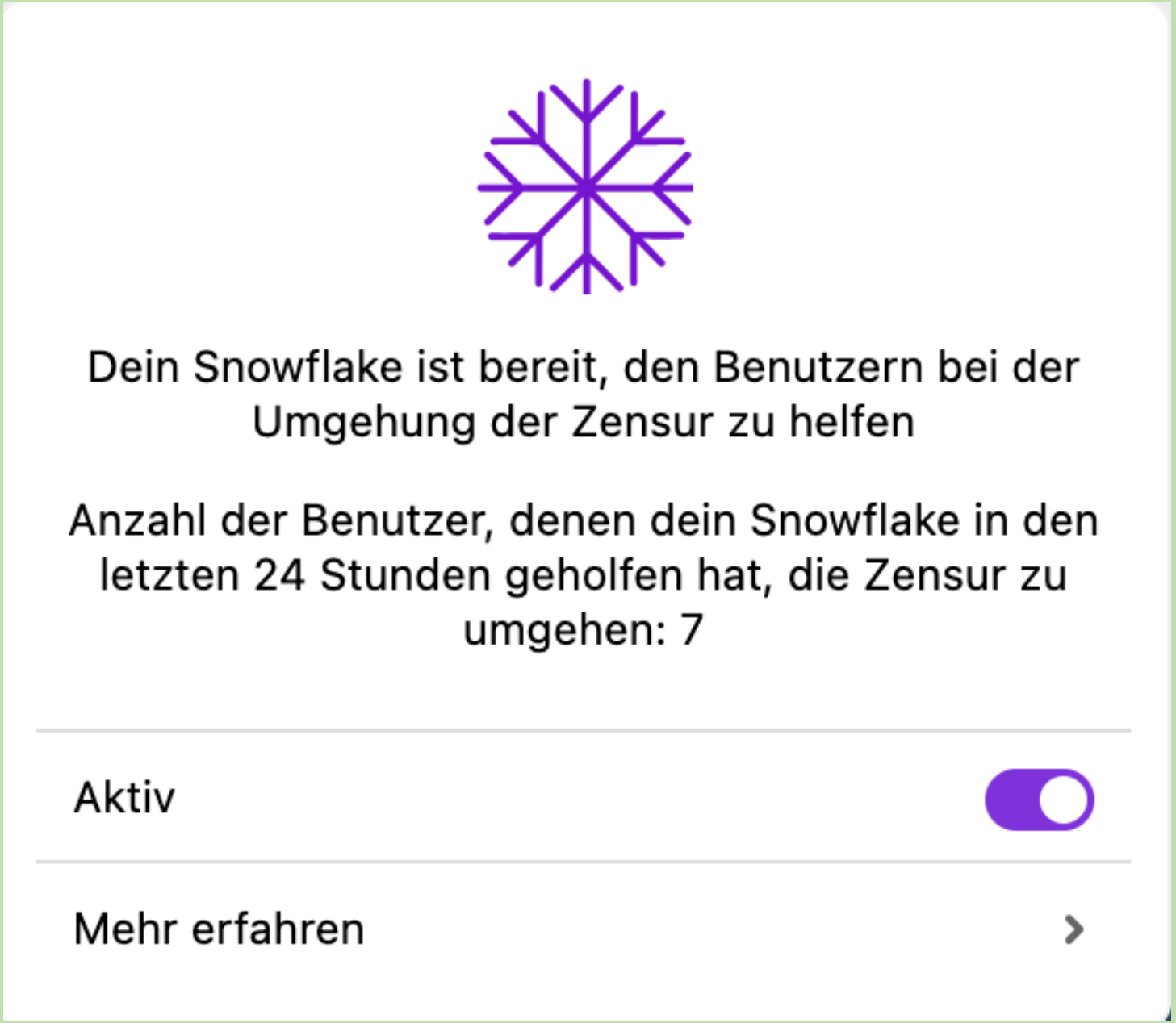
Anstieg der TOR-Nutzung seit dem Angriff auf die Ukraine



Mit dem **Snowflake**-Addon für Firefox

(12.000 Installationen) als nichtöffentliche Eingangsknoten helfen wir Menschen in Ländern mit Zensur voll auf das Internet zuzugreifen.
Voraussetzung für Installation: Internet bei uns nicht bereits stark zensiert.
Unbedenklich: Sichtbare IP-Adresse wird die des Tor-Ausgangsknotens sein, nicht unsere (da wir Eingangs-punkte sind).

Direkt in den TOR-Einstellungen können in zensierten Ländern die Snowflake-Brücken aktiviert werden.


Dein Snowflake ist bereit, den Benutzern bei der Umgehung der Zensur zu helfen
Anzahl der Benutzer, denen dein Snowflake in den letzten 24 Stunden geholfen hat, die Zensur zu umgehen: 7
Aktiv
Mehr erfahren

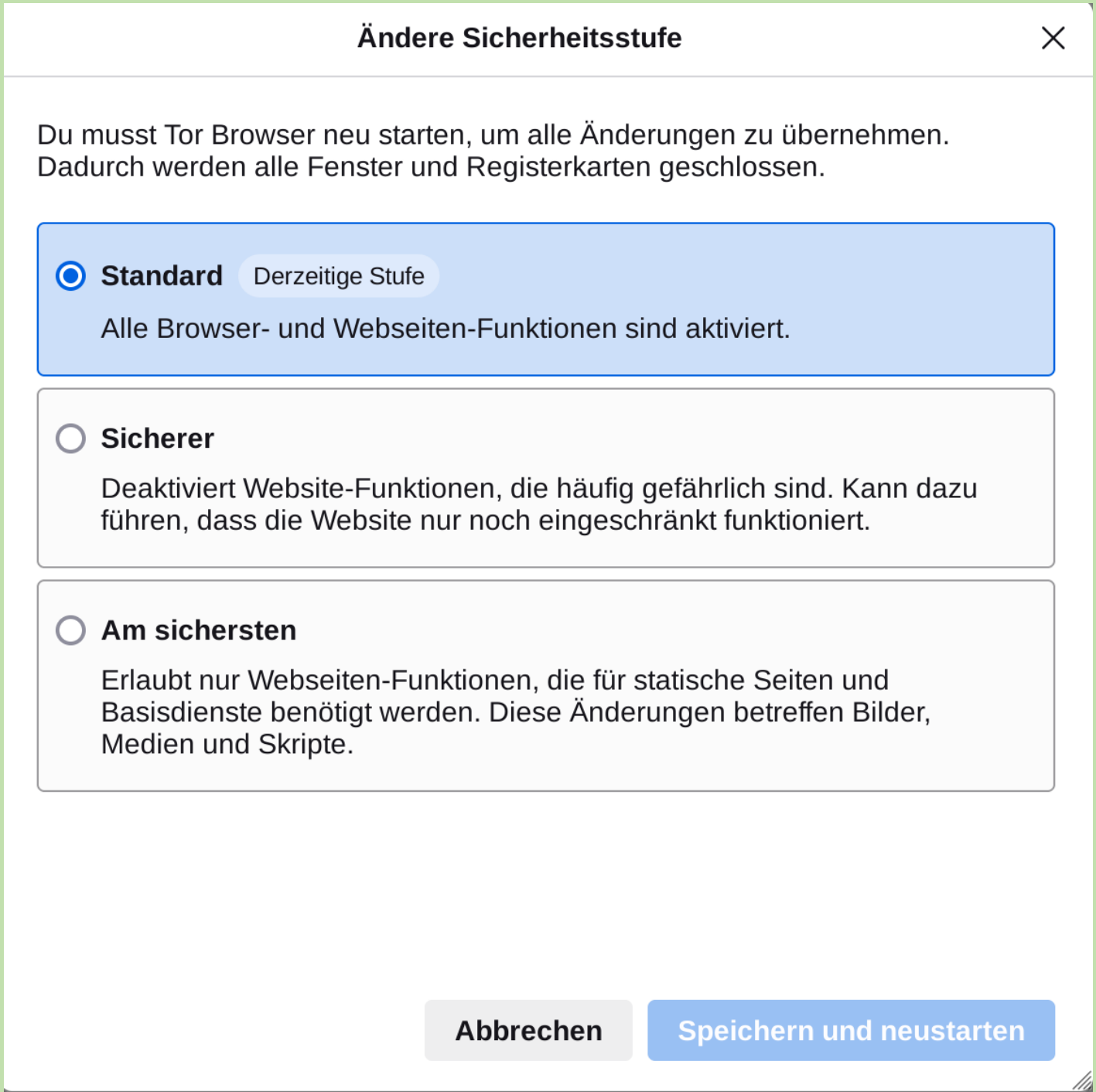
„Unsichtbar“ durch Veränderung der MAC-Adresse

- Netzwerkschnittstellen wie WLAN-Karte oder kabelgebundenes LAN melden sich mit eindeutiger MAC-Adresse (Media-Access-Control) z.B. B4:89:91:C1:F4:CE beim Router an. Fremde Router können das protokollieren
- TAILS ändert die MAC-Adresse bei jedem Start
- > Kein Zugang bei Router-Einstellung mit beschränkender Liste von erlaubten MAC-Adressen!

TOR-Nutzung

- Verschleierung der Identität unterschieden von Verschlüsselung der Verbindung
- Sinnhaftigkeit von End-to-End-Verschlüsselung
- Trennung von personalisierter Nutzung: Bank ... und anonymer Recherche im Netz
- Nutzung anonymes E-Mail-Konto
- Sicherheitsstufen in TAILS > Administrator-Kennwort
- Firefox-Add-Ons: NoScript HTTPS-Everywhere

Sicherheit abgestuft



TAILS-Benutzer

- Journalisten und Whistleblower benutzen TAILS, um Fehlverhalten von Regierungen und Konzernen aufzudecken.
- Menschenrechtsorganisationen benutzen TAILS, um sich vor Zensur zu schützen und Menschenrechtsverletzungen aufzudecken.
- Überlebende von häuslicher Gewalt benutzen TAILS, um der Überwachung im eigenen Zuhause zu entkommen.
- Bürger, die sich um ihre Privatsphäre sorgen benutzen TAILS, um ein Tracking ihrer Aktivitäten im Internet zu verhindern.

Wie kommt man an TAILS?

- TAILS-Clone von vertrauenswürdiger Person auf USB-Stick (oder auf DVD)

  oder

- Download von der Website
- https://tails.boum.org/install/download/index.de.html
- Verifizieren der Integrität und Authentizität

TAILS-Verifizierung

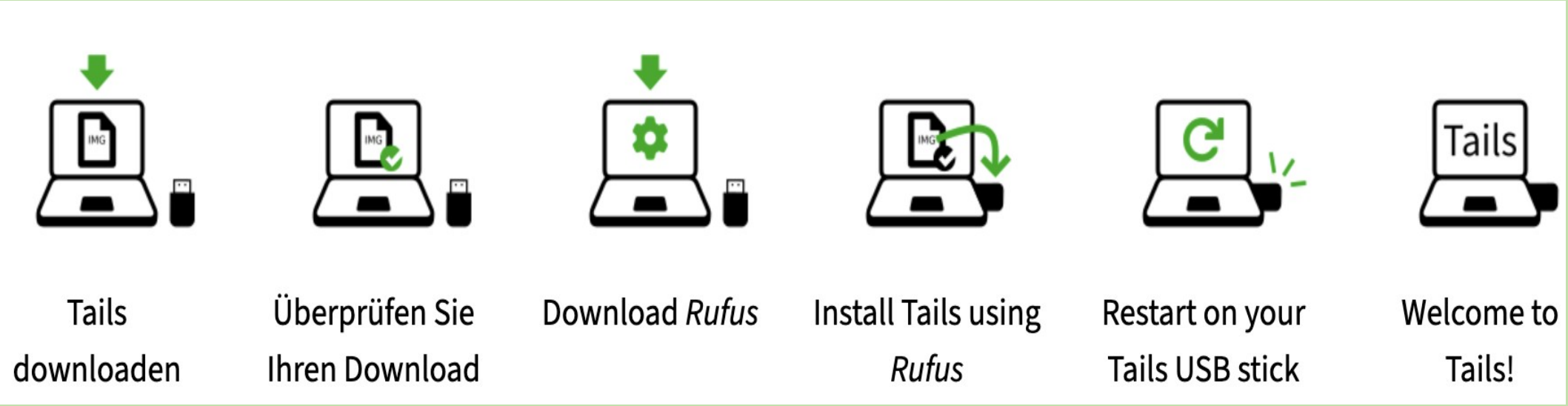
2/3 Überprüfen Sie Ihren Download

Überprüfen Sie Ihren Download, um sicherzustellen, dass er sicher ist und während des Downloads nicht beschädigt wurde.

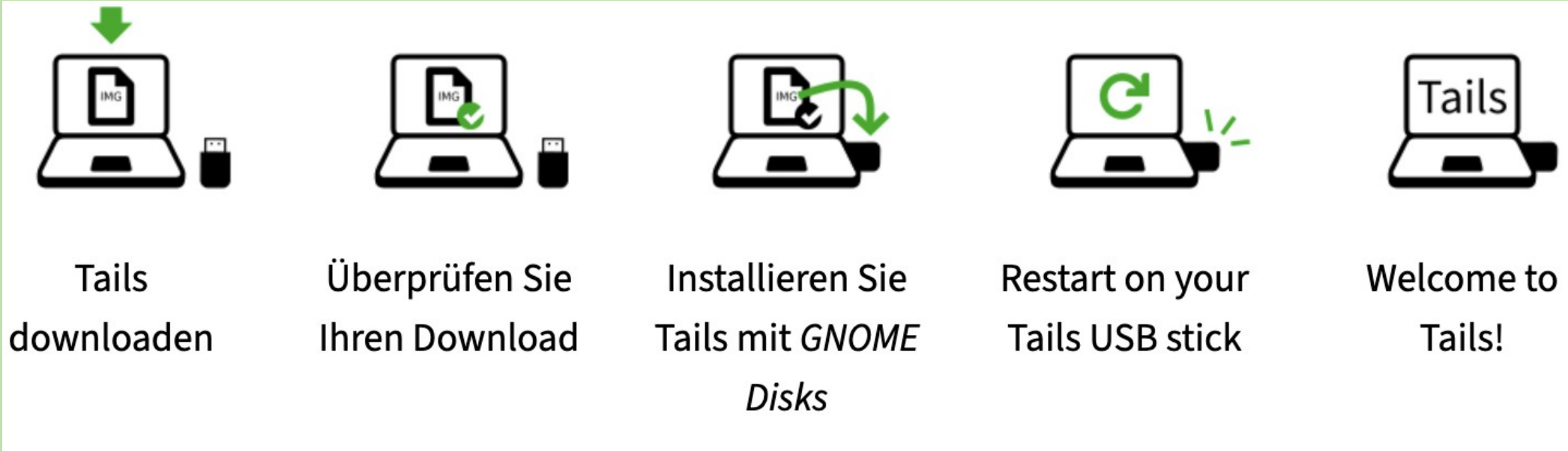
Select your download to verify…

oder verifizieren Sie mit der OpenPGP-Signatur

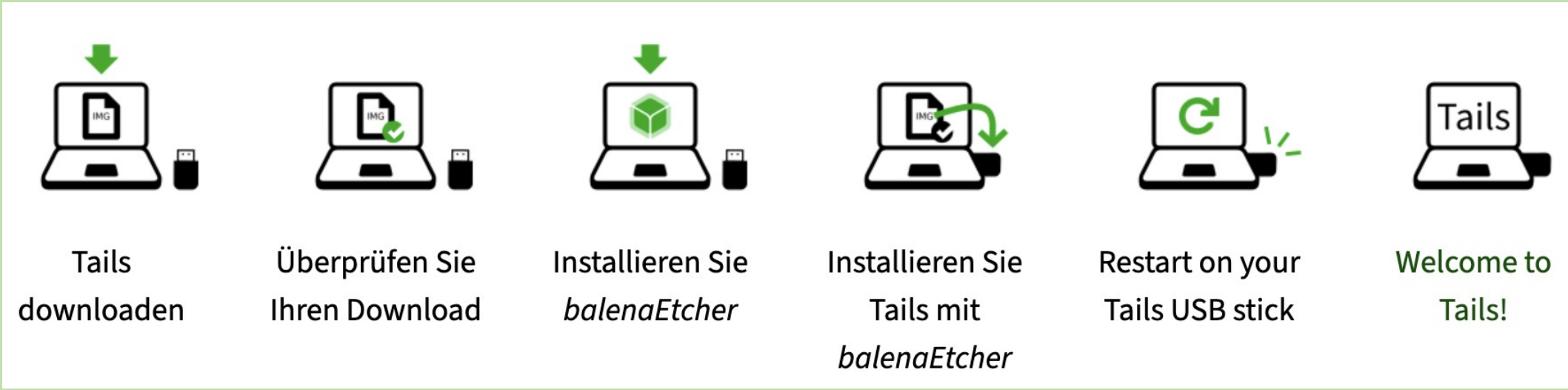
TAILS-Installation mittels Windows-Rechner



TAILS-Installation mittels LINUX-Rechner



TAILS-Installation mittels Apple-Rechner



Zügige Installation

DOWNLOAD der TAILS Version 6.17 am 15. Juli: 5 min

Aktualisierung eines eingerichteten TAILS-USB-Sticks: 3 min

FLASHEN eines leeren USB-Sticks mit Balena-Etcher: 3 min

STARTEN VON TAILS

Vom USB-Stick starten (=„booten“)

Datenträger einlegen/einstecken, dann Computer einschalten

Rechtzeitig Rechner-spezifische Taste (s.u.*) gedrückt halten um

„Boot-Reihenfolge“ im sogenannten BIOS dem Basis-Betriebssystem (Basic-Input-Output) zu ändern

Rechner-spezifischer BIOS-Zugang

> Beim Start eine dieser Tasten drücken:

Acer:	Esc, F12, F9
Asus:	Esc, F8
Dell:	F12
Fujitsu:	F12, Esc
HP:	Esc, F9
Lenovo:	F12, Novo, F8, F10, Return
Samsung:	Esc, F12, F2
Sony:	F11, Esc, F10
Toshiba:	F12
Apple:	option
Andere:	F1, F2, DEL, ESC, F10 oder F12

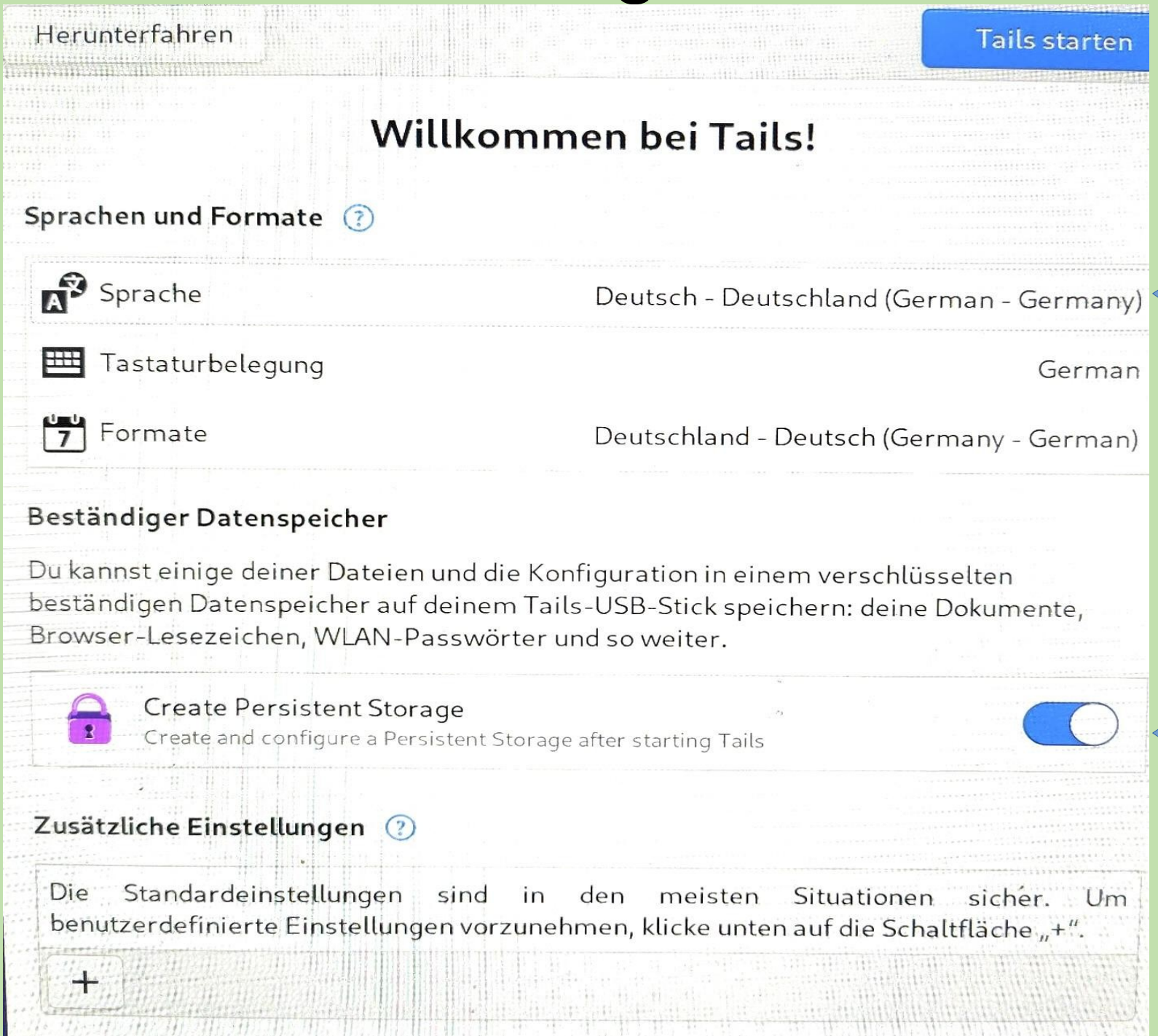
Boot-Vorgang abschließen

Mit „Edit Boot Order“ Boot-Reihenfolge ändern:

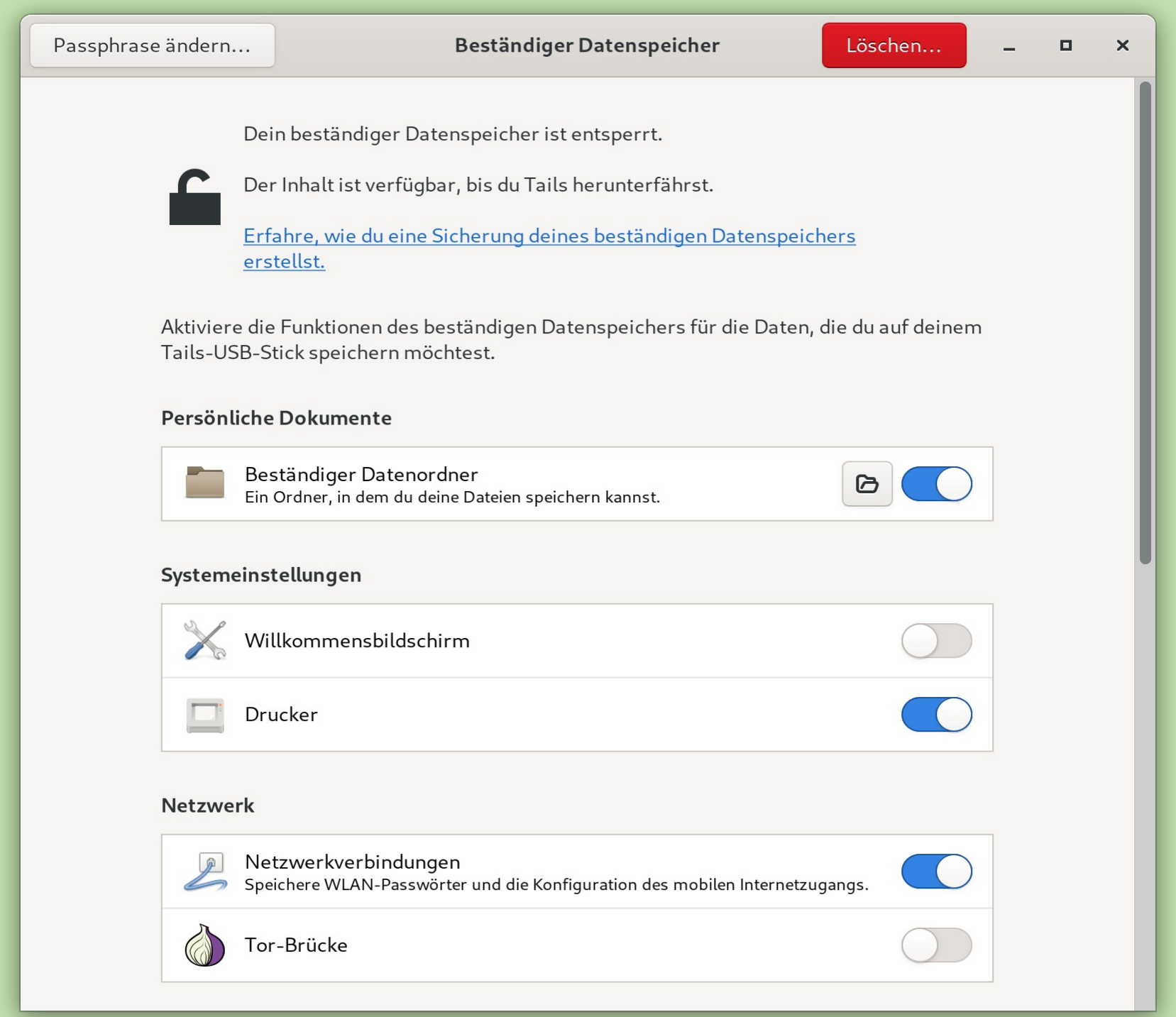
„removable drive“, „external USB disk“ oder „USB media“ an Listenanfang vor „HD“ oder „harddisk“ setzen.

„Save changes and exit“ sichert und fährt fort

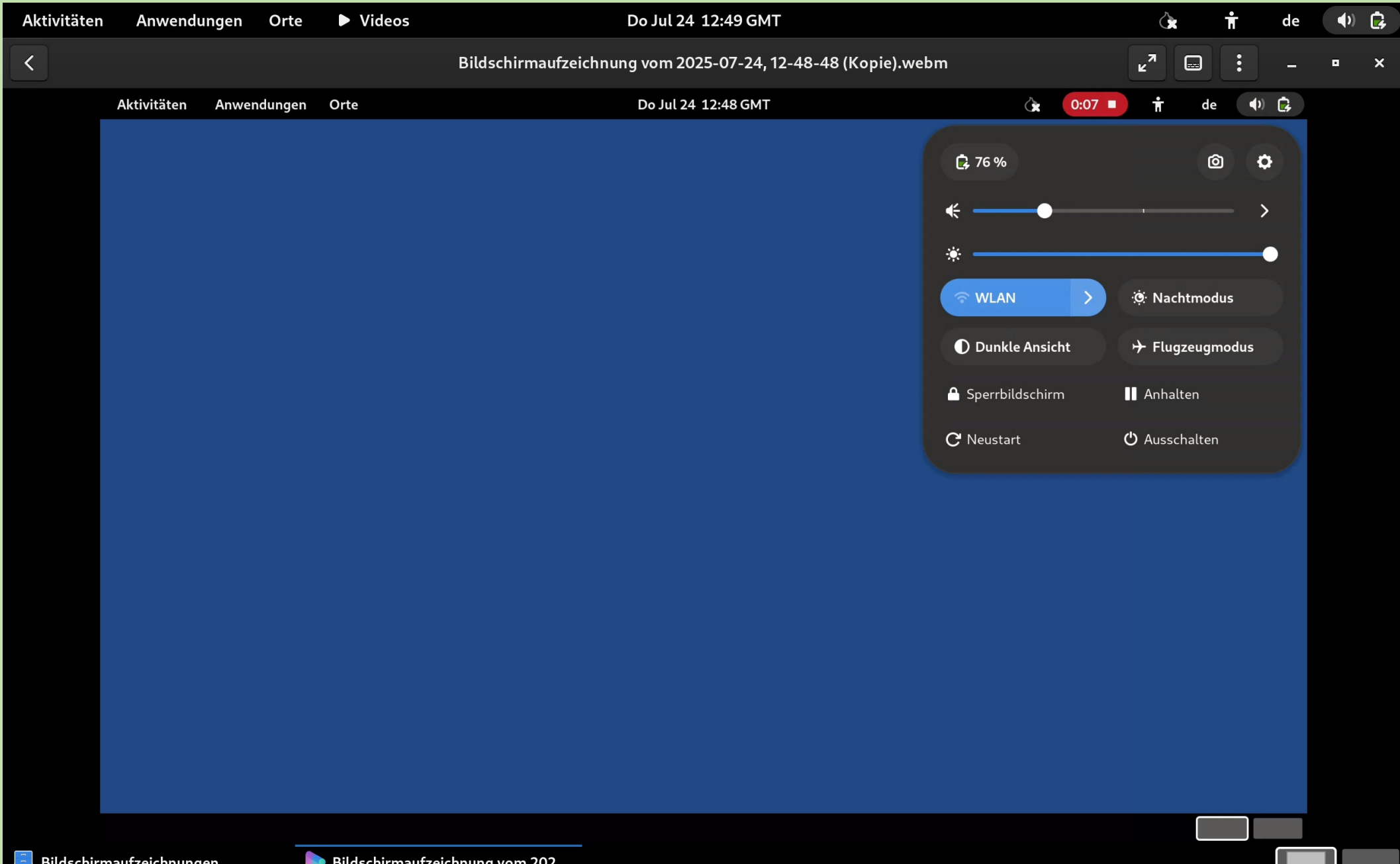
TAILS konfigurieren



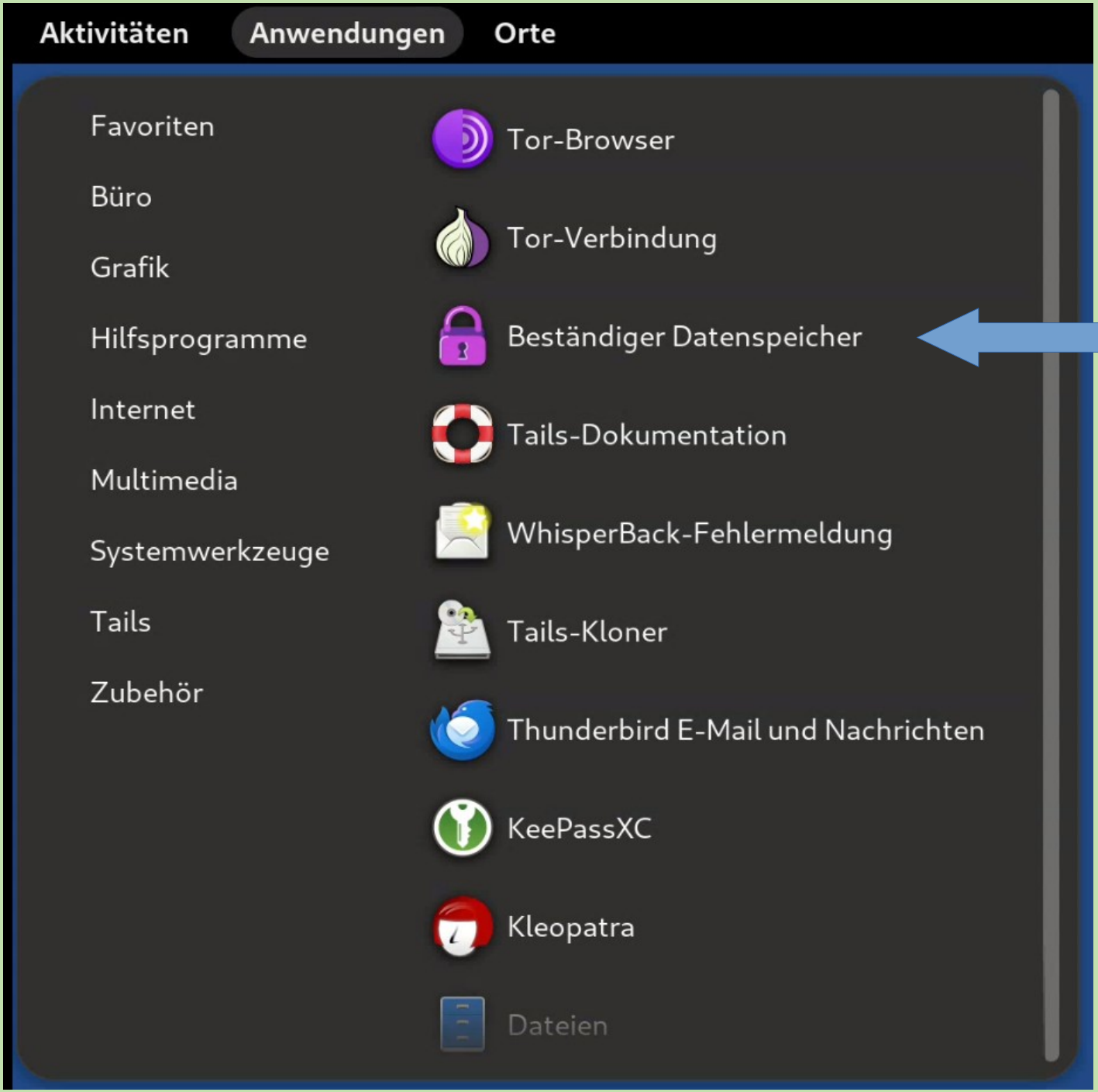
„PERSISTENT“ EINRICHTEN



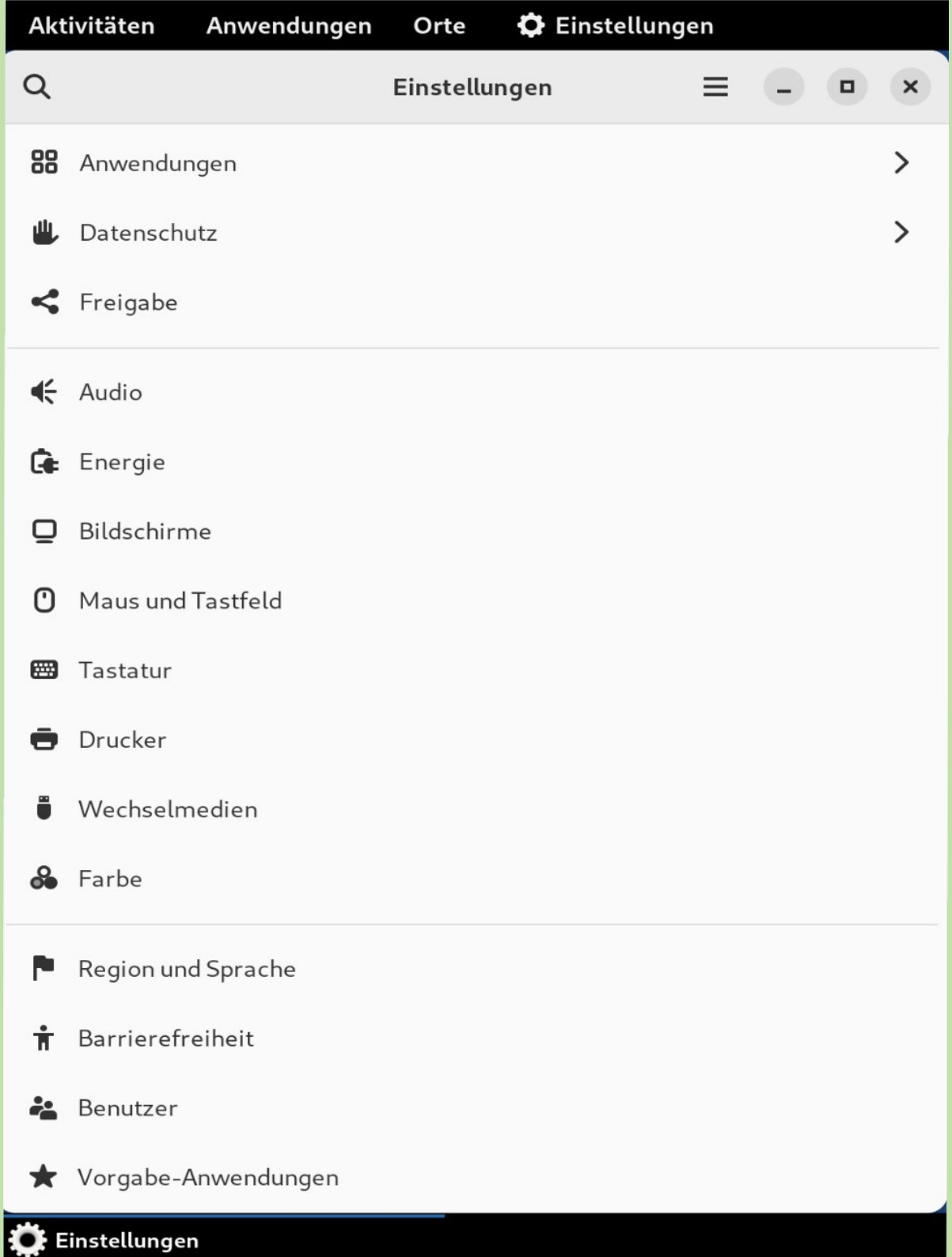
WLAN EINRICHTEN



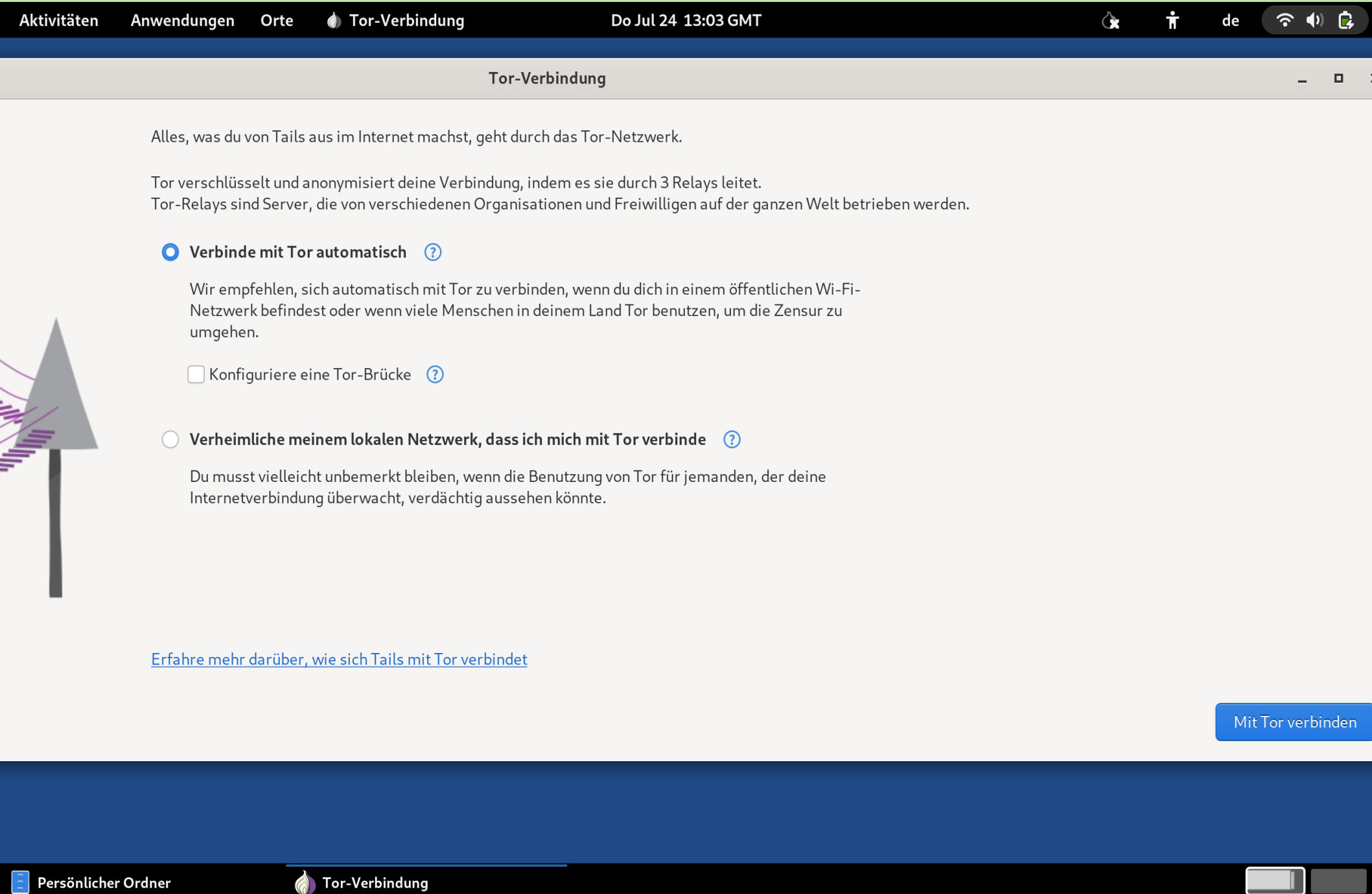
Übersichtliche Programm-Kategorien



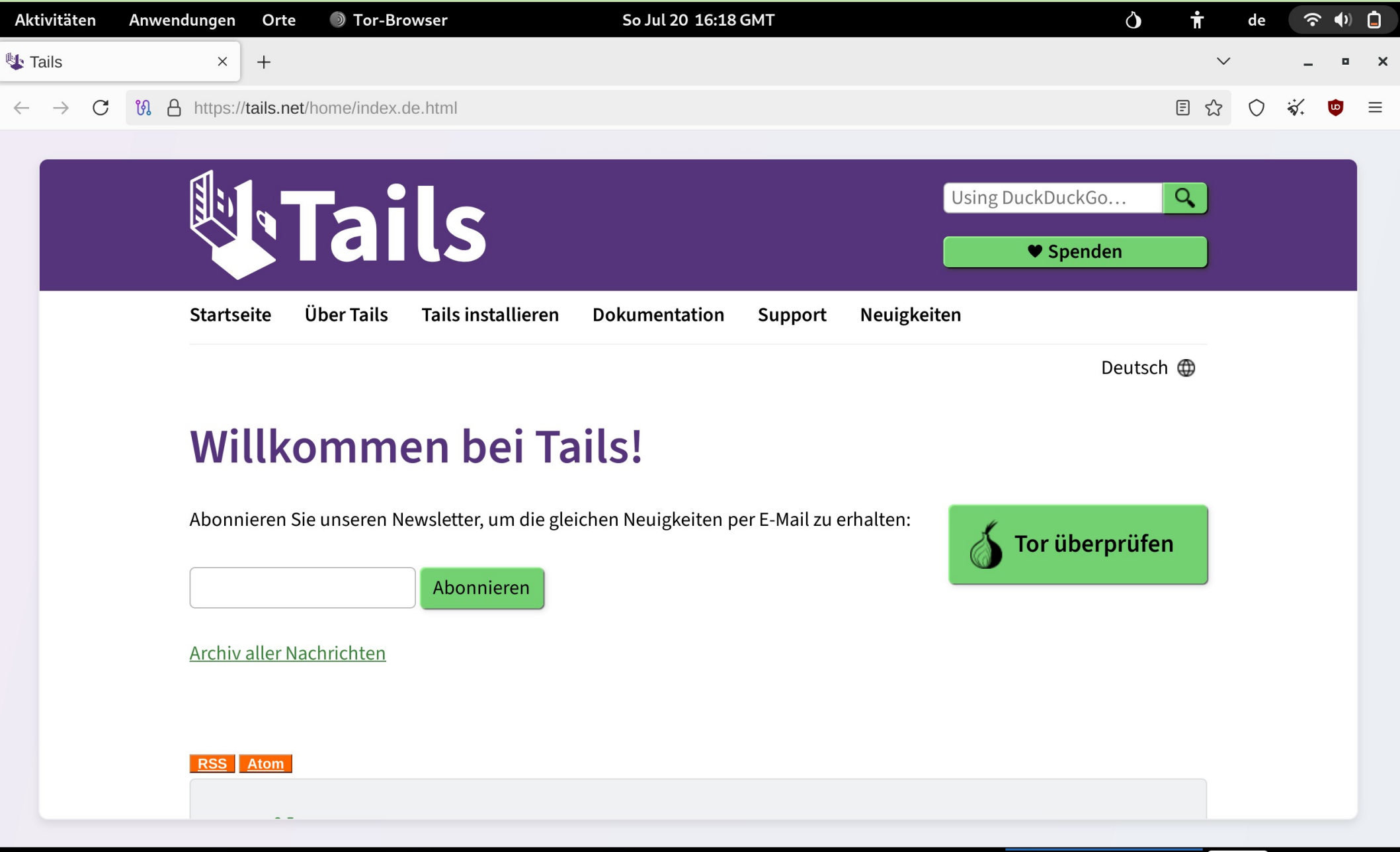
Programm-und Arbeitsbildschirm-Überblick


Aktivitäten
Anwendungen
Orte
Einstellungen
Einstellungen
Anwendungen
Datenschutz
Freigabe
Audio
Energie
Bildschirme
Maus und Tastfeld
Tastatur
Drucker
Wechselmedien
Farbe
Region und Sprache
Barrierefreiheit
Benutzer
Vorgabe-Anwendungen
Einstellungen

TOR-Verbindung herstellen



TAILS-Website
nach Start des TOR-Browsers



Wenn Tails startet, ist die Zeitzone des Systems auf GMT (Greenwich Mean Time) eingestellt.

> Schutz der Anonymität!

Wenn eine Anwendung die tatsächliche Zeitzone preis-gibt, könnte dies helfen, den Nutzer zu identifizieren.

TAILS-(Sicherheits)-Updates

- Sind essentiell!
- Werden alle 1-2 Monate erstellt
- Werden beim 1. Öffnen des Tor-Browsers auf der TAILS-Website automatisch angeboten
- Umfassen alle Systembestandteile und Programme von Linux (Debian) und TOR

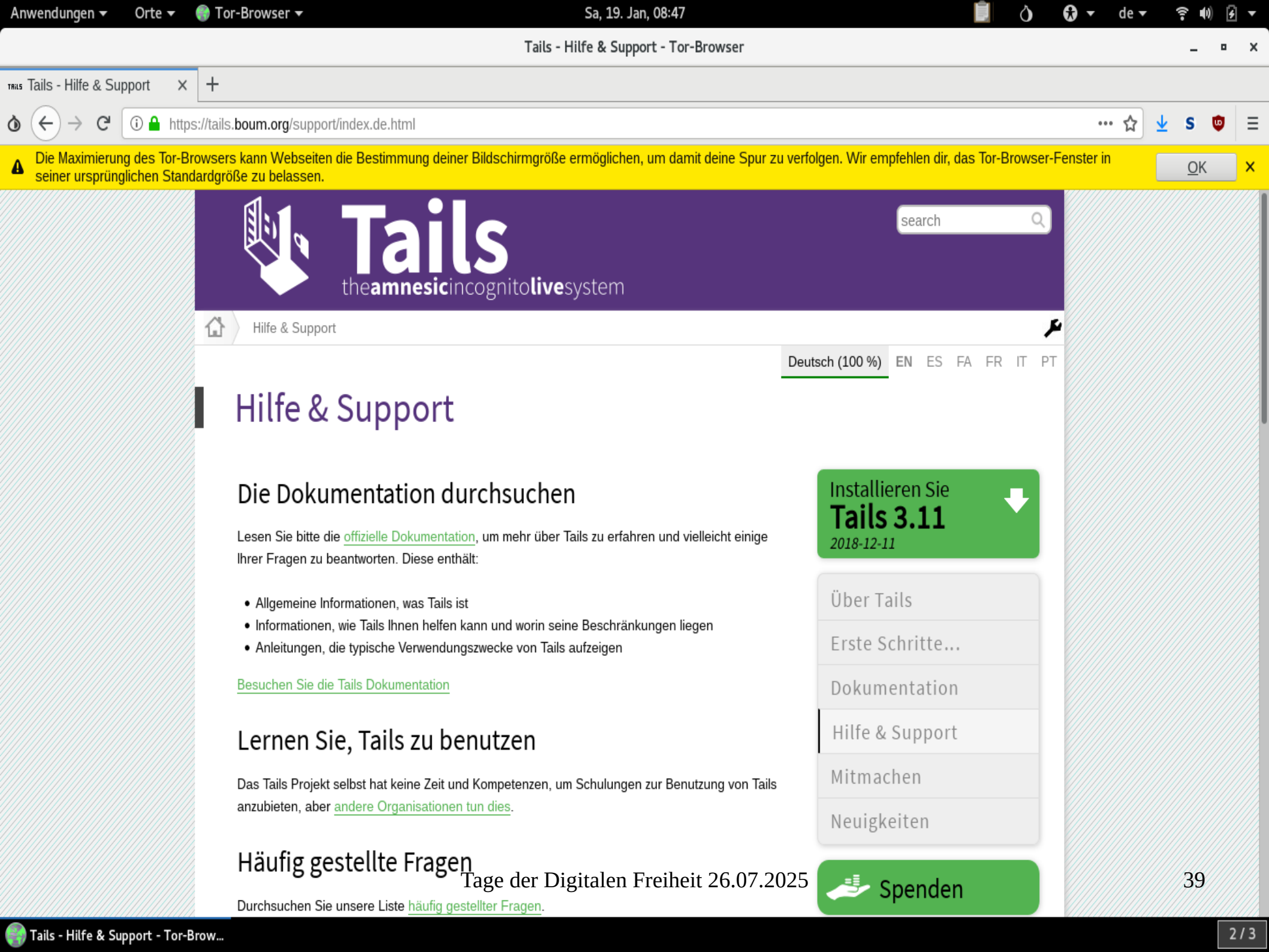
Fallstricke - Identitätspreisgabe

- TAILS-Nutzung über Smartphone-Hotspot oder UMTS-Stick:

  > Die Identifikationsnummer der SIM-Karte (IMSI) und die Seriennummer des Sticks (IMEI) werden bei jeder Netzeinwahl an den Mobilfunkanbieter übertragen > Identifikation und geografische Lokalisierung!!
- Anonymes Browsing und (!) personalisierte Nutzung (Bank-Account etc.) in 1 Sitzung

Fallstricke - Identitätspreisgabe

- Versehentliches unverschlüsseltes Abspeichern von sensiblen Inhalten auf Datenträgern.
- immer gleiche Muster = Pattern im Aufrufen von Webseiten => wiedererkennbare Nutzung => wiedererkennbarer Nutzer
- Veränderung der Standardgröße des TOR-Browser-Fensters ergibt Rechner-individuelles Muster


Anwendungen
Orte
Tor-Browser
Sa, 19. Jan, 08:47
de
Tails - Hilfe & Support - Tor-Browser
Tails - Hilfe & Support
https://tails.boum.org/support/index.de.html
Die Maximierung des Tor-Browsers kann Webseiten die Bestimmung deiner Bildschirmgröße ermöglichen, um damit deine Spur zu verfolgen. Wir empfehlen dir, das Tor-Browser-Fenster in seiner ursprünglichen Standardgröße zu belassen.
OK
Tails
theamnesicincognitolivesystem
search
Hilfe & Support
Deutsch (100 %) EN ES FA FR IT PT
Hilfe & Support
Die Dokumentation durchsuchen
Lesen Sie bitte die offizielle Dokumentation, um mehr über Tails zu erfahren und vielleicht einige Ihrer Fragen zu beantworten. Diese enthält:
Allgemeine Informationen, was Tails ist
Informationen, wie Tails Ihnen helfen kann und worin seine Beschränkungen liegen
Anleitungen, die typische Verwendungszwecke von Tails aufzeigen
Besuchen Sie die Tails Dokumentation
Lernen Sie, Tails zu benutzen
Das Tails Projekt selbst hat keine Zeit und Kompetenzen, um Schulungen zur Benutzung von Tails anzubieten, aber andere Organisationen tun dies.
Häufig gestellte Fragen
Durchsuchen Sie unsere Liste häufig gestellter Fragen.
Installieren Sie
Tails 3.11
2018-12-11
Über Tails
Erste Schritte...
Dokumentation
Hilfe & Support
Mitmachen
Neuigkeiten
Spenden
Tails - Hilfe & Support - Tor-Brow...
2 / 3

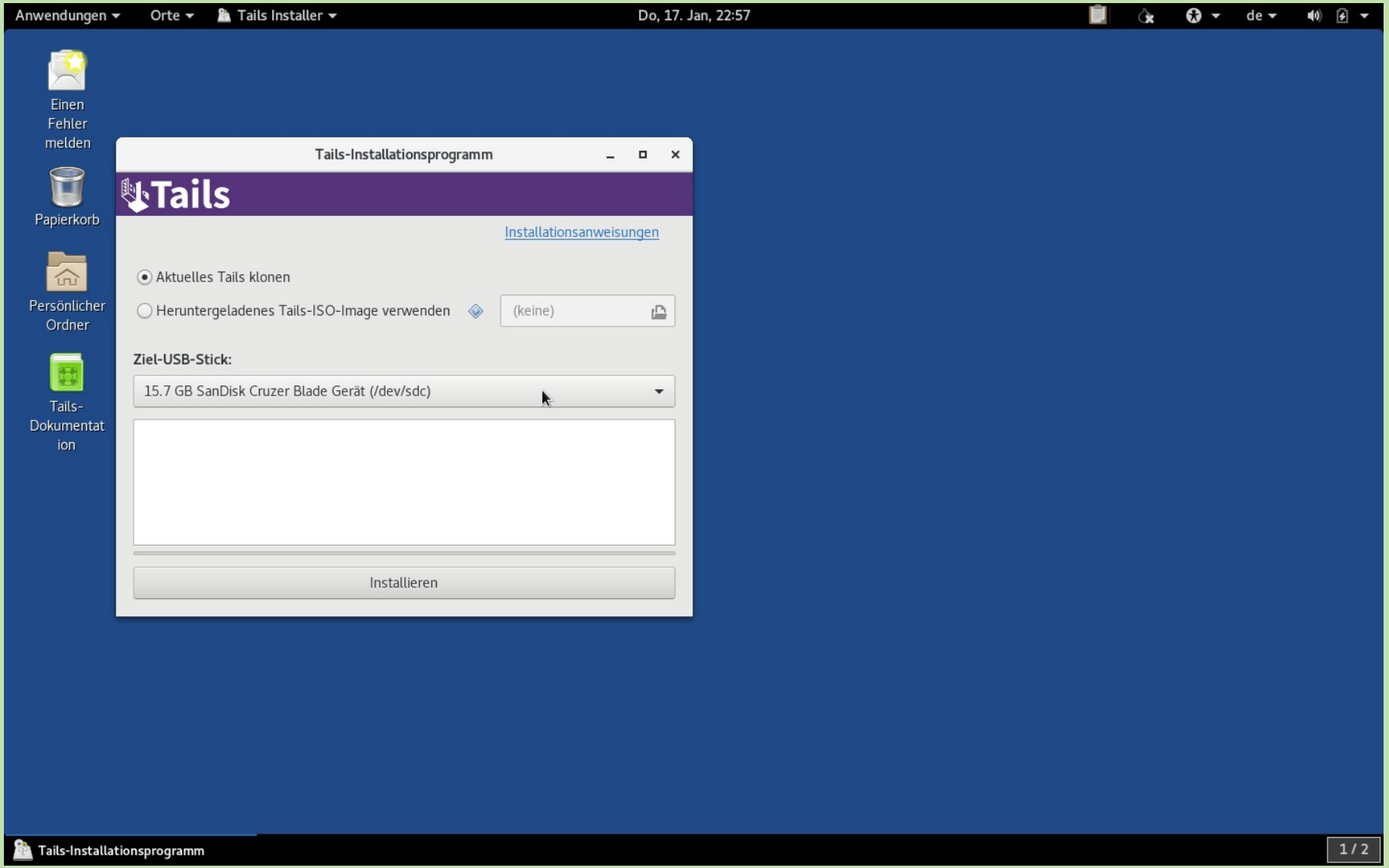
Lesenswerte Übersicht zur Sicherheit von TOR

- „Je länger eine Verbindung steht und je öfter ein Nutzer die gleichen Ziele ansteuert, desto größer die Wahrscheinlichkeit, dass diese Korrelation zur Deanonymisierung führt. Untersuchungen gehen davon aus, dass es durchschnittlich mehr als ein halbes Jahr dauern würde, um eine einzige Person zu enttarnen.“
- https://www.golem.de/news/hidden-services-die-deanonymiserung-des-tor-netzwerks-1501-111747-3.html

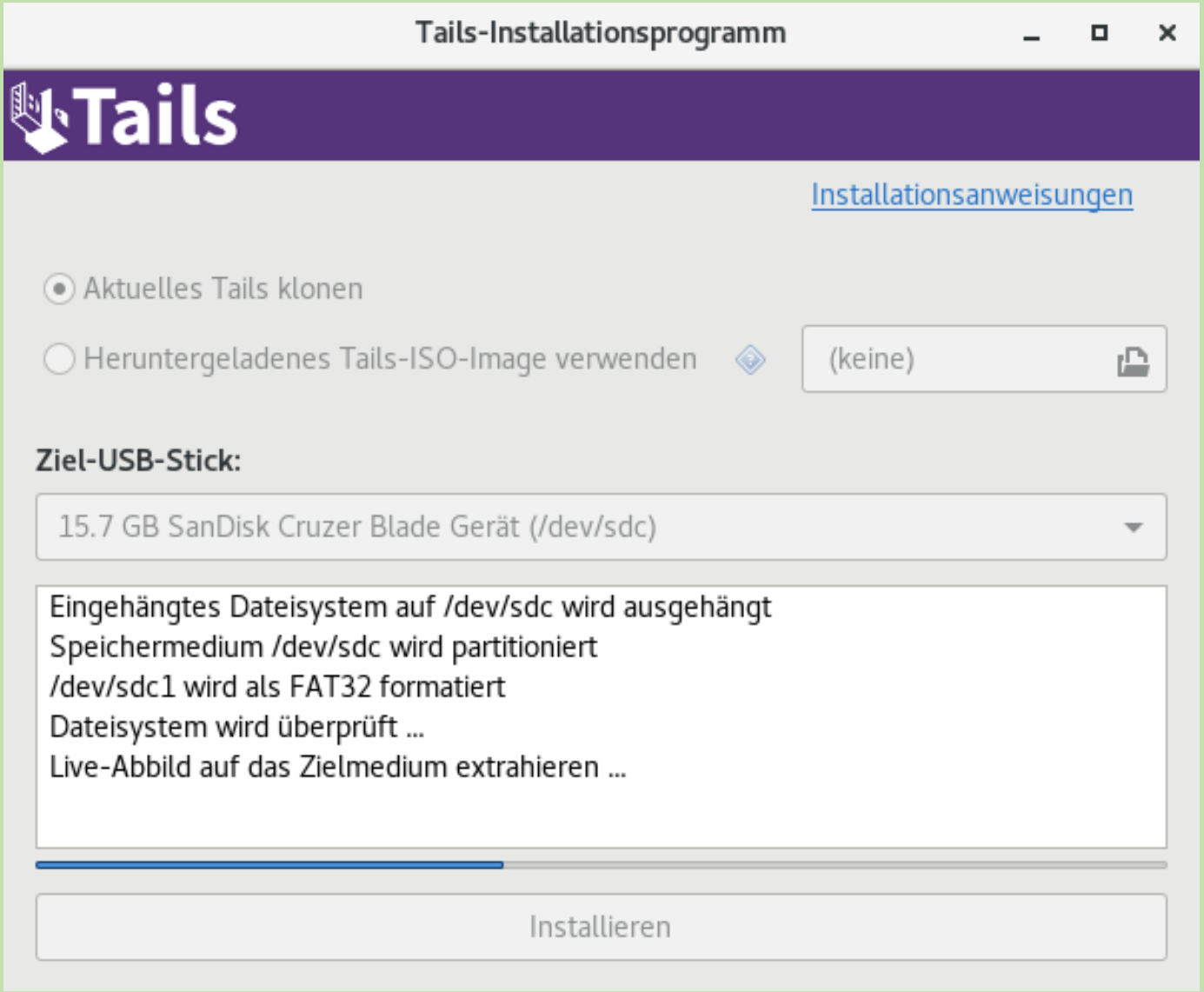
TAILS klonen

- Kopien des jeweils aktuellen sauberen Systems (ohne individuelle Einstellungen wie WLAN-Zugang ...) sind in ca 6 Minuten auf weitere USB-Sticks zu erstellen, z.B. um sie an Freunde weiterzugeben.
- USB-Stick-Mindestgröße: 8GB, mehr ist besser
- TAILS Installer aufrufen
- Formatieren löscht alle Daten auf dem Stick

Klonen - Start



Klonen - Ablauf



Die bereits in TAILS enthaltenen regelmäßig aktualisierten Open-Source-Programme decken die wesentlichen Standard-Anwendungsfälle ab!

Quellen:

- TAILS-Website: https://tails.boum.org/
- Video zu TOR „Anonym Surfen: https://de.wikipedia.org/wiki/Datei:Anonym_Surfen_einfach_erklärt.webm
- Electronic frontier foundation: Interaktion TOR und HTTPS: https://tor-https.eff.org/
- Hefte zur Förderung des Widerstands gegen digitalen Zugriff
  Band I: Tails – The amnesic incognito live system
  capulcu productions 7. überarbeitete Auflage
  https://capulcu.noblogs.org/files/2021/04/Tails-2021-04-12.pdf

DANKE!

Folien-Download, Veranstaltungen:

https://cryptoparty-tuebingen.de/

USB-Sticks mit Schreibschutz

z.B. Kanguru Flashblu30 16GB - USB 3.0 Stick