zweite erweiterte Auflage

Tails

The amnesic incognito live system

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

2. erweiterte Auflage

Hefte zur Förderung des Widerstands gegen den digitalen Zugriff

Band I: Tails – The amnesic incognito live system

capulcu productions 2. erweiterte Auflage | April 2015
V.i.S.d.P. E. Schmidt | Am Zuckerberg 14 | 21984 Silikontal

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

Eine digitale Version dieser Anleitung sowie redaktionell bearbeitete Anmerkungen, Änderungen und Neuerungen findet ihr unter **https://capulcu.blackblogs.org** . Die Verbindung zur Webseite erfolgt verschlüsselt. Um zu überprüfen, dass ihr wirklich auf unserer Seite gelandet seid, drucken wir hier zwei *Prüfsummen* unseres Webseiten-Zertifikats ab:

sha1: AC:4B:68:3D:E6:DB:9F:36:2D:88:E9:D4:6B:52:E4:0E:DF:6E:70:33
md5: C5:2D:C6:DB:FF:2B:F2:A3:B7:1E:5F:D3:AF:F4:7D:3B

Wir freuen uns über Feedback. Den *Schlüssel* zu unserer Mail-Adresse findet ihr auf unserer Webseite **https://capulcu.blackblogs.org** . Wir drucken hier zur Überprüfung der Echtheit den *Fingerprint* diese Schlüssels ab:
capulcu@nadir.org AF52 0854 7EF1 711A F250 57CB D0D0 A3C5 DF30 9590

Für Kontakt zu den Tails-Entwickler*innen findet ihr den Schlüssel auf der Seite **https://tails.boum.org**
tails@boum.org A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F

Inhalt

Einführung

Seit den „späteren“ Snowden-Veröffentlichungen vom März 2014 wissen wir leider mit Sicherheit, dass die Geheimdienste NSA, GCHQ und weitere für eine maßgeschneiderte Infiltration unserer Rechner keine menschlichen Hacker mehr benötigen, sondern automatisiert mit dem Spionageprogramm *Turbine*[1] unbemerkt spezifische Schnüffel-Software auf unseren Rechnern installieren.

Wir empfehlen angesichts dieser Angreifbarkeit über massenhaft infizierte Rechner, *Tails* als unveränderliches „Live-Betriebssystem“ für das Kommunizieren, die Recherche, das Bearbeiten und Veröffentlichen von sensiblen Dokumenten zu benutzen. Ein Live-Betriebssystem ist ein eigenständiges Betriebssystem, was von DVD oder USB-Stick gestartet werden kann, ohne es zu installieren. Euer Standard-Betriebssystem auf der Festplatte wird nicht angefasst.

Tails hilft euch bei der Bearbeitung von sensiblen Text-, Grafik- und Tondokumenten. Tails verwendet beim Surfen, Mailen und Chatten automatisch die Anonymisierungssoftware „*Tor*“ und verändert zusätzlich die sogenannte „MAC-Adresse“ eurer Netzwerkkarte. Was das ist und wozu das von Nutzen ist, erklärt euch die Einführung dieser Anleitung.

Tails hinterlässt bei richtiger Nutzung keine Spuren auf dem Rechner - eure Festplatte bleibt unberührt. Ein eventuell (auf Betriebssystemebene) eingeschleuster Schadcode kann sich auf einer Live-DVD oder einem schreibgeschützten Live-USB-Stick[2] als Start-Medium nicht „festsetzen“ und euch beim nächsten Rechnerstart nicht mehr behelligen[3].

Konkrete Blockade digital-totalitäter Erfassung

Wer sich gegen die Verletzung von Persönlichkeitsrechten durch das Ausspionieren jeglicher Netzdaten, gegen DNA-Datenbanken und (Drohnen-)Kameraüberwachung politisch aktiv zur Wehr setzt, sollte auch bei der Preisgabe seiner Alltagsdaten nicht nur sparsamer, sondern vor allem strategisch (und damit ganz anders als üblich) vorgehen.

Insbesondere das Zusammenführen unserer verschiedenen Aktivitäten, Interessen, Neigungen, Einkäufe, Kommunikationspartner*innen, (…) zu einer integralen „Identität“ ist die Grundlage für die Mächtigkeit von schnüffelnden Analysewerkzeugen - egal ob sie ökonomisch-manipulativen oder repressiven Absichten entspringen. Das im Folgenden beschriebene Live-Betriebssystem *Tails* hilft Nicht-Expert*innen, mit annehmbarem Aufwand dieses „integrale Ich“ auf unterschiedliche digitale Identitäten zu verteilen. Noch besser: Ihr nutzt mit mehreren vertrauenswürdigen Personen *einen gemeinsamen* Mail-, Chat-, Blog-, oder Forum-Account *Orts-anonymisierend*. Auch das erledigt *Tails* über die Anonymisierungssoftware *Tor*.

Zur (Wieder-)Erlangung eines Mindestmaßes an Privatheit und Daten-Souveränität raten wir darüber hinaus zur Verschlüsselung aller Inhalte, zum lokalen Speichern eurer Daten (ohne Cloud), zur Facebook-Verweigerung, zur gezielten Drosselung unserer Teilhabe am digitalen Dauersenden (das möglichst „unsmarte“[4]! Mobiltelefon so oft es geht zu Hause lassen) und zum Offline-Einkauf mit Barzahlung.

Im Netz möglichst wenig Spuren zu hinterlassen, muss zu den Grundfertigkeiten einer jeden Aktivist*in gehören. *Tor* muss unser alltägliches Standardwerkzeug werden und Tails hilft uns, (unter anderem) bei der Nutzung von *Tor* möglichst wenig Fehler zu machen.

Verglichen mit dem, was wir an Selbstbestimmtheit bereits verloren haben, ist der Aufwand für ein abgeändertes Alltagsverhalten minimal, auch wenn es vielen von uns „unbequem“ erscheint. Die „bequeme“ Alternative hingegen bedeutet Kontrollierbarkeit, Vorhersagbarkeit, Manipulierbarkeit und erhöhtes Repressions-Risiko – es liegt an euch!

Wozu ein Live-Betriebssystem (auf DVD oder USB-Stick) ?

Die wichtigsten Gründe für die Verwendung eines Live-Betriebssystems wie Tails sind dessen *Vergesslichkeit* und *Unveränderbarkeit*.

Nach dem Herunterfahren des Rechners sind alle Daten, die ihr zuvor nicht explizit auf einen (externen) Datenträger gesichert habt, wieder weg. Der ohnehin vergessliche Arbeitsspeicher eures Rechners wird beim Herunterfahren zusätzlich mit Zufallszahlen überschrieben und die Festplatte bleibt von der Tails-Sitzung unberührt[5]:

1 The Intercept, Glenn Greenwald, Ryan Gallagher, 12.3.2014 https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/

2 USB-Sticks mit mechanischem Schreibschutzschalter sind leider nur selten im Offline-Handel erhältlich. Hersteller solcher Sticks ist u.a. die Firma *Trekstor*.

3 Gegen eine Infiltration des Rechners über manipulierte Hardware oder das BIOS (=Basisbetriebssystem eines Computers) ist mensch damit nicht geschützt!

4 Ein Mobiltelefon ohne WLAN und Bluetooth ist ein besserer Schutz.

5 Es sei denn, ihr speichert explizit einzelne Dateien auf die interne

Keine Systemdateien, die verraten, welche USB-Sticks ihr benutzt habt, keine versteckten Rückstände eurer Internetrecherche, kein Hinweis auf „zuletzt bearbeitete“ Dokumente, keine Überbleibsel einer Bildbearbeitung und vor allem auch keine Schad-/Schnüffelsoftware, die sich während eurer Sitzung irgendwo in den Betriebssystemdateien eingenistet haben könnte – alles weg nach Abschluss eurer Arbeit. Euer „normales“ Betriebssystem (auf der Festplatte) dieses Rechners bleibt unverändert. Der Rechner trägt auch keine Spur, die darauf hindeutet dass es diese Tails-Sitzung gegeben hat.

Um bei sensibler Arbeit wirklich sicher zu gehen, dass tatsächlich nichts zurückbleibt, sollte sich das Tails Live-Betriebssystem entweder auf einem unveränderlichen Datenträger befinden (z.B. eine gebrannte DVD oder ein USB-Stick mit mechanischem Schreibschutzschalter), oder aber (per Startoption toram[6]) vollständig in den Arbeitsspeicher des Rechners geladen werden. Dann könnt ihr nämlich den Datenträger, auf dem sich Tails befindet, nach dem Hochfahren des Rechners noch vor Arbeitsbeginn auswerfen/abziehen.

Vorteile bei der Nutzung von Tails

Bei Tails werden zudem alle Netzwerkverbindungen nach „draußen“ über eine fertig konfigurierte *Tor*-Software geleitet[7]. Das heißt, ihr habt weniger Möglichkeiten, über eine falsche Einstellung von *Tor*, eure Identität versehentlich doch preiszugeben. Selbstverständlich müsst ihr auch mit Tails wichtige Grundlagen für die *Tor*-Nutzung[8], wie z.B. den Unterschied zwischen Verschleierung der Identität und Verschlüsselung der Verbindung, berücksichtigen. Aber dazu später mehr. Tails hat darüber hinaus viele sicherheitsrelevante Softwarepakete integriert und wird kontinuierlich gepflegt.

Da Tails mittlerweile ein sehr umfangreiches und vielseitig einsetzbares Live-System ist und die (derzeit nur in englischer und französischer Sprache vollständige) Dokumentation auf der Webseite https://tails.boum.org entsprechend reichhaltig ist, versuchen wir hiermit eine verdichtete, aber trotzdem verständliche Einführung für Computer-Nicht-Expert*innen zur Verfügung zu stellen.

Wir werden im Folgenden drei Nutzungsmodelle für Tails beschreiben:

a) Tails als System für sensible Arbeiten auf einem Rechner mit Internetzugang

Hier lernt ihr den Umgang mit den von Tails zur Verfügung gestellten Programmen. Die Verbindung zum Netz erledigt ein weitgehend automatisierter und einfach zu bedienender Netzwerk-Manager. Die Oberfläche sieht sehr ähnlich aus wie bei eurem normalen Betriebssystem auf der Festplatte - egal ob ihr Windows, Mac-OS X oder ein Linux-Betriebssystem nutzt, ihr werdet euch bei Tails schnell zurecht finden.

b) Tails als „Quasi-Schreibmaschine“ für hoch-sensible Arbeiten auf einem völlig abgeschotteten Rechner ohne Netz, bei dem Festplatte(n), WLAN- und Bluetooth-Adapter ausgebaut sind.

Hier lernt ihr den Umgang mit besonders sensiblen Dokumenten. Das kann die Bearbeitung von Texten, Fotos, Tonaufnahmen oder die Erstellung ganzer Bücher sein. Hier darf nichts schief gehen. Deshalb raten wir in solchen Fällen zu einem Rechner mit beschränkten Fähigkeiten *(keine Festplatte, keine Internetverbindung, kein WLAN, kein Bluetooth)*, der euch zudem nicht persönlich zugeordnet werden kann.

c) Persistenz: Tails als Reise- und Alltagssystem

In Erweiterung zur ersten Auflage dieses Heftes haben wir uns entschlossen, eine weitere Nutzungsmöglichkeit von Tails zu dokumentieren: Tails auf einem USB-Stick mit einer zusätzlichen (verschlüsselten) Daten-Partition[9], auf der Einstellungen, Mails, oder andere Daten dauerhaft gespeichert bleiben. In dieser Nutzungsart ist der Tails-Stick nicht mehr *unveränderbar*[10] und Tails nicht mehr vollständig *vergesslich*.

Im Vergleich zu a) und b) ist diese Nutzung also explizit unsicherer! Im Vergleich zu eurem Alltagsrechner auf der Festplatte aber in der Regel viel sicherer, denn Tails lenkt weiterhin jede Kommunikation mit der Außenwelt sicher durch das Anonymisierungsnetz *Tor*. Wer also einen Reiselaptop mit Netzzugang nutzt, aber z.B. seinen Aufenthaltsort beim Mailen und Chatten nicht verraten will, und dennoch bequemen Zugriff auf seine bisherigen Mails und Dokumente benötigt, der sollte Tails als sicherere Alternative zu einem Standard-Betriebssystem in Erwägung ziehen. Diese Methode beschreiben wir im Kapitel *Persistenz*.

Festplatte. Davon raten wir ab!

6 siehe Kapitel *Tails Starten*

7 Es sei denn, ihr wählt explizit den unsicheren Internet Browser - ohne *Tor*. Davon raten wir dringend ab!

8 https://tor.eff.org/download/download-easy.html.en#warning

9 Ein Datenträger kann in mehrere getrennte Partitionen aufgeteilt sein.

10 Der Datenträger wird dazu ohne Schreibschutz genutzt!

Systemvoraussetzungen und Betriebsarten von Tails

Tails läuft auf den meisten Rechnern, die nach 2005 gebaut wurden[11]. Ihr benötigt einen Rechner mit einem internen oder externen Laufwerk, das DVDs lesen und *booten* (=starten) kann, oder aber einen Rechner, der von einem USB-Stick oder einer SD-Karte *booten* kann.

Zusätzlich sollte euer Rechner für einen fehlerfreien Betrieb über einen Arbeitsspeicher (RAM) von mindestens 1 GB verfügen[12]. Tails läuft auf allen herkömmlichen PCs, nicht jedoch auf Smartphones (ARM-Prozessoren) oder PowerPCs (ältere Apple-Rechner).

Da die Sicherheit von Tails maßgeblich von der Unveränderbarkeit dieses Live-Systems abhängt, empfehlen wir *nur in zwei Ausnahmefällen* Tails mit der Startoption **toram** zu benutzen. Dann wird das gesamte Betriebssystem von Tails mit allen Anwendungsprogrammen zu Beginn in den Arbeitsspeicher geladen. Dazu sollte euer Rechner über mindestens 2 GB Arbeitsspeicher verfügen.

1) Wenn ihr einen Tails-USB-Stick ohne mechanischen Schreibschutzschalter oder eine Tails-SD-Karte[13] benutzt. Mit der Startoption **toram** können diese Datenträger nach dem Start[14] von Tails entfernt werden noch bevor ihr mit der Arbeit beginnt. Damit sind diese Datenträger vor einem eventuellen Angriff (eingeschleust über das Internet oder andere Datenträger) sicher.

2) Wenn ihr eine Tails-DVD benutzt und in eurer Sitzung Daten auf CD oder DVD brennen wollt. Mit der Startoption **toram** kann die Tails-DVD nach dem Hochfahren des Rechners herausgenommen werden. Damit ist das Laufwerk während der Sitzung frei.

Nur über Tor ins Netz

Bevor wir erklären, wie Rechner im Netz kommunizieren, auf das *Tor*-Prinzip und dessen Nutzung eingehen sowie eine Reihe Fallstricke[15] darstellen, gleich ein Ratschlag vorweg:

11 Auch noch ältere Modelle können oftmals (mit Einschränkungen) für Tails genutzt werden.

12 Bei weniger als 1 GB Arbeitsspeicher kann der Rechner manchmal „einfrieren“. Der Grund dafür liegt darin, dass Tails selbstverständlich nicht auf die sogenannte Auslagerung-Partition (SWAP) der Festplatte zurückgreifen darf: Ein Auslagern von Daten und Programmen auf die Festplatte würde ja nachvollziehbare Datenspuren hinterlassen!

13 Der Schreibschutz von SD-Karten lässt sich software-seitig umgehen und bietet daher keinen Schutz. Nur bei USB-Sticks wird der mechanische Schreibschutzschalter tatsächlich „respektiert“.

14 Sobald sich der Rechner (nach Boot- und Start-Bildschirm) mit der Tails-Arbeits-Oberfläche meldet.

15 https://tor.eff.org/download/download-easy.html.en#warning

Die Software Tor (The Onion Router) sollte auch außerhalb von Tails euer Standard beim Surfen, Mailen und Chatten werden – nur wenn ihr per Tor keinen Zugang zu spezifischen Inhalten/Diensten erhaltet und genau wisst, was ihr tut, solltet ihr auf einen „normalen“ Browser (ohne Tor) zurückgreifen.

Identifizierung im Netz per IP- und MAC-Adresse

Ein großer Teil der digitale Kommunikation identifiziert die Kommunizierenden über die sogenannte IP (Internet Protocol)-Adresse. Ein *Router*, über den ihr ins Netz geht, bekommt diese **IP-Adresse** (z.B. 172.16.254.1) vom Internetanbieter zugewiesen. Die IP-Adresse wird bei jeder Netzaktivität über ein standardisiertes Protokoll (lesbar) mitgeschickt. Euer surfen, chatten oder mailen ist (ohne *Tor*) mit der *Identität und Lokalität dieses Routers* nachvollziehbar verknüpft.

Wenn ihr keine zusätzlichen Vorkehrungen trefft, verrät die übertragene IP-Adresse den geografischen Ort des Routers, über den ihr ins Netz geht.

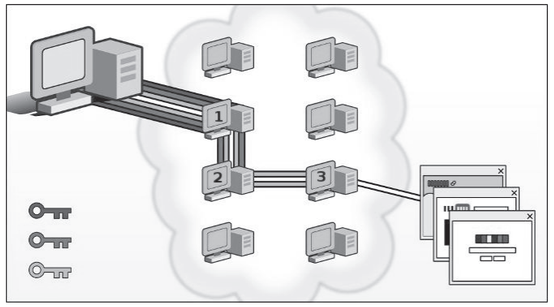
Zusätzlich besitzen alle Netzwerkadapter eine zusätzliche Kennung- die **MAC-Adresse** (z.B. B4:89:91:C1:F4:CE). Jede Netzwerkschnittstelle (z.B die WLAN-Karte oder das kabelgebundene LAN) eures Rechners meldet sich mit einer eigenen, eindeutigen (physikalischen) MAC-Adresse (Media-Access-Control) beim Router an. Beim aktuell verwendeten Internetprotokoll (ipv4) wird diese jedoch nicht „*nach draußen*“ (ins Netz) übertragen[16].

Aber: Wenn ihr z.B. per WLAN in einem öffentlichen Café ins Netz geht, kann der Betreiber oder ein Angreifer ohne technischen Aufwand eure MAC-Adresse mitprotokollieren. Damit ist dann eure Internet-Aktivität nicht mehr nur dem WLAN-Router des Cafés sondern exakt dem von euch verwendeten WLAN-Adapter eures Computers zuzuordnen! Auch zu Hause kann ein Angreifer, der sich in euren Router hackt, unterscheiden welcher Rechner (z.B. in der WG) eine bestimmte Mail verschickt hat. Wir kommen gleich dazu, wie ihr euch gegen eine Identifikation per MAC-Adresse schützen könnt.

16 Bei dem neueren Internetprotokollstandard *ipv6* kann die MAC-Adresse in der IP mitkodiert werden. Das würde die Verschleierung des verwendeten Rechners gefährden. Deshalb verwendet Tails diesen Protokollstandard nicht!

Das *Tor*-Prinzip (The Onion Router)

Statt in eurem Standard-Browser (*Firefox* oder ähnliche) z.B. die Webseite http://tagesschau.de direkt zu besuchen und dieser beim Kontaktaufbau die IP-Adresse eures Routers mitzuteilen, geht ihr beim voreingestellten *Tor-Browser* von Tails einen Umweg über drei Zwischenstationen. Diese drei Rechner werden von der *Tor*-Software aus weltweit (derzeit) über 5000 verfügbaren *Tor*-Rechnern *zufällig* ausgewählt.



Der Inhaber des Servers, auf dem die Zielwebseite liegt (oder ein dort mitlesender Schnüffler) erhält nicht eure IP-Adresse, sondern die vom *Tor*-Exit-Rechner **3** als Besucher-IP. Zwar ist erkennbar, dass es sich hierbei um einen Rechner des *Tor*-Netzwerkes handelt (die Liste aller verfügbaren *Tor*-Rechner ist öffentlich einsehbar), aber eure Identität ist nicht rekonstruierbar, es sei denn, der Inhalt eurer Kommunikation mit der Zielwebseite verrät euch (persönliche Identifikation). Keiner der drei *Tor*-Rechner kennt den kompletten Pfad von eurem Rechner bis zum Zielserver. Nur ein Angreifer, der den Netzverkehr *aller drei Tor*-Rechner (aus 5000 möglichen) kennt, kann eure IP eindeutig mit dem Besuch der Ziel-Webseite in Verbindung bringen[17].

Verschleierung der Identität bedeutet nicht automatisch Verschlüsselung

Die Verbindungen von eurem Rechner zum *Tor*-Rechner **1**, sowie **1—2** und **2—3** sind verschlüsselt. Damit ist der Inhalt bei einem Schnüffel-Angriff auf diese Verbindungen, bzw auf die *Tor*-Rechner **1** und **2** nicht lesbar. *Die Verbindung von* **3—Ziel** *ist hingegen unverschlüsselt!*

Nur wenn Ihr eine Webseite beginnend mit HTTP**S** besucht wie z.B. http**s**://linksunten.indymedia.org ist auch der Inhalt dieser letzten Verbindung verschlüsselt. Der *Tor*-Browser von Tails versucht immer eine HTTP**S**-Verbindung zum Ziel aufzubauen. Bietet der Webseitenbetreiber jedoch nur HTTP-Verbindungen an, ist eure Kommunikation mit diesem Server unverschlüsselt und kann dort bzw. auf dem *Tor*-Exit-Rechner **3** oder dazwischen mitgelesen werden!

17 Korrekt: Eine umfassende Traffic-Analyse ermöglicht einem Angreifer eine Zuordnung (mit Einschränkung) auch dann, wenn er den vollständigen Netzverkeht der *Tor*-Rechner **1** und **3** protokolliert. Wir gehen später darauf ein.

Verschiedene Nutzungsmodelle von *Tor*

Tor verschleiert eure IP-Adresse mit der ihr zum Surfen, Mailen oder Chatten mit anderen Servern Kontakt aufnehmt. Einer der Zwecke von *Tor* liegt in der **Verschleierung der eigenen Identität**.

Als Besucher einer Webseite geht das, solange ihr dort keine Daten über euch preisgebt, oder spezifische Inhalte euch eindeutig identifizieren. Beim Mailen können euch Mail-Kontakte oder Mail-Betreffzeile leicht verraten, selbst wenn ihr peinlich genau darauf geachtet habt, dass (inklusive Account-Eröffnung) über die gesamte Historie der Account-Nutzung alles anonym ablief.

Deshalb wird vielfach behauptet, dass *Tor* unsinnig ist wenn ihr euch persönlich (ohne Pseudonym bei eurer Bank einloggt oder eine Mail von einer Adresse verschickt, die mit eurer Person eindeutig in Verbindung steht. Das stimmt nur zur Hälfte. Richtig ist, dass ihr mit einem (realen) persönlichen *login* eure Identität gegenüber dem Server offenbart – da hilft auch kein *Tor*. Aber ihr könnt auch in diesen Fällen *Tor* zur **Verschleierung eures Aufenthaltsortes** nutzen. Ein weiterer Anwendungsfall für *Tor* ist das **Erschweren von Zensur und Überwachung euerer Netzwerkaktivitäten**.

> ***Wir raten euch, IMMER per Tor ins Netz zu gehen und eure Netzaktivitäten entlang verschiedener Identitäten „aufzutrennen".***

Identitäten sauber trennen

Es ist nicht ratsam, in ein und derselben Tails-Sitzung, verschiedene Aufgaben im Internet zu erledigen, die nicht miteinander in Verbindung gebracht werden sollen. Ihr müsst selbst verschiedene (kontextuelle) Identitäten sorgsam voneinander trennen!

Ein Beispiel: Es ist gefährlich, in der gleichen Sitzung per *Tor* (ortsverschleiernd) die persönlichen Mails abzurufen und anonym bei indymedia einen Text zu publizieren. Das heißt, ihr solltet nicht gleichzeitig *identifizierbar* und *anonym* ins *Tor*-Netz. Ihr solltet auch nicht gleichzeitig unter Pseudonym A und Pseudonym B ins *Tor*-Netz gehen, denn diese Pseudonyme könnten auf einem überwachten/korrumpierten *Tor*-Exit-Rechner **3** miteinander in Verbindung gebracht werden.

Da ihr euch nicht in allen Fällen auf die Funktion „*Neue Identität*" im *Tor*-Browser verlassen könnt, um die verschiedenen Netzaktivitäten (durch verschiedene IP-Adressen der verschiedenen *Tor*-Exit-Rechner) voneinander zu separieren, lautet die unbequeme aber sichere Empfehlung:

> ***Tails zwischen Netzaktivitäten unterschiedlicher Identität herunterfahren und neu starten!***

Denn sogenannte *cookies*[18], ein *Tor*-Anwendungsfehler eurerseits oder eine (noch nicht bekannte oder behobene) Sicherheitslücke in einem Programm innerhalb von Tails könnten Informationen über Eure Tails-Sitzung offenlegen. Diese könnten offenbaren, dass ein und dieselbe Person hinter den verschiedenen Netzaktivitäten der gleichen Tails-Sitzung (trotz wechselnder IP-Adresse des *Tor*-Exit-Rechners **3**) steckt.

Ist *Tor* noch sicher?

Diese Frage ist nicht nur aufwändig in der Beantwortung, denn dazu müssen wir die (uns) bekannten Angriffe analysieren, sie ist vor allem immer mit folgender Warnung zu beantworten:

> ***Geheimdienste attackieren das Tor-Netzwerk, um die Anonymität der Tor-Nutzer*innen zu brechen. Wir können die Effektivität von Tor nicht garantieren !***

Wir analysieren im Kapitel „*Warnung: Grenzen von Tails*" verschiedene Angriffe gegen *Tor*. Die bislang veröffentlichten „Enttarnungserfolge" öffentlich gewordener Angriffe auf *Tor* beruhten auf Sicherheitslücken des verwendeten Browsers, auf Anwendungsfehlern oder auf immer gleichen Nutzungsverhalten im Netz. Allerdings sind auch Sicherheitslücken im *Tor*-Protokoll gefunden und behoben worden. Ob sie in dieser Zeitspanne zur Enttarnung von Nutzer*innen geführt haben, ist uns nicht bekannt.

Wir wissen, dass es massive Angriffe von sehr starken Angreifern (NSA, FBI) auf sogenannte „hidden sevices" im *Tor*-Netz gibt; das ist ein Teil des sogenannten „darknet" und beschreibt nicht die in diesem Heft dargestellte Standard-Nutzung von *Tor*.

Wir können die Sicherheit von *Tor* gegenüber diesen Angreifern nicht garantieren. Dennoch ist *Tor* das beste was es derzeit gibt. *Tor* wird ständig weiterentwickelt, um neu entdeckte Sicherheitslücken zu schließen. Daher nutzt auf jeden Fall immer die neueste Tails-Version !

18 Cookies sind kleine Dateien, die z.B. ein Webseitenbetreiber auf eurem Rechner als Webseitenbesucher zur Wiedererkennung von bestimmten Einstellungen ablegt. Tails untersagt das Speichern der meisten Cookie-Sorten. Andere, zugelassene Cookies verbleiben im flüchtigen Arbeitsspeicher und verschwinden bei einem Neustart.

Das Ergebnis bleibt leider unbefriedigend: Erst bei Kenntnis des Versagens des *Tor*-Netzwerks sind wir in der Lage, eine klare (negative) Aussage zu treffen - d.h. erst wenn das Kind in den Brunnen gefallen ist, können wir mit Sicherheit sagen, dass es so ist. Das bedeutet – ihr müsst bei der Bewertung etwaiger Konsequenzen von der *Möglichkeit* ausgehen, dass eure **IP-Adresse** einer Recherche oder einer Veröffentlichung zugeordnet werden *könnte*. Der Ort des Routers wäre in einem solchen Fall enttarnt. Die durch Tails veränderte **MAC-Adresse** hilft euch zumindest zu verschleiern, welcher Rechner an dem dann enttarnten Router für diese Netzaktivität verantwortlich sein soll *(siehe nächstes Kapitel)*.

Da niemand kategorisch ausschließen kann, dass auch diese zusätzliche Ebene der Verschleierung technisch durchbrochen werden *könnte*, solltet ihr *zusätzlich* auf für euch kontrollierbare Sicherungsmethoden zurückgreifen. Zu zwei dieser Methoden raten wir bei besonders sensiblen Aktivitäten im Internet: Geht nicht von einem für euch gewöhnlichen Ort ins Netz und nutzt keinen Rechner, der euch zugeordnet werden kann (d.h. nicht übers Internet, sondern so anonym wie möglich *offline* besorgt).

Damit ergeben sich dann folgende Sicherungsebenen zur Anonymisierung *besonders sensibler Netzaktivitäten*:

> **1) Sichere Konfiguration der jeweiligen Anwendungsprogramme** *(in dieser Anleitung)*
>
> **2) Verschleierung der IP-Adresse per Tor**
>
> **3) Verschleierung der MAC-Adresse per Tails** *(siehe nächstes Kapitel)*
>
> **4) Netzzutritt an einem für euch ungewöhnlichen Ort ohne Kameras, ohne euer Handy/ andere WLAN-, oder Bluetooth-Geräte**
>
> **5) Anonymer Kauf und versteckte Lagerung eines „Recherche-Computers"**

Tails ändert eure MAC-Adressen

WLAN ständig auf der Suche nach verfügbaren Netzen

Wenn Ihr mit angeschaltetem Laptop, Tablet oder Smartphone bei aktiviertem WLAN[19] durch die Stadt geht, dann meldet sich eure WLAN-Karte mit ihrer MAC-Adresse bei allen WLAN-Routern in Funkreichweite. Und das ohne dass ihr im Netzwerk-Manager eine solche Verbindung aktiv auswählt und herstellt! Die Router aller dort gelisteten WLAN-Netze der Umgebung haben euren Computer bereits über dessen WLAN-MAC-Adresse bei einer *initialen* Begrüßung identifiziert! Ihr hinterlasst also eine zurückverfolgbare Spur, falls diese flüchtigen „Begrüßungen" aufgezeichnet werden[20].

Im Falle eines Anwendungsfehlers oder sonstigen Tor-Problems könnte ein Angreifer euren Rechner anhand der aufgezeichneten MAC-Adresse des WLANs identifizieren, sofern er sich Zugang zum Router verschafft, über den ihr ins Netz gegangen seid.

Zur zusätzlichen Sicherheit ersetzt Tails (seit März 2014) vor der ersten Netzeinwahl (beim Start von Tails) die MAC-Adresse(n) aller im BIOS aktivierten Netzwerkadapter eures Rechners durch zufällige Adressen.

Es gibt allerdings Situationen, in denen das nicht funktioniert: Manche Netzwerke erlauben nur einer beschränkten Liste von voreingestellten MAC-Adressen den Zugang. Nur wenn Ihr glaubt, auf diese zusätzliche Sicherheit verzichten zu können, könnt ihr Tails neu starten und beim Tails-Begrüßungsfenster „*Ja*" (für weiter Optionen) anklicken und dann die (standardmäßig gesetzte) Option „*Alle MAC-Adressen manipulieren" abwählen*! **Wir raten jedoch zugunsten eurer Anonymität davon ab!**

Vorsicht beim UMTS-Stick

Auch das ist ein eigenständiger Netzwerkadapter, der somit auch eine eigene MAC-Adresse besitzt. Auch diese wird von Tails beim Start mit einer Zufallsadresse überschrieben. Dennoch muss man hier auf die zusätzliche Sicherheit einer veränderten MAC-Adresse verzichten, da auch die eindeutige Identifikationsnummer eurer SIM-Karte (**IMSI**) und die eindeutige Seriennummer eures Sticks (**IMEI**) *bei jeder Netzeinwahl an den Mobilfunkanbieter übertragen* werden und eine Identifikation sowie eine geografische Lokalisierung ermöglichen. Der UMTS-Stick funktioniert wie ein Mobiltelefon!

Wer nicht möchte, dass verschiedene Recherche-Sitzungen miteinander in Verbindung gebracht werden können, darf weder den UMTS-Stick noch die SIM-Karte mehrmals benutzen![21]

Für sensible Recherchen oder Veröffentlichungen sind sowohl der UMTS-Stick als auch die SIM-Karte zu entsorgen.

Andernfalls wären verschiedene Recherchen über die gemeinsame IMEI oder die gemeinsame IMSI miteinander verknüpft. *Der Austausch der SIM-Karte allein genügt ausdrücklich nicht!*

Wir legen euch einige weitere Anmerkungen zu den Grenzen von Tails (im Anhang) ans Herz! Nach diesen Vorüberlegungen und Warnungen zur Sicherheit im Netz wird es nun praktisch.

19 Das WLAN lässt sich bei TAILS wie bei allen Betriebssystemen über den Netzwerk-Manager an- und abschalten, sofern ihr es nicht im BIOS deaktiviert habt.

20 In der Standard-Einstellung der Router werden solche Ereignisse nicht mitprotokolliert. Werbeanbieter*innen nutzen allerdings genau diese Möglichkeit, um potentielle Kund*innen vor dem Schaufenster oder im Laden zu identifizieren und ihre Verweildauer zu messen – mit ganz normaler Hardware!

21 Das gilt auch bei anonymem Erwerb von UMTS-Stick und SIM-Karte und deren anonymer Freischaltung.

Tails starten

Wir gehen in diesem Kapitel davon aus, dass ihr einen aktuellen *Tails-USB-Stick*, eine *Tails-SD-Karte* oder eine *Tails-DVD* habt. **Wie ihr das Tails-Live-System herunterladen und überprüfen! könnt**, um ein solches Start-Medium zu erzeugen, **beschreiben wir im Anhang** dieser Anleitung. Wir gehen ebenfalls davon aus, dass euer Computer bereits so eingestellt ist, dass er von einem der drei Medien *booten* (=starten) kann. Auch diese minimale **Einstellung im BIOS** ist **im Anhang** beschrieben.

Tails booten

Wenn ihr auf die Sicherheit durch die im vorigen Kapitel beschriebene Veränderung der MAC-Adresse eures WLANs setzen wollt, **dann muss der Tails-Datenträger vor dem Start eingelegt/eingesteckt sein – andernfalls würde ein „Fehlstart" mit eurem Standard-Betriebssystem euren Laptop per originaler MAC-Adresse eures WLANs in der Funkreichweite bekannt machen!**

Bei den meisten Computern genügt es, beim wenige Sekunden später erscheinenden **Boot-Bildschirm** die voreingestellte Auswahl *Live* mit der Enter-Taste zu bestätigen oder zehn Sekunden zu warten. Nur wenn Tails danach keine sichtbaren Startbemühungen unternimmt, solltet ihr in einem neuen Start-Versuch die Option *Live (failsafe)* auswählen.

Ein spezieller Recherche-Computer, aus dem ihr die Festplatte ausbaut und den ihr damit nur für Live-Systeme wie Tails nutzbar macht, löst das „Fehlstart"-Problem und verhindert zudem ein „versehentliches" Speichern von Daten auf Festplatte!

Zusätzliche Boot-Optionen

Um (eine) zusätzliche Boot-Option(en) auszuwählen, müsst ihr hingegen bei Erscheinen des Boot-Bildschirms

1. die *Tabulator*-Taste 

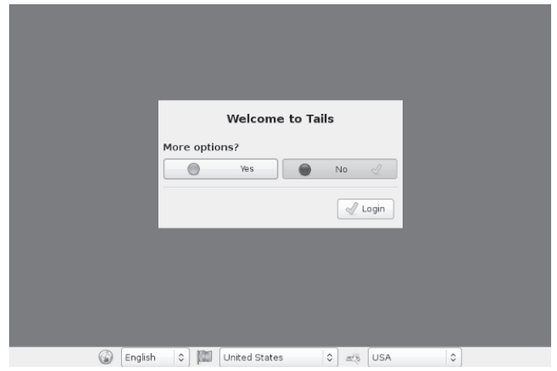
drücken und
2. ein *Leerzeichen* eingeben. Dann die jeweilige(n) Boot-Option(en jeweils durch ein Leerzeichen getrennt) eingeben und mit *Enter* abschließen:

- **toram** - lädt Tails komplett in den Arbeitsspeicher (mindestens 2 GB). Nur dann empfehlenswert, wenn ihr *a)* eine SD-Karte oder einen USB-Stick ohne Schreibschutzschalter als Tails-Boot-Medium verwendet oder *b)* eine Tails-DVD nutzt, das DVD-Laufwerk aber zum Brennen von Daten in der Sitzung benötigt.

- ~~**truecrypt**~~ - diese Option gibt es wegen der Unsicherheit[22] von *TrueCrypt* seit Oktober 2014 nicht mehr! Ihr könnt lediglich noch *TrueCrypt* verschlüsselte Daten *entschlüsseln*. Dazu braucht ihr aber keine Boot-Option angeben. Ihr müsst lediglich beim Tails-Startbildschirm ein Passwort festlegen.Wie das geht, erläutert das nächste Kapitel. Alles weitere zum Thema *TrueCrypt* findet ihr im Kapitel „*Daten verschlüsselt aufbewahren*"

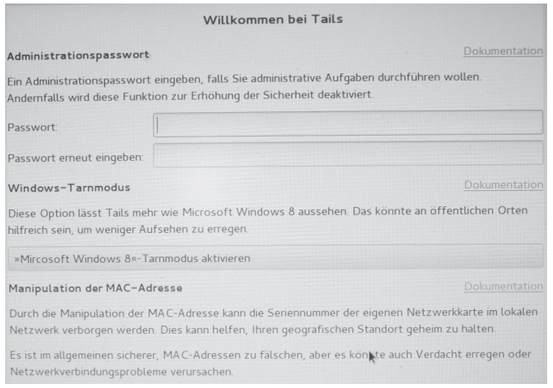
22 Die Bedenken gegen *TrueCrypt* sind im Kapitel *Daten verschlüsselt aufbewahren* nachzulesen.

Tails-Startbildschirm



Nach erfolgreichem Boot-Vorgang erscheint folgender Startbildschirm, bei dem ihr durch Auswahl der Option „*Deutsch*" (links unten) auf eine deutsche Tastaturbelegung und deutschsprachige Menüs umschalten könnt.

Durch die Auswahl *Ja* und *Vorwärts* bei „*weitere Optionen?*" habt ihr folgende weitere Start-Optionen:



- **Festlegen eines Administrations-Passworts** - das benötigt ihr, wenn ihr für ein Programm Administrator-Rechte braucht. Dies ist z.B. notwendig für das Installieren eines Druckers. Ihr könnt Euch im dann folgenden Dialog ein beliebiges Passwort ausdenken (und merken!). Es behält seine Gültigkeit nur für diese eine Tails-Sitzung.

- **Windows-Tarnung aktivieren** - gegenüber neugierigen Blicken sieht die Tails-Oberfläche dann auf den ersten Blick aus wie Windows.

- **Manipulation aller MAC-Adressen ausschalten**

Wenn der Netzzugang nur bestimmten Computern gewährt wird und ihr auf die zusätzliche Sicherheit einer geänderten MAC-Adresse verzichten könnt[23], könnt ihr das standardmäßig gesetzte Häkchen wegnehmen.

Nachdem ihr den Schalter *Anmelden* angeklickt habt, meldet sich Tails mit der grafischen Oberfläche und den zwei Hauptmenüs **Anwendungen, Orte.** Damit Tails erkennt, ob ihr eine veraltete Version benutzt, wird zu Beginn euerer Sitzung (nach erfolgreich hergestellter Netzwerk-Verbindung) einmal nach Hause telefoniert. Ihr werdet ggfs. aufgefordert, per *Upgrade* eine neue Version einzuspielen. Wie das geht, erläutern wir im Anhang im Kapitel *Tails-Installer* bzw. *Tails-Upgrader.*

Zur gleichzeitigen Arbeit mit mehreren Programmen sind vier Arbeitsflächen voreingestellt - damit es auf einem kleinen Bildschirm nicht zu voll wird. Per linkem Mausklick auf die vier kleinen Bildschirme unten rechts könnt ihr zwischen ihnen wechseln[24].

Datenträger werden nicht automatisch „geöffnet"

Anders als ihr es gewohnt seid, wird ein eingelegter/eingesteckter externer Datenträger nicht automatisch geöffnet und damit verfügbar gemacht. Ihr sollt damit (absichtlich) die Kontrolle über alle Datenorte behalten und nicht aus Versehen doch etwas auf die Festplatte speichern!

> ***Datenträger werden erst über das aktive Anwählen (linker Mausklick) unter „Orte ▸ Rechner" in das System eingebunden. Vorher können von/auf ihm keine Daten gelesen/gespeichert werden.***
>
> ***Bevor ihr den Datenträger nach fertiger Arbeit abziehen könnt, müsst ihr ihn unter „Orte ▸ Rechner" mit der rechten Maustaste anklicken und dann „Laufwerk sicher entfernen" wählen!***

Tails Programme

Das Tails-Live-System ist eine Zusammenstellung von vielen Programmen auf der Basis eines *Debian-Linux*. Alle Programme zu erläutern, erfordert viel zu viel Platz – selbst wenn wir nur deren grundlegende Handhabung beschreiben würden. Daher hier nur die Links zu Anleitungen für die wichtigsten Tails-Programme:

Surfen	Tor-Browser	https://tails.boum.org/doc/anonymous_internet/Tor_Browser/index.en.html
Mailen	Claws Mail	http://wiki.ubuntuusers.de/Claws_Mail
Chatten	Pidgin + OTR	https://tails.boum.org/doc/anonymous_internet/pidgin/index.en.html
Office	LibreOffice	http://wiki.ubuntuusers.de/LibreOffice
Layout+Satz	Scribus	http://www.scribus.net/
Videos abspielen	Totem	http://wiki.ubuntuusers.de/Totem
Grafikbearbeitung	Gimp	http://wiki.ubuntuusers.de/GIMP
Tonbearbeitung	Audacity	http://wiki.ubuntuusers.de/Audacity
Videobearbeitung	Pitivi	http://wiki.ubuntuusers.de/PiTiVi
Newsfeeds lesen	Liferea	http://wiki.ubuntuusers.de/Liferea
Metadaten entfernen	MAT	https://mat.boum.org/
Datenträger überschreiben	Wipe	http://wiki.ubuntuusers.de/wipe
Drucken	CUPS	http://wiki.ubuntuusers.de/GNOME_Druckerkonfiguration
Scannen	Simple scan	http://wiki.ubuntuusers.de/Simple_Scan
CD/DVD brennen	Brasero	http://wiki.ubuntuusers.de/Brasero
Passwort-verwaltung	KeepassX	http://wiki.ubuntuusers.de/KeePassX
Internet-verbindung	Network-manager	http://wiki.ubuntuusers.de/Network-Manager

Netzwerkverbindung herstellen

Tails sucht nach dem Start selbständig nach verfügbaren Netzwerkverbindungen. Wenn ihr beim Start von Tails ein Netzwerkkabel eingesteckt habt und euer LAN-Zugang nicht Passwort-geschützt ist, dann startet Tor automatisch. Der Aufbau eines Tor-Netzwerks mit der dazu notwendigen Synchronisation der Systemzeit dauert eine Weile – bei Erfolg erscheint die Meldung, *„Tor ist bereit. Sie haben jetzt Zugriff auf das Internet"* Ab jetzt werden alle Surf-, Chat-, Mail-Verbindungen durch das Tor-Netz geleitet.

Für eine (in der Regel Passwort-gesicherte) WLAN-Verbindung könnt ihr den Netzwerkmanager in der oberen Kontrollleiste anklicken oder über das Menü *Anwendungen ▸ Systemwerkzeuge ▸ Einstellungen ▸ Netzwerkverbindungen* auswählen und dann das Passwort eingeben.

Surfen über Tor

Wenn der Netzwerkmanager von Tails eine Netzwerkverbindung hergestellt hat, könnt ihr den Tor-browser starten. Entweder per Klick auf das Symbol in der Kontrolleiste oben links, oder im Menü:
Anwendungen ▸ Internet ▸ Tor-Browser.

Skripte verbieten – NoScript

Es gibt aktive Inhalte auf Webseiten, die eure Anonymität gefährden können. Oft nutzen Webseiten Javascript, Java-Applets, Cookies, eingebettete Flash- oder Quicktime-Filmchen, PDF-Dokumente oder nachzuladende Schriften. Derartige *aktive* Webseiteninhalte können über einen so genannten „Finger-Print" viele Einstellungen und Charakteristika eures Rechners übertragen (Prozessor, Bildschirmauflösung, installierte Schriften, installierte Plugins, etc.), sodass ihr im ungünstigen Fall doch identifizierbar seid. Die Tor-Installation von Tails kümmert sich um die Deaktivierung vieler dieser Inhalte. Wir empfehlen jedoch gleich zu Beginn eurer Netzaktivitäten eine noch restriktivere Einstellung in eurem Tor-Browser vorzunehmen:

> ***Mit dem NoScript-Button im Tor-Browser alle Skripte verbieten!***

Im voreingestellten Tor-Browser von Tails sind *Skripte* und *Plugins* zunächst erlaubt.

Mit der Option NoScript (Button in der Browser-Kontrollleiste) verbietet ihr zunächst alle! Skripte und jeden Plugin-Code global. Empfehlenswert ist, Skripte bei den besuchten Webseiten (und ihren Unterseiten) jeweils *erst dann* zuzulassen, wenn es für eure Aktivität notwendig ist- wenn also etwas auf der jeweiligen Webseite „nicht wie gewohnt funktioniert". Beachtet, dass ihr dadurch eure Anonymität verlieren könnt!

In Ausnahmefällen ohne Tor ins Netz ?

Einige öffentliche WLAN-Zugänge in Cafés, Universitäten, Büchereien, Hotels, Flughäfen, etc. leiten Webseitenanfragen um auf spezielle Portale, die ein *login* erfordern. Solche Zugänge sind nicht über Tor erreichbar.

> ***Wir raten dringend von der Nutzung des Browsers ohne Tor ab!***

Nur wenn ihr auf die Verschleierung eurer Identität und auf die Verschleierung eures Standortes verzichten wollt und könnt, gibt es in Tails die Möglichkeit auch ohne! Tor ins Netz zu gehen. Bedenkt, dass euch alles was ihr damit „ansurft", zugeordnet werden kann. Ihr könnt den unsicheren Browser starten über:
Anwendungen ▸ Internet ▸ Unsicherer Internet Browser.

> ***Auf keinen Fall solltet ihr diesen „nackten" Browser parallel zum anonymen Tor-Browser nutzen. Das erhöht die Angreifbarkeit und die Verwechselungsgefahr mit eventuell katastrophalen Konsequenzen!***

Daten verschlüsselt aufbewahren

Wie bereits erwähnt, Tails speichert nichts auf eurer Festplatte, es sei denn, ihr verlangt dies explizit durch die Auswahl der Festplatte im Menü *Orte ▸ [Name der Festplatte]*. Nach dem Ausschalten des Rechners gehen alle Daten verloren. Ihr solltet daher einen **Daten-USB-Stick** zur Aufbewahrung eurer Daten nutzen. Aus Sicherheitsgründen sollte dieser *nicht identisch mit dem* (möglichst schreibgeschützten) *Tails-Betriebssystem-Stick* sein!

Da wir grundsätzlich alle Daten verschlüsselt aufbewahren, legen wir auf einem neuen Daten-USB-Stick eine *verschlüsselte Partition* an. Tails nutzt die Linux-Verschlüsselungssoftware *dm-crypt*. Ihr könnt die Daten dann auf allen Linux-Betriebssystemen entschlüsseln. **Ein Datenaustausch mit Windows- oder MAC OS X Betriebssystemen ist damit allerdings nicht möglich!**

Verschlüsselte Partition auf einem Datenträger anlegen[25]

1. **Laufwerksverwaltung starten**
   Anwendungen ▸ Zubehör ▸ Laufwerksverwaltung
   Die Laufwerksverwaltung listet alle derzeit verfügbaren Laufwerke und Datenträger.

2. **Daten-USB-Stick identifizieren**
   Wenn ihr jetzt den neu zu verschlüsselnden USB-Stick jetzt einsteckt, sollte ein neues „Gerät" in der Liste auftauchen. Wenn ihr draufklickt seht ihr die Details des Datenträgers.

23 Bitte lest dazu die Hinweise im Kapitel T*ails ändert eure MAC-Adresse*.

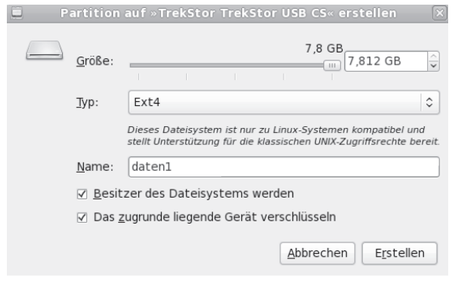
24 Der Wechsel zur jeweils nächsten Arbeitsfläche rechts/links erfolgt auch über die Tastenkombination STRG + ALT + (Pfeiltaste) → / ←.

25 Weiterführende Infos: https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.en.html

3. **USB-Stick formatieren**
Überprüft genau, ob die Beschreibung (Marke, Name, Größe) mit eurem Gerät übereinstimmt! Eine Verwechslung mit einem anderen Datenträger wird diesen löschen! ***Nur wenn alles übereinstimmt, klickt ihr auf*** *Laufwerk formatieren.* ***Alle existierenden Partitionen und damit*** **alle Daten darauf gehen verloren!**

Ihr werdet aufgefordert dies zu bestätigen.

4. **Eine verschlüsselte Partition erzeugen**
Klickt auf Partition erstellen. Nun erscheint ein Fenster, in dem ihr die neue Partition erstellen könnt.



- **Größe:** Ihr könnt die Größe der zu verschlüsselnden Partition auch verkleinern, damit noch andere Partitionen auf dem USB-Stick Platz finden. Wir raten euch jedoch, sensible Datenprojekte *nicht mit anderen Daten auf dem gleichen Stick* zu speichern.

- **Typ:** Ihr könnt die Einstellung des Dateisystems auf *Ext4* belassen.

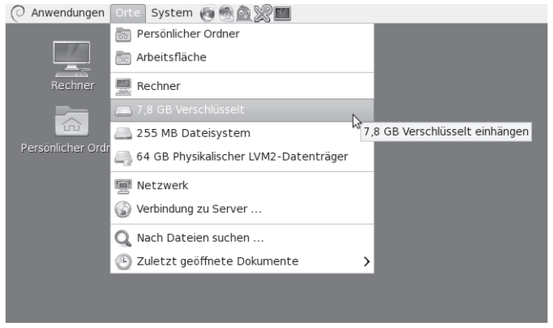
- **Name**: Hier könnt ihr einen Namen für den Datenträger wählen, um ihn später identifizieren zu können. Beachtet: Dieser Name ist für alle lesbar!

- **Das zugrunde liegende Gerät verschlüsseln:** Hier ein Häkchen setzen.

Nachdem ihr auf *Erstellen* klickt, werdet ihr nach einem Passwort gefragt. Dieses Passwort[26] sollte komplex genug sein, damit es nicht geknackt werden kann. Aber ihr müsst es euch auch merken können! Erneut *Erstellen* klicken. Dieser Prozess kann eine Weile dauern. Wenn die Fortschrittsanzeige erlischt, seid ihr fertig.

Verschlüsselte Partition öffnen

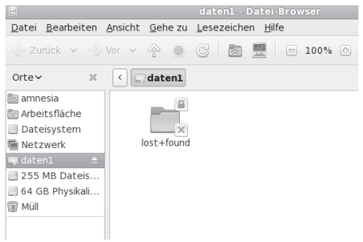
Wenn ihr einen verschlüsselten USB-Stick einsteckt, wird er (wie alle Datenträger) in Tails *nicht automatisch* geöffnet, sondern erst wenn ihr ihn im Menü *Orte* anwählt.



Ihr werdet aufgefordert, das Passwort einzugeben:

26 Hinweise zu einem sicheren Passwort im Anhang.

Wenn es das richtige Passwort ist, dann wird die Partition im Datei-Manager wie ein Datenträger angezeigt. Ihr könnt nun Dateien hinein kopieren oder sonstige Dateioperationen durchführen.



Bevor ihr den Datenträger nach fertiger Arbeit abziehen könnt, müsst ihr ihn unter *Orte* ▸ *Rechner* mit der *rechten Maustaste* anklicken und dann *Laufwerk sicher entfernen* wählen!

Bedenken gegen TrueCrypt

Obwohl die betriebssystem-unabhängige Alternative *TrueCrypt* auf freier Software basiert, gibt es starke Bedenken bezüglich deren Sicherheit - nicht nur wegen nicht mehr erfolgter Updates, sondern auch wegen der „geschlossenen" Entwicklung und der damit erschwerten Nachvollziehbarkeit für kritisch prüfende Sicherheitsfans[27]. Die im Mai 2014 erschienene letzte *TrueCrypt*-Version wird von den Entwickler*innen selbst als *nicht sicher(!)* eingestuft und erlaubt nur noch das Entschlüsseln bereits vorhandener *TrueCrypt*-Container.

Aus diesen Gründen rät Tails von dessen Nutzung dringend ab. Tails ermöglicht den Nutzer*innen seit Oktober 2014 lediglich das *Entschlüsseln* von *TrueCrypt*-verschlüsselter Dateien bzw. Datenträger. Ein *Verschlüsseln* mit *TrueCrypt* ist nicht mehr möglich.

Um nicht in die missliche Lage zu kommen, irgendwann die alten Datenträger nicht mehr entschlüsseln zu können, raten wir, zu sichernde *TrueCrypt*-verschlüsselte Inhalte zu entschlüsseln und umzukopieren auf *dm-crypt*-verschlüsselte Datenträger (erster Abschnitt dieses Kapitels).

27 Es wurde bislang keine „*Hintertür*" in *TrueCrypt* entdeckt. Das Zwischenfazit einer fortdauernden, unabhängigen Quellcode-Überprüfung vom April 2014 findet ihr hier: → Open Crypto Audit Project: TrueCrypt Security Assessment

TrueCrypt entschlüsseln

Solltet ihr trotz der zuvor dargelegten Bedenken TrueCrypt-Partitionen (Volumes) oder -Dateien (Container) zum betriebssystemübergreifenden Datenaustausch verwenden, bietet dm-crypt nur noch Möglichkeit zum **Lesen** der Partition bzw. des Datei-Containers. Dazu gibt es jedoch kein Programm mit einer grafischen Oberfläche. Ihr müsst ein sogenanntes *Root-Terminal* über *Anwendungen* ▸ *Zubehör* ▸ *Root-Terminal* öffnen (dazu müsst ihr beim Tails-Startbildschirm ein Passwort festlegen) und dann einige Linux-Kommandos eingeben. Die Anleitung dazu findet ihr in der Tails-Dokumentation unter *Opening TrueCrypt volumes using cryptsetup.*

Identifikation von externen Datenträgern

Jeder externe Datenträger *(Festplatte, USB-Stick oder SD-Karte)* wird von der Laufwerksverwaltung des Betriebssystems (Linux, Windows und auch MAC OS X) identifiziert und registriert. Die Nutzung eines solchen Datenträgers unter Tails hinterlässt KEINE Spuren, da alle Protokoll-Dateien beim Ausschalten des Rechners aus dem (flüchtigen) Arbeitsspeicher verschwinden und dieser zusätzlich mit Zufallszahlen überschrieben wird, aber:

> ***Wenn ihr einen Datenträger (auch) an einem Rechner OHNE Tails benutzt, dann wird sich dieser Rechner über eine eindeutige Identifikationsnummer an diesen Datenträger „erinnern".***

Bei einer Beschlagnahmung des Rechners bzw. einer feindlichen Übernahme lässt sich damit nachvollziehen, dass und wann z.B. ein bestimmter USB-Stick zum Einsatz kam[28]. Die eindeutig identifizierbaren Spuren in den System-Protokolldateien „verbinden" also euren USB-Stick mit allen Rechnern in denen er jemals gesteckt hat. Wir erzählen das, weil wir damit deutlich machen möchten:

> ***Datenträger, die zum Speichern eines sensiblen Dokuments benutzt wurden, müssen (z.B. nach dessen Veröffentlichung) vollständig gelöscht und vernichtet werden.***

Wie das geht, erfahrt ihr im nächsten Kapitel.

28 Umgekehrt gilt das nicht: Ein (nicht gehackter) USB-Stick merkt sich nicht, in welche Rechner er gesteckt wurde.

Daten löschen

Es ist leider sehr kompliziert, einmal erzeugte Daten „sicher“ loszuwerden. Alle wissen vermutlich, dass es mit dem normalen Löschen einer Datei nicht getan ist – die Datei bleibt vollständig erhalten, ihr Name wird lediglich aus der Liste verfügbarer Dateien auf diesem Datenträger ausgetragen. Der belegte Platz wird freigegeben, aber nicht überschrieben.

Leider führen aber auch Software-Techniken, die einzelne Bereiche eines Datenträgers mit verschiedenen Datenmustern mehrfach überschreiben, z.B. bei USB-Sticks nicht zum gewünschten Ergebnis! Für Ungeduldige auch hier gleich das Ergebnis unser Ausführungen vorweg:

> ***Die sicherste Variante ist, Daten nur (temporär) im Arbeitsspeicher zu halten!***
>
> ***Wenn Daten dauerhaft gesichert werden müssen, dann muss es a) ein externer Datenträger sein und dieser muss b) komplett verschlüsselt sein. Ein sicher verschlüsselter Datenträger ist der beste Schutz gegen (lesbare) Überreste.***
>
> ***Sämtliche Löschprgramme wie z.B. „wipe“ sind c) zusätzlich nur brauchbar beim Überschreiben des gesamten Datenträgers. Datenträger mit hochsensiblem Inhalt zerstören wir d) zusätzlich.***

Probleme beim Überschreiben von Datenträgern

Physikalische Eigenschaften der Datenträger erlauben es, den ehemaligen Inhalt einer überschriebenen Speicherstelle zu rekonstruieren. Wir ersparen euch hier Details und erläutern lieber, warum es dabei weniger um die Anzahl der Überschreibvorgänge geht!

Bei **magnetischen Festplatten** gibt es das Problem, dass defekte Sektoren (=Speicherbereiche) von der Festplattensteuerung aussortiert werden und ehemals dort gespeicherte Daten umkopiert werden. Ein Überschreib-Programm zum „sicheren“ Löschen hat dann auch keinen Zugriff mehr auf diese defekten Sektoren. Im Forensik-Labor hingegen lassen sich diese Bereiche auslesen – mit unter Umständen fatalen Folgen für euch.

Bei sogenannten Flash-Speichermedien, wie z.B. **USB-Sticks, SD-Karten, CompactFlash-Karten und die neueren SSD-Festplatten (Solid-State-Disks)** ist dieses Problem des internen Umkopierens (außerhalb der Kontrolle des Anwenders) wegen der besonders hohen Fehleranfälligkeit des Speichers kein Ausnahmefall, sondern die Regel[29]. Eine Überschreibeprozedur zum „sicheren“ *Löschen einzelner Dateien* „erwischt“ dann nur eine von mehreren Kopien. Eine der neueren Forschungsarbeiten bescheinigt sämtlichen Software-Löschtechniken, dass sie angewendet auf Flash-Speicher selbst beim **Überschreiben des gesamten Speichermediums nur unzuverlässig** funktionieren[30]. **Das sichere Löschen von einzelnen Dateien hingegen gelang mit keinem der getesteten Programme!**

Mit diesen Einschränkungen (als dringliche Warnung) zeigen wir euch, wie ihr bei Tails die Löschroutine *wipe* **zum Überschreiben des gesamten Datenträgers** nutzen könnt:

1. ***Datenträger im Dateimanager auswählen:*** *Orte* ► *(Name des Datenträgers)*
2. ***Im Dateimanager bei*** *Ansicht* ► *Verborgene Dateien anzeigen* ***ein Häkchen setzen***
3. ***Alle Ordner und Dateien markieren***
4. *(rechter Mausklick)* ► *wipe*
   (Die Dateien sind *für euch* ***unwiderruflich weg!)***
5. ***Im (danach leeren) Feld dieses Datenträgers:*** *(rechter Mausklick)* ► *wipe available diskspace*
6. ***Drei Durchläufe bei*** **zweifachem Überschreiben** ***(also sechsfach) genügen bei neueren Datenträgern - bei Unsicherheit und bei alten Festplatten könnt ihr*** *38-faches Überschreiben* ***wählen.***
7. ***Warten – je nach Größe des Datenträgers einige Minuten bis viele Stunden.***

Datenträger vernichten

Gerade wegen der Unzulänglichkeit vieler Software-Löschtechniken und der weitgehenden Möglichkeiten von forensischer Daten-Wiederherstellung solltet ihr sensible Datenträger lieber zusätzlich zerstören. Auch das ist leider problematischer als gedacht - optische Medien sind am einfachsten zu zerstören.

29 Zur ausgewogenen Belastung der Speicherstellen werden Bereiche ständig umkopiert. Mehr als zehn versteckte Kopien einer Datei sind keine Seltenheit bei Flash-Speicher.

30 Michael Weie et. al.: „Reliably Erasing Data From Flash-Based Solid State Drives“ 9th USENIX Conference on File and Storage Technologies. „For sanitizing entire disks, built-in sanitize commands are effective when implemented correctly, and software techniques work most, but not all, of the time. We found that none of the available software techniques for sanitizing individual files were effective.“ http://static.usenix.org/event/fast11/tech/full_papers/Wei.pdf

Magnetische Festplatten sind sehr schwer zu zerstören. Ihr könnt sie nicht einfach ins Feuer werfen. Die Temperaturen, die ihr damit an den Daten-tragenden Scheiben (Aluminium mit Schmelzpunkt 660°C oder Glas wird zähflüssig >1000°C) erreicht, ermöglichen gerade mal eine leichte Verformung. Ein Aufschrauben des Gehäuses und der Ausbau der Scheiben ist mindestens notwendig, um mit einem Lötbrenner an der Scheibe selbst höhere Temperaturen zu erzeugen. Ein Campinggas-Lötbrenner reicht dazu jedoch nicht aus. Ein Zerbrechen der Scheiben in kleine Stücke und verteilter Entsorgung ist zumindest ein „Ausweg“ – wegen der hohen Datendichte könnten Forensiker darauf jedoch noch reichlich Datenfragmente finden! Alternativ könnt ihr die Oberfläche, der einzelnen Scheiben mit einer Bohrmaschine und Drahtbürstenaufsatz abschleifen.

Flash-Speicher (USB-Sticks, SSD, SD-Karten, ...) lässt sich ebenfalls nur unvollständig zerstören. Mit zwei Zangen könnt Ihr die Platine aus dem Gehäuse herausbrechen, um dann die Speicherchips samt Platine einzeln in Stücke zu brechen und in die Flamme eines Campinggas-Lötbrenner zu halten. Ihr erreicht auch hierbei nur eine partielle Zersetzung des Transistor-Materials. Vorsicht – Atemschutz oder Abstand! Die Dämpfe sind ungesund.

Optische Medien (CD, DVD, Blueray) lassen sich mit genügend großer Hitze vollständig und unwiderruflich zerstören. Das Trägermaterial Polycarbonat schmilzt bei 230°C (Deformation). Die Zersetzung gelingt bei 400°C und bei 520°C brennt es. Ein Campinggas-Lötbrenner reicht aus, die Scheiben aus Polycarbonat, einer dünnen Aluminiumschicht und einer Lackschicht zu Klump zu schmelzen oder gar zu verbrennen. Vorsicht – Atemschutz oder Abstand! Die Dämpfe sind ungesund. Alternative ist die Zerstörung des Datenträgers in der Mikrowelle (wenige Sekunden auf höchster Stufe)

Metadaten entfernen

Die meisten von euch kennen das Problem bei Fotos von Aktionen. Bevor diese veröffentlicht werden können, müssen nicht nur Gesichter unkenntlich gemacht werden[31], sondern auch die sogenannten Metadaten entfernt werden, die im Bild mit abgelegt sind und die Kamera, mit der das Bild aufgenommen wurde, eindeutig identifizieren. Neben der Uhrzeit und der Seriennummer sind bei einigen neueren Kameras (insbesondere Smartphones) sogar die GPS-Koordinaten in diesen sogenannten *EXIF*-Daten abgespeichert. Ein sogenanntes *Thumbnail* (Vorschau-Foto im Kleinformat) kann Bilddetails preisgeben, die ihr im eigentlichen Bild verpixelt oder anderweitig unkenntlich gemacht habt. Diese Metadaten müssen entfernt werden!

Leider tragen z.B. auch LibreOffice-/Worddokumente und PDF-Dateien Metadaten in sich. Anwendername, Computer, Schriftarten, Namen und Verzeichnisorte eingebundener Bilder, … lassen Rückschlüsse auf euch bzw. euren Rechner zu.

Tails hat dazu eine umfassende Reinigungssoftware an Bord. Das **Metadata Anonymisation Toolkit** (**MAT**)[32] kann folgende Datentypen säubern: *PNG*- und *JPEG*-Bilder, *PDF*-Dokumente, *LibreOffice* und *Microsoft Office* Dokumente, *MP3* und *FLAC* (Audio-) Dateien und *TAR*-Archivdateien.

Anwendungen ► *Zubehör* ► *Metadata Anonymisation Toolkit.*

Das Programm ist nahezu selbsterklärend:

Öffnet ein Dateimanager-Fenster, über das ihr die zu checkenden / säubernden Dateien hinzufügen könnt.

Überprüft, ob die angewählten Dateien sauber oder dreckig sind.

Die angewählten Dateien werden bereinigt und unter dem gleichen Namen wie die Originaldatei abgelegt. Ihr könnt dieses Werkzeug auch auf ganze Ordner anwenden. Bedenkt, dass die Originaldatei auf DIESEM DATENTRÄGER immer noch rekonstruierbar ist!

Beachtet, dass MAT z.B. bei Text-Dokumenten nicht gesichert *alle Merkmale* aus den Dokumenten entfernen kann. Wasserzeichen oder andere mitunter versteckte Kennungen bleiben erhalten. Grundsätzlich gilt:

> *Je größer das Sicherheitsbedürfnis, desto simpler sollte das Datenformat sein, das ihr für die Übermittlung wählt.*

Reines Textformat verrät am wenigsten über den Rechner, an dem der Text erstellt wurde. Beachtet, dass der *Name eines Dokuments* unter Umständen ebenfalls Rückschlüsse auf die Autor*in oder deren Rechner zulässt.

31 Zur Grafikbearbeitung könnt ihr das Programm GIMP verwenden.

32 https://mat.boum.org/

Mailen über Tor

Webmail

Die einfachste Methode in Tails Emails zu versenden und zu empfangen ist der Zugriff (über *Tor*) auf ein *Webmail-Konto*. Wurde das Mail-Konto anonym angelegt, lässt sich darüber die eigene *Identität* verschleiern. Andernfalls könnt ihr immerhin euren *Aufenthaltsort* verschleiern.

Für alle, die **verschlüsselten Mail-Text per Webmail** verschicken wollen, stellen wir im folgenden zwei Methoden der PGP-Verschlüsselung vor.

> ***Warnung: Es ist unsicher, vertraulichen Text direkt in einen Webbrowser einzugeben, da Angreifer mit JavaScript aus dem Browser heraus darauf zugreifen können.***
>
> ***Ihr solltet euren Text daher mit dem* Tails OpenPGP Applet *verschlüsseln, und den verschlüsselten Text in das Browserfenster einfügen. Ihr müsst zusätzlich alle Skripte über NoScript verbieten!***

A) PGP-Verschlüsselung mit öffentlichem Schlüssel

Bei dieser Methode nutzt ihr die sehr sichere Standard-PGP-Verschlüsselung: Verschlüsseln mit den öffentlichen Schlüsseln der Empfänger. Falls ihr noch nie mit PGP gearbeitet habt, könnt ihr Methode B) verwenden.

1. Schreibt euren Text in einen Texteditor, *nicht direkt in das Browserfenster eures Webmail-Anbieters!* Zum Beispiel könnt ihr dazu *gedit* öffnen über *Anwendungen ► Zubehör ► gedit Text Editor*.

2. Markiert dort den zu verschlüsselnden oder zu signierenden Text mit der Maus. Um ihn in die Zwischenablage zu kopieren, klickt ihr mit der rechten Maustaste auf den markierten Text und wählt den Menüpunkt *Kopieren* aus. Das Tails OpenPGP Applet zeigt durch Textzeilen an, dass die Zwischenablage *unverschlüsselten Text* enthält.

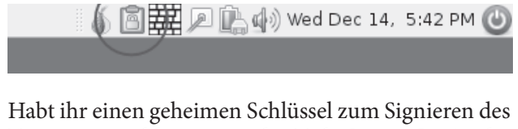
3. Klickt auf das Tails *OpenPGP-Applet (in der Tails-Menüleiste oben rechts)* und wählt die Option **Zwischenablage mit öffentlichem Schlüssel signieren/verschlüsseln** aus. Sollte die Fehlermeldung *„Die Zwischenablage beinhaltet keine gültigen Eingabedaten.“* angezeigt werden, versucht erneut den Text gemäß Schritt 2 zu kopieren.

4. Falls ihr den Text verschlüsseln wollt, wählt einen oder mehrere öffentliche Schlüssel für die Empfänger des verschlüsselten Textes im *„Schlüssel wählen“*-Dialog aus *(siehe dazu das Kapitel PGP-Schlüssel importieren).*

5. Falls ihr den Text signieren wollt, wählt den geheimen Schlüssel aus der *„Nachricht signieren als“*-Dropdown-Liste aus. Bedenkt, dass der Besitz dieses Schlüssels die Urheber*innenschaft der so signierten Mail schwer abstreitbar macht.

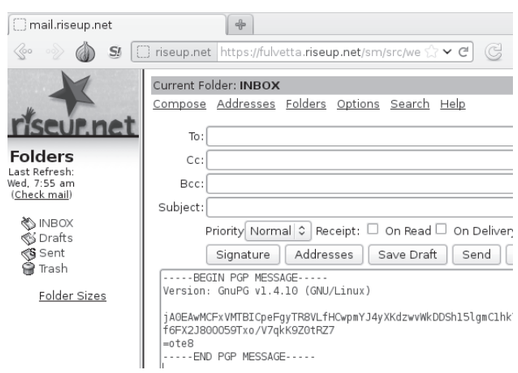
6. Klickt auf *OK*. Falls die Frage *„Vertrauen Sie diesen Schlüsseln?“* angezeigt wird, beantwortet dies entsprechend.

7. Falls ihr einen oder mehrere öffentliche Schlüssel zum Verschlüsseln des Texts ausgewählt habt, zeigt das Tails OpenPGP Applet durch ein *Vorhängeschloss* an, dass die Zwischenablage nun verschlüsselten Text enthält.



Habt ihr einen geheimen Schlüssel zum Signieren des Texts ausgewählt, so zeigt das Tails OpenPGP Applet nun durch ein *Siegel* an, dass die Zwischenablage signierten Text enthält.

8. Um den verschlüsselten oder signierten Text in das Webmail-Fenster eures Mail-Anbieters (oder eine andere Anwendung) einzufügen, klickt mit der *rechten Maustaste* auf das Eingabefeld, in das ihr den Text einfügen möchten, und wählt die Option *Einfügen* aus dem Menü aus.



B) PGP-Verschlüsselung mit Passphrase

Bei dieser Methode müsst ihr eine geheime Passphrase mit den Personen teilen, die die Nachricht entschlüsseln sollen. *Ihr müsst die Passphrase also zuvor über einen sicheren Kanal (im günstigsten Fall face-to-face) kommunizieren!*

Die beiden ersten Schritte sind identisch mit 1. und 2. aus Methode A). Dann geht es weiter mit:

1. ***Klickt auf das Tails OpenPGP Applet und wählt die Option* Zwischenablage mit Passwort verschlüsseln *aus. Sollte die Fehlermeldung „Die Zwischenablage beinhaltet keine gültigen Eingabedaten.“ angezeigt werden, versucht erneut den Text gemäß Schritt 2 zu kopieren.***

2. ***Gebt eine Passphrase in den* Passphrase *Dialog ein. Wiederholt die gleiche Passphrase im zweiten Dialog.***

3. ***Das Tails OpenPGP Applet zeigt durch ein Vorhängeschloss an, dass die Zwischenablage verschlüsselten Text enthält.***

4. ***Dieser Schritt ist identisch mit Schritt 8 aus Methode A).***

Entschlüsseln oder Signatur überprüfen

Die Entschlüsselung eines verschlüsselten Textes / einer verschlüsselten Mail funktioniert *für beide Verschlüsselungs-Methoden* folgendermaßen:

1. ***Markiert mit der Maus den verschlüsselten bzw. signierten Text (z.B. in eurem Webbrowser), den ihr entschlüsseln bzw. überprüfen möchtet. Schließt die Zeilen “-----BEGIN PGP MESSAGE-----“ und “-----END PGP MESSAGE-----” mit in die Markierung ein.***

2. ***Ist der ausgewählte Text verschlüsselt, zeigt dies das Tails OpenPGP Applet durch ein* Vorhängeschloss *an. Ist der ausgewählte Text nur signiert, aber nicht verschlüsselt, wird dies durch ein* Siegel *im Tails OpenPGP Applet angezeigt.***

3. ***Klickt auf das Tails OpenPGP Applet und wählt* Zwischenablage entschlüsseln/überprüfen *aus dem Menü aus.***

   - Ist der ausgewählte Text nur signiert und die Signatur gültig, erscheint direkt das GnuPG-Ergebnis Fenster.
   - Ist der Text signiert, aber die Signatur ungültig, wird das GnuPG-Fehler Fenster mit der Nachricht *FALSCHE Unterschrift von...* angezeigt. Ihr könnt euch nicht sicher sein, dass der angegebene Absender auch der tatsächliche ist.
   - Ist der Text **mit einer Passphrase** verschlüsselt, erscheint die Aufforderung *Geben Sie die Passphrase ein...*, danach auf OK klicken.
   - Ist der Text *mit einem öffentlichen Schlüssel verschlüsselt* worden, können zwei verschiedene Dialoge angezeigt werden:
     - Ist die Passphrase zu einem geheimen Schlüssel noch nicht zwischengespeichert, dann erscheint ein Dialog mit der Nachricht: *Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren*. Gebt die Passphrase für diesen geheimen Schlüssel ein, danach auf *OK* klicken.
     - Falls sich kein zum verschlüsselten Text passender geheimer Schlüssel im Schlüsselbund befindet, wird die GnuPG Fehlermeldung *Entschlüsselung fehlgeschlagen: Geheimer Schlüssel ist nicht vorhanden* angezeigt.
   - Ist die Passphrase falsch, so wird ein *GnuPG-Fehler* Fenster mit der Meldung *Entschlüsselung fehlgeschlagen: Falscher Schlüssel* angezeigt.
   - Ist die Passphrase korrekt, oder ist die Signatur auf den Text gültig, so wird das *GnuPG-Ergebnis*-Fenster angezeigt.
   - **Der entschlüsselte Text erscheint im Textfeld Ausgabe von GnuPG.** Im Textfeld *Andere Nachrichten von GnuPG* zeigt die Nachricht *„Korrekte Unterschrift von...“* an, dass die Signatur gültig ist.

PGP-Schlüssel importieren

Da Tails über die aktuelle Sitzung hinaus keinerlei Daten speichert, müsst ihr für die Verschlüsselung mit Methode A bzw die Entschlüsselung zunächst einen PGP-Schlüssel von einem (hoffentlich verschlüsselten!) Datenträger importieren.

> ***Ihr solltet niemals private PGP-Schlüssel auf einem unverschlüsselten Datenträger speichern!***

Klickt dazu auf das Tails *OpenPGP-Applet (in der Tails-Menüleiste oben rechts)* und wählt die Option **Schlüssel verwalten.** Es öffnet sich die Passwort und Schlüsselverwaltung von Tails. Hier könnt ihr unter *Datei ► Importieren* einen verfügbaren Datenträger und dort den gewünschten Schlüssel auswählen. Beachtet, dass ihr zum **Entschlüsseln** *euren privaten PGP-Schlüssel* benötigt. Zum

Verschlüsseln (mit Methode A) benötigt ihr hingegen den *öffentlichen Schlüssel des Empfängers*.

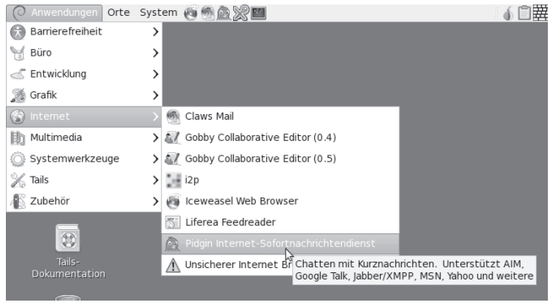
Ab jetzt stehen euch die so importierten PGP-Schlüssel bis zum Ende der Tails-Sitzung (also bist zum Herunterfahren des Rechners) zur Verfügung.

Chatten über Tor

Pidgin ist der Name des Chatclients, der bei Tails mitgeliefert wird. Im Vergleich zu einer Pidgininstallation unter einem „normalen" Linux ist das Pidgin von Tails speziell auf Verschlüsselung abzielend vorkonfiguriert.

Es wird nur eine limitierte Auswahl an Chatprotokollen angeboten: Varianten von *XMPP* und *IRC*. Für diese beiden Protokolle stehen Verschlüsselungsmethoden bereit, die anderen Protokollen fehlen. Die Voreinstellungen, die die Tails-Variante von Pidgin mitbringt, deaktivieren das *logging*, also das Mitprotokollieren von Sitzungen. Auch mitinstalliert ist das OTR-Plugin, welches eine Ende-zu-Ende Verschlüsselung erlaubt[33].

Für den einmaligen Einsatz muss nichts weiter vorbereitet werden. Pidgin bei Tails kommt mit zwei vorkonfigurierten (zufälligen) Accounts daher, die direkt verwendet werden können. Für den regelmässigen Einsatz (mit eigenem Account) müsstet ihr Pidgin wegen der Vergesslichkeit von Tails jedes Mal neu konfigurieren, oder die privaten Schlüssel auf einem Datenträger sichern.



Pidgin findet sich unter *Anwendungen* ► *Internet* ► *Pidgin Internet-Sofortnachrichtendienst*.

Wenn Pidgin startet, zeigt es die sogenannte *Buddylist*, das ist soetwas wie ein Adressbuch. Nach dem ersten Start muss (mindestens) ein *Chat-Account* angelegt werden (das ist vergleichbar mit einer Email-Adresse) - es sei denn ihr benutzt einen der beiden vorkonfigurierten Accounts.

Im Menü *Konten* ► *Konten verwalten* aufrufen. Zum Anlegen eines neuen Accounts auf „*Hinzufügen*" klicken. Hier die Daten des Chataccounts eintragen. Pidgin hat

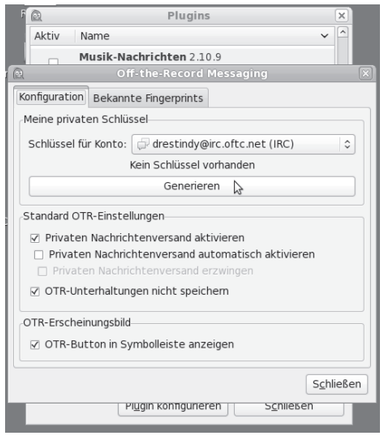
die Besonderheit, dass ein Chat-Account *name@jabber.server.org* getrennt eingetragen werden muss: „*name*" kommt in das Feld „*Benutzer*" und *jabber.server.org* in das Feld „*Domain*". Der Rest kann leer gelassen werden.

Verschlüsselte Sitzung

OTR verwendet das gleiche Schema wie auch PGP für seine Schlüssel: Es gibt einen öffentlichen und einen privaten. Es empfiehlt sich, dieses Schüsselpaar explizit zu erzeugen – Pidgin macht das zwar auch bei der erstmaligen Benutzung von OTR, was leider nicht immer fehlerfrei funktioniert (Bug).

> ***Chatsitzungen von Pidgin sind beim Start nicht verschlüsselt – das Erste, was also (für jede Chatsitzung) gemacht werden muss, ist die „Private Unterhaltung" zu starten! Damit ist eine Ende-zu-Ende Verschlüsselung via OTR gemeint.***

Im Menü „*Werkzeuge*" von Pidgin den Punkt „*Plugins*" auswählen, in der Dialogbox den Punkt „*OTR*" finden und auswählen, danach unten auf „*Plugin konfigurieren*"

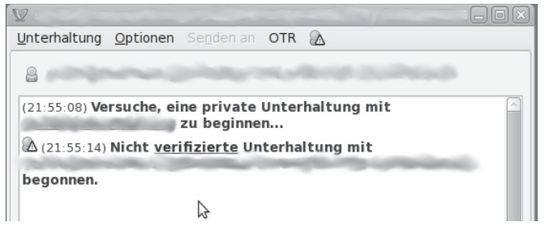


33 *OTR*: Off The Record – Ausdruck, der in Gesprächen signalisiert, dass das jetzt Gesagte nicht zitiert werden darf. Mehr zu OTR: https://otr.cypherpunks.ca/

klicken. In der folgenden Dialogbox den Button „*Generieren*" klicken – vorher aber den richtigen Account aus dem darüberliegenden Popup-Menü wählen. (Im Screenshot ist einer der vorinstallierten Accounts angezeigt.)

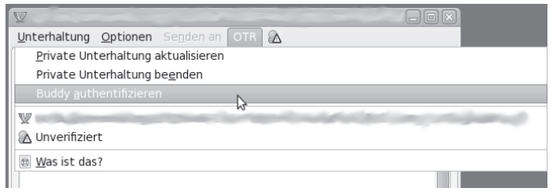
Nach der Auswahl des Menüpunktes „*Private Unterhaltung*" startet eine verschüsselte Sitzung.

Tippt sensible Inhalte erst nach dem Erscheinen der Meldung „*Unterhaltung mit ... begonnen*". Erst ab dieser Stelle wird alles, was in dieser Sitzung geschrieben wird, verschlüsselt übertragen.



Was auf dem Screenshot allerdings sichtbar wird ist, dass das Gegenüber nicht verifiziert ist - sprich, **es ist nicht sicher, dass das Gegenüber die Person ist, für die sie sich ausgibt.**

Echtheit des Gegenübers verifizieren



Um Zweifel auszuschliessen, enthält Pidgin mehrere Methoden das Gegenüber zu identifizieren. **Es stehen drei Methoden zu Verfügung:**

- **Frage und Antwort:** Die Idee hinter dieser Methode ist, dass euer Gegenüber die Frage nur dann richtig beantworten kann, wenn sie die richtige Person ist. Fragen wie „Wie lautet mein Nachname" scheiden also aus, da die Antwort erraten werden kann. Vorteil dieser Methode ist, dass ihr euer Gegenüber nicht vorher getroffen haben müsst, um ein entsprechendes Frage/Antwort-Paar vereinbart zu haben. Nachteil ist, dass eine entsprechende

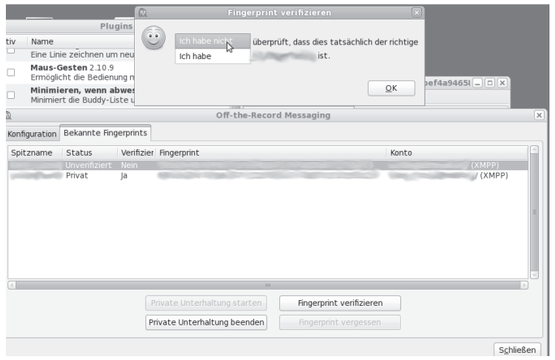
Frage mit nicht oder schwer erratbarer Antwort nicht leicht zu finden ist. Auf der anderen Seite sieht es dann so aus:

- **Gemeinsam bekannte Passphrase:** Einfacher ist es da schon, über einen sicheren Kanal ein gemeinsames „Passwort" oder gleich einen ganzen Satz zu vereinbaren. Dieser muss natürlich geheim bleiben.

- **Manueller Fingerprint-Vergleich:** Mit dieser Methode werden die öffentlichen Schlüssel direkt miteinander vergleichen - ihr habt den Fingerabdruck des öffentlichen Schlüssels eures Gegenübers und diese*r natürlich auch (ist ja ihr eigener). Sind die Abdrücke gleich, dann sind auch die öffentlichen Schlüssel gleich. Mit der Methode lässt sich ausschliessen, dass jemand in der Mitte der Verbindung sitzt und beiden Seiten vorspielt, die jeweils andere Seite zu sein.

Am sichersten, aber wohl auch am umständlichsten, ist der *Fingerprint*-Vergleich. Die beiden anderen Verfahren haben entweder das Problem, ein gemeinsames Geheimnis sicher auszutauschen oder aber eine nicht erratbare Antwort auf eine Frage zu entwerfen. Von der Frage/Antwort-Variante raten wir also ab, es sei denn, diese sind über einen sicheren Kanal vereinbart worden.

Hier der Fingerprintvergleich als Screenshot, am Ende des Vergleichs wird das Ergebnis gespeichert, sodass der Vergleich nur einmal notwendig ist.



An dieser Stelle die Anmerkung, dass gespeicherte Fingerprints (ob überprüft oder nicht) ein Beleg für einen Kommunikationsvorgang sind und sich darüber ein Abbild eines soziales Netzes (wer kennt wenn, wer kommuniziert mit wem) ansammelt. Überlegt Euch, ob es euch das Wert ist - die Alternative wäre allerdings ein erneutes Überprüfen der Fingerprints bei jeder Sitzung, und wenn ihr die Schlüssel von OTR nicht speichert, sind auch die jedesmal neu mit entsprechend neuem Fingerprint.

Aktionsfotos bearbeiten

Bild öffnen

Ihr startet das Grafik-Programm *Gimp* unter *Anwendungen ► Grafik ► GNU Image Manipulation Program* und wählt euer Bild unter *Datei ► Öffnen* aus.

Bild skalieren

Heutige Digital-Kameras machen Fotos mit weit über zehn Megapixel Bildauflösung. Das kann für Plakate und Broschüren sinnvoll sein, ist aber für eine digitale Veröffentlichung z.B. bei *indymedia* oder eine Verschickung per Mail unnötig groß. Um das Bild kleiner zu machen, wählt ihr in *Gimp* die Funktion *Bild ► Bild skalieren*. Der Dialog zur Einstellung einer neuen Breite und Höhe ist selbsterklärend. Wenn ihr Breite und Höhe „verkettet“ lasst, ändert sich das Seitenverhältnis des Bildes nicht. Eine Breite von z.B. 800 Pixel für ein Bild im Querformat ist für die meisten Internetzwecke ausreichend. Ihr beendet den Dialog mit dem Button „*Skalieren*“.

Bild-Bereiche unkenntlich machen

Ihr wählt im „Werkzeugkasten“ das Werkzeug „Rechteckige Auswahl“ und markiert einen Bereich, den ihr unkenntlich machen wollt. Der Bereich ist nun von einer laufenden gestrichelten Linie gerahmt. Ihr wählt *Filter ► Weichzeichnen ► Verpixeln* als eine Möglichkeit, den Informationsgehalt dieses Bildbereichs tatsächlich zu reduzieren. In der Vorschau seht ihr das Verpixelte Ergebnis.

Ihr könnt die Pixelgröße einstellen und danach mit „*OK*“ bestätigen. Mit der Wiederholung dieser Prozedur könnt ihr viele Bereiche (in denen z.B. Gesichter oder andere identifizierende Merkmale, wie z.B. Tatoos oder Schuhe zu sehen sind) unkenntlich machen.

Wenn ihr mit manchen Resultaten nicht zufrieden seid, lassen sich die Operationen Schritt für Schritt rückgängig machen mit der Funktion *Bearbeiten ► Rückgängig*.

Bild speichern

Dazu wählt ihr in *Gimp* die Funktion *Datei ► Exportieren* und gebt einen Namen für das zu speichernde Bild an (zum Beispiel *1.jpg*). Abhängig vom so gewählten Dateiformat (hier *jpg*) könnt ihr in diesem Dialogfenster noch die Qualität des zu speichernden Bildes beeinflussen (100 bedeutet keine Kompression, also hohe Detailgenauigkeit aber auch größere Datei). Zum Abschluss klickt ihr auf „*Exportieren*“.

Beachtet, dass das bearbeitete Bild wie im Kapitel „*Metadaten entfernen*“ beschrieben, bereinigt werden muss, um Metadaten wie z.B. die Kamera-Seriennummer und unverpixelte Vorschaubildchen zu entfernen!

Drucken

Zum Drucken den Drucker per USB-Kabel anschließen, anschalten und danach den Druckmanager unter *Anwendungen ► Systemwerkzeuge ► Systemverwaltung ► Drucken* starten. Dort *Server ► Neu ► Drucker* auswählen und den (hoffentlich erkannten) Druckernamen mit „*Vor*“ bestätigen.

Nun müsst ihr in der (lokal vorhandenen) Datenbank einen Druckertreiber finden. Dazu wählt ihr zunächst den Druckerhersteller und dann ein Modell, was eurem möglichst ähnlich ist. Häufig ist es ausreichend, das nächst ältere Modell samt dem vom Manager empfohlenen Treiber auszuwählen, falls ihr euer Druckermodell nicht findet. Ihr bestätigt die Wahl abschließend mit „*Anwenden*“ und könnt eine „*Testseite drucken*“.

Hinweis: Ein eventuell schon vor der Druckerinstallation geöffnetes Programm (z.B. OpenOffice) muss erneut gestartet werden, um den „neuen“ Drucker zu erkennen und für den Druck anzubieten.

Wer mehrfach den gleichen Drucker benutzt, kann sich die Installation am Anfang einer jeden Tails-Sitzung erleichtern, in dem er im Netz nach einem passenden Linux-Druckertreiber sucht. Die so heruntergeladene *.ppd-Datei* kann auf einem Datenstick dauerhaft gespeichert und anstelle der Suche in der lokalen Treiber-Datenbank angegeben werden.

Beachtet, dass ein Ausdruck über das spezifische Druckbild bei einer forensischen Untersuchung eindeutig einem einzelnen Drucker (nicht nur einem Druckertyp!) zugeordnet werden kann. Manche *Farbdrucker* hinterlassen zur Identifikation eine Kennung aus Einzelpunkten, die mit dem Auge nicht zu identifizieren ist[34]. Es handelt sich hierbei um unsichtbare Wasserzeichen, die einem Drucker eindeutig zugeordnet werden können *(machine identification code (mic))*.

Das bedeutet für eine sensible Print-Veröffentlichung, dass ihr preiswerte „Wegwerf“-Schwarzweiß-Drucker benutzen müsst. Wer durch anschließendes mehrfaches Kopieren (mit unterschiedlichen Kontraststufen) das Druckbild des Druckers verschleiern will, sollte beachten, dass fast alle Copy-Shops digitale Kopierer einsetzen, die mit einer großen Festplattenkapazität auch noch nach Wochen auf die einzelnen Druckaufträge inklusive exaktem Datum zugreifen können.

Scannen

Zum Scannen den Scanner per USB-Kabel anschließen, anschalten und danach das Programm „*Simple Scan*“ unter *Anwendungen ► Grafik ► Simple Scan* starten. Einfache (einseitige) Scanner funktionieren oft erst dann korrekt, wenn ihr im Programm unter *Dokument ► Einstellungen ► Scan Side* auf „*Front*“ setzt. Falls gewünscht könnt ihr die Scan-Auflösung für Fotos bzw. Text verändern. Dann könnt ihr die Einstellungen „*Schließen*“. Achtet auch hier auf die Zuordenbarkeit zwischen Scan und Scanner.

Jetzt könnt ihr im Programm *Dokument ► Scannen ► Text /Foto* wählen, um anschließend mit dem Button „*Scannen*“ eine Seite zu scannen. Falls die Einstellung

34 https://eff.org/issues/printers

Text zu keinem Ergebnis führt, schaltet auf die Einstellung Foto um. Ihr könnt die Seite(n) noch drehen oder auf einen bestimmten Bereich zuschneiden, bevor ihr das Dokument mit „*Speichern*“ sichert.

Für eine weiterführende Nachbearbeitung des abgespeicherten Scans empfehlen wir das Programm *Gimp*[35] unter *Anwendungen ► Grafik ► GNU Image Manipulation Program*.

Beamer benutzen

Wenn ihr in eurer Gruppe Texte bzw. Recherechergebnisse gemeinsam diskutieren wollt, kann ein Beamer helfen. Falls euer Computer den Beamer nicht automatisch erkennt, müsst ihr in folgender Reihenfolge vorgehen: den Beamer mit dem Computer verbinden, z.B. via VGA-Kabel  oder HDMI-Kabel  einschalten und dann in Tails unter *Anwendungen ► Systemwerkzeuge ► Einstellungen ► Systemeinstellungen ► Monitore* die Option „*Gleiches Bild auf allen Bildschirmen*“ auswählen und bestätigen.
Falls euer Rechner den Beamer immer noch nicht als externen „Bildschirm“ erkennt, könnt ihr euren Rechner mit einer der Funktionstasten[36] dazu bringen, das Bild auch an den VGA-Ausgang zu schicken. Mehrmaliges Drücken dieser Funktionstaste schaltet bei vielen Modellen zwischen den drei Einstellungen „*nur Laptop-Bildschirm*“, „*nur Beamer*“ oder „*beide*“ um.

Warnung: Grenzen von Tails

Wir stellen hier einige Warnungen zur Nutzung von Tails und *Tor* zusammen, die ihr zur Bewertung eurer Sicherheit und zur Überprüfung nutzen könnt, in welchem Umfang Tails für eure spezifischen Anforderungen geeignet ist[37].

Tails verschlüsselt *nicht automatisch* eure Dokumente, löscht *nicht automatisch* die Metadaten aus euren Dokumenten und verschlüsselt auch keine Mail-Header eurer verschlüsselten Mails!

Tails nimmt euch auch nicht die Arbeit ab, eure Netzaktivitäten (entlang tätigkeitsbezogener Identitäten) auf-

35 siehe Kapitel *Aktionsfotos bearbeiten*
36 Welche Funktionstaste zum externen Bild umschaltet, hängt leider vom Rechner-Hersteller ab, ist aber als Symbol auf der Tastatur erkennbar.
37 https://tails.boum.org/doc/about/warning/index.de.html

zutrennen und Tails macht schwache Passwörter[38] nicht sicherer.

Kurzum, Tails ist kein Wunderheiler für Computer-Nicht-Expert*innen. Ihr müsst also grob verstehen, was ihr (mit Hilfe von Tails) macht und ihr müsst euer Netzverhalten neu entwerfen (siehe Kapitel *Nur über Tor ins Netz*).

Ihr könnt nicht verschleiern, dass ihr *Tor* und Tails verwendet

Tor-Nutzer*innen sind als solche erkennbar – folglich auch die Nutzer*innen von Tails, denn Tails schickt automatisch alle Verbindungen über das *Tor*-Netzwerk. Der Zielserver (z.B. die Webseite, die ihr besucht) kann leicht feststellen, dass ihr *Tor* nutzt, da die Liste der *Tor*-Exit-Rechner **3** (siehe Kapitel *Nur über Tor ins Netz*) für alle einsehbar ist.

Tails versucht es so schwer wie möglich zu machen, *Tails*-Nutzer*innen von *anderen Tor*-Nutzer*innen abzugrenzen, insbesondere von Nutzern des *Tor Browser Bundles* .

Manche Webseiten fragen viele Informationen über die Browser der Besucher ab. Zu den gesammelten Informationen können unter anderem Name und Version des Browsers, die Fenstergröße, eine Liste mit den verfügbaren Erweiterungen und Schriftarten, sowie die Zeitzone gehören. Einige dieser Merkmale können z.B. über die Nutzung von *NoScript*[39] im *Tor*-Browser unterdrückt werden. Andere, wie z.B. die Bildschirmauflösung und die Farbtiefe können unseres Wissens nicht unterdrückt werden. Diese Kennungen können eine Identifikation des Rechners erleichtern, bzw eine Zuordnung eures Aufrufes einer Webseite zu anderen bereits besuchten Webseiten ermöglichen[40].

Tor schützt nicht vor einem globalen Angreifer

Wie sicher ist die Verschleierung der IP-Adresse bei Benutzung des *Tor*-Netzwerks? Ergänzend zum Kapitel „*Ist Tor noch sicher?*“ in der Einführung hier noch einige Anmerkungen.

Ihr könnt in jedem Fall enttarnt werden, wenn ihr es mit einem *globalen Angreifer* zu tun habt, d.h. wenn jemand alle Rechner des *Tor*-Netzwerks korrumpiert hat bzw. den Datenverkehr zwischen allen *Tor*-Rechnern in Echtzeit mitprotokolliert. Einem solchen Angreifer ist es möglich über die Analyse von Zeitstempeln und Größe der ausgetauschten (verschlüsselten) Datenpakete, einzelne *Tor*-Nutzer*innen den jeweiligen Zielservern zuzuordnen – also die Anonymität aufzuheben![41]

Jeder Mensch weltweit mit einem Netzanschluss genügend großer Bandbreite kann seinen Rechner dem *Tor*-Netzwerk zur Verfügung stellen – auch Behörden und andere verdeckte Angreifer. Verteilt über die ganze Welt beteiligen sich derzeit über 5000 Rechner von verschiedenen Institutionen und Privatmenschen am *Tor*-Netzwerk.

Eine im Oktober 2013 veröffentlichte Studie von Wissenschaftler*innen[42] befasste sich mit dem bereits bekannten Problem der ausgedehnten Protokollierung des *Tor*-Netzwerkverkehrs. Ziel war es, die Wahrscheinlichkeit und den Zeitraum einschätzen zu können, der benötigt wird, um genügend Daten (über Alltagsroutinen im Netz) für eine Zerstörung der Anonymität zu sammeln. Nach dem dort untersuchten Modell könnte in sechs Monaten durch den Betrieb eines einzigen *Tor*-Rechners, die Anonymität von 80% der verfolgten Benutzer*innen durch gezielte Suche nach wiederkehrenden Traffic-Mustern gebrochen werden.

Die Praxis schien zumindest *zum Zeitpunkt der von Snowden kopierten Geheimdokumente* (im Frühjahr 2013) etwas komplizierter als derartige Modelle. Ein Artikel der britischen Zeitung The Guardian berichtete im Herbst 2013 von geringen Erfolgen, welche die NSA beim Versuch verbuchte, *Tor*-Benutzer*innen zu identifizieren. Zugrunde lagen dem Artikel die Snowden-Dokumente über *Prism*. „Wir werden niemals alle *Tor*-Nutzer identifizieren können“, zitierte der Guardian aus einer Top-Secret-Präsentation mit dem Titel „*Tor* stinks“. Mit manueller Analyse sei man *(damals)* lediglich in der Lage (gewesen), einen sehr kleinen Anteil der *Tor*-Nutzer*innen zu identifizieren. Insbesondere habe die Agency bislang keinen Erfolg damit gehabt, Anwender*innen auf konkrete Anfragen hin gezielt zu de-anonymisieren.

Die bislang veröffentlichten „Enttarnungserfolge“ beruhten auf (noch nicht geschlossenen) Sicherheitslücken des verwendeten Browsers, auf Anwendungsfehlern oder auf immer gleichen Mustern der Nutzer*innen. Allerdings sind auch Sicherheitslücken im *Tor*-Protokoll gefunden und behoben worden. Ob sie in dieser Zeitspanne zur Enttarnung von Nutzer*innen geführt haben, ist uns nicht bekannt.

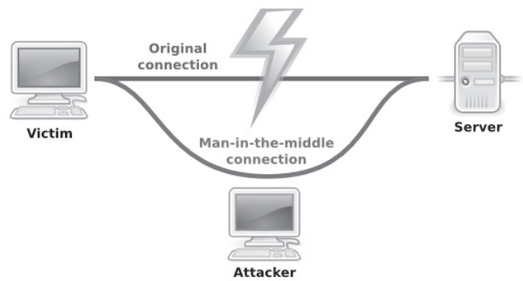
38 siehe dazu das Kapitel *Sichere Passwortwahl*
39 siehe dazu das Kapitel *Surfen über Tor*
40 http://heise.de/-1982976

41 Wer mehr über die Zielsetzung und das Bauprinzip von *Tor* erfahren will: *Tor* Project: The Second-Generation Onion Router (Kapitel 3, Design goals and assumptions) https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf
42 http://www.ohmygodel.com/publications/usersrouted-ccs13.pdf

Man-in-the-middle-Angriffe

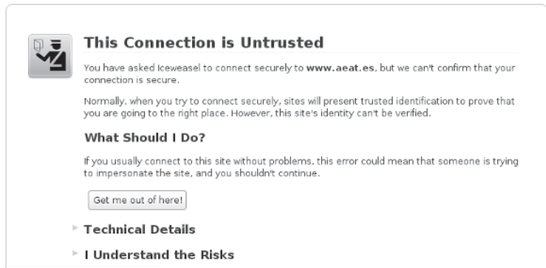
Bei einer solchen Attacke greift ein *Man-in-the-middle* aktiv in die Verbindung von eurem Rechner zu einem Zielserver ein: Ihr denkt, dass ihr direkt mit dem Server eures Mail-Anbieters oder mit der Eingabemaske des Nachrichten-Portals de.indymedia.org verbunden seid, tatsächlich sprecht ihr mit der Angreifer*in, die das eigentliche Ziel imitiert[43].

Auch bei der Benutzung von *Tor* sind derartige Angriffe möglich - sogar *Tor*-Exit-Rechner[44] können solche Angreifer sein[45]. Eine verschlüsselte Verbindung (SSL-Verschlüsselung für euch im Browser am https://... erkennbar) ist hilfreich, aber nur dann, wenn ihr die Echtheit des *Zertifikats einer solchen Verbindung überprüfen* könnt.



Wir gehen hier nicht tiefer auf Zertifizierungsmethoden und deren Verlässlichkeit ein, wollen euch aber zumindest die Basis für ein gesundes Misstrauen mitgeben:

Wenn euch dieser Bildschirm beim Verbindungsaufbau angezeigt wird, dann konnte die *Echtheit eures Zielservers* (in unserem Beispiel der Mailanbieter oder indymedia) nicht garantiert werden. Damit ist nicht gesagt, dass an der Verbindung wirklich etwas „faul“ ist.



43 Die NSA geht hier noch einen Schritt weiter und erweitert Man-in-the-middle-Angriffe durch Man-on-the-side-Angriffe: Diese Variante hat den „Vorteil“, dass keine Verzögerungen im Datenverkehr wahrgenommen werden. Siehe dazu: https://en.wikipedia.org/wiki/Man-on-the-side_attack
44 siehe zur Funktionsweise von *Tor* das Kapitel Nur über *Tor* ins Netz
45 Man-in-the-middle Angriffe von *Tor*-Exit-Rechnern ausgeführt: http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks

Wenn ihr jedoch die Möglichkeit habt, den unter „*Technical Details*“ angezeigten (vorgeblichen) *Fingerprint* eures Zielservers zu überprüfen (Besuch der Seite von einem anderen Rechner aus, oder andere Quellen), dann solltet ihr das tun!

Das wehrt nicht alle Arten von Man-in-the-Middle-Attacken ab, erschlägt aber einen großen Anteil.

> ***Tails unterstützt euch mit dem Tor-Browser-Plugin** HTTPS-Everywhere **dabei, (wo möglich) SSL-verschlüsselte Verbindungen aufzubauen. Wenn ihr die Möglichkeit habt, die Echtheit dieser Verbindung über den** Fingerprint **zu überprüfen, solltet ihr das unbedingt tun.***

Cold-Boot Angriffe

Bei der Benutzung eines Computers werden alle bearbeiteten Daten temporär im Arbeitsspeicher zwischengespeichert - auch Passwörter und PGP-Schlüssel!

Nachdem ihr den Computer ausschaltet, geht der Inhalt des Arbeitsspeichers nicht sofort, sondern (je nach Temperatur[46]) erst *nach einigen Minuten* verloren. Angreifer*innen können diese Zeit zum Auslesen des Arbeitsspeichers nutzen, benötigen dazu jedoch physischen Zugang zum Rechner.

Tails überschreibt beim Herunterfahren bzw. Ausschalten des Rechners (per Power-Off) den Arbeitsspeicher deswegen mit Zufallszahlen. Das klappt jedoch nicht bei allen Computern: Wenn sich euer Rechner beim Herunterfahren oder beim „Auschalten“ nach zwei Minuten nicht selbstständig ausschaltet, dann gibt es keine Garantie dafür, dass das Überschreiben (vollständig) funktioniert hat.

> ***Im Fall einer überraschenden Beschlagnahmung eures Rechners sofort den Ausschalter drücken! Es ist ratsam, den Rechner herunterzufahren, wenn er längere Zeit unbeaufsichtigt ist - z.B. in der Nacht.***

Keylogger

Wenn ihr einen nicht vertrauenswürdigen Computer verwendet, z.B. einen für alle zugänglichen in einer öffentlichen Bibliothek, dann kann potentiell alles, was ihr über die Tastatur eingebt, von einem *Hardware Keylogger* aufgezeichnet werden.

46 Je kälter, desto länger „hält sich“ der Speicherinhalt. Daher benutzen Forensiker zur Datenwiederherstellung beschlagnahmter Geräte Kältemittel zur kurzfristigen „Daten-Konservierung“.

Um die Eingabe von Passwörtern oder sensiblen Texten vor einem Keylogger zu schützen, könnt ihr die *Bildschirmtastatur* verwenden. Um die Bildschirmtastatur anzuzeigen, klickt ihr auf das **Tastatursymbol in der Kontrollleiste oben**. Jeder Klick auf dieser *virtuellen* Tastatur ersetzt dann einen *realen* Tastaturanschlag. Da auch das Fernauslesen des Bildschirminhalts nachweislich zu den Angriffsmethoden der Geheimdienste gehört, raten wir grundsätzlich:

> ***Wenn ihr der Hardware nicht trauen könnt, benutzt sie nicht für sensible Arbeit!***

Gefahren von kabellosen Schnittstellen

> ***Derzeit werden beim Start von Tails die kabellosen Schnittstellen* WLAN, wwan, wimax, bluetooth** *- sofern in eurem Computer vorhanden - (mit geänderter MAC-Adresse)* **aktiviert.**

Beim **WLAN** reicht die Manipulation der MAC-Adresse aus, um von anderen Geräten in Reichweite *falsch* identifiziert zu werden.

Die **Bluetooth**-Schnittstelle eures Laptops hingegen benutzt zur Identifikation nicht nur eine der MAC ähnliche Adresse sondern auch eine andere, nicht veränderbare Geräte-Adresse[47]. Das heißt aber:

Euer Laptop kann von anderen Geräten mit einer Bluetooth-Schnittstelle identifiziert werden – je nach Übertragungsstandard zwischen ein und 100 Meter weit[48]!

Daher ist es für eine sichere Betriebsart von Tails unerlässlich, sämtliche nicht benötigte Funkschnittstellen abzuschalten. Wir beschreiben hier drei unterschiedliche Methoden. Wir halten Variante 1 für die sicherste:

47 Die Situation ist ähnlich dem im Kapitel *Tails ändert eure MAC-Adressen* beschriebenen Problem mit den UMTS-Sticks, die zur Anmeldung beim Mobilfunk-Anbieter zusätzlich die IMSI der SIM-Karte und die IMEI des Sticks übermitteln.

48 *Die häufigsten Bluetooth-Geräte (der Klasse 2) haben mit einer Sendeleistung von 2,5 mW etwa 10m Reichweite. Im Freien können sie aber aus bis zu 50 Metern Entfernung noch erkannt werden!* Die selteneren Geräte der Klasse 1 können eine Reichweite drinnen und draußen von 100 Metern erreichen, benötigen dafür aber auch 100 mW. Gegenwärtig liegen Geräte mit Bluetooth der Klasse 3 im Trend. Mit einer Leistungsaufnahme von 1 mW sind sie nur für den Einsatz bei kurzen Strecken und in Geräten mit langer Akkulaufzeit gedacht, wie etwa Headsets, Hörgeräten oder Pulsmessern, die beispielsweise ihre Daten an Smartphones weitergeben. Durchschnittlich liegt deren Reichweite bei etwa einem Meter, maximal sind es zehn.

1. **Bluetooth[49] ausbauen**
   In vielen neueren Laptops findet sich *eine Karte*, die sowohl das WLAN, als auch das Bluetooth-Modul beinhaltet (siehe Abbildung rechts). Nach Lösen aller Schrauben des Laptop-Bodens und dem Abnehmen des Bodendeckels könnt ihr die beiden Antennenanschlüsse abziehen und die Karte(n) herausnehmen. Im Falle einer kombinierten Bluetooth/WLAN-Karte[50] müsst ihr diese durch eine reine WLAN-Karte ersetzen.

2. **Bluetooth im BIOS deaktivieren**
   Dies ist leider nicht bei allen Computern möglich.
3. **Software-seitig abschalten**
   Solange Tails in seinem Startbildschirm *nicht* die Option anbietet, Bluetooth und andere Funkschnittstellen vor Systemstart zu deaktivieren, müsst ihr einen umständlichen *workaround* nutzen: An einem für euch untypischen Ort Tails starten, dann alle Geräte in Tails manuell deaktivieren und danach einen **Ortswechsel** vornehmen, um woanders mit der Arbeit zu beginnen. Dazu müsst ihr:
   - Beim Startbildschirm *„weitere Optionen“* wählen und ein *Administrator-Passwort* eingeben[51].
   - Nach dem Start *Anwendungen* ▸ *Zubehör* ▸ *Root Terminal* anklicken. Jetzt werdet ihr nach dem zuvor eingegebenen Administrator-Passwort gefragt. Bei richtiger Eingabe öffnet sich ein so genanntes Terminal, in dem ihr folgende Befehlssequenz eintippt und mit der *Eingabe-Taste* abschickt:
   - **rfkill block bluetooth wimax wwan**[52]

Fertig - Jetzt könnt ihr an den *Ort wechseln*, an dem ihr per WLAN ins Netz gehen wollt. **Achtet darauf, dass der Rechner während des Ortswechsels nicht ausgeht!**

Bei der (unsichersten) Variante 3 habt ihr das Problem jedoch lediglich software-technisch auf Betriebssystem-Ebene gelöst. Eine eventuell während der Sitzung eingeschleuste Schadsoftware kann eben diese Deaktivierung aller Funkschnittstellen mit einem weiteren Kommando genauso einfach rückgäng machen.

49 Da die Bauart dieser Karten und die Orte wo (im Rechner) genau sie verbaut sind, variieren, müsst ihr in der Betriebsanleitung (User Manual) eures Computers nach einer Beschreibung zu deren Ein-und Ausbau suchen.

50 siehe dazu das Kapitel *Tails als Quasi-Schreibmaschine*.

51 Siehe dazu das Kapitel *„Tails starten“*

52 mit **rfkill block bluetooth** bzw **rfkill block wlan** lassen sich die Schnittstellen auch einzeln abschalten, falls ihr die jeweils andere benötigt.

Tails als Quasi-Schreibmaschine

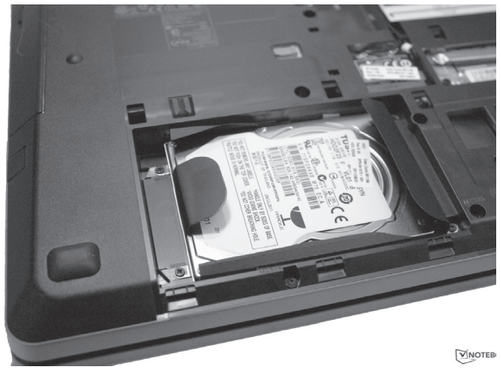
Im Februar 2015 veröffentlicht der Antiviren-Software-Hersteller *Kaspersky,* dass die NSA in größerem Umfang die Firmware von Festplatten infiziert. Die eingeschleuste Schadsoftware überlebt eine Formatierung der Festplatte oder Neuinstallation des Betriebssystems und sei nicht zu entdecken. Gleichzeitig werde sie genutzt, um einen versteckten Bereich auf der Festplatte zu schaffen, auf dem Daten gesichert werden, um sie später abgreifen zu können. Die einzige Möglichkeit, die Schadsoftware loszuwerden sei die physikalische Zerstörung der Festplatte.

Für eine sicheres, spurenfreies Bearbeiten von extrem sensiblen Dokumenten empfehlen wir die Arbeit an einem Rechner, der weitgehend abgeschottet ist und insbesondere keine Festplatte(n) besitzt.

Festplatte(n) abschalten

Zwar müsstet ihr die im Computer vorhandene Festplatte, wie jeden anderen Datenträger auch, in Tails erst im Menü *Orte* ▸ *Rechner* verfügbar machen bevor ihr (versehentlich) darauf etwas speichern könnt. Aber genau solche „Versehen“ und die Möglichkeit, dass eine in der Sitzung eingeschleuste Schadsoftware doch auf die Festplatte zugreifen könnte wollen wir ausschalten. Wir stellen euch zwei Methoden vor. Wir empfehlen die erste:

- **Festplatte ausbauen**
  In der Bedienungsanleitung *(ansonsten User Manual im Internet suchen)* eures Rechners sind die dazu notwendigen Schritte erläutert. Als erstes müsst ihr den Akku aus eurem Laptop herausnehmen und den Netzstecker abziehen. *Bei vielen Laptops* müsst ihr die Schrauben auf dem Boden lösen und den Boden abnehmen. Die Festplatte ist mit dem Restgehäuse zusätzlich verschraubt. Nachdem ihr diese gelöst habt, könnt ihr die Festplatte vom Stecker abziehen.



- **Festplatte im BIOS deaktivieren**
  Wenn euch der Ausbau zu aufwändig erscheint, müsst ihr zumindest im BIOS die interne(n) Festplatte(n) eures Computers deaktivieren[53].

Alle kabellosen Schnittstellen abschalten

Das kabelgebundene Netz (LAN) lässt sich einfach über das Abziehen des Netzwerkkabels „deaktivieren“. Zusätzlich ist es für diesebesonders sichere Betriebsart von Tails als „Quasi-Schreibmaschine“ unerlässlich, sämtliche Funkschnittstellen abzuschalten. Wir beschreiben hier drei unterschiedliche Methoden *(1 ist die sicherste, 3 die unsicherste)*:

1. **WLAN und Bluetooth[54]ausbauen**
   analog zu Schritt 1 im vorherigen Kapitel Gefahren von kabellosen Schnttstellen. Ihr ersetzt die ausgebaute Karte jedoch nicht.
2. **Alle Netzwerkadapter im BIOS deaktivieren** ***(leider nicht bei allen Computern möglich)***
3. ***Analog zu Schritt 3 im vorherigen Kapitel** Gefahren von kabellosen Schnttstellen**. Ihr ersetzt den Befehl jedoch durch:* **rfkill block all**

> ***Ein vollständig abgeschotteter** Schreib-Computer**, aus dem ihr die Festplatte(n) und alle kabellosen Netzwerkadapter ausbaut, gibt euch erhöhte Sicherheit beim Erstellen und Bearbeiten von Dokumenten: Ihr seid ohne weiteres nicht zu identifizieren und zu lokalisieren und ihr verhindert ein „versehentliches“ Speichern auf Festplatte!***

53 Unmittelbar nach dem Computer-Start eine der Tasten F1, F2, DEL, ESC, F10 oder F12 gedrückt halten (auf einen Hinweis auf dem *kurz* erscheinenden Startbildschirm achten), um in das BIOS-Setup zu gelangen. Die meisten Rechner bieten nur ein englisch-sprachiges BIOS-Menü.

54 Da die Bauart dieser Karten und die Orte wo (im Rechner) genau sie verbaut sind, variieren, müsst ihr in der Betriebsanleitung (User Manual) eures Computers nach einer Beschreibung zu deren Ein-und Ausbau suchen. Hier ein Abbild einer kombinierten WLAN- und Bluetooth-Karte eines Laptops.

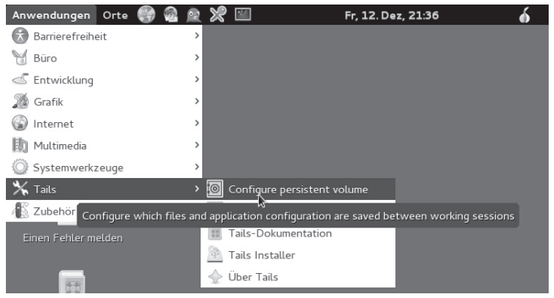
Persistenz

Daten und Einstellungen bleiben auf dem Tails-USB-Stick erhalten

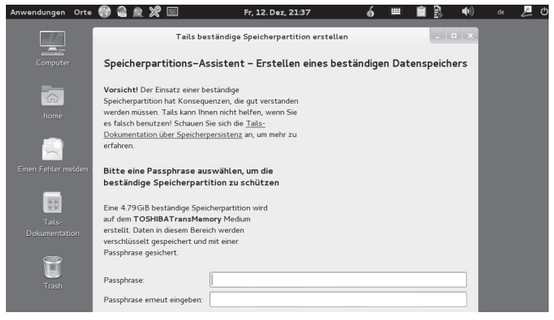
Bei normaler Benutzung werden alle Daten und alle Einstellungsänderungen (gespeicherte Texte, Bilder, Verschlüsselungskeys, Programmkonfigurationen, etc) mit dem Runterfahren des Rechners verworfen. Das hat den Vorteil, dass keine individuellen Spuren auf dem Stick verbleiben, schränkt aber die bequeme Benutzbarkeit für einige Anwendungen ein. Um dem zu begegnen, gibt es bei der Nutzung von Tails auf einem USB-Stick die Möglichkeit, ein sogenanntes *"persistent volume"* zu verwenden. Gemeint ist damit ein Speicherbereich auf dem Tails-Stick, welcher eben nicht vergesslich ist. Dieser Speicherbereich wird von dem Platz auf dem USB-Stick abgezweigt, der nicht von der Tailsinstallation (etwa 1 GB) belegt wird. Je mehr Kapazität also der USB-Stick hat, um so größer fällt das *"persistente Volume"* aus.

Anlegen eines Persistent Volumes

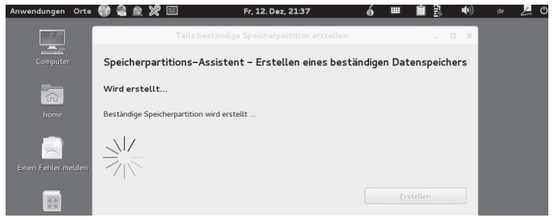
Ihr bootet normal und deaktiviert im Begrüßungsdialog den Punkt mit der "Persistence" (voreingestellt), denn noch gibt es das persistente Volume nicht. Ist der Rechner bis in die graphische Oberfläche gebootet, dann wählt *Anwendungen ►Tails ►Configure persistent Volume* aus.



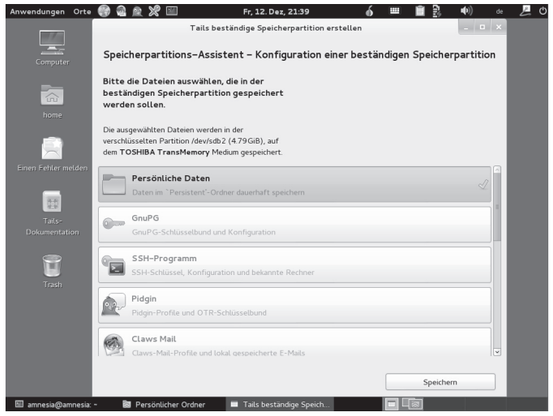
Es erscheint ein Dialog mit Hinweisen und der Abfrage des Passworts. Bitte beachtet die Hinweise in dieser Broschüre zur Auswahl eines starken Passworts.



Nach Eingabe des Passwortes wird das persistente Volume erzeugt, das kann einen Moment dauern.



Ist dieser Vorgang abgeschlossen, folgt der Dialog zu Konfiguration des persitent Volume. Ihr könnt übrigens diese Konfiguration zu jedem späteren Zeitpunkt anpassen. Eine Erkärung des Konfigurationsdialogs:



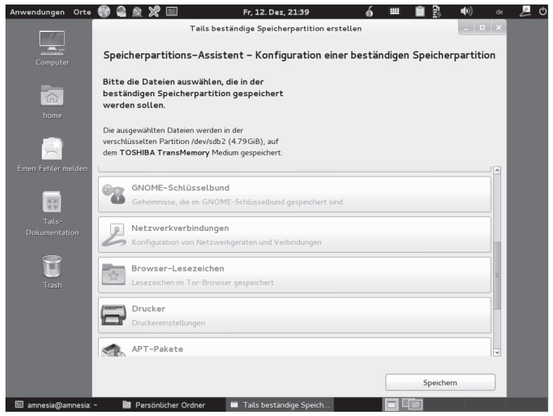
* **Persönliche Daten:** In Eurem home-Verzeichnis wird ein Ordner "Persistent" erzeugt. Dokumente (Bilder, Texte, etc) die in diesem Ordner liegen, "überleben" einen reboot von Tails uns sind in der nächsten Sitzung immer noch vorhanden.

* **GnuPG:** Öffentliche und private GPG/PGP Schlüssel bleiben erhalten.

* **SSH-Programm:** Schlüsselmaterial des SSH-Programms bleiben erhalten. Wenn ihr nicht wisst, was SSH ist und wozu es gebraucht wird, dann könnt ihr diesen Punkt weglassen.

* **Pidgin:** Auch das Chat-Programm Pidgin verwendet Schlüssel, um eine sichere Kommunikation zu erlauben. Sollen diese Schlüssel erhalten bleiben, dann aktiviert diesen Punkt. Mehr dazu im Kapitel *Chatten über Tor*.

* **Claws Mail:** Tail bringt ein E-Mailprogramm mit, dessen Einstellungen (Mailserver, Accountdaten, etc) aber auch heruntergeladene Mails bleiben erhalten, wenn dieser Punkt aktiviert ist. Mehr dazu im Kapitel *Mailen mit Persistenz*.



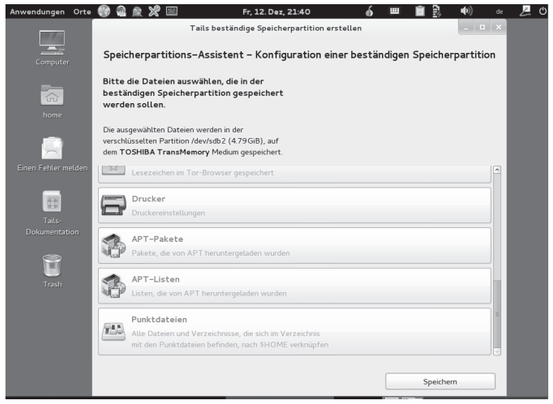
* **Gnome Schlüsselbund:** Tails benutzt einen Keymanager, der dafür sorgt, dass Passwörter, die ihr für einen Dienst eingebt nicht nochmal eingegeben werden müssen, wenn ihr diesen Dienst ein zweites Mal verwendet – das GPG-Passwort ist ein Beispiel dafür: Einmal eingegeben, wird es bei der nächsten verschlüsselten Mail wiederverwendet. Aktiviert ihr diesen Punkt, dann bleiben diese Passwörter auf dem Stick gespeichert. Wir raten von der Benutzung ausdrücklich ab!

* **Netzwerkverbindungen:** Habt ihr spezielle Netzwerkkonfigurationen (UMTS-Sticks, zB), ohne die ihr nicht ins Internet kommt, dann könnt ihr die durch Aktivierung dieses Punktes haltbar machen.

* **Browser-Lesezeichen:** Aktiviert ihr diesen Punkt, dann bleiben die Bookmarks erhalten.

* **Drucker:** Eure Druckerkonfiguration bleibt erhalten.

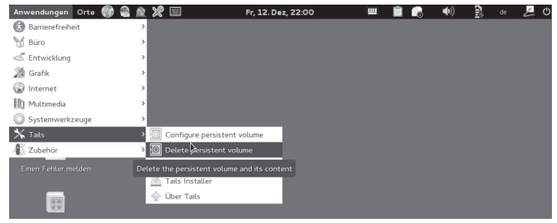
* **APT-Pakete:** Habt ihr auf dem Tails Stick eigene Software installiert, so ist diese normalerweise nach einem Reboot verschwunden. Aktiviert ihr diesem Punkt bleibt sie erhalten.



* **APT-Listen:** APT ist eine oder besser die Softwareverwaltung von Debian, aus welchem Tails besteht. APT pflegt Listen von Softwarepaketen, die installierbar sind inklusive der Versionsnummern, sodass veraltete Pakete erkannt werden. Wenn ihr eigene Software installiert, dann aktiviert auch diesen Punkt.

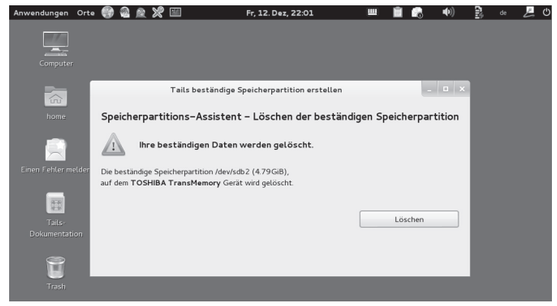
* **Punktdateien:** Tails bringt eine Menge Programme mit. Passt ihr deren Konfiguration an, dann werden diese in sogenannte Punktdateien (dot-files) gespeichert. Aktiviert diesen Punkt, wenn ihr eure individuellen Anpassungen behalten wollt und diese nicht durch die oben genannten Punkte bereits abgedeckt sind.

Anpassen und Löschen des Persistent Volumes



Den oben beschriebenen Konfigurationsdialog bekommt ihr unter *Anwendungen ►Tails ►Configure persistent Volume*

Solltet ihr euer persistent Volume löschen wollen, dann wählt *Anwendungen ►Tails ►Delete persistent Volume*.



Wenn ihr jetzt auf *"Löschen"* klickt sind die Daten in dem persistenten Volume unwiederbringlich weg! Ihr könnt zu einem späteren Zeitpunkt die ganze Prozedur wiederholen, um ein neues persistentes Volume zu erzeugen.

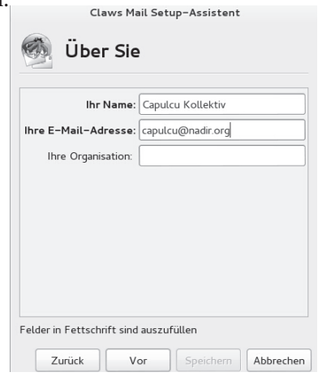
Benutzung des Persistent Volumes

Damit ihr das Persistent Volume benutzen könnt, müsst ihr rebooten. Im Anfangsdialog werdet ihr gefragt, ob ihr das Persistent Volume benutzen wollt. Bejaht das und gebt das Passwort ein. Fertig.

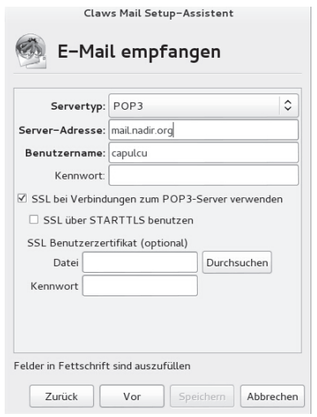
Mailen mit Persistenz

Mit der Tails-Persistenz könnt ihr das Mail Programm *Claws Mail*, das bei Tails mitgeliefert wird, verwenden, da eure Einstellungen im Mail Programm und eure Mails auch nach Neustart erhalten bleiben. Voraussetzung dafür ist, dass beim Erstellen der Persistenz, diese sowohl für GnuPG als auch für Mail (Claws Mail) aktiviert wurde *(siehe voriges Kapitel)*.

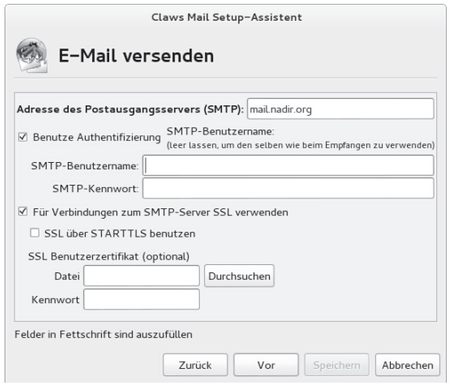
Claws Mail startet ihr entweder über das Icon in der oberen Menuleiste oder unter *Anwendungen* ► *Internet* ► *Claws Mail*. Beim ersten Starten führt euch ein Setup-Assistent durch die Konfiguration eures E-Mail-Postfaches. Es müssen zuerst der Name und die E-Mail-Adresse eingegeben werden.



Danach müssen die Einstellungen für das Empfangen von Mails eingegeben werden. Also der Servertyp (POP3 oder IMAP), die Serveradresse und der Benutzername eingegeben werden. Wisst ihr diese Einstellungen nicht auswendig, könnt ihr entweder in eurem bisherigen Mail-Programm wie Thunderbird oder auf der Internetseite eures Mailanbieters diese Einstellungen nachschauen. Wichtig ist, dass der Haken bei *„SSL bei Verbindungen zum POP3-Server verwenden“* gesetzt ist. Einige Mail-Anbieter benötigen auch den Haken bei *„SSL über STARTTLS benutzen“*.

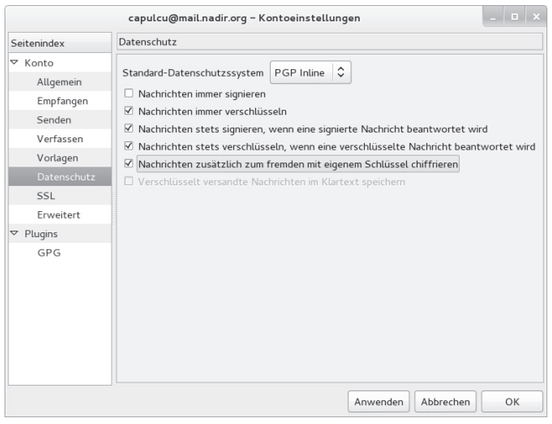


Im Fenster danach müssen die Einstellungen für das Senden von Mails eingestellt werden. Notwendig ist hier meist nur die Adresse des Postausgangsserver und der Haken bei *„Benutze Authentifizierung“*. Auch in diesem Fall könnt ihr euch an den Einstellungen eures bisherigen Mail-Programm oder an den Beschreibungen auf der Webseite eures Anbieters orientieren. Und auch hier ist es wichtig den Haken bei *„Für Verbindungen zum SMTP-Server SSL verwenden“* bestehen zu lassen. Einige Mail-Anbieter benötigen hier ebenfalls den Haken bei *„SSL über STARTTLS benutzen“*.



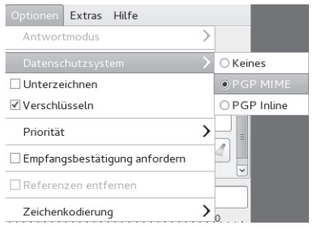
Der Mailbox-Name im Dialogfenster *„Abspeichern der Mail“* kann übernommen werden. Nach einem weiteren *„Vor“* und *„Speichern“* ist das Mail-Programm Claws Mail eingerichtet.

Nun muss noch GPG zur Verschlüsselung von E-Mails eingerichtet werden: Dazu geht ihr zu den Kontoeinstellungen *Konfiguration* ► *Konten bearbeiten* ► *Bearbeiten*. Dort wählt ihr zuerst den Reiter „Datenschutz“ aus. Um Mails verschlüsseln zu können, muss das *„Standard-Datenschutzsystem“* auf *„PGP MIME“* gesetzt werden. Außerdem sollten Haken an die Optionen *„Nachrichten immer verschlüsseln“* und *„Nachrichten zusätzlich zum fremden mit dem eigenen Schlüssel chiffrieren“* gesetzt werden, wenn gesendete Nachrichten auch nachträglich für den Absender entschlüsselbar bleiben sollen. Die zwei Optionen zum Signieren von E-Mails können nach Bedarf eingestellt werden.



Jetzt muss noch euer GPG-Schlüsselpaar importiert werden. Dazu klickt ihr in einem Dateimanagerfenster mit der rechten Maustaste auf die Datei, die das Schlüsselpaar enthält und wählt *„Mit Schlüssel importieren öffnen“*. Alternativ kann ein neues Schlüsselpaar erzeugt werden. Klickt auf das *„OpenPGP-Verschlüsselungs-Applet“* in der oberen Menuleiste, dann *„Schlüssel verwalten“*. Nach einem Klick auf das blaue „+“, wählt ihr *„PGP-Schlüssel“* aus.

Zurück in Claws-Mail: Zum Verfassen einer verschlüsselten/signierten E-Mail muss *Optionen* ► *Verschlüsseln* / *Optionen* ► *Unterzeichnen* aktiviert sein. Falls diese nicht anwählbar sind, muss unter *Optionen* ► *Datenschutzsystem „PGP MIME“* ausgewählt sein.



Anhang

Hier stellen wir euch vor, wie ihr die jeweils aktuelle Version von Tails *herunterladen und überprüfen!* könnt, um daraus eine(n) „bootfähige“ Tails-DVD, USB-Stick bzw SD-Karte zu erstellen.

Da einige, abhängig vom Rechner und dessen BIOS-Einstellmöglichkeiten, *Schwierigkeiten beim Booten* von einem der Startmedien haben, gehen wir kurz auf die häufigsten Fallstricke ein.

Falls euch (wider Erwarten) dennoch das erstmalige Starten von Tails nicht gelingen sollte, holt euch *einmalig* Hilfe bei der BIOS-Einstellung, oder bei der Überprüfung der Tails-Version auf ihre Echtheit - das ist kein hinreichender Grund, auf die *viel einfachere Benutzung* von Tails zu verzichten!

Abschließend geben wir euch Tipps zur Wahl und Handhabung von möglichst sicheren Passwörtern.

Wie bekomme ich Tails

Im Kapitel *„Warnung: Grenzen von Tails“* haben wir die Praxis von *Man-in-the-Middle*-Angriffen diskutiert, bei denen sich die Angreifer*in in die Datenströme hängt, um sie zu *kontrollieren* und/oder zu *manipulieren*. Insbesondere beim Herunterladen von Software ist daher darauf zu achten, deren „Echtheit“ zu überprüfen. Andernfalls kann euch leicht ein manipuliertes Tails untergeschoben werden. Der folgende Teil dieser Anleitung mag euch kompliziert erscheinen - aber ihr dürft ihn nur dann ignorieren, wenn euch eine Person eures Vertrauens mit der jeweils neuesten Tails-Version versorgt. Wer so auf eine bereits überprüfte Version von Tails zurückgreifen kann, hat es mit dem Kapitel *Tails Upgrader* und *Tails Installer* zum Erzeugen eines neuen / weiteren Tails-Stick wesentlich leichter. Im folgenden lernt ihr, dies eigenständig zu erledigen. Wir stellen euch drei Wege vor - je nachdem ob ihr normalerweise **Windows**, **Mac**, oder **Linux**- Nutzer*in seid.

Digitale Signaturen

Durch digitale Signaturen kann die „Echtheit“ einer Software überprüft werden. Hierfür wird der öffentliche PGP-Schlüssel des Entwickler-Teams benötigt, mit dem die Software unterschrieben wurde. Die Unterschrift garantiert, dass es sich um eine unveränderte Version der bezogenen Software handelt.

Wenn ihr euch z.B. die aktuelle Version der Live-DVD Tails besorgt, findet ihr im Download-Bereich eine entsprechende Signatur mit der ihr die „Echtheit“ der Software überprüfen könnt. Dafür benötigt ihr noch den PGP-Schlüssel der Entwickler*innen, der ebenfalls auf der Download-Seite erhältlich ist. Nach erfolgreichem Import dieses Schlüssels könnt ihr über grafische Tools oder über eine sogenannte Kommandozeile die Authentizität der Software überprüfen. Wie dies funktioniert stellen wir euch in den nächsten Kapiteln vor.

Theoretisch wäre es durch einen Man-in-the-Middle-Angriff trotzdem noch möglich, euch eine falsche Signatur und eine dafür angepasste Software, sowie einen falschen Schlüssel zu übermitteln. Ein Weg dies zu umgehen, ist die Software und deren Signatur über verschiedene Netzwerke zu besorgen - z.B. einmal von eurer Arbeit aus, dann von eurem Anschluss in eurer WG und ein zusätzliches mal über *Tor*. Anschließend könnt ihr die Software über ihre *Hashwerte*[55] vergleichen. Ein Abgleich einer *sha256-Prüfsumme* bei der Software, die ihr euch über unterschiedliche Wege besorgt habt, muss das gleiche Er-

55 Ein *Hashwert* ist eine Prüfsumme einer Datei, um deren Unveränderheit festzustellen: https://de.wikipedia.org/wiki/Hashfunktion

gebnis liefern. Zusätzlich könnt ihr die Prüfsumme der Software mit jener auf der Hersteller*in Seite abgleichen. Auch eine Suche im Netz kann dafür genutzt werden, die Authentizität, der von euch besorgten Software, zu verifizieren, da viele Webseiten die Prüfsummen von unterschiedlicher Software online ablegen[56].

Tails herunterladen und überprüfen

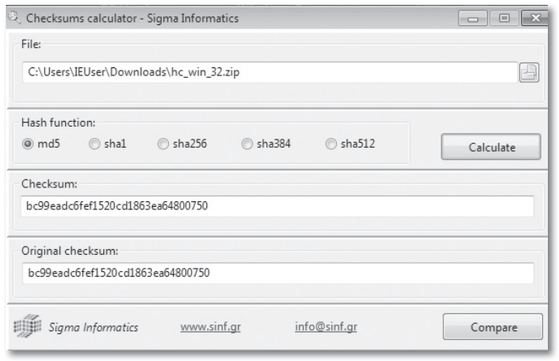
Die aktuelle Version von Tails, z.B. *tails-i386-1.3.1.iso* findet ihr im Internet, den entsprechenden Link und Prüfsummen in der Tabelle am Ende dieser Broschüre.

> ***Die Echtheit eurer heruntergeladenen Tails-Version solltet ihr über die Prüfsumme und über die PGP-Signatur überprüfen. Wir beschreiben im Folgenden beide Vorgehensweisen für Windows, Mac und Linux-Nutzer*innen.***

Auf der Webseite findet ihr auch die Signatur sowie den PGP-Schlüssel des Tails-Entwickler-Teams. Ladet beide Dateien zur späteren Verwendung herunter.

Windows: Tails-Prüfsumme verifizieren

Da Windows keine Funktionalität zum Überprüfen von digitalen Signaturen enthält, solltet ihr euch **hash_calc_32** besorgen und installieren (Link ist in der Tabelle am Ende des Kapitels zu finden). Nach erfolgtem Download könnt ihr das Programm zum Überprüfen von Hashwerten nutzen[57]. Für das Programm **hash_calc_32** selbst findet ihr die Prüfsumme ebenfalls am Ende des Kapitels.



Über den *Datei-Auswahl-Button* im **Checksums calculator** müsst ihr die zuvor heruntergeladene Datei *hc_win_32.zip* auswählen. Dann wählt ihr *„Hash function“* **sha256** und tragt den in unserer Tabelle stehenden **sha256**-Hashwert unter *Original checksum* ein.

56 Die sha1-Prüfsumme von gpg4win beispielsweise findet sich auf über 120 unterschiedlichen Webseiten.
57 https://de.wikipedia.org/wiki/Hashfunktion

Nun betätigt ihr noch den Button *Calculate*. Das Programm vergleicht nun die Hashwerte miteinander.

Falls ihr eine Meldung mit *„Checksums are identical“* erhaltet, könnt ihr davon ausgehen, dass es sich um eine originale Software handelt.

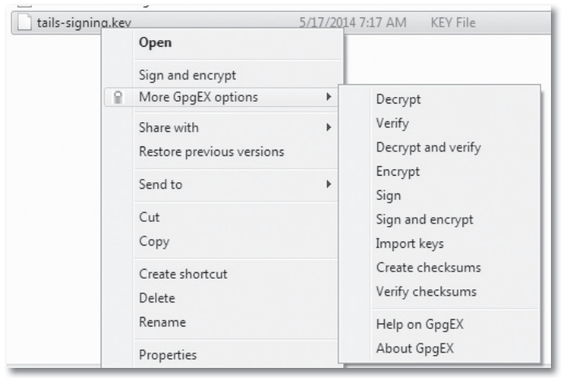
Über den gleichen Weg könnt ihr die iso-Datei von Tails auf ihre Authentizität prüfen. Unter der *Orginal Checksum* muss dann der entsprechende Wert (siehe Tabelle) eingetragen werden. Nach Angabe des vollständigen Pfades, (Ort, wo eure heruntergeladene Datei z.B. *tails-i386-1.3.1.iso* liegt), drückt ihr wieder *Calculate.*

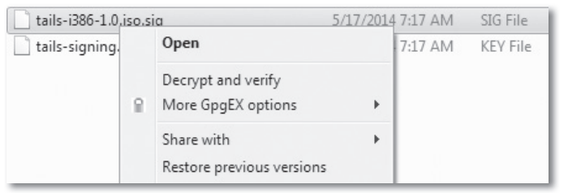
Windows: PGP Signatur prüfen

Zum Überprüfen der Signatur müsst ihr **GPG** bei euch installieren, wir empfehlen gpg4win (siehe Tabelle)[58].

Auch hier überprüft ihr wieder die Prüfsumme des Programms selbst (wie unter *Tails Prüfsumme verifizieren* beschrieben), die in der Tabelle findet. Ist der Hashwert korrekt, könnt ihr gpg4win auf eurem Rechner installieren. Nach erfolgreicher Installation müsst ihr euch noch den *öffentlichen PGP-Schlüssel der Tails-Entwickler* holen und importieren.

Dies erreicht ihr, indem ihr euch den Schlüssel von der Tails-Download Seite ladet und anschließend mit der *rechten Maustaste* darauf klickt. Nun sollte ein Fenster erscheinen unter dem ihr *„More GpgEX options ▸ Import keys“* auswählt“.





58 GPG ist die Open Source-Variante von PGP.

Gpg4win sollte euch hier den Import des Schlüssel bestätigen.

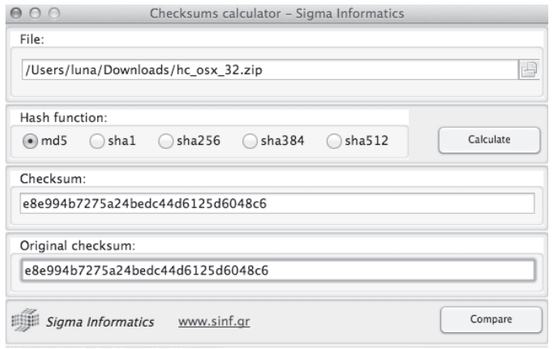
Wenn ihr die Datei *tails-i386-1.3.1.iso* heruntergeladen habt, müsst ihr mit der *rechten Maustaste* auf die Tails-Signatur klicken (*tails-i386-1.3.1.iso.sig*) und *„Decrypt and verify“* wählen.

Nach einer zweiten Betätigung des Buttons *„Decrypt/Verify“* und einer kurzen Wartezeit solltet ihr folgende Meldung erhalten (*show Details)*: „Not enough information to check signature valditity. Signed on 22 Mar 2015 19:15:44 CET by tails@boum.org (Key ID: 0x58ACD84F)“.

Dies bestätigt, dass die Software von Tails unterschrieben wurde und somit korrekt ist. Lasst euch hier nicht von der Validity-Meldung abschrecken: sie sagt nur aus, dass der Tails Schlüssel noch nicht als vertrauenswürdig markiert wurde. Wichtig ist das in der Kommandozeile folgende Nachricht erscheint: „Good Signatur ...“ („Korrekte Unterschrift ...“). Das Warning könnt ihr an dieser Stelle ignorieren[59].

Mac: Tails-Prüfsumme verifizieren

Zur Überprüfung des sogenannten Hashwerts benötigt ihr das Programm *Checksums calculator*, welches über die entsprechende URL aus der Tabelle bezogen werden kann. Die **sha256**-Prüfsumme findet ihr ebenfalls in der Tabelle.



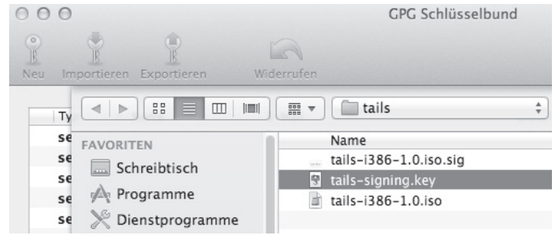
Zum Berechnen und Überprüfen der Checksummen vom Checksum Calculator und von Tails, verfahrt ihr wie unter Windows.

Mac: PGP Signatur prüfen

Wenn ihr die OpenPGP Signatur von Tails durch ein Programm mit einer grafischen Oberfläche überprüfen wollt, müsst ihr euch **gpgtools** dafür besorgen. Links und Checksummen sind in der Tabelle.

59 https://tails.boum.org/doc/get/verify_the_iso_image_using_the_command_line/index.en.html

Ihr könnt den Hashwert wie bereits zuvor beschrieben über den *Checksums calculator* überprüfen. Den PGP-Schlüssel der Tails-Entwickler*innen importiert ihr über das Unterprogramm *„GPG Schlüsselbund“*: *GPG Schlüsselbund ▸ Importieren:* tails-signing.key



Die Signatur könnte ihr durch einen *rechten Mausklick* auf die Signatur-Datei überprüfen. Dafür müsst ihr **„Öffnen mit ▸ GPGServices.service“** auswählen.

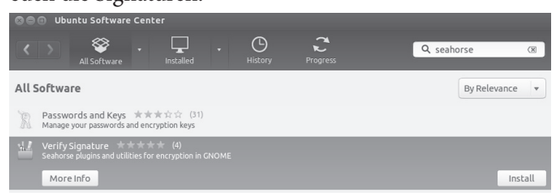
Nach einer kurzen Wartezeit sollte ein Fenster mit den Verifikationsergebnissen erscheinen: Auch hier muss *„Signed by: Tails developers (signing key)“* stehen.

Linux: Tails-Prüfsumme verifizieren

Eine Möglichkeit zur Überprüfung der Hashwerte bietet auch unter Linux das Programm **Checksums calculator** (Links und Checksummen in der Tabelle). Wie ihr damit die Hashwerte von Dateien überprüfen könnt, findet ihr im Abschnitt „Mac: Tails Prüfsumme verifizieren“.

Linux: PGP Signatur prüfen

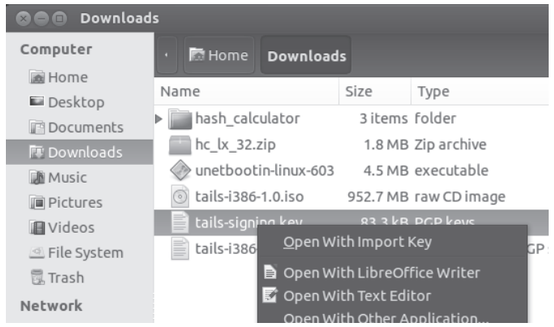
Unter Linux habt ihr die Möglichkeit die Signatur von *tails-i386-X.Y.Z.iso.sig* über grafische Tools zu testen. Dafür müsst ihr über das Ubuntu Software Center nach *„seahorse“* suchen und das gefundene Paket anschließend installieren. Das Software Center überprüft dabei für euch die Signaturen.



Nach erfolgreichem Download müsst ihr den Tails Entwickler Schlüssel noch importieren. Dafür klickt ihr mit der *rechten Maustaste* auf die Datei *„tails-signing.key“* und wählt die Option *„Open With Import Key“ (Mit Schlüssel importieren öffnen)* aus dem dem Drop-Down-Menü aus.

Nach kurzer Zeit sollte eine Meldung erscheinen, dass der Schlüssel importiert wurde.

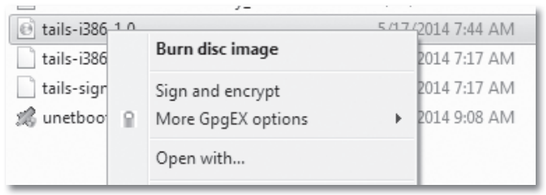
Nachdem ihr euch die Signatur des Tails-Image geholt habt, müsst ihr mit der *rechten Maus-Taste* auf die Datei klicken und **„***Open With Verify Signature*“ (*„Mit Signatrur-Datei überprüfen öffnen*“) auswählen. Nach einer kurzen Wartezeit sollte eine Meldung erscheinen, dass es sich um eine passende Signatur handelt.



Tails auf DVD brennen

Windows

Nachdem ihr nun davon ausgehen könnt, dass ihr eine korrekte Version von Tails besitzt (z.B. *tails-i386-1.3.1.iso)* muss das Betriebssystem noch auf eine DVD gebrannt werden.Verwendet dafür am besten eine *nicht-wieder-beschreibbare DVD* mit der Bezeichnung: DVD + R. Sie sollte auf keinen Fall die Bezeichnung DVD + RW oder DVD + RAM besitzen.



Um die DVD zu brennen müsst ihr mit der rechten Maustaste auf die Tails.iso-Datei klicken und „*Datenträgerabbild brennen*“ auswählen. Anschließend muss noch der Brenner ausgewählt werden und der Button „*Brennen*“ betätigt werden.

Als Alternativ-Software kann auch der Infra-Recorder zum Brennen der Tails-Live-CD genutzt werden (siehe Tabelle).

Mac

Um Tails auf eine DVD zu brennen müsst ihr das „*Festplattendienstprogramm*“ unter „*Programme/Dienstprogramme*“ öffnen und die Tails.iso Datei dort hinein ziehen. Danach kann das Live-System über den Button „*Brennen*“ auf eine DVD gebrannt werden.

Alternativ könnt ihr Tails auch über das „*Festplattendienstprogramm*“ durch „► *Images* ► *Brennen*“ dauerhaft auf eine DVD bringen.

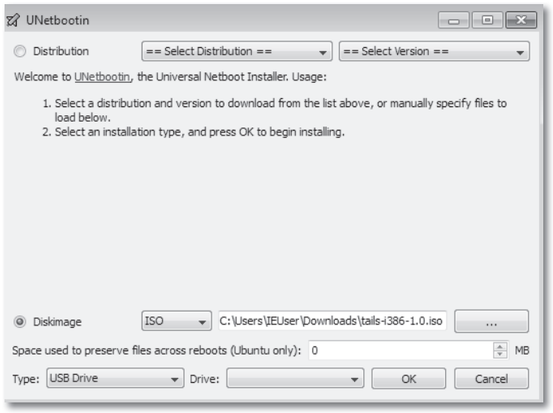
Linux

Tails könnt ihr euch unter Ubuntu oder Debian auf DVD brennen, indem ihr mit der *rechten Maustaste* aus die Tails.iso Datei klickt und „*Open With Brasero Disc Burner*“ (*„Mit Brasero öffnen“)* auswählt. Mit einem Bestätigen über den Button „*Create Image*“ (*„Abbild erstellen“)* wird Tails auf eine DVD gebrannt.[60]

Tails auf USB-Stick installieren

Windows

Der einfachste Weg hierfür ist die Nutzung der Software **UNetbootin** (siehe Tabelle).



Nach Öffnen des Programms müsst ihr „*Diskimage*“

60 Für neuere Ubuntu-Versionen (nach 12.10) findet ihr eine Anleitung zum Erstellen der DVD unter folgender Webseite: https://help.ubuntu.com/community/BurningIsoHowto

auswählen und den Button auf der rechten Seite mit der Bezeichnung „ ...“ drücken und anschließend die zuvor heruntergeladene Tails.iso-Datei auswählen. Nun muss ein USB-Stick in euren Rechner gesteckt werden und nach einem Klick auf den „*OK*“-Button sollte Tails auf dem Stick installiert werden. Am besten ihr entfernt vor diesem Vorgang sämtliche externen USB-Festplatten um nicht aus Versehen einen Datenträger von euch zu überschreiben.

Mac

Da es sich bei der Anwendung zur Erstellung eines Tails-USB-Sticks um dasselbe Programm handelt, könnt ihr die Beschreibung dazu unter *Windows* nachlesen. Über diesen Weg erstellte USB-Sticks sind nicht für Macs nutzbar, sondern nur auf PCs bootfähig[61]. Link und Prüfsumme findet ihr in der Tabelle.

Linux

Da es sich bei der Anwendung zur Erstellung eines Tails-USB-Sticks um dasselbe Programm handelt, könnt ihr die Beschreibung dazu unter *Windows* nachlesen. Ihr könnt euch die Software über das Paketverwaltungssystem von Ubuntu (Software Center) oder Debian besorgen.

Tails-Installer

Wenn ihr schon ein lauffähiges Tails-System auf einem USB-Stick oder einer DVD habt und einen weiteren USB-Stick (keine DVD) erstellen wollt, könnt ihr den „*Tails Installer*“ verwenden. Den „*Tails Installer*“ findet ihr unter *Anwendungen* ► *Tails* ► *Tails Installer*. Wenn ihr ihn startet, erhaltet ihr den folgenden Bildschirm, auf dem ihr zwischen drei Möglichkeiten auswählen könnt:

61 https://tails.boum.org/blueprint/UEFI/

„*Klonen & Installieren*“ wählt ihr aus, wenn ihr die Tails Version des laufenden System auf einen anderen USB-Stick übertragen wollt. Alle Daten auf dem anderen USB-Stick werden dabei gelöscht. Es wird ausschließlich das Tails System übertragen, nicht eventuell vorhandene Daten der Tails-Persistenz.

„*Klonen & Aktualisieren*“ wählt ihr aus, wenn auf dem zu beschreibenden USB-Stick bereits ein Tails-System vorhanden ist und ihr dieses nur mit dem aktuelleren Tails, von dem ihr gerade gestartet habt, überschreiben möchtet. Eventuell vorhandene Daten der Tails-Persistenz werden auf dem Datenträger nicht überschrieben. Auch hier werden keine Daten der Tails-Persistenz des aktuell gestarteten Systems übertragen.

„*Von ISO aktualisieren*“ wählt ihr aus, wenn auf dem zu beschreibenden USB-Stick bereits ein Tails-System vorhanden ist und ihr dieses mit einem heruntergeladenen ISO-Abbild einer neueren Tails Version überschreiben möchtet.

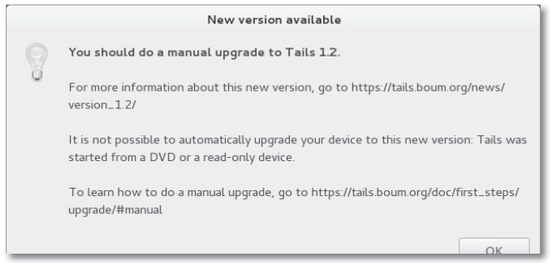
Spätestens nachdem ihr euch für eine Funktion entschieden habt, müsst ihr den USB-Stick einstecken, der das neue Tails-System erhalten soll. Um zu vermeiden, den falschen USB-Stick zu löschen, solltet ihr darauf achten, dass außer dem originalen und dem zukünftigen Tails-Stick keine anderen USB-Sticks oder SD-Karten eingesteckt sind. Ist dies der Fall, wird im nächsten Fenster als „*Zielmedium*“ nur eine Option, euer eingesteckter USB-Stick, vorhanden sein (siehe Abbildung). Andernfalls muss der gewünschte USB-Stick als Zielmedium ausgewählt werden. Nachdem ihr nun auf „*Tails installieren*“ geklickt habt, müsst ihr noch einmal bestätigen, dass ihr auch wirklich diesen Stick überschreiben möchtet. Danach kann die Erstellung des neuen Sticks ein paar Minuten in Anspruch nehmen. Ausschließlich bei der dritten Option „*Von ISO aktualisieren*“ müsst ihr zusätzlich noch das zu verwendende, bereits heruntergeladene Live-System-ISO-Abbild auswählen.

Tails-Upgrader

Bei jedem Start von Tails wird, direkt nachdem die Verbindung zu dem *Tor*-Netzwerk hergestellt wurde, überprüft, ob die aktuelle Tails Version verwendet wird.

Es ist wichtig, immer die aktuelle Version zu verwenden, da regelmäßig Sicherheitslücken in den von Tails verwendeten Programmen entdeckt werden, die im schlimmsten Fall dazu führen, dass eure Identität, eure IP-Adresse, etc nicht verschleiert werden. Durch ein Tails Upgrade werden diese Sicherheitslücken gestopft und meist auch andere Fehler behoben.

Falls ihr Tails mit DVD verwendet oder Tails manuell auf den USB-Stick gespielt habt ohne die Verwendung des Tails Installers, bekommt ihr die Meldung „You should do a manual Upgrade“. Das heißt ihr solltet manuell eine neue Version von Tails herunterladen, überprüfen und auf DVD brennen oder einen USB-Stick spielen.



Habt ihr jedoch euer Tails mit dem Tails Installer auf einen USB-Stick gespielt, habt ihr nun Glück, denn in diesem Fall macht der Tails Upgrader für euch die Arbeit. Ihr werdet gefragt ob ihr ein Upgrade sofort oder später durchführen wollt. Wenn ihr auf „Upgrade Now“ klickt, wird das Upgrade automatisch heruntergeladen und überprüft. Dies erspart euch die aufwendigere Überprüfung der Checksumme, die ihr durchführen solltet, wenn ihr ein ISO-Abbild herunterladet. Wenn der Download-Vorgang beendet ist, wird das Upgrade auf eurem USB-Stick installiert. Nach einem Neustart ist das Tails-System auf dem aktuellen Stand. Daten auf einer eventuell vorhandenen Tails-Persistenz sind davon nicht betroffen und bleiben weiterhin bestehen. Falls ein Stick mit Schreibschutzschalter verwendet wird, müsst ihr diesen natürlich für die eine Sitzung, in der ihr das Upgrade durchführt, auf beschreibbar stellen.

Bekommt ihr allerdings nach dem Start von *Tor* die Meldung „Nicht genügend Speicher vorhanden, um nach Aktualisierungen zu suchen.“ hat euer Rechner zu wenig Arbeitsspeicher oder ihr habt schon speicherhungrige Programme wie LibreOffice oder den *Tor*-Browser gestartet. In diesem Fall kann es helfen, nach einem Neustart und der Meldung „*Tor* ist bereit“ zunächst keine weiteren Programme zu starten.

Bootreihenfolge im BIOS ändern

Um euren Rechner in die Lage zu versetzen, ein Betriebssystem von DVD bzw. vom USB-Stick starten (=„booten“) zu können, müsst ihr in der Regel die „Boot-Reihenfolge“ im sogenannten BIOS ändern. Das BIOS ist sozusagen das Basis-Betriebssystem eines Rechners, das grundlegenden Rechnerfunktionen an/ausschaltet und festlegt, in welcher Reihenfolge beim Start auf welchen Datenträgern nach bootfähigen Betriebssystemen gesucht werden soll.

- Datenträger einlegen/einstecken und Computer neu starten.
- Unmittelbar nach dem Start eine der Tasten F1, F2, DEL, ESC, F10 oder F12 gedrückt halten (auf einen Hinweis auf dem kurz erscheinenden Startbildschirm achten), um in das BIOS-Setup zu gelangen. Die meisten Rechner bieten nur ein englisch-sprachiges BIOS-Menü.
- Suche im Menü nach „*Edit Boot Order*“ (Boot-Reihenfolge ändern).
- Setze den Eintrag „*DVD*“ oder aber einen der Einträge „*removable drive*“, „*external USB disk*“ oder „*USB media*“ an den Anfang der Liste der zu durchsuchenden Geräte. Auf jeden Fall vor den Listeneintrag eurer internen Festplatte „*HD*“ oder „*harddisk*“.
- Danach mit „*Save changes and exit*“ das BIOS verlassen und den Betriebssystemstart fortsetzen. Jetzt sollte der Rechner die geänderte Boot-Reihenfolge berücksichtigen.

Booten „fremder Systeme“ zulassen

Falls Tails trotz geänderter Boot-Reihenfolge nicht startet, und der Tails-Stick bzw. die Tails-DVD korrekt erstellt wurde[62], dann überprüft bei neuerem Computer, ob ihr im BIOS eine der folgenden Funktionen finden und auswählen könnt:

- Enable Legacy mode
- Disable Secure boot
- Enable CSM boot
- Disable UEFI

62 Einfach durch Test an einem anderen Computer zu überprüfen!

Wenn Tails nicht vom USB-Stick startet

- Bootreihenfolge im BIOS überprüfen – sucht das BIOS wirklich auf einem externen USB-Gerät bevor die Festplatte durchsucht wird?
- Ältere Rechner (vor 2001) sind teilweise nicht in der Lage von USB zu „booten“.
- Andere externe USB-Geräte zum Start abziehen.
- Verwende einen anderen USB-Anschluss – Das BIOS mancher Rechner überprüft bei der Suche nach bootfähige Datenträgern nur „die ersten“ der vorhandenen USB-Anschlüsse.
- Überprüfe ob der Stick wirklich „bootfähig“ ist. Führe erneut die Schritte zum „Brennen“ des USB-Sticks durch. Es genügt nicht, die Dateien auf den Stick zu „kopieren“.

Mac booten

Beim Hochfahren eures Macs müsst ihr die *Alt-Taste* oder die *C-Taste* gedrückt halten, damit anschließend die Tails-DVD als Startmedium bestimmt wird (oft wird sie fälschlicherweise als Windows-CD angezeigt). Alternativ könnt ihr sie auch unter „*Systemeinstellungen* ▸ *Startvolume*“ auswählen. Bei Mac-Laptops ist das Track-Pad unter Tails oft nicht richtig nutzbar.

Sicherere Passwortwahl

Es ist immer noch so, dass gängige Verschlüsselungstechniken (bei ausreichender Schlüssellänge) „*nicht knackbar*“ sind, bzw. der Rechenaufwand für Geheimdienste dazu gigantisch hoch ist.

Hauptangriffspunkt, um an verschlüsselte Daten zu kommen, ist daher meist das verwendete Passwort, mit dem z.B. ein Schlüssel gesichert ist. Mit bereits im Einzelhandel erhältlichen Computern, die leistungsfähige Grafikchips für einfache Rechenoperationen nutzen, ist das Knacken von Passwörtern für Angreifer*innen immer einfachergeworden. Eine Mischung aus simpler Rechenleistung, riesigen Tabellen bereits geknackter Passwörter und clever programmierter Software macht das Passwort-Knacken erschreckend effizient. Daher kommt der richtigen Passwortwahl eine wichtige Bedeutung zu.

ERSTENS: Je „unmenschlicher“ desto besser

Rein mathematisch sieht die Lage für uns Passwort-Nutzer*innen gar nicht schlecht aus. Die Zahl aller möglichen Passwörter wächst exponentiell mit deren Länge und der Größe des verwendeten Zeichenraums. Diese muss eine Angreifer*in im Prinzip durchprobieren *(Brute Force-Methode)*, oder aber die Verschlüsselung zur Ablage der Schlüssel auf dem Computer knacken.

Fast alle Angriffe basieren mittlerweile auf Wörterbüchern und Namenslisten erweitert um riesige, gehackte Datenbanken mit mehreren 100 Millionen Passwörtern.

Die Programme zum Knacken von Passwörtern nutzen darüber hinaus zusätzliche „*Regeln*“ *zur Modifizierung* solcher Wörter und orientieren sich dabei an „*menschlichen*“ *Mustern* der Veränderung. Die Kombination von Wörtern sowie das Anhängen von Ziffern und insbesondere die *Ersetzung einzelner Buchstaben*, wie das übliche „*3*“ statt „*E*“ oder „*1*“ statt „*i*“ oder „*l*“ stellen für diese Programme kein Problem dar. Darüber werden selbst sicher aussehende Passwörter wie „*polU09*&l1nk3d1n*“ geknackt.

ZWEITENS: Kein Wort für viele Zwecke

Neben der Komplexität des verwendeten Passworts entscheidet die Art wie es auf eurem Rechner, beim Mail-Anbieter oder Online-Shops abgelegt ist über dessen Sicherheit.

Kein System sollte Nutzer*Innen-Passwörter im Klartext speichern. Aber die Verschlüsselungsmethoden für die Ablage von Passwörtern sind unterschiedlich gut. Beim eigenen Rechner haben wir bedingt Einfluss darauf, wie leicht unsere Passwörter zu rekonstruieren sind. Bei irgendwelchen Diensten im Internet müssen wir (häufig zu Unrecht) darauf vertrauen, dass damit sorgsam umgegangen wird. Millionen geklauter Kundendaten inklusive Passwörter von unterschiedlichen Service-Anbietern sind eindeutiger und dringender Appell, das dort verwendete Passwort nicht identisch für andere, sensiblere Zwecke zu nutzen!

Vollständig zufällige Passwörter mit mehr als 16 Zeichen gelten auf absehbare Zeit als sicher. Sogar bei Verwendung von Supercomputern – aber sie sind auch sehr schwer zu merken. Daher verwenden viele vermeintlich individuelle Kombinationen, Abkürzungen und Veränderungen existierender Worte. Das macht Passwörter angreifbar.

Nun habt ihr wahrscheinlich Probleme, möglichst lange und komplexe Passwörter für jeden genutzten Dienst er-

zeugt zu haben, aber merken könnt ihr euch davon bestenfalls drei oder vier. Die einen nutzen daher spezielle Programme wie *KeePassX* (in Tails), die Passwörter in einer sicheren Datei abspeichern und müssen sich daher nur ein *Master-Passwort* merken. Andere nutzen lieber mehrere Basis-Passwörter, aus denen sie dann verschiedene Varianten generieren. Welche Methode ist sicherer? An der Frage scheiden sich die Geister. Wir wollen euch beide Möglichkeiten vorstellen, entscheiden müsst ihr.

Methode I: Verschlüsselte Passwort-Datei

Alle verwendeten Passwörter werden in einer zentralen, *verschlüsselten Datei* gespeichert. Dies hat den Vorteil, sich nur ein Passwort merken zu müssen. So können für alle anderen genutzten Dienste oder Programme auch möglichst sichere und unabhängig voneinander generierte Passwörter genutzt werden. Aber diese Variante hat auch klare Nachteile. Zum einen seid ihr von der einen Datei oder dem einen Programm abhängig. Geht diese verloren oder ihr vergesst das Passwort, verliert ihr damit im Zweifel auch den Zugriff auf alle damit gesicherten Dienste. Das andere große Problem bei dieser Variante ist, wenn jemand an dieses eine **Master-Passwort** herankommt, z.B. über einen eingeschleusten *Keylogger*[63], hat die Person gleichzeitig **Zugriff auf alle anderen Passwörter!**

Um *KeePassX* zu starten, wählt ihr: *Anwendungen* ▸ *Zubehör* ▸ *KeePassX*.

Um eine neue Passwortdatenbank zu erstellen, wählt ihr *Datei* ▸ *Neue Datenbank*. Die Passwortdatenbank ist verschlüsselt und durch eine Passphrase geschützt. Dazu gebt ihr eine Passphrase eurer Wahl in das Textfeld *Passwort* ein *(mindesetns 16 Zeichen!)* und klickt anschließend auf *OK*. Wiederholt die gleiche Passphrase im nächsten Dialog und klickt dann auf *OK*. Das Programm bietet euch ebenfalls an, starke Passwörter (über einen Zufallszahlengenerator) zu erstellen. Zusätzlich bietet KeyPassX, eine *Schlüsseldatei* auszuwählen, ohne die sich die Datenbank nicht verwenden lässt.

Um die Passwortdatenbank für die zukünftige Verwendung auf einem Datenträger zu speichern, klickt ihr auf *Datei* ▸ *Datenbank speichern*.

63 Ein *Keylogger* zeichnet jeden Tastenanschlag der Tastatur auf und kann somit auch eure Passwörter mitprotokollieren. Ein Keylogger kann eingeschleuste Schadsoftware oder aber auch ein nachträglich in die Tastatur oder am Verbindungskabel eingebauter Chip sein. Gegen letztere Varianten schützt Tails nicht!

Methode II: Individuelle Gedächtnisstütze

Ihr merkt euch eine zufällig gewählte Seite eines euch bekannten Buches und denkt euch daraus eine *fiktive Schablone* aus, die verschiedene Buchstaben eines Satzes oder eine Abschnitts auf dieser Seite markiert. Verändert dann das so entstehende Wort durch das Einfügen von Ziffern und Sonderzeichen und das Anhängen weiterer Worte.

Ein praktisches Beispiel: Ich merke mir den Namen eines mir in Erinnerung bleibenden Buches und die Seite 373. Auf dieser Seite finde ich den Satz „*Er wollte sich mir nicht anvertrauen – und jetzt ist es zu spät.*“ Daraus bastle ich die Basis meines Passworts aus den Anfangsbuchstaben **Ewsmna-Ujiezs**. Dieses **Basis-Passwort** verwende ich nirgendwo. Ich nutze lediglich zwei *verschiedene Ableitungen* davon für unterschiedliche Zwecke. **Variante eins** (die Ziffern der Seitenzahl an ihrer jeweiligen Positionen eingefügt) für den Zugang zu meinem privaten pgp-key: **Ews3mna7-Uji3ezs** sowie **Variante zwei** (373 → §/§ auf einer deutschen Tastatur) für das Entschlüsseln meiner Festplatte: **Ew§/§smna-Ujiezs_against_the_empire**.

Dies ist u.a. vor dem Hintergrund der gesetzlich gedeckten Praxis zur Herausgabe von Passwörtern an Sicherheitsbehörden durch Diensteanbieter absolut notwendig!

> ***Verwendet ein solches Basispasswort zum „Erzeugen“ weiterer Passwörter nur für die gleiche „Klasse“ von Passwörtern. Also Passwörter für** pgp, Datenträgerverschlüsselung **nicht mischen mit solchen für** ebay, amazon.*

Diese Methode hat jedoch den Nachteil, dass sich über die selbst ausgedachten Varianten des Basis-Passworts zwangsläufig menschliche „Muster“ einschleichen, die es eigentlich zu vermeiden gilt.

Überschätzt euch nicht bei der Wahl eines zu komplexen Passworts. Gelingt euch die Rekonstruktion des Passowrt über die Gedechnisstütze nicht bleiben die Daten für *euch* immer unzugänglich.

Es gibt keine 100%ige Sicherheit bei der Auswahl des *„richtigen“ Passworts*. Und es wird, wie ihr in der Ergänzung im nächsten Abschnitt lesen könnt, noch komplizierter, wenn ihr den technischen Fortschritt mitzuberücksichtigen versucht. Letztendlich müsst ihr **zwischen Sicherheit und Nutzbarkeit abwägen** und selbständig entscheiden, was ihr euch zutraut und euren Bedürfnissen nach Sicherheit im Alltagsgebrauch am Nächsten kommt.

Hier nochmal kurz das Wichtigste zusammengefasst:

- Verwendet auf keinen Fall dieselben Passwörter für mehrere Zugänge. Also nicht für euer Mail-Postfach oder euer ebay-Konto dasselbe Passwort verwenden wie für den Zugang zu eurem Rechner.
- Hängt nicht einfach eine Zahlenkombination an ein existierendes Wort.
- Verwendet keine einfachen Buchstabenersetzungen wie m!s3r4b3| ← (MISERABEL).
- Auch keine einfache Zusammensetzung von (leicht veränderten) Wörtern.
- Entscheidet euch für eine der beiden Varianten: Merken oder verschlüsseltes Speichern eurer Passwörter. Notizen auf Zettel sind dabei eine sehr schlechte Alternative.
- Eine sogenannte **Passphrase** (komplexeres Passwort) für die Nutzung eures privaten *PGP-Schlüssel*, oder die Datenträgerverschlüsselung sollte tatsächlich länger und komplexer sein als ein (einfaches) Passwort für euren Mail-Account. Um auch zukünftig noch auf der sicheren Seite zu stehen, sollte sie mindestens 16 Zeichen lang sein.
- Wechselt eure Passwörter regelmässig, je öfter, desto besser.

DRITTENS: In Zukunft unsicher

Wir wollen nicht in die Details kryptografischer Methoden verschiedener Verschlüsselungs-Algorithmen gehen. Nur so viel - die Sicherheit wichtiger Verschlüsselungsverfahren (wie z.B. pgp) basiert auf der Zerlegung sehr großer Zahlen in sogenannte Primfaktoren. Während das Überprüfen, ob ein privater und ein öffentlicher Schlüssel zusammenpassen eine leichte Aufgabe ist, stellt das Auffinden eines zum öffentlichen passenden privaten Schlüssels eine extrem rechenintensive Aufgabe dar. Klassische Computer müssen schlicht alle möglichen Paare von Primfaktoren durchprobieren. *Der Aufwand, eine solche Verschlüsselung (mit klassischen Computern) zu knacken, wächst exponentiell mit der Schlüssellänge.*

Moore's Gesetz

Etwa alle 20 Monate verdoppelt sich die Leistung neuer Computerchips. Das hat mit der immer noch fortschreitenden Miniaturisierung klassischer Schaltkreise in diesen Chips zu tun. Obwohl diese Entwicklung absehbar an physikalische Grenzen stoßen wird, sagen Chipentwickler*innen eine Gültigkeit dieses „Gesetzes“ bis etwa 2025 voraus. *Das gefährdet die Sicherheit der Verschlüsselung mit Schlüsseln mit einer Länge von (weniger als) 2048 Bit.* Bis dahin droht jedoch ein weiteres Problem:

Quantencomputer

Den zur Primfaktor-Zerlegung notwendige Algorithmus hat Peter Shor bereits 1994 (ohne die zugehörige Hardware) entwickelt. Der Rechenaufwand dieses Quantenalgorithmus wächst nicht mehr exponentiell mit der Schlüssellänge. Daher reicht es auch nicht aus, die verwendete Schlüssellänge zu vergrößern. Die Entschlüsselung bleibt auch dann ein für Quantencomputer lösbares Problem. Es müssten dann neue Verschlüsselungsmethoden eingesetzt werden.

> ***Sollte in einigen Jahren die Hardware für universelle Quantencomputer mit ausreichend vielen Quantenbits entwickelt werden, sind aufgezeichnete Daten trotz Verschlüsselung auch rückwirkend lesbar.***

Es klingt zunächst akademisch, hat aber handfeste Konsequenzen für die Sicherheit wirklich sensibler Daten, die ihr z.B. auf einem verschlüsselten USB-Stick ablegt. Sind diese Daten auch in zehn Jahren noch vor unerwünschtem Zugriff sicher? Stellt euch vor, dass eine Behörde oder jemand anderes vor fünf Jahren eine Kopie eines verschlüsselten Datenträgers oder einer verschlüsselten Mail angefertigt hat. Diese Verschlüsselung mag zwar vor fünf Jahren „sicher“ gewesen sein. Sie könnte aber mit deutlichem Zuwachs an gebündelter Hardware und intelligenterer Software in absehbarer Zukunft zu knacken sein!

> ***Überlegt gut, welche Daten überhaupt (selbst verschlüsselt) auf der Festplatte eures Alltagsrechners, per Mail oder über Filesharing-Dienste bei den Schnüffelbehörden landen dürfen!***

Stand April 2015 - Immer die neueste Version herunterladen !!!	**Prüfsumme** *(zur Überprüfung der Software auf ihre Echtheit)*
Software	***Downloadlink***
Tails 1.3.1	*sha256: 897fc177af1596101368160396e85c36922da4ce86a744da3fe47c5bae7832cf*
Tails 1.3.1 *PGP-Signatur*	
Tails-Entwickler-Team *PGP-Schlüssel*	*A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F*
Checksums calculator *Windows*	*sha256: 79229fcf011ec80a4366ce1c7d2d9e829ba20a7cf8943de6d816df82872fa2be*
Checksums calculator *Mac OS X*	*sha256: 7cc313a7f7378142b272d2386495700b7e1d9577290ea7c18b5174a8b26186b121*
Checksums calculator *Linux*	*sha256: 7203f21555becf288fbfae0c7b45f15b569b12329592ba91f6f1c6854db2d229*
Gpg4win 2.2.3 *Windows*	*sha256: 560f97103b302a8cc40879d9272e026acf5303912a71d1d0d198f50e16ed13367*
GPG Suite 2015.02-b5 *Mac OS X*	*sha256: 711e175595fd4c1525de90b741fa0d02793df753465d27c6cefc35eb0573cd33*
InfraRecorder 0.53 *Windows*	*sha256: 8cee83f7f489a6aef4218a953b87b1c22d6a93c966e79275c8cb2abe830d0731*
Unetbootin 608 *Windows*	*sha256: fd982d09a59d89cebf17bca3fee6ad0e54b692e3d711ec38af9f9412c864fec5*
Unetbootin 608 *Mac OS X*	*sha256: 6348a25607b08426759063a77719b208f3efef3cf0721c3dbcc521b32e6a5ad5*

Index

Hefte zur Förderung des Widerstands gegen den digitalen Zugriff
Band I: Tails - The amnesic incognito live system

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

zweite erweiterte Auflage