Fachhochschule Wedel
Seminararbeit

Fachrichtung
Wirtschaftsingenieurwesen

Kryptoparty Anonymität: Tor-Browser und OnionShare

Erstellt von:	Bastian Stender (Mat-Nr. 101141) wing101141@fh-wedel.de
Erarbeitet im	8. Semester
Abgegeben am:	17.06.2018
Betreuender Dozent:	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 140 22880 Wedel Tel. (04103) 804824 E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

Durch die stark gestiegene Überwachung unserer Internetaktivitäten durch Regierungen, Großkonzerne oder Hacker, wird der Selbstschutz in diesem Bereich immer wichtiger.

Schon lange werden unsere Suchverläufe von Suchmaschinen wie Google genau aufgezeichnet und analysiert, um uns die auf uns zu geschnittene Werbung zu bieten. Man kann sagen, dass die Privatsphäre im Internet nicht respektiert wird und wir in diesem Bereich, ohne eigene Maßnahmen, schutzlos dastehen. Auch der Austausch von Nachrichten oder Dateien kann man nicht Tätigen, ohne dass dieser überwacht wird.[1]

Noch vor einigen Jahren wurde diese Überwachung nicht stark behandelt und nur die wenigsten haben sich Gedanken darüber gemacht. Aber spätestens seit der Snowden-Affäre im Jahr 2013 ist dieses Thema aktuell und nicht nur Experten beschäftigen sich mit einer sicheren Nutzung des Internets.

Obwohl vielen Leuten die Überwachung durchaus bewusst ist, wissen sie nicht, wie sie sich davor schützen können. Ein weit verbreiteter Irrglaube ist außerdem, dass die meisten Maßnahmen zum anonymen Surfen im Internet illegal sind.

Diese Arbeit beschäftigt sich mit zwei Maßnahmen, um seine Privatsphäre im Internet zu schützen. Die erste Maßnahme wird sich mit dem anonymen Surfen im Internet beschäftigen. Die zweite Maßnahme erklärt das Verschicken von Dateien ohne die Überwachung von Dritten. Dabei wird besonders auf die praktische Umsetzung eingegangen.

[1] (T.Hübner, 2015)

2. Tor-Browser

Der Tor-Browser ist ein Internet Browser wie Firefox, Google Chrome oder Microsoft Edge. Die Benutzung unterscheidet sich nur geringfügig und auch die Installation funktioniert wie bei jedem anderen Programm. Der größte Unterschied besteht in der Sicherheit und der Anonymität bei der Nutzung, welche beim Tor-Browser deutlich besser sind. Als Nachteil ist die Geschwindigkeit zu nennen, welche durch die erhöhte Sicherheit niedriger ist als bei den anderen Browsern.

Die verbesserte Sicherheit und das langsamte Surfen im Internet liegen an dem Zwiebelprinzip des Tor-Browser, bestehend aus drei Verschlüsselungsschichten, welches auch das Logo von Tor bildet. Verwendet man den Tor-Browser, wird dieser bei der Verbindung ins Internet nicht direkt eine Verbindung herstellen. Der Tor-Browser baut eine Verbindung über drei andere Computer bzw. IP-Adresen auf. Dadurch kann nicht zurückverfolgt werden von wo man ins Internet geht. Im weiteren Verlauf dieser Arbeit wird dies noch gezeigt werden.
Einen weiteren Vorteil bilden die bereits vorinstallierten Add-ons „HTTPS Everywhere“ und „NoScript“. Diese Add-ons können zwar auch bei anderen Browsern installiert werden, beim Tor-Browser muss man sich darum allerdings nicht selbst kümmern.

Durch den Tor-Browser ist auch der Zugang ins Darknet möglich. Auch dies ist mit einem herkömmlichen Browser nicht möglich. Das „Hidden Wiki“ ist eine Ansammlung an Links die unter anderem auch in das Darknet führen. [2][3]

In den folgenden Seiten wird der Download, die Installation und der Umgang mit dem Tor-Browser erklärt und erläutert.
Um diese Schritte durchführen zu können, ist kein extra Programm oder Zusatzwissen erforderlich. Man benötigt lediglich einen Computer mit Internetzugang. Als Betriebssystem können Windows, Apple MacOS oder Linux verwendet werden. Außerdem sind sowohl 32-bit wie auch 64-bit Versionen erhältlich.

[2] (M.Humpa, 2018)
[3] (Anon., 2018)

2.1 Installation des Tor-Browsers

Um den Tor-Browser Downloaden zu können, benutzt man am besten die offizielle Internetseite von Tor, *https://www.torproject.org/projects/torbrowser.html.en?* . Hier erfährt man alles, was man über Tor wissen muss und wie man den Browser downloaden kann. Die Internetseite ist nur auf Englisch, allerdings sind keine großen Englischkenntnisse erforderlich.

Falls man sich vor dem Download noch etwas informieren möchte, gibt es eine Infoseite, wo alles über den Tor-Browser steht. Diese Option befindet sich in der Oberen Leiste unter „About Tor“. Durch einen Links-Klick auf diesen Reiter öffnet sich das folgende Fenster:

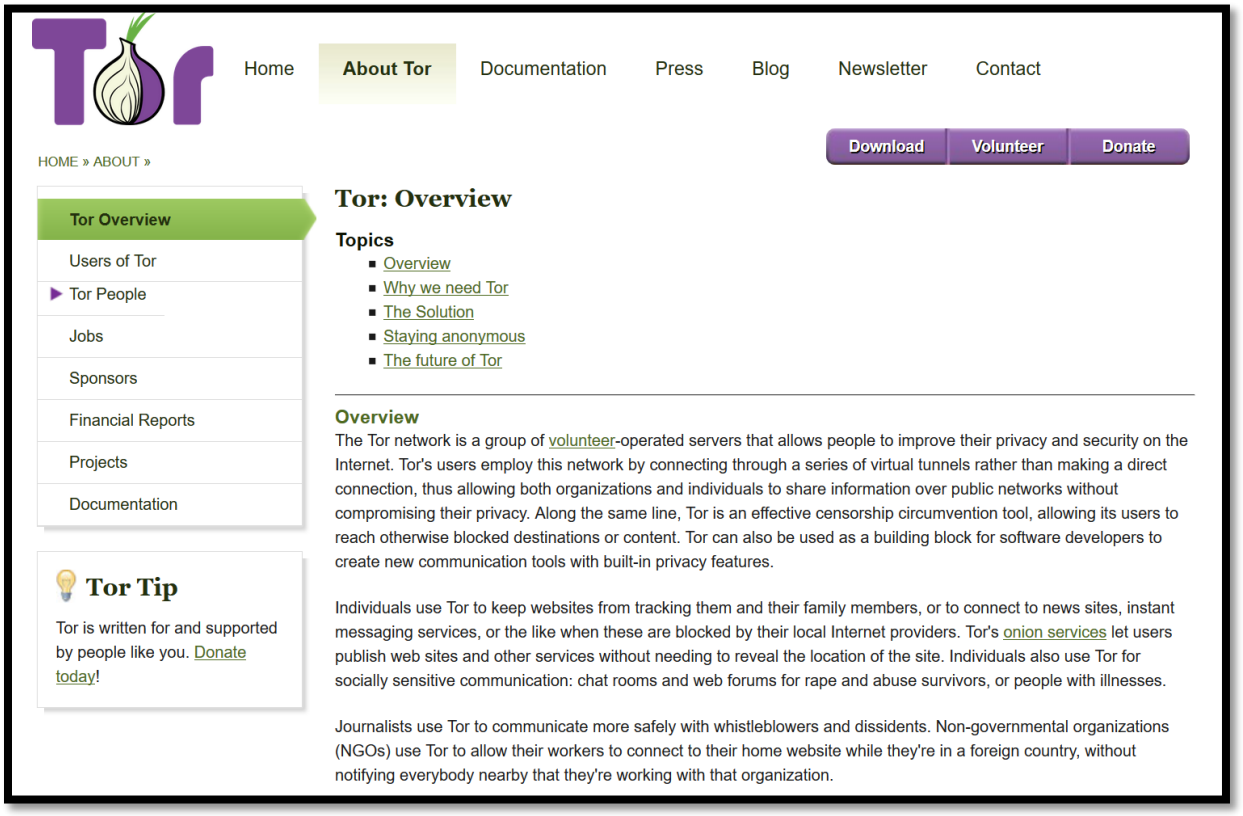
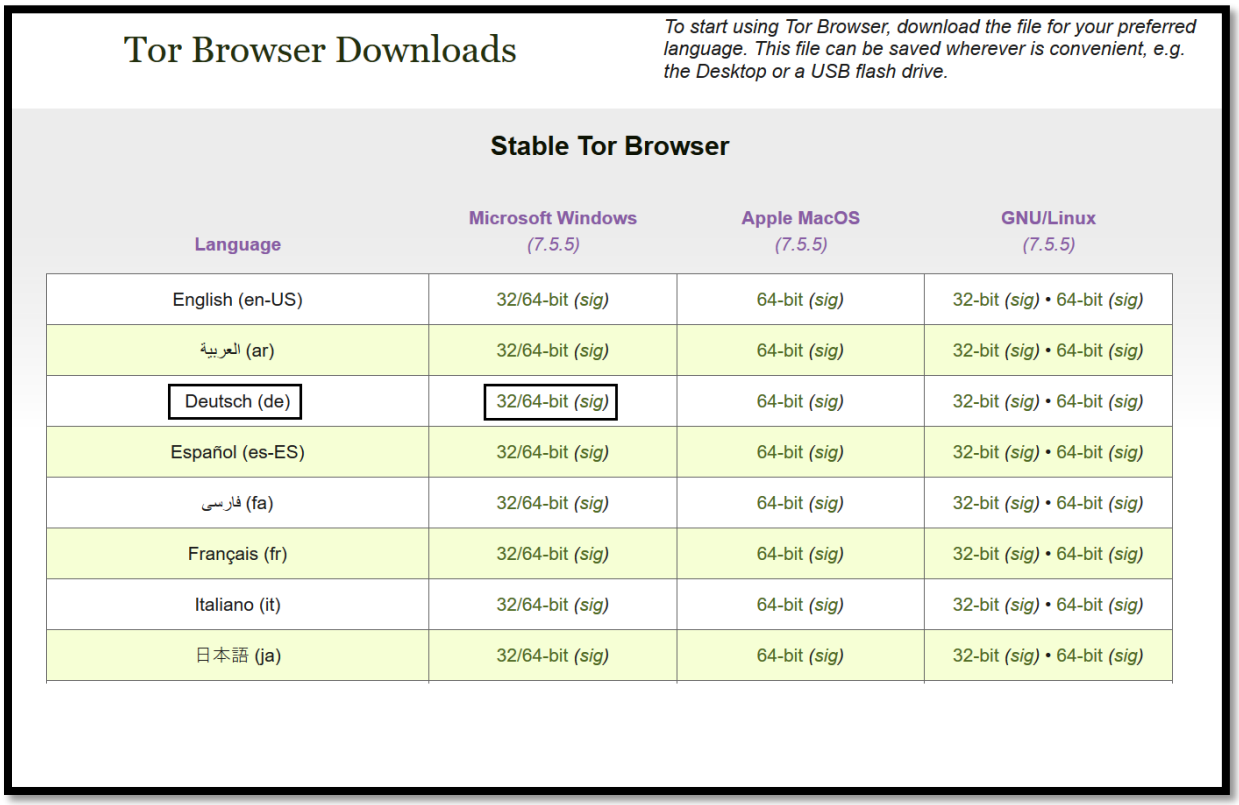


Abbildung 1 About Tor

Die Infoseite ist auch in „Topics“ eingeteilt um die Navigation noch einfacher zu machen. Auf der linken Seite kann man sich zusätzlich noch über anderen Dinge, wie z.B. Sponsoren und andere Projekte, informieren.

Um den Tor-Browser zu downloaden scrollt man auf der Startseite ein Stück herunter und erhält eine große Auswahl an Downloadmöglichkeiten. Hier kann zwischen den Sprachen und den Betriebssystemen gewählt werden. In dieser Arbeit wird Windows als Betriebssystem verwendet und dient somit als Vorlage.
Wir wählen die deutsche Version mit Windows:



Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

Stable Tor Browser

Language	Microsoft Windows *(7.5.5)*	Apple MacOS *(7.5.5)*	GNU/Linux *(7.5.5)*
English (en-US)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
العربية (ar)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
Deutsch (de)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
Español (es-ES)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
فارسی (fa)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
Français (fr)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
Italiano (it)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*
日本語 (ja)	32/64-bit *(sig)*	64-bit *(sig)*	32-bit *(sig)* • 64-bit *(sig)*

Abbildung 2 Downloadmöglichkeiten

Nach dem Anklicken der 32/64-bit Version startet der Download automatisch. Nach Abschluss des Downloads kann die Datei ausgeführt werden.
Als Erstes wird, wie bei fast allen Programmen, die Sprache ausgewählt. Danach wird der Speicherort ausgewählt. Es bietet sich hier an den Desktop zu nutzen, weil man im Nachhinein diesen Ordner auf einen USB-Stick ziehen kann und man den Tor-Browser somit jederzeit und überall nutzen kann. Nach der Installation kann man noch die Haken bei „Tor ausführen“ und „ Add Start Menu“ entfernen falls man dies nicht möchte. Durch einen Klick auf „Fertig stellen“ ist die Installation abgeschlossen.

Der entstandene Ordner auf dem Desktop „Tor Browser“ kann jetzt geöffnet werden. Hier befinden sich ein weiterer Ordner und eine Verknüpfung. Der Ordner enthält alle Dateien um den Tor-Browser nutzen zu können, deswegen funktioniert dieser auch von einem USB-Stick aus. Die Verknüpfung startet den Tor-Browser direkt. Durch einen Klick auf die Verknüpfung startet sich der Tor-Browser und es erscheint folgender Hinweis:

Abbildung 3 Tor verbinden

Dieser Hinweis erscheint nur beim ersten Starten und ist nur für bestimmte Nationalitäten wichtig. In Deutschland ist der Tor-Browser erlaubt und durch einen Klick auf „Verbinden“ starten wir den Browser. Wohnt man allerdings in einem Land wie China, wird der Tor-Browser blockiert. In diesem Fall kann man die Regierung durch einen Klick auf „Konfigurieren“ umgehen.

2.2 Bedienung des Tor-Browsers

Der Tor-Browser ist nun in einem kleinen Format geöffnet und einsatzbereit. Man kann das Fenster vergrößern, allerdings rät der Tor-Browser einem davon ab, weil man dadurch leichter verfolgt werden kann.
Als Erstes sollte man die Sicherheitseinstellungen des Tor-Browsers einstellen. Diese Option befindet sich links oben durch einen Klick auf die „Zwiebel“.

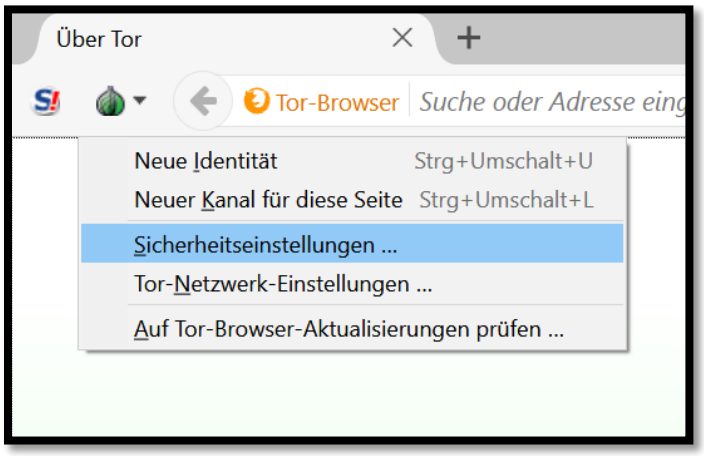


Abbildung 4 Sicherheitseinstellungen

Durch die Auswahl der Sicherheitseinstellungen öffnet sich ein weiteres Fenster wo man zwischen Standard, Sicherer und am Sichersten wählen kann. Der Text rechts daneben beschreibt die einzelnen Änderungen. Man sollte hier die oberste Möglichkeit, am Sichersten, wählen um optimal geschützt zu sein.

Die restliche Seite des Tor-Browsers dient der Informationsgewinnung. In der Mitte befindet sich die Suchmaschine des Tor-Browsers „DuckDuckGo“. Google funktioniert mit dem Tor-Browser nicht. Da der Tor-Browser wie Firefox aufgebaut ist, befindet sich auf der rechten Seite das Menü, um die bereits erwähnten Add-ons zu finden.

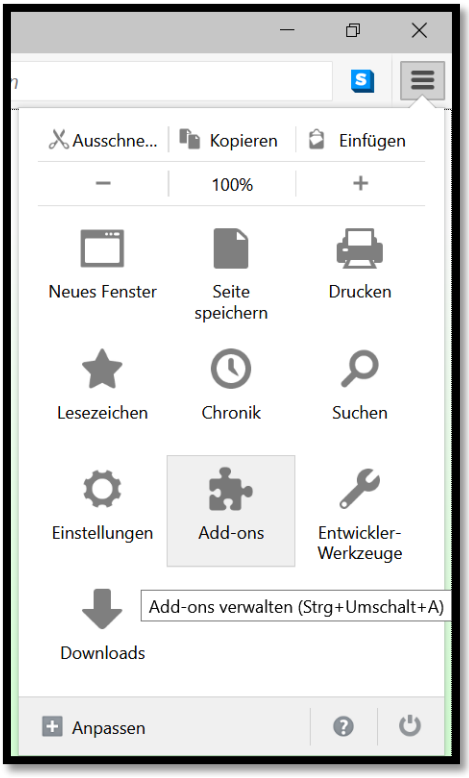


Abbildung 5 Add-Ons

Der Tor-Browser hat zurzeit noch keine Verbindung ins Internet aufgebaut. Dies kann man durch einen Klick auf die Zwiebel oben rechts sehen, weil dort die Verschlüsselungsschichten angezeigt werden – dort steht noch nichts.
Durch das Eingeben eines Suchbegriffs bei „DuckDuckGo“ baut der Tor-Browser eine Verbindung auf. Bevor die Seite geladen wird, erscheint ein Hinweis, ob der Tor-Browser nur englische Seiten anzeigen soll, dies erhöht die Sicherheit. Nach dem Klick auf „Ja“ oder „Nein“, je nachdem wie sicher man seinen Browser möchte, baut sich die Verbindung auf. Worüber diese Verbindung läuft, lässt sich durch einen Klick auf die Zwiebel sehen.

Abbildung 6 Verschlüsselungsschichten

An diesem Beispiel ist zu erkennen, dass der Tor-Browser erst eine Verbindung an eine IP-Adresse in Deutschland, dann nach Amerika und zum Schluss nach Irland aufbaut bevor er tatsächlich die gewünschte Seite aufruft.

Der Tor-Browser ist nun vollständig nutzbar. Im Folgenden befinden sich noch zwei Webseiten mit Links für das Tor-Netzwerk und für das Darknet. Diese sind nur mit dem Tor-Browser erreichbar, weil diese das Kürzel „.onion“ besitzen.

Tor-Links (Alphabetisch geordnete Linkliste): *http://torlinkbgs6aabns.onion*

Hidden-Wiki (Auflistung zahlreicher Webseiten): *http://wikitjerrta4qgz4.onion*

3. OnionShare

Mit dem Tor-Browser kann man sich jetzt zwar anonym im Internet bewegen, aber das anonyme verschicken von Dateien ist noch nicht möglich. Möchte man aber auch beim Weitergeben von Dateien jeglicher Art anonym sein, benötigt man ein spezielles Programm. Wenn man zudem in der Dateigröße nicht eingeschränkt sein möchte, ist OnionShare das einzige Programm, um dies zu realisieren.

Das Programm OnionShare wurde von Micah Lee im Jahre 2014 veröffentlicht und ist somit seine Antwort auf die Snowden-Affäre von 2013. Zu dieser Zeit existierten zwar schon Programme um mit anderen anonym zu schreiben, aber bei Dateien hatte man keine Möglichkeit diese anonym zu verschicken.[4]

OnionShare funktioniert im Prinzip wie alle anderen Filehosting Dienste z.B. Google Drive oder Dropbox. Der wohl größte Unterschied liegt darin, dass OnionShare ausschließlich mit dem Tor-Browser bzw. dem Tor-Netzwerk arbeitet und somit automatisch von den Vorteilen des Tor-Browsers profitiert. Möchte man eine Datei zum Download bereitstellen, erstellt OnionShare eine temporäre Webseite mit einer spezifischen URL-Adresse. Nur über diese kann man die Webseite, und somit die Dateien erreichen. Hier liegt auch das einzige Problem von OnionShare, die Übertragung der URL-Adresse an den Empfänger. Hierfür gibt es tendenziell viele Möglichkeiten wobei hier nur drei kurz erklärt werden.[5]

Die erste und einfachste Möglichkeit ist die Versendung der URL-Adresse per E-Mail. Sollte aber diese E-Mail abgefangen werden, hat der Hacker auch den Link und somit die Datei.

Die zweite Möglichkeit ist das vorherige Verschlüsseln der URL-Adresse und dem anschließenden Verschicken per E-Mail. Auf diese Weise kann der Hacker die E-Mail zwar abfangen, erreicht aber trotzdem nicht die Datei.

Die dritte Möglichkeit besteht darin, dass man einen sicheren Chat benutzt, welcher über das Tor-Netzwerk läuft. Hierfür gibt es einige Alternativen.

In den folgenden Seiten wird der Download, die Installation und der Umgang mit OnionShare erklärt. Möchte man lediglich Dateien empfangen, benötigt man nur den Tor-Browser aber nicht das Programm OnionShare. Möchte man Dateien selber verschicken, benötigt man sowohl den Tor-Browser als auch das Programm OnionShare.

[4] (J. Thoma, 2014)
[5] (J.E. Burkert, 2018)

3.1 Installation von OnionShare

Um OnionShare zu downloaden kann man selbstverständlich den Tor-Browser benutzen, dies wird allerding länger dauern als z.B. mit Firefox. Für welche Variante man sich auch entscheidet, der Download erfolgt am besten von der eigenen OnionShare Internetseite: *https://onionshare.org/* . Die Internetseite ist sehr einfach aufgebaut. Möchte man sich vorab noch mehr informieren, drückt man auf das Icon „Lern More“.
Für den eigentlichen Download kann man zwischen MacOS und Windows wählen. Durch einen Klick auf das verwendete Betriebssystem beginnt der Download.

Abbildung 7 Download OnionShare

Durch die Ausführung der heruntergeladenen Datei, muss als Erstes ein Speicherort festgelegt werden. Dieser ist frei wählbar. Man sollte aber wissen, wo dieser ist, da sich die Datei, die man zur Nutzung des Programmes benötigt, mit in diesem Verzeichnis befindet.

Nach einem Klick auf „Install“ startet die Installation. Nach dem Abschluss klickt man auf „Close“ und öffnet den entstandenen Ordner „OnionShare“, welcher sich im vorher gewählten Arbeitsverzeichnis befindet.

3.2 Bedienung von OnionShare

Der Ordner „OnionShare“ enthält alle Dateien, die das Programm zur Nutzung benötigt. Zur Ausführung von OnionShare muss die Anwendung „onionshare-gui“ gestartet werden.

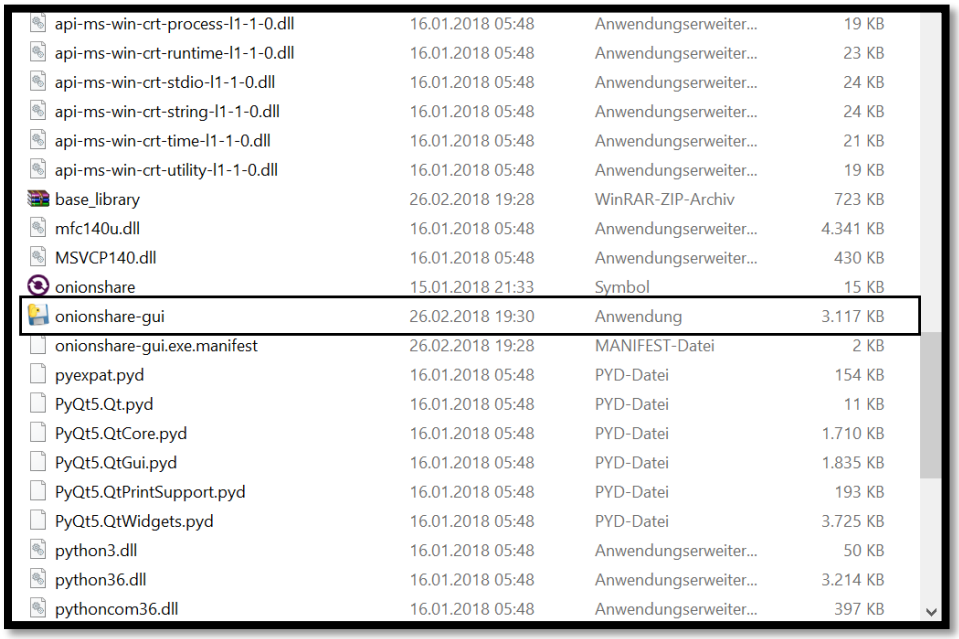


Abbildung 8 Start von OnionShare

Das Programm beginnt sofort, eine Verbindung mit dem Tor-Netzwerk aufzubauen. Dies kann eine kurze Zeit dauern. Nachdem die Verbindung aufgebaut ist, erscheint ein kleines Fenster in der Mitte des Bildschirms. In der Mitte dieses Fensters steht „Drag&Drop“, man kann dort also seine Dateien, die man verschicken möchte, hineinziehen.

Bevor man allerdings seine Dateien online stellt um sie zu verschicken, sollte man die Einstellungen überprüfen, welche sich unten rechts befinden – das kleine Zahnrad. Durch einen Linksklick öffnen sich die Einstellungen. Dieser Bereich ist ausschließlich auf Englisch und bietet viele Einstellungsmöglichkeiten.

Im Folgenden werden die einzelnen Bereiche, die dort eingestellt werden können erklärt.

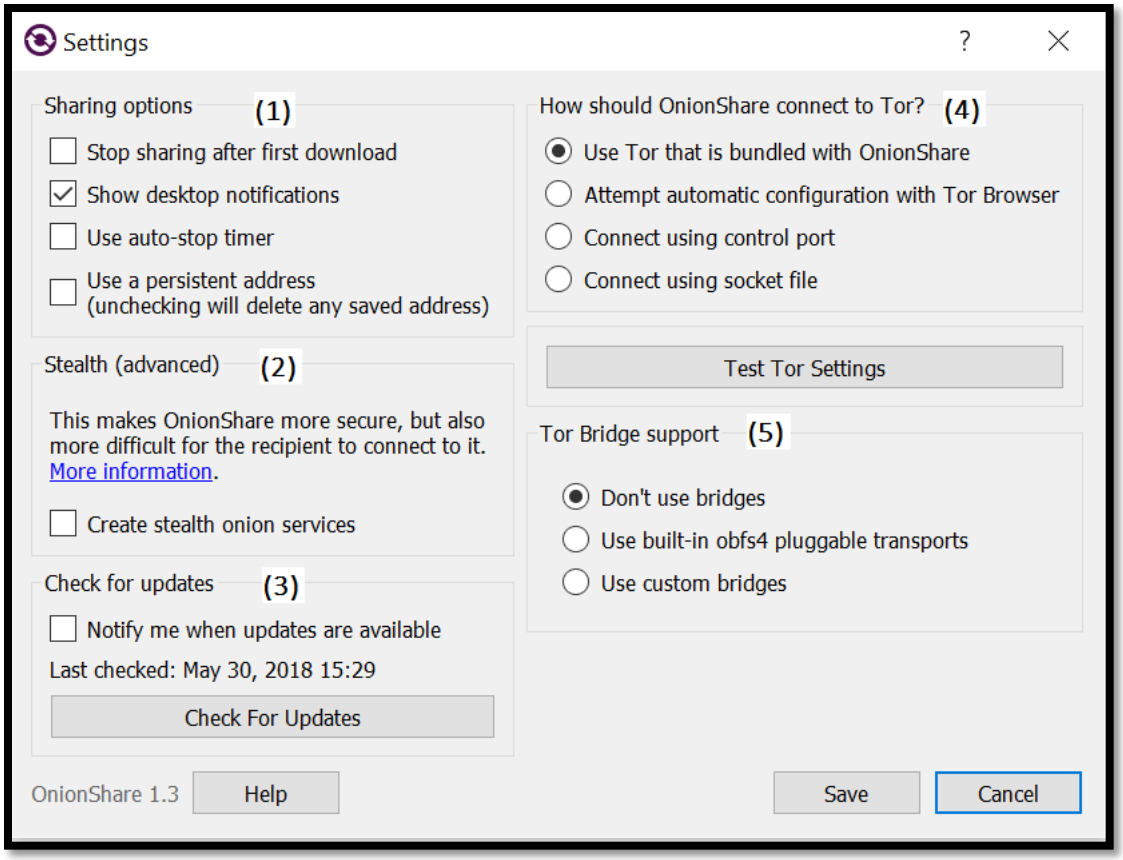


Abbildung 9 OnionShare Einstellungen

1. Hier lässt sich einstellen ob der Download nur für eine Person, oder für mehrere Personen zugelassen ist. Man kann aber auch die Möglichkeit des Downloads mit einem festen Zeit-Intervall einstellen.
2. Durch diese Option erhöht man die Sicherheit von OnionShare noch weiter, was allerdings die Versendung der Dateien komplizierter macht.
3. Hier stellt man die automatische Benachrichtigung für Updates ein.
4. Unter diesem Bereich lässt sich Einstellen wie OnionShare sich mit dem Tor-Netzwerk verbinden soll.
5. Dieser Bereich ist nur für Experten gedacht und für den normalen Nutzer zu vernachlässigen.

Nachdem die Einstellungen vorgenommen wurden, kehrt man durch einen Klick auf „Save“ zum ursprünglichen Fenster zurück und kann beginnen die Dateien die verschickt werden sollen festzulegen. Das sieht dann wie folgt aus:

Alle Dateien werden mit der Größe aufgelistet. Der Graue Punkt unten rechts „Ready to Share“ zeigt an, das die Dateien noch nicht erreichbar sind.

Durch einen Klick auf „ Server starten“ baut OnionShare eine temporäre Webseite auf und erzeugt eine URL Adresse.

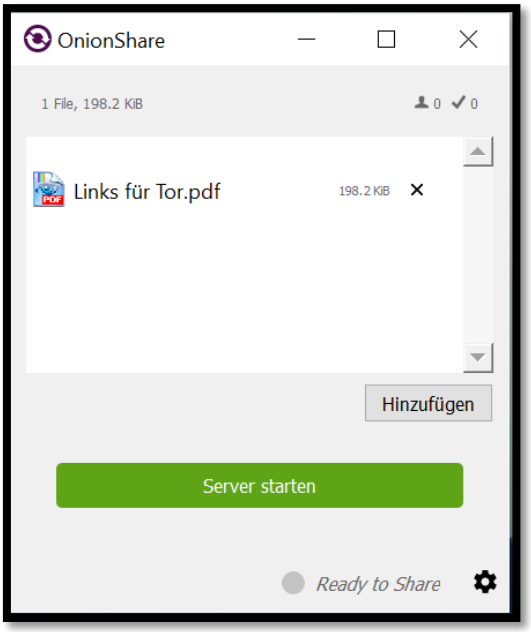


Abbildung 10 OnionShare – Ready to Share

Nach einem kurzen Moment erscheint folgende Ansicht. Hier befindet sich die URL-Adresse, die wie bereits vorab erwähnt, weitergeleitet werden muss. Durch einen Klick auf „URL kopieren“ kann die Adresse weitergeleitet werden.

Oben rechts kann man sehen wie viele Personen die Datei bereits heruntergeladen haben und wie viele noch dabei sind. Der grüne Punkt mit dem Zusatz „Sharing“ zeigt an, dass die Webseite online ist und dass die Datei gedownloadet werden kann.

Durch einen Klick auf „Server anhalten“ kann die Webseite jederzeit geschlossen werden. Dadurch erlischt die URL-Adresse und ist nicht mehr nutzbar.

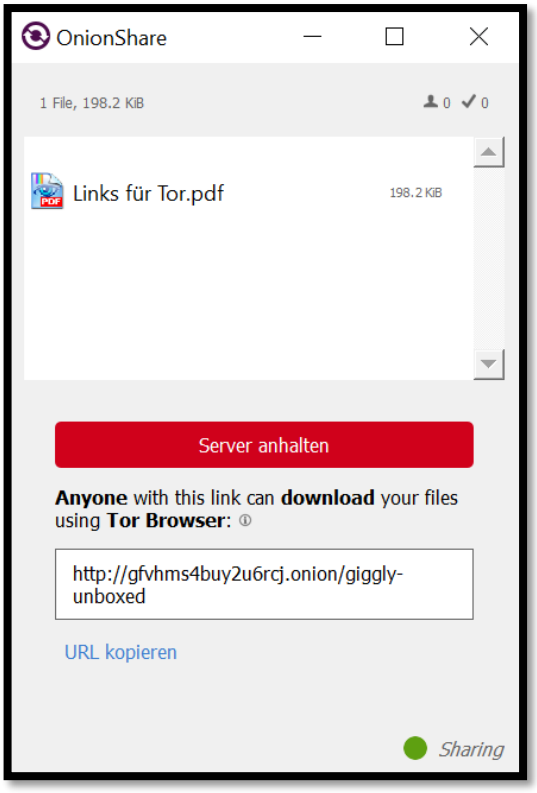


Abbildung 11 OnionShare - Sharing

Sollte man nicht der Sender sondern der Empfänger sein, so muss man als Erstes die URL-Adresse im Tor-Browser einfügen. Nur mit dem Tor-Browser lässt sich die Webseite, die OnionShare erstellt hat, erreichen. Folgende Internetseite erscheint:

Abbildung 12 Temporäre Webseite - Online

Auf dieser Webseite kann man nun die freigegebenen Dateien downloaden. Diese Seite ist so lange erreichbar bis die Bedingungen des Senders, durch z.B. Anzahl der Downloads, erfüllt sind oder der Sender den Server anhält. Sobald dies geschieht, ist die Internetseite nicht mehr erreichbar.

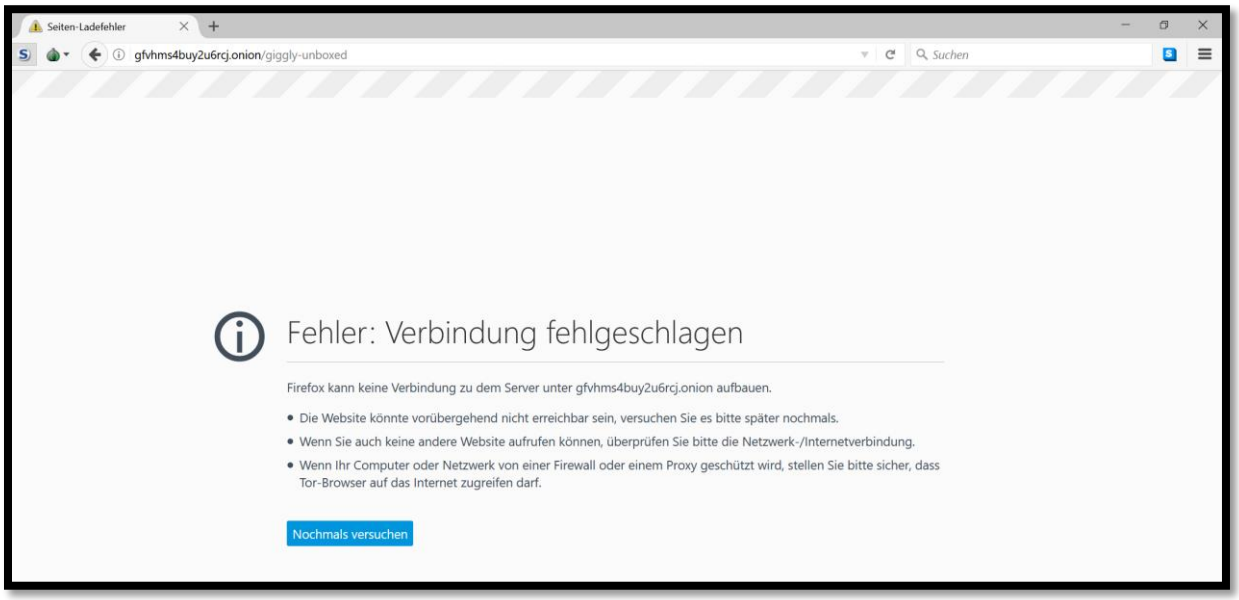


Abbildung 13 Temporäre Webseite - Offline

4. Fazit

Vor der Ausarbeitung dieses Themas durch die Seminararbeit habe ich den Browser Firefox benutzt und habe mir über das Thema Ausspionieren nicht viele Gedanken gemacht. Ich wusste zwar, dass es den Tor-Browser gibt, allerdings dachte ich, dass die Installation und die Nutzung sehr schwierig sind. Meine Ausarbeitung zeigt allerdings ganz deutlich, wie einfach es ist den Tor-Browser zu installieren und zu nutzen, da diese wie jeder andere Browser funktioniert. Gerade Nutzer von Firefox kennen die Benutzeroberfläche von Tor, da dieser ja auf Firefox aufbaut. Als größter Nachteil von Tor wird meist die langsamere Verbindung genannt, wobei ich sagen muss, dass diese zwar langsamer, aber nicht viel langsamer ist. Hier finde ich den Kompromiss zwischen etwas langsamer aber viel sicherer besser als andersherum.

Auch durch die Ausarbeitung des Programmes OnionShare wird deutlich, wie einfach es ist anonym Dateien zu verschicken. Hier stellt die URL-Adresse natürlich ein Hindernis dar und wenn man diese wirklich sicher weiterleiten möchte, muss man sich noch genauer informieren. Aber generell ist dies eine einfache und anonyme Methode, um Dateien zu verschicken. Ein weiterer Nachteil ist, dass der Empfänger den Tor-Browser benötigt. Obwohl dieser einfach zu beschaffen und zu nutzen ist, verwendet ihn dennoch nicht jeder.

Abschließend ist noch zu sagen, dass die beiden vorgestellten Programme die eigene Anonymität im Internet natürlich stark verbessern, allerdings sind diese Maßnahmen sinnlos, wenn man sich sonst im Netz verhält wie vorher. Der Tor-Browser bietet hier eine Informationsseite an, wie man sich richtig im Internet verhält um Anonym zu bleiben. Ich empfehle jedem, der sich ernsthaft anonym im Internet bewegen möchte, sich an diese Tipps zu halten.

Ich persönlich werde mich noch weiter mit diesem Thema beschäftigen und versuchen mich möglichst anonym im Internet zu bewegen. Da das Internet ein sich stetig veränderter Bereich ist und es hier häufig Neuerungen gibt, muss man stets auf dem neusten Stand sein, wenn man anonym bleiben möchte.

5. Verweise

T.Hübner, 2015. BR [Online]
Available at:
https://www.br.de/br-fernsehen/sendungen/faszination-wissen/ueberwachung-nsa-internet-100.html
[Accessed 09.06.2018]

M.Humpa, 2018. Chip [Online]
Available at:
http://www.chip.de/downloads/Tor-Browser-Paket_22479695.html
[Accessed 09.06.2018]

Anon., 2018. TorProjekt [Online]
Available at:
https://www.torproject.org/about/overview.html.en
[Accessed 09.06.2018]

J. Thoma, 2014. Golem [Online]
Available at:
https://www.golem.de/news/onionshare-filesharing-fuer-das-tor-netzwerk-1405-106650.html
[Accessed 10.06.2018]

J.E.Burkert, 2018. PC Magazin [Online]
https://www.pc-magazin.de/ratgeber/onionshare-dateien-anonym-versenden-teilen-tor-service-3199048.html
[Accessed 10.06.2018]