PrivacyMachine 0.9-beta

Benutzerhandbuch

Version **V02** vom 26.11.2016
Gibt es hier eine aktuellere Version des Benutzerhandbuchs?
https://www.privacymachine.eu/de/user-manual/

Hinweise zur Beta-Version:
Wichtige Änderungen an der Beta-Version werden hier bekannt gegeben:
https://www.privacymachine.eu/de_post/

Inhaltsverzeichnis

Allgemeines

Auch wenn viele Onlinedienste kein Geld kosten, bezahlt man dafür meistens mit seinen persönlichen Daten. Jeder deiner Clicks wird für immer gespeichert und dein Surfverhalten mit dem anderer verglichen. Diese "Profile" bilden deine Lebenssituation ab und werden weiterverkauft. Du wirst über die eindeutigen Kenndaten deines Computers/Tablets/Handys, den Fingerprint, wiedererkannt.

Diese gesammelten digitalen Spuren sind das wertvollste Gut der Datendealer.

Im Internet lauern viele Gefahren:

- Viren & Trojaner
- Diskriminierung/Mobbing
- gläserne Identität: Sie wissen wer du bist und wo du warst
- Zensur
- Vorselektion: Man glaubt zu wissen was du suchst
- weitere Schadsoftware: Cryptlocker/Ransomware

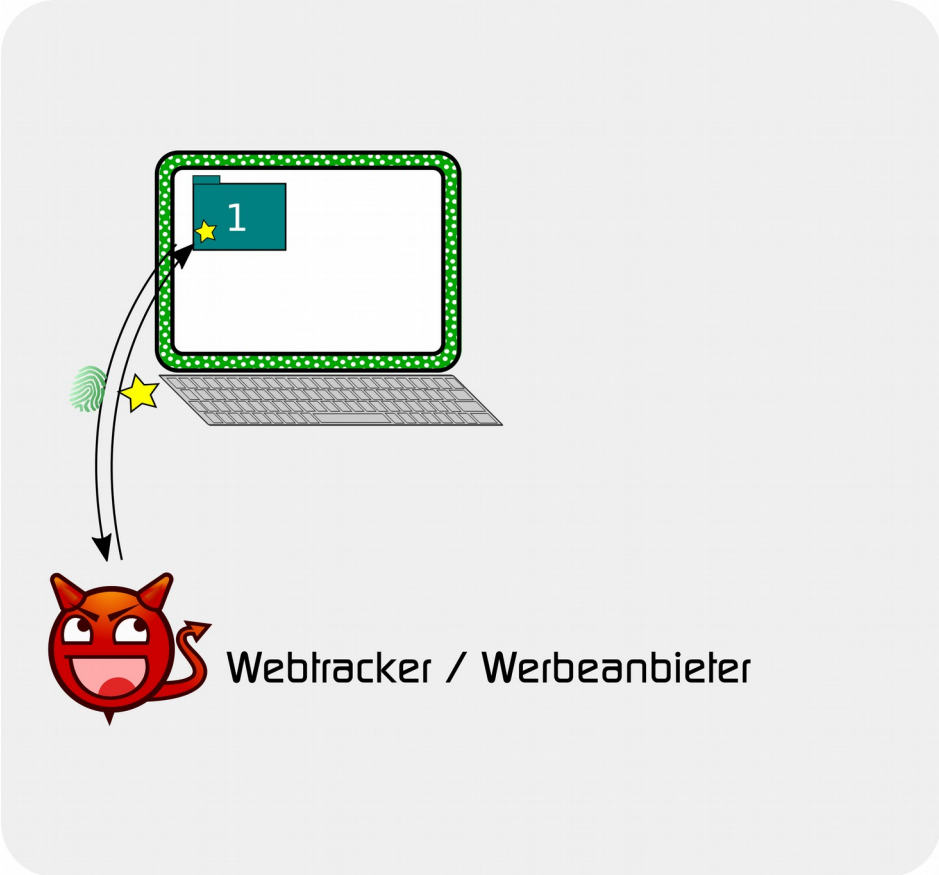
Bis jetzt funktionierte die Wiedererkennung mittels Cookies. Da man diese einfach löschen kann sind Fingerprints die neue Technologie dich immer wiederzuerkennen.

Wie schützt dich die PrivacyMachine?
Die PrivacyMachine bildet eine Schutzschicht(VM-Maske) um einen normalen Browser. Technisch funktioniert dies mittels einer virtuellen Maschine. Aus dieser Schutzschicht kann ein eventuell installierter Virus nicht ausbrechen.
Weiters schützt diese VM-Maske vor Webtracking.
Webtracking ist das permanente Wiedererkennen deines Computers auf allen Webseiten. Wenn du dich einmal auf einer Webseite einloggst wird dein Fingerprint deines Computers deiner Person zugeordnet.

Durch Verändern der Eigenschaften dieser Schutzschicht kann die PrivacyMachine den Fingerprints deines Computer verändern.

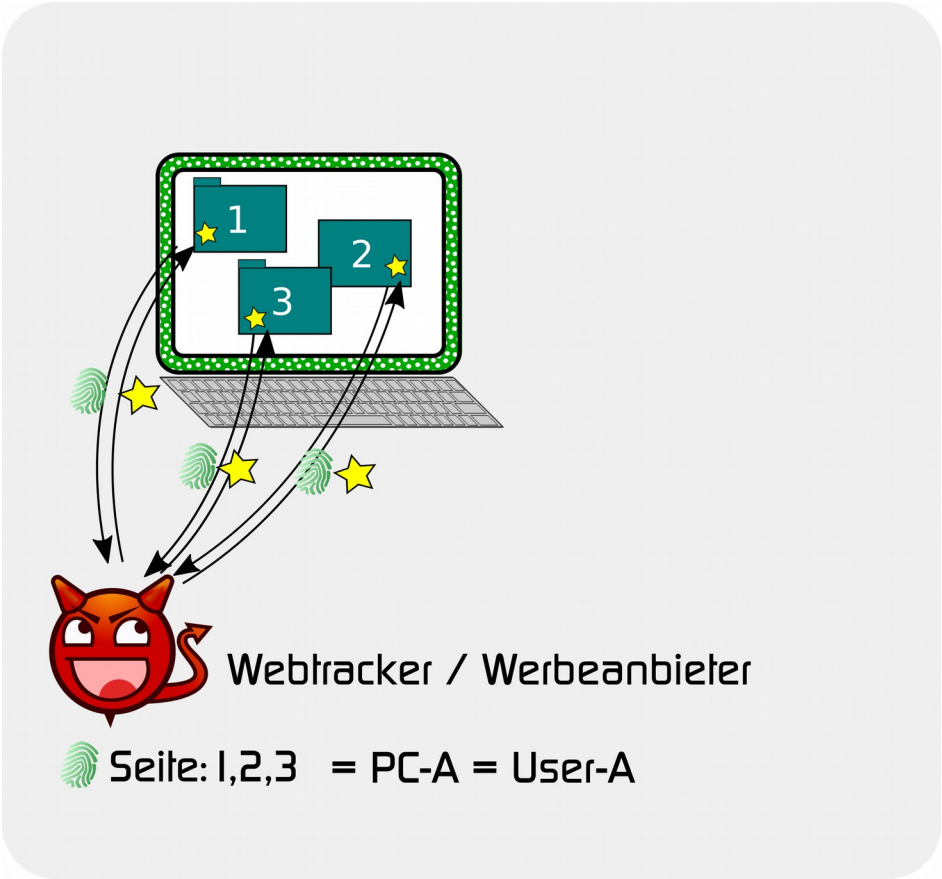
Webtracking anhand eines Beispiels erklärt

Du surfst mit deinem Computer eine bestimmte Homepage „1“ an.
Auf dieser Homepage „1“ wird Werbung eingeblendet. Diese Werbung (gelber Stern) kommt aber nicht direkt von Homepage „1“, sondern dein Browser lädt sie direkt vom Werbeanbieter herunter.



Beim Herunterladen von Werbung findet ein Datenaustausch **in beide** Richtungen statt:

- Dein Browser sendet bei der Anfrage nach Werbung deinen Fingerprint (grüner Fingerprint für grünen Computer) zum Werbeanbieter
- Der Werbeanbieter sendet dir Werbung (gelber Stern) zurück, die dir dein Browser auf Homepage „1“ angezeigt.

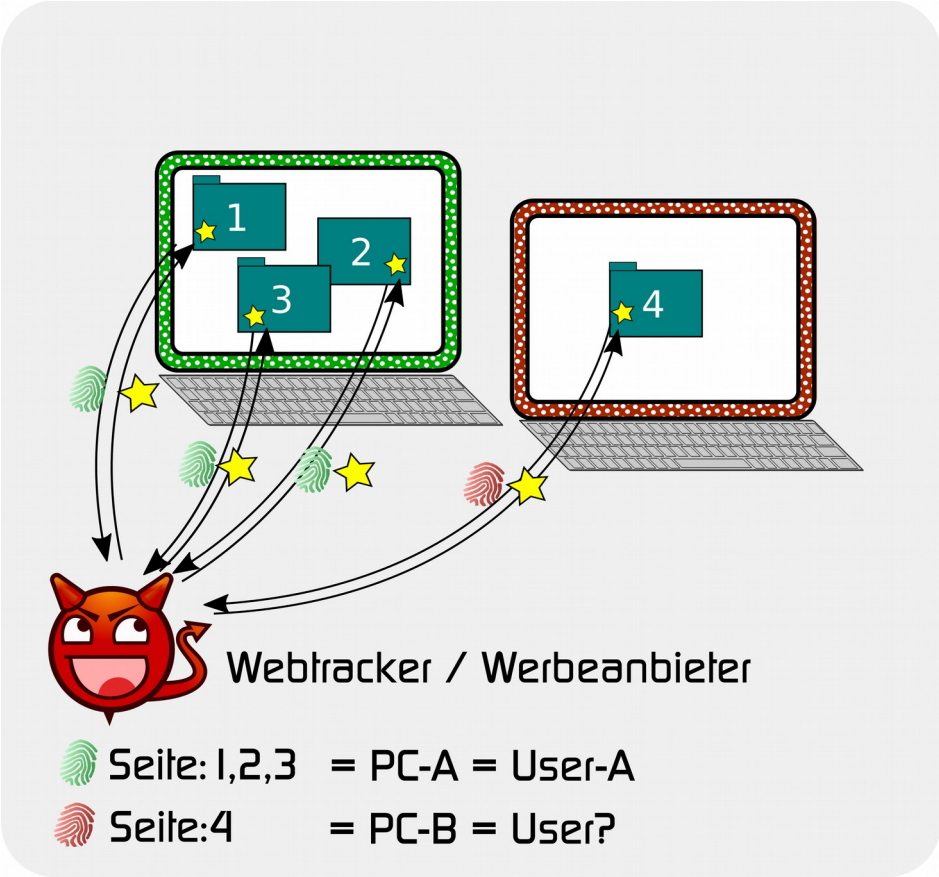


Es gibt nur sehr wenige Werbeanbieter die aber in sehr vielen Homepages eingebunden sind. Dadurch ruft dein Browser sehr oft Werbung vom selben Anbieter ab, an dem du jedes mal deinen eindeutigen Fingerprint sendest.
Wenn du dich nun in einer beliebigen Seite einloggst, kann der Werbeanbieter den Fingerprint deines Computers deiner Person zuordnen und erkennt dich auf allen Webseiten wieder.

Warum das aus deinem Surfverlauf entstehende Personen-Profil hoch brisant ist und sich gut weiterverkaufen lässt wurde bereits oben erklärt.

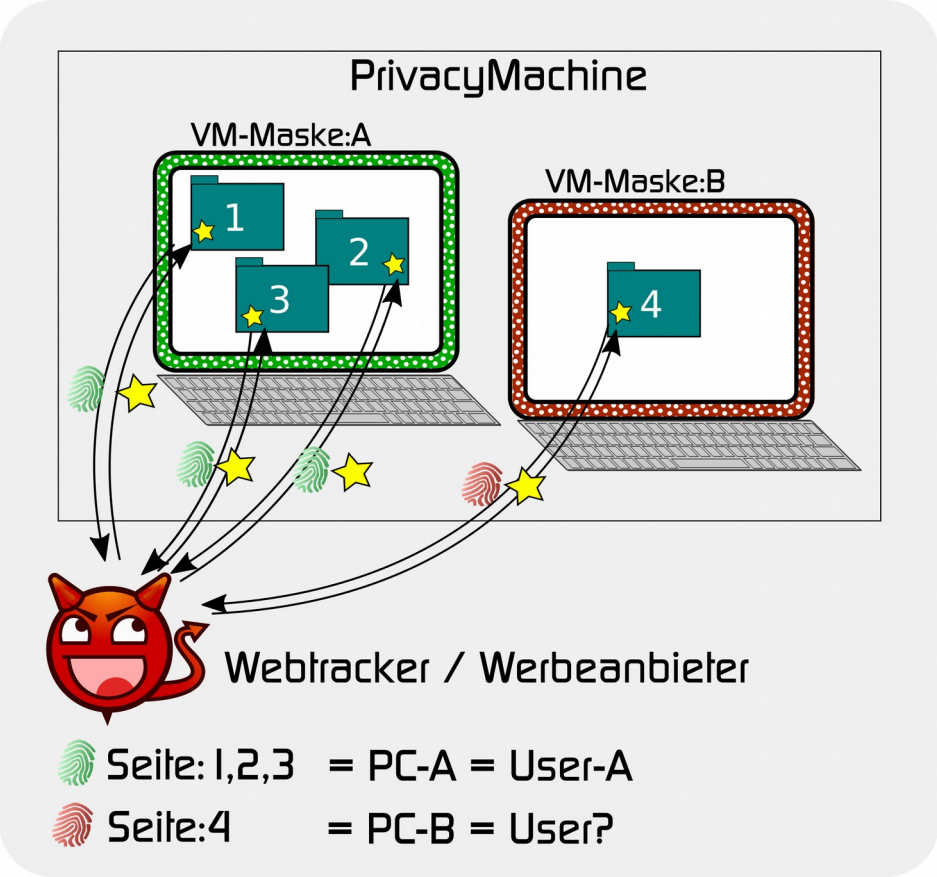
Was kann man nun dagegen machen?

Praktisch wäre es, wenn man nun einen zweiten Computer besitzt, der ja einen anderen Fingerprint hat (hier rot dargestellt). Wenn man sich mit diesem Computer niemals einloggt und nur auf Seiten zu einem bestimmten Thema surft, kann der Werbeanbieter zwar Werbung anzeigen, hat aber keine Information darüber, wem dieser Fingerprint gehört.



Nach dem Surfen solltest du diesen Computer wegwerfen und dir einen neuen Computer mit einem neuen Fingerprint besorgen.

Zu teuer? Zu unökologisch?
Dann verwende die PrivacyMachine!



Die PrivacyMachine verwendet VM-Masken, das sind simulierte Computer (Virtuelle Maschinen), die jeweils einen anderen Fingerprint erzeugen.

Wenn du diese VM-Maske schließt werden nicht nur alle Arten von Cookies gelöscht (Ein „Snapshot“ einer virtuellen Maschine wird wieder hergestellt), sondern beim erneuten Start wird ein anderer Fingerprint (im Bild: neue Farbe statt grün) erzeugt.

Wenn du zwei VM-Masken parallel nutzt, kann ein Werbeanbieter dies nicht mehr erkennen.
Sehr wohl erkennt er als zusammenhängend mehrere Browser-Tabs die du in einer VM-Maske geöffnet hast, bis du die gesamte VM-Maske wieder schließt.

Das bedeutet:

- Wenn du dich in einer VM-Maske anmeldest werden alle Seiten in dieser VM-Maske deiner Person zugeordnet → auch Browser-Tabs, welche du bereits geschlossen hast.
- Wenn du zu zwei unterschiedlichen Themen surfst, z.B. Facebook checken und Arztbefunde recherchieren: verwende zwei unterschiedliche VM-Masken. Jeder Click auf einen Link in deiner Facebook-Seite wird deiner Person zugeordnet. Abhilfe, wenn es sich um einen externen Link handelt: den Link in die Zwischenablage kopieren und in einer anderen VM-Maske öffnen.

Wie du VM-Masken bearbeiten/umbenennen/anlegen kannst ist auf der Homepage im Kapitel VPN erklärt: https://www.privacymachine.eu/de/vpn/

Software PrivacyMachine

Systemanforderungen

Leider werden zur Simulation der VM-Masken recht viel Resourcen benötigt.

Anforderungen Windows:
- 64Bit-Version von Windows 7 (Windows XP und Windows Vista gehen nicht, Windows 8, 8.1 und Windows 10 sind nicht getestet)
- RAM: 3GB

Anforderungen Linux:
- RAM: 2GB
- Es wird nur die Version unterstützt die direkt von VirtualBox gewartet wird.

Benötigte zusätzliche Software

Um die PrivacyMachine zu benutzen musst Du folgendes vorab durchführen:
- Installiere Oracle VirtualBox:
  https://www.virtualbox.org/
- Falls das Programm "Oracle VirtualBox Manager" gerade gestartet wurde beende dieses nun.
- Lade das **ExtensionPack** von VirtualBox herunter:
  https://www.virtualbox.org/wiki/Downloads
  Der Link heisst "All supported platforms"
- Installiere die heruntergeladene Datei
  „Oracle_VM_VirtualBox_Extension_Pack-[AktuelleVersion].vbox-extpack“
  per Doppelklick.

Hardware Virtualisierungssupport

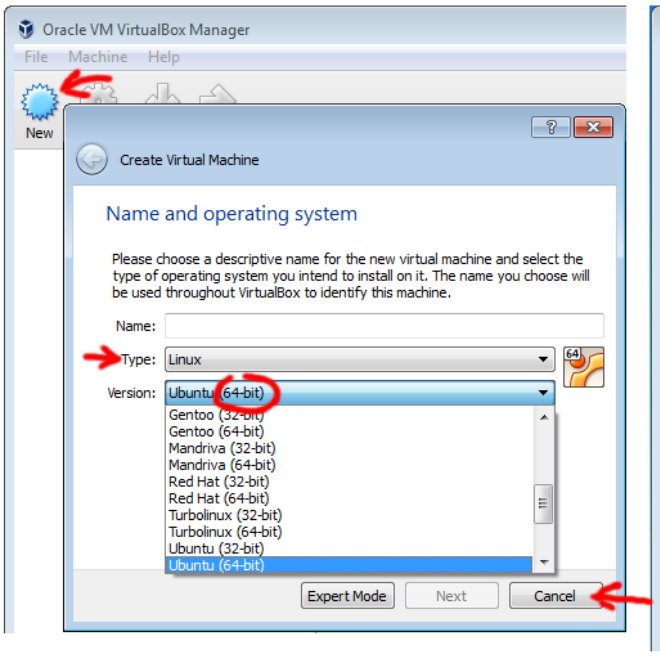
Eine BaseDisk ist eine virtuelle Festplatte von der die VM-Masken starten.

Die BaseDisks ist eine 64-Bit-Linux-Installation und benötigt „Hardware Virtualisierungssupport“ deines Prozessors. Bei den meisten Computern ist dieses Feature bereits eingeschaltet, wenn nicht, musst du selbst ins BIOS wechseln und diesen aktivieren.

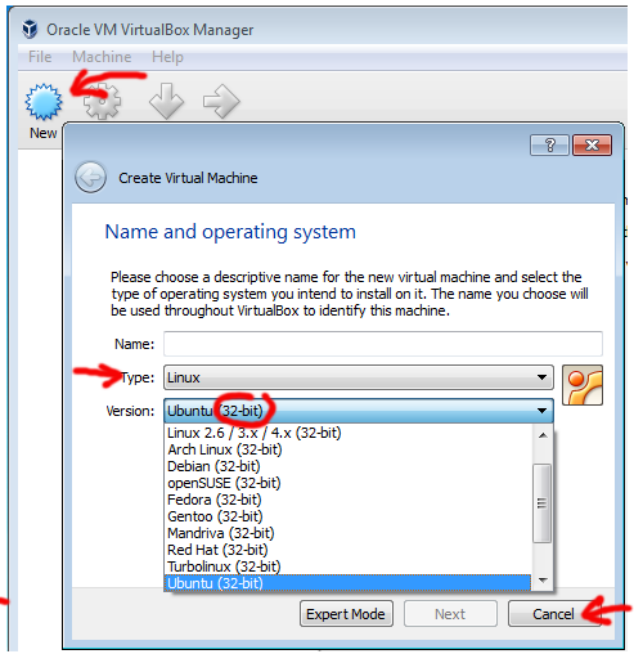
So überprüfts Du ob „Hardware Virtualisierung Support“ bereits eingeschalten ist

- Starte „Oracle VirtualBox“
- Klicke auf den blauen Stern, um eine neue Virtuelle Machine anzulegen
- Wähle als Typ „Linux“ aus.
- Wenn du nun in der Versionsliste 32-bit und 64-bit Betriebssystem auswählen kannst ist alles ok.
- Wenn in der Versionsliste nur 32-bit Betriebssysteme erscheinen musst du „Hardware Virtualisierungssupport“ einschalten um die PrivacyMachine starten zu können.

OK: With Hardware (VT-x/AMD-V)-Support:



Not OK: Without (VT-x/AMD-V)-Support:



- Den Dialog kannst du nun mit „Cancel“ wieder beenden.

Wie aktiviert man die „Hardware Virtualisierung“?

- Du musst den Computer neu starten und per Tastendruck während des Bootvorgangs in das BIOS wechseln. Meist ist das einer der Tasten <DEL>, <F2> oder <F4>
- Die Funktion heisst leider in jedem BIOS etwas anders, gängige Namen sind „Virtualisation Support“, VT-x oder AMD-V.

Hier findest du weiter Informationen:
Erklärung auf howtogeek.com

Installation der PrivacyMachine

Bei der Installation wirst Du nach dem Zielverzeichnis der PrivacyMachine gefragt.
Unabhängig davon wird in deinem Benutzerverzeichnis (meist auf C:\ ) 5GB freier Platz für die BaseDisk benötigt.

Beim ersten Start der PrivacyMachine erscheint eine Warnung der Windows-Firewall die bestätigt werden muss:

Hintergrundinfo: Für jede virtuelle Maschine einer VM-Maske wird ein Prozess von VirtualBox namens „VboxHeadless.exe“ gestartet. Da die VM-Masken Netzwerkzugriff benötigen muss diese Meldung einmalig bestätigt werden.

Hier kannst du dir die installierbare Version herunterladen:
https://www.privacymachine.eu/de/download/

Nach der Installation findest du die PrivacyMachine in deinem Startmenü.

Updates

Wieso sind Updates wichtig?

Ganz allgemein gilt, dass Software aufgrund der Komplexität leider nie frei von Fehlern sein wird.

Wenn der Hersteller einer Software einen sicherheitskritischen Fehler in seiner Software findet behebt er diesen üblicherweise und bietet den Nutzern ein Update an. Durch die Analyse der Änderungen nach der Installation dieses Updates können Experten relativ einfach herausfinden, was das Problem war und schlimmer: wie man es ausnutzen kann. Kriminelle Naturen können nun direkt z.B. einen Erpressungstrojaner installieren oder sie verkaufen diese Informationen (Exploit) für ca. 100.000$ am Schwarzmarkt.

Jeder Nutzer der Software kann sich nun relativ einfach vor diesem Angriff schützen, indem er das Update installiert.

Ein bildlicher Vergleich: Jedes Sicherheitsupdate das man nicht installiert hat ist wie ein Wohnungsschlüssel, den man auf der Straße verliert: hoffentlich war keine Adresse dabei und hoffentlich findet es niemand mit bösen Absichten.

Wie bekommst Du diese Updates?

Die PrivacyMachine enthält einen Update-Mechanismus, welcher die PrivacyMachine selbst und die BaseDisk updated. Die BaseDisk ist eine virtuelle Festplatte auf der das Betriebssystem Debian-Linux installiert ist und das Software wie z.B. Firefox enthält.

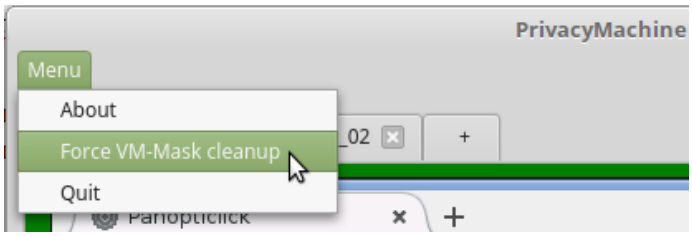
Wenn nun Mozilla eine neue Version des Firefox mit Sicherheitsupdates freigibt, erstellt das PM-Team eine neue BaseDisk und verteilt diese über den Updatemechanismus an alle User.

Dazu wird bei jedem Start der PrivacyMachine der Update-Server des PrivacyMachine-Teams kontaktiert, ob es neue Updates gibt.

Die Adresse dieses Updateservers ist konfigurierbar, d.h. Experten, Universitäten oder größere Firmen können selbst einen Updateserver betreiben.

Achtung: Bei der derzeitigen Beta-Version der PrivacyMachine sind hierfür folgende einfache manuellen Schritte notwendig, um eine neue BaseDisk zu erhalten:

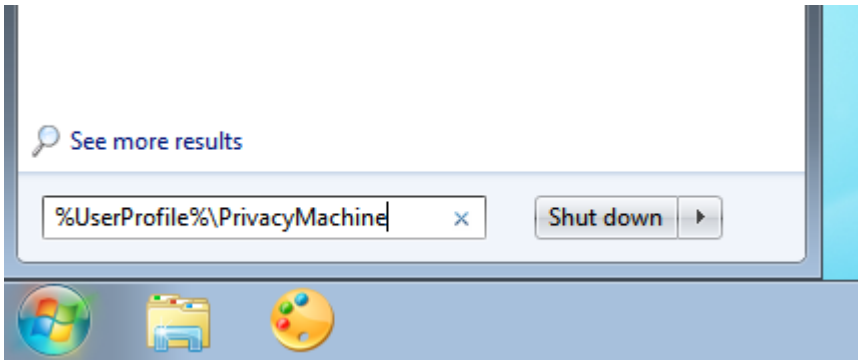
1. Starte die PrivacyMachine und wähle den Menüpunkt: „Menu→Force VM-Mask cleanup“



   Dabei werden die virtuellen Maschinen entfernt, welche die BaseDisk verwenden.

   Die PrivacyMachine schließt sich nach der Durchführung selbst.

2. Navigiere mit dem Explorer in das Konfigurationsverzeichnis der PrivacyMachine: diesen Ordner öffnet man, indem man unter Windows links unken auf das Startmenü klickt, im Suchmenü **%UserProfile%\PrivacyMachine** eingibt und die "Eingabetaste/Enter" drückt.



   Linux-User finden diesen Ordner unter „**~/.config/privacymachine**“

3. Nun muss manuell der Ordner „base-disk“ gelöscht werden.
4. Beim erneuten Start der PrivacyMachine wird automatisch die aktuelle BaseDisk heruntergeladen und alle notwendigen Initialisierungsschritte zur Erstellung der VM-Masken die auf der neuen BaseDisk basieren durchgeführt.

Beta-Version: Ob deine BaseDisk aktuell ist erkennst du am Datum der BaseDisk unter https://update.privacymachine.eu/

Allgemein geben wir wichtige neue Versionen auch über unseren Blog https://www.privacymachine.eu/de_post/ bekannt.

Ein Problem? Benötigst Du Hilfe?

1.) Überprüfe die Logfiles

In den Logdateien findet sich manchmal ein detaillierter Hinweis auf dein Problem.

Die PrivacyMachine schreibt während des Betriebs Log-Dateien in den Ordner „PrivacyMachine\logs“ welcher in deinem Benutzerverzeichnis „%UserProfile%“ liegt.
Wenn dein Windows-Loginname z.B. Franz ist, liegt dieser Ordner unter:
C:\Users\Franz\PrivacyMachine\logs\

Die Datei PrivacyMachineLog.log ist die Datei die während des letzen Starts angelegt wurde.
Die Datei PrivacyMachineLog.log.1 ist die Datei vom Start davor, usw.

Diese Dateien kannst Du z.B. mit der Software Notepad++ öffnen.

2.) Gibt es vielleicht eine Lösung für dein Problem in der FAQ auf der Homepage?

https://www.privacymachine.eu/de/faq-software/

3.) Verwende den ProblemReporter und kontaktiere das PM-Team

Der ProblemReporter wird mit der PrivacyMachine mit installiert und dient dazu, ein Zip-File mit allen relevanten Informationen (Logfiles) zu erstellen.
Dieses Zipfile kannst Du zusammen mit einer ausführlichen Problembeschreibung an beta-support@privacymachine.eu senden.

Bevor du den ProbelemReporter startest schließe bitte die PrivacyMachine.

Du musst einen Speicherort für das Zip-File und eine Fehlerbeschreibung eingeben, um das Erstellen des Zip-Files starten zu können.

Die Zip-Datei bietet dir eine einfache Möglichkeit zu überprüfen, welche Informationen du an den Support versendest.

Allgemeine Hinweise

Hinweise zu Tor

Tor ist ein Anonymisierungnetzwerk und verschleiert die IP-Adresse. Der Internetverkehr deines Browsers wird über mehrere Tor-Server geleitet, anonymisiert und dann erst ins normale Internet weitergeleitet.

Das bringt ein hohes Maß an Anonymität und Zensurresistenz, falls dein Rechner hinter einer Firewall steht die bestimmte Domains nicht zulässt.

Nachteil: Jeder kann einen sogenannten Tor-Exit-Knoten betreiben, um Informationen aus dem Tor-Netzwerk in das normale Internet weiterzuleiten. Dabei kann man den Inhalt nicht nur mitlesen sondern auch verändern.

D.h. ein Download eines PDF‘s von z.B.: http://bekannte-sichere-seite.at kann auf dem Weg von der Homepage zu deinem Computer mit einem Virus verseucht werden.

Dies kann nicht passieren wenn Du über https://bekannte-sichere-seite.at surfst.

Wir empfehlen bei der Verwendung von Tor:

- dich nirgends einzuloggen
- keine Dateien downloaden (PDF, Exe, MP3, Videos...)

Hinweise zu VPNGate

Hier stellen Privatpersonen ihren Computer als VPN-Server zur Verfügung.

Vorteil: Viele IP-Adressen, d.h. gut für die Verschleierung des Fingerprints

Nachteil:

- siehe Sicherheit von Tor
- wenn die Benutzer ihren Computer abschalten geht auch die VPN-Verbindung zu (in diesem Falle kann man noch die Adressen der angesurften Seiten per Copy&Paste herauskopieren und die VM-Maske erneut starten)

Wann kann/sollte man die eigene IP verwenden?

Wenn man sich z.B. bei der Bank oder beim Finanzamt einloggt besteht kein Anonymisierungsbedarf.

Danksagung

Wir möchten uns an dieser Stelle nochmals herzlich für die Förderung von netidee.at bedanken, ohne die die Fertigstellung der PrivacyMachine nicht möglich gewesen wäre!