

GUIDE: ANONYMITY AND PRIVACY FOR ADVANCED LINUX USERS

Created by: **beac0n** brought to you by DeepDotWeb.com

INTRO

The goal is to bring together enough information in one document for a beginner to get started. Visiting countless sites, and combing the internet for information can make it obvious your desire to obtain anonymity, and lead to errors, due to conflicting information. Every effort has been made to make this document accurate. This guide is image heavy so it may take some time to load via Tor.

SOME GENERAL SOURCES/BIG THANKS

For more general guides checkout:

[EFF Surveillance Self-Defense project](#)

[Riseup.net Security Guide](#)

[Security in a box](#)

[TAILS Documentation](#) – for those looking for a solid starting place TAILS OS is a great choice.

Thanks!

[securityinabox.org](#)

[Deepdotweb.com](#)

[EFF](#) and [EPIC](#)

[riseup.net](#)

For educational purposes.

Not legal advice or call to action.

Table of Contents

- [1 Intro](#)

- 2 Some general sources/Big Thanks
- 3 Technical Information
 - 3.1 Strong Passwords
 - 3.2 Internet Connectivity
 - 3.2.1 Firewall
 - 3.2.2 Changing MAC Address
 - 3.2.3 Intrusion Detection
 - 3.2.4 Disk Encryption
 - 3.2.5 Browsers
 - 3.2.6 Router Configuration
 - 3.2.7 Anonymity Networking
 - 3.2.8 VPN
 - 3.2.9 Proxy Chains
 - 3.3 Operating Systems
 - 3.3.1 Flash Firmware
 - 3.3.2 Enabling a BIOS boot password
 - 3.3.3 USB Bootable Operating Systems:
 - 3.3.4 Linux (image files can be found at <http://distrowatch.org>)
 - 3.4 Secure Data-Wiping Linux
 - 3.5 Physical Destruction
 - 3.6 Cold-Boot Attack
 - 3.7 Basic Communications
 - 3.7.1 Images
 - 3.7.2 Email Providers

- 3.7.3 Jabber_XMPP/OTR
- 3.7.4 Alternative Messaging Options
- 3.8 GNUPG/PGP Basics
 - 3.8.1 TAILS PGP
 - 3.8.2 Additional reading on PGP
 - 3.8.3 PGP Versions
- 3.9 Validating Files with MD5 or SHA1:
 - 3.9.1 SHA1 Sum
 - 3.9.2 MD5 Sum

TECHNICAL INFORMATION

STRONG PASSWORDS

It's difficult to remember many passwords. First off it's good to select a strong password manager. [Keepassx](#) is cross-platform, and has good security features, like encryption by password and using a keyfile. It also allows you to generate strong passwords, so if you're not worried about memorization it's good practice to let Keepassx generate secure random passwords.

It's best not to use services that store your passwords in the cloud. If you need you can back up your encrypted password database, on a secure server, in an encrypted directory, and store your keyfile in a separate location.

Passwords for encryption and critical access should be prioritized. Even a long randomized password may not be a secure enough method. EFF recommends you try the diceware method, or basically randomly chain a number of words selected from a word list based on dice roles. Full details are [available here](#).

Although it's an annoyance, passwords are the ever present key to what

matters most to you.

INTERNET CONNECTIVITY

No service provider should be presumed to completely protect your privacy. Even if your VPN/Proxy or other ISP promises no logs, or identifiable information, time and time again information has been collected and used against those seeking anonymity. Open-Source technologies where you are able to examine source, yet trust is still ultimately placed in the hands of developers, are better than trusting a Government or other entity with your security.

Consider reading the Terms of Service any time you sign up for a service or install something.

Also remember that the times you use technology can be used to build a profile of your location for identification. Consider changing up your times of connectivity. On forums, chat and other services, it may be worthwhile to disable the notification that outwardly displays when you are on line or select invisible mode when applicable.

FIREWALL

UFW (Uncomplicated Firewall) is a great general firewall for linux

1. `sudo apt-get install ufw`
2. `sudo ufw enable`
3. `sudo ufw default deny incoming`

as some malware may utilize outgoing traffic, like encrypted udp, it may be worthwhile to limit outgoing ports

1. `sudo ufw default deny outgoing`

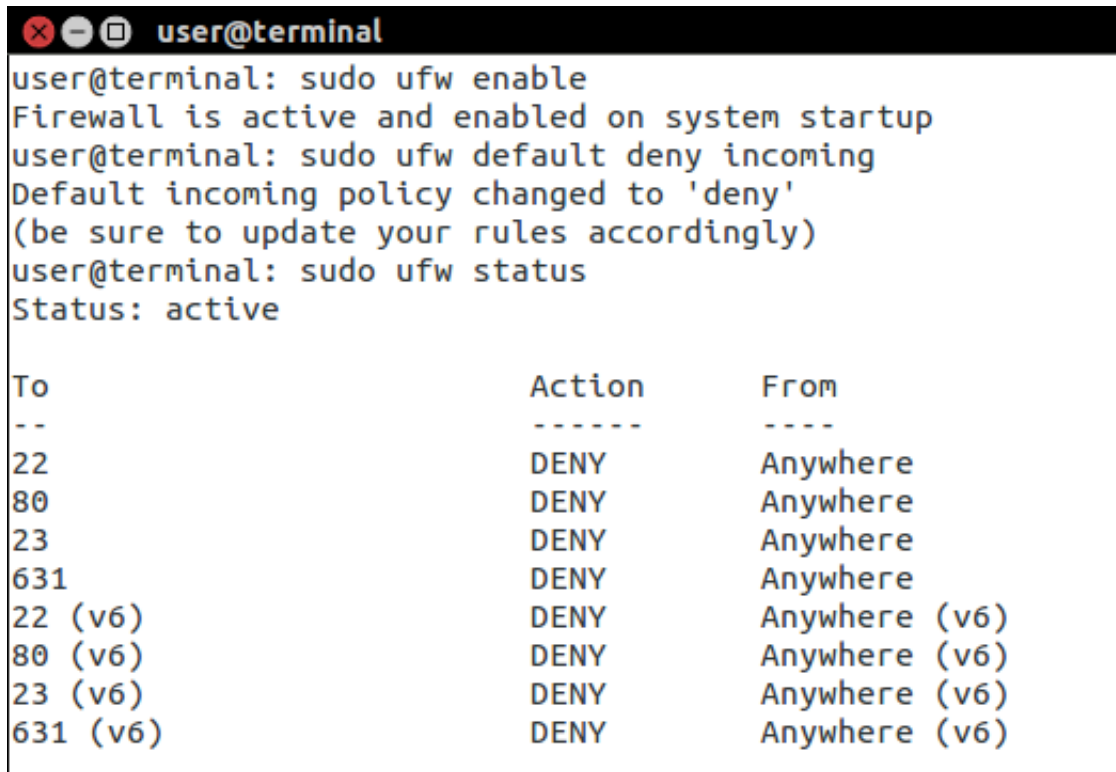
it may be better to specifically allow/deny the specific ports of concern.

1. `sudo ufw allow port/tcp`

2. `sudo ufw allow port/udp`

Then when you're done check the status

```
1 sudo ufw status
```



A terminal window titled 'user@terminal' showing the output of several ufw commands. The first command is 'sudo ufw enable', which returns 'Firewall is active and enabled on system startup'. The second command is 'sudo ufw default deny incoming', which returns 'Default incoming policy changed to 'deny' (be sure to update your rules accordingly)'. The third command is 'sudo ufw status', which returns 'Status: active' followed by a table of rules.

To	Action	From
--	-----	----
22	DENY	Anywhere
80	DENY	Anywhere
23	DENY	Anywhere
631	DENY	Anywhere
22 (v6)	DENY	Anywhere (v6)
80 (v6)	DENY	Anywhere (v6)
23 (v6)	DENY	Anywhere (v6)
631 (v6)	DENY	Anywhere (v6)

you can see I've blocked some specific ports in this example

For more advanced configuration [visit](#).

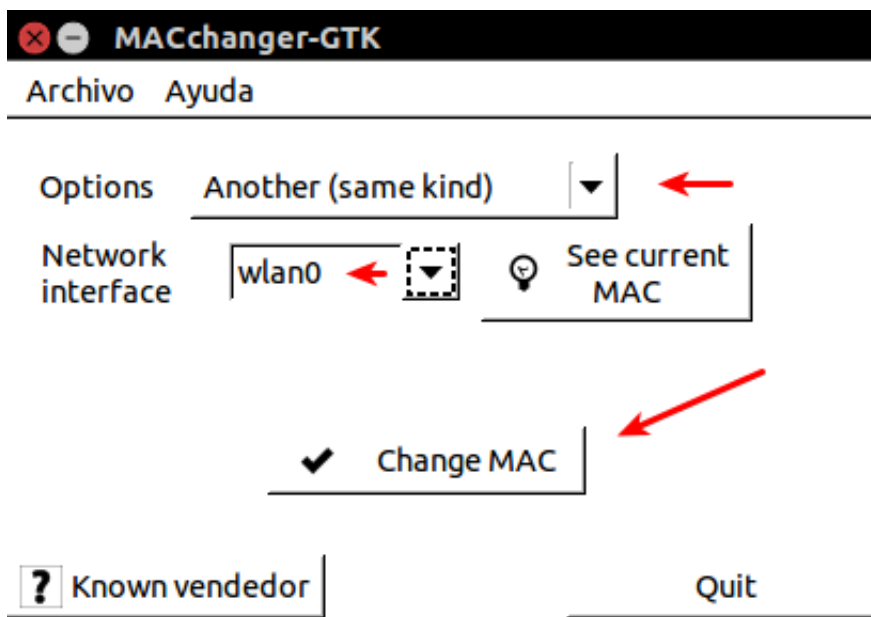
CHANGING MAC ADDRESS

A MAC Address is a hardware specific identifier for you network interface. In some cases it may be useful to change your mac address to avoid detection.

[Arch Linux Guide](#):

```
1 sudo apt-get install macchanger
2 for a gui
3 sudo apt-get install macchange-gtk
```

With macchanger-gtk



heck your current mac addresses for future reference

```
1 macchanger eth0
2 macchanger wlan0
```

for a random macaddress

```
1 sudo ifconfig wlan0 down
```

```
1 sudo macchanger -r wlan0
```

This will change the mac address to a random value

```
1 macchanger -e wlan0
```

will change the mac address but keep it as the same vendor. This can be useful if you're spoofing your address but you don't want it obviously coming from a device not on the network.

```
1 sudo macchanger -A wlan0
```

This will change the devices MAC to a random MAC of any kind, regardless of the original device.

```
1 sudo macchanger -mac=XX:XX:XX:XX:XX:XX interface
```

Will change to a specific mac address of your choice

You may want to write a script to start automatically on network manager start, and network manager shut down.

```
1 sudo nano /etc/init/macchanger.conf
```

```
1 description      "change mac addresses"
2
3 start on starting network-manager
4
5 pre-start script
6     /usr/bin/macchanger -A wlan0
7     /usr/bin/macchanger -A eth0
8     /usr/bin/macchanger -A wmaster0
9     /usr/bin/macchanger -A pan0
10    #/usr/bin/logger wlan0 `/usr/bin/macchanger -s wlan0`
11    #/usr/bin/logger eth0  `/usr/bin/macchanger -s eth0`
12 end script
13
```

you can switch out -A for -r or whatever other configuration you might want.

```
1 sudo nano /etc/network/if-post-down.d/random-mac
```

```
1 #!/bin/sh
2
3 MACCHANGER=/usr/bin/macchanger
4
5 [ "$IFACE" != "lo" ] || exit 0
6
7 # Bring down interface (for wireless cards that are up to scan for network)
8 /sbin/ifconfig "$IFACE" down
9 macchanger -A "$IFACE"
10
```

1. sudo chmod +x /etc/network/if-post-down.d/random-mac
2. sudo service network-manager restart

INTRUSION DETECTION

The basic premise is monitoring the system for unusual activity. First is to keep an eye on the logs, and the next step is to consider an IDS like snort. There's a learning curve, but here are some useful tools, that with some research can increase security especially if you allow others to access the system.

1. logwatch
 1. help.ubuntu.com
1. snort
 1. snort.org
 2. <http://manual.snort.org/>
1. Open Source SECurity
 1. www.ossec.net
 2. http://www.ossec.net/?page_id=160

You may want to get yourself acquainted with some of the common security tools available. Here's a good list, definitely nmap, tcpdump, netcat and wireshark [are useful](#).

DISK ENCRYPTION

On first install of a linux operating system you should be prompted to create an encrypted LVM partition, and encrypt your home folder. This is a good start. For further security there is veracrypt.

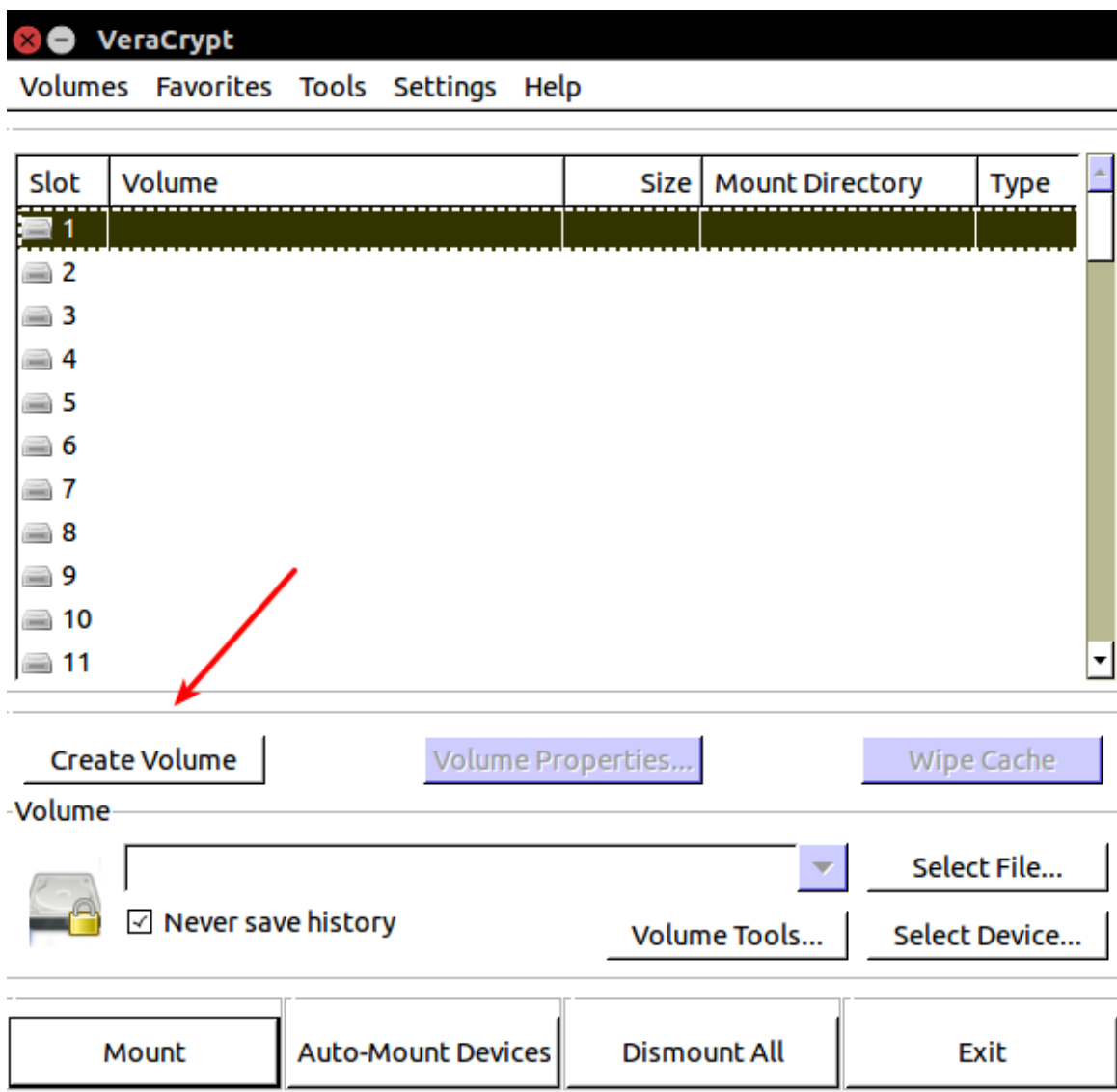
Veracrypt is a fork of Truecrypt that is better at patching vulnerabilities. I see a lot of tutorials touting Truecrypt, and it's in most package managers. However, you should download Veracrypt.

Download: veracrypt.codeplex.com/releases/view/56...

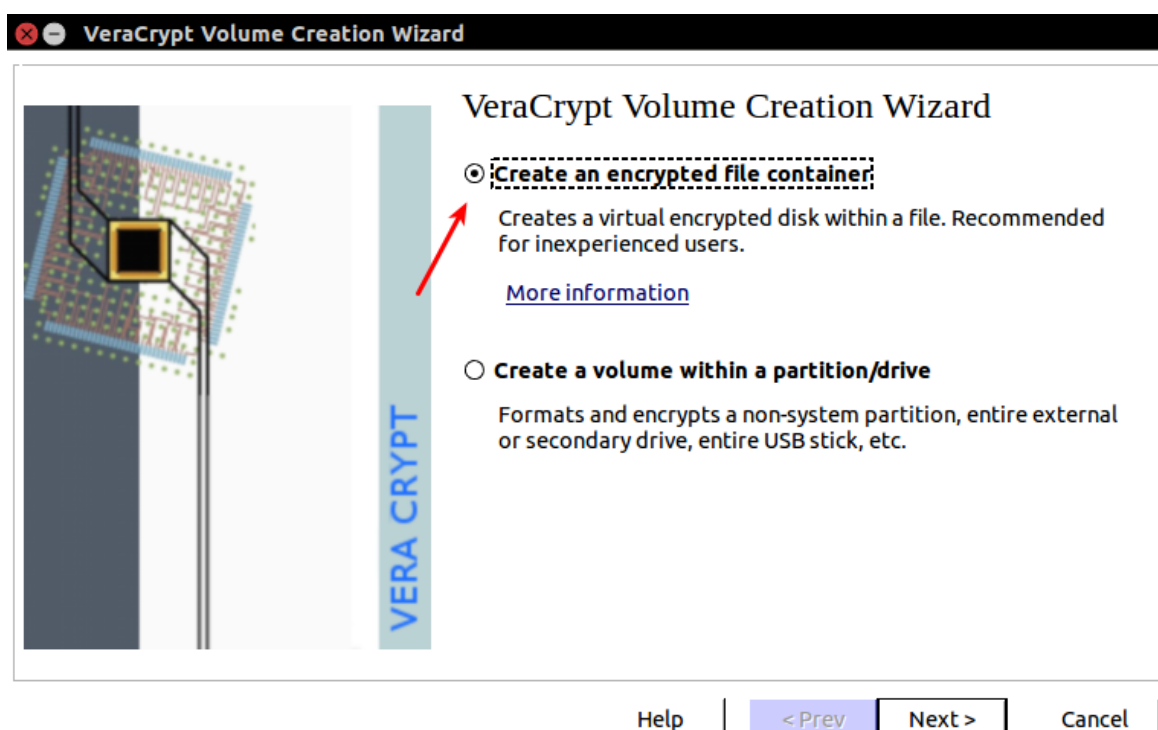
[Here's a good beginners tutorial for Veracrypt](#)

How to create a hidden encrypted volume with Veracrypt

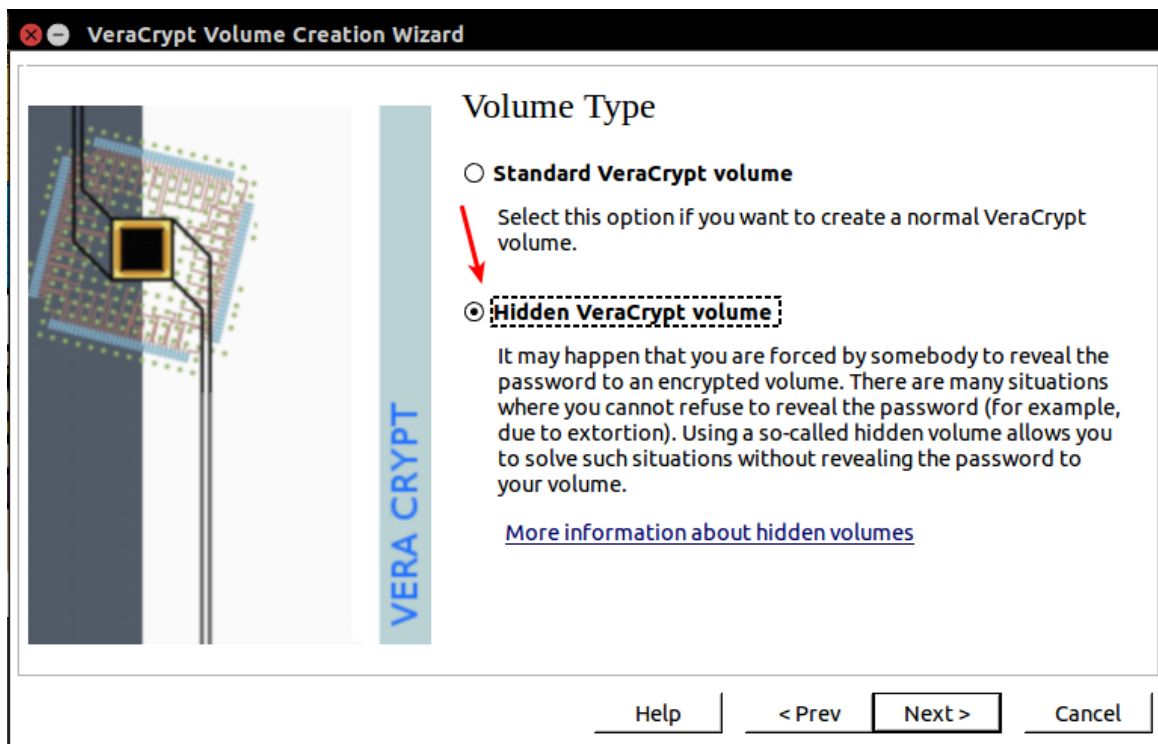
Select Create Volume



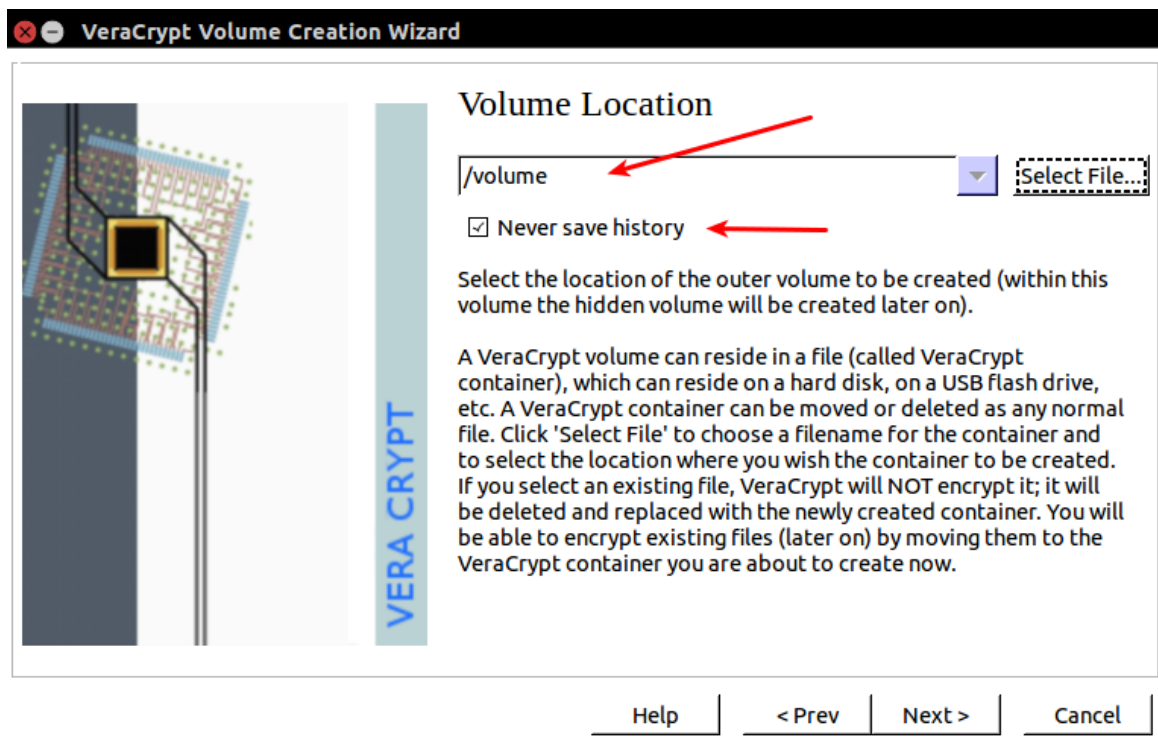
Select Create an Encrypted File Container



Select Hidden Veracrypt volume

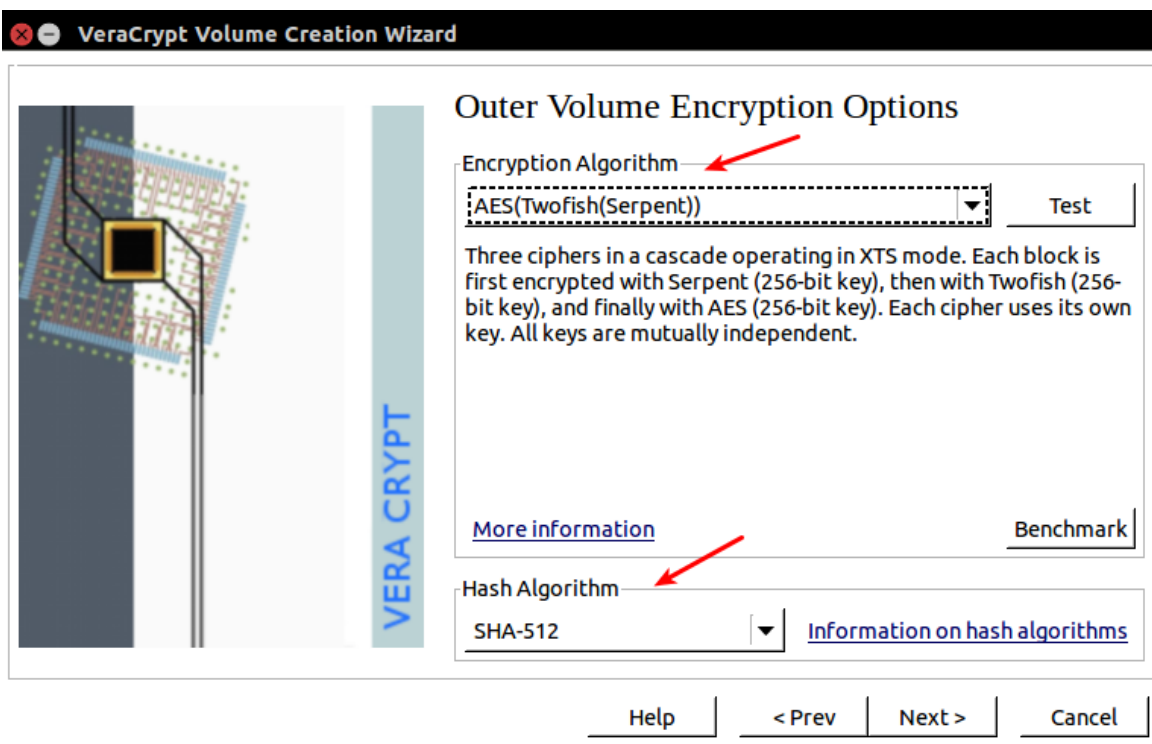


Choose volume location and select never save history:

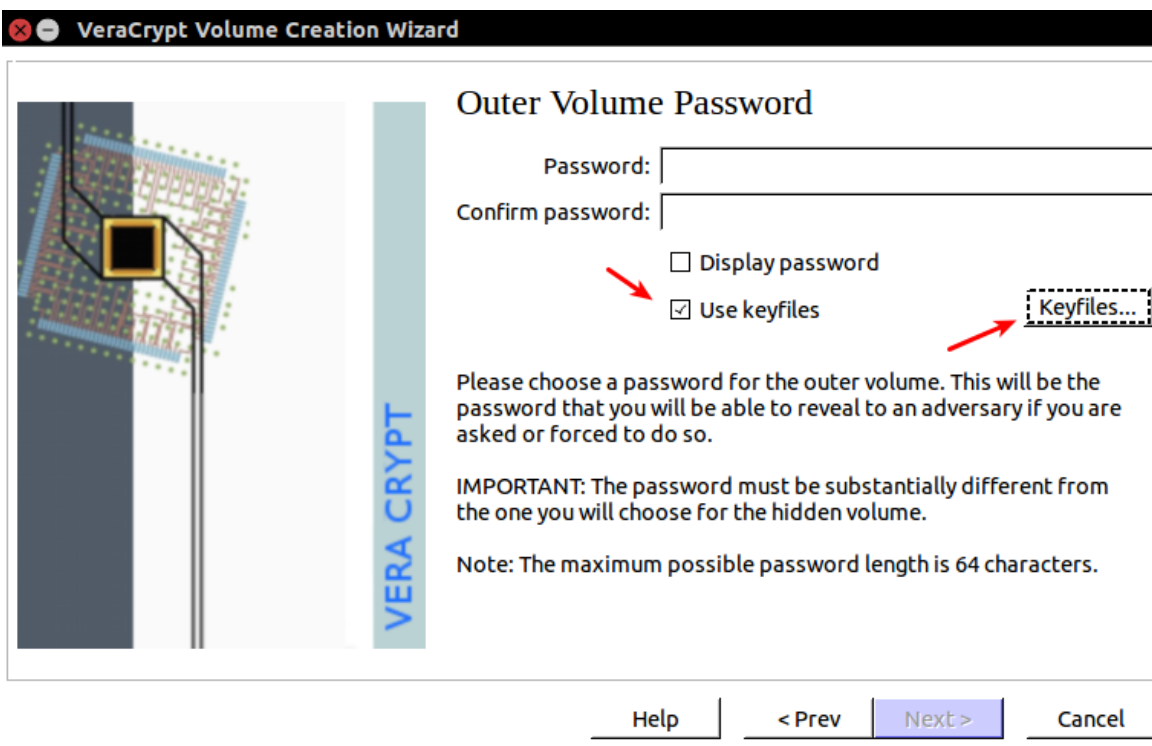


Select your encryption algorithm, AES is fine, but you may chose more secure

Select Hash Algorithm, SHA-512 is sufficient



Select Use Key files and click the key files box... **optional**:



Generate save the new key.

Mixing PRF: SHA-512 ▼


Random Pool: BCF5FB86C5AC393D47BCCDFE71F4CBDA6496A4B62414E087.. ☒ Show

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the keyfile.

Number of keyfiles: 1 ▲▼

Keyfiles size (in Bytes): 64 ▲▼ ☐ Random size (64 <-> 1048576)

Keyfiles base name: key

 [Generate and Save Keyfile...](#) [Close](#)

Click add files and add the key


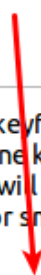
Click Generate Random Keyfile box if you want another key

You may also use existing keys:

Select Keyfiles

Keyfile
'key'

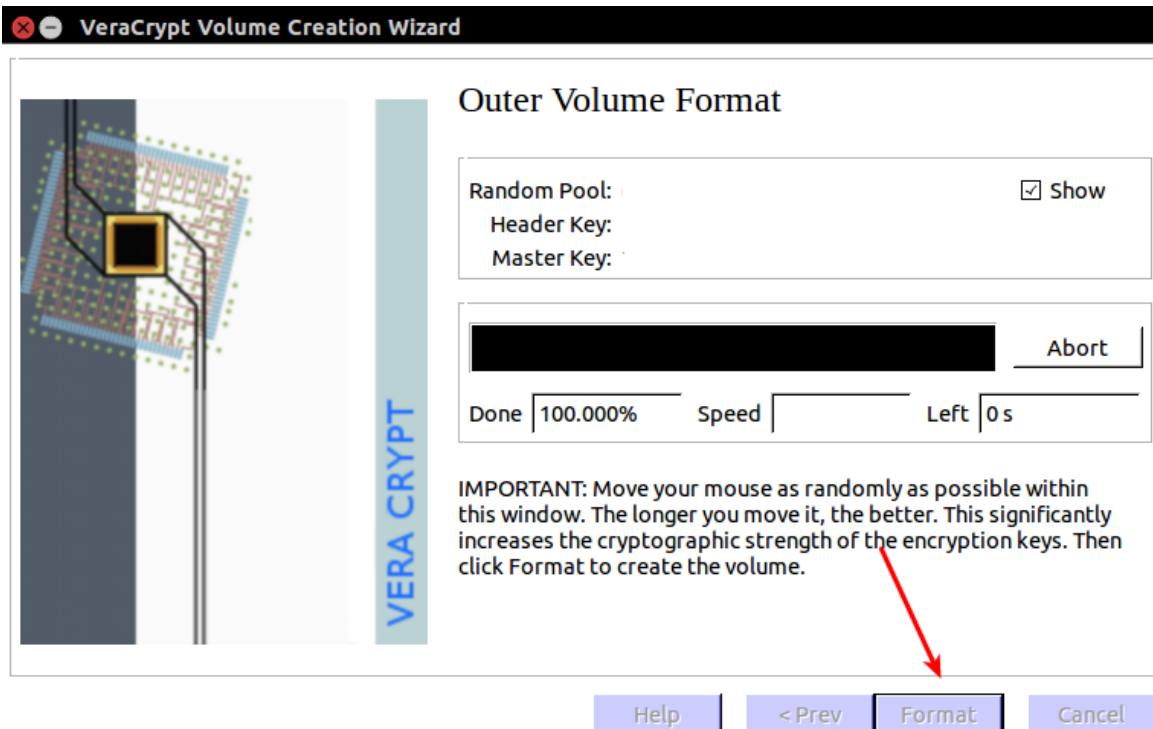
[Add Files...](#) [Add Path...](#) [Add Token Files...](#) [Remove](#) [Remove All](#)

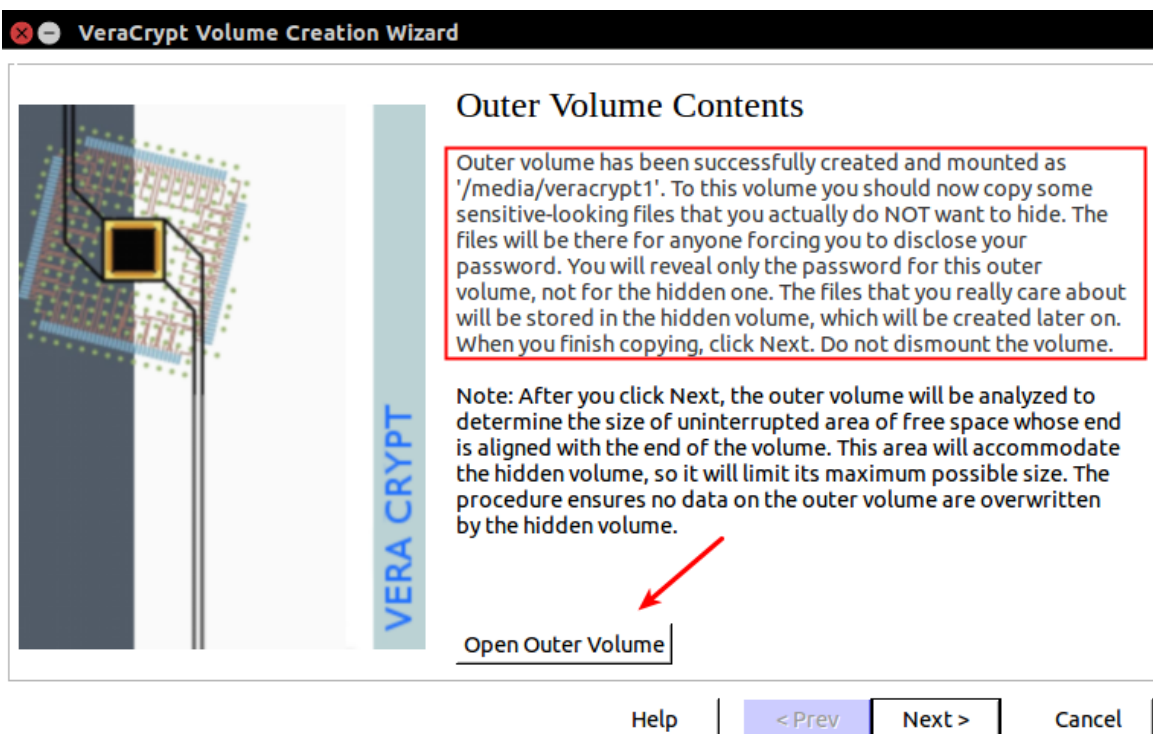
Any kind of file (for example, .mp3, .jpg, .zip, .avi) may be used as a VeraCrypt keyfile. Note that VeraCrypt never modifies the keyfile contents. You can select more than one keyfile (the order does not matter). If you add a folder, all non-hidden files found in it will be used as keyfiles. Click 'Add Token Files' to select keyfiles stored on security tokens or smart cards (or to import keyfiles to security tokens or smart cards).

[More information on keyfiles](#) [Generate Random Keyfile...](#)

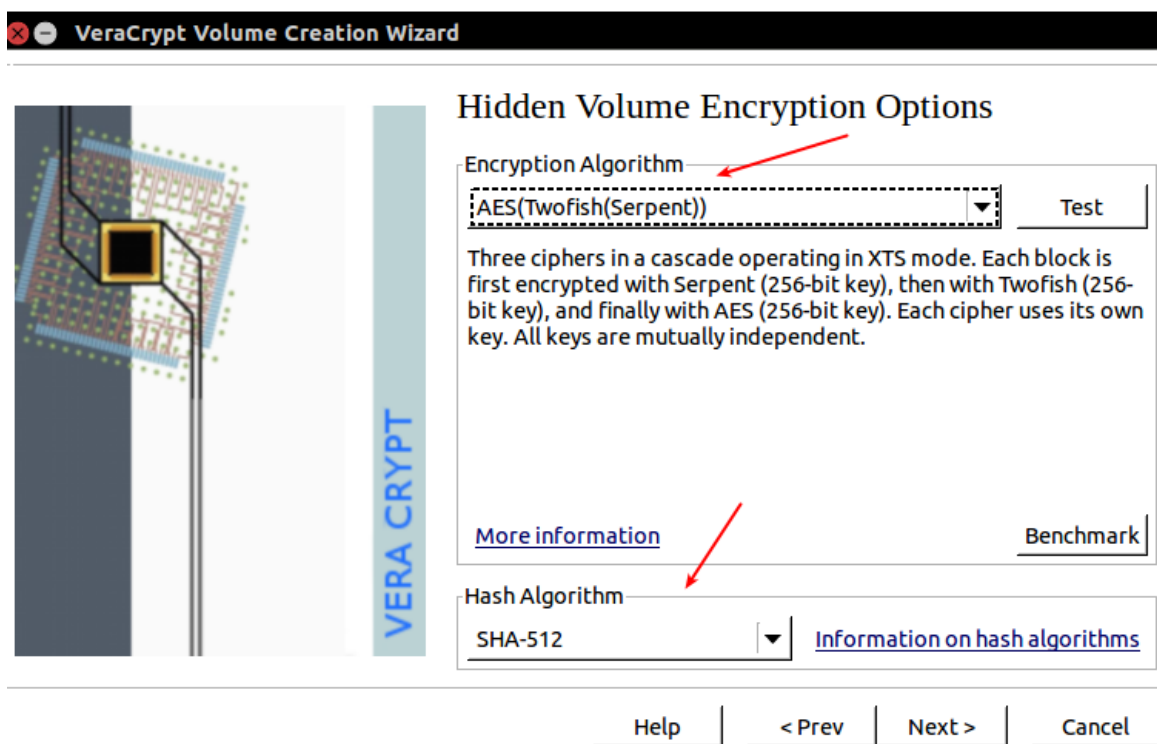
Click format to create the volume that will be visible:



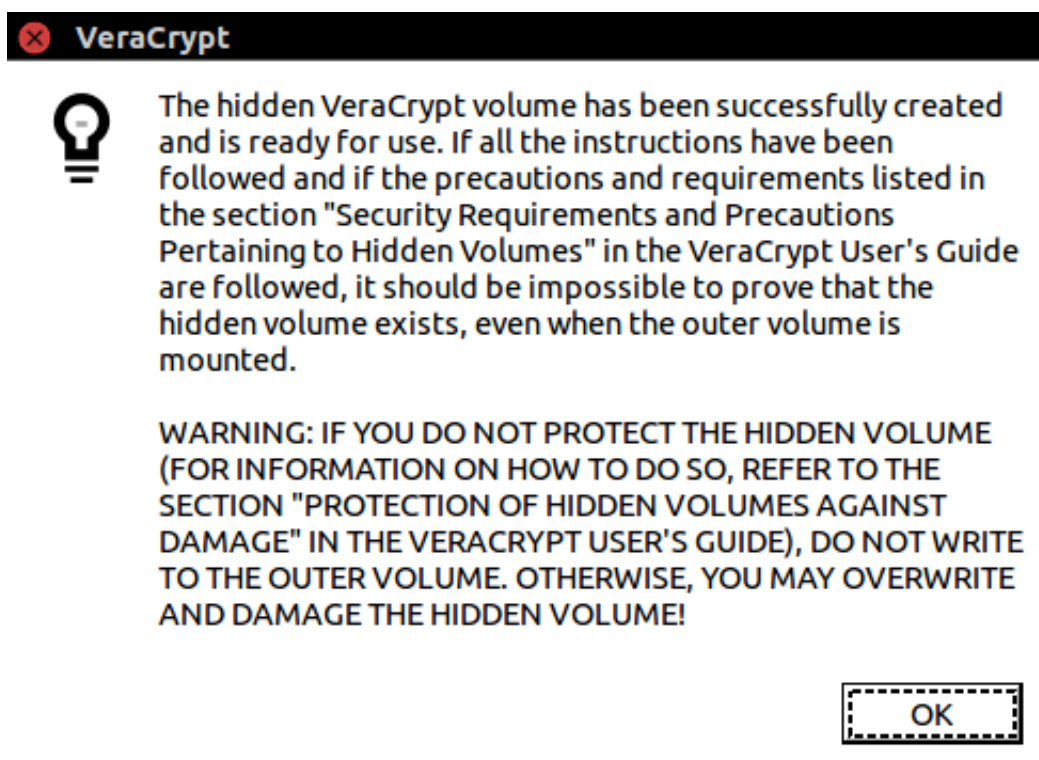
Now it's recommended to load this volume with contents that appear sensitive



You will follow the same steps, remember this is the hidden volume consider it's security most important.



When complete you will see this warning, read it carefully.



BROWSERS

TOR BROWSER

Download at: torproject.org

All Tor network addresses will be followed with .onion, not .com. It is far

more secure browsing .onion services.

In depth explanation of Tor [by its head developer Arma](#).

Once you've download tor browser, expand the zipped file. Then

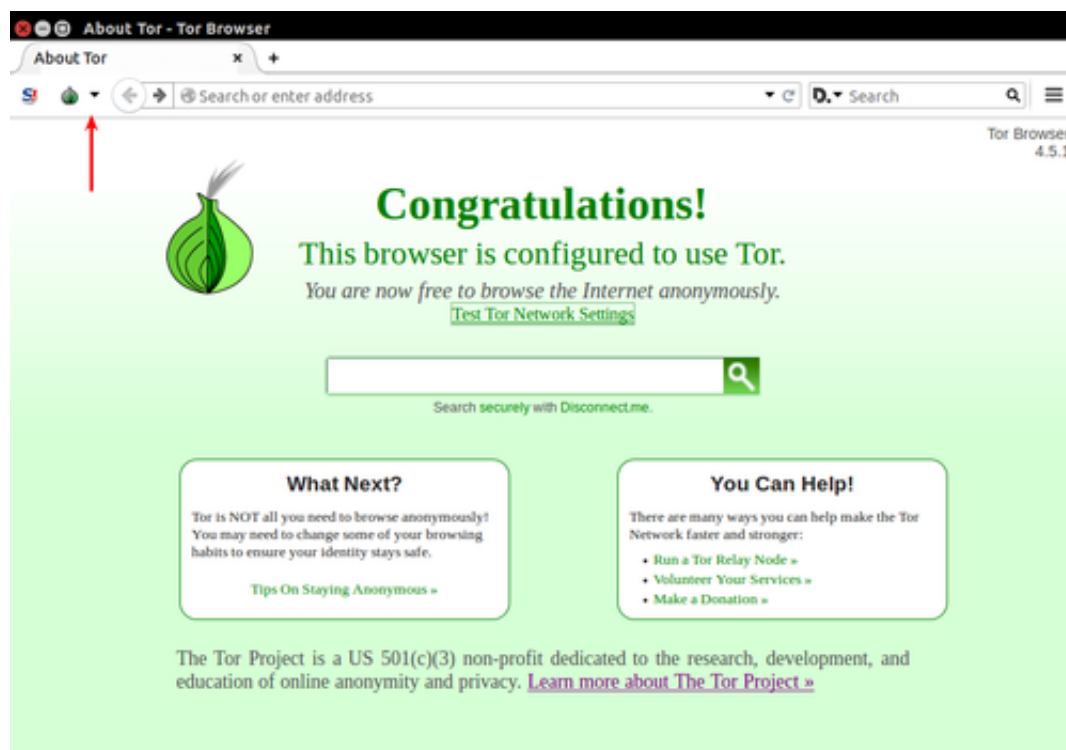
```
1 cd tordirectory
2 ./start-tor-browser.desktop
```

```
user@terminal
user@terminal: cd ~/Downloads/tor-browser_en-US/
user@terminal: ./start-tor-browser.desktop
Launching './Browser/start-tor-browser --detach'...
user@terminal: _
```

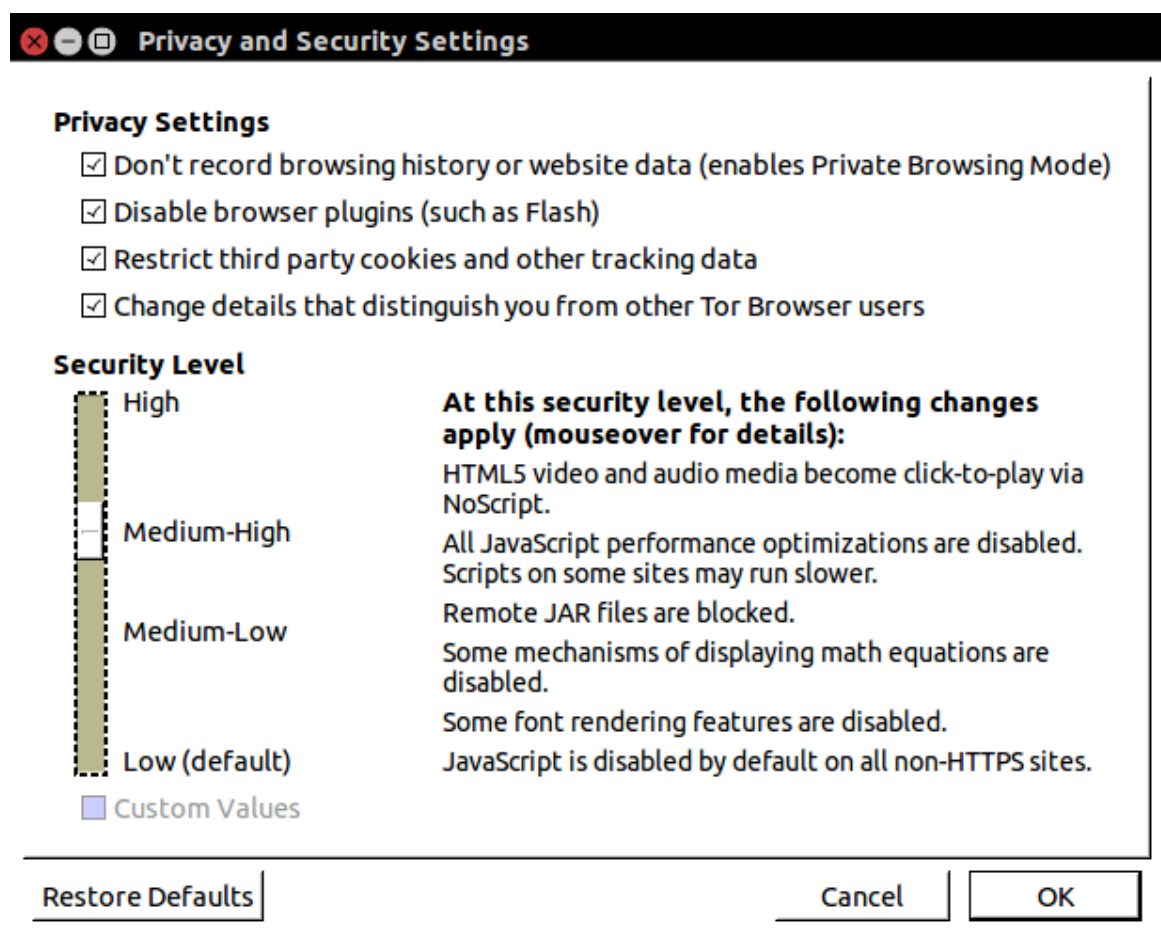
Forbidding javascript and other elements can make web browsing less convenient, but by allowing more elements you open yourself to potential vulnerabilities. It's best to find the best possible security setting you can withstand while the web browsing experience is still functional.

Configuring Security Settings

Privacy and security settings can be easily configured. Click on the Onion in the top left.

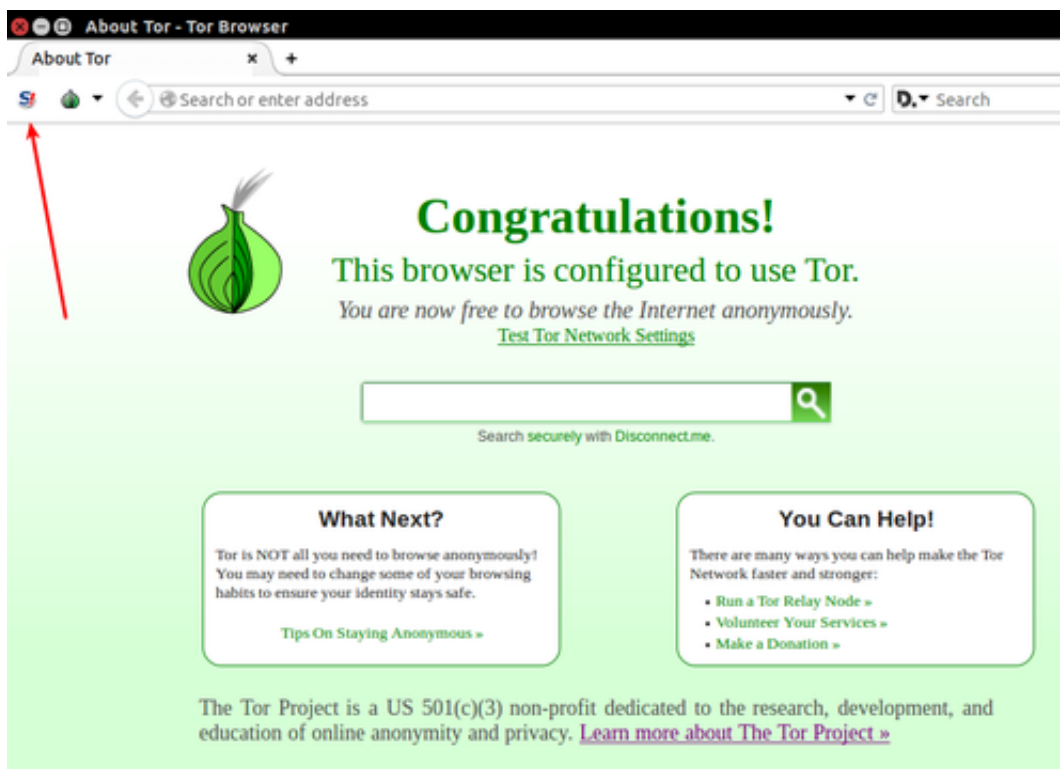


Select "Privacy and Security Settings" Adjust the slider to your desired level of security.



Noscript basics

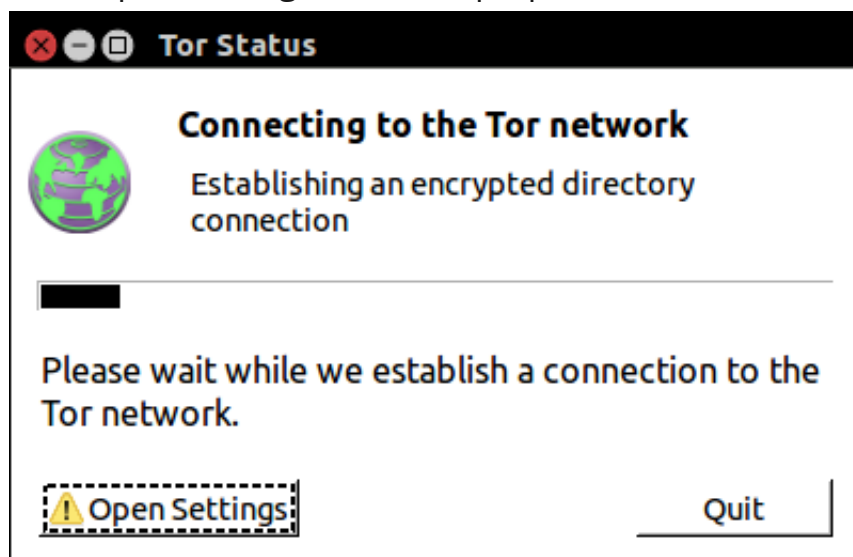
Depending on your security level selected in Tor, Noscript may not provide any advantage. That main advantage of Noscript is it's easier to tailor allowing on specific sites, or for specific elements on the fly. Click the S in the Top Left next to the Tor Onion symbol and select forbid scripts globally. You should see a red line across the S. If you allow specific sites, you should check that the red line is there for those you do not allow. Allowing only specific sites may create a fingerprint of your activity. There are some advanced settings under options worth taking a look at.



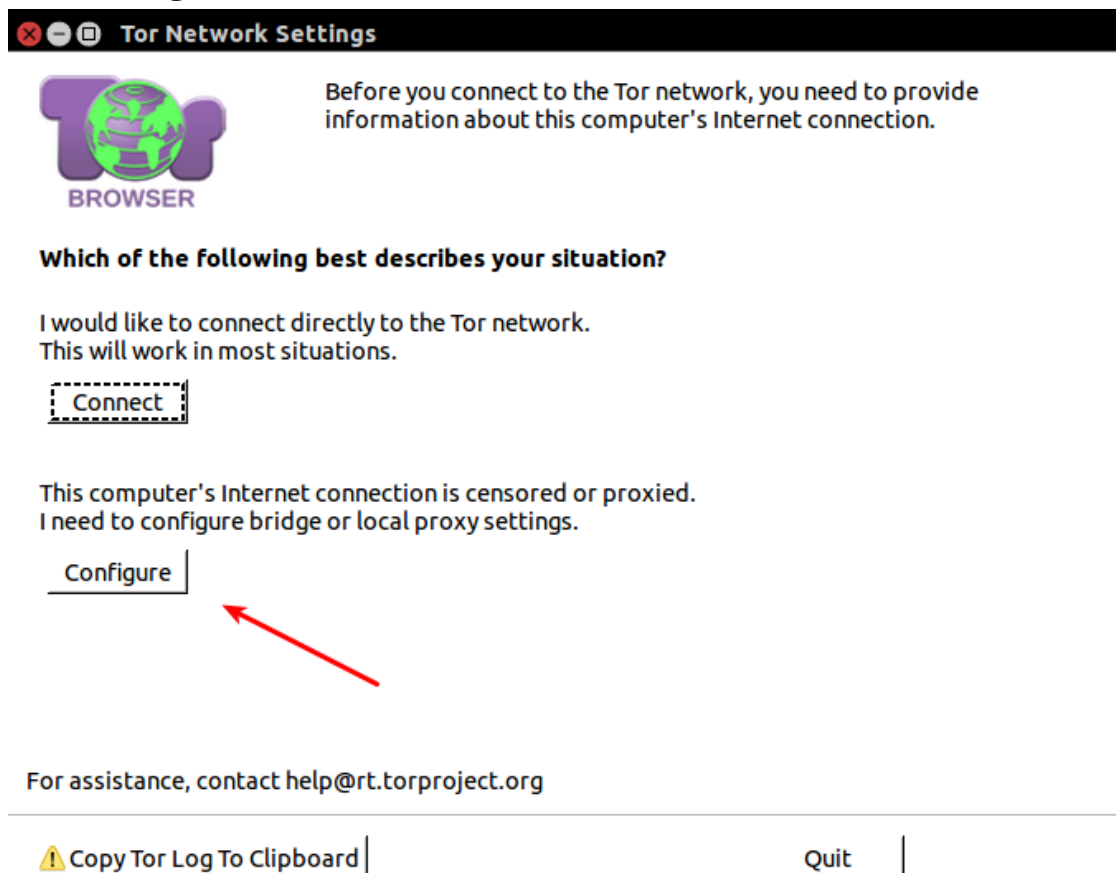
TOR BRIDGE

in some cases if Tor is blocked or you wish to conceal the use of Tor a bridge can be configured. This makes it more difficult for an ISP to detect Tor. Bridges can help avoid censorship, and if your ISP Blocks Tor Traffic it is much more difficult to detect the nature of the traffic unless deep packet inspection is employed. It's one of those things that since it's there, might as well set it up as a per-cautionary measure and see if your connection is still, reliable and fast enough for your standards.

- Click Open Settings on the Pop-up Connection Box



- Click configure



Tor Network Settings

TOR BROWSER

Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?


I would like to connect directly to the Tor network.
This will work in most situations.

Connect

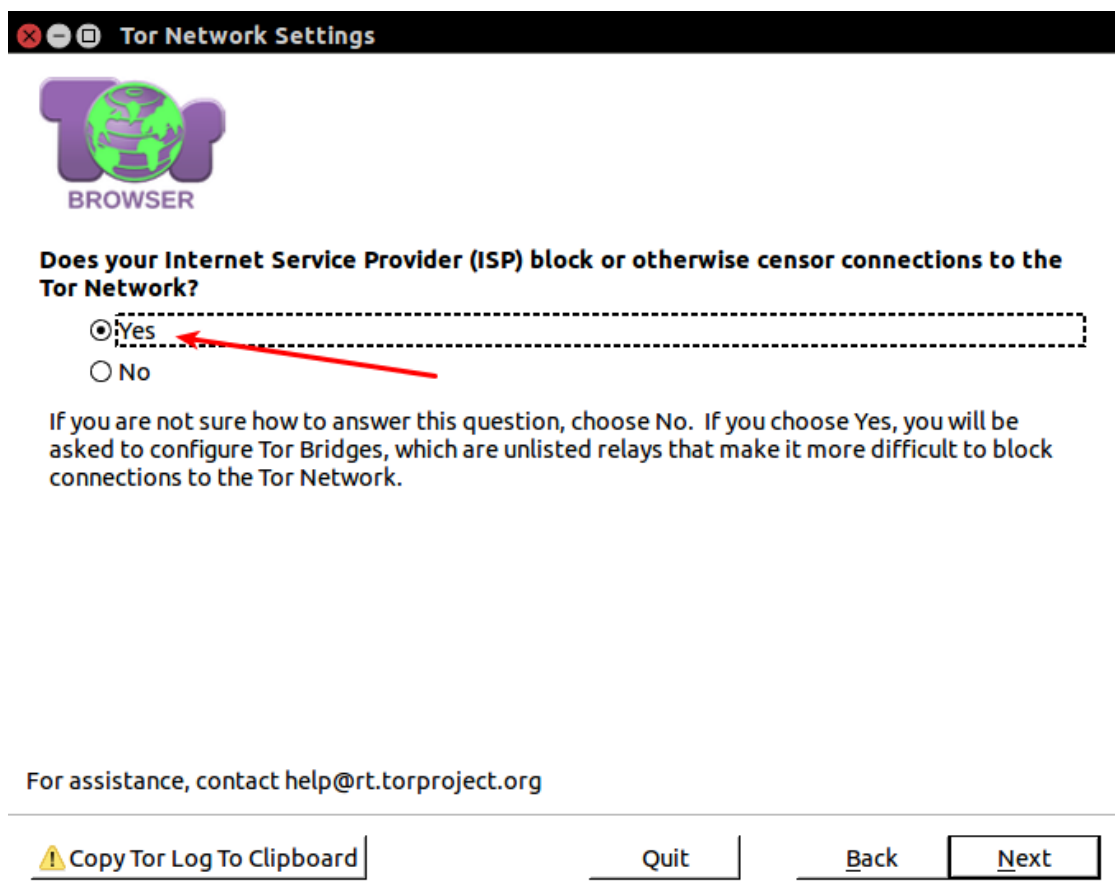
This computer's Internet connection is censored or proxied.
I need to configure bridge or local proxy settings.

Configure

For assistance, contact help@rt.torproject.org

 Copy Tor Log To Clipboard Quit

- Select Yes to ISP Censors or Blocks



Tor Network Settings


TOR BROWSER

Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor Network?

☒ Yes ☐ No


If you are not sure how to answer this question, choose No. If you choose Yes, you will be asked to configure Tor Bridges, which are unlisted relays that make it more difficult to block connections to the Tor Network.

For assistance, contact help@rt.torproject.org

 Copy Tor Log To Clipboard Quit Back Next

- obfs3 is fine, see below for information on other options.

Tor Network Settings



You may use the provided set of bridges or you may obtain and enter a custom set of bridges.

☒ Connect with provided bridges
 Transport type: obfs3 (recommended)


☐ Enter custom bridges [Help](#)
 Enter one or more bridge relays (one per line).

For assistance, contact help@rt.torproject.org

[! Copy Tor Log To Clipboard](#) [Quit](#) [Back](#) [Next](#)

- Most likely just skip use a local proxy
- Click connect

Tor Network Settings



Does this computer need to use a local proxy to access the Internet?

☐ Yes
☒ No

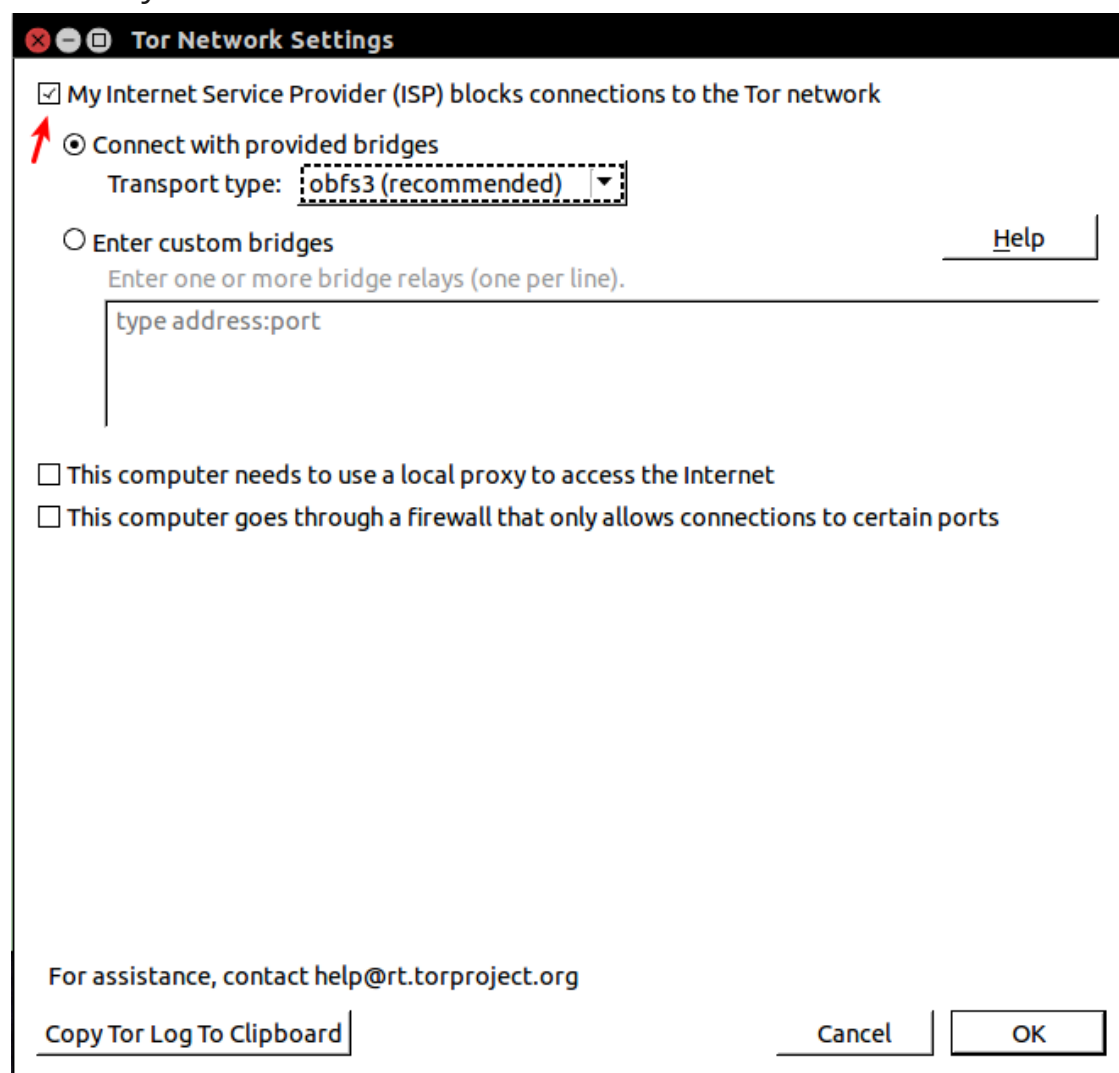
If you are not sure how to answer this question, look at the Internet settings in another browser to see whether it is configured to use a local proxy.

For assistance, contact help@rt.torproject.org

[! Copy Tor Log To Clipboard](#) [Quit](#) [Back](#) [Connect](#)

Optionally if Tor is already started you can:

- click the onion icon in the top left of the browser and select
- Open Network Settings
- check My ISP Blocks Connections and hit OK.



- Use obfs 3 which is recommended, see next section on other types.

PLUGGABLE TRANSPORTS

Pluggable Transports are extensions to Tor which utilize it's pluggable transport API. These are more advanced ways to disguise traffic flow, for instance making it appear as skype traffic or utilizing a flash proxy. Many are now included in the Bridge Option Menu, so this is a good resource to learn more about the specifics. Some may require **custom installation**.

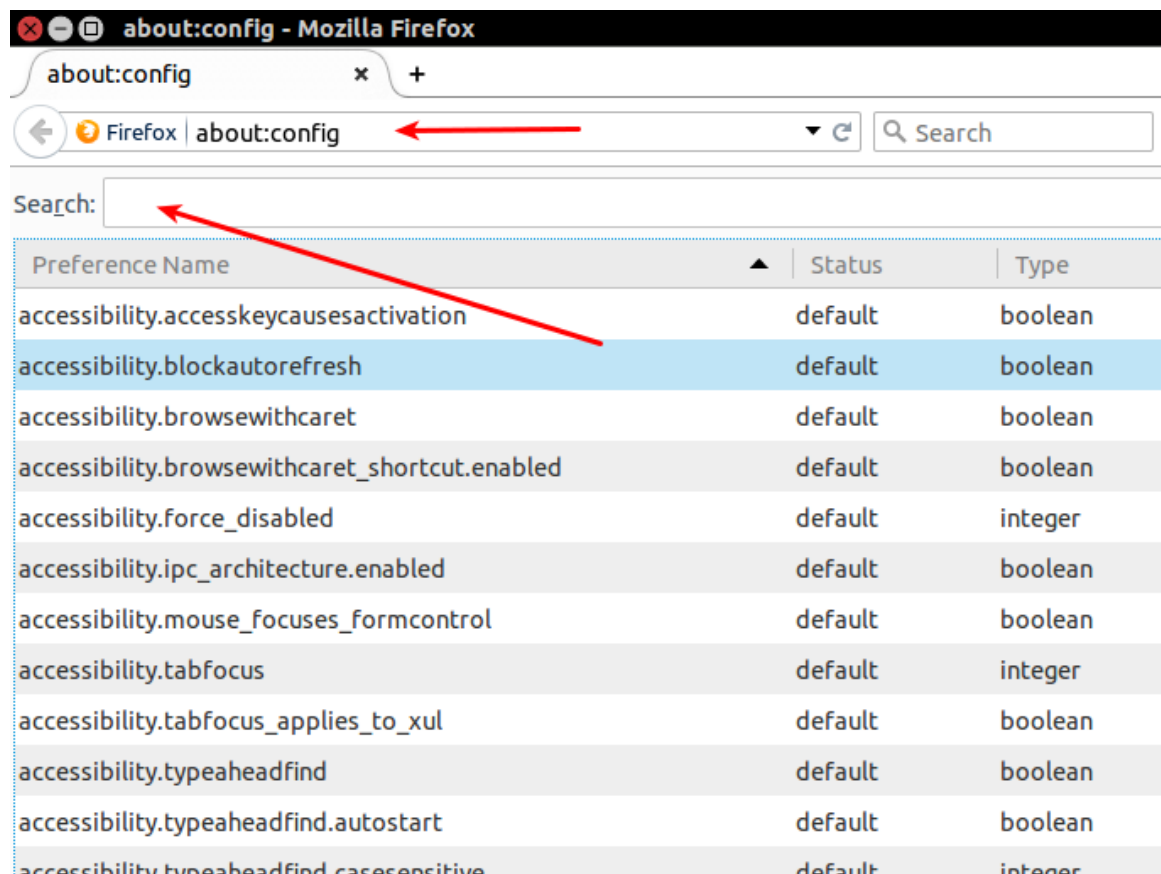
FIREFOX

If you need to use another browser Firefox is preferred. Here are some

configuration settings and extensions that can be helpful.

Optional Configuration:

In the URL Bar enter: about:config



- geo.enabled = false
- geo.wifi.uri = leave blank
- network.http.accept.default =
text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
- network.http.use-cache = false
- network.http.keep-alive.timeout = 600
- network.http.max-persistent-connections-per-proxy = 16
- network.proxy.socks_remote_dns = true
- network.cookie.lifetimePolicy = 2
- network.http.sendRefererHeader = 0

- network.http.sendSecureXSiteReferrer = false
- network.protocol-handler.external = false #set the default and all the sub-settings to false
- network.protocol-handler.warn-external = true #set the default and all the sub-settings to true
- network.http.pipelining = true
- network.http.pipelining.maxrequests = 8
- network.http.proxy.keep-alive = true
- network.http.proxy.pipelining = true
- network.prefetch-next = false
- browser.cache.disk.enable = false
- browser.cache.offline.enable = false
- browser.sessionstore.privacy_level = 2
- browser.sessionhistory.max_entries = 2
- browser.display.use_document_fonts = 0
- intl.charsetmenu.browser.cache = ISO-8859-9, windows-1252, windows-1251, ISO-8859-1, UTF-8
- dom.storage.enabled = false
- extensions.blocklist.enabled = false

Other useful options:

1. Disable all plugins: tools → addons → plugins
2. Disable all live bookmarks: bookmarks → bookmarks toolbar → R/click latest headlines → delete
3. Disable all updates: tools → options → advanced → update
4. Enable 'do not track' feature: tools → options → privacy

5. Enable private browsing, configure to remember nothing & disable 3rd party cookies: tools → options → privacy

Useful plugins:

it's best to keep plugins at a minimum but here are some to consider

- [HTTPS Everywhere](#)
- [Privacy Badger](#)
- [Close n forget](#)
- [ublock](#)
- [Modify Headers](#)
- [NoScript](#)
- [RefControl](#)
- [User Agent Switcher](#)
- [Adblock plus](#)

You may consider visiting ip-check.info to see what data your browser is sending.

ROUTER CONFIGURATION

It's recommended to get a router compatible with an open source firmware. The two major recommended firmwares are Tomato and dd-wrt. In some cases Tor, or a vpn can be run directly on the router, and this can be useful if you find yourself forgetting at times to enable your desired connection. A backup router only used for specific connections may also be useful to swap in and out when secure connection is needed.. For the crafty, a Raspberry Pi can be configured as a local device to route connections through.

Installation is device specific navigate to either the Tomato or dd-wrt site for more information.

TOMATO

tomatousb.org

Tor Version: (may not work for all versions)

dd-wrt

www.dd-wrt.com/site/support/router-data...

Tor: do your own research

RASPBERRY PI

raspberrypi.hq.com/how-to-turn-a-raspher...

makezine.com/projects/browse-anonymousl...

ANONYMITY NETWORKING

TOR

The stand alone Tor daemon can be found in the Ubuntu/Debian/Arch package manager.

```
sudo apt-get install tor
```

```
sudo pacman -S tor
```

However, you may wish to visit [this link](#) and add their PPA to get the latest version.

You can use Tor as a socks proxy once the service is started, either with the browser bundle or Tor daemon.

Navigate to the Network Settings, and Proxy section of the desired application.

Select Socks 4 Proxy and enter 127.0.0.1 port 9050.

This will route desired connections through Tor. TAILS automatically routes all connections through Tor.

I2P

Alternative to Tor, not as widely used since it requires some more dependencies and not as simple setup. i2p addresses always display as .i2p

Unlike tor i2p is a self contained network, it does not function as a proxy with traditional exit nodes. It is generally used to browse with the network of what are called eepsites.

Ubuntu/Debian based systems

1. follow guide to add i2p to package list
2. for ubuntu: `sudo apt-add-repository ppa:i2p-maintainers/i2p`
3. for debian
4. other see, and download necessary java files.

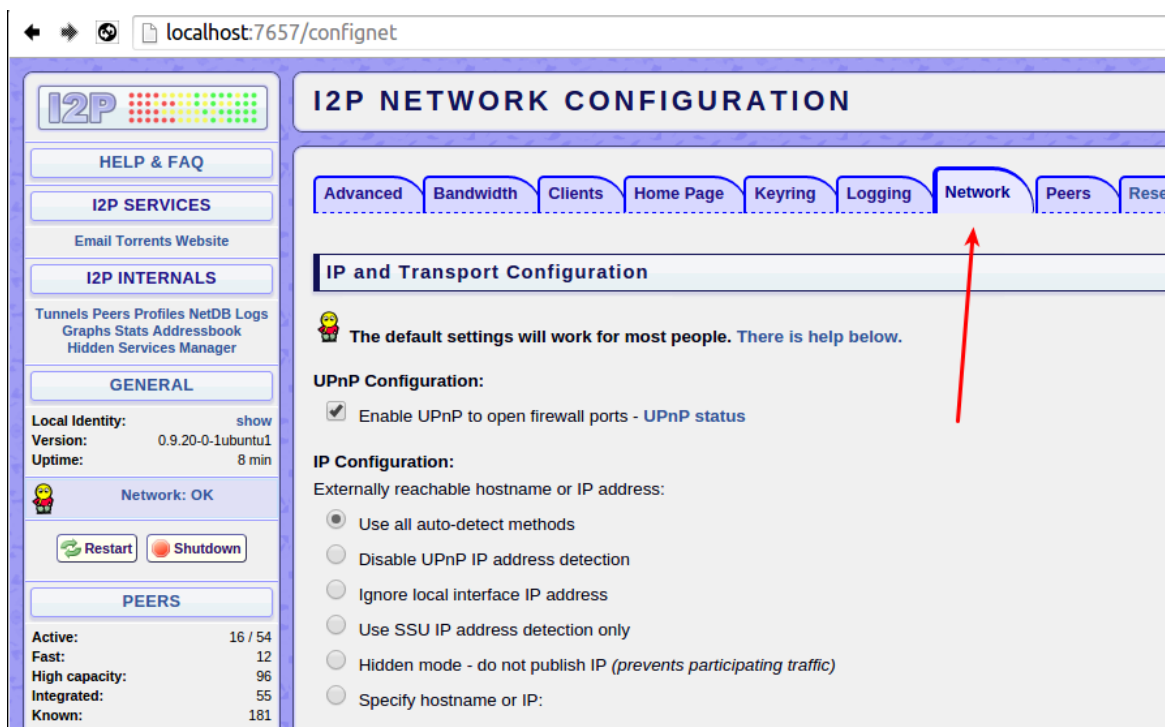
1. `sudo apt-get update`
2. `sudo apt-get install i2p`

starting i2p in terminal:

do not run as root or use sudo

- i2p router start

If you have issue connecting to .i2p addresses check configuration by visiting: `localhost:7657/confignet`



One main issue is your firewall or router is blocking connections. Click networking.

This screenshot shows the 'UDP Configuration' and 'TCP Configuration' sections. In the 'UDP Configuration' section, the 'UDP port' is set to 20026, highlighted by a red arrow. Below it is a checkbox for 'Completely disable (select only if behind a firewall that blocks outbound UDP)'. The 'TCP Configuration' section follows, with a message: 'Externally reachable hostname or IP address:'. It includes several radio button options: 'Use auto-detected IP address (currently 76.126.66.160) if we are not firewalled', 'Always use auto-detected IP address (Not firewalled)', 'Specify hostname or IP:' (with an empty text box), 'Disable inbound (Firewalled)', and 'Completely disable (select only if behind a firewall that throttles or blocks outbound TCP)'. Below these is the 'Externally reachable TCP port' section, which has a red arrow pointing to it. It includes radio button options: 'Use the same port configured for UDP (currently 20026)' and 'Specify Port:' (with an empty text box). At the bottom, there are notes: 'Notes: a) Do not reveal your port numbers to anyone! b) Changing these settings will restart your router.'

Basic port unblocking

IP Tables

1. `sudo iptables -A INPUT -p tcp --dport i2p port here -j ACCEPT`
2. `sudo iptables -L`

UFW

1. `sudo ufw allow i2p port here/tcp`
2. `sudo ufw status`

OTHER ANONYMITY NETWORKS AND SOFTWARE

Here are two good resources for additional information on available Anonymity Networks and Software:

gnunet.org/links/

freehaven.net/anonbib/topic.html

VPN

COMMUNITY VPNS

Good for activists and journalists:

riseup.net

autistici.org

Paid VPNs

Recommended resource:

[torrentfreak comprehensive VPN review](#) (2014) (remember their claims, are not a promise and even their systems could be vulnerable)

FREE VPNS

I don't recommend these at all but will list one that has been reliable. You'll have to search for more.

Unfortunately you should have no expectation of privacy on a free VPN but for one time use if you have no other choice it may be helpful.

VPNBOOK.COM

Of the free VPNs seems most reliable, please delicately read terms of service and

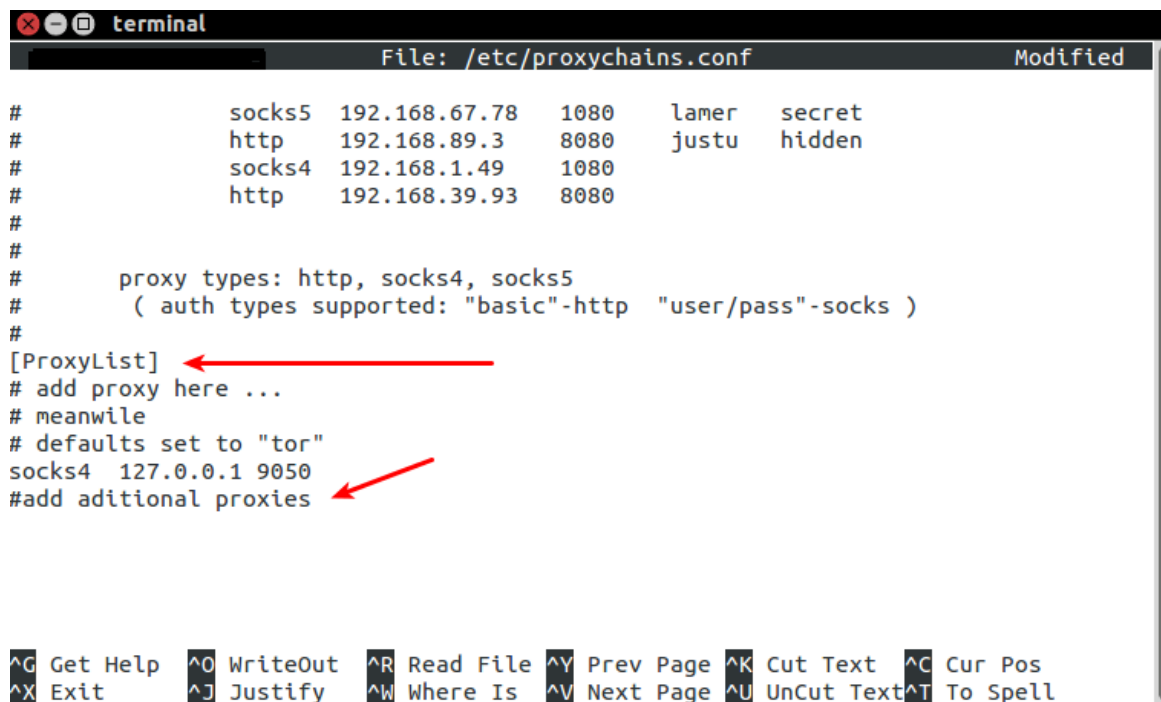
utilize Tor on-top of the VPN with any sensitive content. Free VPNs are often banned from posting on many services due to trolling. You can search for others but so far VPNBOOK just works.

PROXY CHAINS

Sometimes it may be necessary to use a proxy after the Tor exit node, for instance to appear in a desired location, or if exit nodes are banned on a service.

The setup is relatively simple on Linux.

1. `sudo apt-get install proxychains`
2. `sudo nano /etc/proxychains.conf`
3. following ProxyList add
socks4 127.0.0.1 9050 #Tor must go first
socks5 ipaddress port
proxies etc.....



```
terminal
File: /etc/proxychains.conf Modified
# socks5 192.168.67.78 1080 lamer secret
# http 192.168.89.3 8080 justu hidden
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
#
#
# proxy types: http, socks4, socks5
# ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
#add additional proxies
```

You will need to search for public socks proxy lists to populate.

start firefox in terminal: `proxychains firefox`

OPERATING SYSTEMS

The best first step is stop the use of Windows and MAC OSX, and stick with Linux.

FLASH FIRMWARE

Locate the firmware model of the motherboard on your computer and flash it with a fresh version. Some deeper level attacks embed themselves in the firmware, so it's good practice for a clean start.

ENABLING A BIOS BOOT PASSWORD

Usually f12 to enter BIOS, find security section (UEFI may be different)

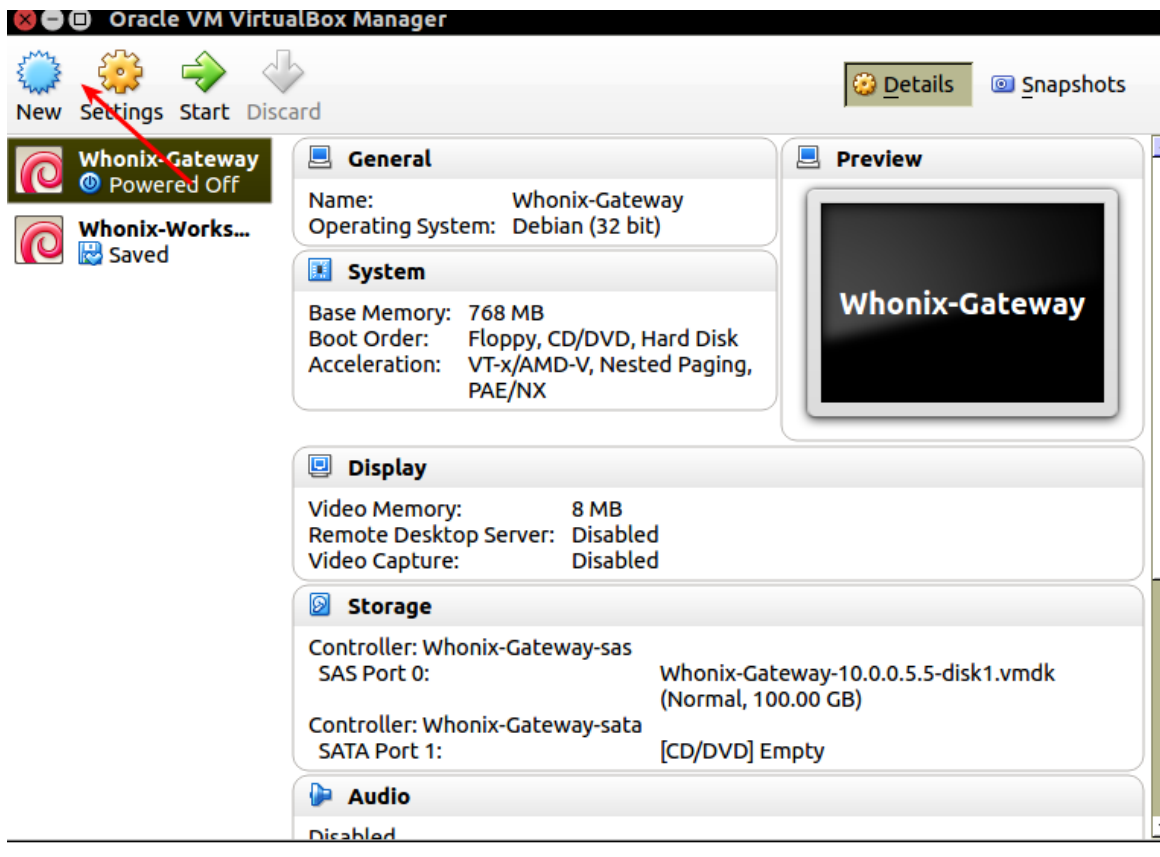
USB BOOTABLE OPERATING SYSTEMS:

Recommended: TAILS, Alternatives: Whonix, Liberté Linux and QubesOS

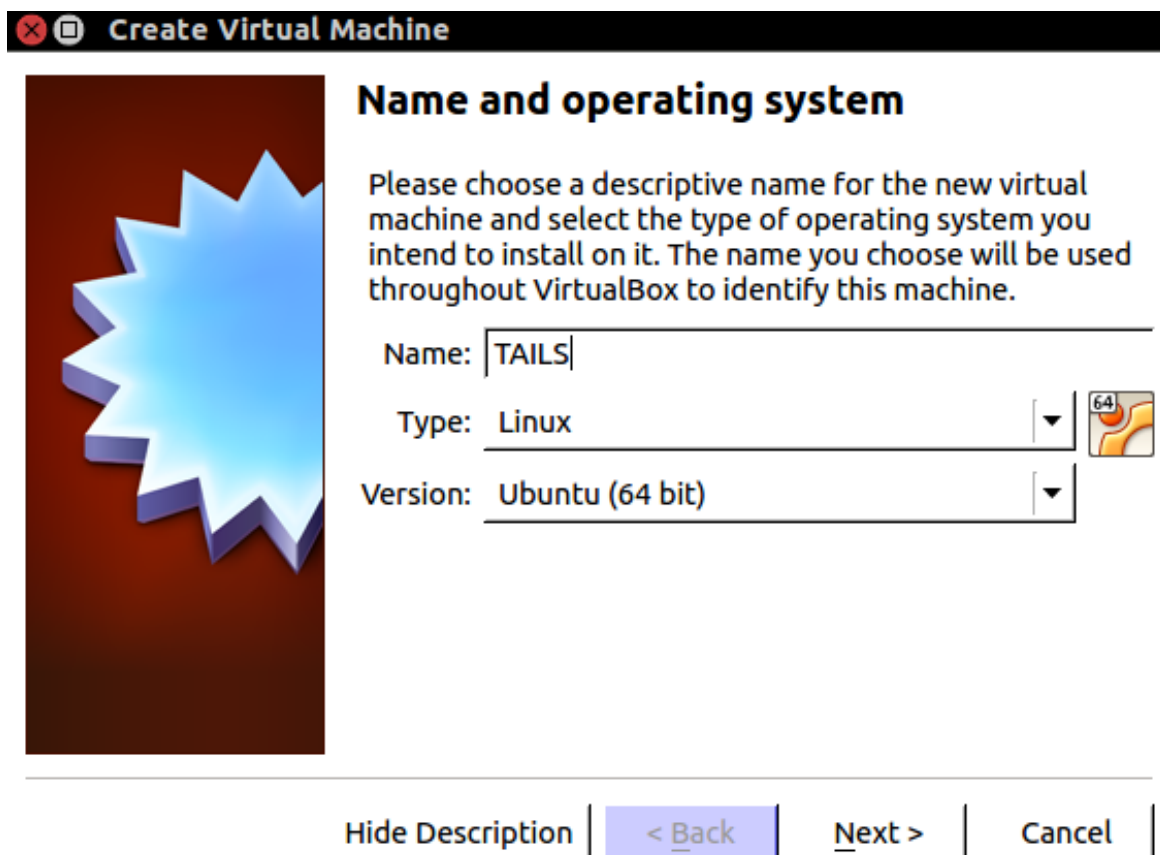
This guide shows how to install TAILS on a USB Drive from a Virtual Machine

1. [Download Virtual Box](#)
2. [Download the latest extension package](#)
3. Double click on the extension package and it should open Virtual Box, click install
4. [Download TAILS](#)
5. Verify file identity with PGP
6. Open Virtualbox and connect the USB drive

Click new in the top left:




Name your VM and select Linux 64bit or 32bit depending on which you downloaded:



Set memory size at least 1024 for smooth performance

Create Virtual Machine



Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **512 MB**.

1024

MB

4 MB8192 MB


< Back

Next >

Cancel

Create a virtual hard drive

Create Virtual Machine



Hard drive

If you wish you can add a virtual hard drive to the new machine. You can either create a new hard drive file or select one from the list or from another location using the folder icon.


If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard drive is **8.00 GB**.

☐ Do not add a virtual hard drive

☒ Create a virtual hard drive now

☐ Use an existing virtual hard drive file

Whonix-Workstation-10.0.0.5.5-disk1.vmdk (N) 

< Back

Create

Cancel

VDI Image is suitable

Create Virtual Hard Drive



Hard drive file type

Please choose the type of file that you would like to use for the new virtual hard drive. If you do not need to use it with other virtualization software you can leave this setting unchanged.

- ☒ VDI (VirtualBox Disk Image)
- ☐ VMDK (Virtual Machine Disk)
- ☐ VHD (Virtual Hard Disk)
- ☐ HDD (Parallels Hard Disk)
- ☐ QED (QEMU enhanced disk)
- ☐ QCOW (QEMU Copy-On-Write)

Hide Description

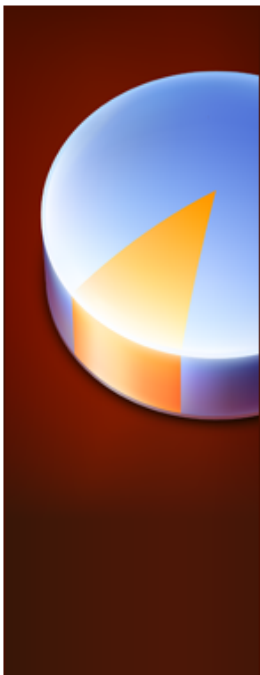
< Back

Next >

Cancel

You can select dynamically allocated and set a starting amount at a couple gigabytes

Create Virtual Hard Drive



Storage on physical hard drive

Please choose whether the new virtual hard drive file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard drive file will only use space on your physical hard drive as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard drive file may take longer to create on some systems but is often faster to use.

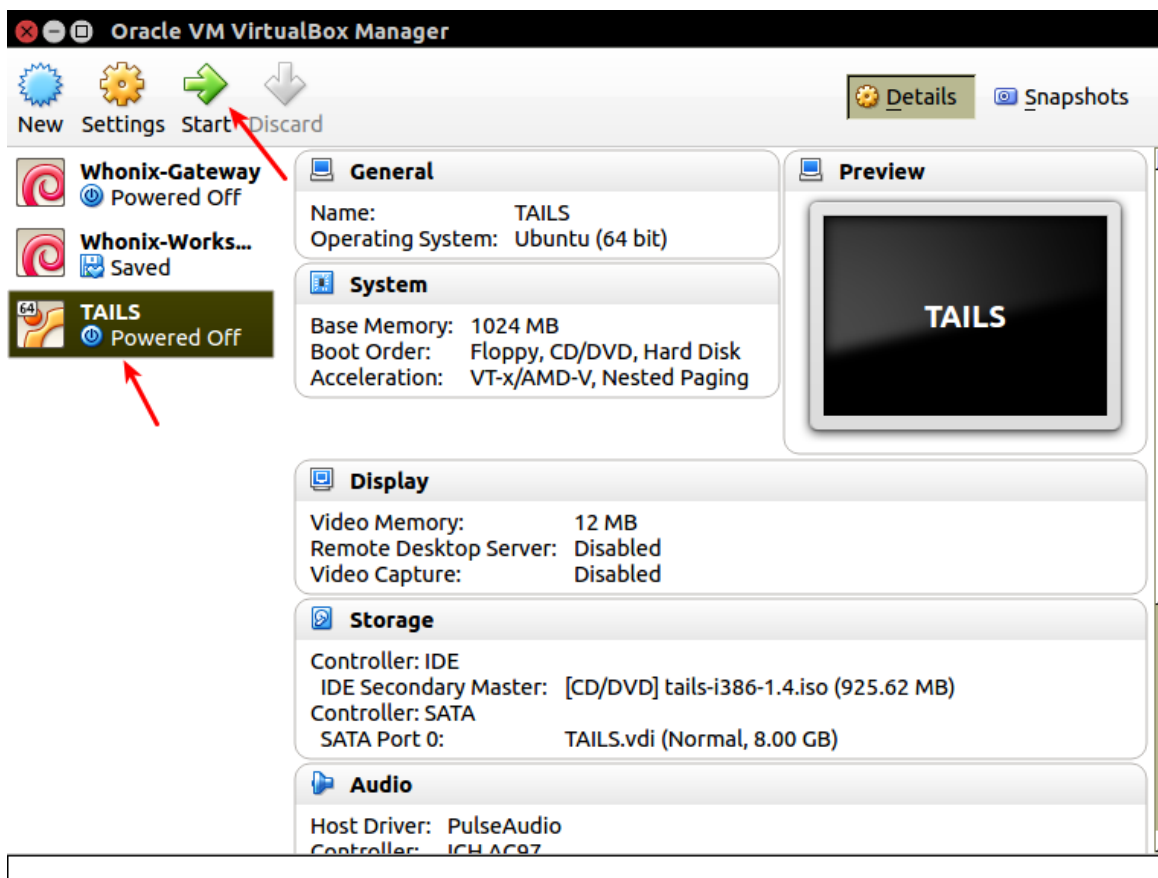
- ☒ Dynamically allocated
- ☐ Fixed size

< Back

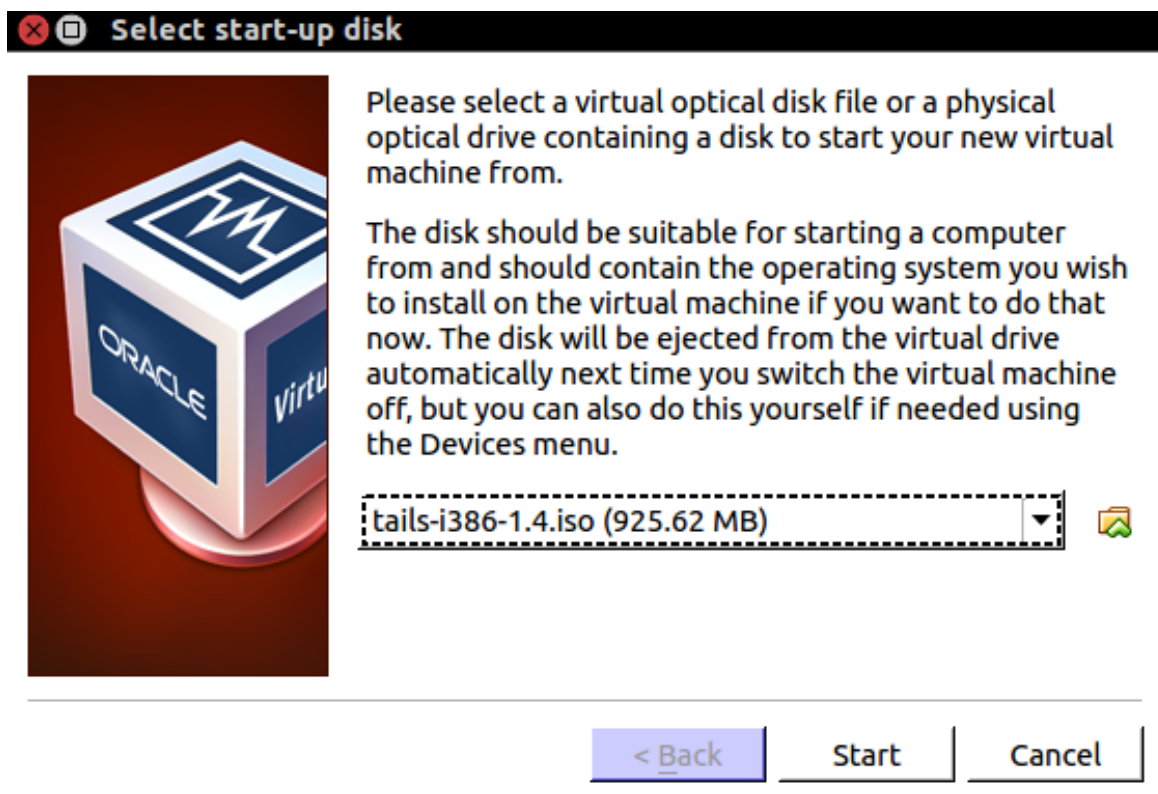
Next >

Cancel

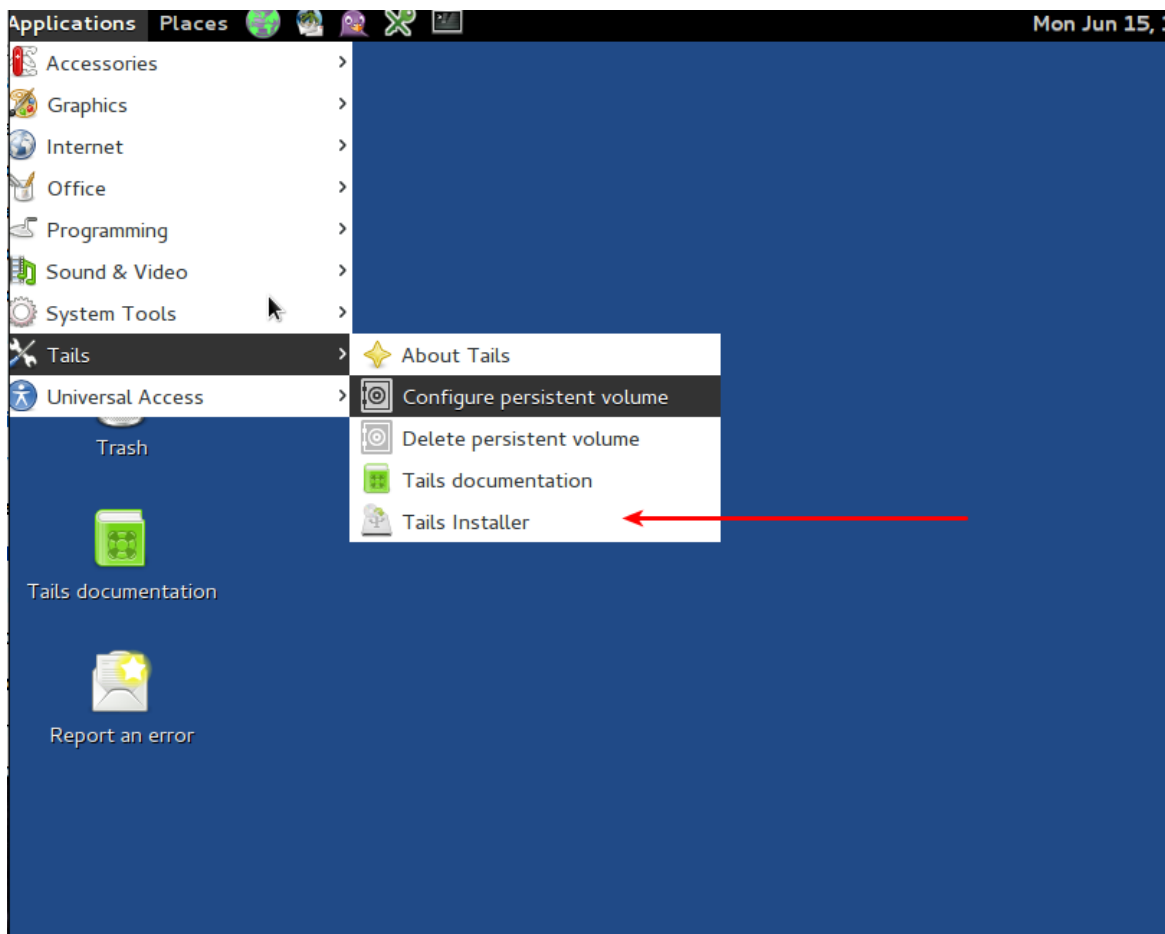
Select the image and click start



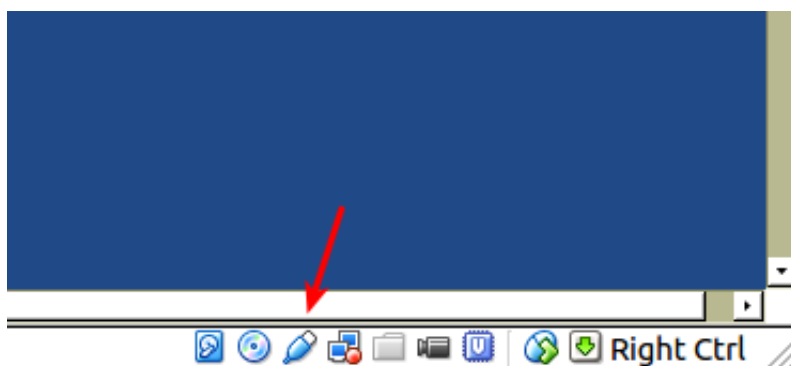
Select the location of the .iso file you downloaded.



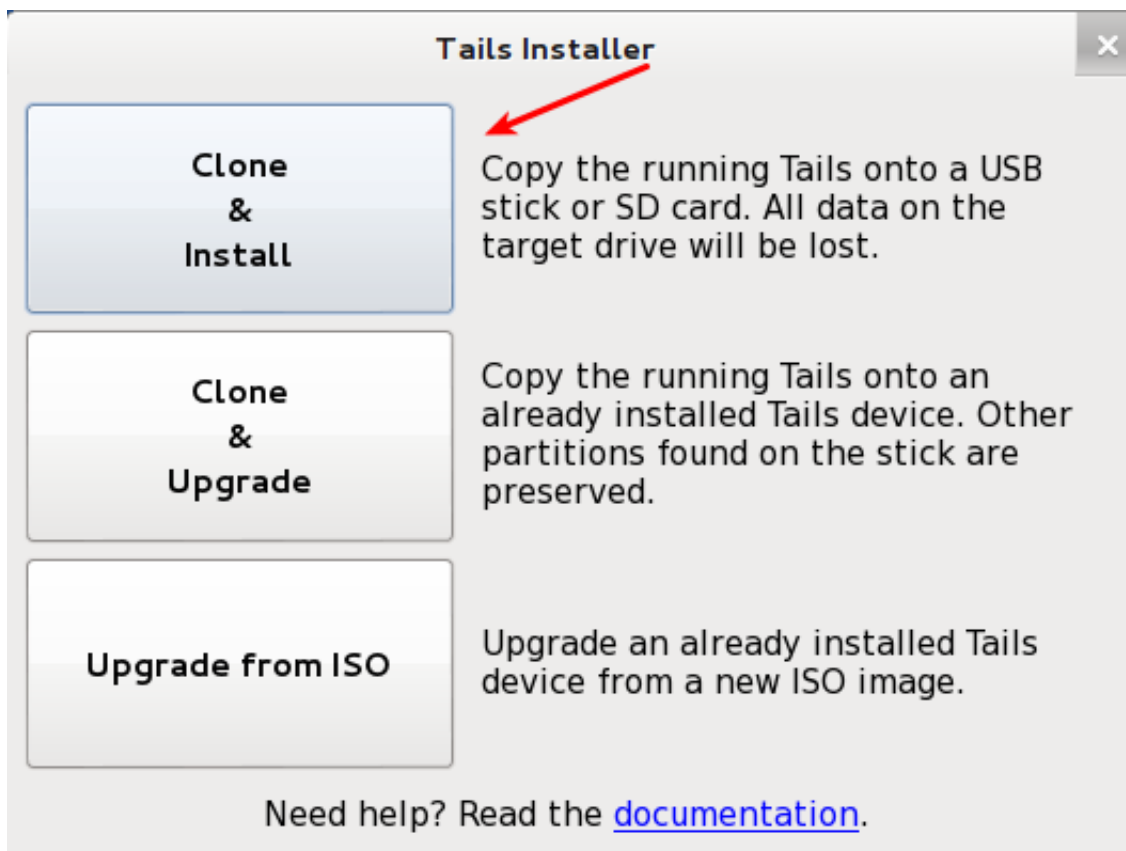
Once started go to Applications → Tails → Tails Installer



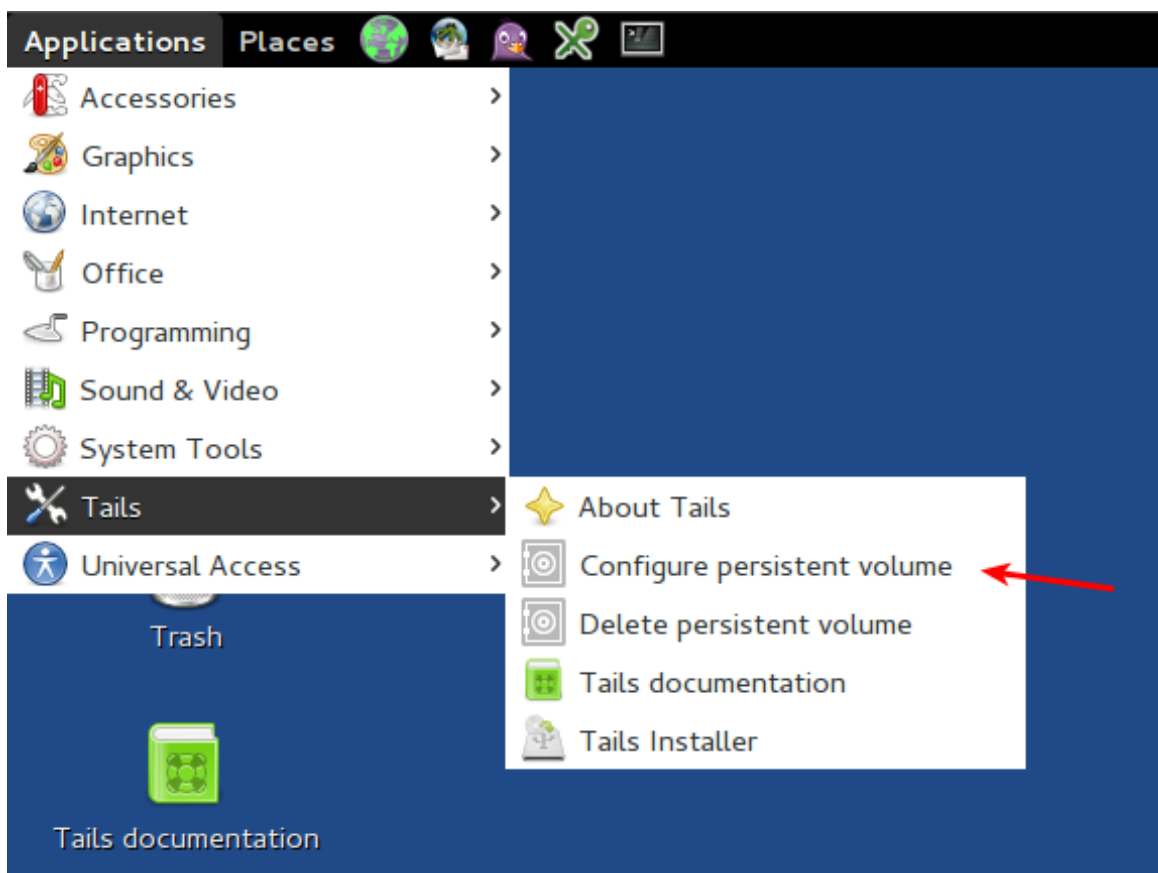
Make sure the USB Drive is present you will see a green plus, over the usb icon in this image



Select clone and install and follow the steps for installation



Once you've started tails you can create a persistent volume to store static content



1. Next reboot you will be prompted if you wish to use persistent or not, only use when necessary.

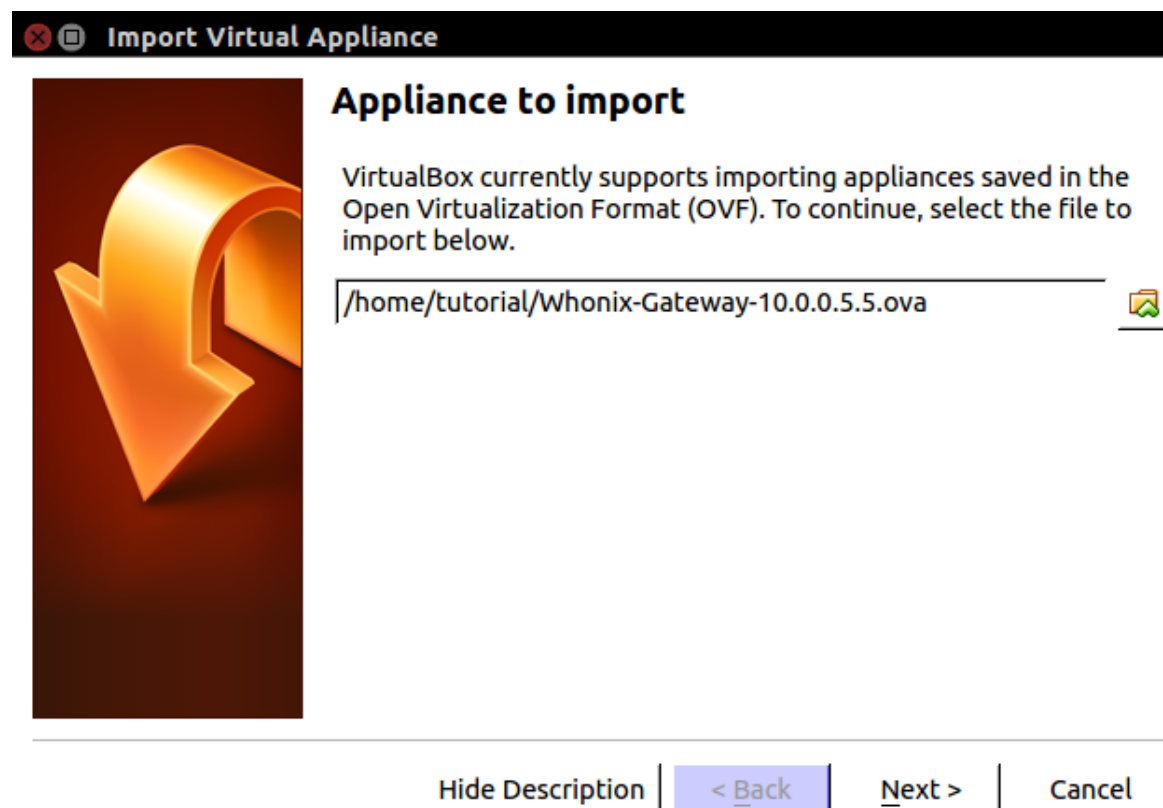
LINUX (IMAGE FILES CAN BE FOUND AT [HTTP://DISTROWATCH.ORG](http://distrowatch.org))

Recommended base Operating Systems: Archlinux, or Kali, alternatives: Debian Mint Ubuntu
although just using Tails as a bootable OS and having some persistent storage is probably better than most can do in terms of hardening their base system.

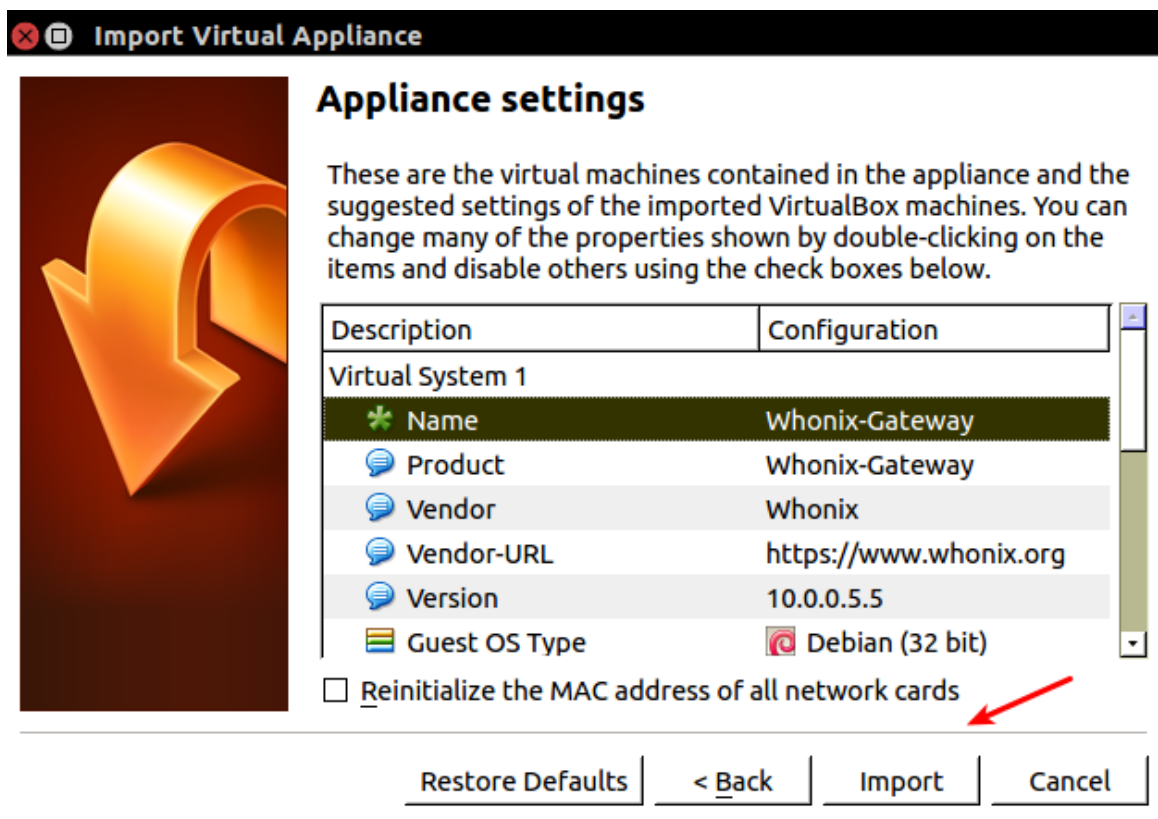
SECURE VM WITH WHONIX AND VIRTUALBOX

1. [Download both Whonix-Gateway and Workstation](#)
2. [Download Virtual Box](#)
3. You may want to verify the file identities using the Signing key see other sections on this.

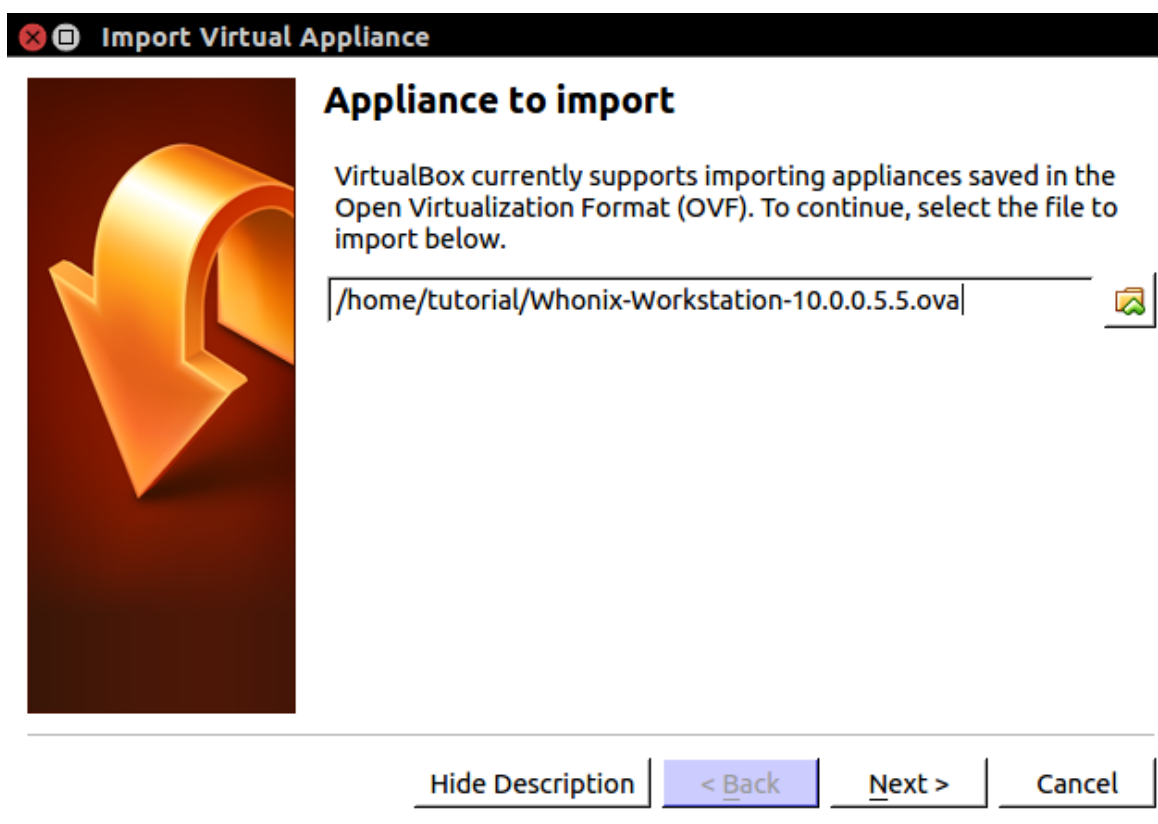
Click file import appliance and select the Whonix Gateway .ova file:



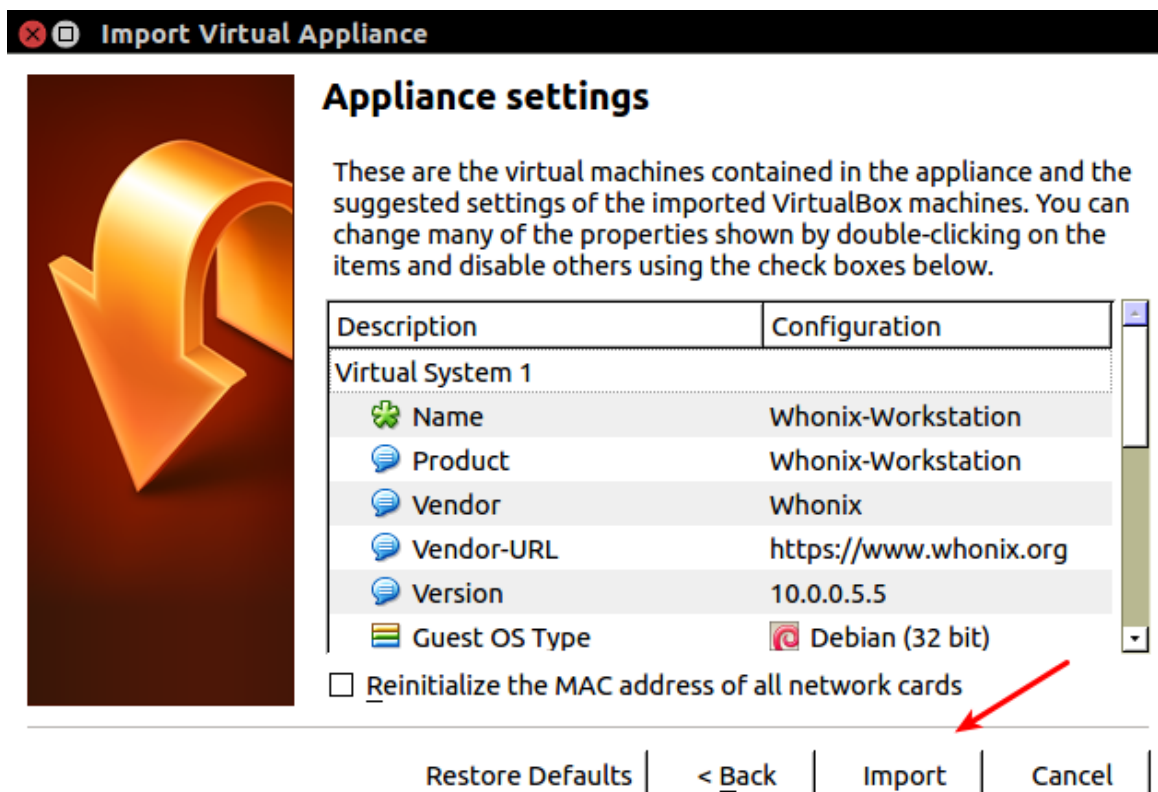
Keep the settings default and click import



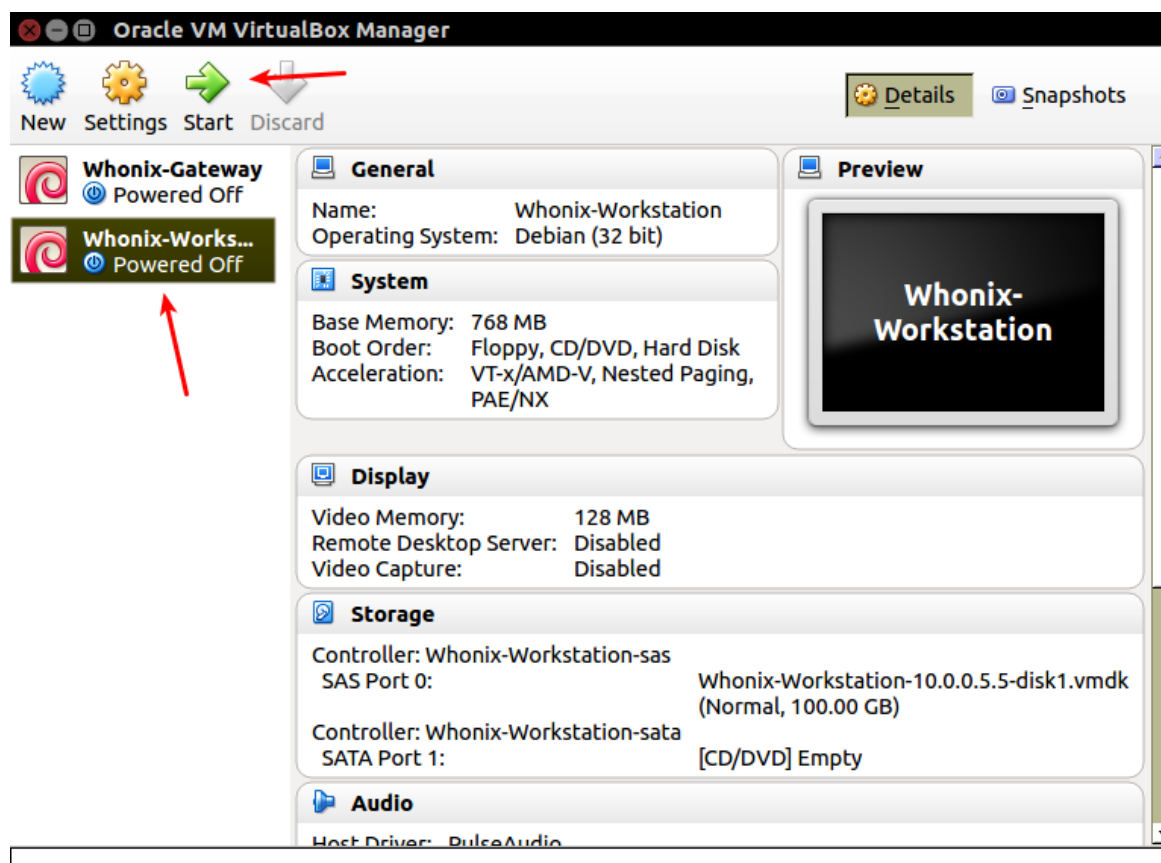
Repeat for workstation, select the .ova



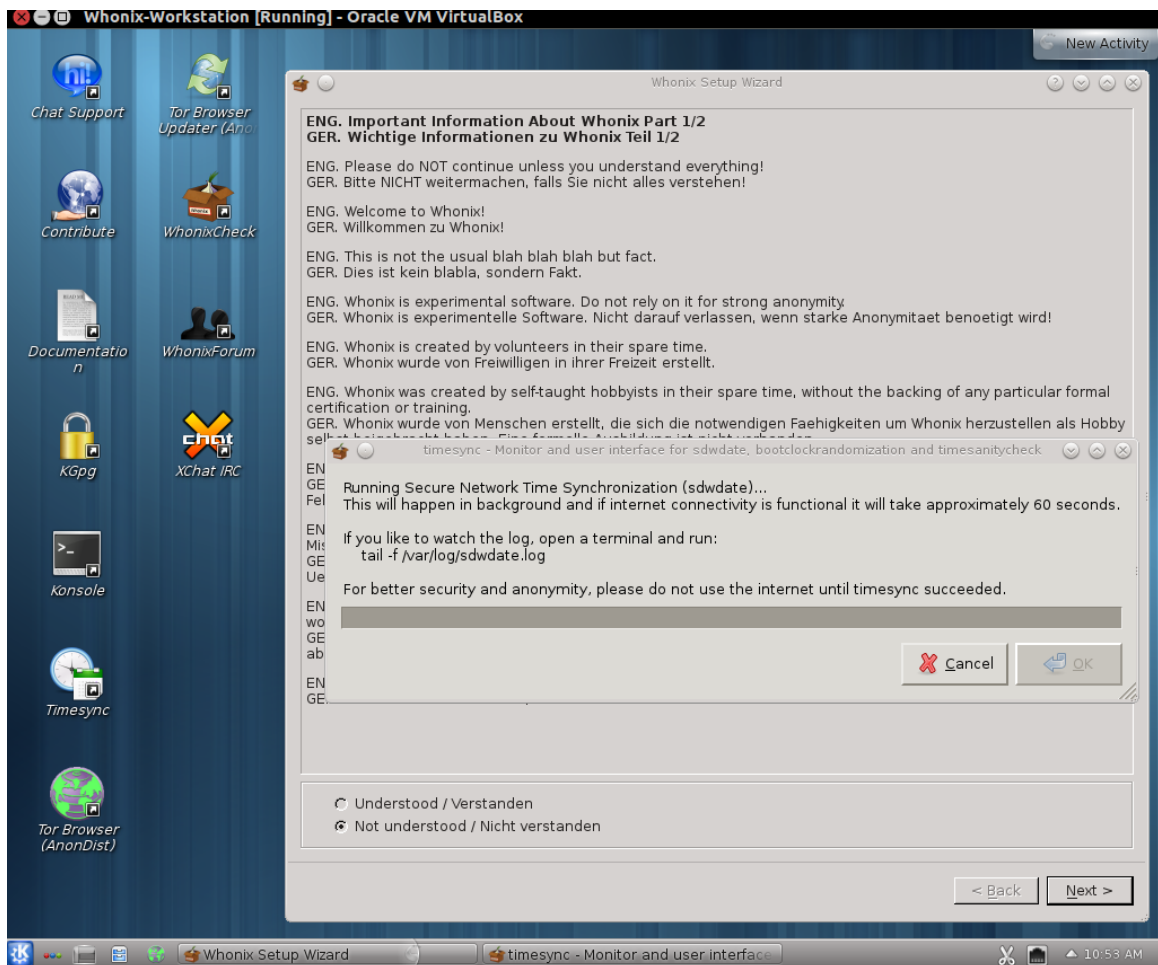
Import without changing settings



Select both and start both at the same time.



Once workstation has finished booting you will see this screen.



You will keep both VM Windows open but all activities will be within the Whonix-Workstation VM Window

BASE SYSTEM

Essentials:

Disk encryption – LVM Encryption during install, encrypt home directory

Bleachbit – clearing day to day files (RAM wiping is experimental but worth it on shutdown)

secure-delete package – secure wiping content

Intro guides on hardening other recommended base systems.

(may be out of date look for hardening guides)

1. Kali has basic hardening
2. Arch Security
3. Ubuntu Security

SECURE DATA-WIPING LINUX

Consider using an OS like TAILS with minimal persistent storage and automatic memory wiping to make this easier.

Proceed with extreme caution, man pages are your friend.

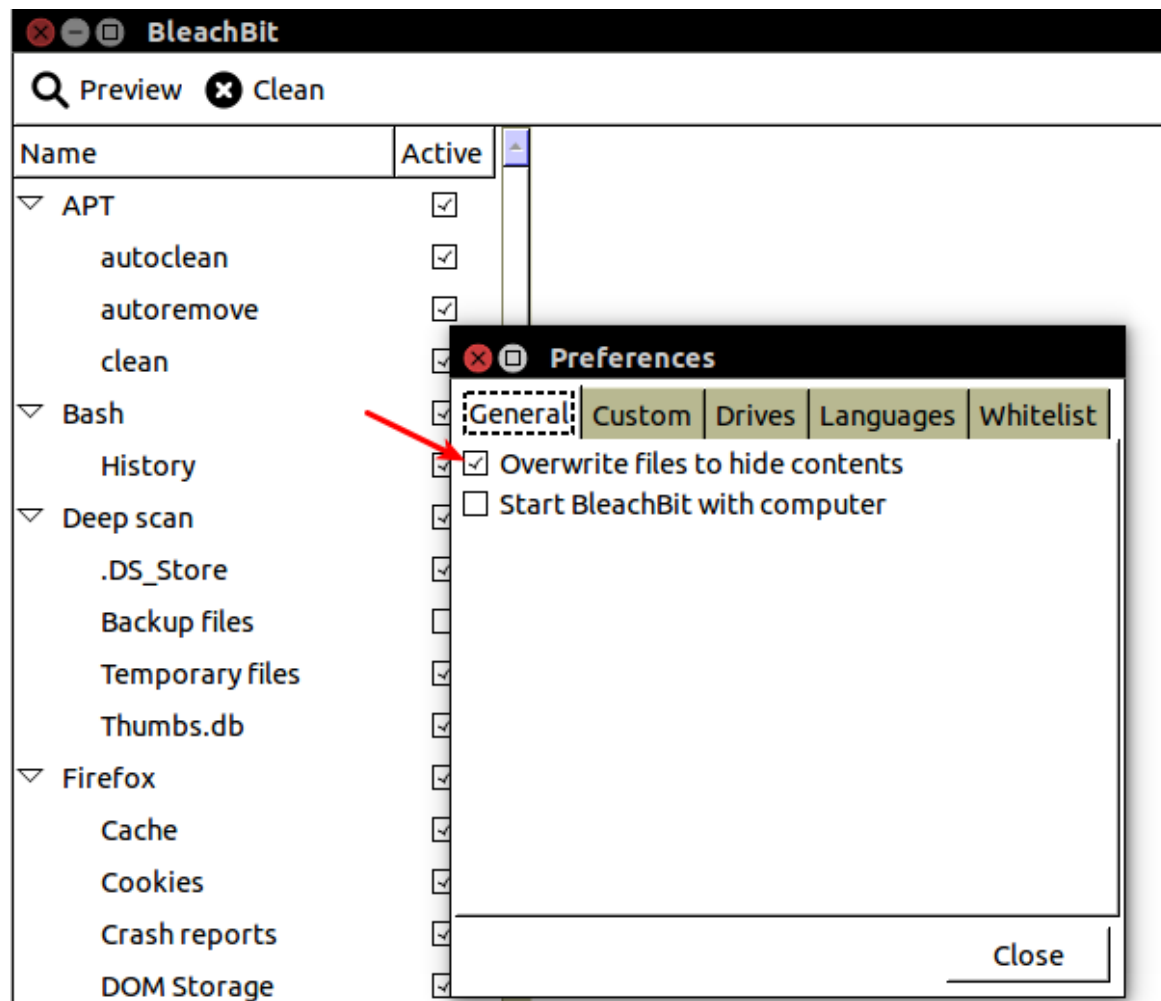
BleachBit

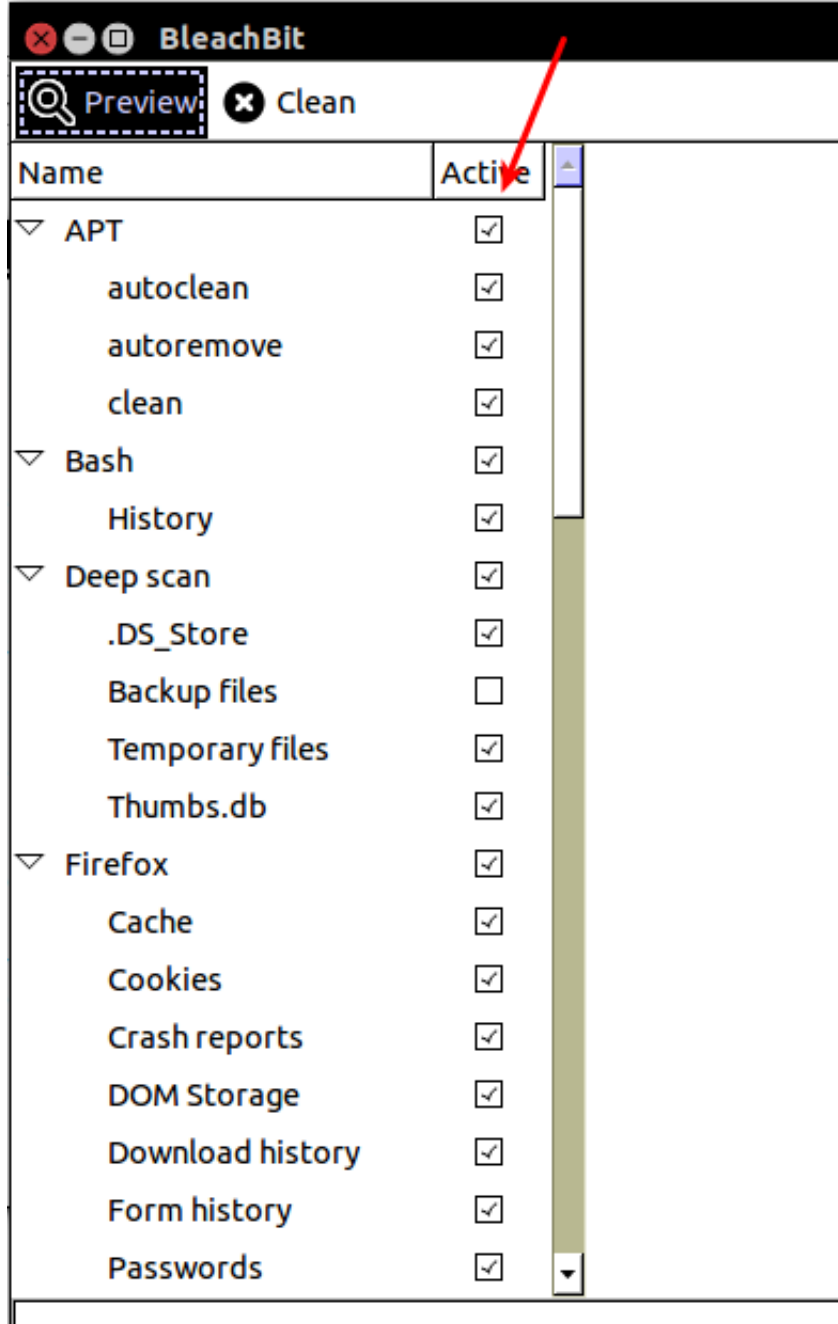
easy, less effective

First:

```
sudo apt-get install bleachbit
```

```
sudo bleachbit
```





You can “Shred” files and folders from the file menu, and wipe free space, which may remove excess data that still exists, without pointers.

file → Shred files

file → Shred folder

file → wipe free space

DBAN

advanced, boot from usb/cd ideal when discarding a hard drive

go to dban.org download the dban.iso and either burn CD/DVD or write to USB and boot off the device.

Select “RCMP TSSIT OPS-II” for the deletion method

Select the drive

Prepare to wait 12+ hours

Secure-Delete

hard mode, more secure deletion than bleachbit, easier to use if you want to remove specific partitions or files, rather than complete wipe with DBAN

you will need to boot off a usb/cd if you wish to wipe your primary hard drive.

Properly deleting a drive will take time, if you're in a hurry, you can at least use fast mode.

First:

```
1 sudo apt-get secure-delete
```

If you're wiping a disk

```
1 fdisk-l
```

find the disk/partition name: should be /dev/sdxx

at this point if you haven't already, consider encrypting the partition, see veracrypt.

wipe space considered free (-f is fast mode "insecure mode")

```
1 sudo sfill /dev/sddisk#
```

if you need to clear swap space-
(-f is fast mode "insecure mode")

1. cat /proc/swaps
2. sudo swapoff /dev/sddisk#
3. sudo sswap /dev/sddisk#
4. sudo swapon /dev/sdFdisk#

if you are strapped for time, use -m for 7 passes or -s for simple 1 pass
"insecure mode"

```
1 sudo srm file
```

or

```
1 sudo srm -r /directory
```

or

```
1 srm /dev/sddisk#
```

At the end you may also be interested at the end to wipe memory on the system.

(-f is fast mode “insecure mode”)

Enter:

```
1 sudo sdmem
```

PHYSICAL DESTRUCTION

Try to at least encrypt the disk first, if you have time to spare, follow the instructions for disk erasure with DBAN.

Open the drive. Find the platter, score it, smash it. Then you will need to locate any memory chips which may store cached files, and destroy them as well. This is an important step, and can be missed easily. Remember not to dispose in normal garbage as it’s not secure. Consider alternate means of disposable for best measure.

Fun Fact: To “officially” destroy all remnants of magnetic data you’ll need to heat it to 1500 kelvin.

COLD-BOOT ATTACK

Older attack method recovering encryption keys stored in RAM. If possible use DDR3 or better memory. When not at the computer always shut down completely.

Consider using Bleachbit or more advanced sdmem to wipe RAM

contents.

BASIC COMMUNICATIONS

Keep in mind that your use of grammar, spelling and language can be used as identifying factors. It is possible to single you out based on your specific ways of communication and link you to other public content linked to your alternate identities. When attempting to communicate anonymously remember not to mention nicknames, locations favorite music, weather or any other information that can be used to reveal your identity. Something that seems mundane and friendly can quickly be used for identification.

IMAGES

JPG, JPEG, TIF and WAV files store EXIF data, or Exchangeable image file format, that can store sensitive information, including GPS-location, and the unique ID of the device used. It is recommended to always use the PNG format, and scrub any metadata, if you need to exchange an image. One option is the Metadata Anonymisation Toolkit that comes with TAILS, and also available at <https://mat.boum.org/>

EMAIL PROVIDERS

No mail provider can be trusted completely no matter what their security claims are. Utilize PGP as often as possible and utilize an anonymous connection when connecting.

PROTONMAIL.CH

Protonmail is currently invite only and requires a wait time of anywhere from a month or more to get in. However, it's a highly respected secure email solution. You can employ PGP and encrypted storage. They have a favorable location

TUTANOTA.COM

Tutanota offers encrypted mail-storage and the use of a one time password, however PGP has to be done manually as there is no smtp or imap mail servers. They have a favorable location that is difficult to retrieve data from with legal orders.

MAIL2TOR.COM

While tor based mail providers have had a storied history. If PGP is utilized for all communications, the threat is eliminated. If you receive something compromising in plain text, don't consider this information secure, and inform any correspondents to employ PGP.

RISEUP.NET

United States based privacy centric collective that offers mail and other privacy capabilities.

OPENMAILBOX.ORG

free, secure email provider

STARTMAIL.COM

paid email

pgp webmail client

offshore hosting more protected from spying

VMAIL.ME

free, no personal information

account deletion

encrypted data storage

user details like ip address and user agent stripped from headers

AUTISTICI

privacy centric collective offering email, hosting, vpn and other anonymity service

JABBER_XMPP/OTR

1. sudo apt-get install pidgin
2. go to tools → preferences
3. Logging: disable log all instant messages/log all chats
4. Go to proxy
5. Select Socks 4
6. enter: 127.0.0.1 9050
7. [Go to this link](#)
8. Under Security
9. Download/Install: Off-The-Record, Pidgin-GPG
10. Install any dependencies Activate Plugins in: Tools → Plugins
11. Once activated, select configure plugin for both

FOR OTR

1. you will need to generate a unique key
2. Enable Private messaging
3. Disable logging
4. Automatically initiate private messaging (optional)
5. Select show OTR in tool-bar
6. If a conversation is not private you will see a box saying Not Private
7. Click Start Private Conversation
8. If your partner has OTR properly configured it will display private.

FOR PIDGIN-GPG

1. select main key in options
2. toggle encryption mode in conversations:
3. options → toggle openpgp encryption

ALTERNATIVE MESSAGING OPTIONS

POND ([POND.IMPERIALVIOLET.ORG](https://pond.imperialviolet.org))

forward secure, asynchronous messaging for the discerning. Pond messages are asynchronous, but are not a record; they expire automatically a week after they are received. Pond seeks to prevent leaking traffic information against everyone except a global passive attacker.

SCRAMBLE.IO

secure messaging between scramble users

BITMESSAGE.ORG

p2p encrypted messaging, like sending messages as Bitcoins

BITMESSAGE.CH (TOR AND I2P URLS AVAILABLE)

webmail gateway for bitmessage with instant send to other users with @bitmessage.ch address

GNUPG/PGP BASICS

A PGP Key is a unique identifier, do not re-use across accounts and especially not with any public address.

Simple PGP On Linux

terminal

Ubuntu- `sudo apt-get install gpa gnupg2`

Arch- `sudo pacman -s gpa gnupg2`

Generating Keys-

1. in terminal enter: `gpg --gen-key` or open gpa in terminal and it will prompt you to create one.
2. follow the prompts

in most cases select option 1 – RSA and RSA (default)

select at least 2048 key size

key expiration, hit enter if not needed.

do not enter real information for contact (unless intended)

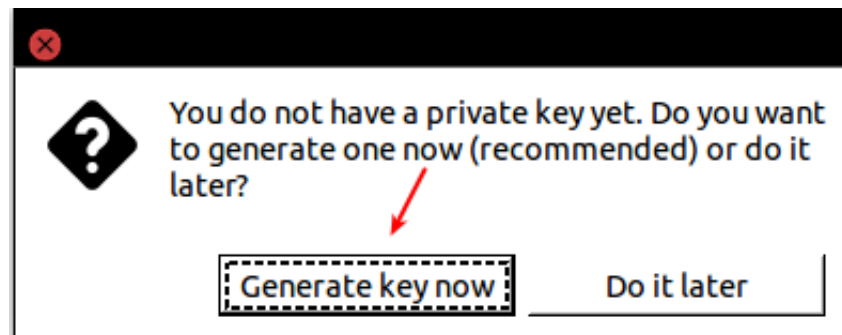
use a secure passphrase for the key

it will then ask you to move the mouse, type etc to create entropy

Simple PGP with GNU Privacy Assistant

If you open gpa it will guide you through creating your first key

don't put real information unless intended, obviously




```

user@terminal: gpg --gen-key
gpg (GnuPG)
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
    0 = key does not expire
    <n> = key expires in n days
    <n>w = key expires in n weeks
    <n>m = key expires in n months
    <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: user@terminal
Email address: user@terminal2
Comment: none
You selected this USER-ID:
    "user@terminal (none) <user@terminal2>"

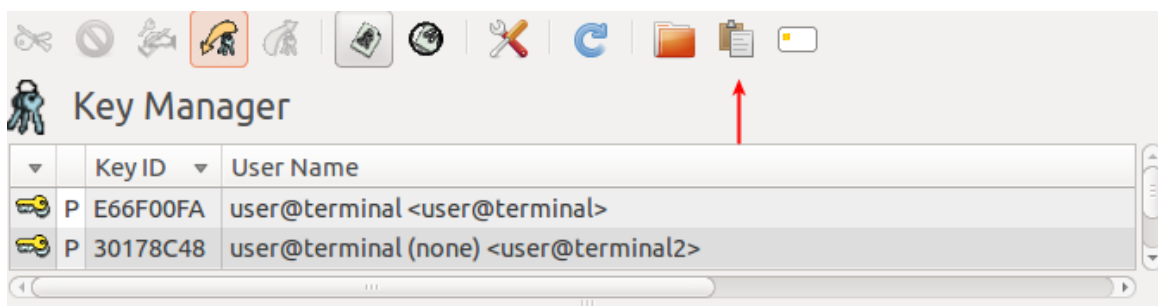
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

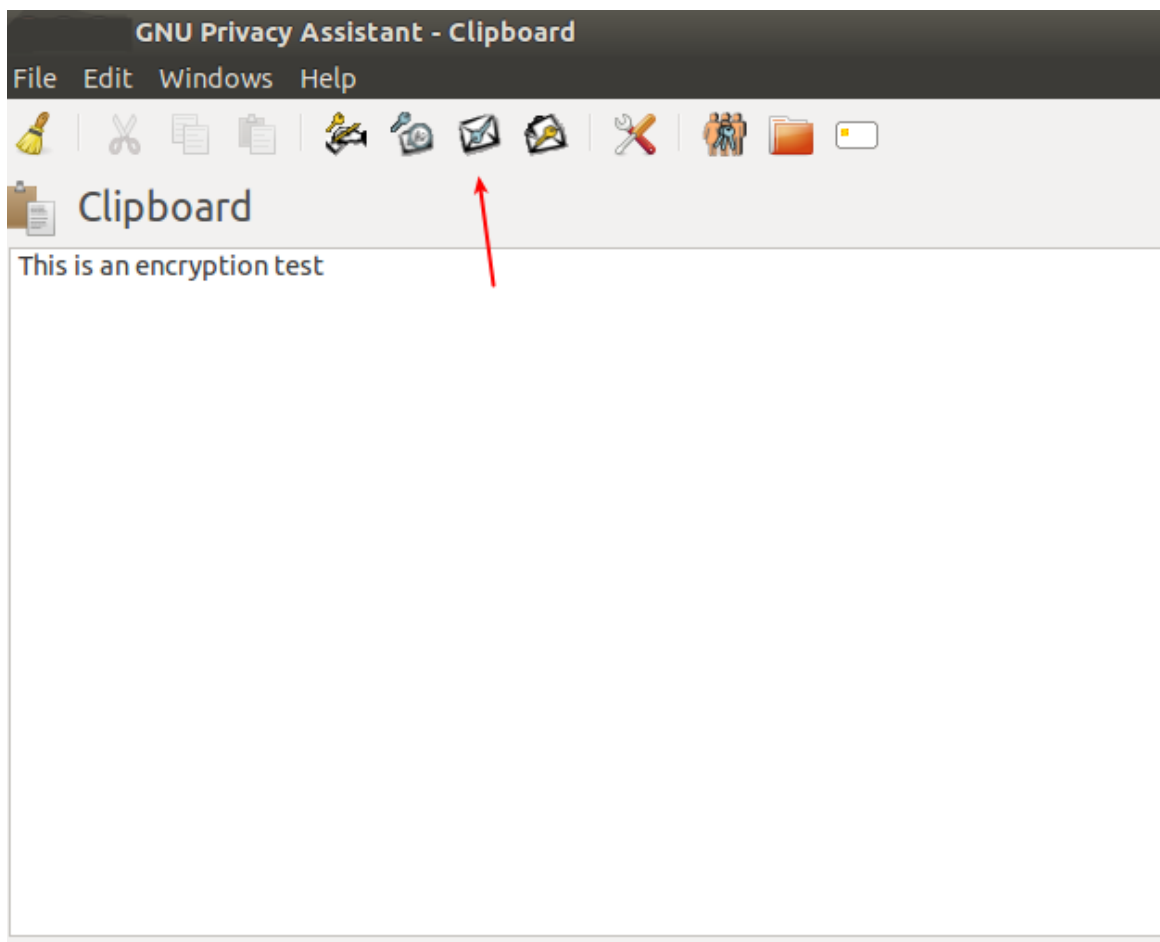
```

Either click refresh or restart gpa and the keys will appear

Click the clipboard



Enter your message



Select the key you wish to sign it with

Encrypt documents

Public Keys

Key ID	User Name
E66F00FA	user@terminal <user@terminal>
30178C48	user@terminal (none) <user@terminal2>

☒ Sign

Sign as

Key ID	User Name
E66F00FA	user@terminal <user@terminal>
30178C48	user@terminal (none) <user@terminal2>

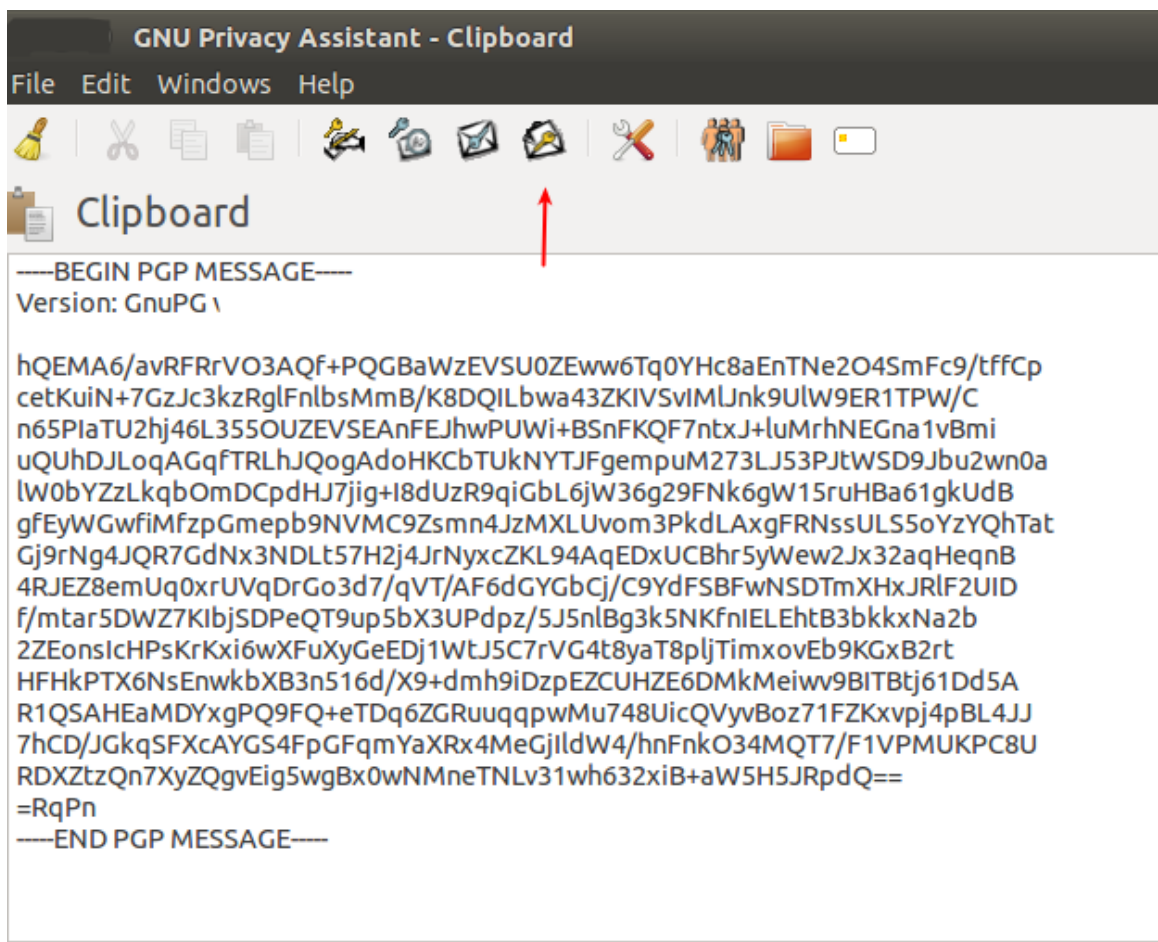
☒ Armor

Cancel

OK

You will now see an encrypted message.

To decrypt a message click the mail icon with the key, and it will allow you to choose the appropriate key.



More details on GPA

Exporting/Importing Public Key

gpa

1. select your key-pair, and then select keys → export or import keys and proceed

Exporting/Importing Private Key

gpa

1. select your key-pair, and then select → keys → export or import keys and proceed
2. either choose where to save or paste the desired key

Verifying a message

gpa

1. select → keys → imports

2. paste the public key
3. Select window → clipboard
4. Paste the entire text
5. Click icon with the green key (hover over for title if hard to see)
6. If the information is genuine it will display the name of the previously imported public key.

Verify a file

1. gpa
2. select → keys → import
3. paste the public key
4. back to terminal
5. `gpg --verify file`

PGP with Email

Thunderbird is probably the most widely known, if you prefer reference the Ubuntu guide below which explains alternates.

1. `sudo apt-get install thunderbird enigmail`
2. Open Thunderbird
3. Open Preferences → enigmail → Preferences
4. Set the GPG path, in Ubuntu default is `/usr/bin/gpg`

You can also cut and paste your messages from GPA into the message window.

TAILS PGP

TAILS has an OpenPGP Applet – [Visual Guide](#)

ADDITIONAL READING ON PGP

Recommended Best Practices for PGP from [Riseup.net](http://nzh3fv6jc6jskki3.onion/en/security/message-security/openpgp/best-practices) or:

<http://nzh3fv6jc6jskki3.onion/en/security/message-security/openpgp/best-practices>

Additional Reading:

- [GnuPrivacyGuardHowto](#)
- [PGP \(Pretty Good Privacy\) and GnuPG \(GNU Privacy Guard\) notes](#)

PGP VERSIONS

PGP Versions can reveal the users operating system, and you should research strange versions as some PGP Libraries are known to have weak encryption.

VALIDATING FILES WITH MD5 OR SHA1:

SHA1 SUM

When the file is provided ideally a SHA1/MD5/PGP Sum will be provided.

It will look like a long string of characters.

In Linux terminal type: sha1sum filename

The output should be the same as the supplied string.

MD5 SUM

When a file is provided ideally an SHA1/MD5/PGP Sum will be provided.

It will look like a long string of characters.

In Linux terminal type: md5sum filename

The output should be the same as the supplied string.

