

***** This tutorial was last updated on March 2021, copied from HackTown (hacktownpagdenbb.onion)*****

OPSEC

Welcome to the first course offered here at HackTown.

This is step one towards your journey in becoming an efficient and effective cybercriminal in 2020 and beyond. This course will teach you how to hide your tracks and prevent you from being followed while launching a cyber attack, posting somewhere, or doing anything that's questionable online. This course is designed to teach you more about cyber security and how to keep your OPSec on point while using the Operating System (OS) of your choice.

If you're looking for more teachings, guidance, and more courses surrounding cybercrime along with how to successfully pull them off then consider purchasing a membership at HackTown.

There will be points throughout this guide marked in **BLUE**. These points are useful to fully grasp the concepts taught and help with understanding techniques and explanations on various topics. It's important that when you read them you stop and take the time to do what they say or follow up with them. The syntax of code to be typed into Terminal or the command line will be **RED**. So anytime you see something in **RED** you know that it's syntax code and should be entered into Tails, Whonix, Kali, Terminal, Windows command line, etc.

This course, like every course here at HackTown, is based on my experience when I was operating as a cybercriminal with the techniques, tactics, and procedures I used during my operations. I was a successful cybercriminal who retired many years ago with cashing out the profits I made through cybercrime and enjoying DAT cryptocurrency boom! I've been floating around in life for quite some time and having too much time on your hands is never a good thing. Since I've always enjoyed writing I've designed these courses around my experience as a cybercriminal giving you the opportunity to duplicate my tactics, techniques, and procedures to experience financial freedom for yourself.

First off there is no one way of doing things. These courses are not the word of law when it comes to cybercrime but are built around my perspective so if you have something to add, have a better way of explaining things, or anything you think that I don't know that pertains to the topics in these courses send me a god damn email and let me know what is WAT. That way we can keep it all updated for everyone to enjoy and cause a fuck show in their hometowns. HackTown will arm you with the right information on cyber warfare which is exactly what you're wanting to learn. Good job my friend you found this place.

This course is meant for the "average" individual who wants more information on remaining hidden and staying anonymous while online so they can begin their career in cybercrime safely. Anyone can apply the concepts taught here to be a ghost online and hopefully you take away many useful points that you're able to incorporate into your daily OPSec activities.

Relevant cybercriminal information is scattered across the web and going through all that reading, researching, testing, etc. will take years. Literally years. I've put it all together for you in a series of courses surrounding specific hacking skills needed along with online fraud knowledge to help level up your knowledge that to the level of script kiddie king right up to an intermediate hacker proficient cybercriminal.

It's assumed you have general knowledge of hacker techniques, lingo, hacking interests, and terminology that is used in this course. This document has been reviewed however there may be some language and grammatical errors as translation sometimes get misunderstood. If you come across errors (spelling or grammar) or have more information that you think can be added please let me know.

You'll understand how people are caught and how you will be too if you're not careful. You may be a complete noob, novice, or a relatively experienced hacker man but the reality is that everyone starts somewhere and starting out can be the most confusing experience when trying to learn something new. Especially if it's illegal. There's never one way of doing something but hopefully this develops your critical thinking and knowledge surrounding such activities and enhances your skill sets. If you want to be a better black hat hacker it's good to have the academics behind you, professional IT experience, computer security knowledge, and current credentials (CISSP, OSCP, CEH, GIAC, A+, etc.) to greatly improve your skills. Both work hand and hand.

As you progress in your cybercriminal career you'll see why and understand that keeping in the know will help you in your future endeavors.

It's important to remain anonymous, blend in, and be very difficult, if not impossible to track while online. Hackers, crackers, carders and the like are quite good at this as it's vital to their freedom and financial success. Unfortunately for you in the beginning when you're learning to master this trade you're bound to make mistakes and be misguided. In this industry you need to practice in order to perfect, sharpen, and hone your skills. Going to jail or being charged with a criminal offence can and will ruin your career goals and your life as you know it so it's best to research the laws in your country to get a handle on the charges that will be laid against you should you make that "mistake". Don't blindly break laws.

[Click to Read - Student gets arrested for DDoS](#)

[Click to Read - Dark web Vendors arrested](#)

By learning how others have been caught, captured, and arrested can help you avoid the same fate. It's important to follow the news, Twitter, Facebook, or whatever social media you use to follow hackers, IT security consultants, whitehats, and everything in between related to IT cyber security. Follow, listen, read, and observe. The quieter you are the more you'll be able to hear as you'll soon come to realize. Being involved this way will help educate you on how other hackers and cybercriminals are caught, the logistics of major hacks, new malware techniques, and the newest cyber-attacks out there.

Today there are a lot of "security researchers" out there trying to make a name for themselves and they will literally make public all the new exploits, o-day's, code, tools, and everything in between that makes your life a heck of a lot easier. You don't even need to rely on finding your own o-day exploit any longer because some security researcher will release it for free and give it to you! In fact it's quite frustrating finding out someone has revealed a "new" vulnerability that you've been using the whole time that is now patched and over used. However, it's definitely taken some of the leg work out of doing it yourself so there are pros and cons.

Lastly, this course does not include EVERYTHING for you. Honestly how could it? It's expected that you're capable of doing some research on your own as well with the new knowledge you'll gain by reading this. These teachings will show you how to stay and remain hidden, but you cannot be expected to be spoon fed with hand holding along the way. Google and YouTube are your friend when you're stuck on something so any question, problem, or error paste it directly into Google and read through forums, blogs, etc. until you find your answer. If you're not capable of this then please stop now before you hurt yourself. You may think this is a cop out but most, if not all, of your questions can be answered this way and realistically the amount of questions you'll have will be vast so it's best to get efficient in searching and finding your answers on your own.

Being able to effectively search, read, learn, and find your answer is a skill on its own so be prepared to be somewhat self-sufficient when going through these courses. YouTube has a large number of videos that can walk you through your problem, literally, at the basic level. Having trouble installing VMware or VirtualBox? Having trouble getting dnsspoof to work? Google it or use YouTube. Use the internet to your advantage without compromising yourself and begin to become self-sufficient. Most people who are good at hacking, carding, etc. have learned step by step from books, others, whatever means they needed to so treat this knowledge like a University or College course and do some homework and read, read, and read some more. If you have major problems following this course and cannot replicate the teachings then what you're attempting to do and learn is way beyond your capabilities and you should stop what you're doing, accept your fate, and focus on

something easier such as cabinet making, cake baking, or watching the world pass you by.

Alright then comrades, let's get into it shall we!

A Jolly Roger catch-up

If you haven't heard about the "Jolly Rogers Security Thread for Beginners" then now is good time to read everything in it. Please keep in mind some topics and links are outdated but you'll still find some important information in it.

There's no need to implement anything unless you feel the need to do so but for now just read it through casually as it will take you sometime to get through it all. If you don't understand everything you read in it this is OK as we'll get into it more in this course! Once you've read through it we'll build on that knowledge moving forward.

Remember, there's no need to rush because sometimes having too much information can be just as confusing and frustrating as having no information at all. Take your time and read casually friends.

Do not stress but do this first before moving forward.

[Click to Read - Jolly Roger's Security Thread for Beginners](#)
(continue in 2b)

Important!

You're going to find out it doesn't matter what you do as long as you choose to operate one way or the other as recommended in this course. That means you're either securing your laptop running macOS or Windows operating in a Whonix Virtual Machine (VM) or you're booting Tails OS directly from a USB.

The end result is the same when your door gets blasted off its hinges and officers coming barrelling in to arrest you. They will either find your encrypted USB or encrypted Tails OS on USB and in the end your problems will be the same that being is the encryption method you used to encrypt your USB good enough AND is your password strong enough to survive brute force attacks?

For now, we're going to focus on making sure your laptop running Windows or macOS is secure as possible. We'll get into VMs, how to encrypt your HD and USBs, and discuss Whonix VM and Tails OS later on.

Regardless of what your host machine is (Windows, macOS, or Linux) you should be doing everything in a Virtual Machine (VM) and not using your host machine to run Tor directly, browse the dark web, store passwords or anything illegal/questionable, etc. saved directly on your HD. Anything questionable should be saved onto a USB that is encrypted so you limit the amount of digital bread crumbs you'll leave behind on your laptop.

Nothing should ever be saved onto your laptop/computer HD is what you should be aiming for except the applications needed installed and anything that is saved on your HD should be something normal and a rational explanation for it being there. All your diabolical plans, files, and VMs should be saved onto a USB that is encrypted at minimum.

This chapter is designed for people who want to harden and secure their computers running Windows, macOS, or Linux. The items discussed in this chapter are meant to be applied to your computer to ensure that it's secured to the best of your ability and that you're operating safely online.

This may seem easy at first but you'll soon come to learn it's not as easy as it may seem and each person will apply the things learned here differently.

Minimum lame requirements for Computer/Laptop

- Intel or AMD CPU
- Minimum 4GB of RAM
- 60+ GB of hard disk space
- Internet access

"Professional" cybercriminal maniacs have their laptops like:

- Intel or AMD CPU
- 32+ GB of RAM
- 1 TB+ of hard disk space
- Internet access

First off, you should purchase your "work" laptop with cash and nothing else. This way if you do something fucking crazy attracting the attention of the coppers and make a mistake online nothing on that laptop/computer can be traced back to you personally. Understand?

The whole point of this course is to in the end give you plausible deniability to save you.

Keep the laptop/computer you use for hacking, carding, or whatever you're doing away from anything personally related to you at all times. This is important, don't get lazy. This means no checking your Facebook, Twitter, e-mail, or any other personal accounts for any reason while you're using that laptop/computer. Never connect your laptop, computer, phone, or any other personal device to the network your dedicated "work" laptop is connected to either.

Keep it separate!

Secondly, the computer you plan on using for anything illegal should never connect to your home Wi-Fi network or any other network that can be associated to your real identity until you have it setup correctly.

Your work laptop can be any laptop that is capable of running multiple Virtual Machines (VM) when needed which will vary in price from \$400 - \$3000 USD. Purchasing your "work" laptop/computer is up to personal preference so there's no one machine for all as it depends on what you need it for but you'll want something with high RAM (8GB+) if you plan on running multiple VMs. Some people use serious beast machines for their needs from Alienware laptops, gaming PC's, and everything in between but the point is your laptop/computer should suit your needs for what you plan on using it for. You want your laptop somewhat portable so keep that in mind but don't over think this too much as you'll soon find out reading through this course that you actually don't need a powerful machine at all, depending on what you're doing of course.

If you're a Vendor looking to sell your products on some darkweb marketplace or an individual looking to purchase drugs online then you might be interested in purchasing a cheap portable laptop and just booting Tails OS from USB. Everyone is different you see?

For example, I personally use Alienware laptops <17" because I prefer the hardware that they come with for other means like gaming, Photoshop, minor GPU WPA/WPA2/Password cracking, and other programs that require a more expensive robust machine for when I'm not actively "hacking" or causing fucking chaos online. As a hacker, if you're involved with a hack and you're waiting for an email reply from a target or a reverse shell to come back in real time either with Metasploit, Empire, or custom malware (specifically with macOS targets) you'll have some time to kill waiting for that shell to drop. I'd be bored as fuckkk waiting for this to happen

so I'd be gaming on a wicked laptop and using Whonix in a VM connected to my VPS while waiting for that shell to drop. Some god damn employee I'd be targeting wouldn't check their emails throughout the day that frequently so I needed to kill some time and using the Tails OS wasn't satisfying my needs. Being a cyber elite hacker with 9000 shells loaded I wanted multiple VMs at my disposal so I needed a more powerful computer/laptop to do this flawlessly for me as well.

My laptop has nothing to do with hardware specifications needed for committing online cybercrimes or "hacking" per se but mostly for pleasure in my down time waiting for shit to happen. There are times when I'm using a piece of shit netbook and booting the Tails OS from USB to log into a Virtual Private Server (VPS) with SSH over Tor that I purchased based in Romania. I have all my hacking programs installed on that server to use as my "front gun server" then the next day I'm using my gaming laptop to use Kali in a VM so I can hack an art gallery Wi-Fi network in order to compromise their Wi-Fi network and push ransomware to everyone on it.

Everyone is different.

Your computer should suit your needs on what you want to use it for. We're all different and there's no one way of doing things so think things over while reading this chapter before deciding what works for you based on your requirements.

Your "work" computer should strictly be meant for "work" and "business". Period.

[Click to Read - Don't connect to Tor while linked to other accounts](#)

I'm going to discuss multiple things in the next couple of paragraphs and it's important you read through it all before making a decision on how you want to operate when stepping into the shadows of becoming a cybercriminal.

There are (3) ways of operating online anonymously.

- Using Tails OS.
- Using Whonix OS inside VM.
- Using Qubes OS - We won't be discussing anything Qubes related.

If you're starting out in the cybercriminal/hacker world the biggest question you need to ask yourself is how do you want to operate? Do you want to use your computer running Windows, macOS, or Linux and save everything to an encrypted USB? Do you want to use only virtual machines (VM) to conduct your dark web activities? Do you want to boot the Tails OS directly from a USB stick for your shady ass business dealings?

The answer is different depending on what type of user you are (hacker, carder, vendor, buyer, forum lurker, etc.) and what you require from your computer. Using VMs and booting directly from a USB presents different problems and each have their weaknesses which we'll discuss this way you can assess your situation making an informed decision on what best suits your needs.

Never use your host machine (Windows, macOS, or Linux) to connect directly to anything criminally related (running Tor, logging into your vendor account, checking emails, etc.). What that means is if you're using a Windows or macOS computer don't just download the Tor Browser Bundle (TBB) and use the Tor browser directly from your computer to connect to a questionable website that you're a member of (fraud, hacking, drugs, etc.). You can use Windows, macOS, and Linux as your host computer but you should always be using a VM when it comes to hacking or anything wicked (illegal).

If you're hell bent on using Windows or macOS then you should be using Whonix OS inside a VM which we'll discuss later on in Chapter 6 but for now we'll be focusing on hardening your main OS.

For the future hackers and crackers out there once you have purchased your laptop it's important to familiarize yourself with the command line interface (CLI) or Terminal. You do not have to be an expert to use the CLI or Terminal but you should know the basic commands and what they do and when to use them. Having the basics down when using the command line or Terminal is ideal so if you don't know anything about Linux/Unix then now is a good time to learn it if you plan on getting your hacker face on. There are many basic Linux books out there that you can purchase or take an online course. YouTube has plenty of tutorials available for free as well but take the time to learn Linux/Unix and feel somewhat familiar with it. You don't need to install Linux/Unix as your primary OS but you should download VirtualBox onto your computer and install a Linux distro of your choice. We'll go over VMs in Chapter 6 but it's recommended to begin with an easier distro such as Ubuntu so you can learn the basics and get familiar with using the CLI or Terminal.

The goal here is to feel comfortable with the command line and have the basics down. I mean the basics! That means how to navigate through directories, open files, edit text files, and how to run scripts or programs. The basics dudes... Don't mess around with the Graphical User Interface (GUI) so much but instead stick to the CLI and Terminal for learning purposes.

If you're using macOS then use Terminal.app for anything command line related as this is very similar to anything *nix related.

In my opinion everyone should learn Windows Command Line, Powershell, and every *nix CLI related for a good handle on all operating systems but you do you.

Figure out what works for you and use the concepts taught in this course to keep you safe regardless of whatever cybercriminal activities you get yourself into.

Alright let's get into it shall we?

Hardening your OS

The problem with using Windows or macOS is those operating systems, like many others, are constantly sending data back to their servers for analysis, marketing, data collection, and a whole bunch of other shit. This is a problem because if you're on a Wi-Fi network committing some wicked cybercrime and your computer is sending data back to your iCloud account linked to your identity this is trivial for police to track once they're on your tail. Right? Some investigation takes place on XYZ network and they see a connection to Apple servers at XYZ time and date. You're there connected to the internet not realizing your computer is constantly sending data from it which is linked to you and can be traced to where ever your location is.

A connection went from your laptop to an Apple iCloud server, police send a subpoena to Apple for when that iCloud account connects back, and now anywhere you go with that laptop and it makes a connection back to whatever account (iCloud, Outlook, etc.) giving them the ability to track that laptop/you anywhere your going buddies.

This is all fucking bad.

I cannot stress enough that whatever OS you're using at minimum you need to be encrypting the HD, using a VPN, saving everything to an encrypted USB, and using Virtual Machines (VM) to conduct your dark web activities or booting into Tails OS from USB.

Windows Users

Windows users are generally the main targets of hackers and Law Enforcement (LE) as "most" people have Windows installed as their main OS with default settings left on. Windows has a large attack surface which presents many ways for a Windows user to be compromised by malware.

If you're insisting on using Windows as your main OS then you need to encrypt your HD with BitLocker, use encrypted USBs for all your "dark" related files and VMs, with ideally having a VPN installed.

Tips for hardening Windows

- Keep your machine updated and apply all new updates, always.
- Save everything to an encrypted USB and avoid writing to the HD.
- Disable Bluetooth
- Use BitLocker to encrypt your HD.
- Setup a BIOS password and disable booting from USB on startup (unless booting from USB).
- Turn on Windows Firewall.
- Install CCleaner and use it before each shutdown.
- Install a reputable Anti-Virus/Anti-Malware or keep Windows Defender up to date.
- Install GlassWire (<https://glasswire.com>) to control all incoming/outgoing network connections from your laptop.

If you're not a Windows user but want to use it in a VM to test your malware or tactics then download the free 90-day trial from Microsoft. You can install it, disable

the time sync with your host machine, create a snapshot, and use it accordingly.

Download the Windows 10 ISO if you want a valid Win 10 VM for free at:
<https://www.microsoft.com/en-us/software-download/windows10ISO>

macOS Users

The macOS is relatively easy for the average user to harden, secure, and lock down. With the latest macOS update "Big Sur" makes it the securest release and is fairly difficult to compromise with malware.

If you're insisting on using macOS as your main OS then you need to encrypt your HD with FireVault, use encrypted USBs for all your "dark" related files and VMs, with ideally having a VPN installed.

Tips for hardening macOS

- Keep your machine updated and apply all new updates, always.
- Save everything to an encrypted USB and avoid writing to the HD.
- Disable Bluetooth
- Use FireVault to encrypt your HD.
- Install CCleaner and use it before each shutdown.
- Setup a BIOS password and disable booting from USB on start-up (unless booting from USB).
- Turn off all sharing on the computer (System Preferences - Sharing).
- Turn on the Firewall (System Preferences - Security & Privacy - Firewall).
- Install a reputable Anti-Virus/Anti-Malware.
- Purchase and install LittleSnitch (<https://www.obdev.at/products/littlesnitch/index.html>) to control all incoming/outgoing network connections.

In Terminal.app type:

export HISTFILE=/dev/null

This will ensure there's no more bash history for anyone to browse through what you've typed into Terminal in the past.

You want to control everything outgoing/incoming to your machine and the applications listed below is a great place to start in having control of your macOS.

Knock Knock

LuLu (Alternative to LittleSnitch)

Do Not disturb

Block Block

<https://objective-see.com/products.html>

It's best to research those programs to see why they're a great addition to your macOS OPSec but in general:

LuLu/LittleSnitch will give you control of any network activity coming to and leaving from your machine

Knock Knock will let you easily see what's persistently installed (what runs on each boot-up).

Do Not Disturb will give you a notification anytime your laptop lid is opened and can actually take a picture with the webcam to see who's opened your laptop when you're not around.

Block Block will let you know if a program is trying to install persistent items on your machine and give you the option to allow or deny.

We already talked about that it but if you're using Tor on any network causing fucking mayhem and your macOS is making connections to your Apple iCloud account that's probably not a great idea is it? We can prevent this from happening by editing the "/etc/hosts" file on your computer.

By replacing your "/etc/hosts" file with items below in **orange** we will redirect all the domains listed in the "/etc/hosts" file to 127.0.0.1 (localhost). This way no connection is made from your computer to any Apple server. This is the list I've collected over the years and it's updated every time I update the HackTown website to make sure it's current.

You can also do this in Windows by editing the "C:\Windows\System32\Drivers\etc\hosts" file.

WARNING

Replacing your "/etc/hosts" or "C:\Windows\System32\Drivers\etc\hosts" file will prevent your OS from properly updating your computer. It's recommended to visit a random coffee shop and replace the modified hosts file with the backup of the original to update as required when needed. You should always keep your host OS up to date and install the latest security fixes.

Open up Terminal and type:

sudo cp /etc/hosts /etc/hosts-backup

sudo rm /etc/hosts

sudo touch /etc/hosts

sudo vim /etc/hosts

Hit the letter "i" on your keyboard so you can enter text with vim.

Copy the text in **orange** below and paste it into Terminal with vim.

##

Host Database

#

```
# localhost is used to configure the loopback interface
# when the system is booting. Do not change this entry.
##
127.0.0.1 localhost
255.255.255.255 broadcasthost
::1 localhost
```

```
127.0.0.1 init-p01md.apple.com
127.0.0.1 p34-fmfmobile.icloud.com
127.0.0.1 swcdn.apple.com
127.0.0.1 AssetCacheLocatorService.xpc
127.0.0.1 news.apple.com
127.0.0.1 kt-prod.apple.com
127.0.0.1 keyvalueservice.icloud.com
127.0.0.1 13-courier.push.apple.com
127.0.0.1 apple.news
127.0.0.1 pancake.apple.com
127.0.0.1 22-courier.push.apple.com
127.0.0.1 32-courier.push.apple.com
127.0.0.1 36-courier.push.apple.com
127.0.0.1 1-courier.push.apple.com
127.0.0.1 push.apple.com
127.0.0.1 32-courier.push.apple.com
127.0.0.1 4-courier.push.apple.com
127.0.0.1 32-courier.push.apple.com
127.0.0.1 3-courier.push.apple.com
127.0.0.1 42-courier.push.apple.com
127.0.0.1 2-courier.push.apple.com
127.0.0.1 gsp-ssl.ls.apple.com
127.0.0.1 37-courier.push.apple.com
127.0.0.1 updates-http.cdn-apple.com
127.0.0.1 27-courier.push.apple.com
127.0.0.1 valid.apple.com
127.0.0.1 19-courier.push.apple.com
127.0.0.1 9-courier.push.apple.com
127.0.0.1 api-glb-use2b.smoot.apple.com
127.0.0.1 6-courier.push.apple.com
127.0.0.1 14-courier.push.apple.com
127.0.0.1 8-courier.push.apple.com
127.0.0.1 7-courier.push.apple.com
127.0.0.1 48-courier.push.apple.com
127.0.0.1 50-courier.push.apple.com
127.0.0.1 17-courier.push.apple.com
127.0.0.1 11-courier.push.apple.com
127.0.0.1 35-courier.push.apple.com
127.0.0.1 34-courier.push.apple.com
```

127.0.0.1 47-courier.push.apple.com
127.0.0.1 28-courier.push.apple.com
127.0.0.1 43-courier.push.apple.com
127.0.0.1 40-courier.push.apple.com
127.0.0.1 20-courier.push.apple.com
127.0.0.1 21-courier.push.apple.com
127.0.0.1 38-courier.push.apple.com
127.0.0.1 15-courier.push.apple.com
127.0.0.1 23-courier.push.apple.com
127.0.0.1 33-courier.push.apple.com
127.0.0.1 41-courier.push.apple.com
127.0.0.2 32-courier.push.apple.com
127.0.0.1 26-courier.push.apple.com
127.0.0.1 12-courier.push.apple.com
127.0.0.1 30-courier.push.apple.com
127.0.0.1 46-courier.push.apple.com
127.0.0.1 44-courier.push.apple.com
127.0.0.1 29-courier.push.apple.com
127.0.0.1 gsp64-ssl.ls.apple.com
127.0.0.1 18-courier.push.apple.com
127.0.0.1 49-courier.push.apple.com
127.0.0.1 24-courier.push.apple.com
127.0.0.1 5-courier.push.apple.com
127.0.0.1 39-courier.push.apple.com
127.0.0.1 16-courier.push.apple.com
127.0.0.1 10-courier.push.apple.com
127.0.0.1 25-courier.push.apple.com
127.0.0.1 31-courier.push.apple.com
127.0.0.1 init.push.apple.com
127.0.0.1 45-courier.push.apple.com
127.0.0.1 p34-keyvalueservice.icloud.com
127.0.0.1 push.apple.com
127.0.0.1 iadsdk.apple.com
127.0.0.1 p34-availability.icloud.com
127.0.0.1 www.apple.com
127.0.0.1 configuration.ls.apple.com
127.0.0.1 p34-escrowproxy.icloud.com
127.0.0.1 api-glb-use2c.smoot.apple.com
127.0.0.1 api-glb-fra.smoot.apple.com
127.0.0.1 bag.itunes.apple.com
127.0.0.1 captive.apple.com
127.0.0.1 cl2.apple.com
127.0.0.1 setup.icloud.com
127.0.0.1 p36-availability.icloud.com
127.0.0.1 gateway.icloud.com
127.0.0.1 mobile.pipe.aria.microsoft.com

127.0.0.1 g.live.com
127.0.0.1 gsas.apple.com
127.0.0.1 metrics.icloud.com
127.0.0.1 aidc.apple.com
127.0.0.1 safebrowsing.googleapis.com
127.0.0.1 api-glb-nyc.smoot.apple.com
127.0.0.1 lcdn-locator.apple.com
127.0.0.1 gspe35-ssl.ls.apple.com
127.0.0.1 init-kt.apple.com
127.0.0.1 swscan.apple.com
127.0.0.1 init.itunes.apple.com
127.0.0.1 itunes.apple.com
127.0.0.1 push.apple.com
127.0.0.1 mesu.apple.com
127.0.0.1 gspe1-ssl.ls.apple.com
127.0.0.1 api.apple-cloudkit.com
127.0.0.1 init.ess.apple.com
127.0.0.1 static.ess.apple.com
127.0.0.1 api.smoot.apple.com
127.0.0.1 api-glb-ash.smoot.apple.com
127.0.0.1 gateway.icloud.com
127.0.0.1 setup.icloud.com
127.0.0.1 p36-availability.icloud.com
127.0.0.1 configuration.apple.com
127.0.0.1 cds.apple.com
127.0.0.1 help.apple.com
127.0.0.1 gsa.apple.com
127.0.0.1 gs-loc.apple.com
127.0.0.1 p36-fmfmobile.icloud.com
127.0.0.1 cf.iadsdk.apple.com
127.0.0.1 partiality.itunes.apple.com

Hit "ESC" on your keyboard then ":wq" keys on your keyboard and finally "ENTER" to save the file exiting vim.

Linux Users

If you're just starting out with Linux I do not recommend on using it as your host machine simply due to lack of experience so stick to installing it in a VM until you're comfortable with using it.

Tips for hardening Linux

- Keep your machine updated and apply all new updates, always.
- Save everything to an encrypted USB and avoid writing to the HD.

- Disable Bluetooth
- Install a reputable Anti-Virus/Anti-Malware.
- Setup a BIOS password and disable booting from USB on start-up (unless booting from USB).
- Use IP tables, snort, or bro (zeek). (These are lengthy topics and not recommended for the new user so we'll not discuss them).

Adding the Glasswire or LittleSnitch products to your Windows or macOS computer will give you the ability to have full control over your computer and feel confident that every connection coming and going from your machine is initiated by you and you only. Once you have Glasswire or LittleSnitch installed any new outgoing connection can be intercepted and added to the new "/etc/hosts" file to block as you see fit. I recommend installing Glasswire or LittleSnitch first then going to your local coffee shop and connect to the Wi-Fi network to see how many outgoing connections are intercepted and add each of those domains/IP's (besides the required networking protocols of course) to your new "/etc/hosts" file. In time you'll ensure the only outgoing connection from your laptop will be something you initiated. No surprises.

Invest into those programs so you control what leaves and enters your machine. You won't be disappointed with the purchases I can assure you.

Only disable boot from USB if you're NOT booting an OS from USB. This should be a no brainer but fuck you never know.

Lastly, place a sticker over your webcam, should you have one, to ensure that if you do get hacked this won't be used against you. The CIA director did this at one point and you should too.

If you're having problems always Google and research your question as you'll find there are plenty of helpful forums, posts, and more out there that will answer your question(s). It's recommended to keep whatever logins, passwords, or sensitive information encrypted with the encryption of your choice on a USB, in a VM, or an encrypted container on your host machine that's proven to be effective in the current time of this writing. If the Windows (BitLocker), macOS (FireVault), or Linux (LUKS) encryption methods are broken you should expect that to make the

news so don't be too paranoid on thinking their encryption is backdoored because this would make major news should it fall apart.

If police have seized your computer they will have your all your unencrypted and encrypted folders, files, and all your shit. It doesn't matter whether you're using Whonix, Tails, etc. because when the cops show up at your house knocking on your door it all comes down to encryption and whether or not you took the proper steps to keep your ass out of jail. Your only safety net is having everything encrypted and stored properly with the main goal of having plausible deniability along with knowing that the encryption you used will stand up to current digital forensics and brute force attacks.

If they have tracked you to your physical location and are now investigating, questioning, and interrogating you then it's up to your physical security to keep you out of harm's way. If you follow the courses offered here at HackTown you'll know how to be a digital ghost so you won't have to even fucking worry about that kind of shit or you can still flip your shit after each marketplace take down, vendor arrest, etc. Whichever bro.

The harsh reality is you should always be doing your dark web activities or anything illegal through Whonix VM on your computer or booting Tails OS directly from USB. Get out of the mentality of using everything on your host OS as this is not safe for you.

Picture this. You're selling drugs online and you've logged into your vendor account on a compromised darknet marketplace owned by police and a Tor Browser exploit is used against everyone connecting to that marketplace who are logged into their accounts. Right now as you're reading this your laptop is compromised and a network connection went from your laptop to a command and control (C&C) server owned by the police. If that happened then they would know your IP, your location, and they're now closing in on you about to make an arrest. Would you even know that you leaked your location or a connection went from your computer to the police?

If your computer sent data from your laptop to a remote server would you know? How would you? Would you notice anything different while using the Tor Browser on your Windows, macOS, or Linux computer? How about when you're using Tails or any other OS? Think about that for a second. All you're doing is blindly trusting the Tor project developers, Windows, macOS, Linux, Tails OS developers, etc. that everything is all good. You have no god damn idea if it's all good which is like %99.9 of all Tor users in my opinion. Everyone just trusts these programs are secure and blindly uses it for their illegal activities online. Is everyone just crossing their fingers that all this shit is legit and performing illegal activities from their home networks while using their personal emails to register for illegal shit? The answer is "YES", which is fucked. Blind trust is never a good idea.

There are always exploits waiting for you and some you don't even know are possible.

An exploit for Tor Browser v8.5.2 was found being exploited in the wild on June 20, 2019 and an immediate critical patch was updated which resulted in the Tor Browser Bundle (TBB) v8.5.3 being released. Exploits are found all the fucking time and to consider anything Tor, Tails, Windows, macOS, Ubuntu, Whonix, Qubes, etc. to be somehow immune to exploits is fucking retarded. Stop being retarded and plan for everything to betray you :)

[Click to Read - Tor team warns of Tor Browser bug](#)

An exploit was used against the Tails OS in 2020 to catch a fucking piece of garbage.

[Click to Read - Exploit in Tails 2020](#)

The point I want to make is we know 0-day exploits that are used against the tools we use to remain anonymous will be bad and have devastating consequences for us. If you're browsing your favorite dark market looking for some new cocaine to shovel right to your face and an exploit is used against the Tor browser that you're using while logged into your drug vendor/buyer account, guess what? Game over. You just showed them your real location while logged in to your vendor or buyer account. Congratulations.

Really think that over for a second. If you've been compromised and you've leaked your IP revealing your true location you wouldn't have a god damn clue whether it happened or not regardless if you're running Tails, Whonix, Kali, Windows, macOS, or any other OS. The end result is the same. Your IP is leaked compromising you and you should be getting ready for jail any day now. The reality is that most people are trusting the applications they're using won't somehow be vulnerable to exploits and people are crossing their fingers that everything is golden but we know that's stupid since we know exploits are dropped on the daily so why is any application/tool that you're any different?

I just want to let that sit with you.

This is why it's important to have full control over your computer and to ensure every connection coming and going to your laptop is initiated by you, nothing personal has touched that computer, and that your hard drives/USB are all encrypted properly.

In the next course at HackTown (ACT I) is where you'll learn some hacking skills on how to hack the Wi-Fi networks around you. That skill is important to have because if an exploit is used against you and your IP is leaked it sure as shit won't be your actual location or linked to you so you can continue on with your chaotic adventures not worried about it since you're not using your own Wi-Fi network.

Knowing how to hack Wi-Fi networks is important for when you're committing online fraud because you want fresh residential IPs that are not known for fraud or blacklisted, yet ;)

For now, keep reading through this course and complete it. Then, when you're ready you can read and complete ACT I so you're able to incorporate Wi-Fi hacking into your toolkit giving you the ability to use other people's Wi-Fi networks to ensure maximum anonymity while operating online.

MAC addresses and their importance

You should be aware that every network card (your hardware that connects to a Wi-Fi network) in a laptop/computer has a Media Access Control (MAC) address associated to it. MAC addresses are "linked" to the physical network card installed in your laptop when they're manufactured. When you're connected to a Wi-Fi network the router uses something called a Address Resolution Protocol (ARP) which associates an IP address to a MAC address on the network. ARP is like a gateway that takes data going to your IP address (from the internet) through a piece of computer hardware (your network card) to you. They work hand in hand.

In very basic drug addict terms, it means your laptop and the router are connected and know about one another on the network so they can send the right data packets to the right computer. This way the router can ensure the data is being sent to the proper person on the network. Makes sense right?

You don't have to know the technical details exactly, but you should have a general understanding of what a MAC address is. So again, the data sent from your computer to the internet has to be sent from your machine, to your Wi-Fi router, then to the internet, and back again through the same process when receiving data. Not rocket science, right? Your router must know which IP to send the data back to or everyone on your network would receive everyone else's data. It would be a fuck show of packets. This obviously wouldn't work so we need the router to associate a MAC address to an IP and keep track of the clients on the network and where to send their packets so everyone receives the right data. Thanks to ARP and the associated ARP table the router knows which MAC address to deliver the data to and what their IP is.

MAC addresses are "unique" to each network card manufactured and can be identified to the specific make of a network card. Consider them as a fingerprint at a crime scene. Should the MAC address be logged when you're on a network and your laptop seized by the feds they could compare their logs and link the MAC address to your laptop linking you to whatever crazy crime you committed.

Hypothetically, let's say you've done something illegal when you were connected to your local library Wi-Fi network with your laptop and have attracted the attention of law enforcement (LE). Now the police are logging MAC addresses that connect to the local library public Wi-Fi network and looking for a suspect who hacked from that location they could potentially sit on that network looking for the same MAC address until they find it again and then begin to profile the people in the area.

Eventually leading them to you.

Whenever you save a network that you've connected to in your computer or cell phone that device will always be looking for that saved network all the time. Your devices are wirelessly sending certain types of packets looking for that network all the time. So when you're hacking your ass off at the local library your cellphone or computer is looking for "My-Home" Wi-Fi network to automatically connect to when it finds it. Anyone in the area

capturing wireless packets would be able to see that device is looking for that specific network and begin to profile individuals in that area.

Remember, MAC addresses are "unique" so just by connecting to your home network and to another Wi-Fi you've used for illegal or questionable purposes you've created a potential connection to YOU, if indeed they're on to your activities and logging shit this isn't good. You've either unintentionally done this with your laptop or you've brought your cellphone with you and used your laptop to connect to an open network. Ultimately, they could associate the MAC address to the make of your computer and hypothetically could determine where that unit was sold. You should've purchased your "work" computer with cash so I wouldn't worry too much here. Investigations work exactly like this and connecting the dots will eventually point LE in the direction of a suspect. Classic police and detective work usually catches most people.

Example of tactics used by Law Enforcement (LE)

- You connect to your home Wi-Fi network and have saved the network in your device so it will automatically connect when in range thus constantly transmitting probe requests out looking for that network which also includes your MAC address in the probe request frame and the name of the Wi-Fi network it's looking for. Anyone sniffing wireless traffic will be able to see this.
- You connect to the library Wi-Fi network without changing your laptop MAC address.
- You launch a hack and try to take over the world. Obviously.
- Police are eventually notified, if what you've done has warranted their attention, they trace the IP back that did the hack back to library public Wi-Fi network and setup a sting/logging investigation.
- You come back to library public Wi-Fi and launch another hack.
- Police now have MAC address of a laptop that connected to the network that launched the hack and begin to connect the dots which would be happening from their end.
- You eventually either return or connect to your Wi-Fi network in close proximity.
- Police see that MAC address sending probe request frames out looking for your home Wi-Fi network and now have a connection/location to who/where you are.
- Of course this all depends on their budget and whether or not you're a target worth their time. In a nut shell if they invest some time in looking for you it's a matter of time until jail if you did not take the proper actions to conceal yourself.

I'd say the majority of people out there know that spoofing their MAC address is a key step in preventing from being tracked while connected to Wi-Fi network you're connected to. I don't think this is news to anyone, however another important tracking method used against you is the hostname of your computer OR your computer name. Your computer name is what you named your laptop such as Funshine-PC, HackTown MacBook, Funshine.local, etc. The hostname can be traceable just as a MAC address if everything is being logged by authorities when on the network. Having random MAC addresses always appearing with the same hostname or computer name on the network is pretty obvious it's the same

individual. All those tracking values should be changed before connecting to any network. Depending on which OS you are using will dictate which program you use and how you do it.

If you're currently connected to a network where you can access the Wi-Fi router login page do so now and login into it. Find out where you're able to see what clients are connected to the network and you should be able to view how many clients are connected to the Wi-Fi network along with what their MAC address and computer name of each device connected to the network. If you have don't know how to access your Wi-Fi router login page then now is a good time to Google "How to access my Wi-Fi router login page".

When I was younger I was spoofing my MAC address for years but didn't realize how ineffective this was until I had an issue on a corporate network that taught me this. There are other network tracking techniques that are used that look for similar computer names and hostnames. You can be linked to your device just as easily with a hostname as well with a MAC. What I want you to understand is how you can be tracked on a network with other items besides your MAC address. Using your MAC address and computer name/hostname against you linking you to other Wi-Fi networks you connected to could help pin-point your computer if you've been tracked to a location from a previous mistake. All bad. Making connections, connections, and more connections...

Note: macOS hostnames usually go by hostname.local by default.

A perfect example to see this is to load up your Kali VM, open Terminal, and type "hostname" to be displayed the hostname of your Kali VM. You'll notice your hostname is "kali". Not really hiding much there are you?.

In the following examples assume the following:

MAC Address	Computer Name	Hostname
A1:B1:C1:D1:E1:F1	Viktor-pc	Viktor.local
A2:B2:C2:D2:E2:F2	Viktor-pc	Viktor.local
A3:B3:C3:D3:E3:F3	Viktor-pc	Viktor.local

Example 1 - Spoofing your MAC

MAC Address	Computer name	Hostname
00:11:22:33:44:55	Viktor-pc	Viktor.local
11:22:11:33:44:11	Viktor-pc	Viktor.local
22:11:22:33:11:44	Viktor-pc	Viktor.local

As you can see just by spoofing your MAC address doesn't really hide who you are too well. Viktor-pc/Viktor.local seems to be the one doing malicious activity on the network but yet their MAC address is different each time...hmm...right? You can see that just because

you're changing your MAC address doesn't mean you're covering up all your tracks.

Example 2 - Spoofing your MAC and changing computer name

MAC Address	Computer name	Hostname
00:11:22:33:44:55	Alexei-pc	Alexei.local
11:22:11:33:44:11	Anna-pc	Anna.local
22:11:22:33:11:44	Dina-pc	Dina.local

I highly suggest changing all values before connecting to any network and on every shutdown of your laptop/computer! This should be done on your **host** machine and whatever VM you have connecting to the network.

You want to get in the habit of spoofing your MAC address, computer name, and hostname of your laptop before connecting to any network. It's best to confirm this yourself if this is your first time spoofing any of these items to ensure that the commands you're typing actually do what they're intended to do.

Spoofing your MAC address

VMware and other Virtualization software can change it before starting up the machine under:

Network Adaptor -> Advanced Settings.

This should be done BEFORE connecting to any networks

Windows

Download and install TMAC. The GUI is pretty self-explanatory

<http://www.technitium.com/tmac>

Use "ipconfig" in the command line to determine your network card needed to change and confirm it has been changed after using the program.

macOS

Download spoof-mac from:

<https://github.com/feross/SpoofMAC>

To spoof your MAC address in Terminal.app type:

sudo spoof-mac randomize eno

eno is the example used and may be different for you. In most cases it will be "eno" or "en1".(use ifconfig to determine your wireless interface)

Linux

sudo apt-get update && sudo apt-get install macchanger -y

Command to use:

sudo macchanger -r wlan0

wlan0 is the network card interface example used and may be different for you.

Kali

sudo macchanger -r wlan0

wlan0 is the network card interface example used and may be different for you.

Spoofing your hostname/computer

This should be done BEFORE connecting to any networks

Windows 7

Click the start button

Right clicking Computer and click Properties

Computer Name tab, click change

Under Computer Name enter the new name

Windows 10

Click on the search bar bottom left of screen

Search for "Control Panel" and open it

Click on "System and Security"

Click on "System"

Click on "Change Settings" under "Computer name, domain, and workgroup settings"

Click on "Change"

Then change your computer name to whatever

macOS

System Preferences – Sharing – Change Computer Name

Change your System Preferences first before using the hostname command below as sometimes it will not set. In the example below I spoof my hostname to "TestName".

In Terminal.app

sudo hostname TestName

Linux

Open Terminal and type "hostname" to see your hostname. In the example below I spoof my hostname to "TestName".

In Terminal:

sudo hostname TestName

Kali

Open terminal and type "hostname" to see your hostname

Not changing the default "kali" hostname will be a problem if there's any Wi-Fi cyber security in place.

In the example below I spoof my hostname to "TestName".

In Terminal type:

sudo hostname TestName

If you've followed these steps it's now considered reasonably "safe" to connect to a Wi-Fi network and feel confident that if there's any logging happening you're always a random connection to the Wi-Fi network each time. Be a ghost.

You should try the above commands and spoof your MAC and computer/host name now. Always remember to spoof your MAC, computer name, and hostname before connecting to any network! It should become common practice to do this every time you start your machine before connecting to a network and before you shut down your machine. Ideally have it scripted, cronjob, and automated.

Encryption

The encryption programs discussed in this chapter are required for encrypting your HD, USB, files and folders on your HD, etc. which currently are considered safe and secure. Obviously, as technology advances these programs and encryption methods may be crackable in the future but as of today's writing of this course they can be considered secure.

[Click to learn how to encrypt containers in Windows - BitLocker](#)

[Click to learn how to encrypt containers in macOS - AES 256](#)

Useful encryption programs to encrypt your folders and USBs with:

<https://www.veracrypt.fr/code/VeraCrypt>

OR

<https://www.truecrypt71a.com>

Default encryption that comes with OS to encrypt your HD with:

FireVault (macOS)

BitLocker (Windows)

LUKS (Ubuntu, *nix, etc.)

Now before you fly off the handle about being recommended Truecrypt 7.1a, FireVault, BitLocker, etc. as some people say closed source encryption cannot be trusted, is compromised, backdoored, not secure, etc. the reality is that none of this is proven to date. You could say that any closed source application can be backdoored and the FBI, NSA, LE, Mi5, Ministry of Intelligence, Federal Intelligence Service, CSIS, ASIS, FSB, and other agencies that have the keys to decrypt everything but the reality is they're not going to waste that ace in their pocket by revealing to the world they caught little old you and that they've broken XYZ encryption. If they have somehow broken or backdoored today's current encryption standards they'll be focusing on actual legitimate state sponsored attackers and bigger fish before letting everyone know that they've broken XYZ encryption and they caught a little fish selling meth online. If they do reveal they've compromised XYZ encryption just to bust you because you're that big of fish well then shit man I think you're fucked. Maybe...

It's important to note that cryptography analysts and cryptography experts would be alerting the public by posting on FB, Twitter, and going to the media if XYZ encryption is broken or backdoored because it sure as fuck won't be you who discovers this. It's in your best interest to be following some sort of social media keeping current on hacker news, IT security, Tor updates, etc. which will alert you of when and how such encryption has been broken.

[Here are some places to bookmark and visit from time to time:](#)

<http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion>

<http://darkfaillnknf4vf.onion>

You're not a cryptography expert and probably will never be one so stay informed as best you can and use the current recommended encryption programs until quantum computing fucks everything up. Keep yourself updated on court cases, arrests, other cases that involve encryption, and watch the news. Don't just implement shit and 5 years down the road be surprised that XYZ encryption is no longer valid. Pay attention because our current encryption standards will one day be broken.

You should be encrypting your hard drive with full disk encryption (BitLocker, FireVault, LUKS) and use a password of at least 15+ characters with special characters which can be remembered easily. Again, choose the encryption that's known at the current time to be effective.

As you'll come to see when you read about the Silk Road creator and AlphaBay admin arrests is that whatever setup you choose to implement whether that's using VMs or booting directly from a USB you want to ensure nothing on your "work" laptop can be associated to your real identity in any way possible. Encrypt your USBs, folders, and encrypt your HD. If you do all of that then you should be fine (unless they've cracked the encryption standards of BitLocker, FireVault, LUKS, Veracrypt, etc. or they grabbed you with your laptop open and unencrypted). If they've cracked those encryptions then yes you're fucked if you've been arrested as is the whole internet really. If this is the case then whatever encryption is broken should make the news headlines as it'll affect everyone globally. Pay attention!

But let's say you fucked up somehow and they do have your laptop. If you've heard of Silk Road then you should be aware it's no longer operational and the administrator has been jailed for life. He made an OPsec error and left his email where he shouldn't have and was captured in a San Francisco Library logged in to Silk Road as the admin among other things. All bad.

This goes the same for the AlphaBay administrator who was caught by Thai police and subsequently killed himself in a Thailand prison before they could extradite him to the US to face charges.

In both cases there was a distraction to get their attention to obtain their laptop powered on, unlocked, and unencrypted. This was key for the police investigation. So if you're a high level Vendor or whatever and they get your laptop when it's open, even though you've followed everything in this course blah blah blah, you're still fucked. Best case scenario is you want your door kicked in when your laptop is off and everything encrypted. If you get grabbed when your laptop is open you should put %110 in getting that laptop locked or turned off because you're fighting for your life here, literally, so treat anything out of the norm as suspicious when sitting at the coffee shop, work, library, etc. and pay attention to your surroundings when doing your thing. But honestly these cops are fucking clever. As long as you're not using your home network or somehow crossed online identities leading them back to you it's very difficult to track you especially if you throw in the items you'll learn in this course you're pretty much impossible to track. But it all doesn't matter if they somehow have caught you with your laptop open and everything unencrypted.

Do you know about Silk Road? Do you really know the story? Do you know about Alphabay? Even if you think you do just read the articles below and relive the drama.

[Click to Read - The untold story of Silk road Act II \(search document for "halfway" and read from there until the next image in the document\)](#)

If you want, you can read part 1 and all of part 2. It's an excellent insight into the arrest of the Silk Road administrator.

[Click to Read - The untold story of Silk road Act I](#)

[Click to Read - The arrest of AlphaBay admin](#)

You read it? Damn right? That's some fucked up shit.

What we can take away from this is we know that by having our laptops powered on, unlocked, and unencrypted when the police nab you then you're fucked. Were the admins of Silk Road and AlphaBay idiots? No! They made a mistake and crossed identities and left a digital trail. If it wasn't for that who knows how long their tyranny could've lasted for. We want to learn from this.

Let's say they do get your laptop, hopefully locked and encrypted or you're done son, say nothing and request a lawyer. They will have circumstantial evidence but will need that solid key piece to actually link it to you! If they have enough evidence against you why in the world would they be wanting the information on your laptop. This is what they will need, and this is what you need to keep clean and secure.

Just like O.J Simpson was thought to be guilty, everyone knew he was, but all the evidence was circumstantial thus he was acquitted. This is basically your goal when law enforcement (LE) has nabbed you, if they nab you. Encrypting sensitive details will keep LE eyes from finding your logins, forum IDs, e-mails, aliases, BTC addresses, etc. which of course will break the connection between you and who they're looking for.

Depending on where you live it may be a crime not to give up your passwords to LE when being investigated for a criminal offence. You should look up what "potential" crimes you will be charged with what you're trying to accomplish or doing right now and then compare the two and see which the lesser crime is to take.

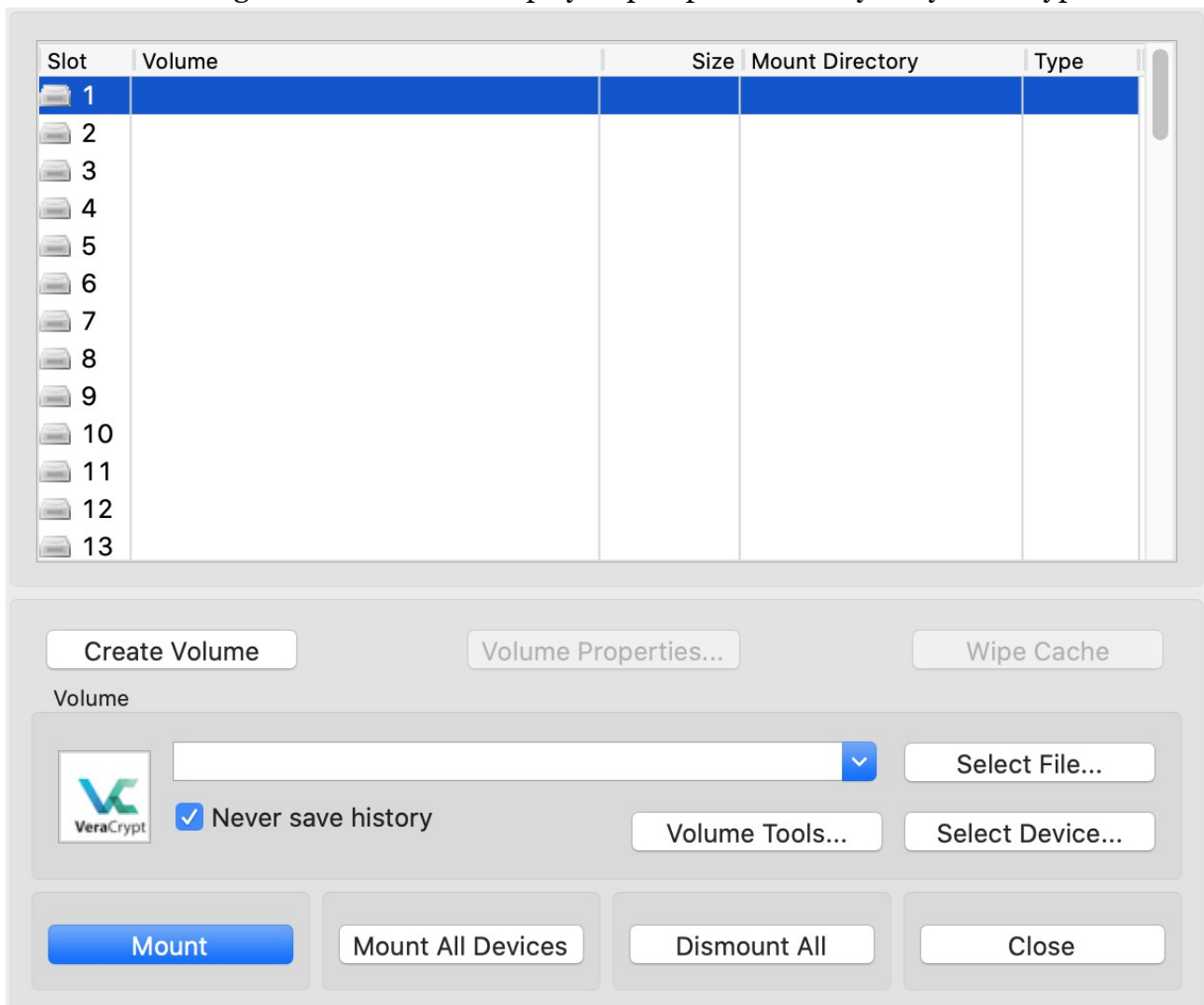
Encrypting your HD, USB, and everything is an important step in securing your laptop so don't overlook it!

VeraCrypt

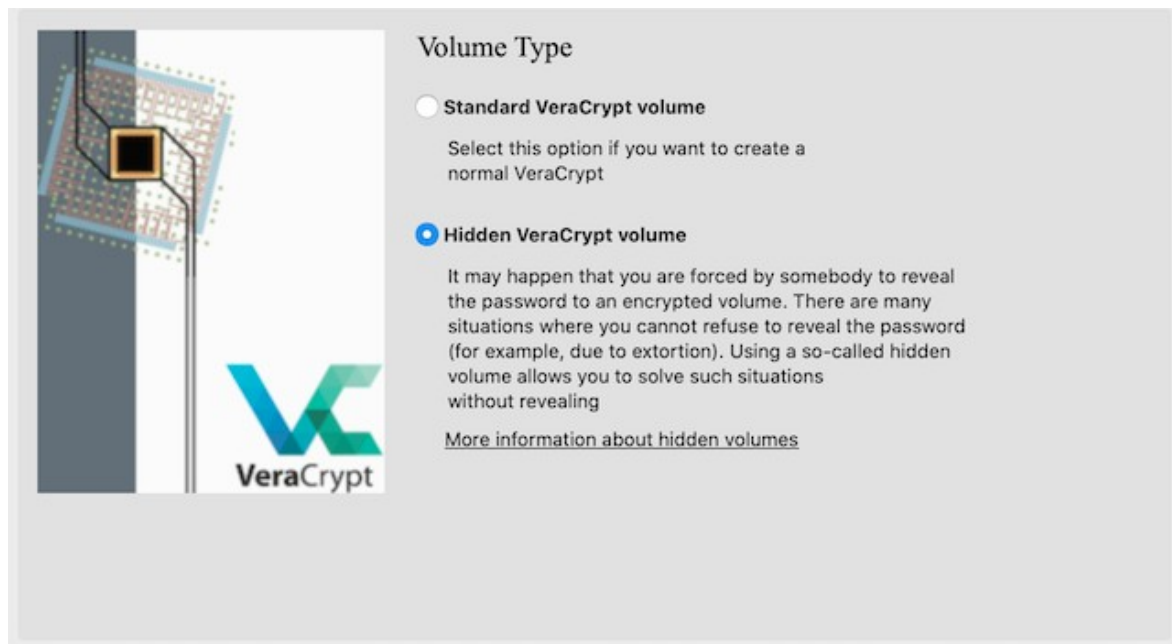
<https://veracrypt.fr>

VeraCrypt is very easy to use and can be used to encrypt any files, folders, portions of your HD, and your USBs.

Once you've downloaded VeraCrypt launch the program and click "Create Volume" and then follow through the instructions step by step as presented to you by VeraCrypt.



Once you've clicked on "Create Volume" you'll have an option to create a "Standard VeraCrypt volume" or a "Hidden VeraCrypt volume". After researching into the Hidden Veracrypt volume it's advisable to create this type of volume when encrypting your HD or any USD/micro SD.



A hidden volume is an encrypted container that is stored within another encrypted container. When you create a VeraCrypt container the entire thing is filled with random data to its capacity which will appear to be only one encrypted data container where in fact you're able to decrypt the first container and store some fake ass files in there in case you'll be forced to supply your password and have your hidden container still encrypted with your devious files. The good news is your hidden encrypted will require a different password to access it so if you're forced to reveal your password for the original container they would see bullshit files and assume that's all there is unless you spill the beans.

It's best to try VeraCrypt out first and encrypt a USB to ensure everything is functioning to your liking before committing to keeping everything on a USB. You want to feel comfortable encrypting and decrypting before putting all your hard earned BTC on a USB only to fuck it all up and corrupt the data.

If you want more information on VeraCrypt Hidden volumes then click on "More information about hidden volumes" when setting your shit up with VeraCrypt. Also, check into the "Security Requirements" as well along with "Precautions Pertaining to Hidden Volumes".

When you come to the option of which Encryption Algorithm to use it's recommended to select "AES" with "SHA-512" or "Whirlpool". The choice of encryption algorithm does not affect securing your data. AES-256 encryption will be exactly as secure as Serpent(AES) or Serpent(Twofish(AES)) but considering AES is the only hardware-accelerated encryption algorithm in all reasonably modern processors choosing any encryption algorithm other than AES-256 will unnecessarily slow down your reading and writing speeds without providing any additional security benefit.



You can read up more VeraCrypt and the encryption algorithms below.

[Click to Read - Comprehensive guide on securing systems](#)

[Click to Read - Breaking VeraCrypt containers](#)

Important!

Before you go on implementing anything learned in this chapter it's best to read through it entirely first and get a feel for the material.

It's most important to read the final paragraphs in this chapter to have an understanding of which method you want to implement into your daily setup as there are weaknesses to using Whonix in a VM as well as booting Tails from a USB.

Virtual Machines (VM)

Virtual machines are an important part of any cybercriminal or hackers toolbox and it's better to do anything illegal/questionable inside of a VM which is much more safer for you.

By using a VM you isolate that operating system (OS) inside of a virtualized environment keeping everything away from your host OS and saved within the VM. If an exploit is used against the Tor Browser and you're using the Tor Browser directly from your host OS this wouldn't be good for you. It would only take (1) exploit for that application exposing your IP bringing down your whole empire. Whereas, if an exploit is used against the Tor Browser within the Whonix VM everything is isolated to that VM and not coming from your host OS which makes it much more difficult to be exploited.

If you use a VM then in order for you to be compromised or leak your IP an exploit would be needed for Whonix, Kali, Tor Browser, etc. **AND** an exploit would be required for VMWare or VirtualBox to get onto your host machine. However, since you should have installed GlassWire or LittleSnitch you're now able to block an unknown outgoing connection from an unknown process, or known process, stopping that unknown connection from getting out.

Look at all that shit that needs to take place in order for you to be compromised which would require multiple 0-day exploits. Do you know how much time and money it would take to develop all those exploits?! Do you think that you're a big enough target that they're going to reveal they have all these exploits just to capture you?! Police only reveal that they used a 0-day exploit to capture someone because those criminals are a much bigger fucking fish than you're drug dealing, hacking, frauding, or carding crimes.

They're going after the true evil mother fuckers out there, not you.

When you're done with this course you'll realize people are caught by making silly mistakes such as linking a personal email to your operations and most are captured with their laptop open, running, and unencrypted. It's all about the police finding your geographical location which is what we're going to prevent from happening.

Before you understand how to run any operating system in a virtualized environment you're going to need to download and install VirtualBox.

Recommendation:

Read through this chapter fully before trying to follow along when setting up Whonix or

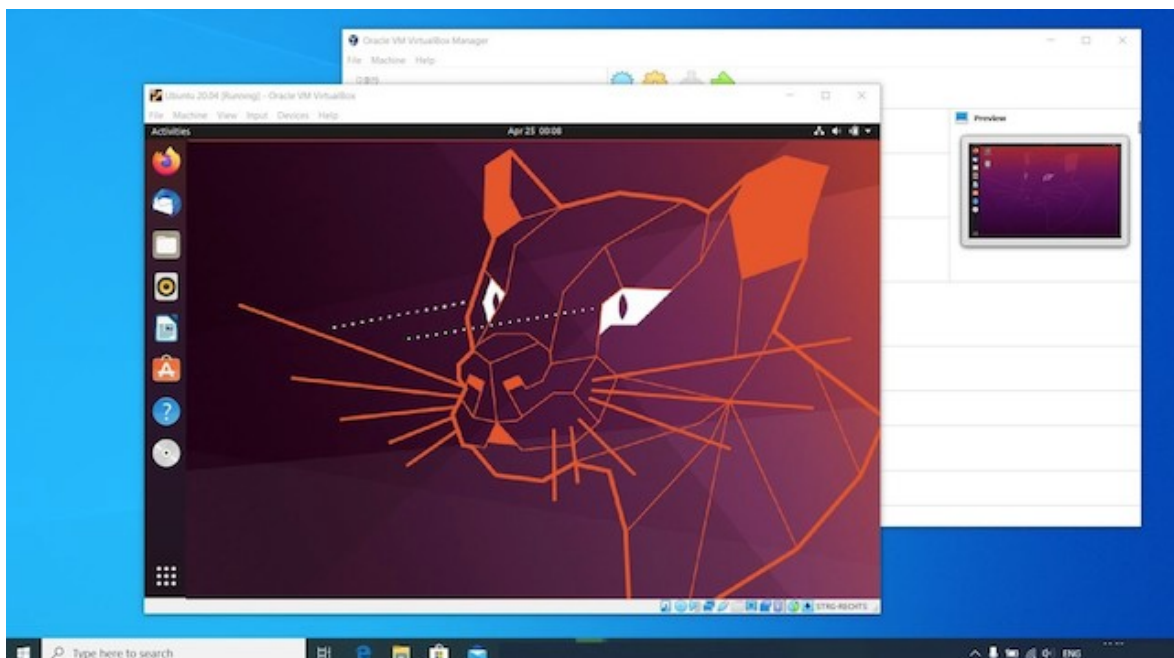
Tails. This way you can see what has to be done and get a feel for it all before implementing any of it. It's best to remember the HackTown URL and plug that in to your Whonix or Tails Tor Browser to follow along when you bootup those operating systems.

VirtualBox

VirtualBox is a free application that can run on Windows, macOS, and Linux based operating systems. With VirtualBox you're able to create and manage other guest virtual machines (VM) running Windows, macOS, or Linux on your main computer in a sperate window.

In the screenshot below I'm running Ubuntu in a VM on my Windows 10 computer.

As you can see I can access Ubuntu and Windows 10 with ease at the same time.



For some VMs you have an option to install the "VirtualBox Extension Pack" which improves performance and allows for more functionality and it's recommended you install it.

It's very easy to get up and running so don't think this is difficult.

Download and install VirtualBox from:

<https://www.virtualbox.org>

Once you've installed VirtualBox it's recommended to install the "VirtualBox Extension Pack" which you can download from:

<https://www.virtualbox.org/wiki/Downloads>

Each VM can be started, paused, and stopped independently within its own VM without affecting your host OS. Your host OS and the guest VM can communicate with each other through a number of mechanisms including a shared common clipboard to copy things from your host OS to your guest VM with ease, shared folder for easy sharing of files between host OS and VM, and a virtualized network so your VMs can have internet connectivity.

Now that you have VirtualBox installed let's discuss the first way of operating online anonymously which is using your main computer to run Whonix inside a VM.

Whonix VM

<https://www.whonix.org>

"Whonix is a desktop operating system designed for advanced security and privacy. Whonix mitigates the threat of common attack vectors while maintaining usability. Online anonymity is realized via fail-safe, automatic, and desktop-wide use of the Tor network. A heavily reconfigured Debian base is run inside multiple virtual machines, providing a substantial layer of protection from malware and IP address leaks. Commonly used applications are pre-installed and safely pre-configured for immediate use. The user is not jeopardized by installing additional applications or personalizing the desktop. Whonix is under active development and is the only operating system designed to be run inside a VM and paired with Tor."

Whonix routes everything through Tor (like Tails) using a Whonix-Gateway VM and a Whonix-Workstation VM to do so. All data is transferred only from the Whonix-Workstation to the Whonix-Gateway and routed all through Tor.

I highly recommend once you've installed the Whonix VMs to then move them onto an encrypted USB and launch them from USB moving forward.

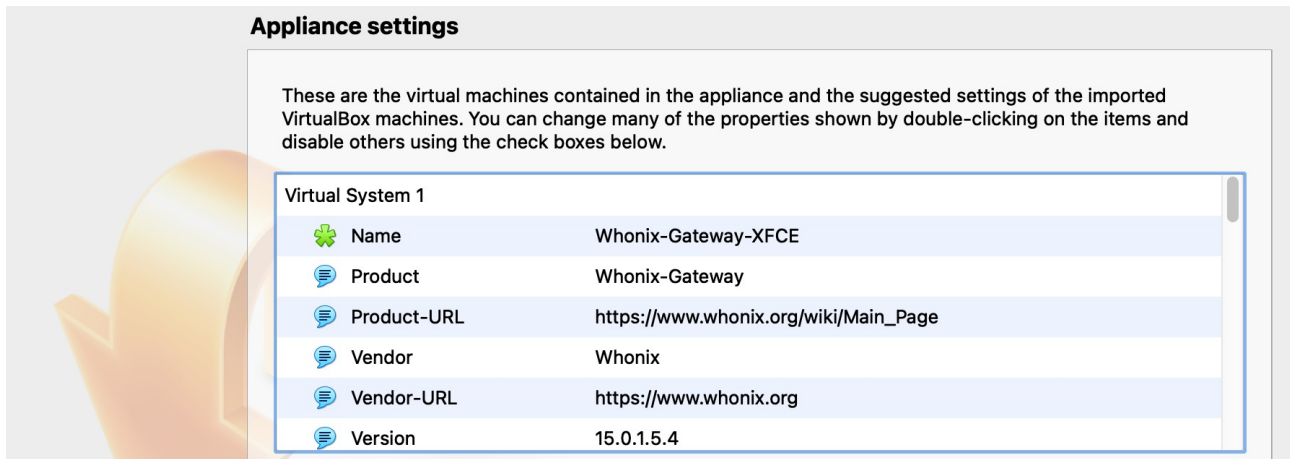
Whonix is very easy to setup!

Head over to <https://www.whonix.org/wiki/VirtualBox/XFCE> and click on the "FREE DOWNLOAD" button to download the VirtualBox .ova file (I recommend using VirtualBox and not VMWare but whatever works for you).

The screenshot shows the Whonix website interface. At the top is a navigation bar with links: HOME, DOWNLOAD, DOCS, FAQ, HELP, CONTRIBUTE, NEWS. A search bar is on the right. Below the navigation bar is a red banner with a heart icon and the text "Please Donate!". The main heading is "Whonix™ for VirtualBox with XFCE". Below this, there are two main steps:

- 1. Download Whonix™ XFCE for Windows, MacOS and Linux FREE**
A green button labeled "FREE DOWNLOAD" is visible. To the right is a small video player showing the Whonix desktop environment. A "[Expand]" link is next to the video player.
- 2. Install VirtualBox**
Text: "Recommended VirtualBox version: 6.1.16".
List of instructions:
 - Windows, Mac: Download VirtualBox [archived] and install.
 - Linux: please press expand on the right side.A "[Expand]" link is at the bottom right of this section.

Once you've downloaded the Whonix OS double click the Whonix-XFCE-15.0.1.5.4.ova file (or whatever the filename is at the time you download it) and it will automatically load it into VirtualBox for you. Ignore all the details and click on "Import" and click on "Agree" twice when prompted. This might take a few minutes importing Whonix OS into VirtualBox.



Whonix functions as a Workstation where you do all your activities and a Gateway which acts a medium between your Whonix-Workstation and Tor.

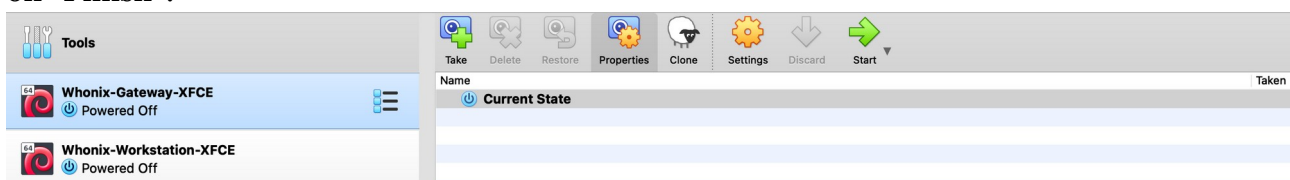
There will be (2) Whonix OS's to select from after you've imported the .ova file but you always want to launch the Whonix-Gateway XFCE VM first, wait until that boots up and is complete, and then launch the Whonix-Workstation XFCE VM after.

All your activities will be done through the Whonix-Workstation VM and nothing is done in the Whonix-Gateway VM. The only time you'll be doing anything in the Whonix-Gateway VM is updating if prompted to do so.

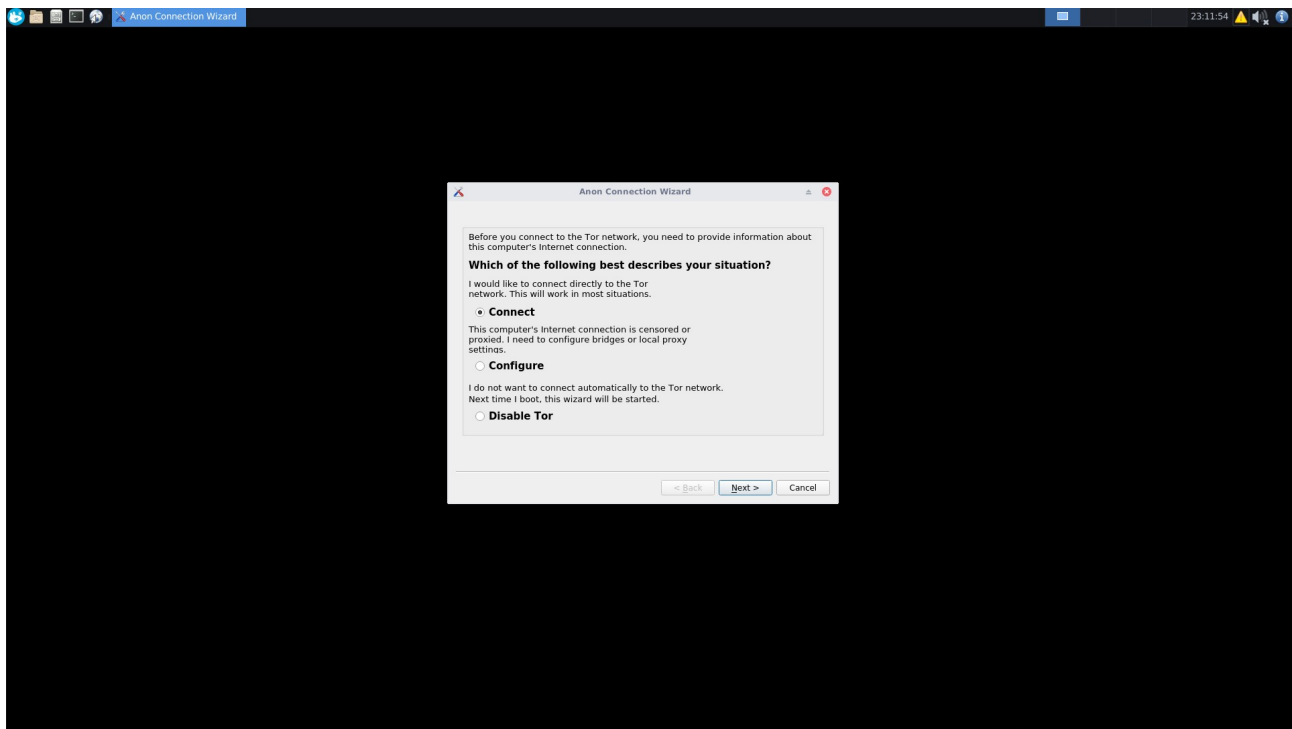
Ok let's start Whonix up.

The default password for Whonix is "changeme"

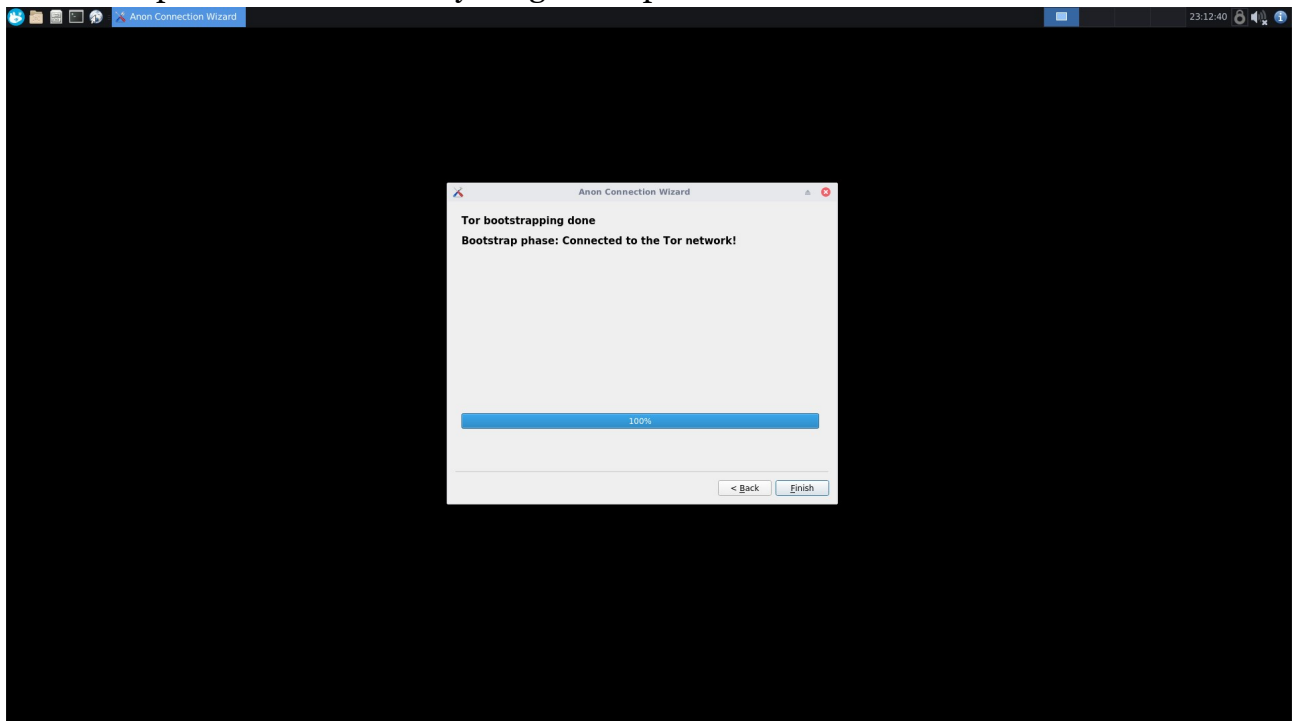
Select the Whonix-Gatway-XFCE and click on "Start". Don't hit any keys and let it boot up automatically then click on "Understood" clicking on "next" through the prompts then click on "Finish".



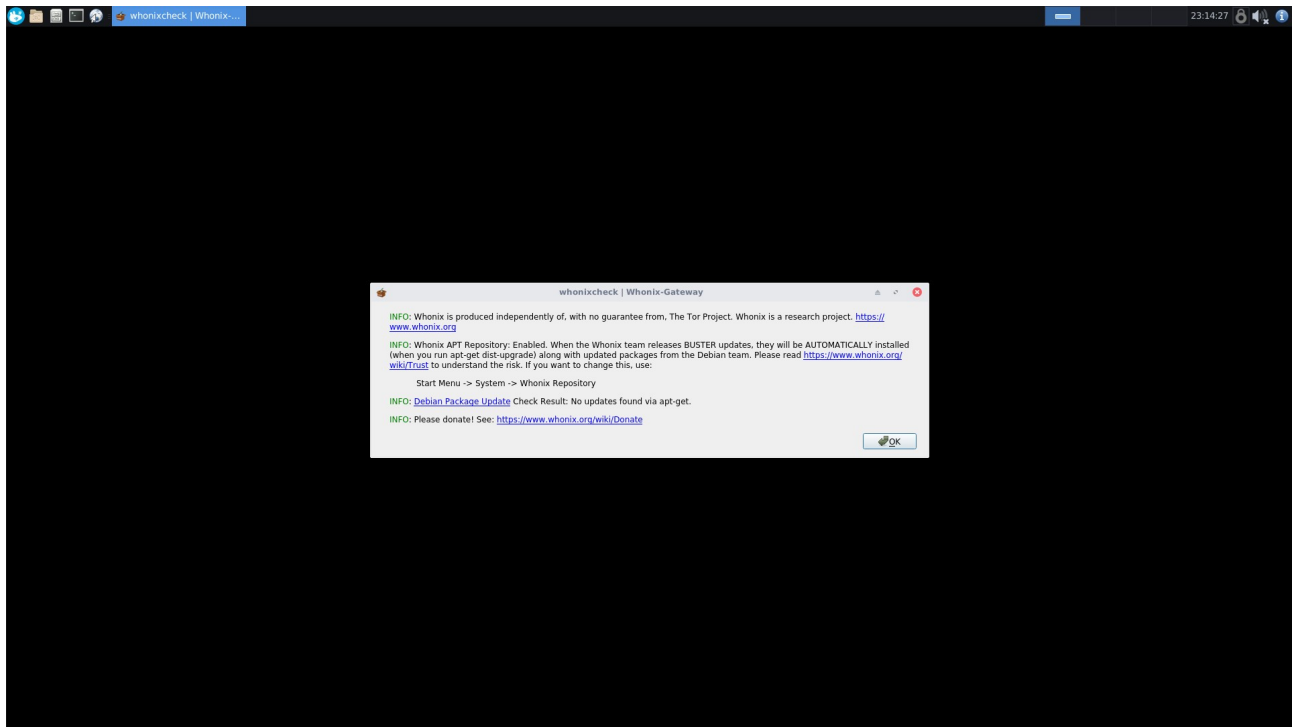
Select "Connect" and click "Next" and then "Next" again. This will setup Tor and ensure everything is routed through Tor from the Workstation to the Gateway.



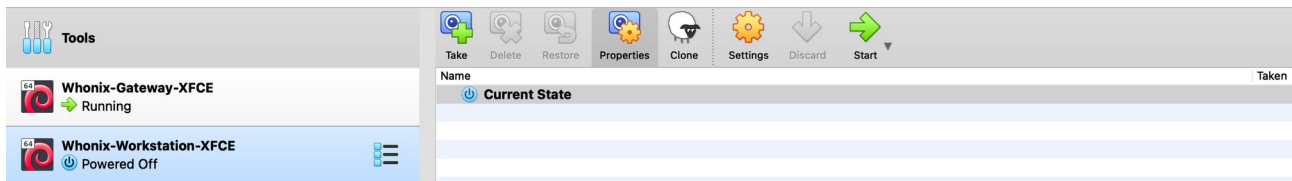
Once it reaches %100 and is completed click "Finish" then let it run through it's Tor testing and auto updates to ensure everything is setup.



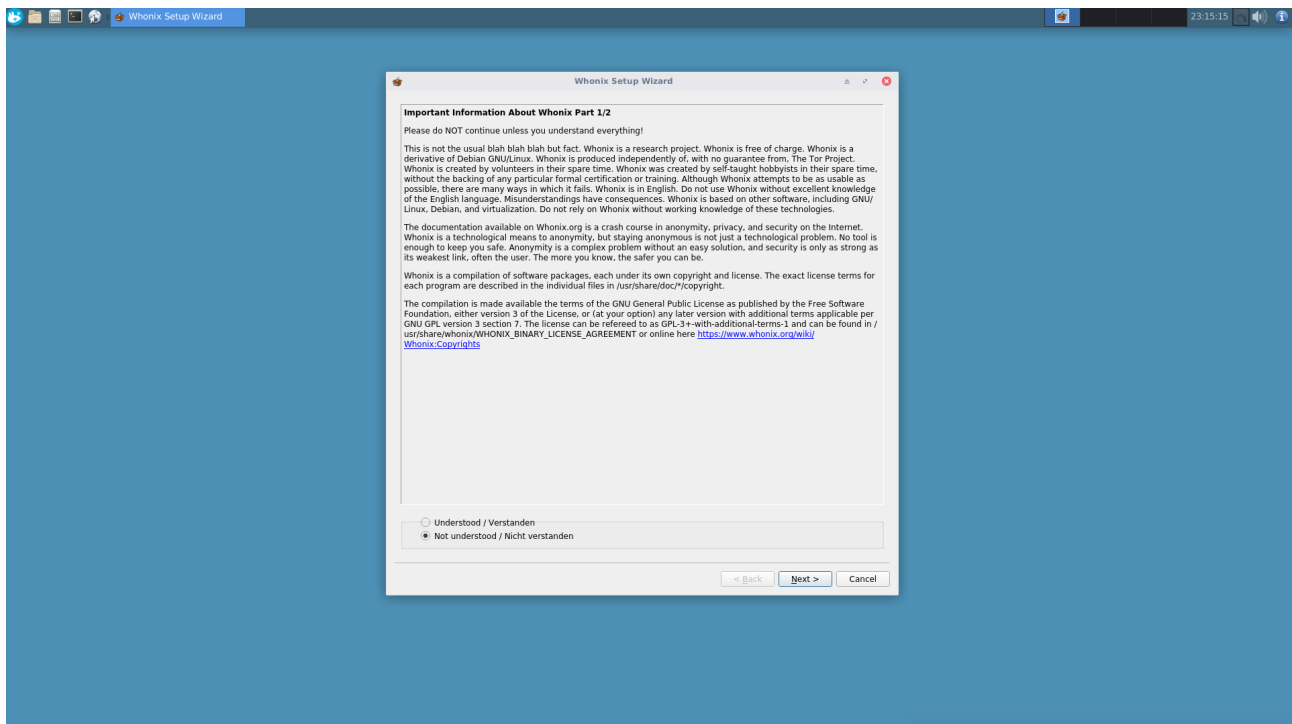
This might take a few minutes and when it's complete it should popup a Window as seen in the screenshot below. Click "OK".



Minimize the Whonix-Gateway VM and leave it running in the background. Now go back to VirtualBox and Start the Whonix-Workstation-XFCE VM.



Don't hit any keys and let it boot up automatically then click on "Understood" clicking on "next" through the prompts then click on "Finish".

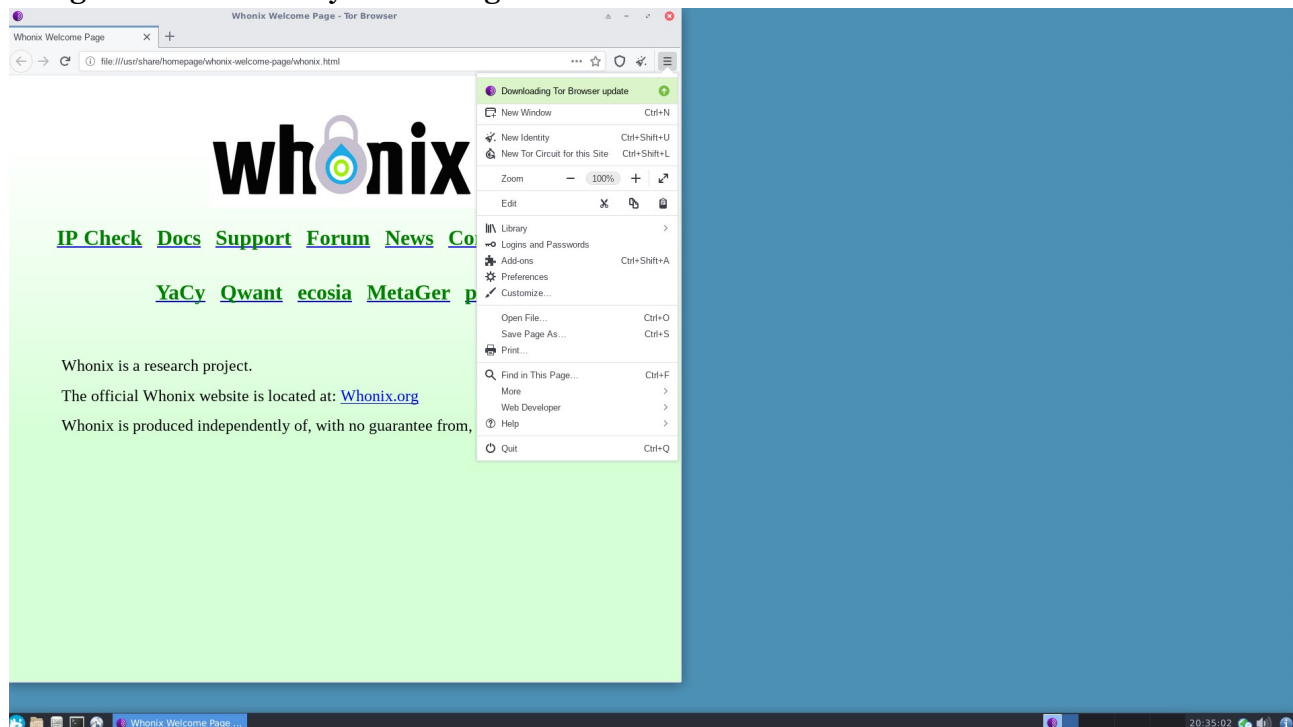


It will automatically setup everything for you just like it did when you ran the Whonix-Gateway VM.

Once it's done setting itself up click on the 5th icon from the right in the top left hand corner of your Whonix-Workstation Desktop to launch the "Web Browser". It's good to run that first as it might need to download and install the latest Tor Browser updates.



You might see that an update is available for the Tor Browser which is no different than using the Tor Browser you're using now.



After that you're good to go with Whonix-Workstation setup to ensure everything you're doing is routed through to the Whonix-Gateway and routed through Tor. Think about the exploits needed to compromise you and expose you with this setup! This is the safest method when it comes to anything dark web related if you insist on using Windows or macOS as your host OS on your computer.

Doing all of your dark web dealings in a Whonix VM that is saved on an encrypted USB while securing your host with everything else discussed in this course is very robust. You should feel very comfortable that your OPsec is on point if you decide to operate with this method including securing and hardening your macOS or Windows main computer.

I won't go into a full tutorial on Whonix because it's important you try it out for yourself and get a feel for the operating system. I suggest you familiarize yourself with it before fully committing to it so create PGP test keys, emails, wallets, etc. before committing to a full dark web handle to see how it functions and re-install it when you're ready to switch over.

If you plan on operating with Whonix

- Make sure your host machine is secured and locked the fuck down.
- Store all your files and VMs on an encrypted USB. Avoid writing to HD.

- Once you've installed your VMs move them to your encrypted USB. Launch them from there.
- Use a VPN on your host OS.
- Use strong passphrases when setting up passwords for everything.
- Ensure you backup important files frequently (PGP keys, passwords, etc.).

The second way of operating is by using a USB to boot directly from into Tails OS which runs only in memory and nothing touches your Hard Drive (HD).

Tails OS

Download the USB image from:

<https://tails.boum.org/install/download/index.en.html>

Click to Read - What is Tails?

Tails must be installed onto a USB that you plug into your computer to boot up into memory with nothing writing to your HD. If you install Tails in a VM then you're not given the option to setup persistence which means you can't save anything after each reboot which is useless. Installing Tails onto a USB is a must so you can install a persistence folder on the USB to keep your bookmarks, passwords, PGP keys, email accounts, etc. saved after each reboot.

Setting up an encrypted persistence folder in Tails is required to operate online properly.

You will need a 8GB USB minimum to install and use Tails properly. I recommend getting a USB with a very high data transfer rate 150 Mbps+ so Tails runs as fast as possible. Since everything is in memory and booting from your USB you don't need a good computer to run Tails.

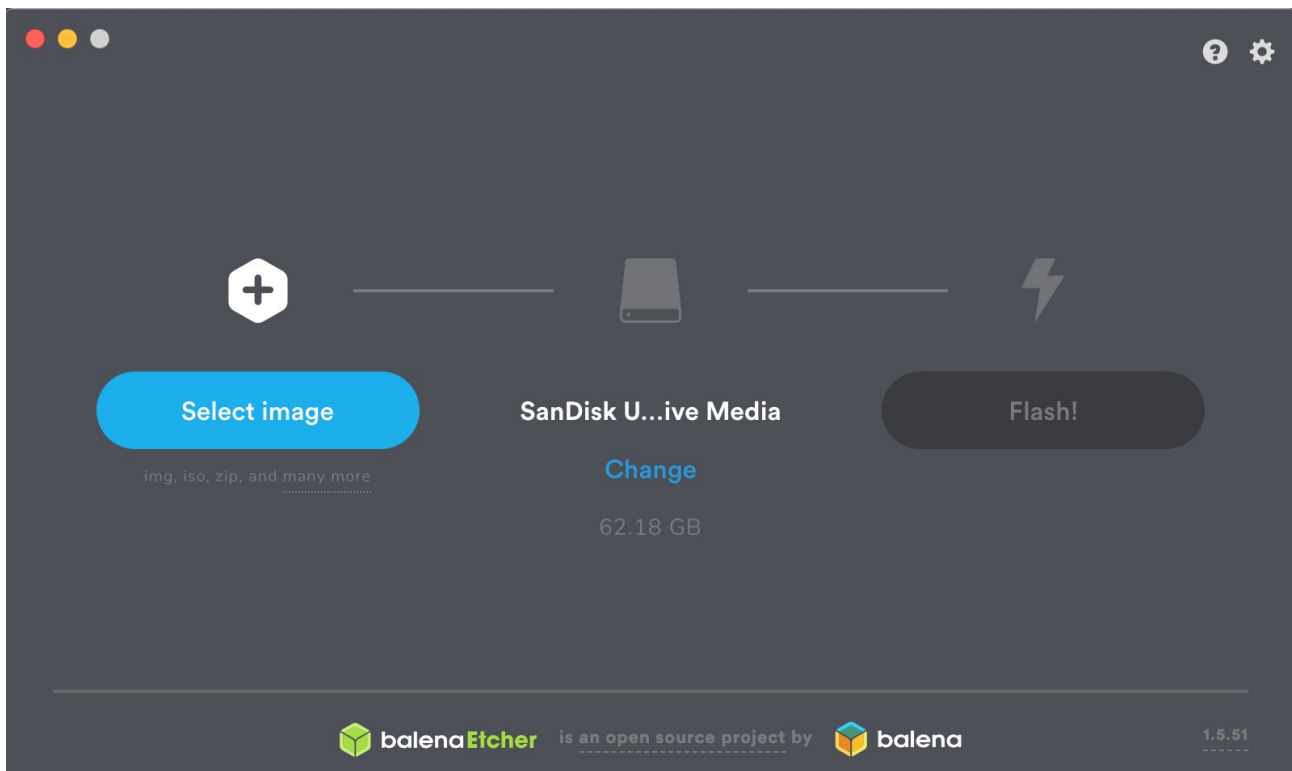
Once you have your USB ready head over to Tails and download the USB image file.

<https://tails.boum.org/install/download/index.en.html>

Download Etcher to install a ISO/IMG onto a USB as a standalone OS.

<https://www.balena.io/etcher>

Once Etcher is installed plug in your USB and click on "Select image", select the Tails file, and click "Flash".



If you want to install any other OS (Kali, Ubuntu, etc.) onto USB then just download the ISO and use Etcher to install it onto USB. Easy shit brothers and sisters.

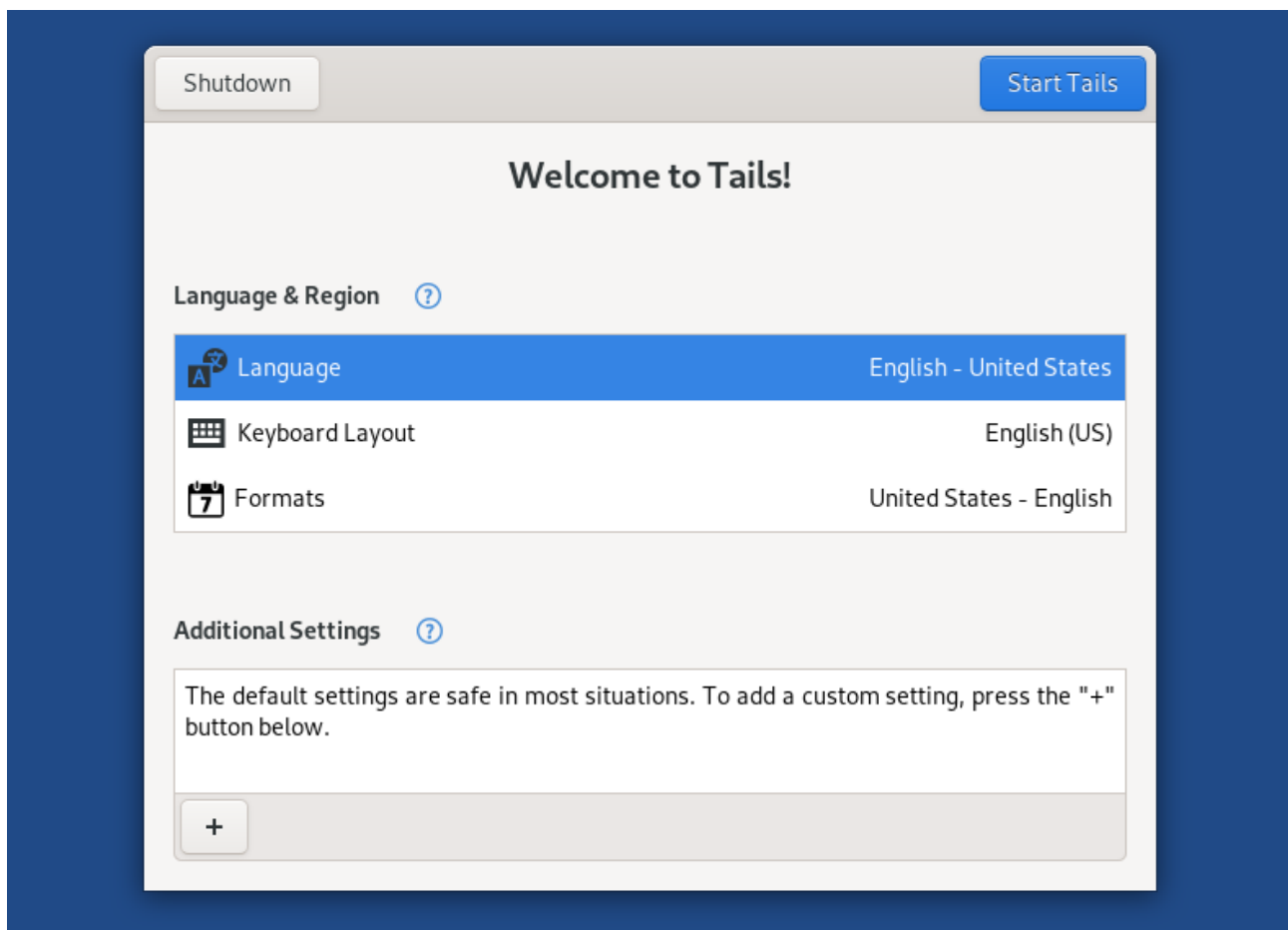
Once installed onto a USB you need to go into your BIOS settings and tell your computer to boot from the USB before booting up your normal host OS.

Each OS is slightly different on how to access your BIOS settings and to enable booting from USB.

[Click to Read - Learn how to boot from USB](#)

Now you know how to boot into Tails OS from USB.

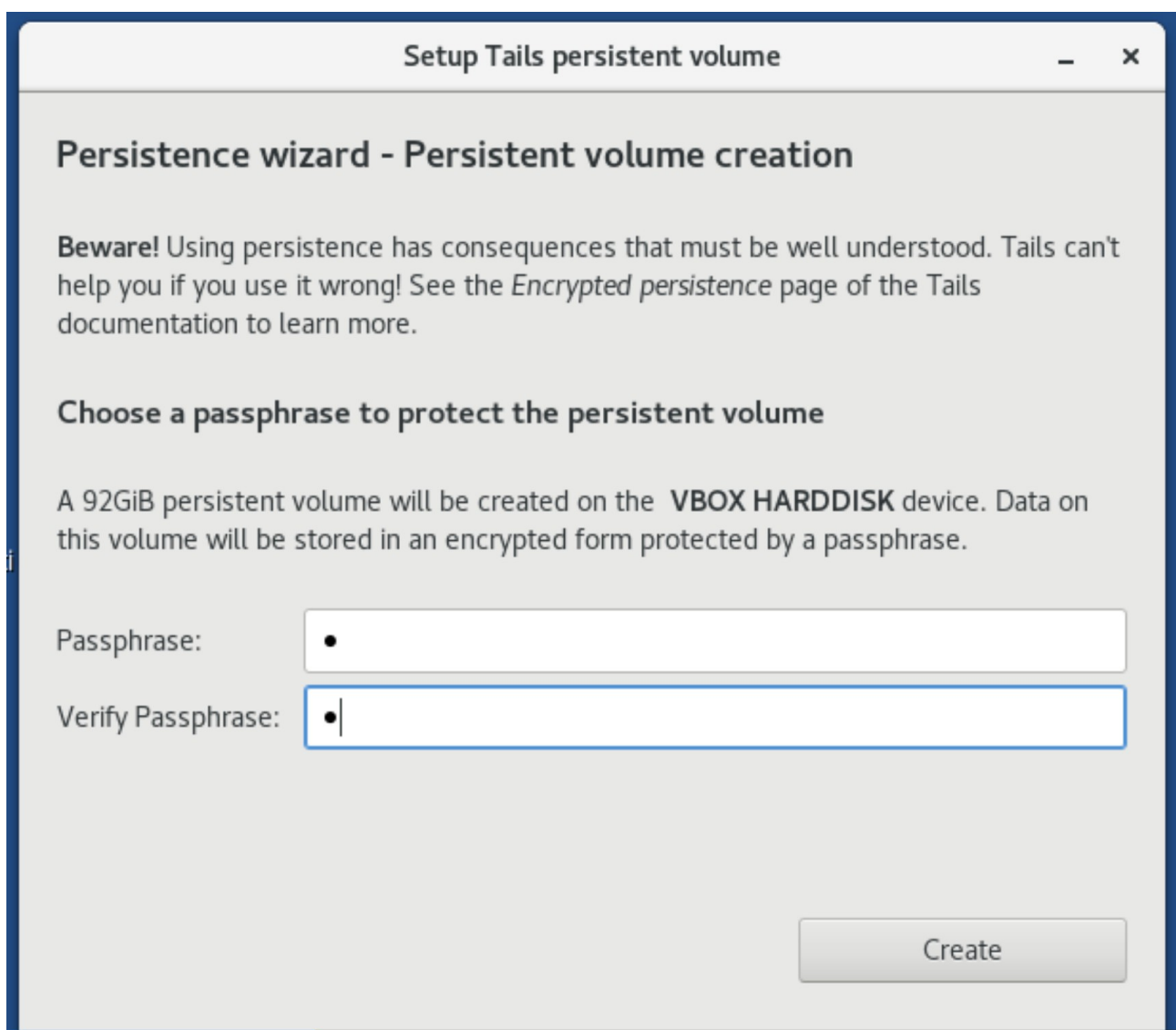
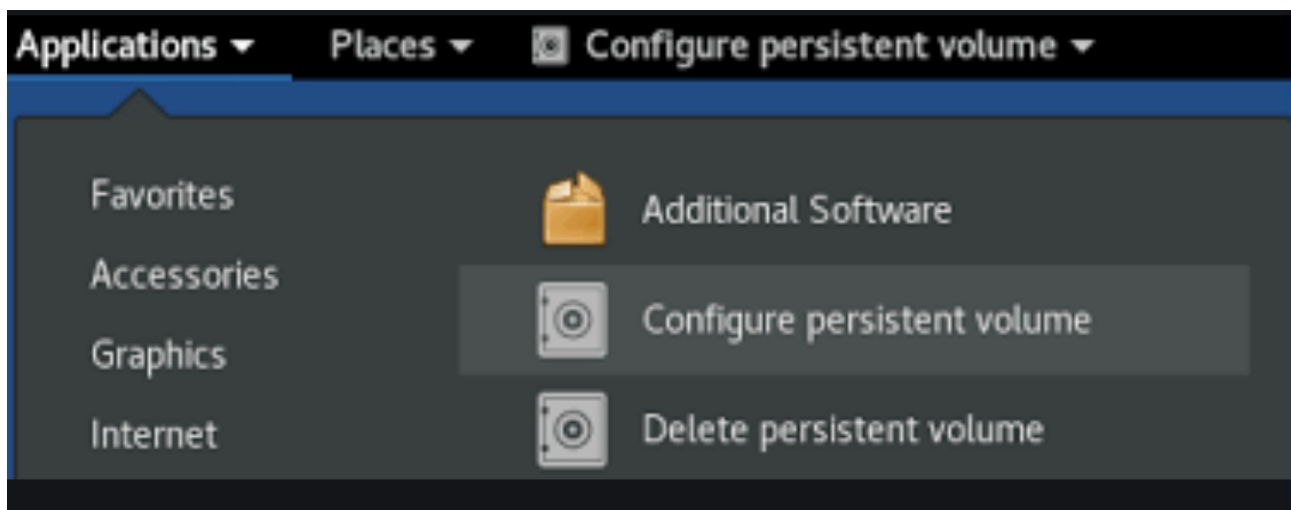
Once Tails boots up for the first time you will see the window below. Click on "Start Tails" and get that shit started.



First things first we need to setup your persistence encrypted folder by configuring your persistent volume. You want to mark persistent the items you will be using for when you're operating online. It's recommended to turn ON your Browser Bookmarks, Thunderbird, GnuPG, Bitcoin Client, SSH Client, and Pidgin. Don't be afraid to select the items you want because when your door gets blasted down it doesn't matter.

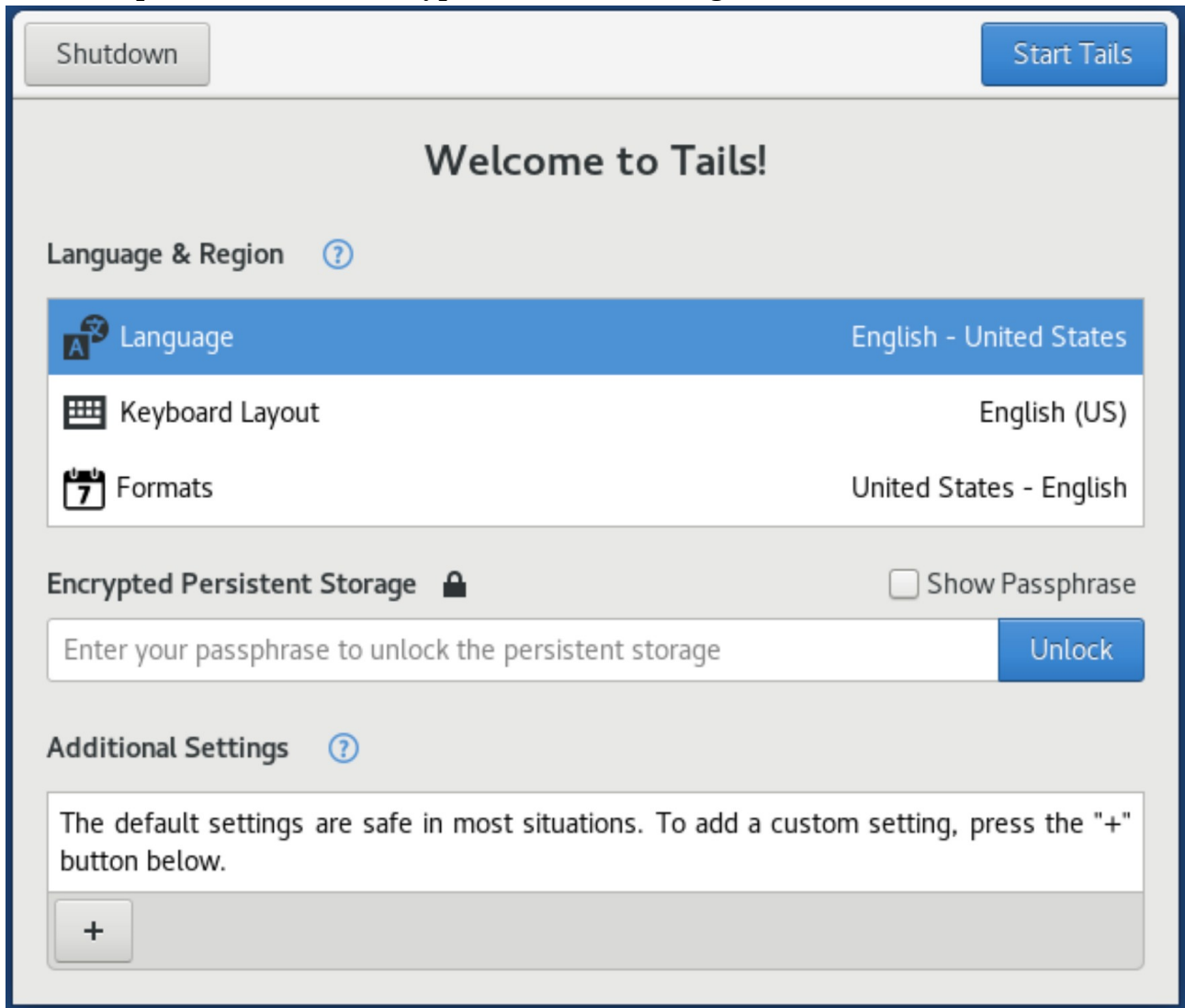
[Click to Read - Tails Persistent options](#)

Click on "Applications" in the top left hand corner and then click "Configure persistent volume". Follow the setup guide.



Alright you now have an encrypted persistent folder in Tails where you can keep all your dick pics secured and encrypted within Tails. That's great!

Now that's done restart Tails again to be greeted with the screen below with a new option to enter a password for an "Encrypted Persistent Storage".



Enter your password to decrypt your persistent files and away you go!

To access your files click on "Places" and then select the "Persistent" folder. Anything saved to this folder will always be there each bootup of Tails.

If your asking yourself right now:

"How the fuck do I transfer all my darknet shit over to Tails"

Read the fuck on!

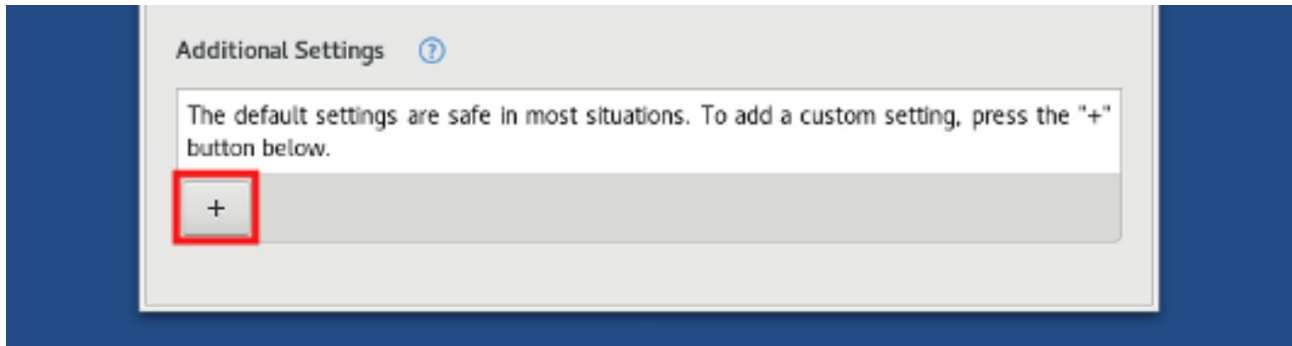
Step 1:

Purchase a fresh USB, encrypt it with VeraCrypt, and transfer your shit over to it. Make

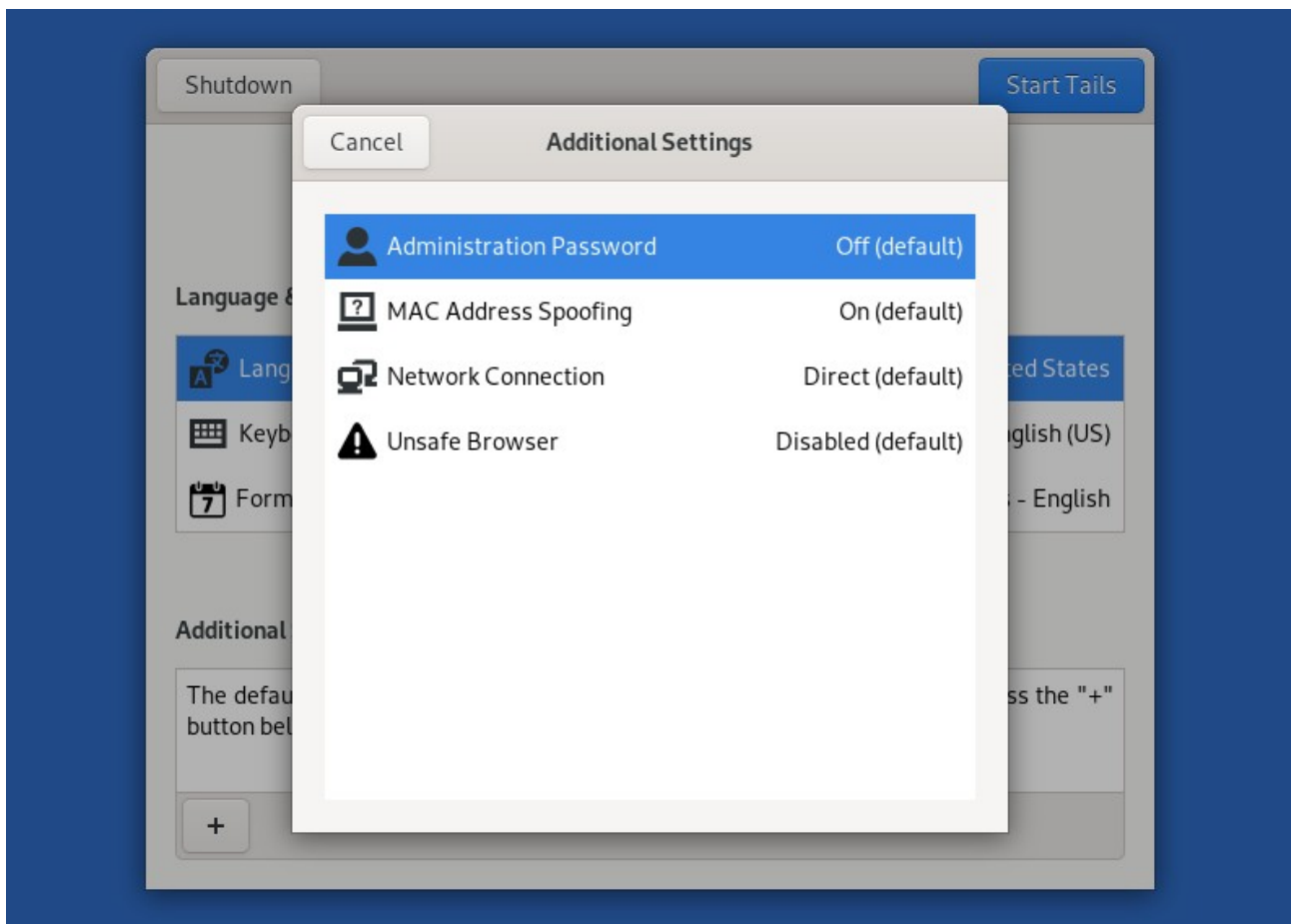
sure you include your PGP keys, KeePass keys, Tor bookmarks, every and anything you want encrypted onto a USB. However you're operating right now move all your shady ass shit to a different USB encrypted with VeraCrypt so you can have those files on your Tails OS.

Step 2:

Plug your Tails USB into your laptop and boot that shit up. Don't forget to unlock your persistent encrypted folder and then click on the + below Additional Settings.



Turn on "Administration Password" and set an Admin password so you can transfer your files from USB to your persistent folder in Tails. Once that's done Start Tails.

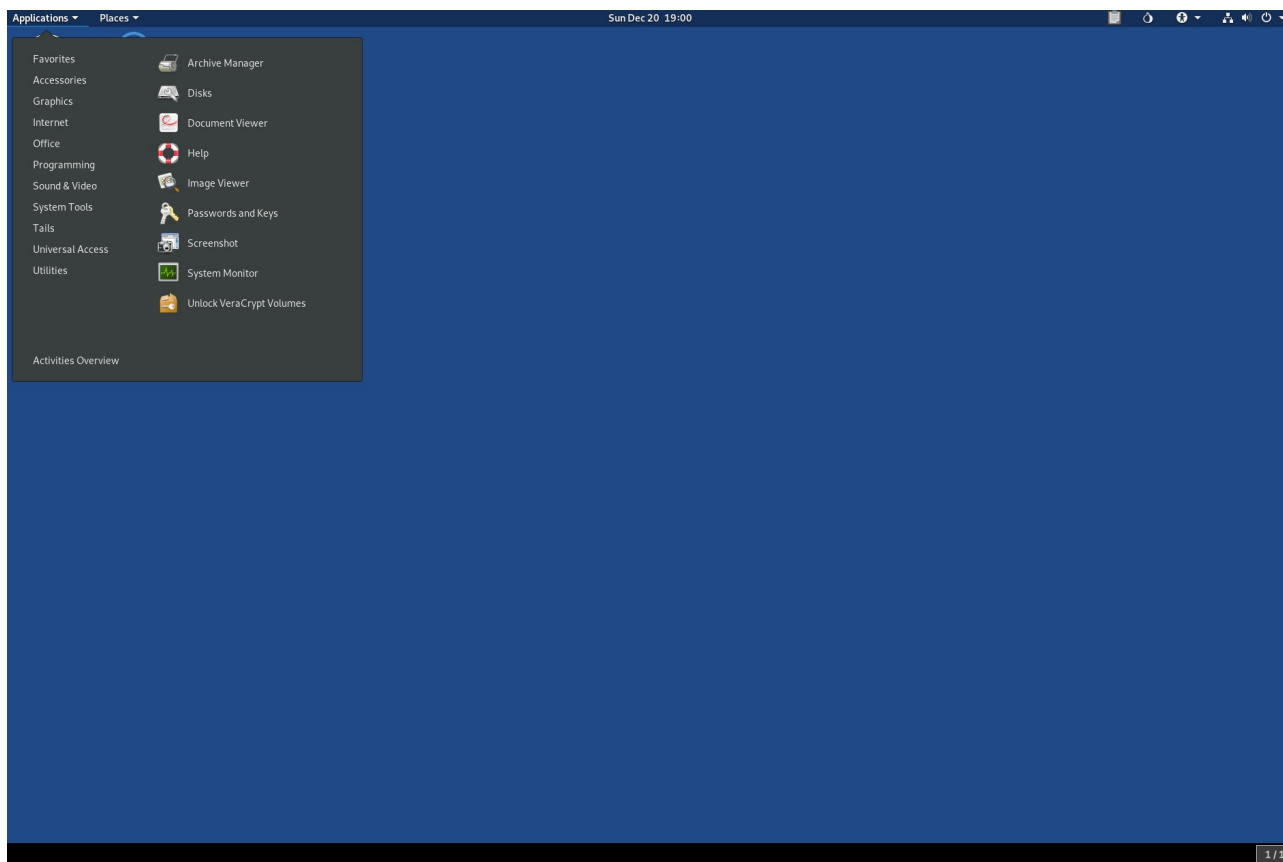


Step 3:

Plug your USB with all your devious fucking sketchy ass plans on it into your laptop with

Tails running.

Click on "Applications" in the top left-hand corner of your screen and then to "Utilities" and click on "Unlock VeraCrypt Volumes". Select your encrypted VeraCrypt USB and click "Unlock".



You now have moved all your files from your encrypted USB to your encrypted persistent Tails folder. You can use that VeraCrypt encrypted USB as a backup should something ever occur to your files. The persistent folder is where you will store all your personal files needed for you to operate online. Remember, it's better to first experiment with a new OS first before moving everything over, using Tails, and ensuring it's up to your liking before fully committing to it.

As a cybercriminal, hacker pro fantastic, or online fraudster there are a few VMs you're going to want at your disposal.

Windows 10

<https://www.microsoft.com/en-us/software-download/windows10ISO>

Ubuntu

<https://ubuntu.com/download/desktop>

Kali

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download>



"Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company."

In other words this OS is designed for hacking and has many of the hacking tools needed to be a successful cybercriminal and hacker.

Make sure you select the VirtualBox image and not the VMWare image!

+ KALI LINUX VMWARE IMAGES

– KALI LINUX VIRTUALBOX IMAGES

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2021.1	3.6G	b907b61ed584c8eef57dcb81e45f8e8af608cc1e0f203711e6c57653b938ef69
Kali Linux VirtualBox 32-Bit (OVA)	Torrent	2021.1	3.2G	fb0ec2dff7d83ec042c2376f740f8c3e92d230caadadee0ffe483c1b809a1013

Caution

Regardless of your OPsec or how you choose to operate everything will come down to one thing.

The USB.

If you've encrypted your USB and are storing your Whonix VM along with everything else on it then that USB will most likely be in your possession when the cyber S.W.A.T team comes crashing through your window and arrests you.

If you've put Tails onto USB and are using the encrypted persistent feature then that USB will most likely be in your possession when the cyber S.W.A.T team comes crashing through your window and arrests you.

Right?

The result is the same.

If something goes fucking crazy and you revealed your true IP to the authorities that USB you have with everything on it will be your down fall. Did you encrypt it properly? Did you use a strong password so your passwords cannot be cracked by the feds? Can anyone tell if the USB is encrypted or if Tails has an encrypted persistent folder on it? Yes, yes they can.

The Weaknesses

OK let's say shit has hit the fan and you're arrested. It doesn't matter how you got arrested the point is your arrested and the police have your computers along with all your USBs, HD, microSD cards, and basically anything capable of storing data will be confiscated.

Assume worst case scenario of the police having your USBs that are encrypted with your shady ass cybercriminal plans saved on it.

Police will be able to determine:

- A) That your hard drive (HD) is encrypted and demand the passphrase to unlock it.
- B) See that you have an encrypted folder on your HD and demand the passphrase to unlock it.
- C) See that your USBs that are encrypted and demand the passphrase to unlock it.
- D) Determine that you have Tails installed on a USB and be able to see an encrypted persistent folder on it and demand the passphrase to unlock it.
- E) Have all your shit.

They can run computer forensics on the USB to find out it's encrypted so there's no hiding from that.

The Tails OS website states:

"The encrypted persistent storage is not hidden. An attacker in possession of the USB stick can know whether it has an encrypted persistent storage. Take into consideration that you can be forced or tricked to give out its passphrase."

We already know that right? When you first booted Tails up there was no option to enter a password for the encrypted persistent folder was there? It doesn't take a rocket scientist to figure out you have an encrypted folder there since anyone could plug that USB into their computer to boot into the Tails welcome screen and see it.

We now know that having Tails with persistence installed on USB and having everything encrypted on a USB (Whonix, etc.) presents the same problem in the end. Whether you choose Whonix or Tails both methods of operating would show there are encrypted

containers on the HD or USB through computer forensics and be able to reveal there is a Tails encrypted Persistent folder on a USB.

The police would demand the passphrases to open it which would seal your fate or you choose not to reveal your passwords and be charged accordingly in your country. Charges for not revealing your passwords vary from country to country and now might be a good time to look that up where you live :)

If you're booting directly from USB (Tails, Kali, etc.) then only (1) exploit would be enough to leak your IP and compromise you. Did you download a copy of Tails, Whonix, etc. that has been compromised? Is this really out of the reality of possibilities?!

Exploits are getting more hard to come by and are of high monetary value available for purchase so you best be worth it.

If you're using Whonix then in order for you to be compromised or have your IP leaked means that an exploit would be needed for Whonix, Tor Browser, then VirtualBox, then possibly another exploit for Windows, macOS, or whatever OS you're using. In today's day and age exploits of that nature are noticed almost immediately with cyber security researchers being all over that shit.

Using Whonix requires multiple exploits needed to compromise you and your computer.

Just that alone gives you more and more barriers when using Whonix. Still, you will leave some sort of a digital trail on your Windows or macOS host computer.

For example, you have VirtualBox installed on your Windows or macOS computer which stores the history on the latest used VMs which points exactly to where you store that VM. Meaning, if they got onto your computer they would be able to see your launching a VM that is saved on a USB and they need to find that USB. You see?

Even if you think you're cleaning all your digital tracks left behind when using a Windows or macOS computer the reality is there's so much you don't realize you're leaving behind and you should be mindful of this.

Whereas if you're booting Tails off a USB into memory nothing ever touches your HD so there is nothing on your computer that would be left behind. Tails wipes the memory before each shutdown ensuring that when you bootup Tails again it's fresh with nothing left behind.

Only (1) exploit would be required to reveal your IP and location when using Tails. You wouldn't even know it happened.

Tails is appealing for the ease of installing it onto a USB and concealing that USB.

Whonix is appealing for the ease of keeping everything on a USB and concealing that USB.

So which method do you pick? Running Whonix in a VM or booting Tails from USB?

When you take the next course ACT I - Wi-Fi Hacking you'll learn how to compromise the Wi-Fi networks around you so you can use other people's internet to conceal yourself even more.

If on that dark day you get compromised and reveal your true location it sure as fuck won't be yours.

Once you know how to hack Wi-Fi networks using Whonix VM or Tails is personal choice.

Think everything over before committing one way or the other and weigh your pros and cons.

VPS, RDP, and VPNs.

Only use anonymous email providers that you can access over Tor when signing up for any service provider and only purchase the RDP, VPS, or VPN with untraceable crypto which you'll learn about in Chapter 8.

Virtual Private Servers (VPS)

Using Virtual Private Servers (VPS) is another tool in your toolkit when in remaining anonymous while hacking or committing whatever cybercrime you're into these days. These "virtual" servers are virtual machines rented out that are on a dedicated or shared hosting provider usually from a Internet hosting service provider or third party provider.

It's good advice to seek out providers that originate in countries that do not cooperate with the country you reside in. The benefit to using VPS's is you're able to log into them over Tor through SSH and can launch a hack from the VPS. Any trace or investigation will lead back to the VPS IP you've rented and since you've logged in through Tor and taken the proper steps to keep yourself anonymous you should have little to worry about.

Another benefit of using a VPS to launch your attacks from is that some scripts, programs, and techniques can take hours, days, if not weeks to complete. It's nice to log into a VPS and launch the attack and check back in a few days when it's completed instead of sitting by your computer waiting for it to finish. Think about the steps you've taken to hinder an investigation just by using a VPS logging in over Tor. Ideally you're on a public Wi-Fi or hacked Wi-Fi network connecting to a VPS over Tor launching your attacks from the VPS. You could even get a VPN or route everything through Tor on your VPS. You think you're going to get tracked? You're good.

It should be noted you should never ever assume your VPS is secure due to the fact that the provider can always see everything on it. They can image your VPS, sniff traffic, and store the image to go through all your information at a later date. You should only be using such things for attacks and should not be storing valuable information on them. A VPS can be configured for the majority of operating systems out there and are reasonably priced between \$5-40 USD/month which can be acquired through Bitcoin or pre-paid methods. As you progress one day you can use the servers you've hacked for the same purpose but for now purchasing a VPS with crypto is a good way to get started and feel comfortable you're not being tracked to your location.

Honestly sometimes using your own VPS with the proper specs to launch an attack is better than acquiring a hacked server. Hacked servers can be a wish wash of things with other hackers already have compromised them, monitored by others, a honeypot, or they have detected a breach and have wiped your access. This isn't good.

No VPS provider is recommended but whatever VPS provider you decide to go with ensure it meets the following criteria:

- Be able to pay with Bitcoin or other forms of anonymous payment (pre-paid VISA, AMEX, etc.)

- Can access the provider website over Tor.
- Can login over Tor.
- Has relatively good customer service for restarting your VPS should you cause problems (you will)

You should research VPS providers that accept Bitcoin or other "anonymous" forms of payment and find the cheapest one to try out. Once you've found one purchase a plan that is the shortest and cheapest with an installation of Ubuntu (or your flavor of Linux). Use fake details but keep note of all the details you've used to register with as you may need them again should you forget your password, logins, need to restart the server, etc. It's best to see which IP you're using while using Tor and research a company in that area to use the details when signing up for things. It'll help bypass some of their online fraud detections.

For example, I'm using Tor and I would check what my IP is at <https://whatismyip.com> or a similar website. In this example my Tor exit IP is located in Mexico. Therefore, I would look for companies in Mexico and use their addresses when registering online to avoid any problems. Each VPS provider is different but why chance it. This way a connection from Mexico is registering on their website with a Mexican address. Use real addresses that are associated to the geographical area that your IP is at the time.

Google Keyword: Bitcoin payment VPS, VPS Bitcoin, VPS Bitcoin payment, etc.

Remember pick providers that you know are in direct conflict with your country and know they will not cooperate with one another easily or in a timely manner.

Once you've completed your purchase it may take a few hours to have the VPS setup and you should either receive your login details at the time of purchase or e-mailed to you afterwards. When you've received your credentials to your VPS you will log into it via SSH over Tor. Do not log into the VPS without SSH over Tor or risk anything that would reveal your IP to the VPS provider. Don't do this. Use SSH over Tor when connecting to the VPS.

If you're using Whonix or Tails you can simply SSH into your VPS over Tor without any worries with:

ssh USERNAME@IP

For the people who want to use Windows or macOS you would need to run the Tor standalone first and then connect to your VPS with the right proxy settings enabled ensuring your connection is routed through Tor.

Below is the information to ensure everything is routed through Tor if you choose not to do it through Whonix or Tails but instead on your host OS (Windows, macOS, etc.).

To SSH into your VPS you'll need to run the Tor standalone file first.

Go to the directory where the Tor Browser has been downloaded into:

Windows (from the command line)

```
cd Tor Browser\Browser\TorBrowser\Tor  
tor.exe
```

Linux (Ubuntu, Kali, etc.)

```
cd tor-browser_en-US/Browser/TorBrowser/Tor  
./tor
```

macOS

```
cd /Applications/Tor\ Browser.app/Contents/MacOS/Tor  
./tor.real
```

OR

```
cd /Applications/TorBrowser.app/Contents/MacOS/Tor  
./tor.real
```

This will start the Tor stand alone and make a connection to the Tor network through the default port 9050. You can now re-direct applications to 127.0.0.1:9050 to funnel them through Tor.

If you're using Windows you will need to download and install Putty and configure it to use a proxy for 127.0.0.1 Port: 9050.

The example below is meant for macOS and Linux based operating systems.

Open a new terminal window while keeping the Tor standalone running and connect to your VPS. Paste the following command into terminal changing the **USERNAME** and **VPS_IP** to match the credentials given to you by the VPS provider

```
ssh -o "ProxyCommand nc -X 5 -x 127.0.0.1:9050 %h %p"  
USERNAME@VPS_IP
```

This command above uses SSH over Tor to connect to your VPS.

Why is this important?

- You launch hacks from the VPS.
- Police are notified of the cyber-attack.
- Police track the IP to the VPS you purchased anonymously with Bitcoin.
- A warrant is sent to the VPS to see what IP connected to the VPS.
- That IP of course is a Tor exit node.

Once logged into your VPS always remember to keep it updated and install the appropriate upgrades needed. In general' these commands will keep your bash history from being spied on:

```
unset HISTFILE  
echo 'set +o history' >> /etc/profile  
echo 'set +o history' >> ~/.bashrc  
export HISTFILE=/dev/null
```

unset HISTFILE = Doesn't keep track of bash history
echo 'set +o history' >> /etc/profile = Ensures there's no bash history stored
echo 'set +o history' >> ~/.bashrc = Ensures there's no bash history stored

You can install any programs on the VPS such as scripts, brute forcing programs, nmap, Metasploit, and other things that will be needed for your cyber warfare madness you plan on doing. Any program that runs on Kali can be installed on the VPS for launching attacks but this course is not meant to tell you what to install but rather give you the basics that you will need to remain as stealthy as possible when launching your attacks.

For example, I like using VPS's for setting up Metasploit listeners, Social Engineering ToolKit (SET), Empire listeners, BeEF, etc. and leaving them running so I can check back at my leisure instead of being glued to a computer.

Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) are essential for using a Windows machine on a VPS. Again, it's best to use a public Wi-Fi, and use VPN/Tor to connect to your RDP. From there you can utilize your Windows machine as another server to launch your attacks from depending on which programs you decide to use (APPscan, Netspark, Acunetix, etc.). Always follow the same VPN/VPS rules when purchasing a RDP from a RDP provider.

Virtual Private Network (VPN)

Using a VPN or your host machine is essential when conducting your dark web activities which you can also apply to your VM, VPS, and RDP machines. Let's assume your actions are being logged while you're connected to a Wi-Fi network either by the feds or at the ISP level. Anything that is sent over the network that's not encrypted will be able to viewed in cleartext like a book.

The VPN will encrypt your communications from your computer/device to the internet which means all your connections are going to your VPN provider and nothing else.

Not using a VPN will show that you're connecting to multiple websites, IP's, or a Tor entry node whereas using a VPN would only show you connecting to (1) IP.

That IP being your VPN provider and all data encrypted.

There's no recommendation on which VPN provider to use but ensure you're registering with them with an anonymous email and paying in anonymous crypto.

Try and use only well known providers that accept crypto such as NordVPN, AirVPN, and many others. A Google search away my friends.

Anonymous Crypto

Bitcoin (BTC), Monero (XMR), Zerocoin (zcash), cash, and pre-paid credit cards purchased with cash are the best options to use when purchasing items when it comes to staying anonymous. Since BTC is the most commonly used cryptocurrency it's always good to have some that's completely anonymous for you to use freely when needed.

It's important to purchase and deposit BTC the most anonymous way possible as we know the blockchain is a public ledger therefore, theoretically, it can be tracked if you're not careful especially if you're using cryptocurrency exchanges to cash out your winnings. We want to avoid our transactions from being tracked for obvious reasons. Purchasing BTC will vary from person to person depending which country you reside in and some methods may not work for everyone.

You should never trust any third party to store your BTC so don't keep them in an online wallet for long if you have to. It's most best to use an offline wallet

<https://localbitcoins.com> recently stopped in person cash buying/selling of BTC as of June 1, 2019 and this method is no longer viable which is annoying but honestly it doesn't matter. Google "BTC ATMs" or go to <https://coinatmradar.com> and see if there are any BTC ATMs in your area you can use to purchase BTC with cash. Simply follow the directions on the ATM and buy BTC with cash it's not that difficult. You'll need a BTC wallet either on your tablet or mobile device but most wallets are very straight forward and can be downloaded from Google Play or the App Store. You can also check good old craigslist.org to meet-up in person to buy BTC for cash.

If you'd rather purchase BTC online from a cryptocurrency exchange be aware it might take a few days to register and be approved depending on which exchange you use. Some exchanges to check out are:

<https://www.bitstamp.net>

<https://www.coinbase.com>

<https://coinmama.com>

<https://www.kraken.com>

There are so many exchanges these days so pick whichever one you feel comfortable with: <https://bitcoin.org/en/exchanges#international>

Using cryptocurrency exchangers is all legit and legal so don't flip your lid about registering because you're not committing a crime. You're simply purchasing an asset and nothing about that is illegal.

Using exchanges to buy and sell cryptocurrencies does present an OPsec problem as most online exchangers require you to register with your real information. Giving out your REAL information for anything is always a problem surrounding criminal/hacking activities. I know that doesn't sound great however we're going to use the latest technology to help "wash" our coins and stay anonymous so no need to overly stress out about this shit. If you don't purchase BTC from a BTC ATM, craigslist, etc. then you'll need to

purchase BTC from an online exchange with whichever method you prefer (Paypal, bank account, credit card, etc.).

Once you have some BTC we'll "wash" your BTC and exchange it for Monero (XMR) and then exchange your XMR back into BTC again.

Converting your BTC into XMR, sending that XMR to another XMR address, and then converting back into BTC again will cut the connection to you making your crypto completely anonymous to spend on whatever your heart desires (heroin and crack most likely). This will also give you the ability to convert that tainted BTC into clean BTC making it untraceable. It's also recommended to use this method each time you plan on cashing out whatever crypto currency you're dealing with.

For example, you made \$1000 in BTC from infecting people with ransomware or you're a vendor and want to cash out the BTC you've made then you'll want to convert that BTC into XMR, send the XMR to another XMR wallet you control, and convert back again into BTC (or whatever cryptocurrency) before "cashing out". We want to ensure your hard earned crypto is completely anonymous and safe to put into your account if you choose to do so. Once converted into XMR you can consider it "washed" and technically untraceable.

Monero (XMR) was designed specifically with privacy in mind as is not traceable as of today. Unsure of what XMR is? Use Google or watch a YouTube video about it.

Alright it's assumed you have some BTC to be converted.

You'll first need to create a Monero (XMR) wallet and the easiest way of doing this is to utilize the online wallet:

<https://wallet.mymonero.com>

Once you have a Monero wallet then you want to convert your BTC to XMR and back again by utilizing the following sites:

<https://www.morphtoken.com>

<https://changenow.io>

<https://changelly.com>

<https://coinswitch.co>

<https://xmr.to/nojs>

<https://localmonero.co>

Once you have your BTC that you consider safe you'll want to use a wallet on your computer or an online wallet (<https://blockchain.info>).

[Click to Read - Is Monero safe?](#)

[Click to Read - Something to pay attention to but not proven yet.](#)

[Click to Read - CipherTrace states they can track XMR. Not proven yet.](#)

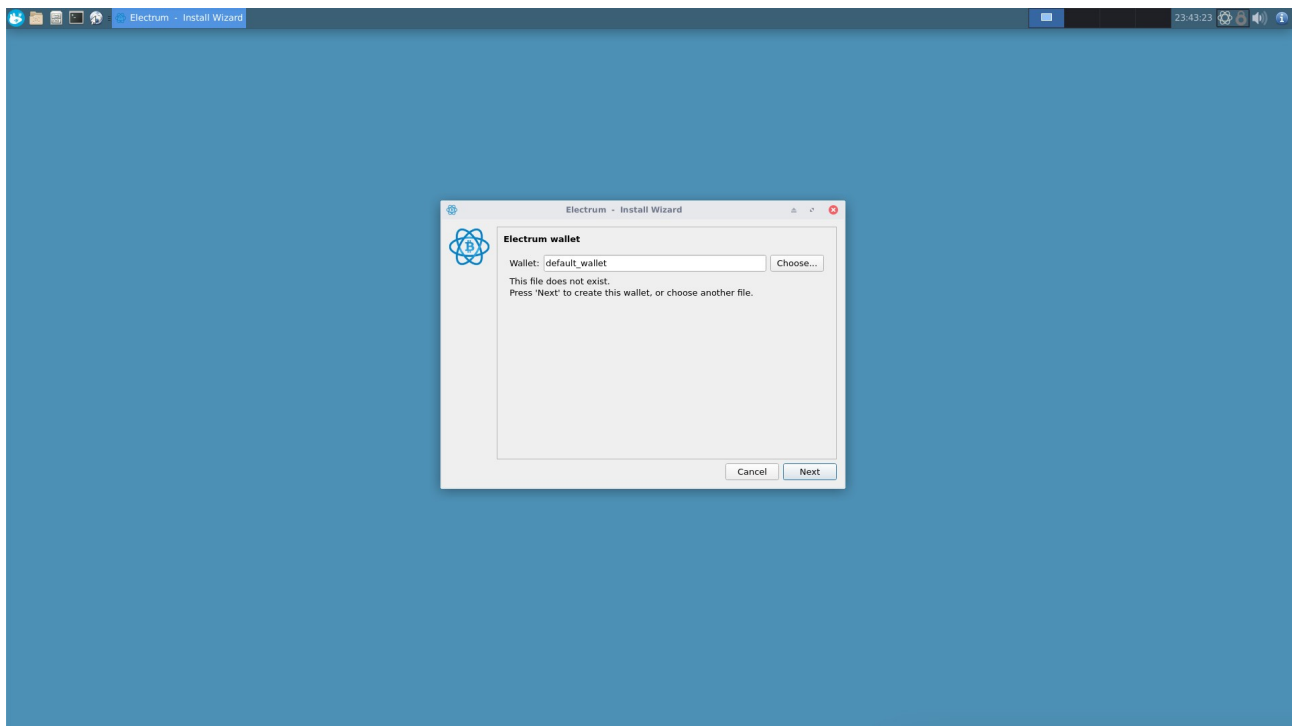
If you're using Whonix or Tails the Electrum Bitcoin Wallet is already installed by default for you.

Setting up Electrum BTC wallet in Whonix VM

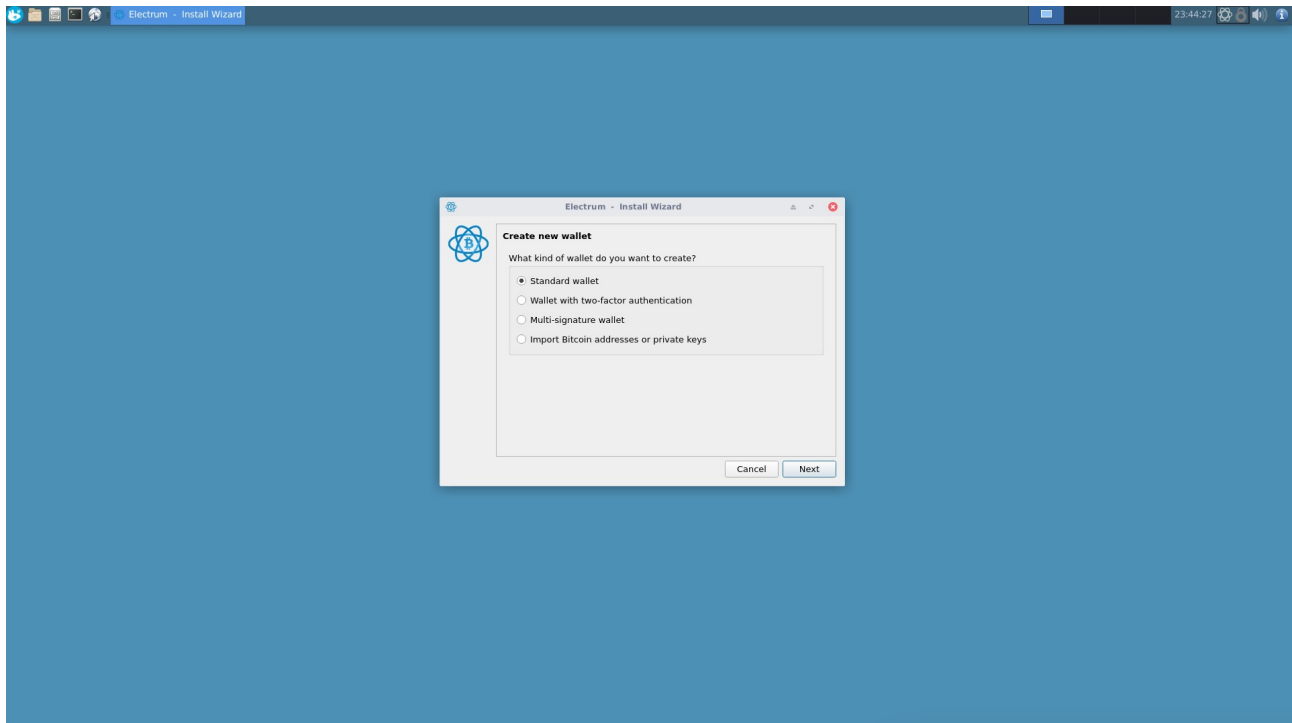
Click on the first icon in the top left hand of your Whonix Desktop then go to "Internet" and click on "Electrum Bitcoin Wallet"



Click "next" and leave the default name of the wallet alone for now then click "next".



Select "Standard Wallet" then "Create a new seed" and click "Next".

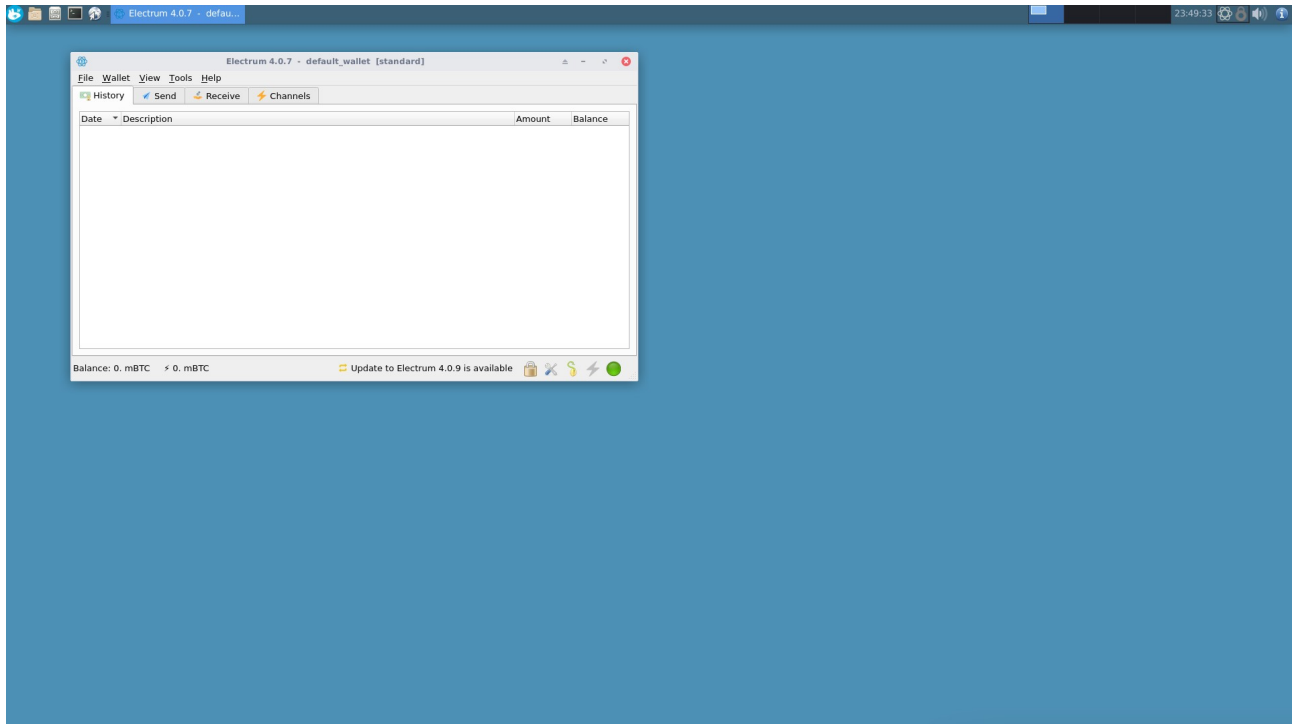


After that select Segwit or Legacy wallet. If you're confused then select Legacy for now.

You'll be presented your wallet seed and it's important to write that down or store it in KeePass to keep it safe. This way you can restore your Electrum wallet with that seed should your shit get corrupted.

Go through the prompts and enter a password needed to access your Electrum wallet.

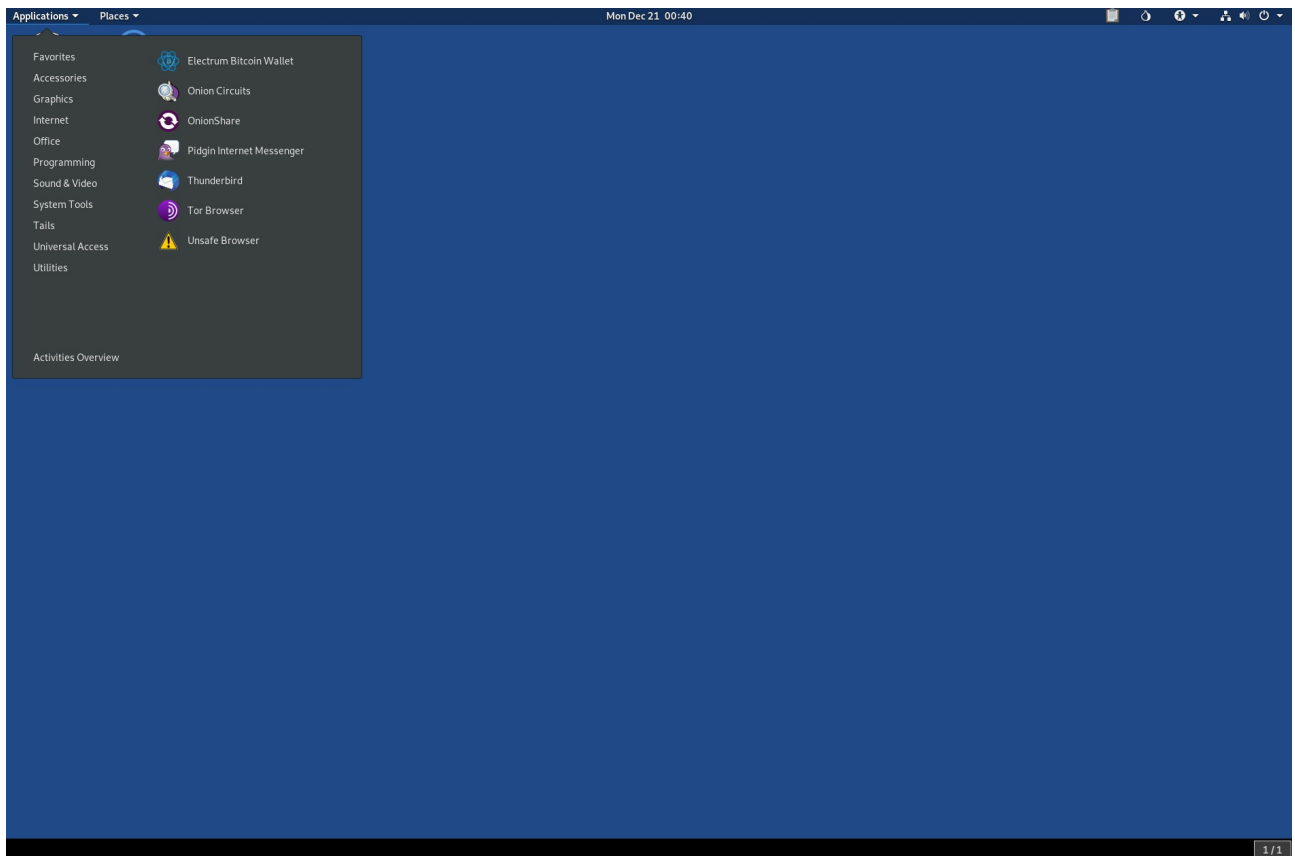
Once you've set everything up it will look similar to the screenshot below.



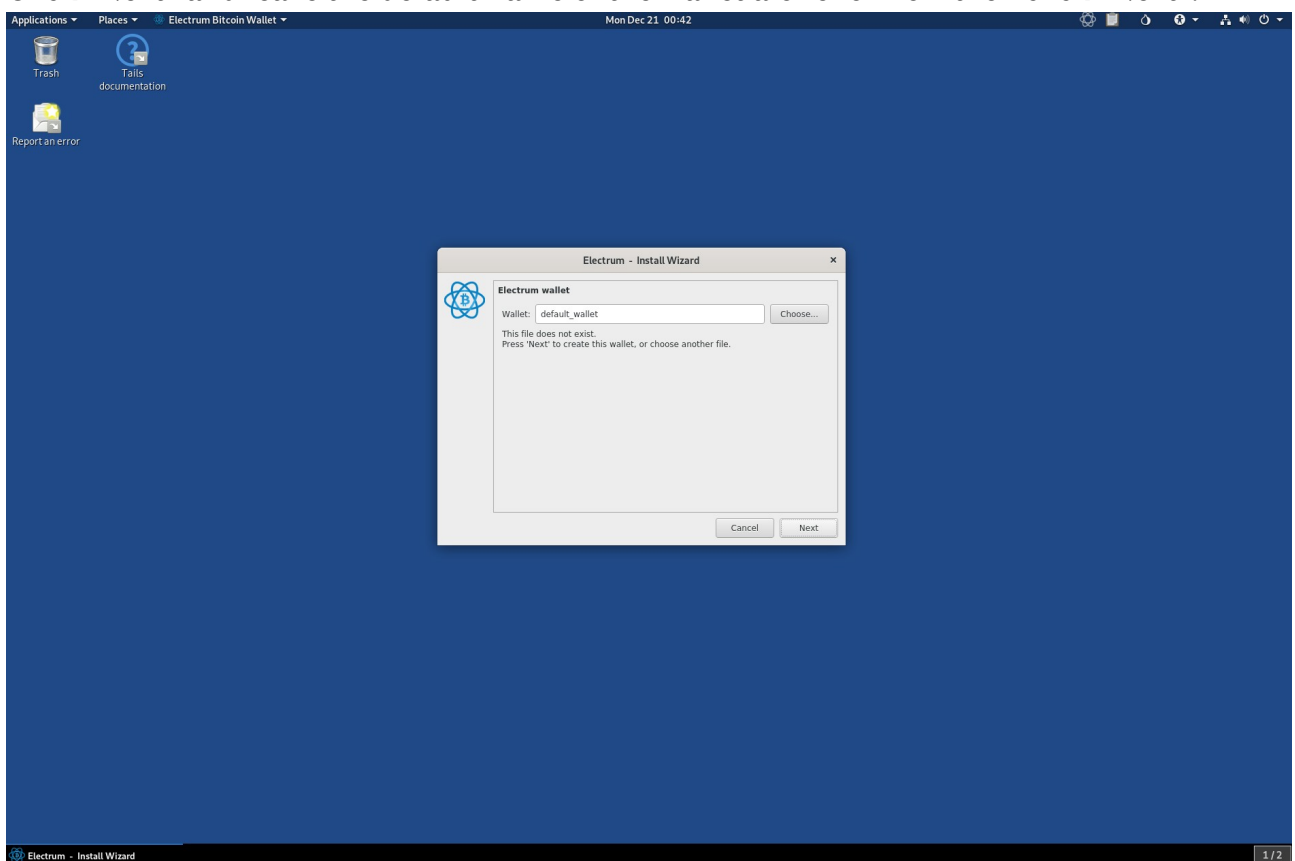
You can now send and receive BTC to your anonymous wallet that's routed through Tor in your Whonix VM. Awesome mother fuckers!

Setting up Electrum BTC wallet in Tails OS

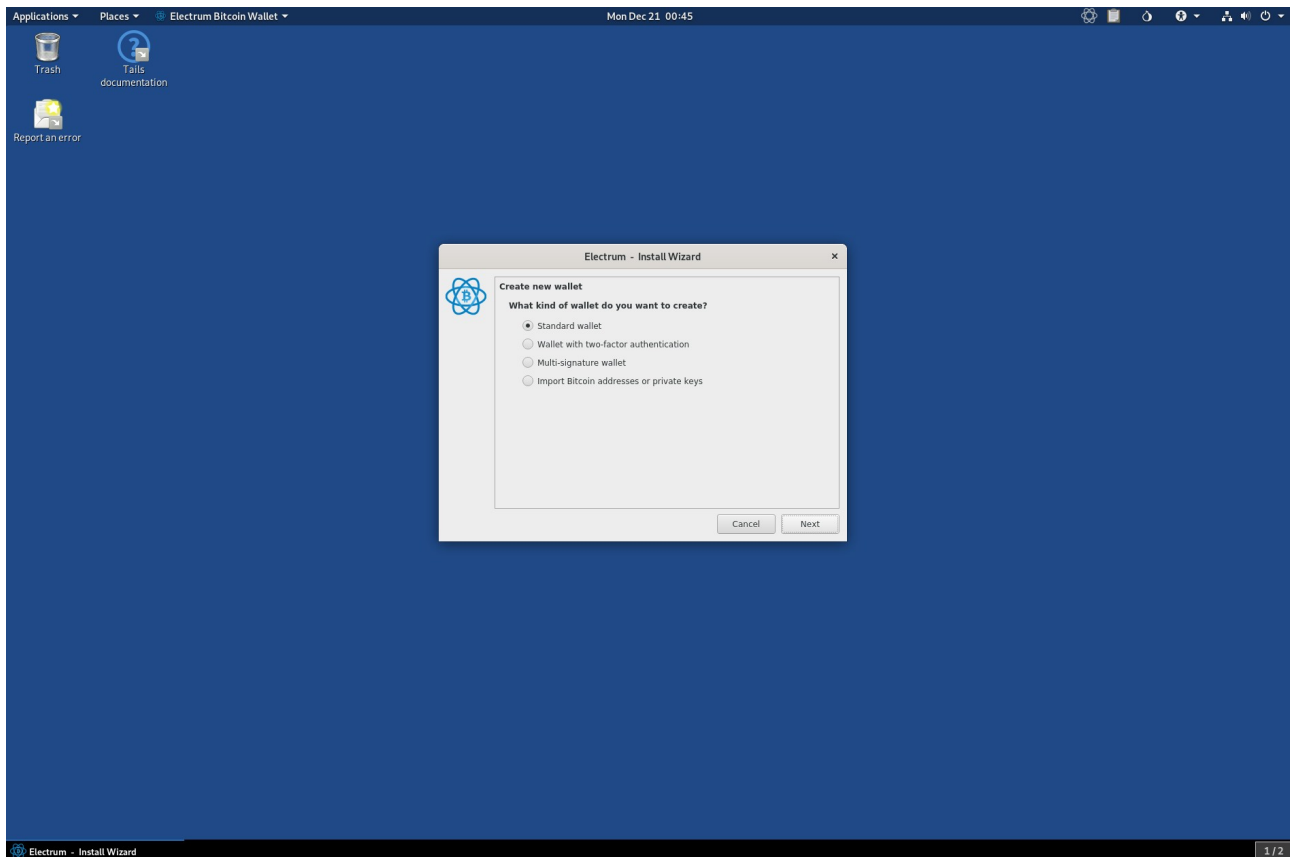
Click on "Applications" in the top left-hand corner of your screen then click "Internet" and then "Electrum Bitcoin Wallet".



Click "Next" and leave the default name of the wallet alone for now then click "Next".



Select "Standard Wallet" then "Create a new seed" and click "Next".

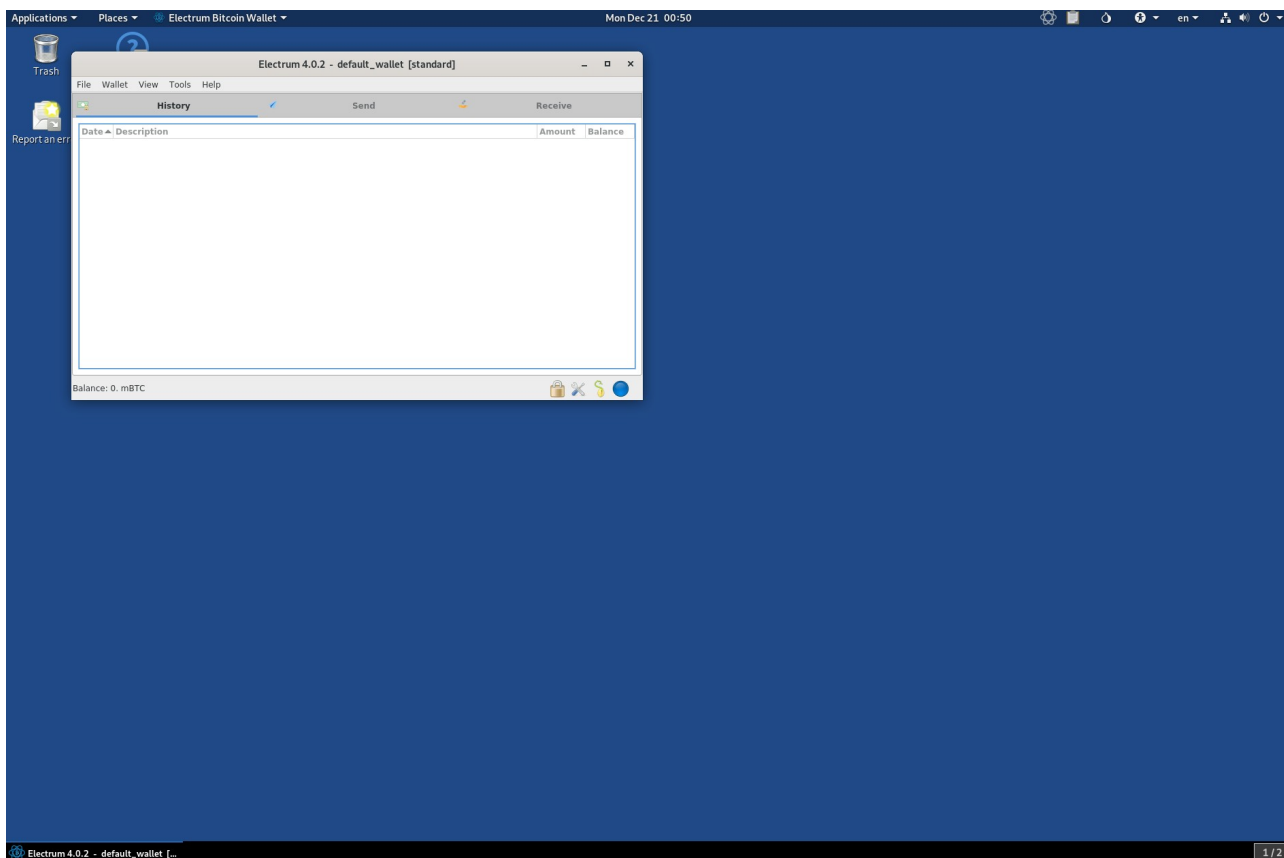


After that select Segwit or Legacy wallet. If you're confused then select Legacy for now.

You'll be presented your wallet seed and it's important to write that down or store it in KeePass to keep it safe. This way you can restore your Electrum wallet with that seed should your shit get corrupted.

Go through the prompts and enter a password needed to access your Electrum wallet.

Once you've set everything up it will look similar to the screenshot below.



You can now send and receive BTC to your anonymous wallet that's routed through Tor in Tails. Awesome mother fuckers!

Now that you have your wallets setup to run through Tor you can feel secure when sending/receiving BTC and since we converted our original purchased BTC into XMR and back again we can feel confident the BTC we've converted is anonymous and secure to spend it as we please.

OR

Clean your BTC so you can cash out your millions, whichever way you're going buddies.

PGP

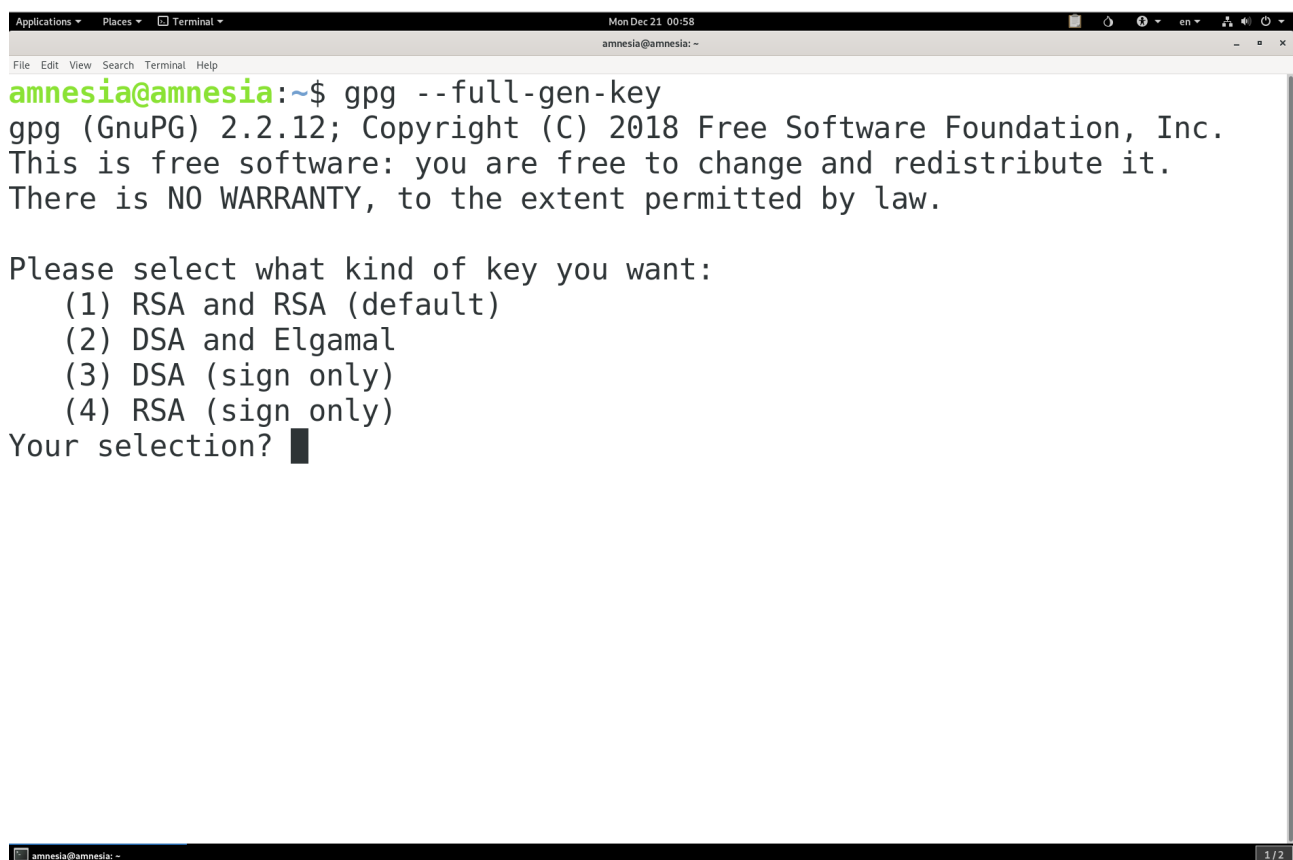
You should have an idea of what PGP is because you've already read the "Jolly Rogers catch-up" chapter. It's always best to test your PGP keys when you've created them to ensure you're able to decrypt messages before you send out your public PGP key to clients, associates, etc.

Since you should be using Whonix in a VM or booting Tails from USB the following examples only apply to those operating systems.

Create your PGP keys

Load up your Whonix VM or Tails OS and open Terminal:

gpg --full-gen-key

A screenshot of a terminal window titled 'Terminal' with a menu bar (Applications, Places, Terminal) and a status bar (Mon Dec 21 00:58, amnesia@amnesia: ~). The terminal shows the command 'gpg --full-gen-key' being executed. The output includes the GnuPG version (2.2.12), copyright information (© 2018 Free Software Foundation, Inc.), and a disclaimer: 'This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.' It then prompts the user to 'Please select what kind of key you want:' with four options: (1) RSA and RSA (default), (2) DSA and Elgamal, (3) DSA (sign only), and (4) RSA (sign only). The prompt 'Your selection?' is followed by a cursor. The terminal window has a standard Linux-style window frame with a title bar and window controls. The status bar at the bottom shows 'amnesia@amnesia: ~' and a page indicator '1/2'.

Hit the number "1" on your keyboard to Select "(1) RSA and RSA (default)" and then "4096" when asked for key size.

```
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? (3072) 4096
Requested keysize is 4096 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) 0
Key does not expire at all
Is this correct? (y/N) y
```

GnuPG needs to construct a user ID to identify your key.

Real name: █

Hit "o" on your keyboard for "o = key does not expire", then enter whatever fake information associated to your fake or darknet handle email address, and then hit "O" on your keyboard for "(O)kay".

You'll be prompted to enter a passphrase which will be used to decrypt the PGP messages that are sent to you. Ensure you remember this passphrase as you'll need it.

Exporting your public PGP key

You need to send someone your public PGP key in order for them to encrypt a PGP message to you.

For the people who want to join HackTowm as a member you'll need to send me your public PGP key when joining.

This is how.

To export your public PGP key you would open Terminal in Whonix or Tails:

```
gpg --export -a "USERNAME"
```

To find your username of the keys you setup simply type:

```
gpg --list-keys
```

PGP OPSec

There are a few concerns about how people use PGP that you should be aware of. Let's look at a few examples that demonstrate the weakness in people when using PGP before you implement it yourself.

When you've received a new public PGP key it should be noted that sometimes when you import a public PGP key it will reach out to PGP servers to validate the key if setup to do so. Since you're using Whonix VM or Tails now you could care less but for the people who choose to use their host machine and not follow proper OPSec this will be a problem. Not every public PGP key will authenticate like this but if you've installed and are using Glasswire or Littlesnitch then you would've caught the outgoing connection to the PGP server when importing the key and denied the connection.

Theoretically LE could give you their public PGP key and collaborate with the PGP servers to determine what IP reached out to it when validating their specific public PGP key. Tin foil hat shit but very plausible it's occurring or will occur.

Below you'll see why using your host OS can be a concern sometimes without you even knowing it. Remember, you should be using Whonix in a VM or booting Tails.

Let's take a look at some examples of when people don't use Whonix or Tails and instead encrypt a PGP message from their host OS:

Example 1:

```
-----BEGIN PGP MESSAGE----- Comment: GPGTools - https://gpgtools.org
hQIMAx8sgPUu2KE5AQ/9GmXrRuRbqSc7rEUHoZHHAlYBFV3Gre7kHQc+A9KO/wvn
Etc90+rz6LVXr3tJcYv3t6he+5XAHAj8gbCFsEyQ1QnVPt3Ggye8fadfS7UyIblG
IAA4LYh4WfpFrhoJGiz2AbjTw1pDj3odALGL+nivaLXWh6FhU1VgeN/GsOIU/cMc
b9ol1YVqreGZ62GNEfhNKq6NGGxhLMS/OL1DnxfJ6x3WqiqyIVSoPSI3x2APUB4r
mB9IQbTNHb/TzPLw4Nt5bqE96KNT86M6o1IhFMAAtKLJDguqaJUzCk5I/1ZeW4yRZ
QpOdLaLq3DAG49sJBIvooAqJgOfCiEUmNzE2Psd2ZSYd8/nEYqQUtqxWGSvPLaLM
eVlehsg+3QL2aWfqm5t5w1G9s6vfpwjQWr7EhSeBrAC5W+kAFZMrAczYVhjkHFo
+Pqj6y1jIDo/FRfYOSIUfRchWPYPvU+l7Wmlz4NkKk9ytuWAO1zbGYFqF/uewFSw
AZMIH58D/Ds7EoTnN7wNp4mLB5iWZszx7lDylQmOYqcXt7IO5tg+8CBotxqOBmV
/5VWsP8TzkqEwE5mq4VT+TnbvJhr5Vo4lKVvkqwlAKM3tLQS1+rIJGfmUyffxu7U
lX2DXpInlHDcIOwq8U4dYpmRqPxx7jXciKZKfBiz5HXnQ+It1rJksoZWqZLw/xvS
QgHrO4H+Ru/2idH1gwHojTlPTWt9+a4RxH9V/fZvz7xfkoH3AUpf93sxoqZSPUM7
uXH5hGic4ECC14Ucm6TdkMSFw== =CxP7 -----END PGP MESSAGE-----
```

Example 2:

```
-----BEGIN PGP MESSAGE----- Version: GnuPG v2.0.22 (MingW32)
hQIMAx8sgPUu2KE5AQ/9GmXrRuRbqSc7rEUHoZHHAlYBFV3Gre7kHQc+A9KO/wvn
```

```
Etc90+rz6LVXr3tJcYv3t6he+5XAHaj8gbCFsEyQ1QnVPt3Ggye8fadfS7UyIblG
IAA4LYh4WfpFrhoJGiz2AbjTw1pDj3odALGL+nivaLXWh6FhU1VgeN/GsOIU/cMc
b9ol1YVqreGZ62GNEfhNKq6NGGxhLMS/OL1DnxfJ6x3WqiqyIVSoPSI3x2APUB4r
mB9IQbTNHb/TzPLw4Nt5bqE96KNT86M6o1IhFMAAtKLJDguqaJUzCk5I/1ZeW4yRZ
QpOdLaLq3DAG49sJBIVooAqJgOfCiEUmNzE2Psd2ZSYd8/nEYqQUtqxWGSvPLaLM
eVlehsg+3QL2aWfqm5t5w1G9s6vfpwjQWr7EhSeBrAC5W+kAFZMrAczYVhjkHFO
+Pqj6y1jIDo/FRfYOSIUfRchWPYPvU+l7Wmlz4NkKk9ytuWAO1zbGYFqF/uewFSw
AZMIH58D/Ds7EoTnN7wNp4mLB5iWZsxx7lDylQmOYqcXt7IO5tg+8CBotxqOBmV
/5VWSP8TzkqEwE5mq4VT+TnbvJhr5Vo4lKVvkqWIAKM3tLQS1+rIJGfmUyffxu7U
lX2DXpInlHDcIOwq8U4dYpmRqPxx7jXciKZKfBiz5HXnQ+It1rJksoZWqZLw/xvS
QgHrO4H+Ru/2idH1gwHojTlPTWt9+a4RxH9V/fZvz7xfkoH3AUpf93sxoqZSPUm7
uXH5hGic4ECC14Ucmc6TdkMSFw== =CxP7 -----END PGP MESSAGE-----
```

Example 3:

```
-----BEGIN PGP MESSAGE----- Version: GnuPG v2.0.22 (GNU/Linux)
hQIMAx8sgPUu2KE5AQ/9GmXrRuRbqSc7rEUHoZHHAlYBFV3Gre7kHqc+A9KO/wvn
Etc90+rz6LVXr3tJcYv3t6he+5XAHaj8gbCFsEyQ1QnVPt3Ggye8fadfS7UyIblG
IAA4LYh4WfpFrhoJGiz2AbjTw1pDj3odALGL+nivaLXWh6FhU1VgeN/GsOIU/cMc
b9ol1YVqreGZ62GNEfhNKq6NGGxhLMS/OL1DnxfJ6x3WqiqyIVSoPSI3x2APUB4r
mB9IQbTNHb/TzPLw4Nt5bqE96KNT86M6o1IhFMAAtKLJDguqaJUzCk5I/1ZeW4yRZ
QpOdLaLq3DAG49sJBIVooAqJgOfCiEUmNzE2Psd2ZSYd8/nEYqQUtqxWGSvPLaLM
eVlehsg+3QL2aWfqm5t5w1G9s6vfpwjQWr7EhSeBrAC5W+kAFZMrAczYVhjkHFO
+Pqj6y1jIDo/FRfYOSIUfRchWPYPvU+l7Wmlz4NkKk9ytuWAO1zbGYFqF/uewFSw
AZMIH58D/Ds7EoTnN7wNp4mLB5iWZsxx7lDylQmOYqcXt7IO5tg+8CBotxqOBmV
/5VWSP8TzkqEwE5mq4VT+TnbvJhr5Vo4lKVvkqWIAKM3tLQS1+rIJGfmUyffxu7U
lX2DXpInlHDcIOwq8U4dYpmRqPxx7jXciKZKfBiz5HXnQ+It1rJksoZWqZLw/xvS
QgHrO4H+Ru/2idH1gwHojTlPTWt9+a4RxH9V/fZvz7xfkoH3AUpf93sxoqZSPUm7
uXH5hGic4ECC14Ucmc6TdkMSFw== =CxP7 -----END PGP MESSAGE-----
```

Notice the line right under "-----BEGIN PGP MESSAGE-----" are different in each example. This is because each PGP message was created on a different operating system.

Example 1 was done on a macOS computer.

Example 2 was done on a Windows computer.

Example 3 was done on a Linux computer.

By mistakenly letting others know what OS you're using allows for your adversaries to know what exploits to send you ;)

This is why we're doing everything through a Whonix VM or booting Tails from USB as it takes care of everything for you.

For the people that do everything from your Windows or macOS computer you expose yourself to unknown risks. Use Whonix in a VM or use Tails.

If you were, for whatever reason, using PGP on Windows, macOS, or Linux there's no need to give out any information that can reveal what type of OS you're using. We ensure we're not leaking any sensitive details by using:

**gpg --encrypt --armor --no-comments --no-emit-version -r
PUBLIC_KEY_OF_RECEPIENT**

When using PGP in Whonix or Tails in Terminal we use:

gpg --encrypt --armor -r KEY

Whonix and Tails to strip out all of that information automatically for you. You can see how this information can reveal more to our adversaries and the rationale for not wanting any of that leaked out.

Verifying PGP signed message.

The final PGP OPSec caution to be aware of is when you're signing a PGP message to verify it's you for whatever reason. You want to ensure you put the date in the message and the reason for the signed PGP message to ensure you don't get impersonated on other forums.

For example, if I've registered on a new hacking forum and existing members want me to prove my identity then I would sign a PGP message associated to my public PGP key. This is quite common and totally safe but below is a **bad way of doing it**.

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 Hey guys it's me. You can trust me because you can trust this is a PGP signed message therefor you know whoever signed this message is the owner of the identity/public PGP key in question. -----BEGIN PGP SIGNATURE-----

iQEzBAEBCAAdFiEEcoVWwfJGdDAknFCXi4KbmP2R1f4FAl5ZzxEACgkQi4KbmP2R1f5zQQf+J/EQNcu4FjJC+4IIou6beHORbTt6bU4F27d9UH0+ZWPs3Gmfo1db/pjS85CPQUTjxCHGHoNvIl2UXhKnGZVfDWb9pNhuN+TGvLrvWEEkcALOCOoZ4EgAH9TIjQy+xGooYoM1FO8SIlgzv4LCcgttFMogHglKNGT6jhsJxvNszaHL77GVRaKFT5sRyAj1M+GyJ5rt5BxU18j+CIFxjCBc4h7Qag14G9rSNU+cAqpQQ7QcIahYAABJHg9K4c3Ts6g71+K2Z11YzSo7AHJSEQ31lZwuxlxVnzRf6s6feJtd5wHXL+GV3DEpioKc dbhaV4bzXFe6HT2FBd9hT5GEss8zlg== =tTf8 -----END PGP SIGNATURE-----

To verify signed PGP messages we would:

gpg --verify

Hit enter on your keyboard then paste the whole signed PGP message It will appear as below:

-----BEGIN PGP SIGNED MESSAGE-----
Everything in between these two lines
-----END PGP SIGNED SIGNATURE-----

Then hit enter once and hold "CTRL" then hit the letter "d" on your keyboard.

People can verify your signed message to know %100 it's you since only the public/private PGP key owner can sign the PGP message to prove their identity. However, since we didn't add any date or any information to the PGP signed message anyone can copy our signed message and use it on any forum attempting to impersonate you. So if you're going to verify yourself via PGP then ensure you cover your ass.

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 It's me and today is July 17, 1984.
Send me your BTC now please thanks. -----BEGIN PGP SIGNATURE-----
iQEzBAEBCAAdFiEEcoVWwfJGdDAknFCXi4KbmP2R1f4FAl4fopsACgkQi4KbmP2R
1f7LDQgAqA1+T6IXnukDqgUg5QIO8ZnRM69HSasxy8NzTQSHyQ96PyUO+wSfnNQ9
E4RTWgvFSzKWsd1p3oVplFDHfNmCzLjcliySJuaFhBKXn69J+k4LBt784kI2qGt
p1KIIdIQcfk9ITMFSXX/kciGYpSIEpoGa4NmNUdOzvvYpy2dhHwb8VEQLuhYKQq34
NHSCWcbhVPM5qKhq+o5QeU5uBXUj6TyI7TSxexETsis43WuGohAivich6QjMBIxK
eaigOM/oveWMglpFwZNx2iWdjE4CICY1BDnrjdHaaBCdAJxELzS9Zii3e5aBtypl
M3zR/JmroVxYOZFWc+BEXKGo7jeplg== =c//H -----END PGP SIGNATURE-----

Food for thought.

Importing someone else's public PGP key

Before you encrypt any messages to your drug cartel gang bangers you need their public PGP key to encrypt messages specifically for them. Their public PGP key would appear like mine does:

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBF3OD6MBCACr37u11G9RacINL1P1G6ecoSABaMxYNOO1UDxz1G7fNLiSZi5b
lj+H2HTSnoGBQpg5gFmCUIMnowFK8rMO2o3oWRBsjfumxAoR4iZzKGs9bvQgM+t
as1LvoCBoIifn6kQEcfA2NovLXTg8TL3qW2R8Bz6SJEoyoAXxt5bVepqqwsWQcDo
pPInmoTsBbmMd8kKs3SCrM6kR+WdNKjV+beFvYs/+4U/GiHopAEOF9UZPBG7xwka
R3/DD8Jalpl2doMW4jQs6fuC/PQafJlqmhJpEZvygJ4qvh1UusM1i2/5kGbSeEfG
ZJfb3vfs7ToUcbJC4mK6EySvVepfgUAZ8KeXABEBAAGoHoZ1bnNoaW5lIDxGdW5z
aGluZUBzZWNTYWwslLnBybz6JAVQEEwEIAD4WIQRzRVVZ8kZoMCSuJeLgpuY/ZHV /
gUCXc4PowIbAwUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRCLgpuY
/ZHV/hAvCACEEFkLni6tahk5DWMPLNQKoGTAowbcRjEKIs578IUovbRqlRCA+g6c
snpcdkCYtQ6YhartRCAdSc6/xIJh86DT27besMaKxmTDuxZmfzyjoxdsiY1ifOr7
CioOXl84A4hg5N/9rpb5mZ8LnJsxW51ZsK7YnhrBthBvn2aGtB81C8SLV6kjaHJV
91ncg8zonrmyKPPno+JJilAUNcP+umSgGDEgAXPBlrPxPWf8iPMW2Z557AseNwDm
d2zPmeYLjitv1rV4ryjrYRZBEV6qGBlr25FMgeUPuQCECAJ+bJNW4zoy1esZpd67

```
iRJoO9DQzsG6fj6aFpKLRrjN+R+6EQnKuQENBF3OD6MBCAC14oLykN/lrNgzrDvY
3GSfu4D2puVuDxpb1CZLg7IFkWzPJqDJ3azJBYP7sykC8NFevlzNfOqdP6jDg8fl
hJu4naFnk8cPDOtsssO2yC324m52kJDfEi2hYD8AFSuuKnvMcDDM8PG8VkuDZ9C7
L2J2pqVLfKS7GEhArSzEB/6Ls3b2ZuRS6qXDRebpottf/L1qStcqPDWFenIDlDWV
E/UaDxl3qTebXbdYbIJKR26FKsu2R/DELOOpGoUUkQ5NjnMdbuR/ogEQlWgEOh5c
4mgLJs1BiiZhgDNcUbvY6LDJGykf9AyTMSpjAjsf22H7FET/D1RSIXoLTnj2Nn7l
mRxZABEBAAGJATwEGAEIACYWIQRzRVVZ8kZoMCScUJeLgpuY/ZHV/gUCXc4PowIb
DAUJA8JnAAAKCRCLgpuY/ZHV/pMCB/98M5usyZqNwcddC7F3vgLlb+rwptIkwoHS
ryz2nd4xk+MzMF+EGdcwYRKNgVxy5DLKzvujFO4ZmYfEBnhEa98T/cChL/YSRVO6
sYe4HGvYUXe8oiJ/N3585WqmawXq6fzMzuyK5zuApymJmNkLDpE2dtiCWBMx1koz
7yTJOM4jCdWCyw/337ToBUSb2W9EBSuyqNK8I4hXWtyLNWcjc64mUT/m5+Hc59TM
AcII4M6u12Xy/ODnmTtLol9bh6F4P8WqShucsGLQGm/omqvPkNQpdqC94ODpKSdY
6cGTTBIKbURbh+HaepwyB56w/QR8j6LAmYCLe/2HU1Xo02WOU9m=eoIe -----END
PGP PUBLIC KEY BLOCK-----
```

When you've received a new public PGP key and you want to import it onto your key ring with PGP we then:

Open up terminal

gpg --import

Hit Enter on your keyboard

Paste my whole public PGP key and then hit enter once then hold "CTRL" and hit the letter "d" on your keyboard.

You can now see my key:

gpg: key 8B829B98FD91D5FE: "Funshine Funshine@secmail.pro>" imported

"8B829B98FD91D5FE" is my key needed to send an encrypted PGP message to me.

In Whonix or Tails in Terminal:

gpg --encrypt --armor -r 8B829B98FD91D5FE

Type out your message and when you're done hit enter then hold "CTRL" and hit the letter "d" on your keyboard which will produce the encrypted PGP message to send.

Encrypt a PGP message.

In Whonix or Tails in Terminal:

gpg --encrypt --armor -r KEY

Type out your message and when you're done hit enter then hold "CTRL" then hit the letter "d" on your keyboard which will produce the encrypted PGP message to send.

Remember to send the whole message including the associated headers to your clients/people.

So you would send everything in **red** below:

-----BEGIN PGP MESSAGE-----

Everything in between

-----END PGP MESSAGE-----

Decrypt a PGP message sent to you.

In Whonix or Tails in Terminal:

gpg -d

Hit Enter on your keyboard

Paste the whole PGP message including the proper headers noted in **red**.

-----BEGIN PGP MESSAGE-----

Everything in between

-----END PGP MESSAGE-----

Hit enter once then hold "CTRL" then hit the letter of "d" when done.

You'll need to enter your passphrase for your public PGP key in order to decrypt the message.

You can store your conversations in a .txt file saved in your encrypted Persistent folder in Tails or in your Whonix VM stored on an encrypted USB.

Ensure you backup your shit from time to time!

Anonymous E-mails

You'll eventually need an e-mail addresses to register, sign-up, and communicate with clients, buyers, etc. Always, always, always use Tor to sign up (preferably in Whonix VM or using Tails OS) when creating the e-mail and only use Tor to check that e-mail. From here on in you should not be using any Wi-Fi networks associated to your personal identity. Coffee shops, open Wi-Fi networks, and soon later on in the next course when you learn how to hack Wi-Fi networks are the only networks you should be using to connect to the internet when performing "business" activities. Remember what you've learned from others and the articles you've already read. Learn from others for fucks sake.

If you require a Gmail, Hotmail, or Yahoo! email address some of those email providers require a mobile number in order to sign up. Depending on what and why you require that type of email you'll be needing a mobile device to sign up with. Any provider that requests a mobile number you'll want to use a pre-paid cell phone (burner phone) that can receive texts. When it comes to purchasing a burner phone it's best to purchase it as far from your physical location as possible and ideally wait at least a month or so before activating/using it. This way hopefully the security footage of where you bought the burner phone from is already recorded over. In any event take efforts to disguise yourself when you're buying a burner phone (sunglasses, hats, wigs, etc.).

It's best to stick with email providers that operate on Tor and use PGP when dealing with clients, buyers, associates, etc.

Recommended email providers on Tor:

<http://secmailw453j7piv.onion>

<http://eludemaihlhqfkh5.onion>

<http://mail2tor2zyjdctd.onion>

<http://cockmailwwfvrtqj.onion>

Remember, it's not so much about the e-mail provider being safe as it is about being safe while using email to communicate with others.

Always connect to the email over Tor and use PGP as much as possible.

Conclusion

You should now have a much better understanding of OPSec and be somewhat comfortable with what has been discussed in this course. It's a good idea to read through this course fully before deciding on what to implement. Think things through on what you require and what is needed for your operations. Reading over this course multiple times will help solidify some points and hopefully spark some ideas into your own mind as well.

Becoming a cybercriminal does not happen overnight so make sure you practice these new found skills before you're comfortable with them before doing whatever it is you plan on doing. You crazy fuck.

You want to stay in the know if you're planning on operating at a high level. What I mean is just because you downloaded Tor, Whonix, or Tails last year doesn't mean it's secure so follow cyber related news on Facebook, Twitter, or whatever means you have available. Keep your applications, OS, passwords, systems, etc. updated and to current versions. You need to ensure everything keeps updated and pay attention to dark web news, Tor project, and especially arrests surrounding cybercrime as this is where you'll learn the newest methods used to catch cybercriminals and what's not safe anymore should something be compromised (Tor, Tails, PGP, etc.).

Now that you know how to remain anonymous online, we can begin to build on this foundation and move onto the next course offered at HackTown, Act I - Wi-Fi Hacking.

ACT I will teach you how to hack the Wi-Fi networks around you so you can use them for your own needs. This is another key piece when increasing your OPSec because moving forward your "work" laptop will use other Wi-Fi networks and not your own. We don't want to use our own Wi-Fi network since we know this is a bad idea now yes?!

Lastly, if you're looking at becoming an effective hacker it's best to research "Ethical hacker", "penetration tester", and "pen tester". These are search terms that will allow you to follow up on the "professional" careers in hacking. The point of doing this is to see how professional hackers test certain websites/organizations and begin to adopt their methodologies for your own goals in hacking. You can download the "Certified Ethical Hacking course" from any torrenting website and read at your leisure. It's highly recommended to do so to fully grasp the hacking knowledge used today and will help you greatly.

Hopefully you've learned something from this course and can add another key piece of information to your cybercriminal mind set before unleashing into the wild. Like any course or tutorial this is not perfect so if you see typos, spelling errors, or have any other useful information to add please email me.

To hammer home the points:

- Your "work" computer should never ever have anything personal on it.
- Your host machine should have Anti-Virus or Windows Defender enabled.
- Your host machine should always be kept up to date with current updates.

- Your host machine should have full HD encryption.
- Your host machine should have Glasswire or LittleSnitch installed.
- Your host machine should have booting from USB disabled in the BIOS settings.
- Your host machine should have a VPN running on it.
- Everything should be saved to the USB and never the HD.
- A password manager should be used for storing your passwords.
- VM should be saved onto on a USB/Micro SD and encrypted.
- Whonix VM or Tails OS should be used to conduct all your dark web activities.
- Spoof your MAC and Computer Name every time on start-up and shutdown.
- Use CCleaner, bleachbit, or similar programs on your host machine before each shutdown.
- Be conscious of other devices you may have on your person that are giving away your location (cell phones are not your friends).

This concludes ACT 0 - OPSec.

Until next time my friends. Stay safe.

Funshine