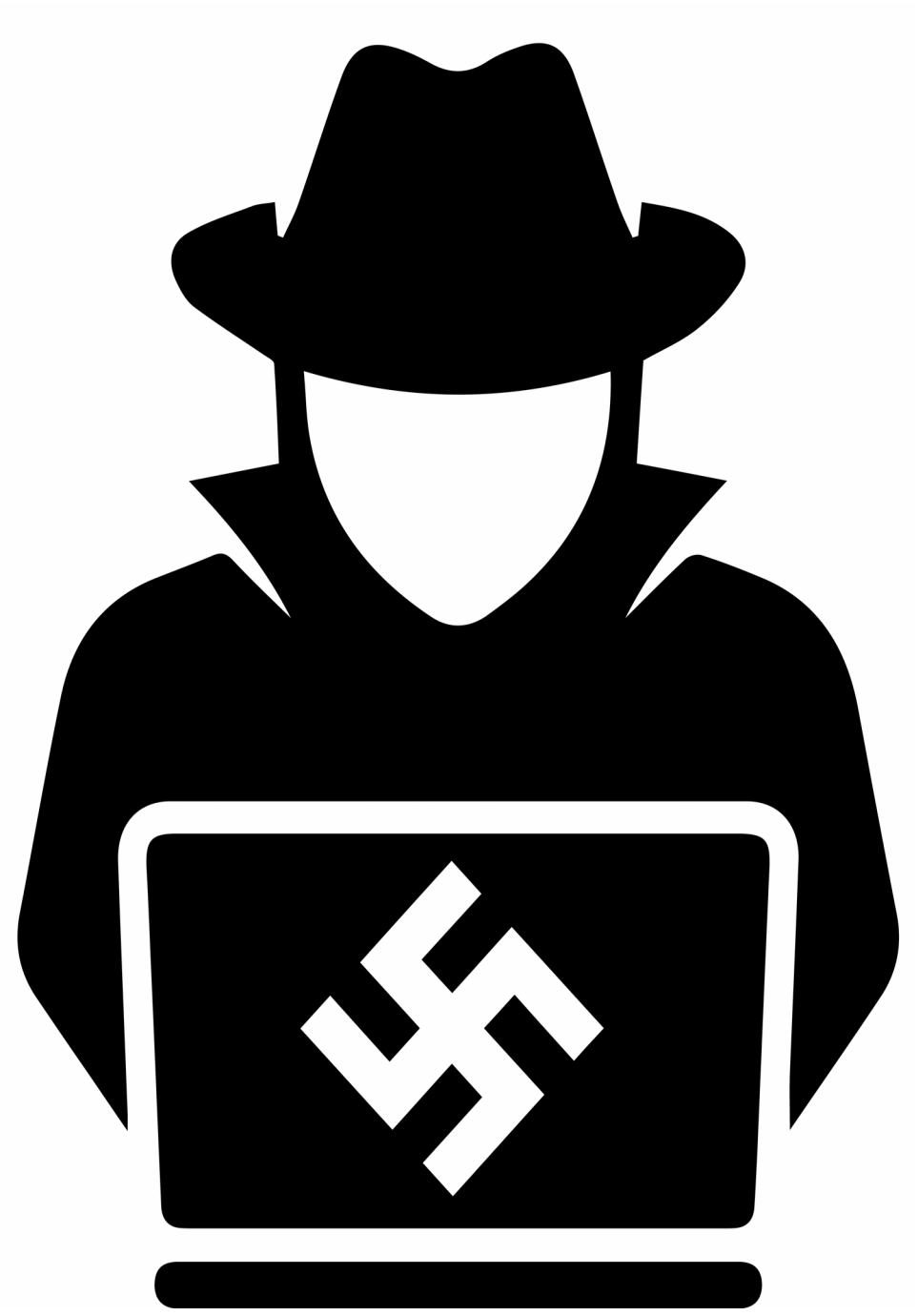
PRIVACY CHECKLIST

A PRIVACY & SECURITY GOYS™ CHECKLIST



BY: OPSECGOY

TABLE OF CONTENTS

INTRODUCTION
WHAT IS THIS?

Welcome! This brief guide is going to be your starting point from normie shit-tier privacy to real dissident far-right opsec. The focus here is going to be on your digital aspect and not so much on real life scenarios.

Who should be reading this? Anyone that does not know where to start with the fundamentals of privacy and security. This guide is going to be basic so if you're a level 9000 autistic system admin reading this, kindly f**k off. This guide is not for you. This is a starting point for the less technically inclined and those that are curious about how to navigate the web with privacy in mind.

The format of this guide will be as follows… First an explanation of each section of the guide going into different levels of detail based on the subject covered. Then at the end will be a checklist you can print off and mark off as you have completed each task. Once complete you will have a very good foundation for your opsec online.

Let us begin!

NORMIE OS
TIME TO BREAK FREE

If you are like most people you are most likely using some form of terrible normie tier operating system (OS). The most popular of these being Windows and Mac. Both are great for normie life and gaming and they're likely what you are used to using, but they are not the greatest at keeping your data safe and secure. These companies are hostile towards whites and you should not expect them to be a safe haven. I recommend switching to some form of Linux. The easiest one for beginners to learn is likely Ubuntu, which you can download for free and burn to a removable usb drive using a tool by Balena called Etcher.

Ubuntu is really not geared towards privacy though and you will find yourself

eventually wanting to move to a better OS. Fedora is another worthwhile OS. If you truly want to be a digital ninja installing a live amnesiatic OS like Tails is your ticket. Tails will load entirely in the RAM of your computer and will not touch the internal storage on the machine. The benefit to this is that once you shut the computer down there is no trace that you were ever on the machine. Also, all of your traffic is routed through the Tor network which keeps your connection reasonably private. If you want something a little more permanent and you are on the paranoid side of things **and comfortable operating a computer using the terminal** then I would recommend installing Artix. One big benefit to Artix is that it does not use systemd which is an issue that we do not have time to cover in this guide.

Once you burn the image file to a removable USB stick you will need to reboot

your computer and choose to boot from the USB drive itself. The methods for this will vary so consult the internet for your particular scenario and try until you find what works for you. If you need help come to the chat https://t.me/privsecchat and someone will be glad to help you. One important thing to note here: if you're opting to install an OS like Ubuntu, make sure you encrypt your drive! There will be a checkbox during installation that says something to the effect of "enable encrypted LVM", **DO THIS!** And create a strong password that you don't forget.

Moving on.

VPN
HIDE THE CONNECTION

Now that you have your fancy new OS installed it is time to hide your internet traffic from your ISP and conceal your true location. Assuming you installed a Linux distro like Ubuntu, or preferrably Artix, it is time to purchase and setup a proper VPN. **This section only applies if you did NOT opt to install Tails.** Oy vey OpSecGoy! I'm going to have to spend my hard earned shekels?! Yes. Relax, AzireVPN and Mullvad are great VPN providers that sell their service for around $5/mo.

Mullvad is great because of how transparent they are and how little information they collect about their users. They do not require any information about you at all really and when you sign up you are give a unique 16-digit account number so that not even an email address is

needed. When you pay there are two acceptable methods, Cash and Bitcoin via XMR.to That is to say, you pay with Monero and they receive Bitcoin via the service mentioned. Mullvad offers both OpenVPN and Wireguard servers. Use the Wireguard servers.

AzireVPN is a little more expensive and requires an email address. The tradeoff here is that they allow you to pay with a variety of cryptocurrencies and they also have wireguard servers. Regardless, get one of these VPN's setup on your device(s) and stop browsing the web with your raw internet.

Important note: If you are trying to not be suspicious make sure you have some normie traffic coming out of your home network. If everything is running through a VPN it is encrypted from your ISP and so you may be scrutinized more if they have reason to start watching your behavior.

For the sake of your security **always** use your VPN on public wifi connections or networks that you do not reasonably trust.

AVOID TRACKING

HARDENING YOUR BROWSER

When you browse the internet you may notice that ads tend to track you around everywhere you go and they seem to know what you are interested in regardless of how many times you clear your browser cache. The reason they can track you so thoroughly is due to a technique called browser fingerprinting. This involves scripts that detect key characteristics about your browser and even your system itself. Things as benign as what fonts you have installed contribute to your fingerprint. So how do we minimize this threat? By hardening your browser!

For this we will use Firefox and Firefox only! **If you have installed Tails you are running the Tor Browser which is a modified**

version of Firefox and so you can also skip this section. So install Firefox on your machine. For the basic config follow these steps…

1. Open the Menu then go to **Preferences.**

2. On the left side click the **Privacy & Security** tab.

3. Change the **Enhanced Tracking Protection** setting to **Custom.**

   a. Check all boxes, **Cookies**, **Tracking-content**, **Cryptominers**, and **Fingerprinters.**
   b. Next to Cookies change the dropdown menu to “**All third-party cookies**”
   c. Set the dropdown menu to “Tracking-content” to **“All windows”**

4. Set Send websites a “Do Not Track” signal that you don’t want to be tracked to whatever you want. Nobody cares.

5. Under **Logins and Passwords** uncheck “Ask to save logins and passwords for websites” and never ever let your browser save your passwords.

6. Under **History** only check the box that says, “**Clear history when Firefox closes**”

7. Check the following…
Block pop up windows,
Warn you when websites try to install add-ons,
Prevent accessibility services from accessing your browser

8. In the “**Firefox Data Collection and Use**” section uncheck everything.

9. Under **“Security”** check everything.

10. Back on the left side menu click the “**General**” tab.

11. Scroll down to the bottom and click the **“Settings…”** button under the **Network Settings** section.

12. Check the box “**Enable DNS over HTTPS**” This will encrypt your DNS queries. Make sure you use a Custom Provider like

https://doh-fi.blahdns.com/dns-query
- or -
https://dns.quad9.net/dns-query
- or -
https://doh.securedns.eu/dns-query

*****For a more advanced setup, download and follow the steps on the ghacks user.js repo.*****

Finally, start using a privacy conscious search engine like https://searx.be and install these add-ons…

uBlock Origin - Finally, an efficient blocker. Easy on CPU and memory.

HTTPS Everywhere - Protect your communications by enabling HTTPS encryption automatically

CyDec Platform AntiFingerprint – Protects you from fingerprinting by deception and obfuscation

SECURE COMMS

ENCRYPT YOUR EMAIL

If you find yourself composing an email for your frens through Gmail, Stop. Right now. Purge the anti-white mainstream from your life. Gmail is going to spy on you as much as possible and when the time comes they will help your government lock you away indefinitely for thought crime. **Do not be lazy here**. You have to get rid of this crap and start fresh.

I always recommend Protonmail and I still stand behind that decision at the time of writing (Early 2020). The thing is you will want to encrypt your email yourself with PGP before sending. Remember to connect to the mail service anonymously. For this I recommend using their hidden service via Tor Browser on a separate

device. Let’s get started with encrypting a message using PGP!

First, you will need to generate a PGP keypair. If you need help with this just ask, or if you are feeling generous you can make a donation to us and we will send you our detailed 46-page guide on PGP. You can also freely search the internet to find answers. I prefer to use GnuPG from the terminal. So I would open a terminal and issue the following command to generate a new key based on eliptical curve cryptography (ECC)...

gpg --expert --full-gen-key

From here you choose **ECC and ECC**
Next, export and store your keys safely. Never give anyone your secret key. If you do they can read all of your messages.

Here’s how I export a secret key…

gpg -a --export-secret-keys > secretkey.asc

Next, export your public key. This is the key you will give out to your boog bros to encrypt your messages with.

gpg -a --export > publickey.asc

Now you will find your keys in the current directory. If you do not know what directory you are in just type **pwd** and press enter.

These keys should be stored in an encrypted fashion on a separate storage device and you should have multiple backups in case of device failure.

Now you need to import your frens PGP key(s). You can find some PGP keys on our directory via the Tor browser at

http://goysec74znsyewq3nu2i3kmwozxptc3lx22jg67km6r2we37ejiaz5yd.onion/pgp.htm

To import their keys you **must first save the key to your computer.** Then issue this command in the terminal…

gpg --import nameofkeyfile.asc

And that is it!

Now you are ready to compose a message. Here is how I do it…

echo "hello world" | gpg -ear jdoe@host.com > encryptedMessage.pgp

Where hello world is the message to encrypt and jdoe@host.com is the email address associated with the public key I want to encrypt my message for and encryptedMessage.pgp is the file the encrypted message will be stored in. Once you enter this command your message will be stored within the encryptedMessage.pgp file. You can either open with a text editor and copy/paste the contents into an email or send as is.

Note: You can also choose the recipient key by the keyid (instead of their email address) presented when issuing the command…

gpg --list-keys

SECURE COMMS

SECURING YOUR TEXT MESSAGES

When you send a text message from your cell phone the message travels through the open air unencrypted. Meta data about the message and the message itself are swept up in a massive dragnet surveillance aparatus that hates you and your people. This aparatus will one day have the technology to quickly scan all the messages swept up in its massive collection and determine who is guilty of crime think. God’s chosen people have also been caught using IMSI catchers to spy on people. You need to fly beneath the radar and stop sending unencrypted messages through the air. It is terrible for opsec and security. Luckily, there are a couple apps that can help out here.

The first and easiest to use is called Signal. This one requires a phone number and I do **NOT** recommend using your real phone number, but instead use a number you have access to. Make sure that this number is not in any way connected to you. Otherwise, you are defeating part of the purpose of Signal in the first place. This only works if the person you are sending a message to is also using Signal. So tell your boog bros to get the app and start sending messages securely. You can also set a self-destruct timer to automatically erase the messages after a given amount of time has passed.

The next application for this is relatively new at the time of writing. It is a fork of the Signal app and claims to be a better version. The app is called Session and it is a decentralized version of Signal which claims to have no idea who you are. There are also some anonymizing

features of the app and the best part is it does not require a phone number to use.

Note: Your mobile phone is one of the most comprehensive surveillance trackers known to man and every year they become even better at what they do. Based on their nature alone cell phones are inherently not private. From cell towers tracking and pinpointing your location and time while logging this data for an indefinite amount of time along with wireless access points being used to track you, you are going to have a hard time being anonymous carrying one of these around. If you are trying to remain completely anonymous it is best to severely limit your interaction with such a device or at least control the information it has access to. This is a more advanced topic to be discussed elsewhere.

VERIFICATION

FAKE NUMBERS

Many services from Telegram to Signal and even some email services require you to give them a phone number so that they can send you a text to verify you are a human. This is another violation of your privacy and the more you sign up using the same number linked to a real person the bigger the trail you create. Instead of giving them your real phone number like a low IQ moron, give them a disposable number.

There are a million different ways to get a disposable number on the internet. From using apps like Quackr TextNow, Burner app and the Hushed app. You can also search the terms “Free receive sms” and you will find a large range of service, but your luck will vary. If you want something a little more serious you can search for

Trial SIM cards. Some cell carriers offer SIM cards that will give you a short term free trial of their service giving you plenty of time to verify the accounts that you need.

DELETE YOUR DOX

DATA BROKERS

Depending on where you live in the world you may or may not be getting sucked up into these massive databases containing the information of millions of people. Any unhinged lunatic that gets wind of your political ideology can simply search for you on one of these websites and suddenly they will have your dox. There is a solution to this problem and that is to request your information be removed from these databases.

A good place to start is with these top data brokers…

1. Acxiom
2. BeenVerified
3. Infotracer
4. Intelius
5. Lexis Nexis
6. Mylife
7. Radaris
8. Spokeo
9. TruePeopleSearch
10. Whitepages

Now that you have removed yourself from the top data brokers it is a good idea to go through the rest of the list at JustDelete.Me and purge your data from the world. This will take a good solid weekend and if you do not have your sh*t together you will end up back in here again.

DELETE YOUR DOX

DELETE OLD ACCOUNTS

Do you remember that old Photobucket account you had back in the early 2000's? Delete it. Remember that old forum from 2010 that you signed up for to discuss [insert random topic here]? Delete the account. All of these accounts can pile up to create a profile of who you are. Establishing interests and a rough idea about where you live can narrow down an investigation quickly so purge your old accounts. They only serve to harm you later. This goes for social media too.

EMBEDDED DATA

REMOVING EXIF DATA

When you take a digital photo or video meta data is embedded into the media. This data is called EXIF data. Mobile phones are particularly notorious for this. Let me brief you on what is going on.

The worst part of mobile phone EXIF data is that it can contain the GPS coordinates of exactly where the photograph was taken along with a timestamp and the model of phone. When you upload images like this to Gmail, Facebook, Twitter, etc… They no doubt scrape this data and store it.

The thing you need to do is turn off **Location Services**. You should do this anyways, but especially for this purpose. To eliminate the rest of this data you can use tools like Scrambled Exif from the F-Droid repo.

ENCRYPTING FILES

VERACRYPT AND HIDDEN VOLUMES

You would not be reading this guide if you did not have the need to protect something. One of the best methods for protecting your data on your computer is to encrypt it. To do this we use **Veracrypt.**

INSTALLATION

If you do not have Veracrypt installed it is as simple as running this command in the terminal:

Debian/Ubuntu

sudo apt install veracrypt -y

Arch/Artix

sudo pacman -S veracrypt -y

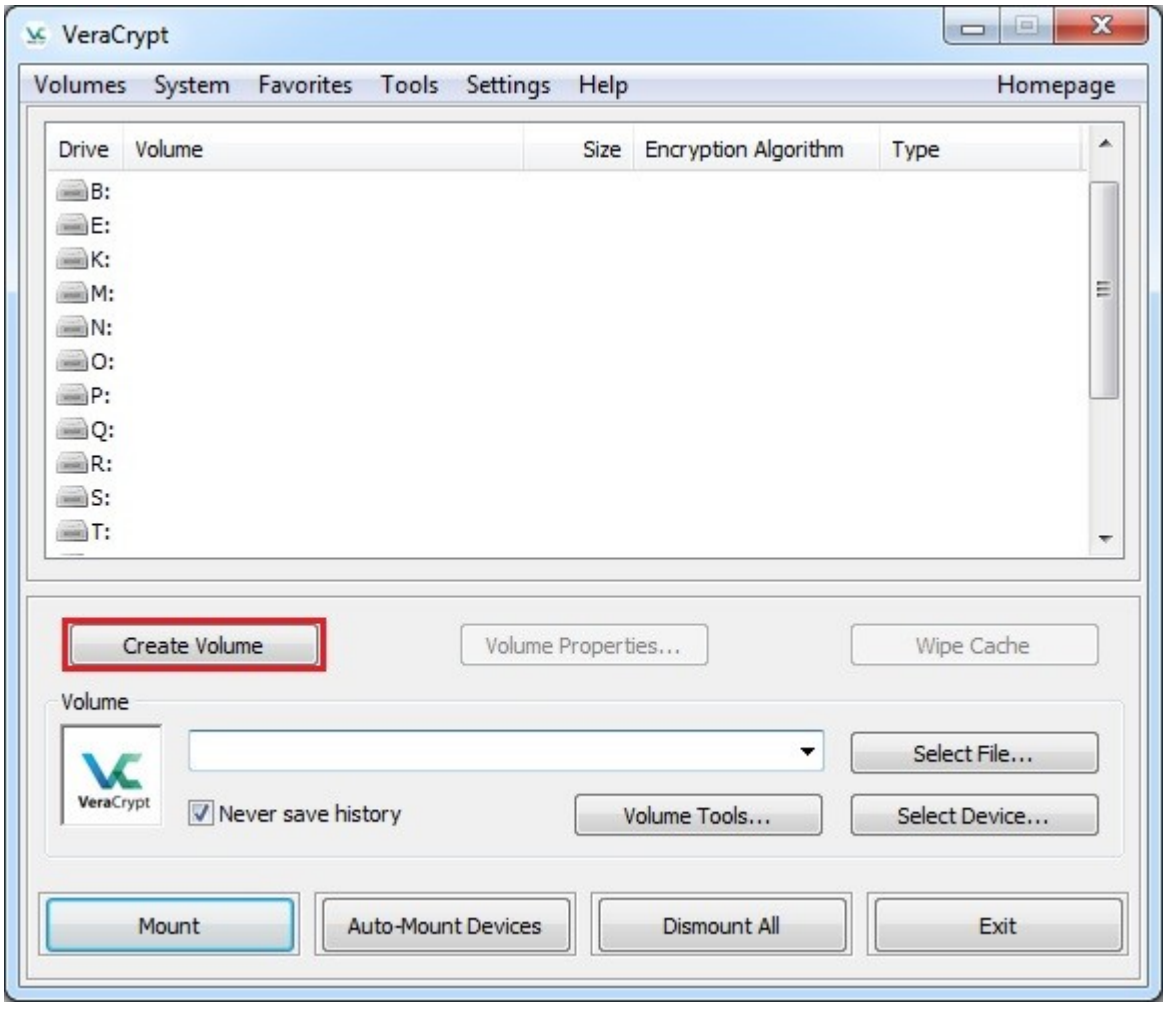
If you prefer, you can also download directly from their GitHub releases page **here**.

SETUP

Note: I stole this from here. Sue me.

1. launch Veracrypt. Either enter **veracrypt** into the terminal and press enter or click the icon in your start menu.

2. Click **Create Volume**



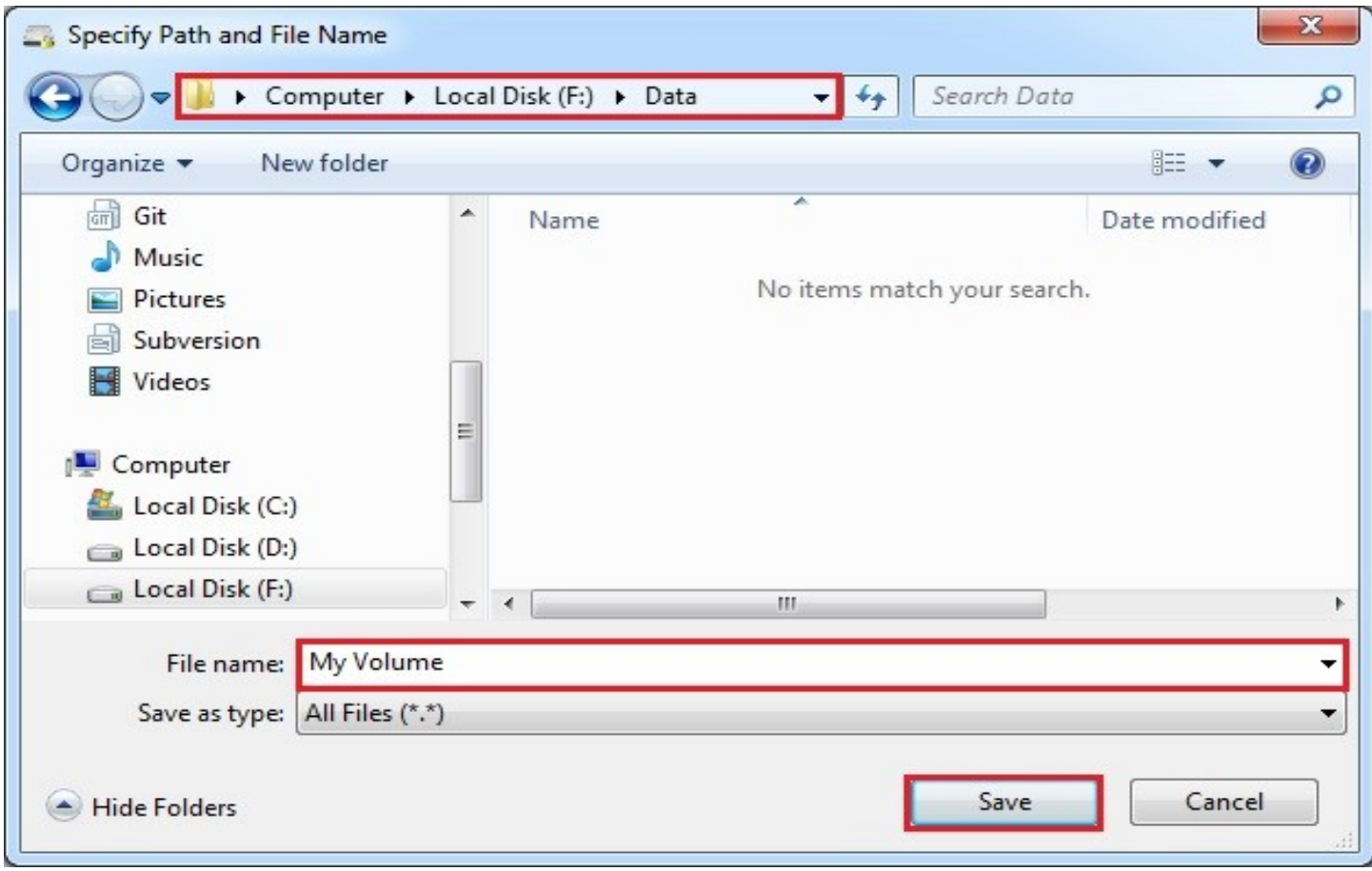
3. The window pops up. Make sure you have **Create an encrypted file** container selected. Then click **Next.**

4.Select **Standard VeraCrypt volume.** Click **Next.**

5. Specify where you want the VeraCrypt file container to be created. Note that a VeraCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

Click **Select File.**

* Note: Make sure **Never save history** is checked

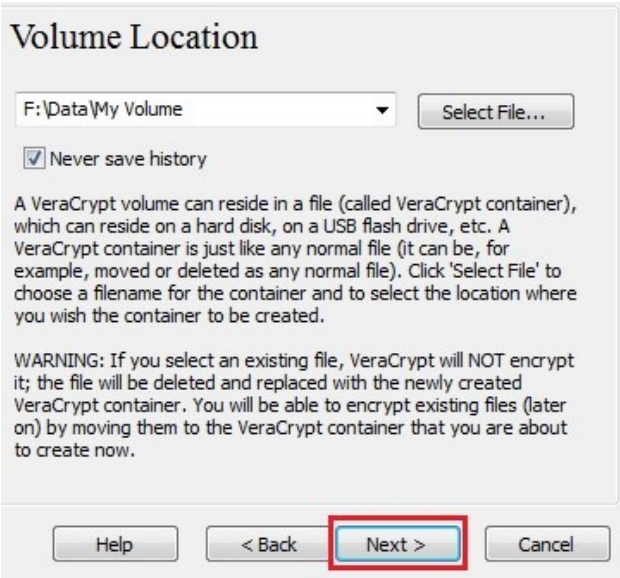


6. Select the desired path where you wish the container to be created in the file selector.

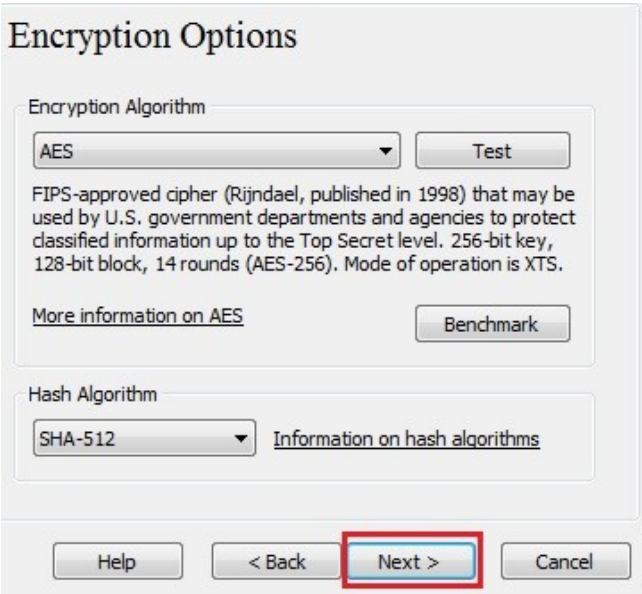
Type the desired container file name in the **Filename** box.

Click **Save**.

* Note: After you copy existing unencrypted files to a VeraCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).



7. In the Volume Creation Wizard window, click **Next.**

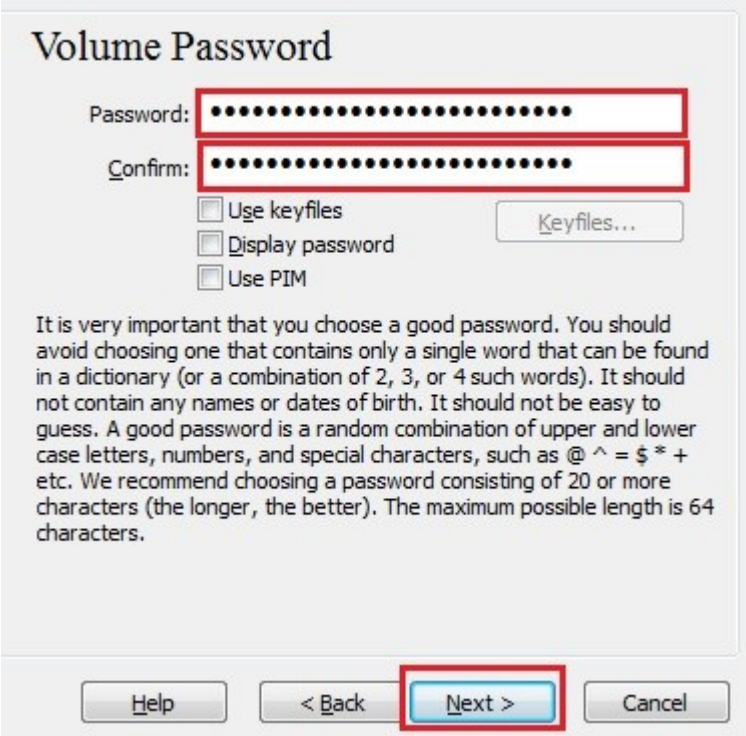


8. Choose an **encryption algorithm** and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click **Next** (for more information, see chapters *Encryption Algorithms* and *Hash Algorithms*).

9. Here we specify that we wish the size of our VeraCrypt container to be 250MB. You may, of course, specify a different size. After you type the desired size in the input field (marked with a red rectangle), click **Next**.

* Note: 250MB is trash. Use something realistic like 4GB or more.

10.

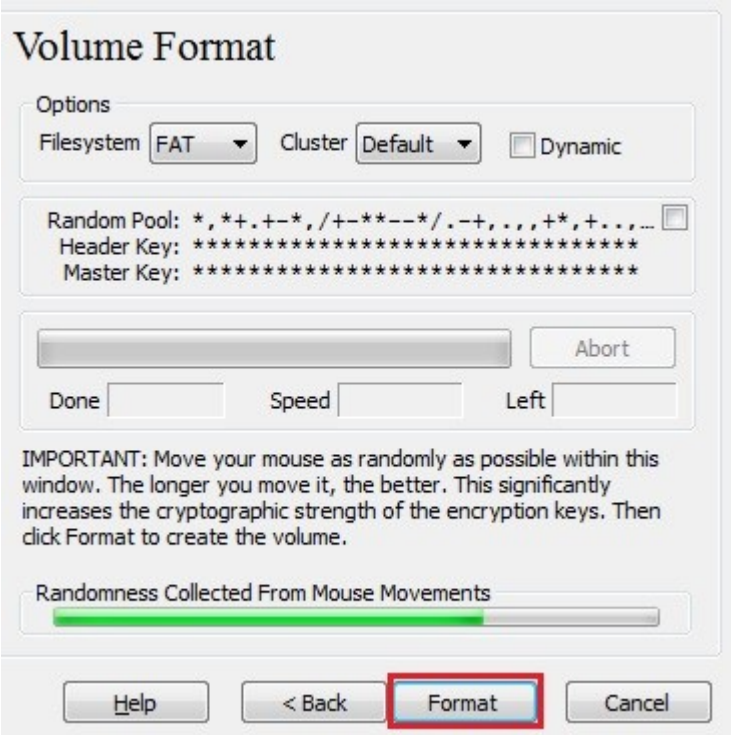


This is one of the most important steps. Here you have to choose a good volume password.

After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click **Next**.

* Note: The button **Next** will be disabled until passwords in both input fields are the same.

11.

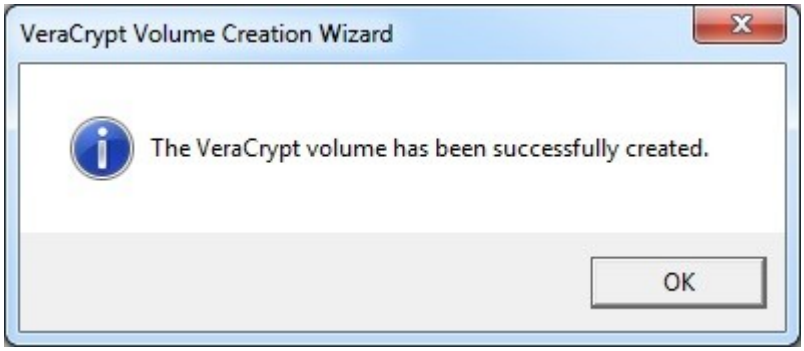


Move your mouse as randomly as possible within the Volume Creation Wizard window at least until the randomness indicator becomes full. The longer you move the mouse, the better (moving the mouse for at least 30 seconds is recommended). This significantly increases the cryptographic strength of the encryption keys (which increases security).

Click **Format**.

Volume creation should begin. VeraCrypt will now create a file called *My Volume* in the folder that we specified in Step 6.

This file will be a VeraCrypt container (it will contain the encrypted VeraCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:



Click **OK** to close the dialog box.

12.

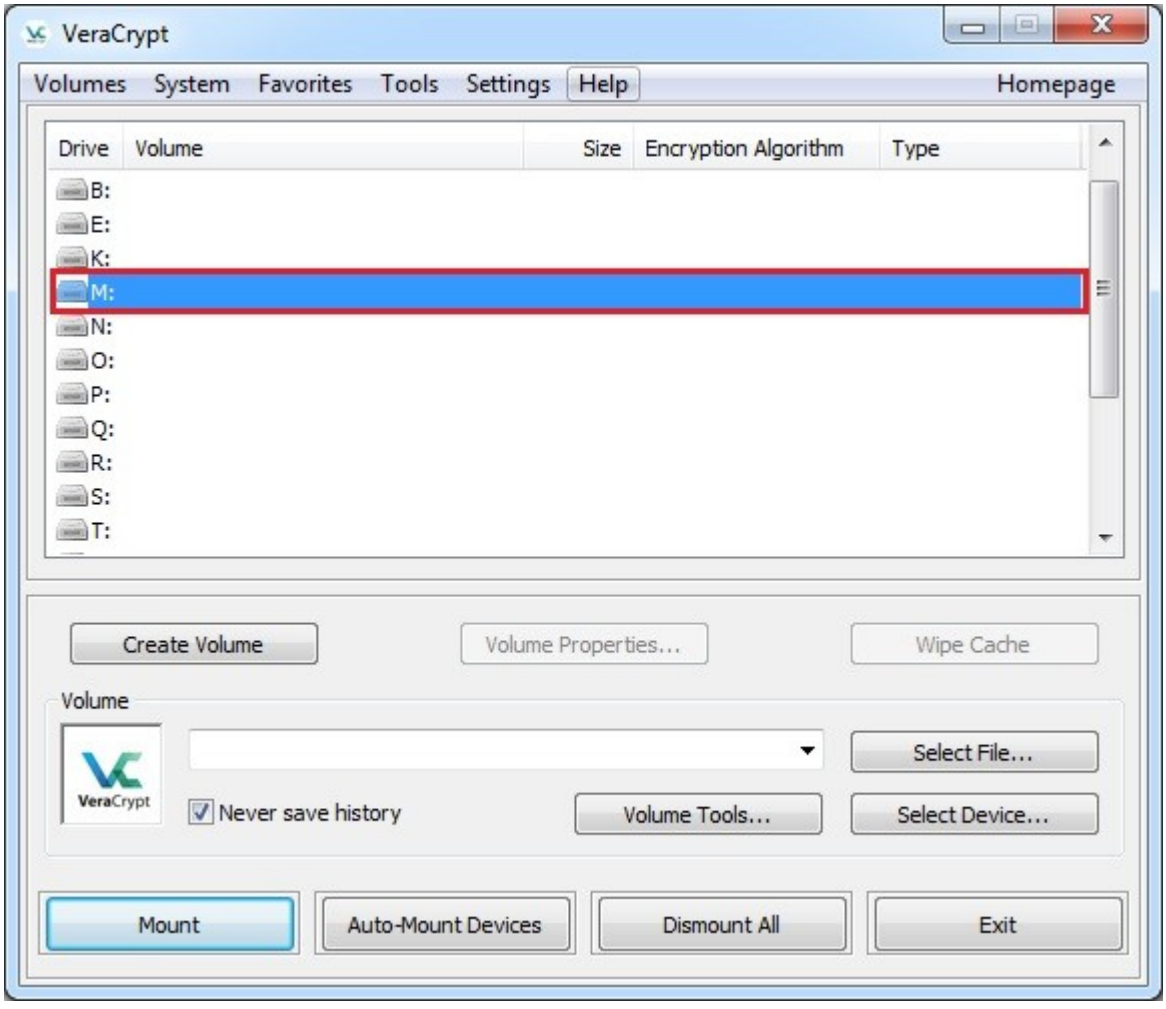
We have just successfully created a VeraCrypt volume (file container). In the VeraCrypt Volume Creation Wizard window, click **Exit**.

The Wizard window should disappear.

MOUNTING THE DRIVE

In the remaining steps, we will mount the volume we just created. We will return to the main VeraCrypt window (which should still be open, but if it is not, repeat Step 1 to launch VeraCrypt and then continue from Step 13.)

13.

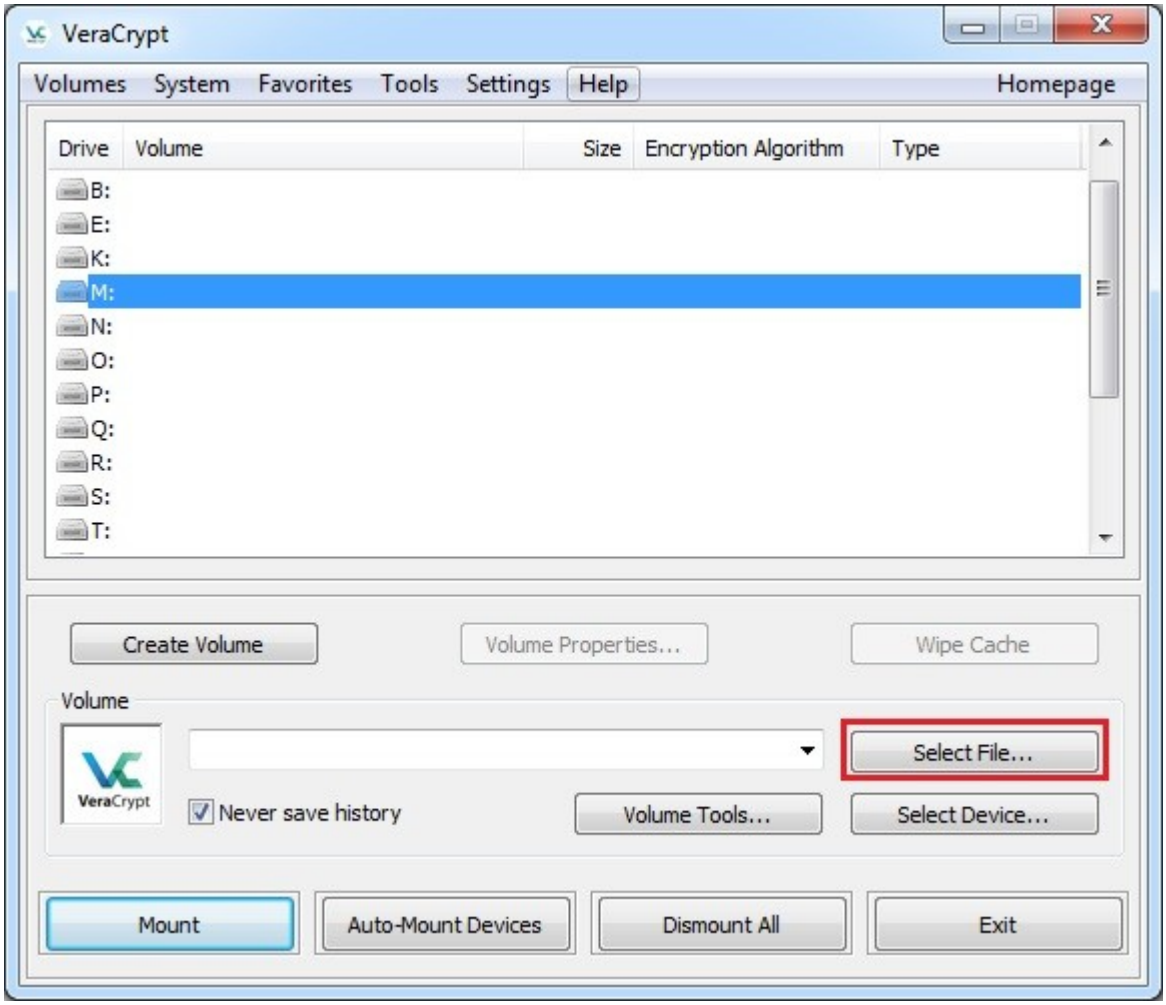


Select a drive letter from the list (marked with a red rectangle). This will be the

drive letter to which the VeraCrypt container will be mounted.

* Note: In this tutorial, we chose the drive letter M, but you may of course choose any other available drive letter.

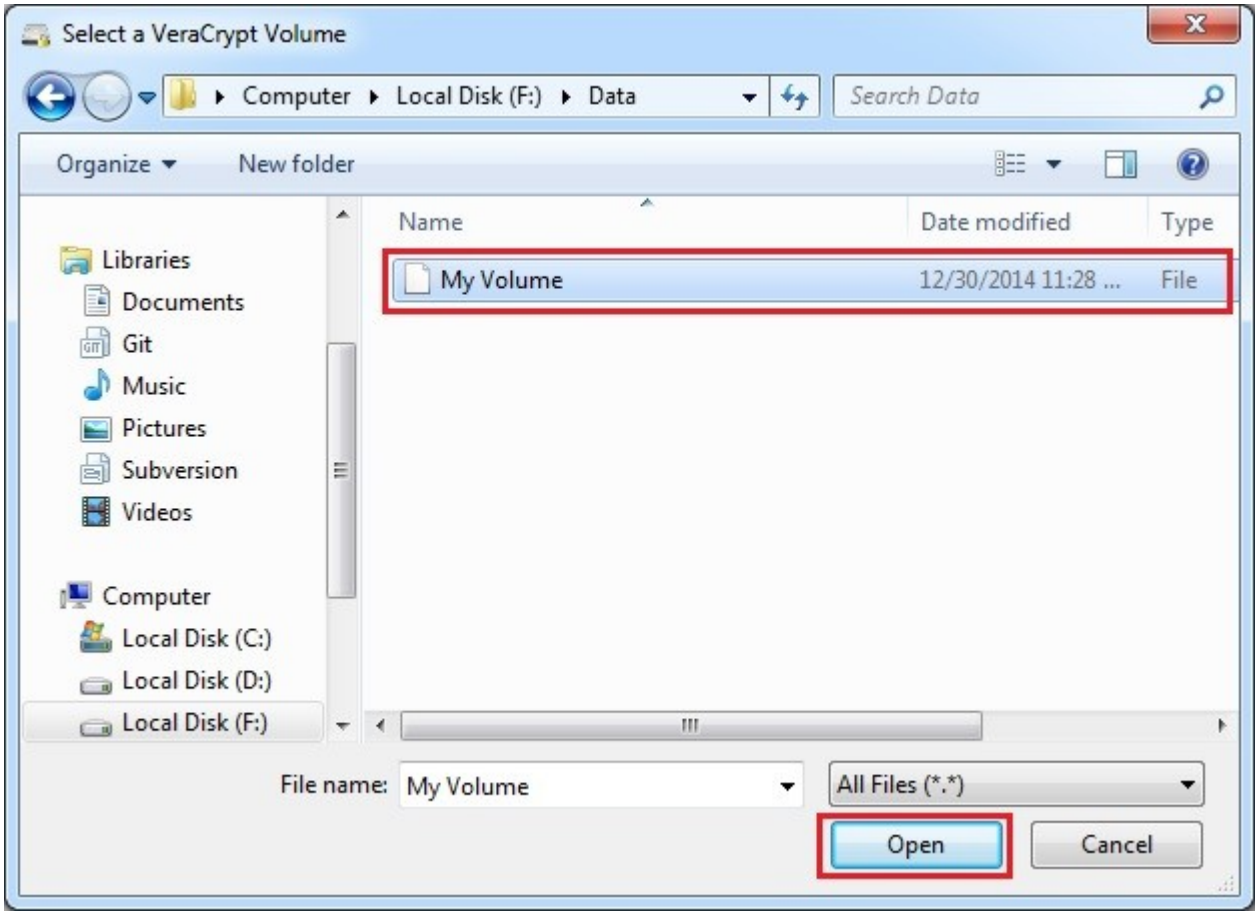
14.



Click **Select File.**

The standard file selector window should appear.

15.

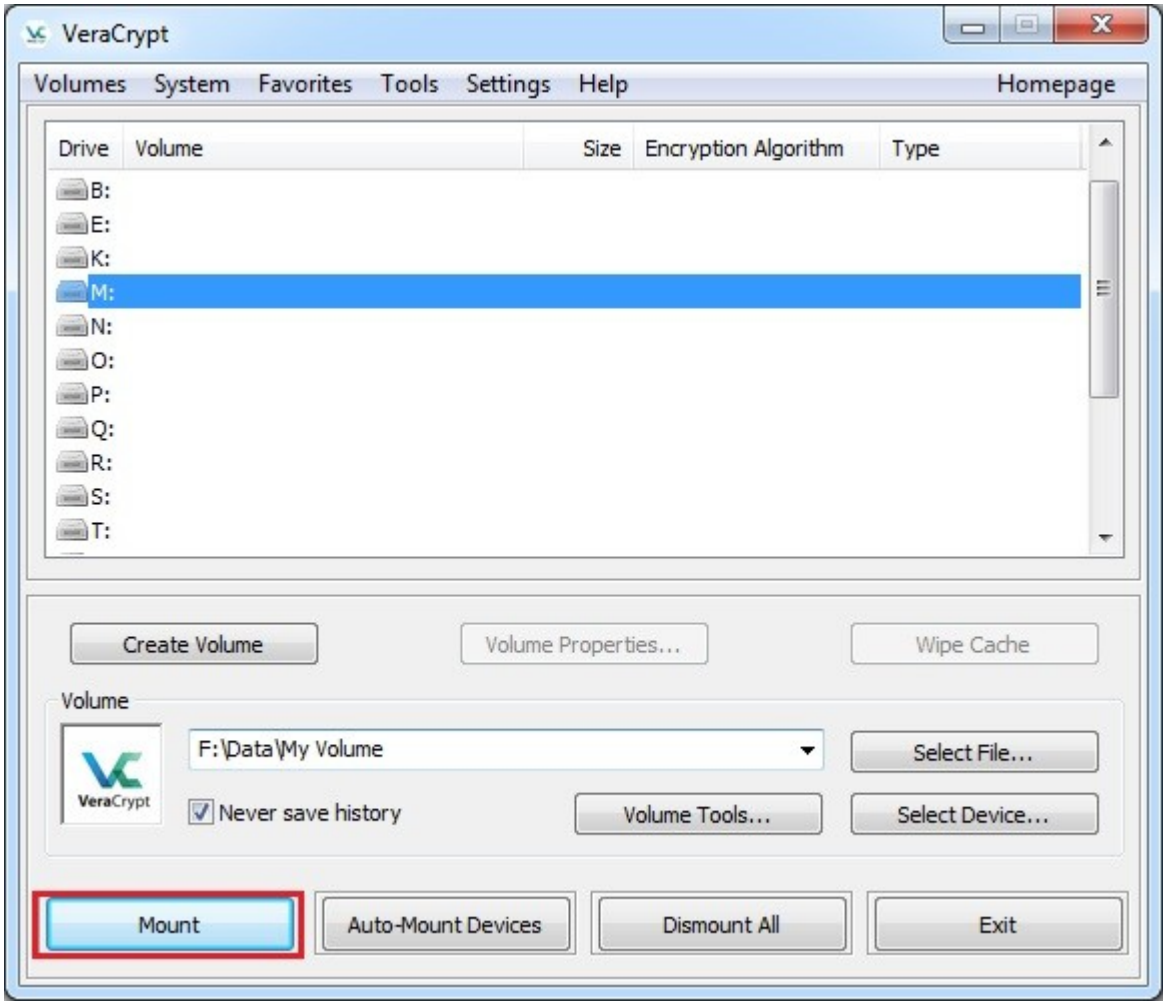


In the file selector, browse to the container file (which we created in Steps 6-12) and select it. Click **Open** (in the file selector window).

The file selector window should disappear.

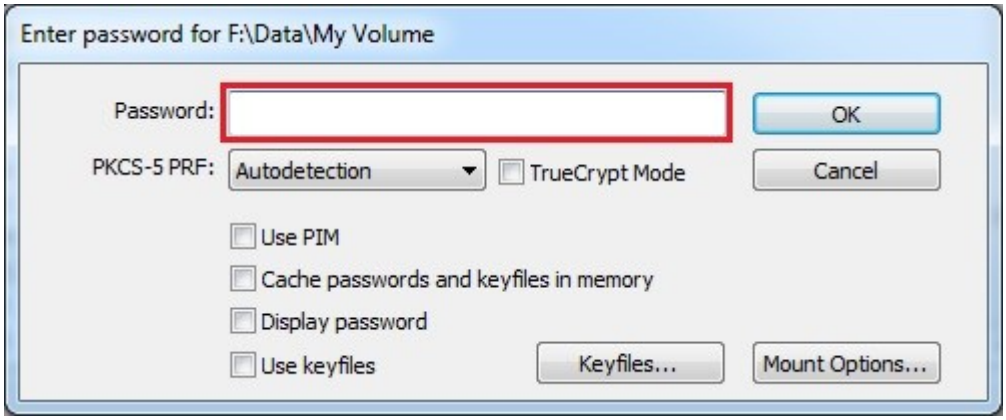
In the following steps, we will return to the main VeraCrypt window.

16.



In the main VeraCrypt window, click **Mount**. Password prompt dialog window should appear.

17.



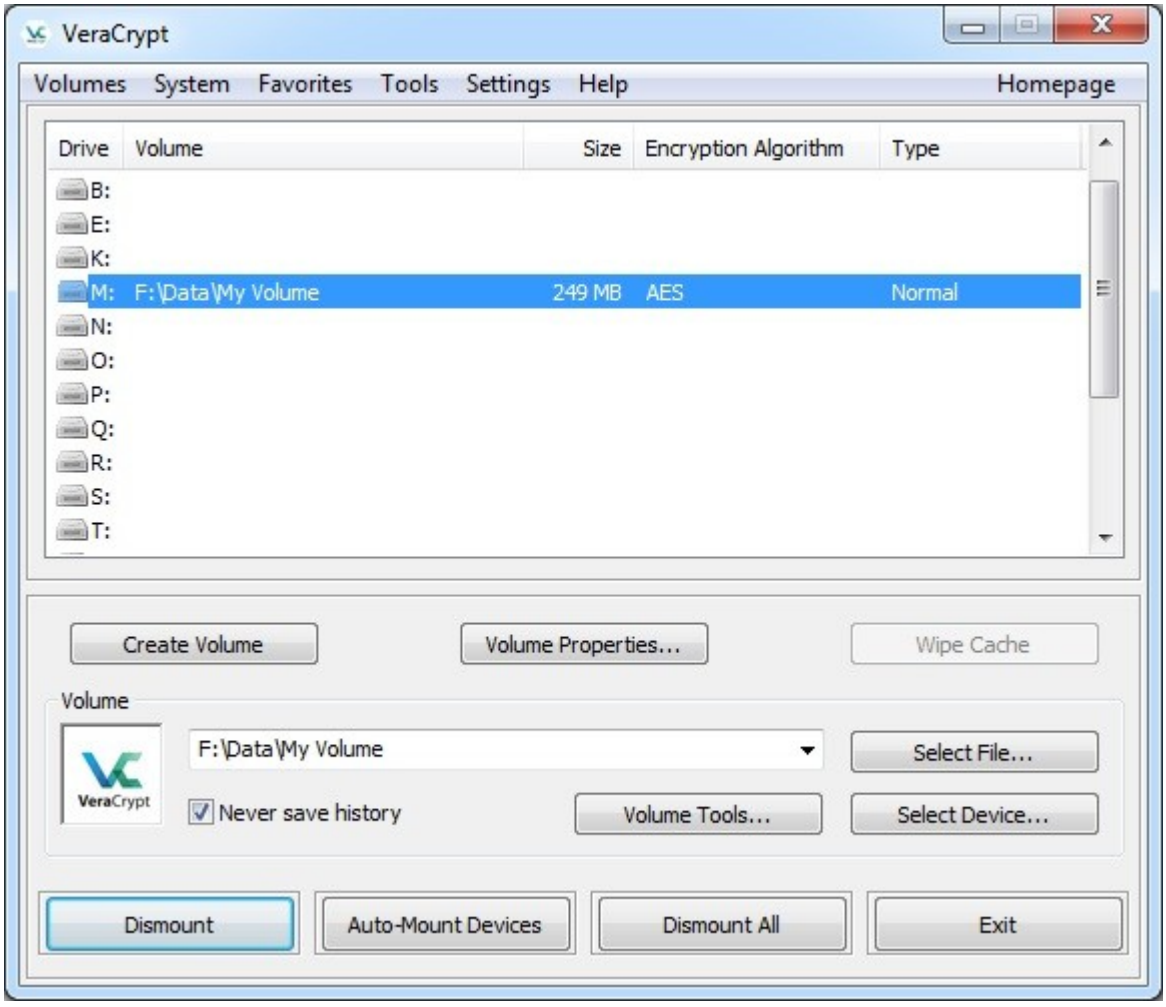
Type the password (which you specified in Step 10) in the password input field (marked with a red rectangle).

18.

Select the PRF algorithm that was used during the creation of the volume (SHA-512 is the default PRF used by VeraCrypt). If you don’t remember which PRF was used, just leave it set to “autodetection” but the mounting process will take more time. Click **OK** after entering the password.

VeraCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), VeraCrypt will notify you and you will need to repeat the previous step (type the password again and click **OK**). If the password is correct, the volume will be mounted.

FINAL STEP:



We have just successfully mounted the container as a virtual disk M:

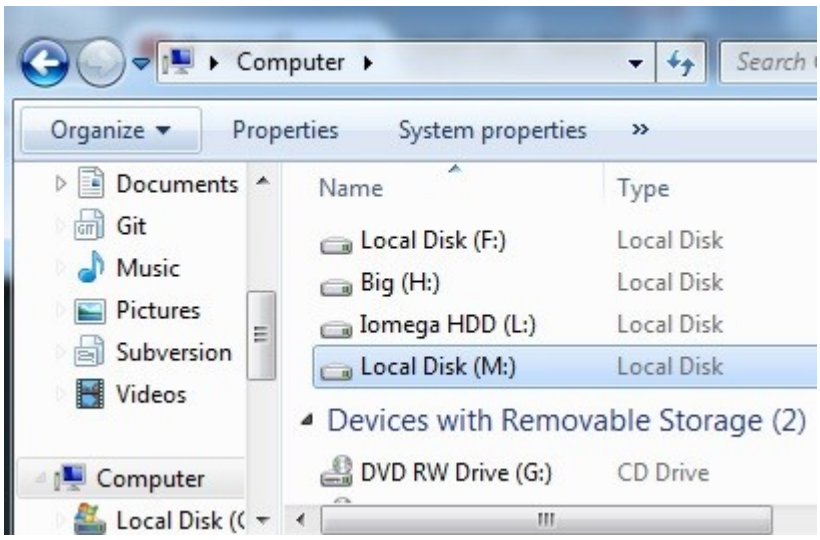
The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.

If you open a file stored on a VeraCrypt volume, for example, in media player, the file will be automatically decrypted to RAM (memory) on the fly while it is being read.

Important: Note that when you open a file stored on a VeraCrypt volume (or when you write/copy a file to/from the VeraCrypt volume) you will not be asked to enter the password again. You need to enter the correct password only when mounting the volume.

You can open the mounted volume, for example, by selecting it on the list as shown in the screenshot above (blue selection) and then double-clicking on the selected item.

You can also browse to the mounted volume the way you normally browse to any other types of volumes. For example, by opening the '*Computer*' (or '*My Computer*') list and double clicking the corresponding drive letter (in this case, it is the letter M).

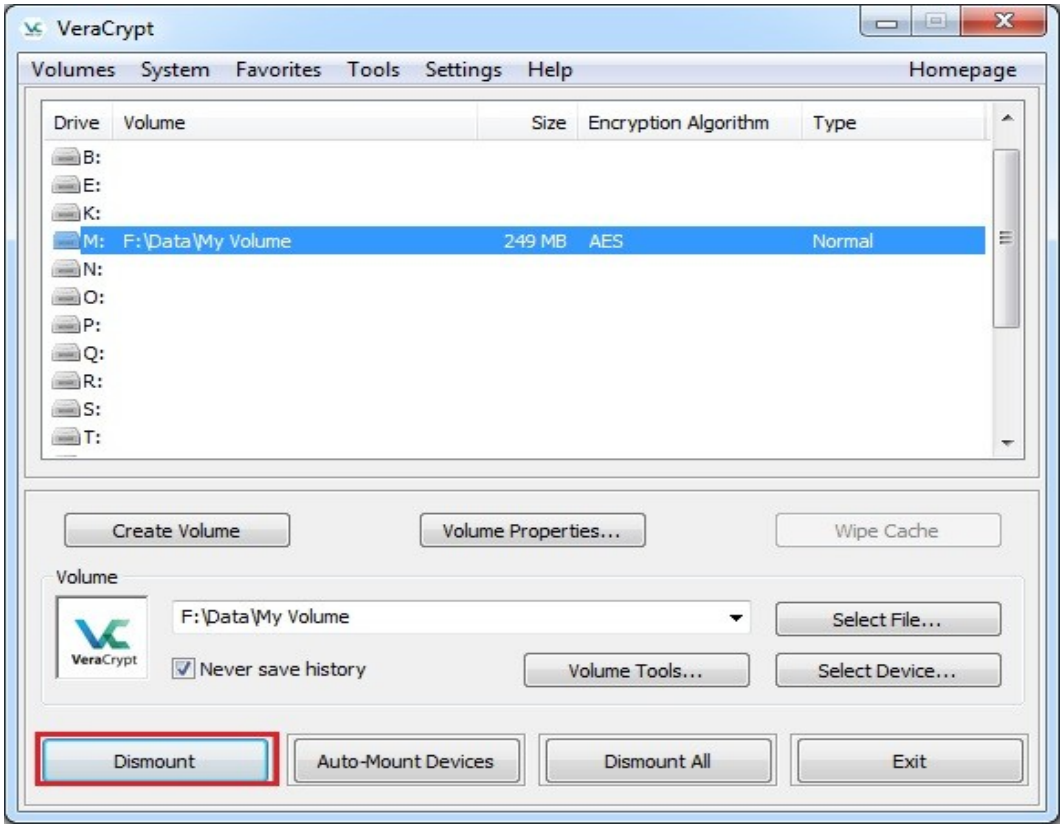


You can copy files (or folders) to and from the VeraCrypt volume just as you would copy them to any normal disk. Files that are being read or copied from the encrypted VeraCrypt volume are automatically decrypted on the fly in RAM (memory). Similarly, files that are being written or copied to the VeraCrypt volume are automatically encrypted on the fly in RAM (before they are written to the disk).

* Note: that VeraCrypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and all files stored on it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), all files stored on the volume will be inaccessible (and encrypted). To make them accessible again, you have to mount the volume. To do so, repeat Steps 13-18.

DISMOUNTING THE DRIVE

If you want to close the volume and make files stored on it inaccessible, either restart your operating system or dismount the volume. To do so, follow these steps:



Select the volume from the list of mounted volumes in the main VeraCrypt window and then click **Dismount** (marked with a red rectangle in the screenshot above). To make files stored on the volume accessible again, you will have to mount the volume. To do so, repeat Steps 13-18.

PASSWORD MANAGEMENT

KEEPASSXC

Instead of using the same two or three shitty passwords over and over again use extremely complicated lengthy passwords and store them all in an encrypted file with an application you can trust. Enter KeePassXC. With this password manager you can generate and store passwords for everything you can imagine. Make sure you protect your password database with a very strong password and have multiple backups of it. Check it out here.

MAC SPOOFING

HIDE YOUR ID

Every device that connects to a network has a MAC address. This address is unique to each device and helps to differentiate between devices on the network. Just by checking the MAC address you can understand the manufacturer of the network card and get a better understanding of who is on the network and what they are doing. You do not want to be tracked or traced back to the network ever.

So you should spoof your MAC address each time before you connect to public wifi networks. There are plenty of tools, the most popular being macchanger. We have also released our own short and sweet open source tool which you can download here.

CONCLUSION

THE MAIN LESSON

The most important lesson to take away from this guide is to compartmentalize your life. That is to say, live your boog life on one device with a separate username, email address, phone number, etc… That is completely unlinked to your normie self. Combine that with some basic privacy tips provided here and you will be much better off. We have witnessed too many of our brothers fail in this endeavour and some have paid the ultimate price because of it. This is an easily avoidable mistake. Below you will find a checklist of things to help you along your journey to increased privacy.

CHECKLIST

1 ___ Install Linux

2 ___ Purchase and setup a VPN

3 ___ Install and harden Firefox Browser

4 ___ Encrypt your emails with PGP

5 ___ Use Signal -or- Session App

6 ___ Use disposable numbers for verification

7 ___ Remove your info from data brokers

8 ___ Delete unused accounts & social media

9 ___ Do NOT post screen shots

10___ Remove and Limit EXIF data

11___ Setup encrypted container (VeraCrypt)

12___ Start using KeePassXC

13___ Spoof your MAC address on public wifi

14___ Split dissident life from normie life

THANK YOU

Thank you for reading this guide! If you found this **free** guide particularly helpful, please consider donating a few shekels our way!

Pro-tip: Before sending any donation to the address listed, make sure you **double-check that the PGP signature** included in the .zip with the document is **valid.**

You can always email me first at OpSecGoy@protonmail.com to confirm.

Thanks again for your help,
“From war to victory!”
-OpSecGoy

卐卐卐

Privacy & Security Goy Hidden Service:

goysec74znsyewq3nu2i3kmwozxptc3lx22jg67km6r2we37ejiaz5yd.onion

Telegram Channel: @PrivSecGoys

Telegram Chat: @PrivSecChat

Monero

44afqsvYK6qeqPsNftcqWeJNSqYjP8jXtFcX2A8AQDKzCR1pusDSUehXNJBCqjmf4oVwd7VsRr2NZVMdEEe6i78ESzYcXWp