General Crash Course in PERSEC

Valkyrie

October, 2016

Contents

1 Disclaimer

By reading this guide, you first of all acknowledge that the information provided herein is subject to change. I cannot guarantee that it is up-to-date by the time you choose to read it. Furthermore, this guide is for educational purposes only and you alone will decide whether or not to apply the knowledge. This too means that I'll definitely not be holding any fucking responsibility in regards to what you choose to do with the information provided in this guide. If it's illegal to read these things in your country - your ass. If you chose to follow the steps in this guide and it didn't work out for you, again - your ass. I only give walkthroughs of the methods that have worked for me. Understand this before you continue to read any further.
Also, about copyright: This guide is free as in free beer.

2 Acknowledgement

I want to express my sincerest gratitude to all the people from the forum, that have halped me put this guide together. Especially Xanatos and Psychlonic for helping me with my shitty grammar and providing me with constructive feedback, you guys helped a lot.

3 Preface

I've written this introductory guide for the current and upcoming users of the NONET forum. I know that some of you take the art of PERSEC very seriously already, but this is targeted for those who don't, or just want to kill some time. For those of you who think "I am untouchable" that may or may not be true, but if the general PERSEC awareness throughout the whole forum is increased it is a benefit to all of us. So if you see someone who is lacking behind in PERSEC, be productive and give the person a friendly heads-up.

We, the NONET members, think that some people out there know of this site but don't visit because they are afraid of increasing the risk of getting caught, even though they might not be doing anything illegal. This guide is here to send a clear message: We care about and embrace PERSEC.
The most important part I want to make clear is that before even thinking about signing up, realize this community is built upon mutual respect. Respect other users and other users will respect you. Remember this: We are Night Oppers, and Night Oppers look out for each other.

4 PERSEC

The word "PERSEC" is an abbreviation for the term "personal security". The practice of PERSEC involves the practitioner to employ techniques that counter threats to personal security. What those threats are is entirely dependent on the activity/area it is supposed to cover. This guide will try to cover some of the most basic threats that could present themselves while using the NONET site.

You might think that PERSEC is an arsenal of tools that you use to protect yourself. This is not true. It is as much, if not even more, a mental state. It requires mental practice to be fully PERSEC-aware and is only acquired by lots and lots of practice.

5 Non-Intentional Disclosure

This section is especially important for those of you who plan to spend some time in the chat.

The NONET chat is a great place, especially when chatting with fellow Night Oppers. Chatting is something different from posting on the forum since it is live and that fact has had impact on many, including me. When you are ready to start chatting, an opening phrase like ”Evening guys” seems fairly harmless at first glance. It is not. As soon as you say ”Evening”, you have revealed something about your location/timezone, unless of course you did it intentionally to mislead. Also, answering to a ”What's up?” question with ”Eating breakfast.” can again reveal something about your location and timezone. This too includes special characters that are unique to your language, your weather, etc.

I could present you with a ton of examples, but there really is no need as long as you understand the basic concept. Even though you are conscious about PERSEC, it can happen that you unintentionally leak sensitive information.

As a conclusion, please think about what you are saying whilst chatting and be careful that you don't talk about stuff that is unique to your current real location.

6 Stylometrics

Everyone has a distinct way of talking. You may not notice, but the chance that you have a set of words which you use very regularly is very high. This means that you can be identified by the way you talk/write. This does also include misspellings/typos, which you are prone to repeat.

For example, when I enter the NONET chat I usually start off by saying one of these two phrases: ”Yo.” or ”Yo tho.”. This is something I repeat over and over, and even if I didn't log into the forum before visiting the chat, people would still have a pretty good idea that it would be me if I started out with one of those two phrases.

Keeping this in mind is especially important if SHTF(”Shit Hit The Fan”), you had to delete your account and now you want a new one. If you create a new one and still talk the same way, people will have a pretty good idea of who it is.

If you are new to the site this is not that important. Although if you have spent a lot of time on other forums this should be taken into account too, since a determined adversary could then cross-reference your stylometrics across multiple sites.

7 Username, Password and Email

A determined adversary, that has a fair amount of time at his/her disposal, can dedicate themselves to try and find out everything about you. This will most likely involve a search for your Username. The same goes for an Email. So, to mitigate these risks the practice of compartmentalization is a very good option. Imagine that you put your NONET account in a box, and that box will never contain anything else. It is from such a standpoint you should create your NONET account.

Before creating an account on the NONET site, you should ask yourself the following questions, and they should all be checked off:
1.0 I have chosen a Username that I haven't used to sign up to any other services.
2.0 I have chosen a Username which is not totally unique, since that will make it easier to track.
3.0 I have chosen a good, long password. This password contains both upper-case letters, lower-case letters, numbers and special characters.
4.0 I have never used this password to sign up to any other services.
5.0 I have used an Email that has never been used for any other services.
6.0 The Email's password and the password for my NONET account are not the same.

If you are in doubt about how to create strong passwords, I recommend the following article by the Boston University, which covers exactly this matter: `http://www.bu.edu/infosec/howtos/how-to-choose-a-password/`

8 Meta-Data

Almost every file has some form of meta-data. This meta-data is there to tell you about some of the file's most basic attributes. This could include size, date of creation etc. A problem with this meta-data is that it can contain some very sensitive information. For example, some smartphones and even digital cameras will provide the time and GPS-coordinates of when the file was created.

In this section, I will try my best to explain to you how to sanitize files before uploading them to the forum. This could for example be applied when uploading a picture to complete a Dare Op.

The tools used herein are Exiftool and MAT. It is strongly encouraged that you sanitize any files before you upload them to the forum to further safeguard your own security.

Exiftool: `http://www.sno.phy.queensu.ca/~phil/exiftool/`
MAT: `https://mat.boum.org/`

8.1 Windows

NOTE: *I have only tested this in Windows 7 32bit but should be the same process for any Windows version.*

Download the Windows executable from the homepage and put it into your desired folder. For simplicity, I'll place it on the Desktop.

Press the Windows icon − > Type: "Run" and press Enter. A little box will appear, and in here you need to type "cmd" and press Enter again. A black window will appear where you are prompted to type any given text. Type "dir", press Enter and all the files in the current directory will be listed. Now you can open the File Explorer to identify exactly where it is located.

The file on the Desktop should be named "exiftool(-k)". You have to remove "(-k)", so that it now is called "exiftool". Go back into the cmd window, type "cd Desktop" and hit Enter. Now type "dir", hit Enter and check if the file that you need to sanitize is listed. If it is not, move it to the Desktop. If it is, then you can start sanitizing it. Type the following into the cmd window: "exiftool.exe -all= picture.png" and hit Enter. This can be any file, given that Exiftool supports the format. This is just an example.

Exiftool will create another file called "picture.png_original", which is a backup of the old file. This can be deleted and now you have the file you started with, including the same filename, on your Desktop. This is now sanitized and ready to be uploaded to the forum.

8.2 OSX

Download the .dmg file from the homepage. Once downloaded, follow the guided installation process. When it has been installed, go to Applications − > Utilities − > Terminal. The directory you start in is your /Users/*user* directory. Let's say that the file you want sanitized is on your Desktop, then you simply type 3cd Desktop4 in the terminal and hit Enter. The process of removing important meta-data from here is fairly simple. Type the following into the terminal and hit Enter: "exiftool -all= picture.png". Exiftool will then create another file as a backup named "picture.png_original". You can delete this file since that still contains the meta-data and therefore is useless. The picture that has been sanitized will have the exact same name as when you started.

8.3 GNU/Linux

For Linux users, you can use Exiftool if you want but I find MAT, at *mat.boum.org*, much more convenient. It has a GUI and is integrated into some File Explorers like Nautilus. If you use MAT, the process is dead-simple. Open it up, add the file, select it and press "Clean".

If you want to stick with Exiftool, then it can be installed using your package-manager or downloaded from their website. For executing a sanitation, the commands are the same ones used for the OSX steps.

9 Tor Browser Bundle

The Tor Browser Bundle("TBB") is one of the best possible tools out there for anyone that is looking for some degree of anonymity. You might have heard of the Tor network, but this is something more with some extra and very nice features included. TBB is brought to you by the same people behind the Tor network and it is a browser with the Tor network integrated.

In a lot of cases, it is possible to connect to the Tor network by other means than TBB. For instance, if you have a router with custom firmware running Tor. These kind of techniques can be very effective if you know what you're doing. Since this is an introductory guide, I'd advise you to stick to TBB instead of using your own browser etc, unless you feel confident enough about networking/routing and feel you have the skill to set such things up without compromising your safety. Then you can do whatever pleases you at your own risk and skip this section.

If you read this and you are fairly new to these concepts, you should realize that the people behind TBB have put a lot of time and energy into this browser. Hardening it and thereby increasing safety and anonymity for its user. There are a myriad of different ways to attack a machine, and TBB does everything it can to counter many of these attacks that threaten your personal security. TBB will mask your IP address and encrypt traffic such that your ISP won't be able to see what you are doing. The ISP will however be able to see that you are using Tor. If this is a problem for you then you should research "Tor Bridges", which does a great deal to counter things like an ISP blocking Tor traffic.

The last risk that comes with using Tor is the way it routes your traffic. The way Tor essentially works is to route your traffic through several other users'/nodes' Tor session. All you need to know is that your encrypted traffic stays encrypted when going from your machine to the last user/node. There it is decrypted. If this last node("exit node") is compromised and is capturing your traffic, they will be able to see the contents but still have a hard time telling where it comes from. Keep this in mind whilst using Tor/TBB.

To install the TBB, just go to their website here: `https://www.torproject.org/projects/torbrowser.html.en` and download the package that is appropriate to your system. There is no need in giving you any instructions on this, since it does almost everything by itself. Once running, click on the little green onion icon and then select the option that says something like "Privacy and Security Settings" in the drop down menu. It'll show a bar that indicates what level of security you wish. This setting should be set to the highest possible and nothing else. That's it! Everything you do in that browser is now routed through the Tor network.

You can have other programs route their traffic through the same connection to the Tor network. You need to find the given applications Network/Proxy settings, which I'll leave as a quest for you. When this is done, you should be able to select "SOCKS" options. As IP address, type 127.0.0.1, which is your own machine("localhost"), and as port 9150.

You can check and see your own IP at: `https://wtfismyip.com/`. It'll notify you if you are using Tor.

There are some guidelines to follow, whilst using the Tor network/TBB. These guidelines go hand in hand with the concept of compartmentalization.
1. Never log into any personal account, like Facebook, when using Tor.
2. Any account created using the Tor Network must never be used outside the Tor Network and vice versa.
3. TBB does not protect against malware etc. If your machine is compromised with for example a RAT, your anonymity will crumble regardless of the use of TBB. Keep your machine clean.
4. If you have multiple accounts at different sites, remember to use the "Change Identity" feature in TBB when switching from one account/site to another.

It is strongly encouraged that you use TBB or the Tor network when accessing the NONET site or any other site where PERSEC is of utmost importance.

10 Virtual Private Network

This will be a fairly short section, since I expect you to put some of your own time into researching this. Setting things up like these are most often idiot-proof and therefore this section will be more about good VPN service-selection and usage.

A Virtual Private Network(”VPN”) is a remote server to which you route your traffic. Just like TBB, a VPN is used to encrypt your traffic, starting at your machine and then being decrypted at the VPN’s servers again before it’s sent out to the desired location. It will mask your IP, making it show as the one of the VPN server.

There are a lot of VPN services out there, and some are free. If you ever see a ”free” VPN service, this should immediately have alarm bells ringing in your head. There is a saying: ”If you’re not paying for the product, you are the product.” This means that if the service is free, they are most likely selling all of your data to third parties.
Here’s a checklist for choosing a VPN service:
1. No-logging policy. They should be serious about never logging anything.
2. Not based in the US, UK, AU, or NZ.
3. Servers in privacy-friendly countries like Switzerland, Iceland etc.

My favorite place for looking at good VPN services is at `https://www.privacytools.io/`. I strongly recommend you to visit this site, read and absorb everything.

When paying for a VPN service, the best solution would be to pay with Bitcoins. If you wish to do so you’ll have to do your own research, since that is way beyond the scope of this guide. Pay for the VPN with a credit card at your own risk.

A VPN service that I recommend is AirVPN(`https://airvpn.org/`). They have good reputation and offer features that integrate the Tor network, such that your traffic can be routed through Tor, then the VPN and then the clear. Or the other way around. If you decide upon this service they have good tutorials, covering installations on almost any device.

If you have a VPN setup ready, you should choose to connect to a server that is located in a privacy-friendly country. I would say that to have at least some PERSEC, you should as a minimum use VPN or Tor, maybe even both at the same time. Using any service or site like NONET with your real IP is just plain stupid.

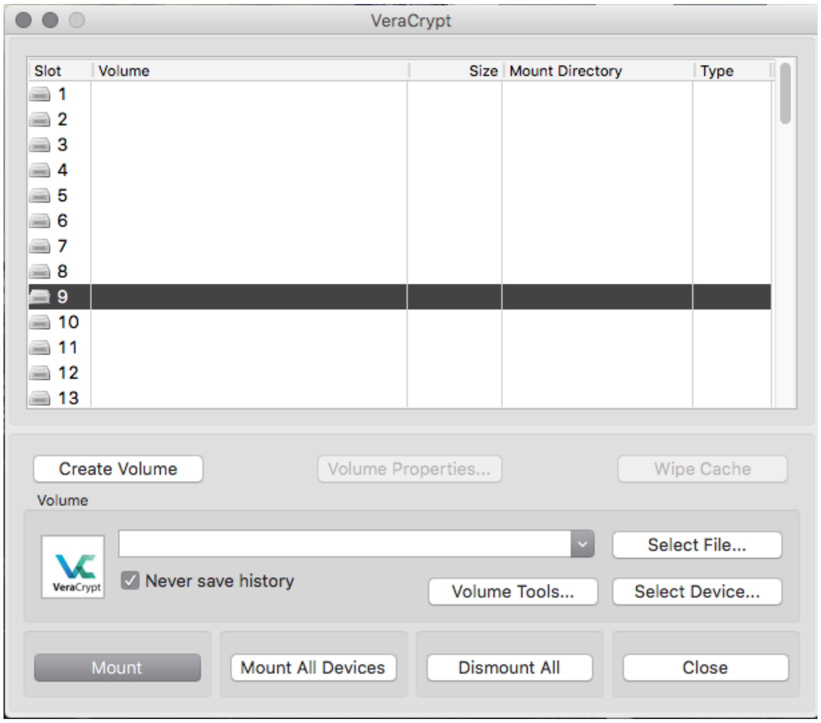
11 Sending Files

Every now and then, it happens that you need to send a file to another user on the site. To avoid that your private files are exposed, even if your account should somehow get compromised, you should encrypt these files before sending them to anybody. Here you would set up an agreed-upon password with the user that is supposed to receive the documents. I suggest using the chat's whisper function to do so but even better would be with other communication platforms.

In this part I will walk you through how to make an encrypted "container" to put your files in before sending them. The tool to do so is the one called VeraCrypt(`https://veracrypt.codeplex.com/`). This tool is based on TrueCrypt and is very useful for especially these kind of situations. It is a cross-platform tool and the steps used are the same across all operating systems.

Step 1

1.0 Grab a copy of the latest VeraCrypt package which fits your system.
1.1 Follow the guided installation.
1.2 When installed, start the application by clicking it's icon.
1.3 This is the first thing you'll see:



VeraCrypt

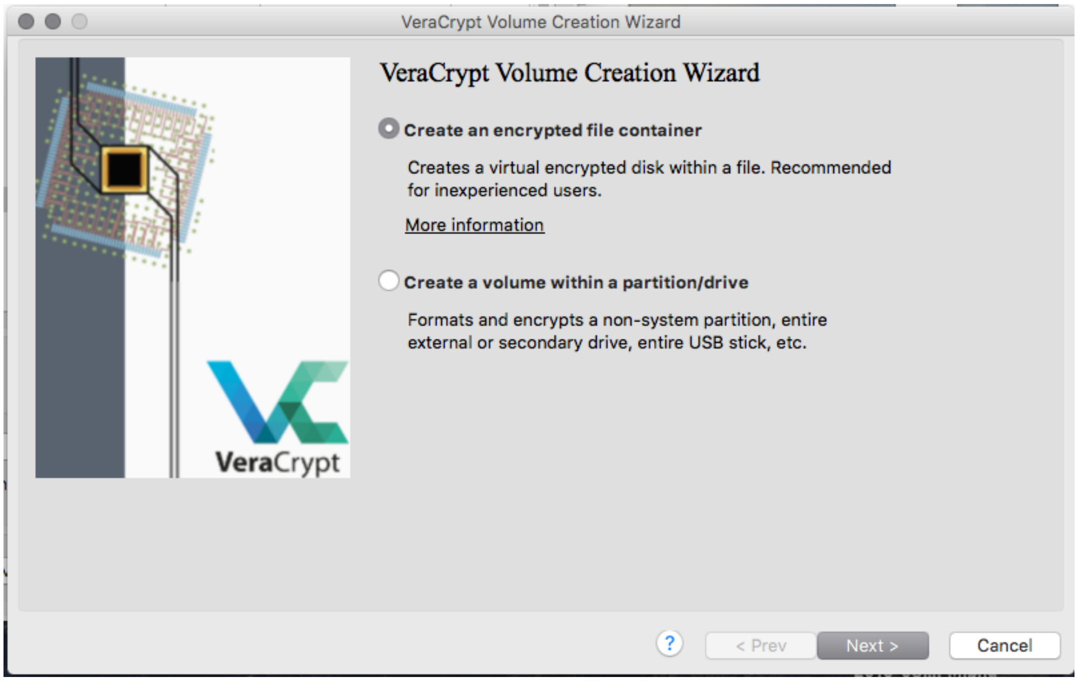
Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

Volume

☑ Never save history

Step 2

2.0 Now press the "Create Volume" bottom on the left.
2.1 Next thing you'll see is this:



VeraCrypt Volume Creation Wizard

VeraCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

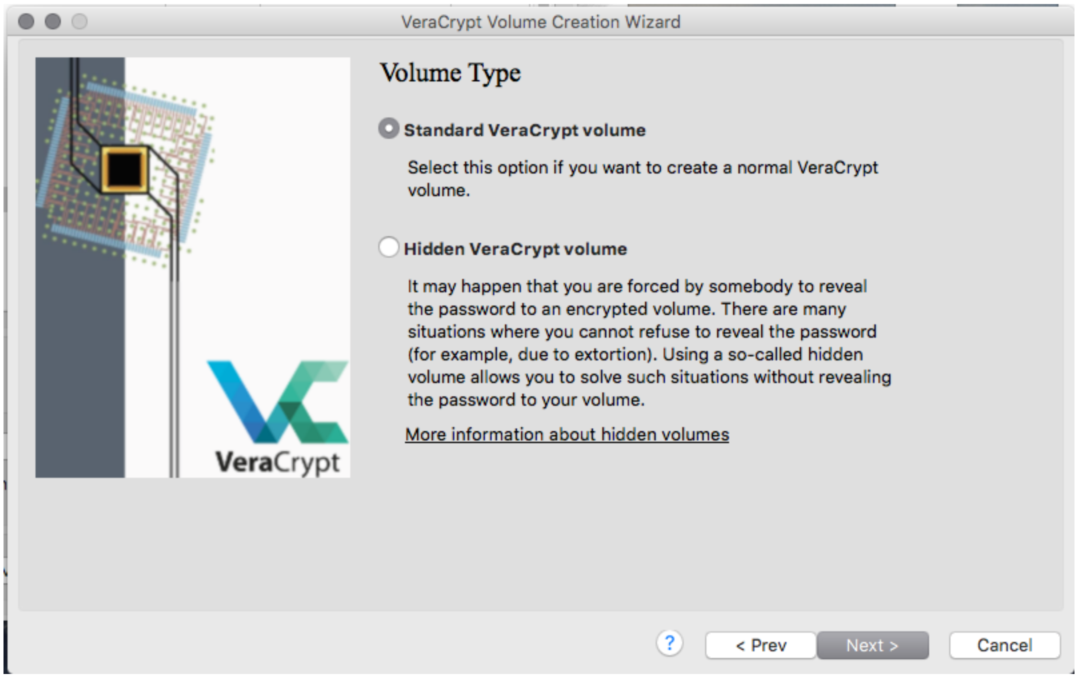
More information

○ Create a volume within a partition/drive

Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.

Step 3

3.0 Select ”Create an encrypted file container” and click ”Next”.
3.1 This will pop up next and you should have the option ”Standard VeraCrypt Volume” selected.



VeraCrypt Volume Creation Wizard

Volume Type

● **Standard VeraCrypt volume**

Select this option if you want to create a normal VeraCrypt volume.

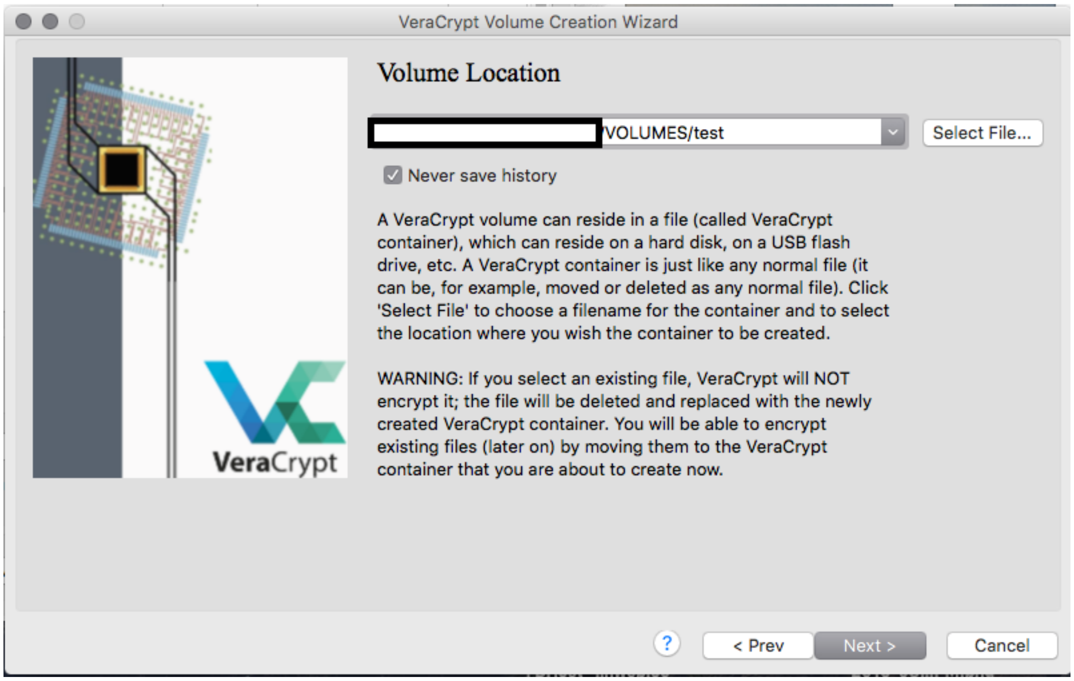
○ **Hidden VeraCrypt volume**

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

Step 4

4.0 Next you will be given the option to select where the container should be saved. Click ”Select File...”, browse to the directory where you want to save it and give it a name. I have called mine ”test”. When this is done, click ”Next”.



Volume Location

[redacted]VOLUMES/test

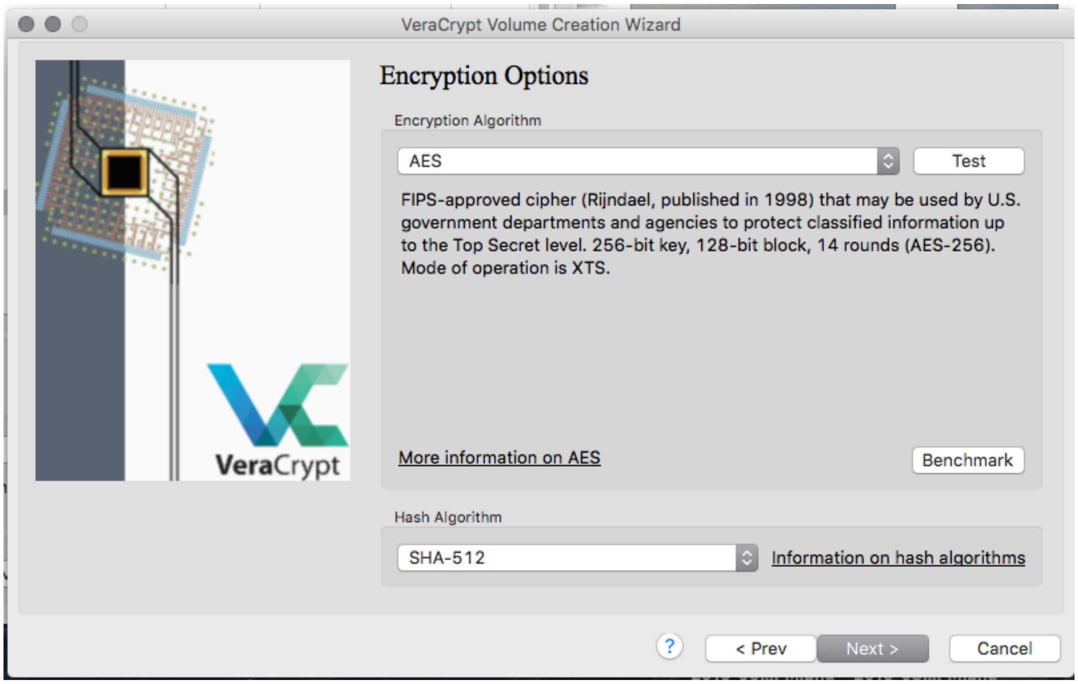
☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

Step 5

5.0 Now you will be given the option to modify the encryption used. These can be left at the defaults as shown in the picture below. To proceed, click ”Next”.



Encryption Options

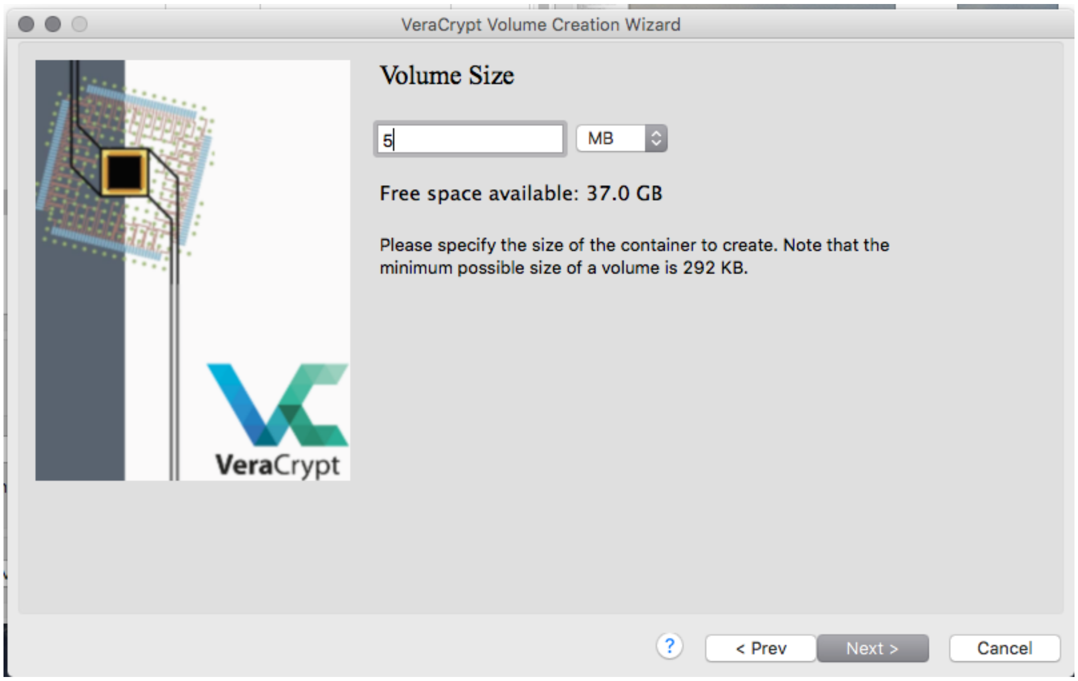
Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: SHA-512

Step 6

6.0 Here you'll be able to specify what size the encrypted container should be. Be aware that attached files for PM's have a limit. I usually set mine to 5MB. This is more than enough to send some documents and some pictures. Click "Next" to continue.



Volume Size

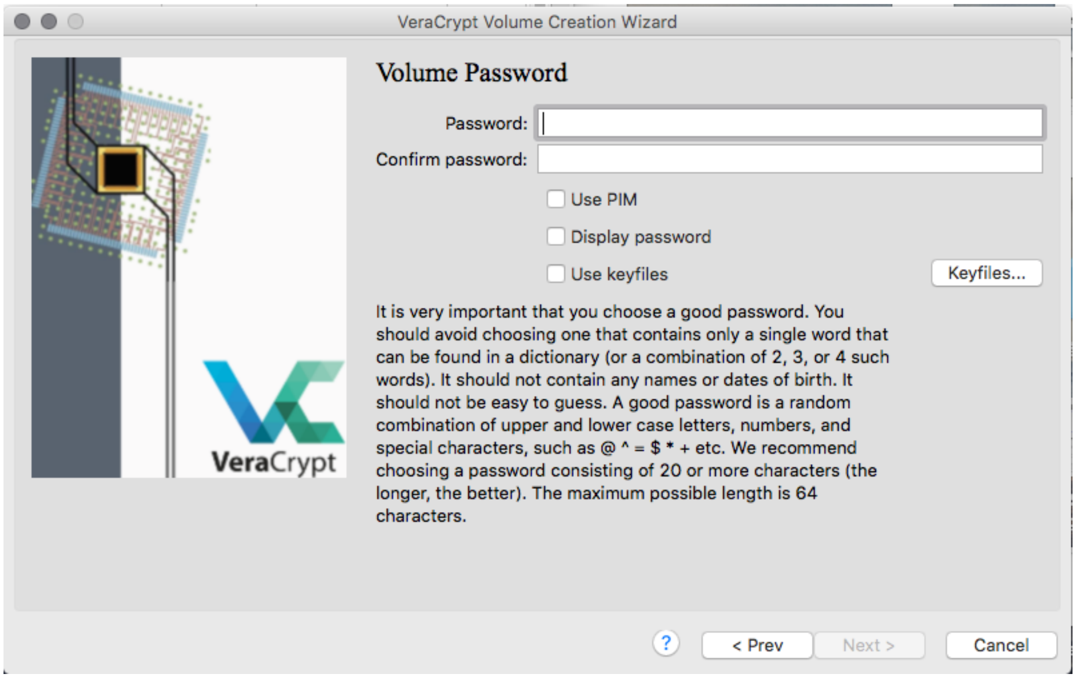
5 MB

Free space available: 37.0 GB

Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.

Step 7

7.0 Now you must enter the agreed-upon password, which has a character limit of 64, and afterwards click ”Next”.



Volume Password

Password:

Confirm password:

□ Use PIM

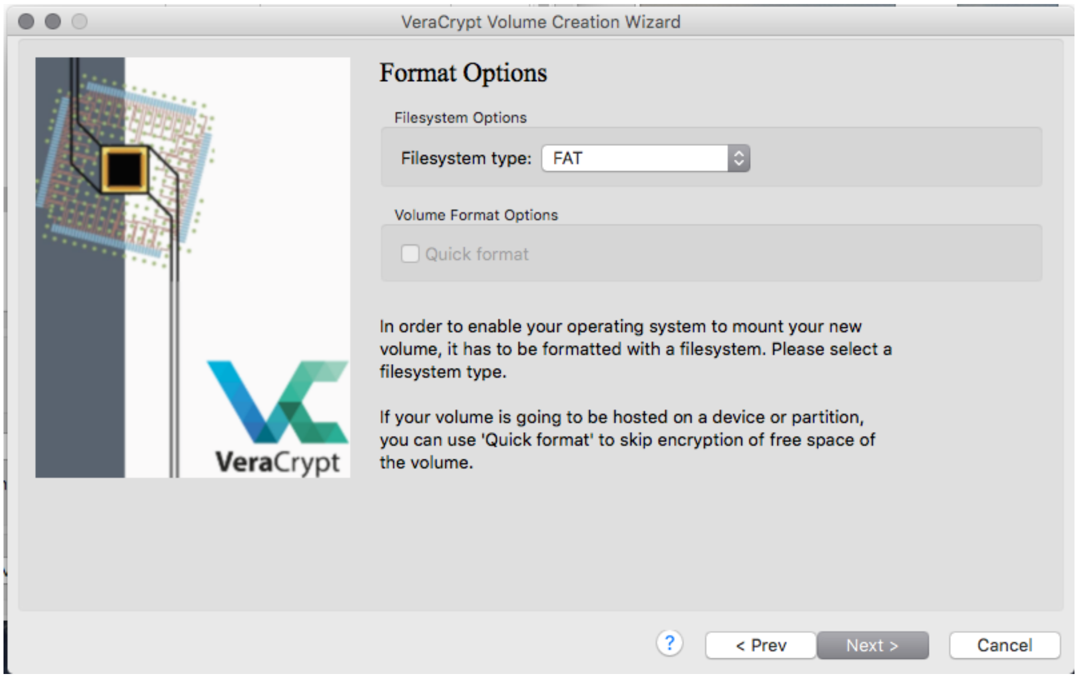
□ Display password

□ Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

Step 8

8.0 You are now prompted with ”Format Options” which should be left with defaults at ”Filesystem type: FAT”.



Format Options

Filesystem Options

Filesystem type: FAT

Volume Format Options

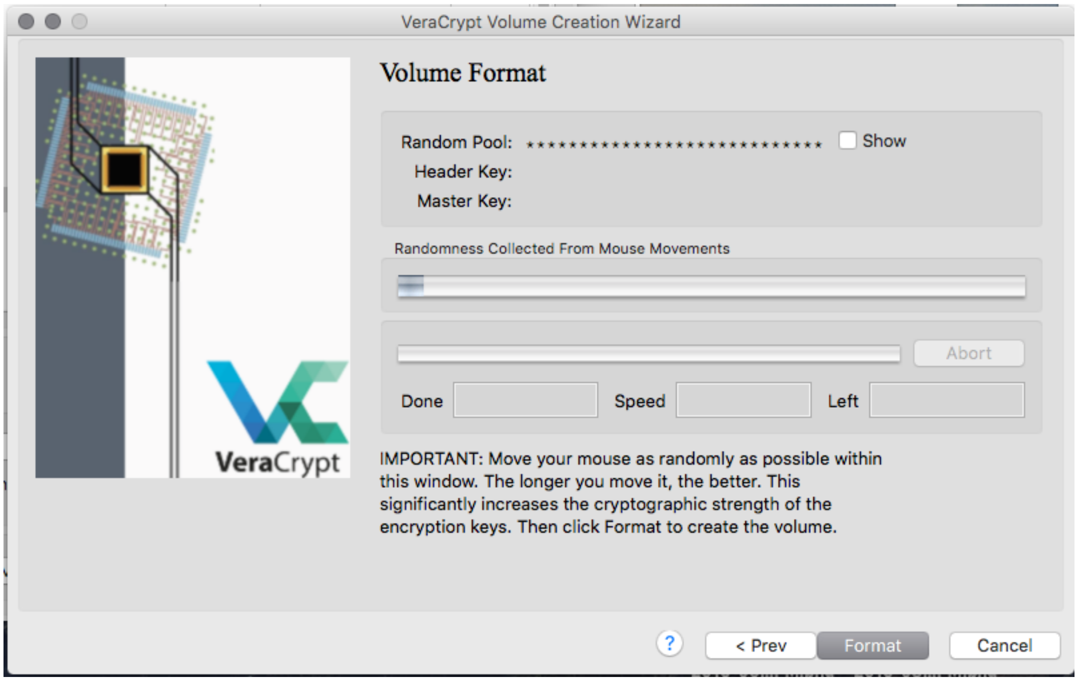
□ Quick format

In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type.

If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.

Step 9

9.0 Almost done. When you get to this point you see a bar called ”Randomness Collected From Mouse Movement”. Move your mouse around as randomly as possible within the window until the bar has been filled. When this is done, click ”Format”.



Volume Format

Random Pool: ******************************** □ Show

Header Key:

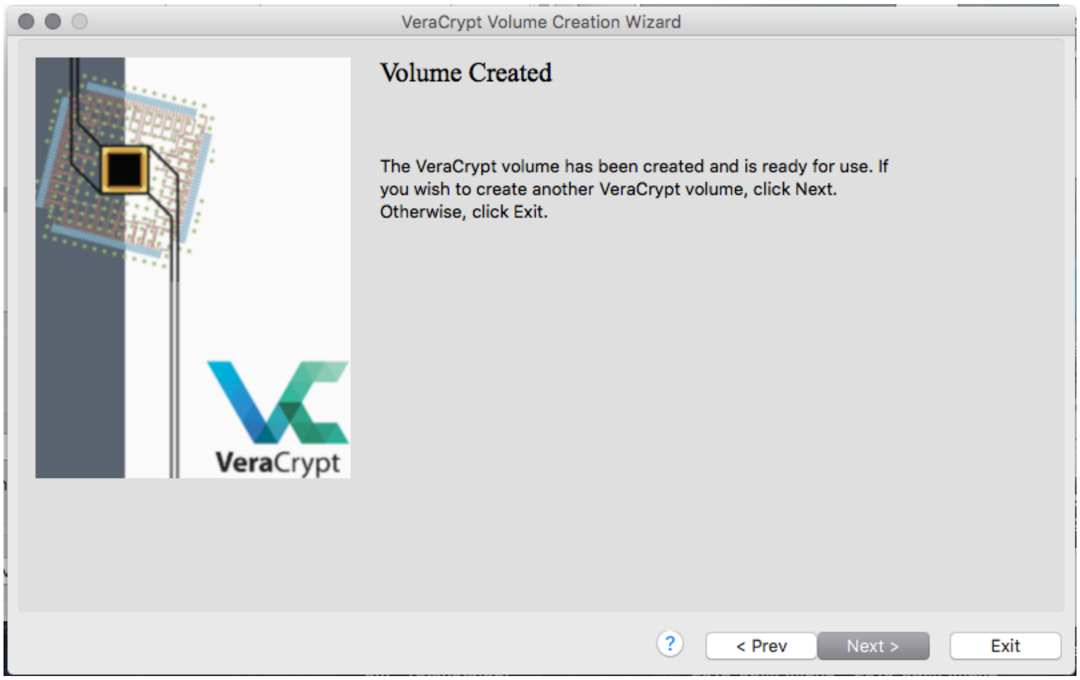
Master Key:

Randomness Collected From Mouse Movements

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Step 10

10.0 When the formatting has completed, you will see a window ”Volume Created”. Click ”Exit”.

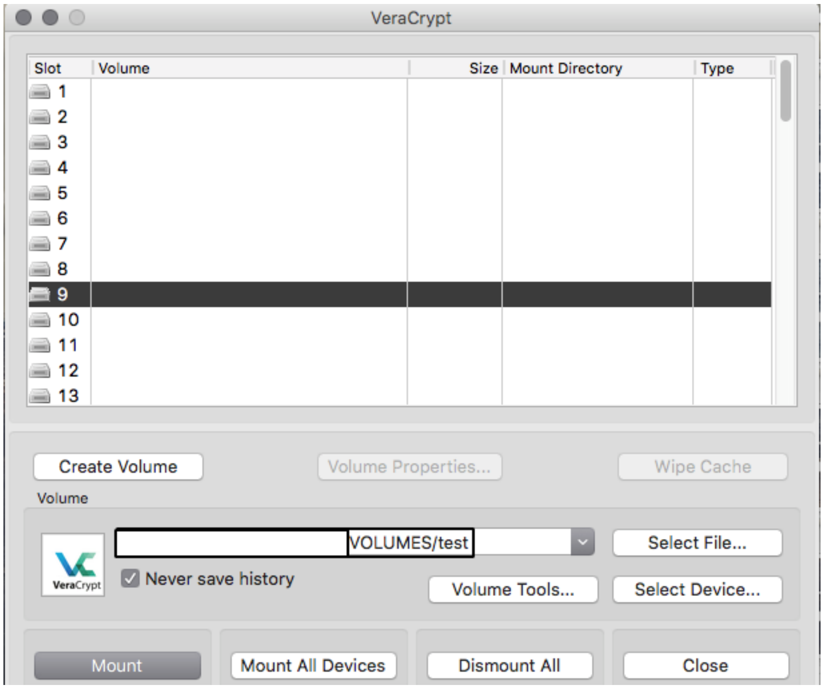


Volume Created

The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.

Step 11

11.0 Now that you have made your encrypted container, you'll have to mount it first before you can throw any files in there. From the main window, as depicted below, click ”Select File...” located to the left and select your VeraCrypt container. In the middle of the window you see a row named ”Slot”. Choose one by clicking on it so that it is selected as in the picture below. At last, press ”Mount” in the bottom right corner and enter your password. Now you can see the container is mounted just like a USB would be mounted. Open it from your File Explorer and in there you can put the sensitive files you wish to send. When you have done this, return to the main VeraCrypt window and click ”Dismount” while your currently mounted container is selected in the ”Slot” row.
Unfortunately the NONET site's PM's file-sending feature does not allow this file type to be sent. Rename the VeraCrypt container to file.zip. Mine would be called test.zip. This file can now be sent with PM's. When the receiver gets the file, all they have to do is download the ”zip” file, rename it by removing ”.zip” and follow the same mounting steps that were just described.



VeraCrypt

Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

Volume: VOLUMES/test

☑ Never save history

12 KeePassX

Two sections have had a focus on strong passwords. You might be thinking "How in the fucking hell do you want me to make so many different, unique and secure passwords?". If that is the case, keep on reading since this section is dedicated to that problem.

A password manager is an application that will manage/organize your accounts. You may have heard of some already. There is for instance LastPass. LastPass should not be used, since it is cloud-based. This means that your passwords are stored on their servers. Any cloud-based service should be avoided if possible. In this section, I'll introduce you to KeePassX.

KeePassX is a password manager that is not cloud-based. It will create a encrypted KeePassX database file at a desired location. This can be your system HDD or a USB. In this database, you can add accounts that include email, password, username etc. It even has a integrated password generator and you best take advantage of it. It will create a fully random password, at a maximum length of 64 characters, and you don't even need to remember it yourself.

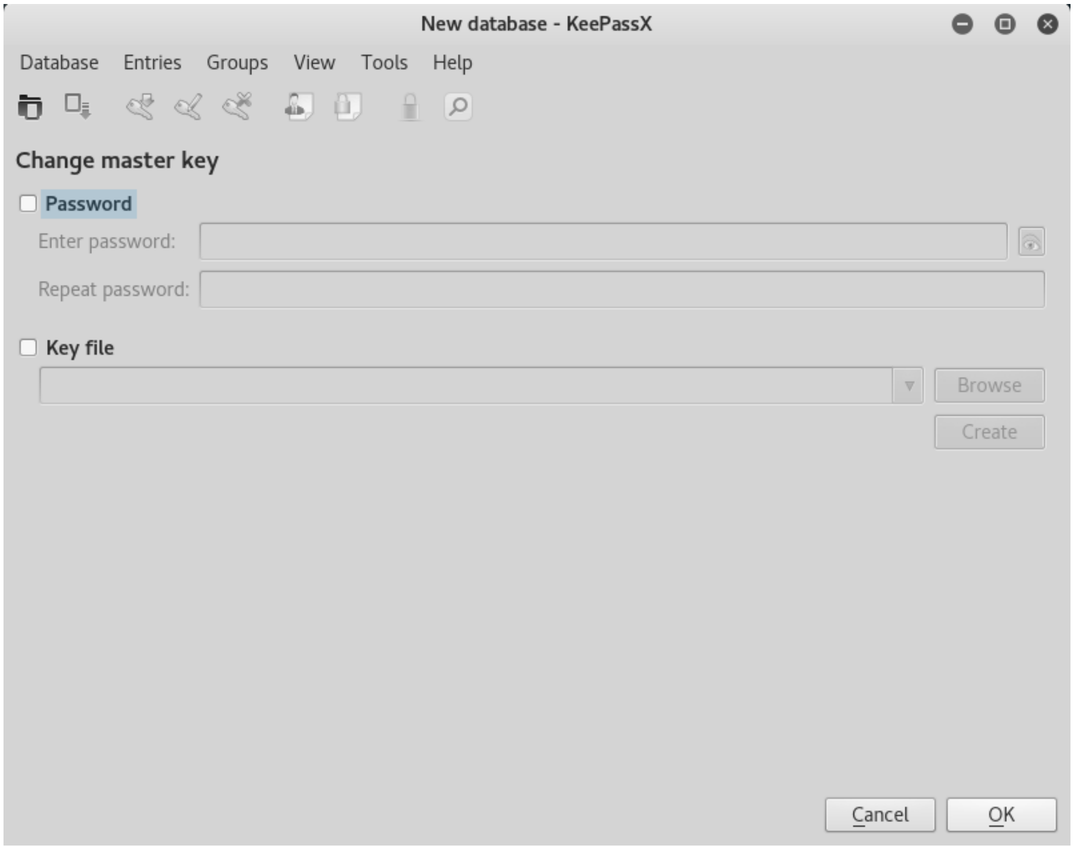
The KeePassX database is encrypted using a master-key: a password of your own choosing. Now you only have to remember one password. Furthermore, it lets you use a Keyfile instead, or at the same time! A Keyfile, is a file you keep on a secured medium, like encrypted USB/VeraCrypt container and use the password, randomly generated in the Keyfile, to unlock the KeePassX database. KeePassX is also cross-platform for Linux, Windows and OSX. Let's get right to it!

Step 1

Download KeePassX from here: `https://www.keepassx.org/` *(If you are on Linux, it'll probably be available in your repositories using the name "keepassx").* Follow the guided installation.

Step 2

Now start KeePassX and you will see somewhat like the following depicted below. It will ask you for a master key or Keyfile. I use both. You can selectively check and un-check both options for what you think is best. I recommend using both at the same time and that is why I will describe the steps used to set it up.



Change master key

□ Password

Enter password:

Repeat password:

□ Key file

Check off ”Password” option and enter the secure password you decided upon. Now check off ”Keyfile” too and press ”Create”. You will be prompted to choose where you want to save the Keyfile. I recommend inside a Veracrypt container or encrypted USB. If both a Keyfile and Password is selected, click ”OK”.

You will now get the contents of your KeePassX database, which at first of course are none. First save the KeepassX database by using the appropriate keyboard shortcut or using the menu in the top-left corner. Select the place you want to save it. You have now created the KeePassX database. I recommend you make a backup of this .kdbx file regularly.

If you want to add an account, press the golden key with a green arrow in the top-left corner. Here you'll be able to enter ”Title”, ”Username” and ”Password”. On the right side of the last password box there is a button called ”Gen.”. Press this to generate a secure password. You can define length, characters included, etc. Keep everything besides the length at default, since most online services have a maximum length for a password. Check it and then go back to KeePassX and generate a password by first selecting the maximum length allowed for the service and then "Accept". At last, you need to click "OK" and you'll return to the initial overview. Remember to save these changes just like you saved the database in the first place.

Step 3

Now every time you need the password for said account, unlock the KeePassX database by entering the master key password and selecting your Keyfile that you saved on that encrypted USB/Veracrypt container, using "Browse". Right-click on the account listed and select "Copy Password". This can now be pasted into the password section of, for example, the NONET site's login screen.

13 Further Resources

* `https://tails.boum.org/`
* `https://dee.su/`
* `https://www.whonix.org/`
* `https://www.qubes-os.org/`
* `https://www.eff.org/`
* `https://theintercept.com/`
* `https://gnupg.org/`
* `https://fakenamegenerator.com`
* `http://justdelete.me/`
* `https://99bitcoins.com/complete-guide-using-bitcoin-anonymously`