A Beginner Friendly Comprehensive Guide to Installing and Using a Safer Anonymous Operating System

Version 0.8.3 February, 2015

With the greatest respect and thanks to The Debian Project, The Tor Project, The Whonix Team, Anonymous and the numerous Open Source Software Creators, all of which made this tutorial possible.

The most current version of this guide will always be available at
https://anonguide.cyberguerrilla.org or http://yuxv6qujajqvmypv.onion.

Contact: anonguide@bitmessage.ch
GPG Key = 0xBD8083C5237F796B
Fingerprint = 6422 2A88 D257 3091 0C47 A904 BD80 83C5 237F 796B

Downloadable PDF for Offline Viewing

- Clearnet PDF: https://anonguide.cyberguerrilla.org/anonguide.pdf
- Clearnet GPG Verification File: https://anonguide.cyberguerrilla.org/anonguide.pdf.asc
- Tor Hosted PDF: http://yuxv6qujajqvmypv.onion/anonguide.pdf
- Tor Hosted GPG Verification File: http://yuxv6qujajqvmypv.onion/anonguide.pdf.asc

Changlelog since version 0.8.2, November 2014.

1. Additional “important notices” regarding the choice of an installation method for Debian and UEFI secure boot added at the beginning of Chapter 1.
2. Steps 10-13, 17-18, 20, 26, 32-33 modified in Chapter 3 to link or reflect Whonix 9.6.
3. Chapter 4 updated with link to Whonix forums for troubleshooting.
4. Chapter 4b updated to reflect current Tor Browser functionality.
5. Official distribution sites for this guide modified on first and last page.
6. Contact information added to first page.
7. Public GPG key and contact information mentioned at beginning and end of guide.
8. Cyberguerrilla.org donation link updated.
9. Whonix Forum link added in conclusion.

Changelog since version 0.8.1, October 2014.

1. Steps 10-13, 17-18, 20, 26, 32-33 modified in Chapter 3 to link to or reflect Whonix 9.4.
2. Chapter 4f, steps 5-6 modified for Jacob Appelbaum's new GPG public key used to verify Torbirdy.
3. Chapter 4f, step 18 modified to add additional temporary substeps to reconfigure Torbirdy to use the appropriate IP address of the Whonix Gateway.

Changelog since version 0.7.2, August 2014.

1. Various steps and links updated to work with Whonix 9 due to the Whonix Project's retirement of Whonix 8.

Changelog since version 0.6.3, July 2014.

1. Added stream isolation to Pidgin in Chapter 4e, Step 24. **Previous users should make this change.**
2. Added “Malware Mitigation” method in new Chapter 4g.
3. Fixed “wget as root” oversight in Chapter 3.
4. Added various warnings at steps regarding the use of “sudo.”
5. Added notes of optional stopping points after the Debian installs Chapter 2a and 2b.
6. Added steps on disabling “Mini Toolbar” for “Full Screen Mode” in Whonix Workstation.

Table of Contents

Introduction . . . . . Page 4

Chapter 1. The Initial Debian Setup and Install. . . . . Page 7

Chapter 2. Choosing your Installation Method. . . . . Page 27

Chapter 2A. Installing an Operating System on an Encrypted USB Flash Drive. . . Page 28

Chapter 2B. Installing the Operating System on an Encrypted Internal Hard Drive Partition with a USB Flash Drive Boot Key. . . . . Page 46

Chapter 3. Final Debian Tweaks and Whonix Installation. . . . . Page 125

Chapter 4. Using Whonix Securely and Anonymously. . . . . Page 179

Chapter 4a. Proper Start Up and Shut Down Procedures for Whonix . . . . . Page 180

Chapter 4b. Using the Tor Browser. . . . . Page 185

Chapter 4c. Using a Password Manager. . . . . Page 194

Chapter 4d. Using the IRC and XChat. . . . . Page 210

Chapter 4e. Using an Instant Messenger. . . . . Page 228

Chapter 4f. Encrypted email with Icedove and Enigmail. . . . . Page 259

Chapter 4g. Malware Mitigation. . . . . Page 330

Chapter 5. Supporting the Projects that Made this Tutorial Possible. . . . . Page 386

Conclusion . . . . . Page 387

Introduction

One of the hardest concepts for many users of networked computers to understand is security, privacy and anonymity. For those who wish to have security, privacy and anonymity, many do not realize or understand how easy it is to lose them all as a result of making common mistakes. This guide will teach you how to build a secure encrypted system that uses Debian and Whonix to help maintain your privacy and anonymity.

Now, before you possibly close this document under the mistaken notion that you will not understand how to use or install the system mentioned above, remember that this guide is written to be beginner friendly. The truth is that, if you can follow the numbered steps, most of which are accompanied by screen shots, you will find this process relatively straightforward. It will just take some time. Do not let the length of this tutorial overwhelm you either. The length is due to the fact that there are screen shots for almost every instruction. **In the end, the time you invest in building this system for yourself will be worth it.**

The benefits of this system for those who wish to have privacy, security and anonymity are numerous.

- Your system will be encrypted with a very strong encryption technology. Thus, unless you give someone your encryption password, they will not be able to read what you keep on this system in a timely manner, if at all. This will protect your data from entities that are made up of anything from powerful governments to common thieves.

- The system consists of a USB flash drive as either your main operating system disk or as your boot disk. Since the device is portable, you can keep it on you at all times and never have to worry about someone tampering with it to get your encryption password by modifying the controlling software. Additionally, you can easily lose it or destroy it, if you so desire, which will make the encrypted data irrecoverable.

- The Debian Operating System (OS), which will be your host OS, is free, open source and has a good track record for security.

- The Whonix OS, which will be the main OS you use on top of Debian, is a customized version of Debian to work with the Tor network. Tor is one of the more powerful anonymizing free proxy systems available to the public. While using Whonix, everything you do will be forced through the Tor network, making it very difficult for you to make a mistake and accidentally reveal your identity through either mistaken use of, or an attacker's exploitation of, software. The use of the web, the Internet Relay Chat, and numerous other Internet services can be done by novice users without having to worry about leaking any damaging information that would reveal their IP address through their computer.

If you are new to private and anonymous communications, you have everything to gain by using this system. Everyone makes mistakes while they learn. This system will provide you with the tools you need to learn while protecting you from the repercussions of common mistakes that people make by not understanding technology. As you learn the more advanced uses of software,

this system will provide a very secure and anonymous base platform from which to operate.

Before you get started, you will need to acquire a USB flash drive. The following is a break down of the two types of systems, their advantages and disadvantages, and what you will need to install them.

Operating System on an Encrypted USB Flash Drive (Most Beginner Friendly)

If you wish to install this entire system on a USB flash drive (which is detailed in Chapter 2A beginning on page 27), you will need the following:

- 1 USB 3.0 flash drive of at least 32 gigabytes.
- Access to computers with at least 2 gigabytes of RAM or more.

There are many benefits to this method. One, you have a mobile operating system that can be used on just about any computer that has enough RAM. So long as you have the option to boot from a USB flash drive on a computer in front of you, you can likely take advantage of your own secure, private and anonymous OS. Two, it will not leave any fingerprints on the computer you use it on if used properly. Three, the small size of USB flash drive makes it very easy to hide or physically destroy/lose.

There are also a few possible disadvantages to this method. The first is that most small USB Flash Drives are not very fast. Thus, the install time to copy the software may be longer. Additionally, the use of the system may feel sluggish at times due to the slower disk read/write speeds. The faster your USB flash drive is, the less noticeable any lag will be. Finally, if you use this system on a machine with less than 2 gigabytes of RAM, the amount of memory caching that will be required will greatly slow down the use of the system, if not make it unusable, depending on the possible read/write speeds you have.

Operating System on an Encrypted Internal Hard Drive Partition with a USB Flash Drive Boot Key

If you wish to install the main operating system on free space existing on your internal hard drive (which is detailed in Chapter 2B on page 45), you will need the following:

- A computer with an internal hard drive that has at least 32 gigabytes of free space for the root operating system.
- 1 USB flash drive of at least 256 megabytes for the System Boot Key. (Choose one with the smallest shape possible. Flash drives are available that are about the size of the finger nail on your thumb.)
- A back up of the existing files on your hard drive.

There are a few advantages to this method. The first and foremost is the speed. You will not notice any sluggishness when you use the system and the install time will likely be much shorter due to the faster disk writes. Another advantage is that you have the option of more hard drive space than you will find on a number of USB flash drives for your operating system. Finally, if you only have access to computers with less than 2 gigabytes of RAM, the faster read and write speeds on an internal hard drive will allow the system to take advantage of memory caching without making the system unbearably slow.

There are a few disadvantages as well. One is that your set up will be tied to one computer. Thus, if you want a mobile set up, you'll need to install this system on a laptop. The other is that, if anyone else looks at your computer with forensic equipment, they will be able to determine that you have an encrypted partition on your hard drive. In various jurisdictions, that may trigger suspicion or possible repercussions. This is a concern for some. However, if you are to turn on your computer for someone who is forcing you to do so, it will boot right into Microsoft Windows or OS X without even providing a hint that there is an encrypted operating system installed on the computer. Furthermore, if you do not have access to your USB Flash Drive Boot Key, you won't be able to give them access to the encrypted drive anyways. Additionally, it is much more difficult to hide or lose a large computer than a USB flash drive. However, if you lose the USB flash drive that serves as your System Boot Key in this method, the data on your internal hard drive will be safely (or frustratingly) irrecoverable. Finally, if you opt to use this method, **please back up your important files**. You will be resizing an existing partition if you use this method which, in a worst case scenario, can lead to data loss. However, such data loss is unlikely. So, don't let this be a concern that would prevent you from trying this method.

The choice you make when it comes to the type of system you use will largely come down to personal comfort and preference. You'll likely find arguments on the Internet for why one of the two methods mentioned above are better than the other. I broke those arguments down to their basic points by explaining the basic advantages and disadvantages of both. If you have the time, try both methods and see which one you like the best. Remember that no system is perfect. Both of the methods mentioned above are solid secure methods that will provide you with a great deal of security if you act appropriately. In addition, **remember that if you forget the encryption password you choose for your operating system or if lose your USB boot key, you will never be able to recover what is on your encrypted drive**. That can be a disadvantage for you if you still want to access your operating system. However, it is a great advantage if someone else gets their hands on your computer or USB Flash Drive.

With that out of the way, let's get started.

Chapter 1. The Initial Debian Setup and Install

The first and most important step is ensuring that you have a clean and secure operating system. Most beginners use either a variant of Windows or Apple's OS X. This guide will not debate the merits of which particular OS is better or more secure than the other. Rather, for the purposes of maintaining your privacy and anonymity, you should simply assume that your operating system is compromised already. A compromised operating system will render everything done later in this tutorial pointless. So, the best thing for you to do is install a new operating system.

First and foremost, you will probably be learning to use a new operating system. In this tutorial, the OS you will be using is Debian, a well known and very good Linux distribution. Do not be intimidated by this. It's much easier than you think and, by the time you've gotten used to it, you will prefer it over anything else. Linux provides much greater privacy and anonymity than the two other dominant operating systems ever will. Since the purpose of this tutorial is to teach you how to use a system that protects both your privacy and anonymity, it is time to embrace Linux. Thus, the first step you need to take is to install Debian onto the USB flash drive that you intend to use as the Debian Install Disk.

For the purposes of this section of the tutorial, please use a plugged in wired connection for your Internet connection. It will make things easier for you.

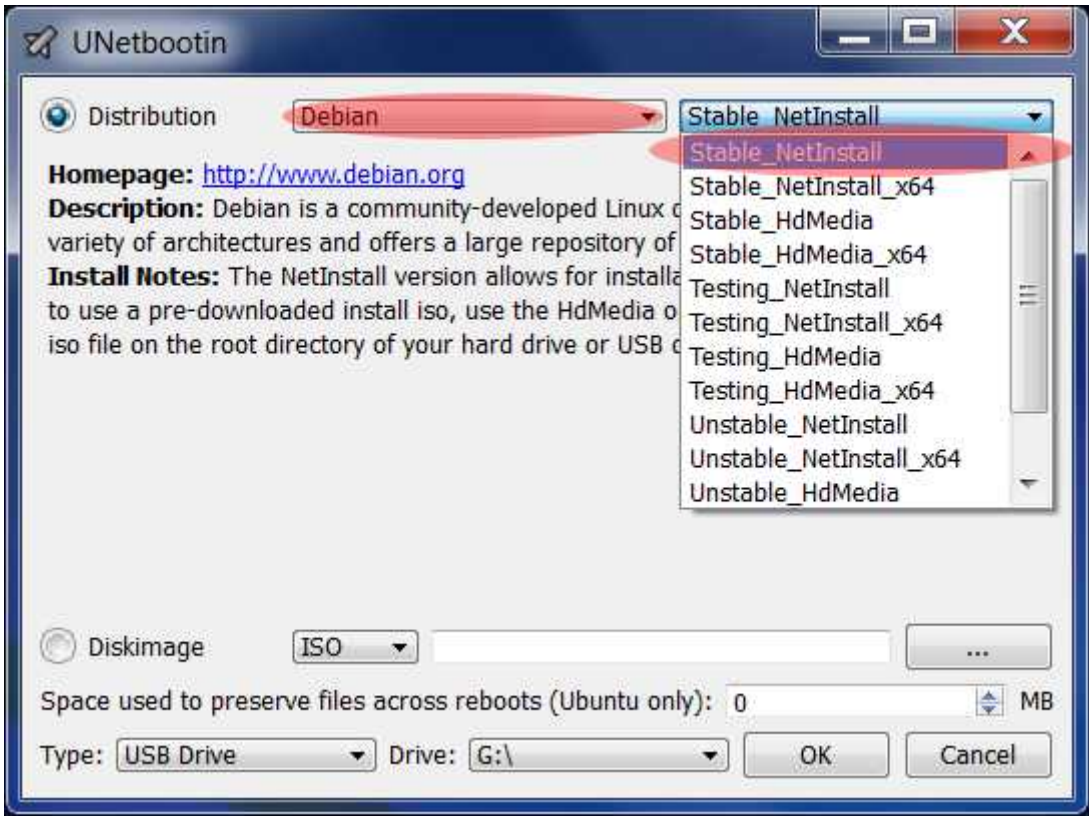
IMPORTANT NOTE: One thing that was not covered in this guide in the past are cameras that are connected to computers. Many computers now have them built in as a sales feature. **BEFORE YOU DO ANYTHING ELSE, IT IS STRONGLY RECOMENDED THAT YOU DISABLE ANY CAMERA CONNECTED TO YOUR COMPUTER AND COVER THE LENS WITH A STRONG OPAQUE PIECE OF TAPE!**

IMPORTANT NOTE REGARDING DEBIAN INSTALLATION: Steps 1-3 of this chapter use the program called “Unetbootin” to download Debian and install it to a USB installation disk. **This is not as secure as manually downloading Debian from http://www.debian.org and verifying the disk images.** If you can manage to download the Debian image manually and then cryptographically verify it, **you are strongly encouraged to do so.**

IMPORTANT NOTE FOR BOOTING: The majority of computers in production now use UEFI instead of BIOS. One feature of UEFI is known as “Secure Boot,” which is often enabled by default. If you discover that you cannot boot into the Debian Installer from your installation disk, you need to enter your computer's “setup” as it first boots up and disable “Secure Boot.”

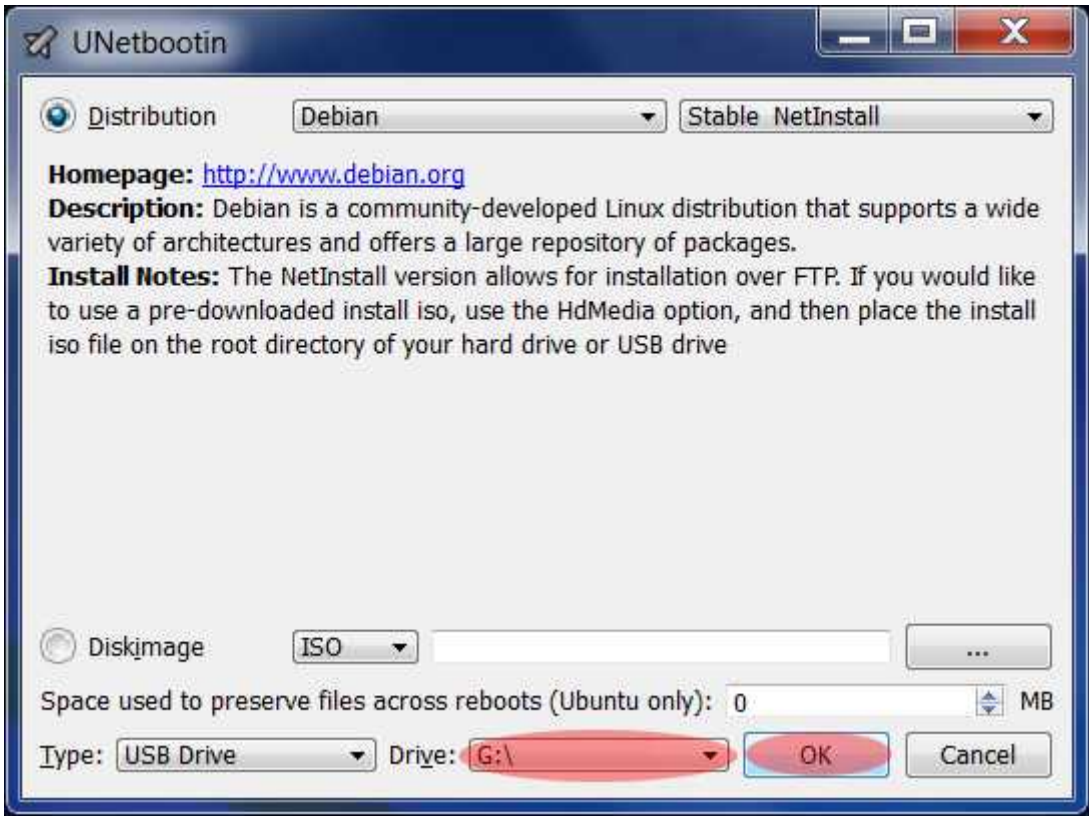
1. Download a copy of Unetbootin that corresponds to the operating system you are currently using from http://unetbootin.sourceforge.net/. Unetbootin is a program that creates a “live disk” on a USB flash drive from a disk image. Insert the USB flash drive that you plan to use with your system and then run Unetbootin.

2. In the Unetbootin window that opens, next to where it says “Distribution,” select “Debian” in the pull down window where it says “Select Distribution” and select “Stable_NetInstall” in the pull down window where it says “Select Version.”



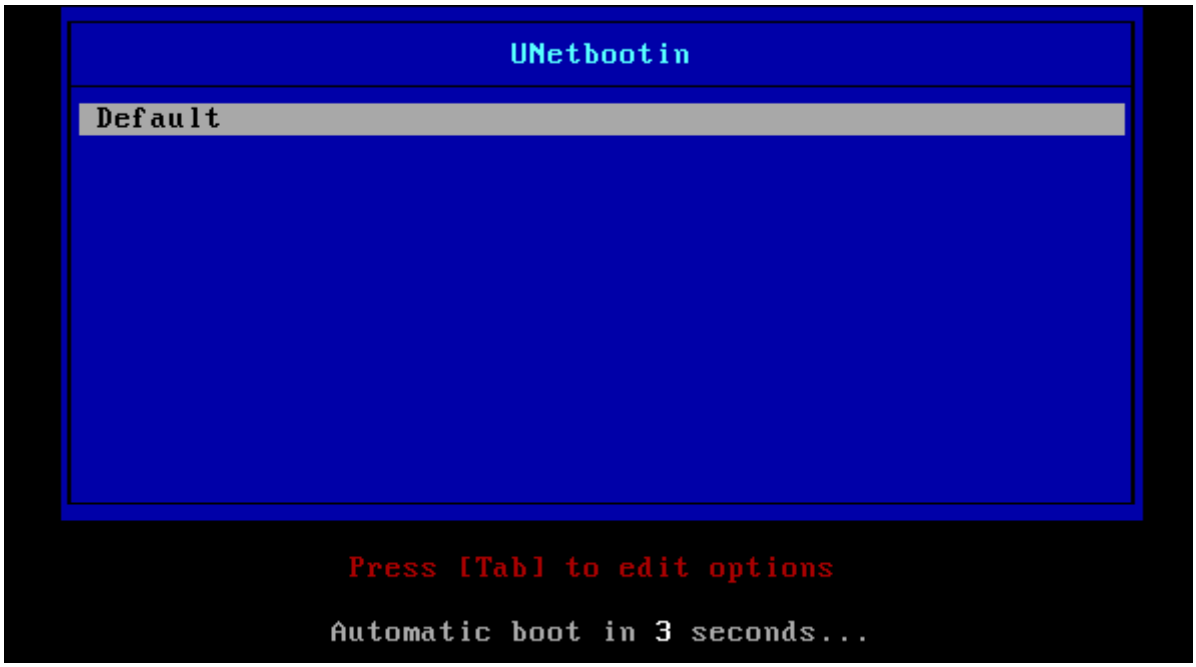
3. Next, select the drive letter of the USB flash drive that you plan to use in the pull down section next to “Drive:”. Then click “OK.”

   NOTE: Depending on what operating system you are using to run Unetbootin, different information may appear for the “Drive” selection. It generally defaults to any USB device currently plugged into your computer. However, you should confirm that to be the case if what appears in the “Drive” field is confusing.

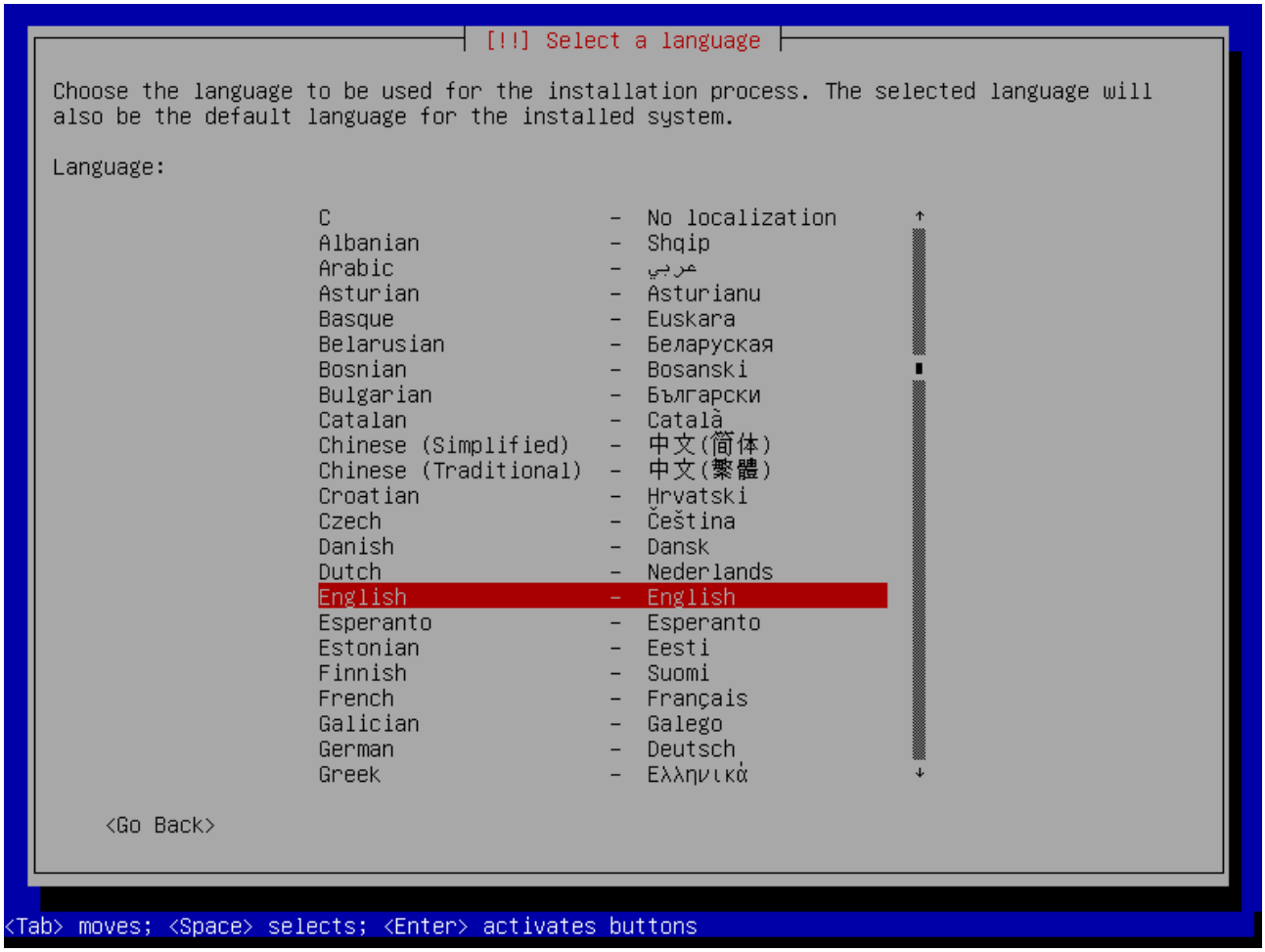


4. When the process is finished and you are prompted, reboot your computer. When your computer is first starting up, you need to boot from your USB Flash Drive that you used in the previous steps. Thus, you need to get to a boot menu. The method for doing this differs on various computers. For example, on a Dell, the boot menu is usually activated by pressing the F12 key as the computer is first starting up. On others, it can be the ESC key. On an Apple, hold the "Option" key while the computer is starting and release it when the “Startup Manager” loads. On whatever platform you use, once you get to a boot menu, select the USB flash drive that you used in the previous step.

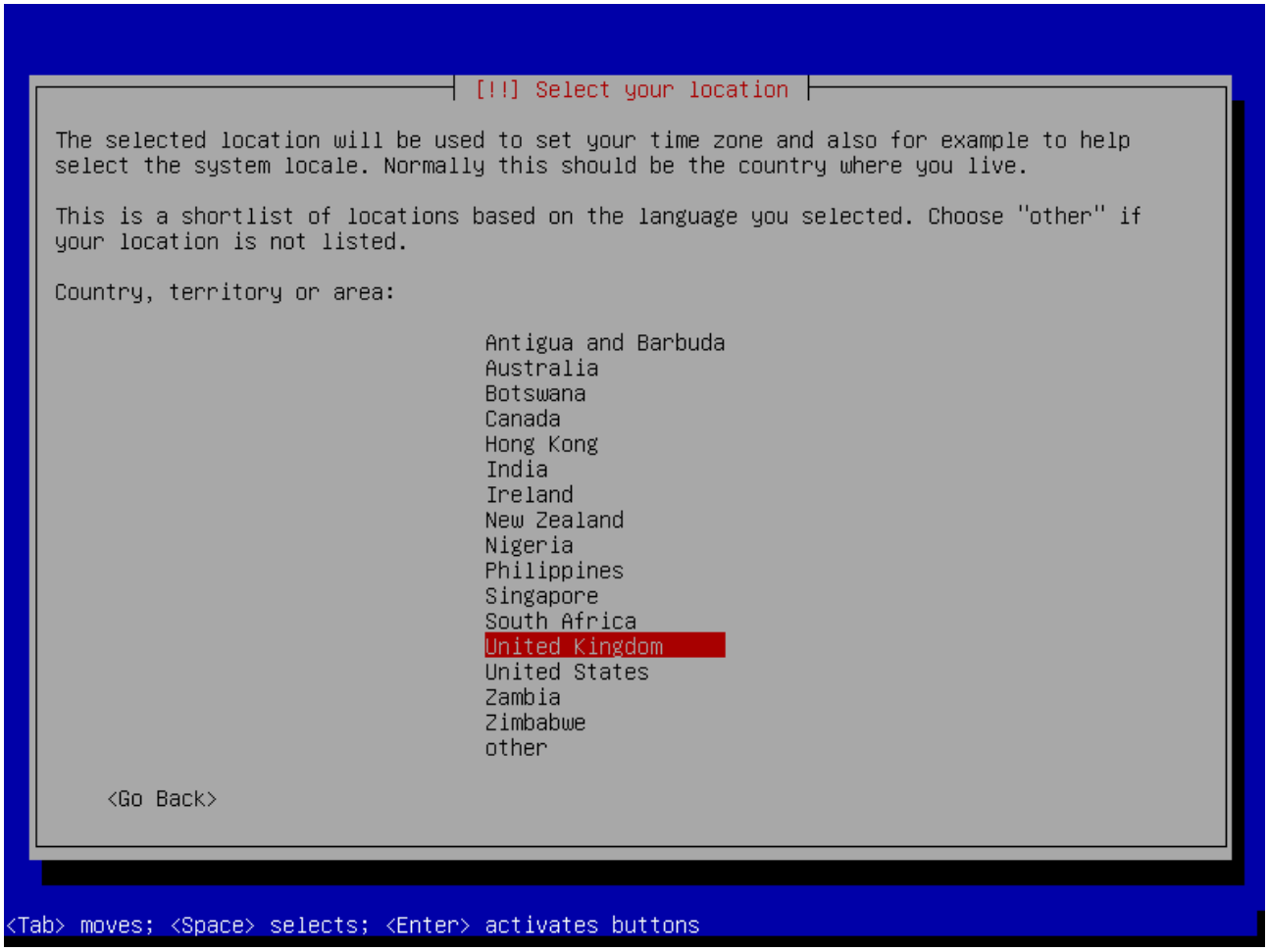
5. When you reach the next menu, you will see one menu choice entitled “Default.” Choose “Default” and press “enter” or simply let it boot automatically. This will take you to the text based Debian installer.



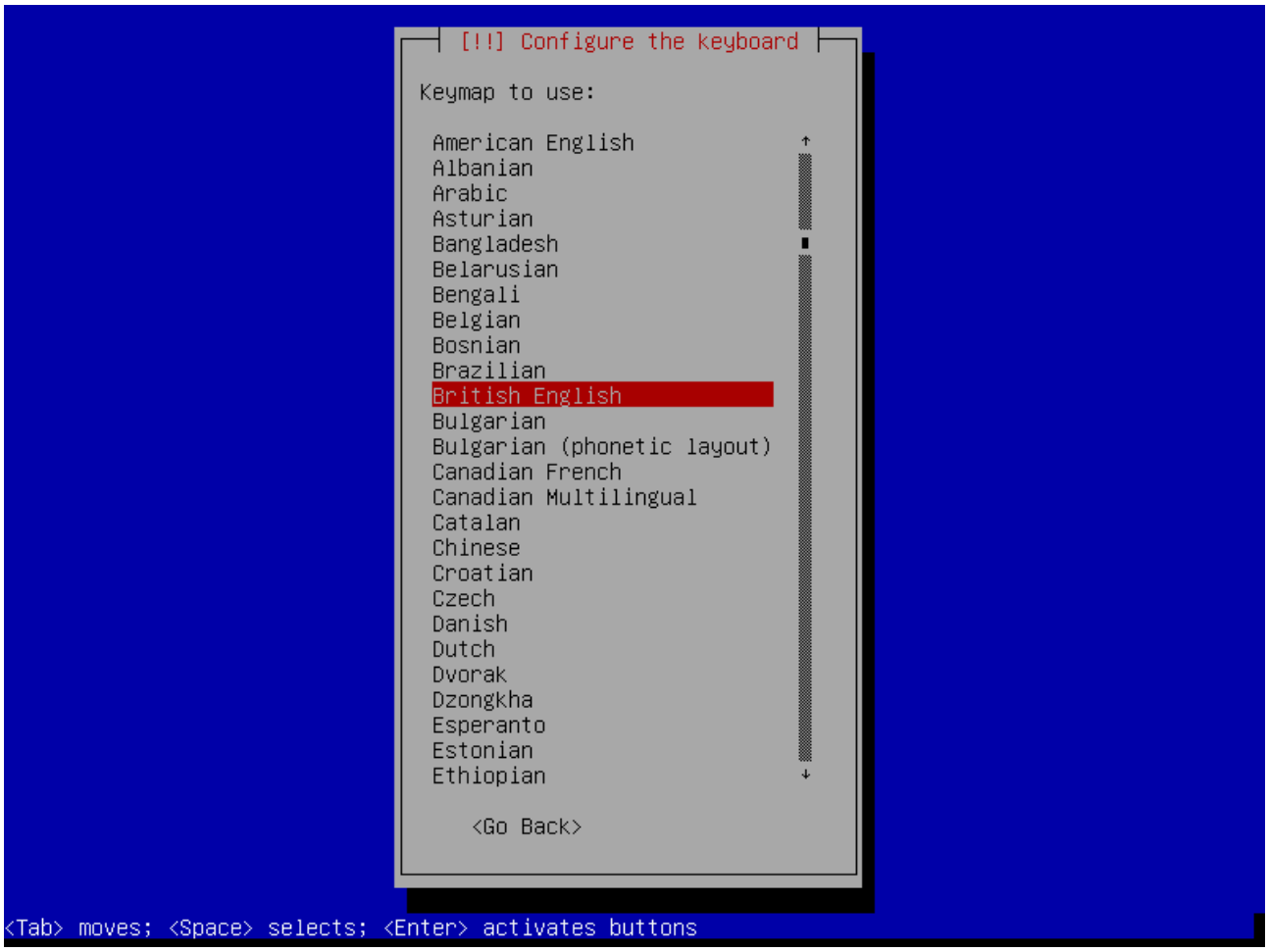
6. On the next screen that appears, choose the default language you want to use and press “enter.”



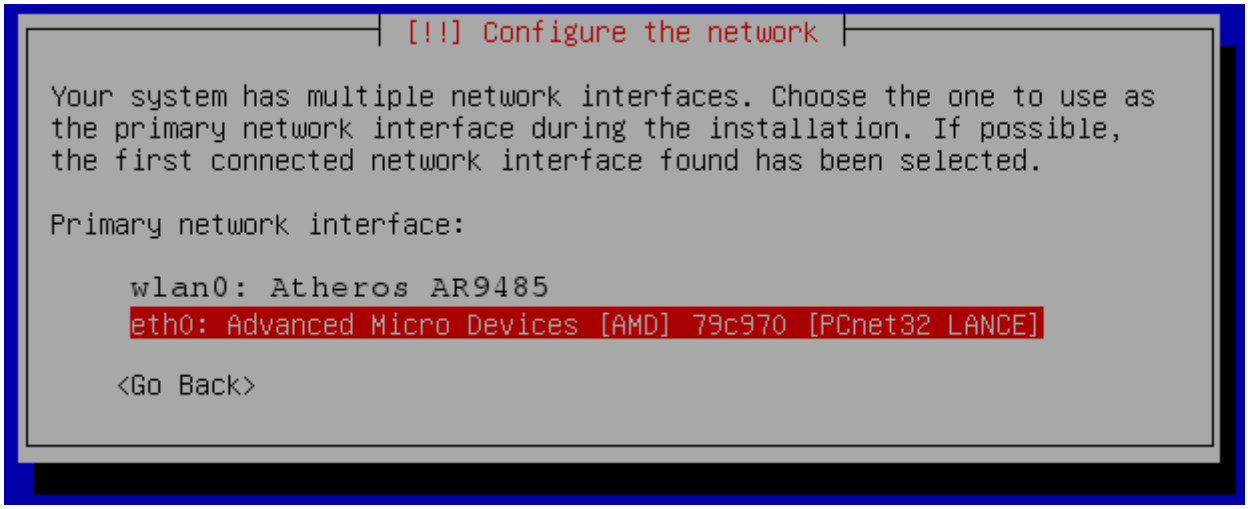
7. On the next screen, choose your default location and press “enter.”



8. On the following screen, choose the settings for your keyboard layout and press “enter.” Debian will likely make a recommendation based on your earlier language choice which you should accept.

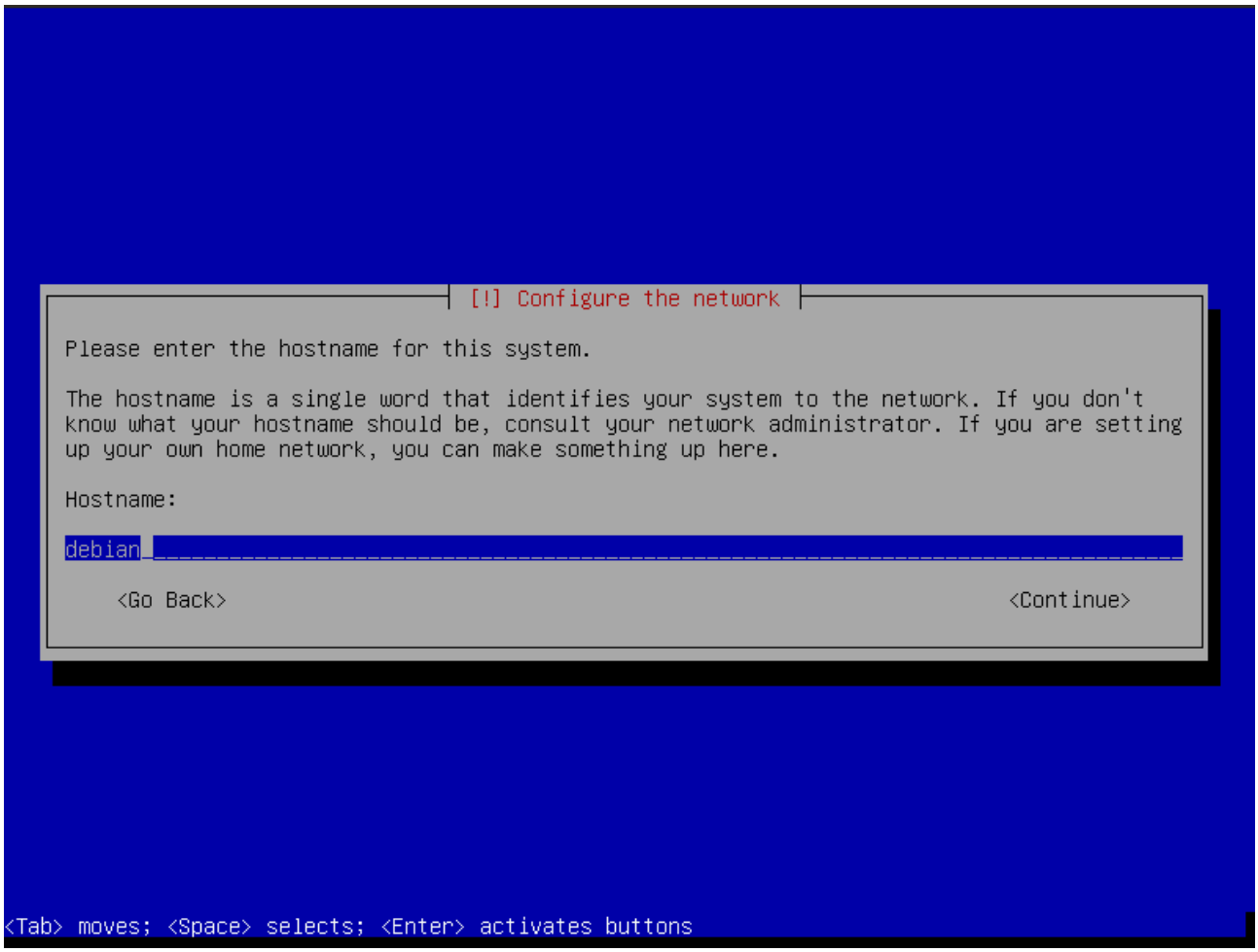


9. The Install process will now perform a number of tasks and attempt to automatically configure your network. If you are using a wired connection, everything will likely be configured automatically and you can continue to the next step. If you also have a wireless network card, you may be prompted by the installer to choose the network card to use. If prompted to choose a "primary network interface," select "**eth0**" and press "enter."

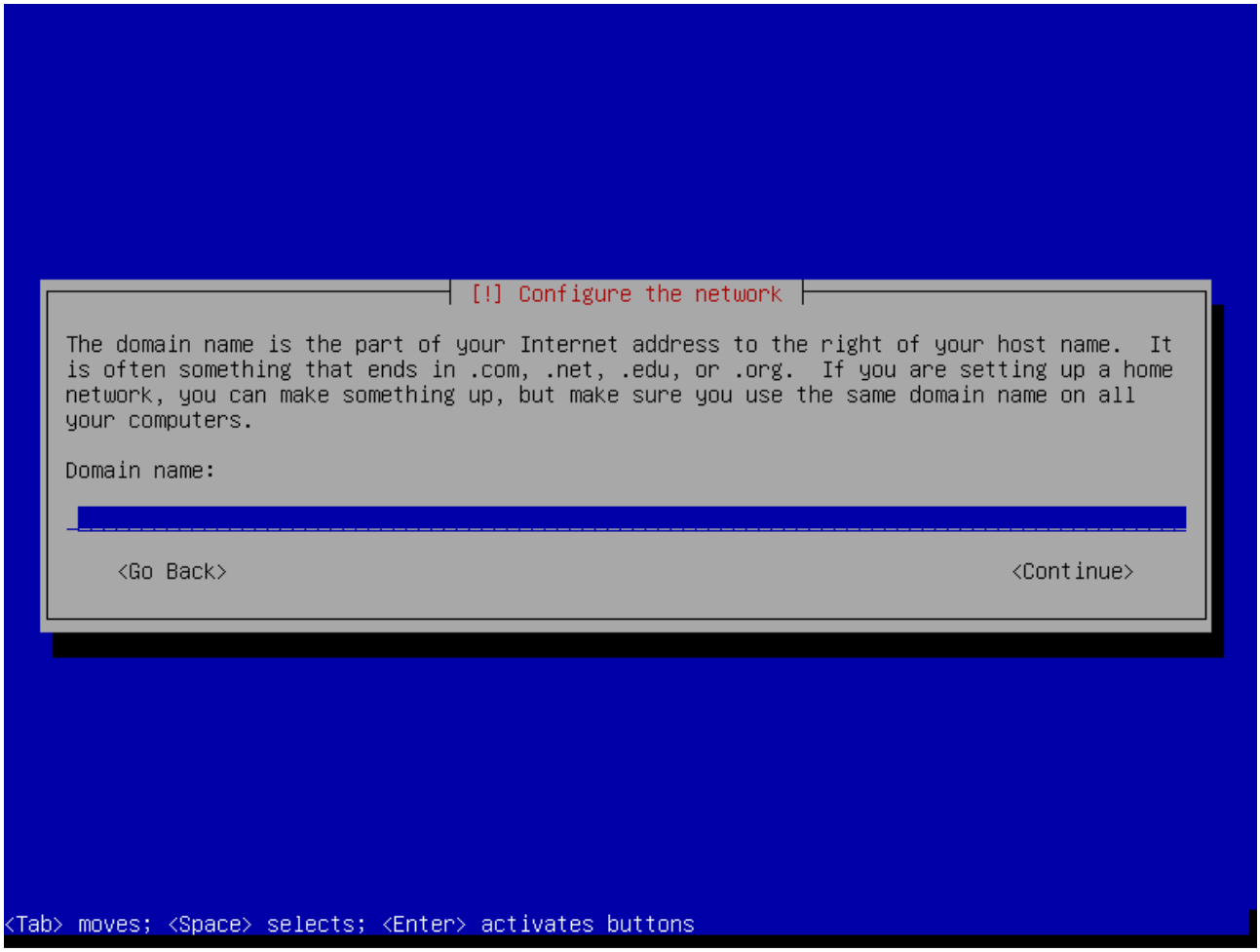


While not recommended, if you are going to use a wireless connection for the installation process, choose "wlan0," press "enter" and continue through the various prompts that will ask for your wireless network name (SSID), password, etc. During this step, you may get a warning stating that you need to install firmware from a disk in order to get the wireless card working properly. If prompted to do that, choose "no," and use a wired connection instead. You can search for your corresponding wireless drivers, in addition to the instructions for installing them, later.

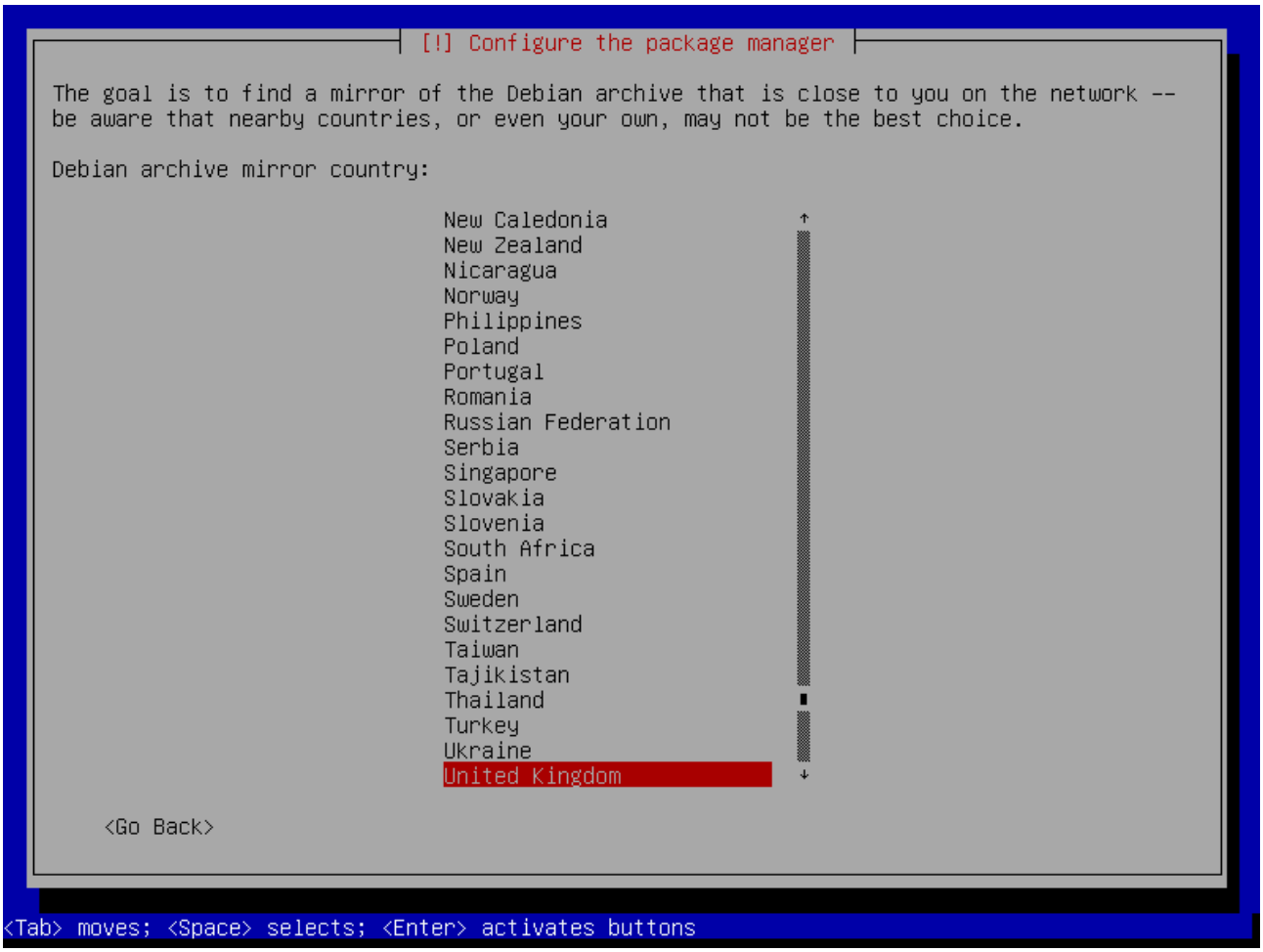
10. Eventually you will be prompted to “enter the hostname for this system.” Leave this as the default which is “debian” and press “enter.”



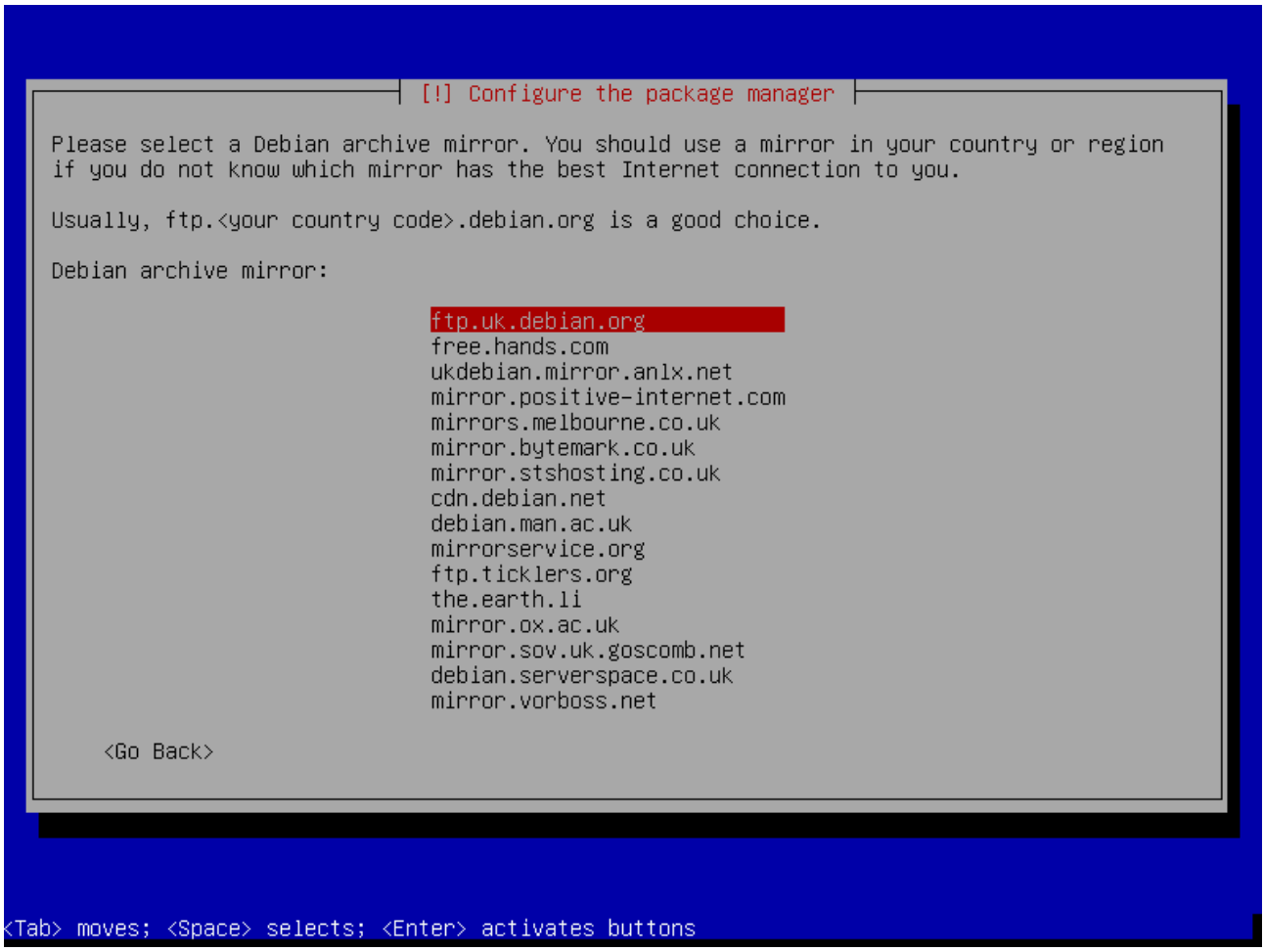
11. The next prompt will ask you for your “domain name.” Leave this blank and press “enter.”



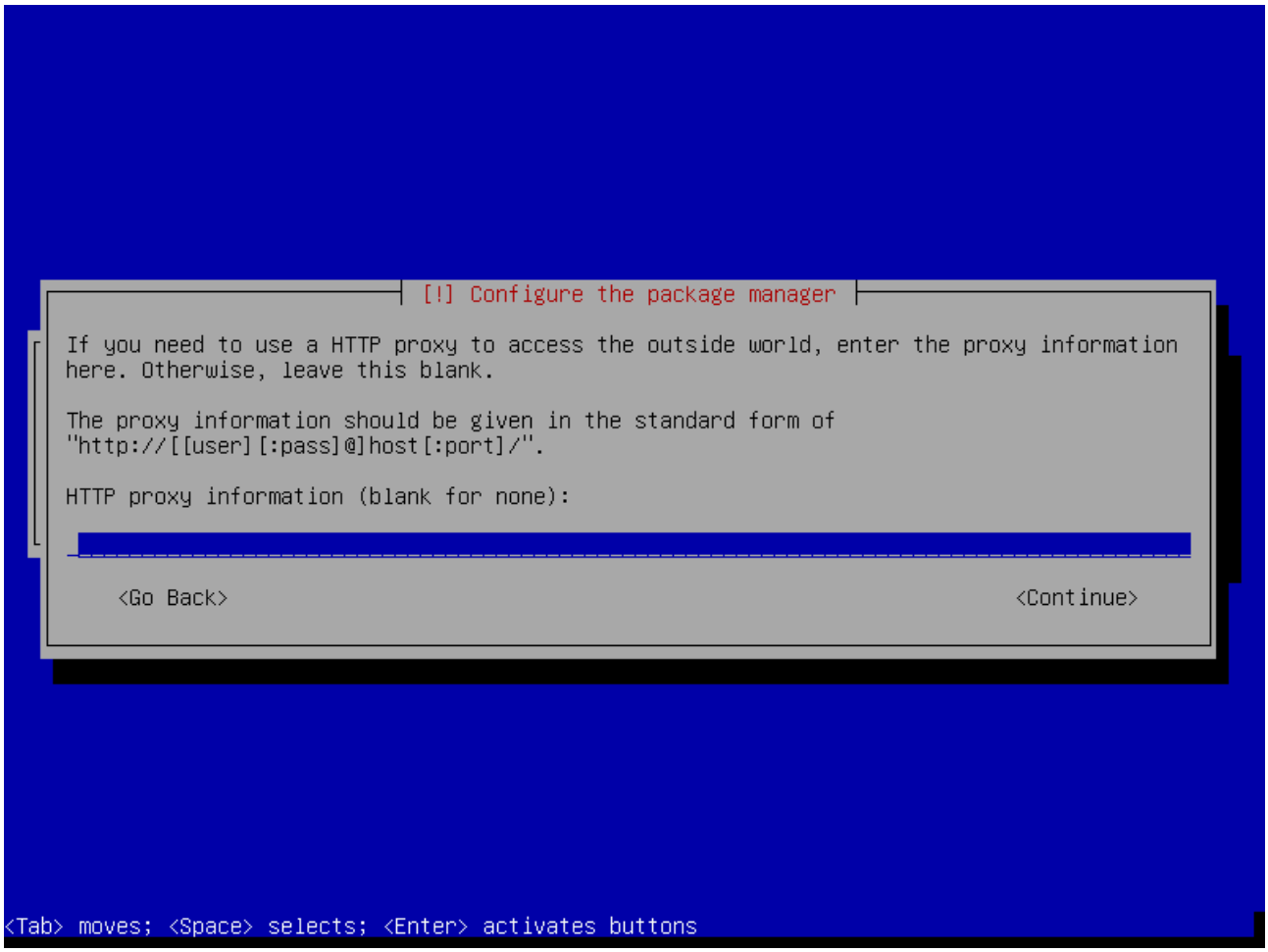
12. In the next screen, you will see a progress bar indicating that it is “installing the base system.” Depending upon the write speed of your USB flash drive, this could take awhile. When it finishes, it will prompt you to choose a “Debian archive mirror country.” A selection will likely be chosen by default based on the location you selected earlier. Select your region and press “enter.”



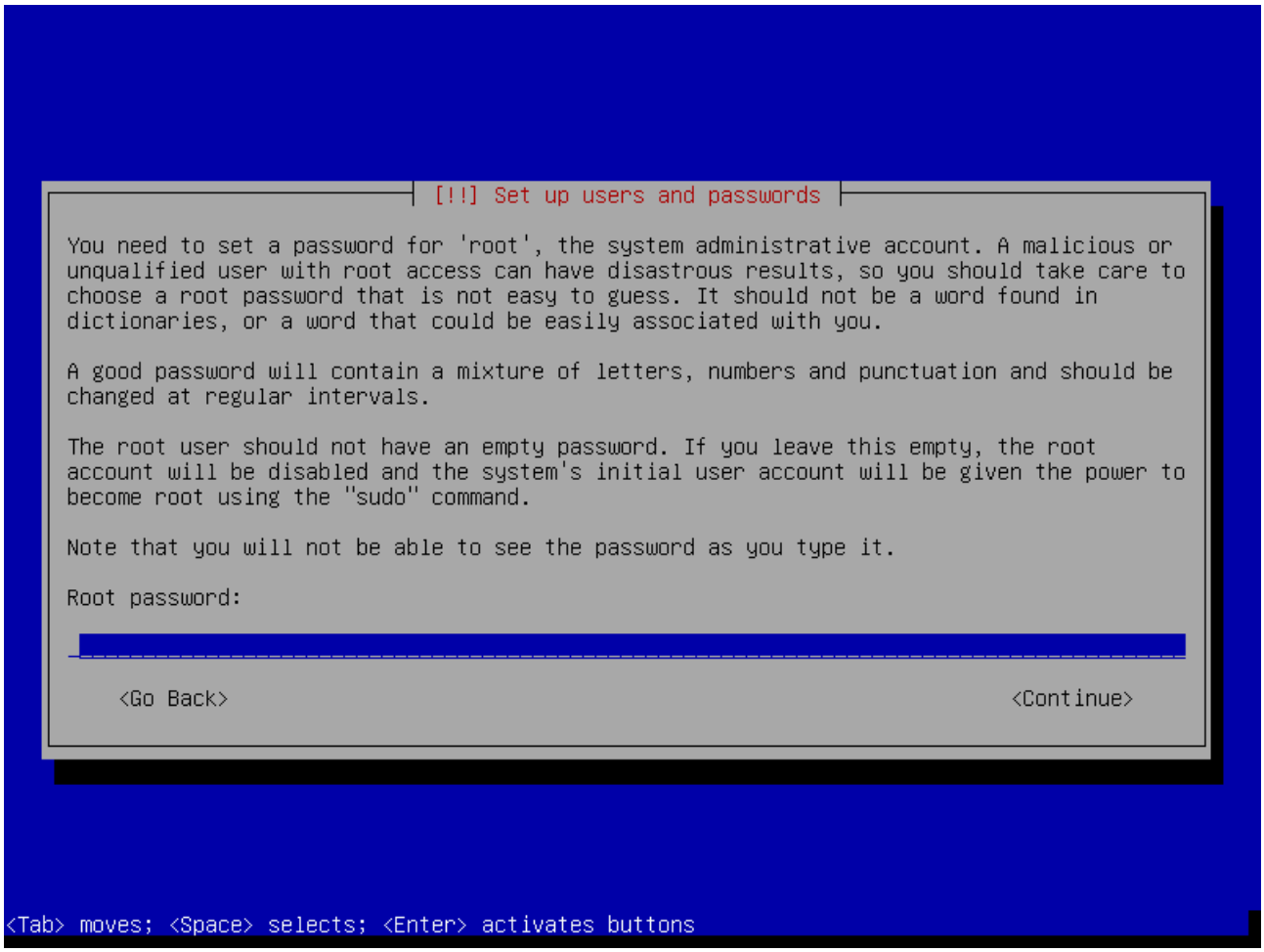
13. The next screen will ask you to choose a “Debian archive mirror” server. Again, you can just choose what the system selected by default by pressing “enter.”



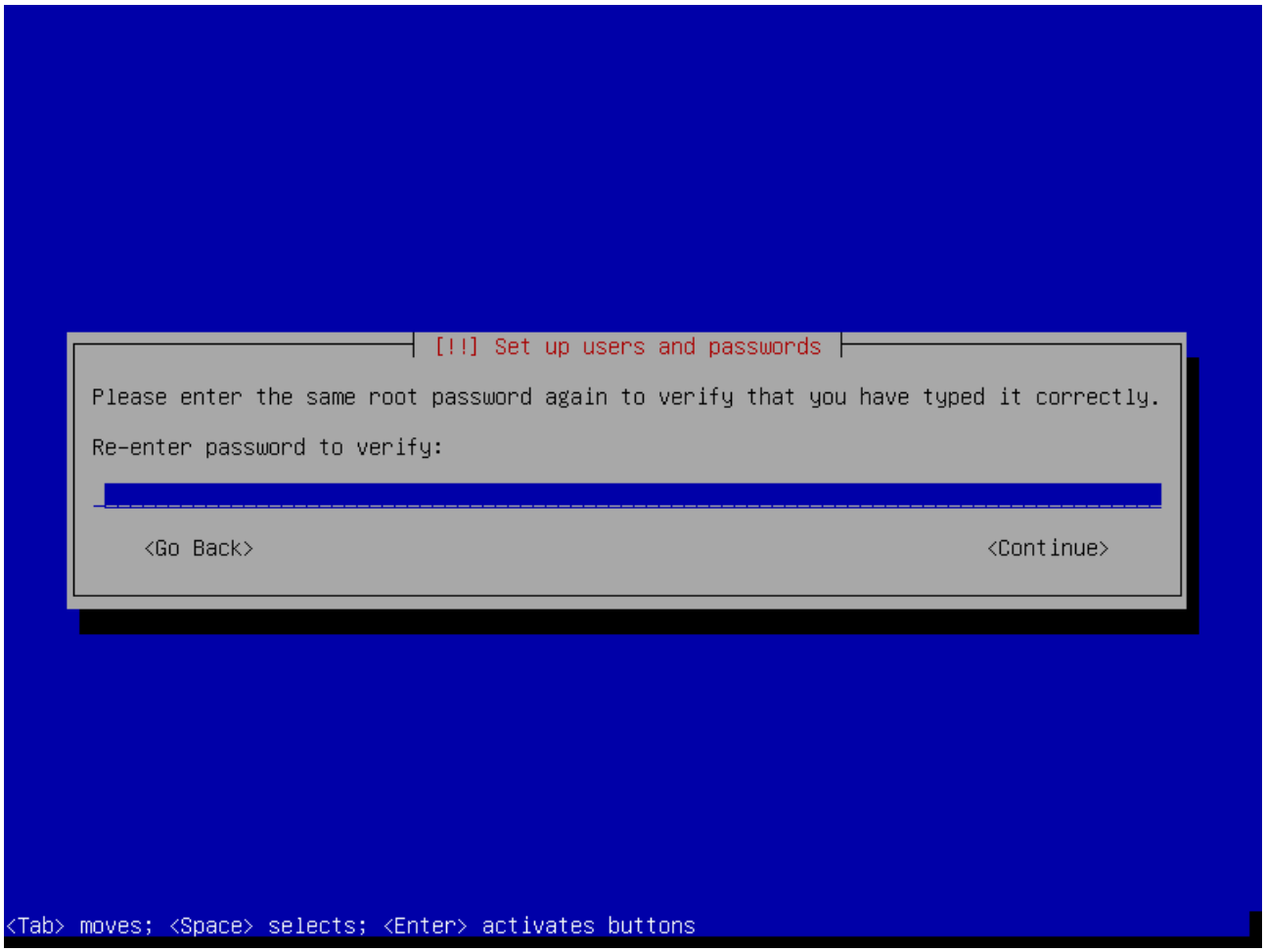
14. The next screen will ask you if you need to use a proxy to access the Internet. If you don't know the answer to that one, you don't need to use a proxy to access the Internet. Press “enter” to continue.



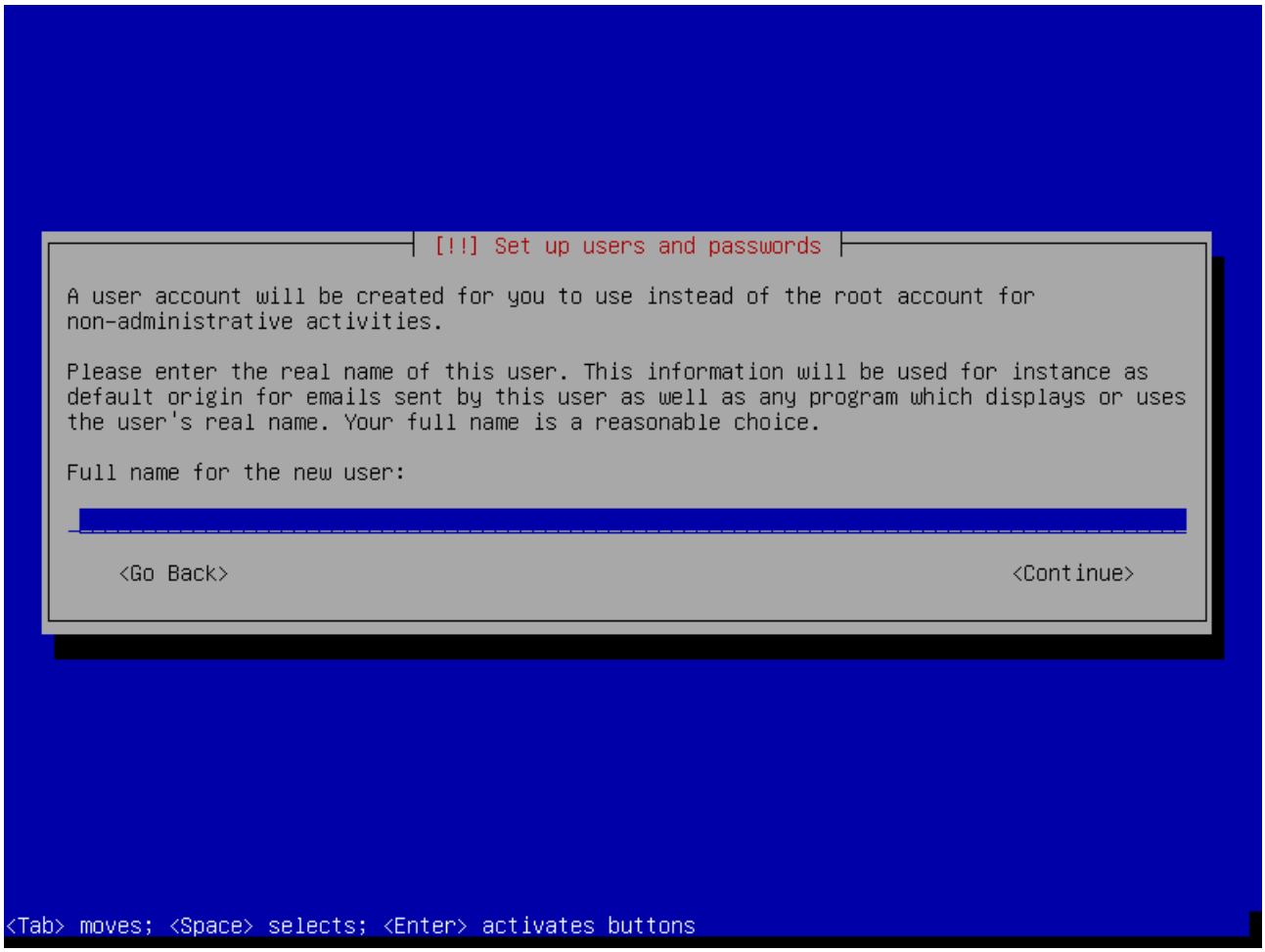
15. The next screen is where you choose the password for your “root” account. Leave the password blank so that the root account is disabled and press “enter.” The root account has the highest access on a Debian system. It is not necessary to have the root account enabled. In fact, many consider enabling the root account a security risk. You will be able to execute any command with root privileges by using the “sudo” command later.



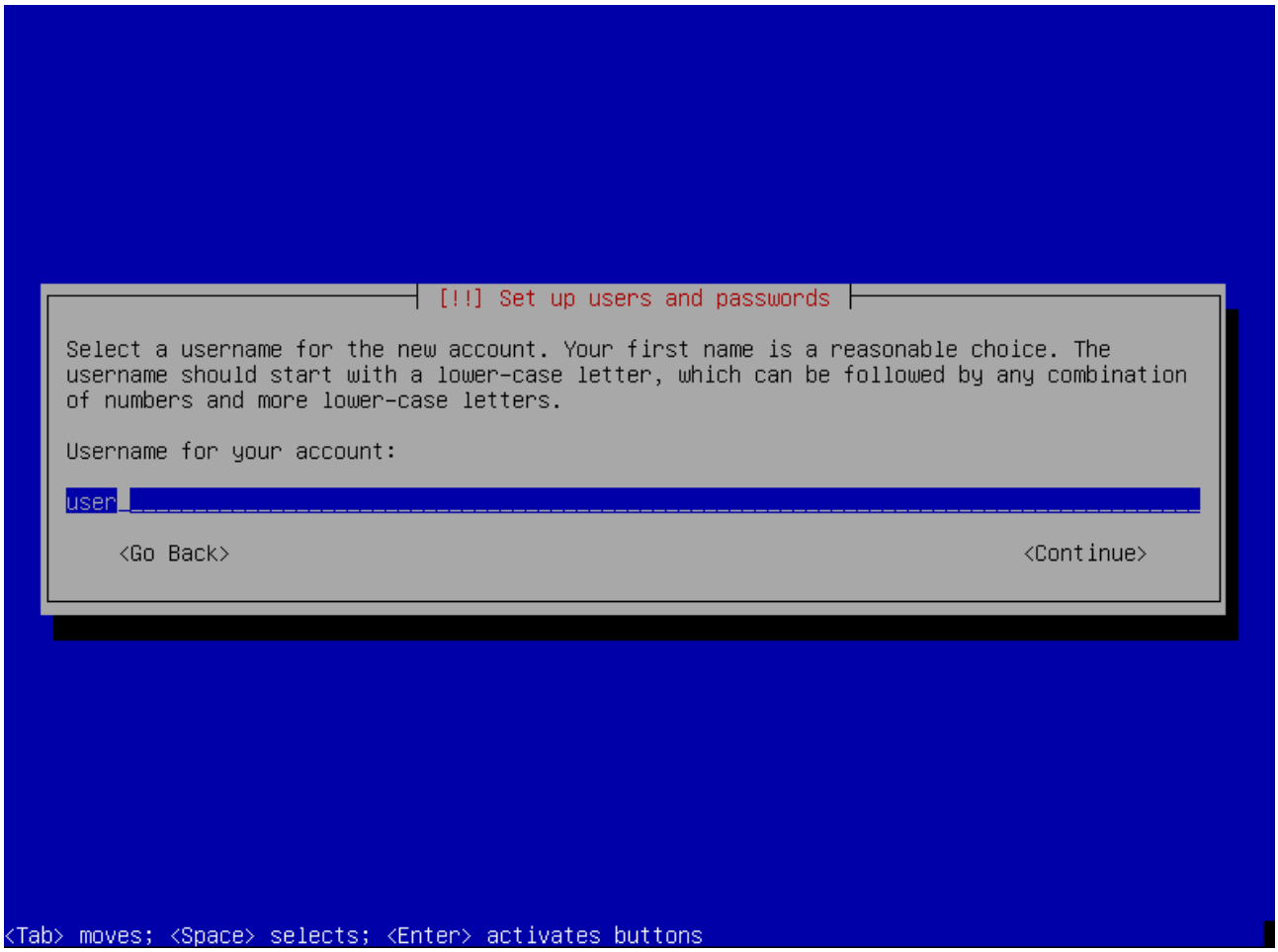
16. The next screen will prompt you to retype your root password. Simply press “enter” to continue on to the next screen.



17. The next screen will ask you for the “full name of the new user.” Leave this blank and press “enter.”

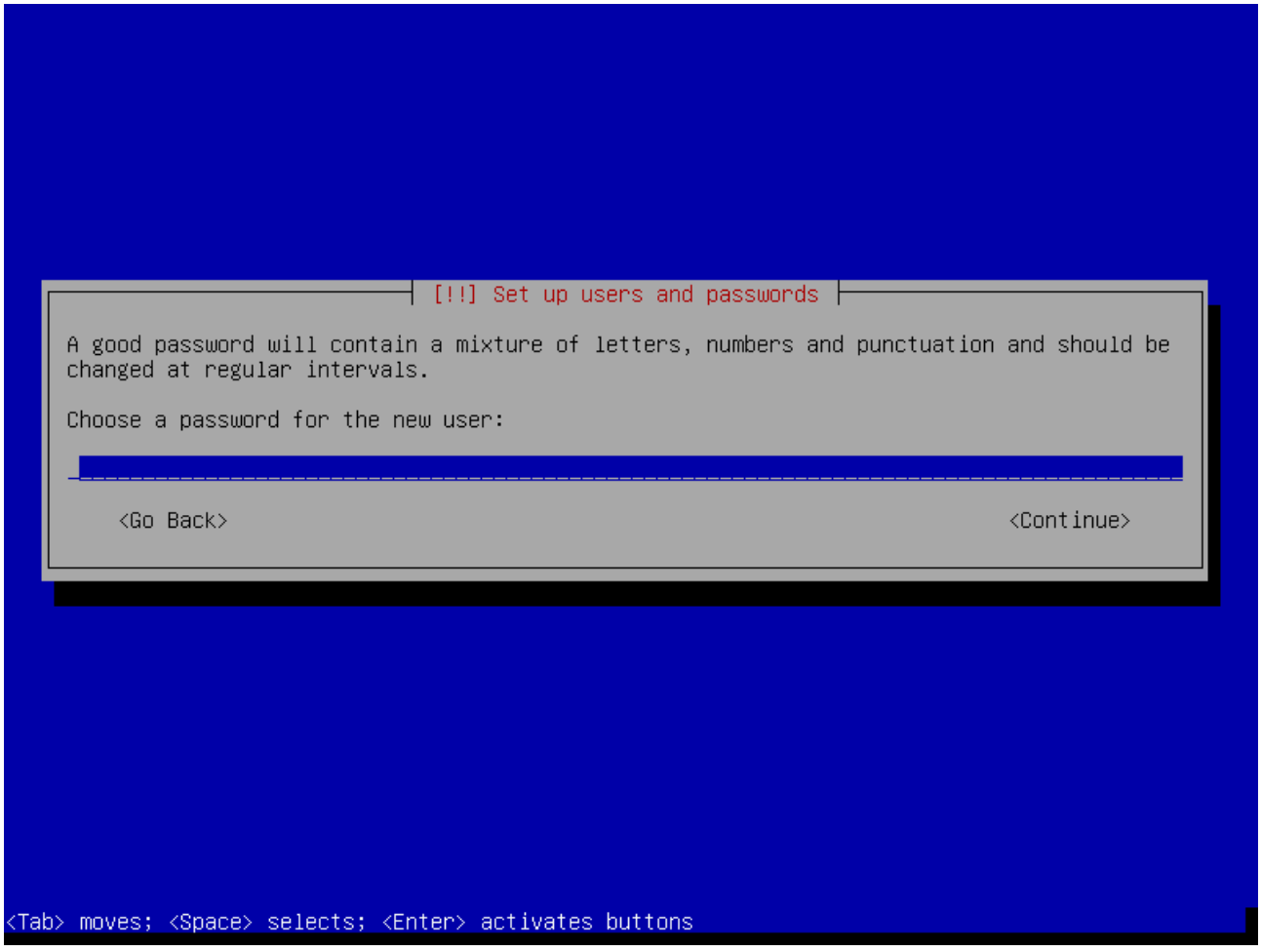


18. The next screen will prompt you to enter a “Username for your account.” Type “user” and press “enter.”

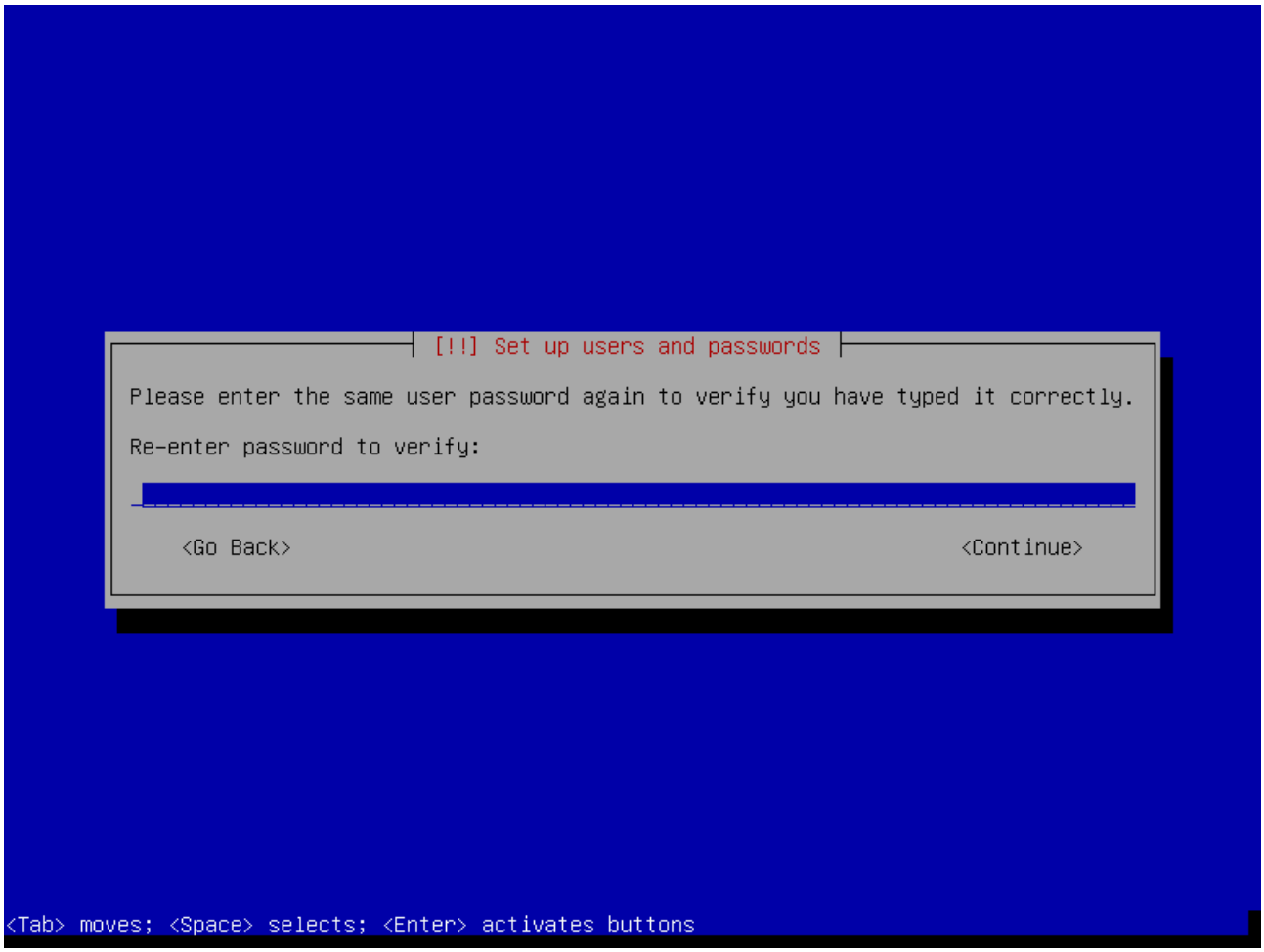


19. The next screen will prompt you to “choose a password for the new user.” It is very important for you to choose a strong password. An 8 character password is never a good password. Rather, choose something that is easy to remember but is also long. Make use of upper case and lower case letters, symbols and numbers.

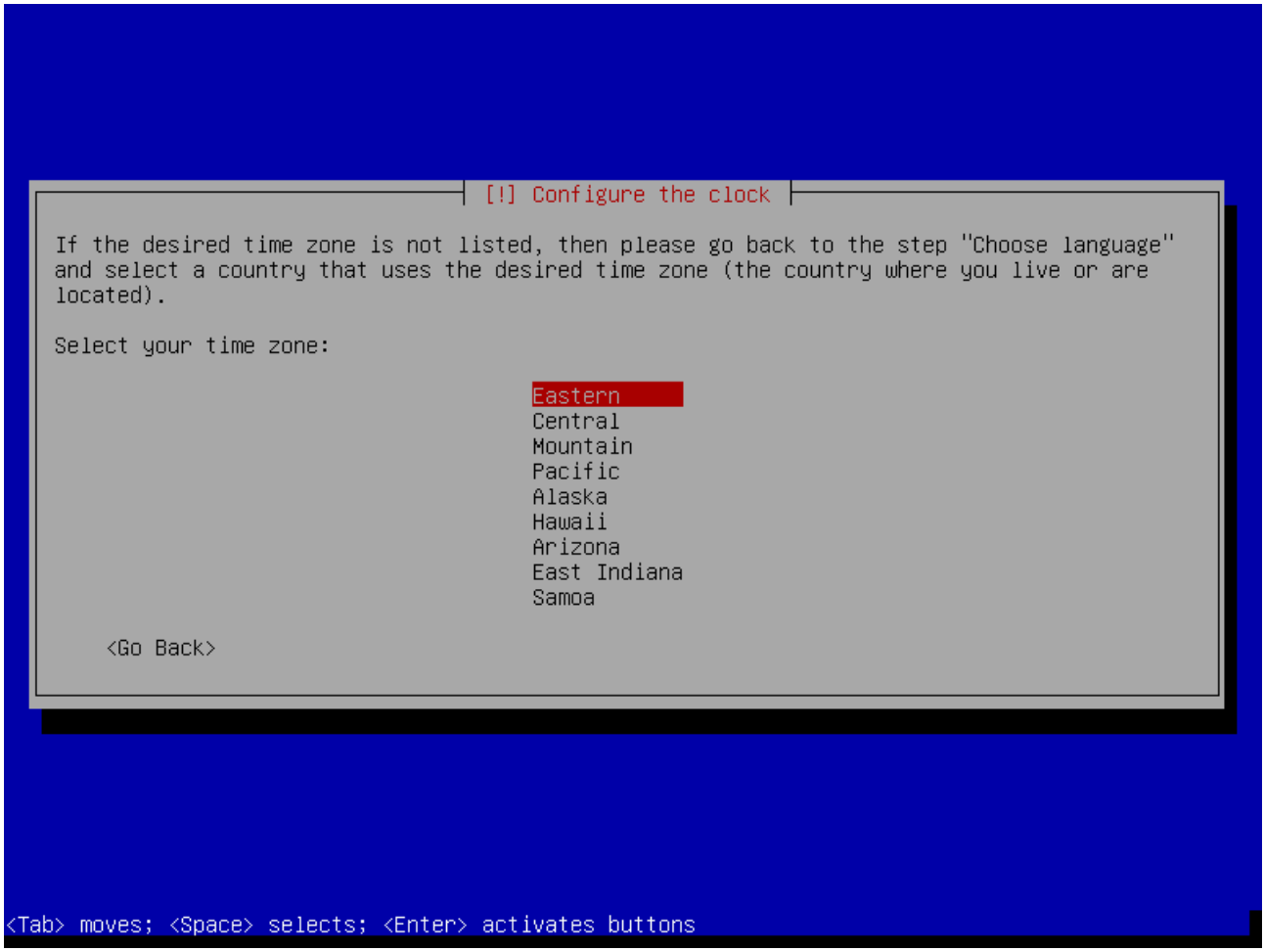
    There are numerous different mental tricks people use to create strong but memorable passwords. Some people use a combination of random words that they can easily remember padded with symbols in between like “Horse-Atlant1c!Ocean-Cheese”. Others use a nonsensical phrase. The example password is nonsensical enough that nobody is likely to guess it. Nor will a similar password appear in any stand alone dictionary file to be used for dictionary based cracking attacks. Additionally, the passwords take full advantage of the spectrum of characters on your keyboard and is lengthy enough to prevent a brute force guess based attack. For any password you create and need to remember, use such a method. **Just don't forget it.** Create your strong password and press “enter.”



20. When prompted to retype the password, retype it and press “enter.”



21. Depending on your choice of region, you may be asked to select a time zone. If prompted for such, select your corresponding time zone.



You have completed the pre-installation steps of this tutorial.

Chapter 2. Choosing your Installation Method

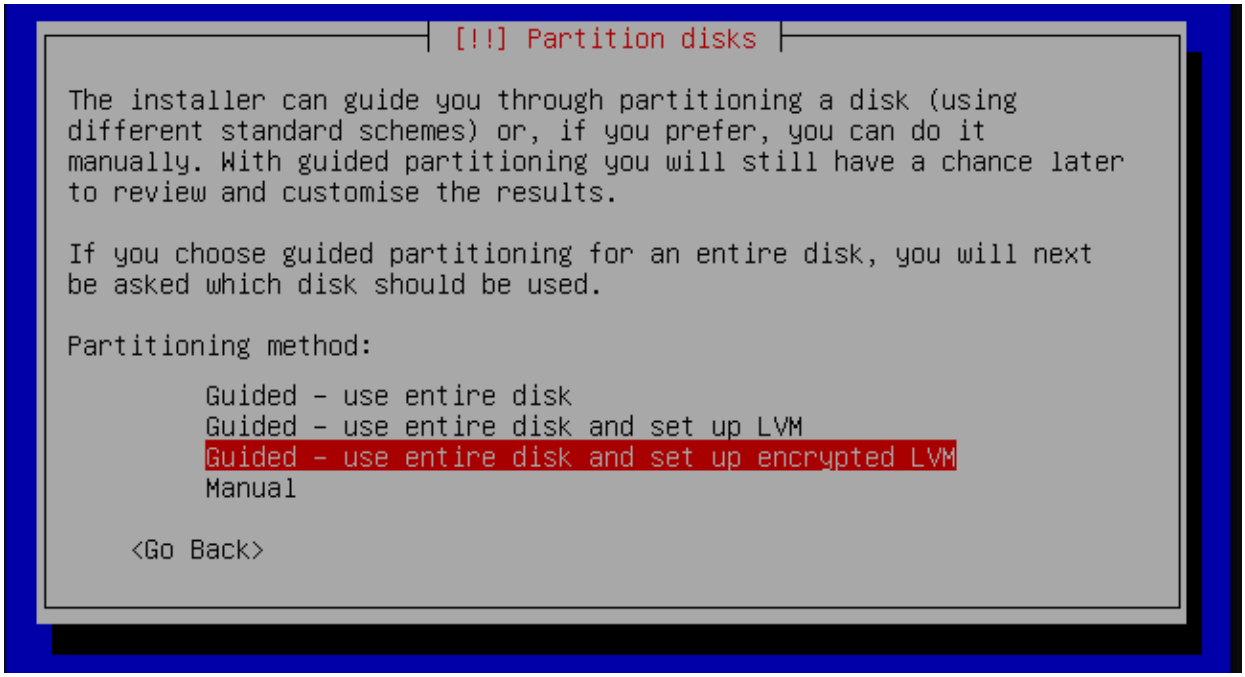
Now you have reached the point where you need to decide how you want to install your new system. As detailed in the introduction to this tutorial, one involves installing the entire operating system on an encrypted USB flash drive. The other involves installing the majority of the operating system on an encrypted internal hard drive partition and using a USB flash drive as a boot key with an encrypted key file to unlock the encrypted internal hard drive.

If you wish to use a USB flash drive for the entire operating system, continue on to Chapter 2A beginning on the next page.

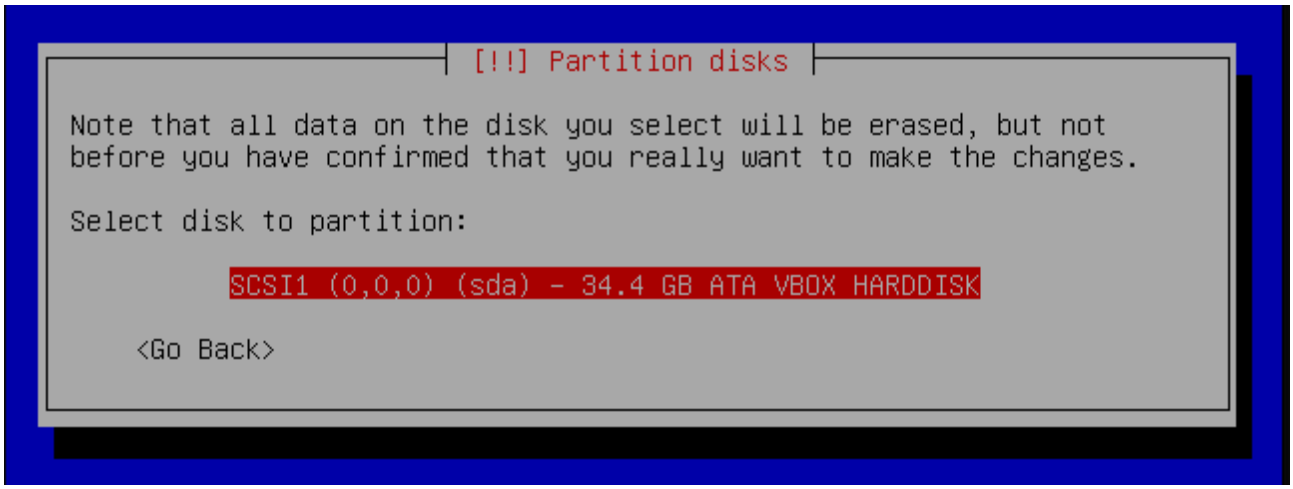
If you wish to install the operating system on an encrypted internal hard drive partition and access it with a USB flash drive boot key, continue this tutorial beginning at Chapter 2B on page 45.

Chapter 2A. Installing an Operating System on an Encrypted USB Flash Drive

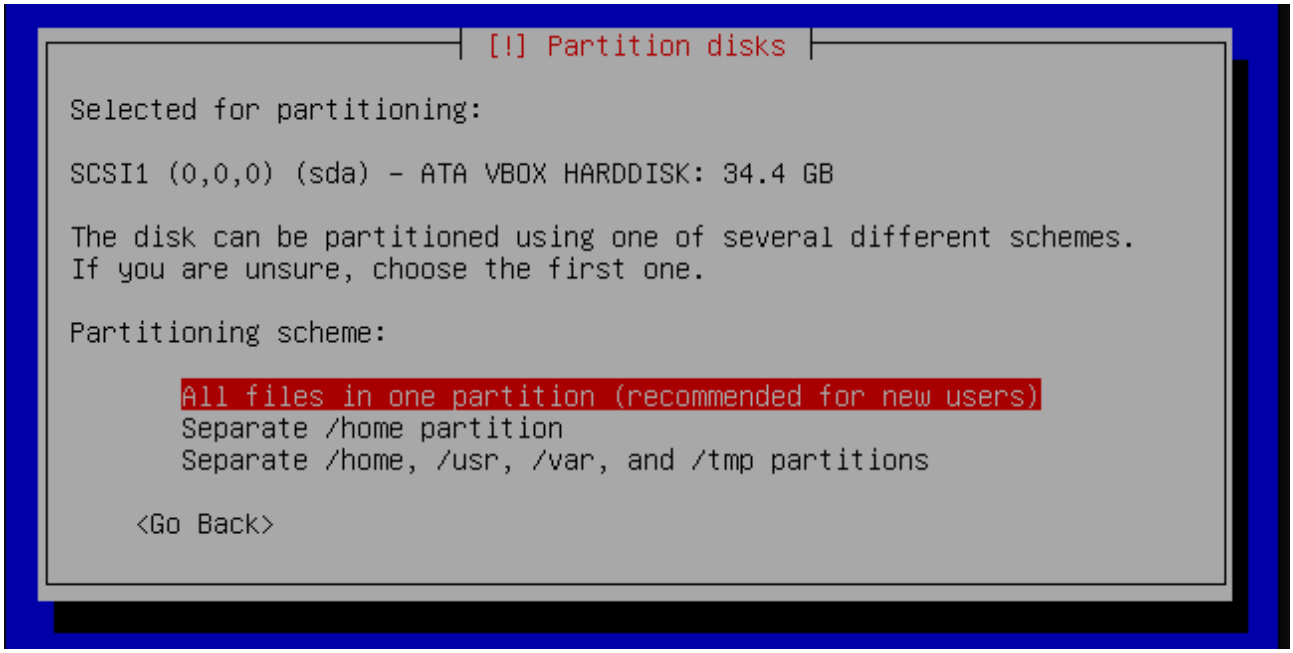
1. When prompted to select a “partitioning method.” Choose “Guided – use entire disk and set up encrypted LVM” and press “enter.”



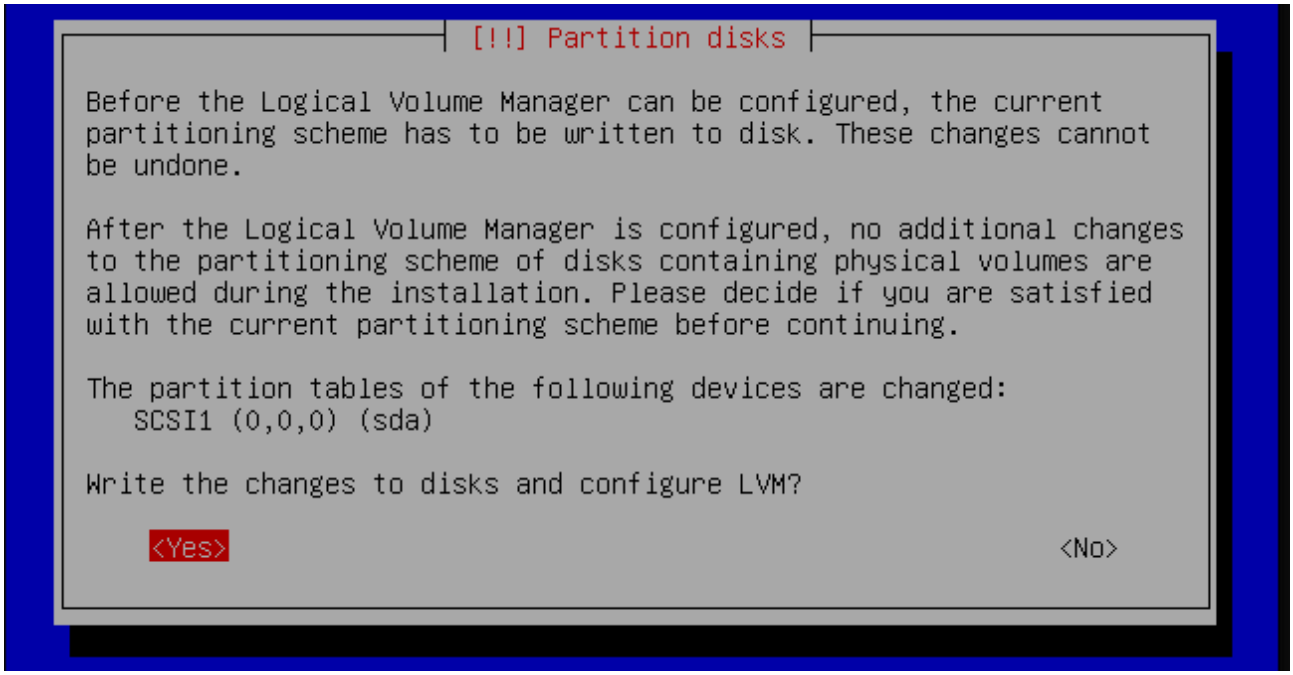
2. On the next screen that appears, choose your USB Flash Drive and press “enter.” You will likely see other choices of disks that differ from the picture below. Make sure you choose your USB Flash Drive since whichever disk you choose will be erased. The amount of disk space available on each drive can be used to determine which is your USB Flash Drive. Also, **make note of your USB Flash Drive's device name and save it for later**. **You will need to know it later in this tutorial.** In the example below, the device name is “**sda**.” It may be different for you.



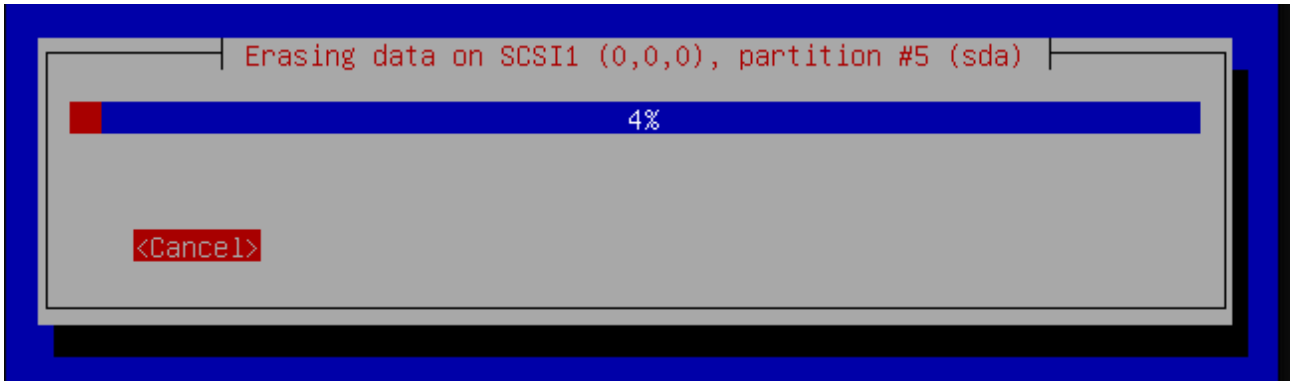
3. On the next screen, select the entry that says “All files in one partition (recommended for new users)” and press “enter.”



4. You will next be prompted to “Write the changes to disks and configure LVM.” Select “Yes” and press “enter.”



5. Next, the installation wizard will eventually begin automatically “erasing data” from your USB Flash Drive. This can take a very long time. If you've ever used the drive to store data that is related to your personal identity, it is probably best to let this process finish. However, if it is a new drive, or you don't have the patience, you can select “cancel” and continue to the next step. All new data that is written to your USB Flash Drive will be encrypted. However, old data on the disk left over from before you encrypted it may be discoverable through digital forensics.



6. On the next screen, you will be prompted for your encryption passphrase. **It is imperative that you choose a very strong passphrase! Otherwise, encrypting your flash drive will simply amount to a waste of time!** As was discussed earlier in step 19 of chapter 1, an 8 character password is never a good passphrase. Since the Debian Installer is making use of the cryptsetup program and the LUKS encryption system, the following breakdown of the importance of a strong passphrase comes from the developer.

   "First, passphrase length is not really the right measure, passphrase entropy is. For example, a random lowercase letter (a-z) gives you 4.7 bit of entropy, one element of a-z0-9 gives you 5.2 bits of entropy, an element of a-zA-Z0-9 gives you 5.9 bits and a-zA-Z0-9!@#$%^&:-+ gives you 6.2 bits. On the other hand, a random English word only gives you 0.6...1.3 bits of entropy per character. Using sentences that make sense gives lower entropy, series of random words gives higher entropy. Do not use sentences that can be tied to you or found on your computer. This type of attack is done routinely today. To get reasonable security for the next 10 years, it is a good idea to overestimate by a factor of at least 1000.

   Then there is the question of how much the attacker is willing to spend. That is up to your own security evaluation. For general use, I will assume the attacker is willing to spend up to 1 million EUR/USD. Then we get the following recommendations:

   LUKS: Use > 65 bit. That is e.g. 14 random chars from a-z or a random English sentence of > 108 characters length.

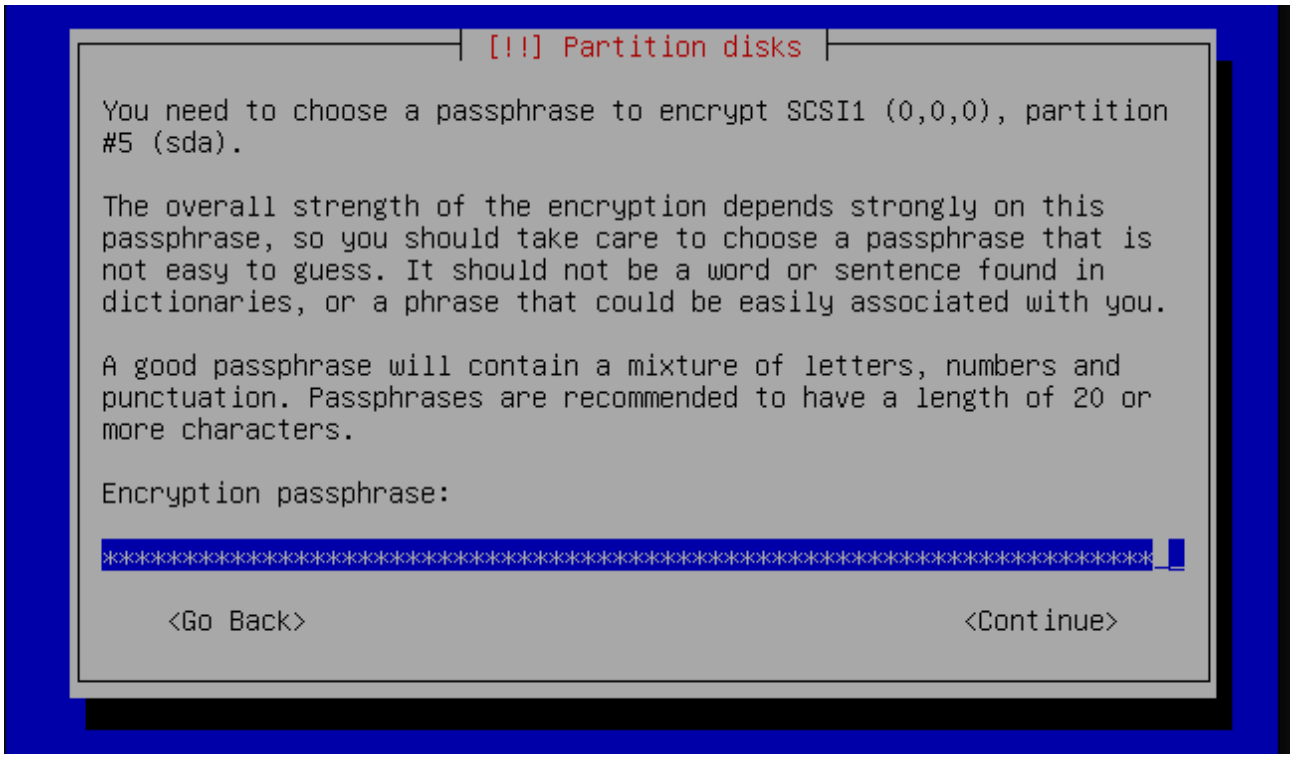
   If paranoid, add at least 20 bit. That is roughly four additional characters for random passphrases and roughly 32 characters for a random English sentence."

   https://code.google.com/p/cryptsetup/wiki/FrequentlyAskedQuestions#5._Security_Aspects

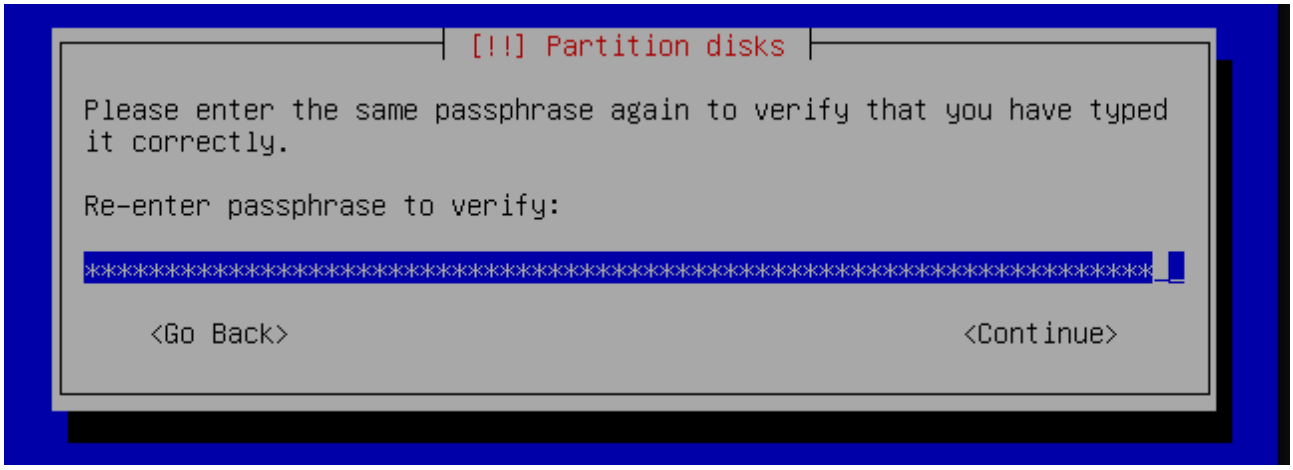
   Not in the mood to do math? The lesson to take away is that length, randomness and nonsense matter. They will get you more entropy. There are many tricks people use to come up with a nonsensical passphrase that they remember. For example, you could use a play on a favorite line from a movie you enjoy combined with a date you would remember like "If My Calculations Are Proper, When This Baby Hits 88 Miles Per Hour, You're Going 2 See Some Serious Business! January-1-2013?". This is a very secure type of passphrase that has plenty of entropy per the suggested numbers by the developer of cryptsetup.

   For further discussion of strong passphrases, go to https://www.grc.com/haystack.htm.

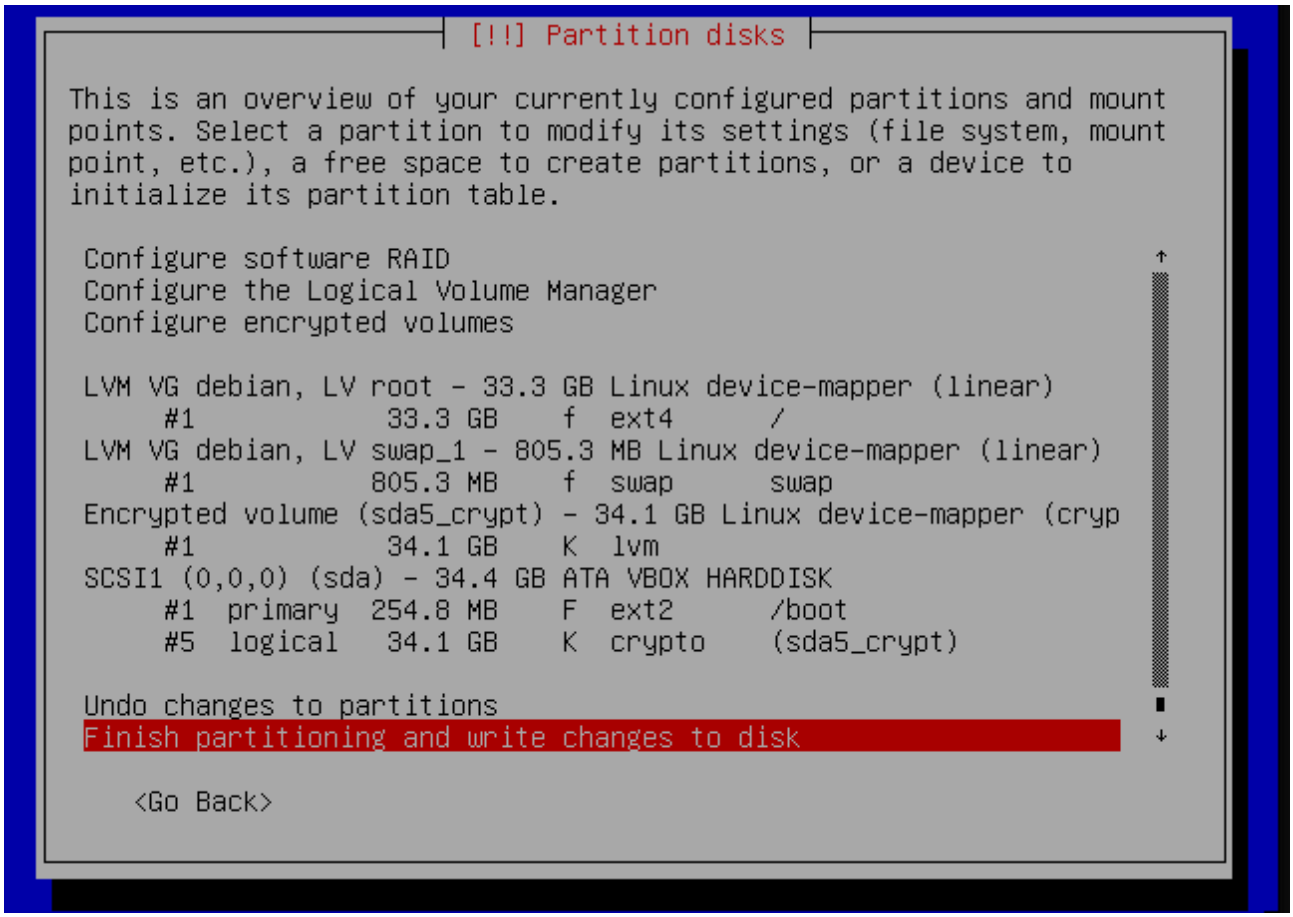
Once you have decided upon a strong passphrase, type it into the “encryption passphrase” field and press “enter.” **Remember, if you forget this passphrase, you have lost everything on your disk! Make sure you remember it! It cannot be recovered!**



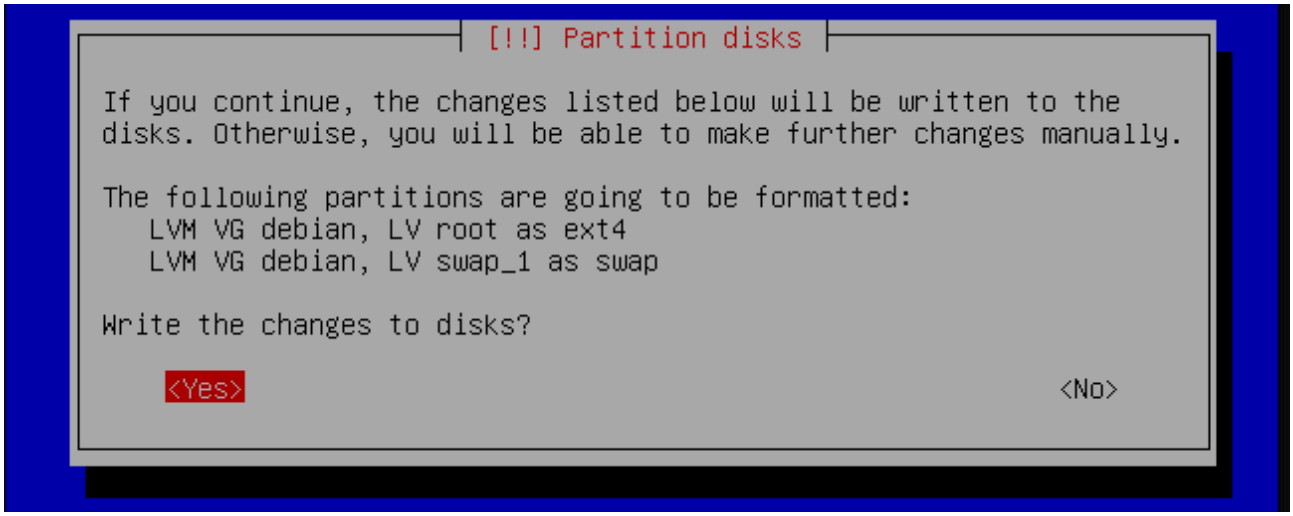
7. On the next screen, you will be prompted to confirm your encryption passphrase. Retype it and press “enter.”



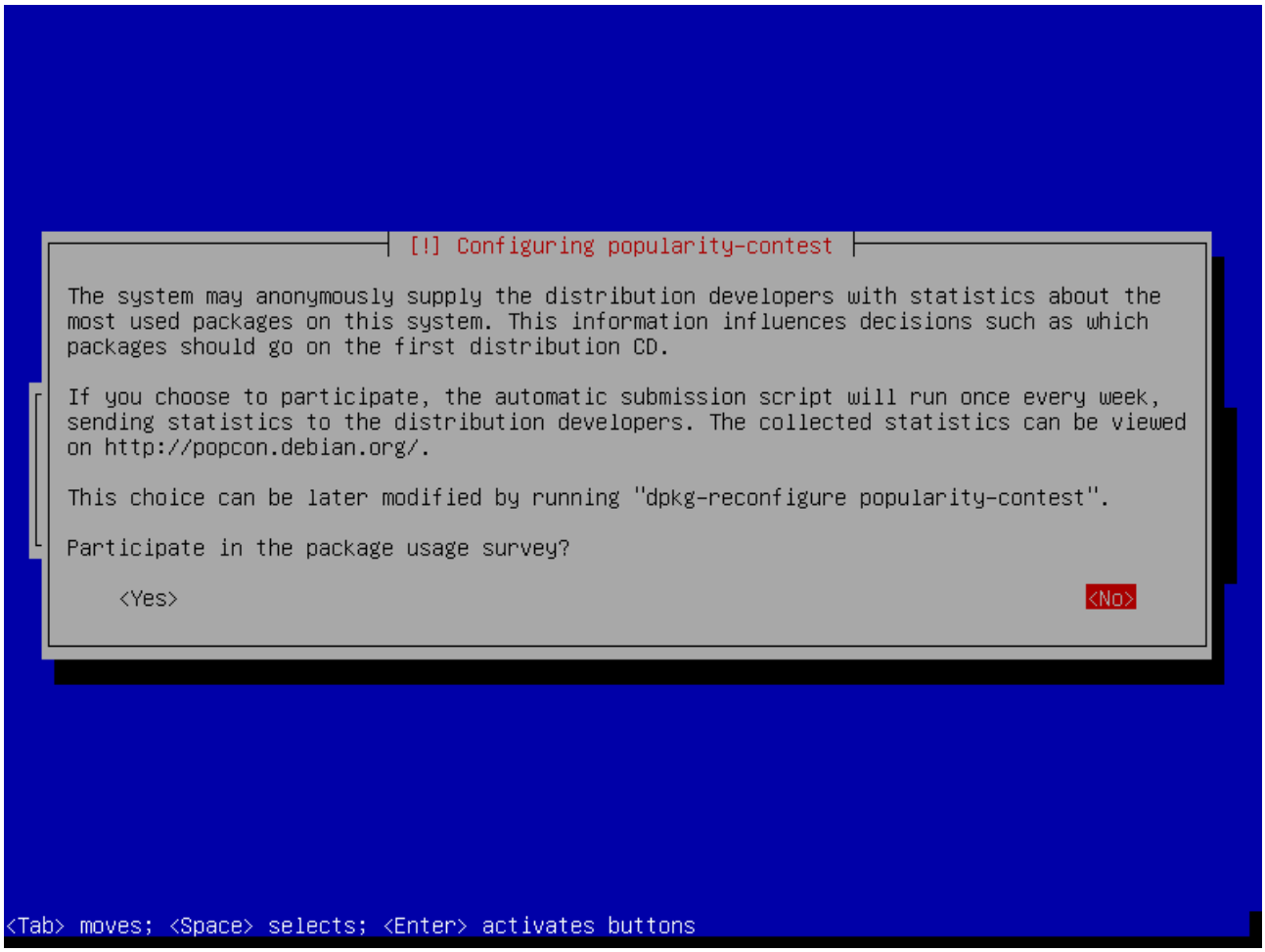
8. On the next screen, select “Finish partitioning and write changes to disk” and press “enter.”



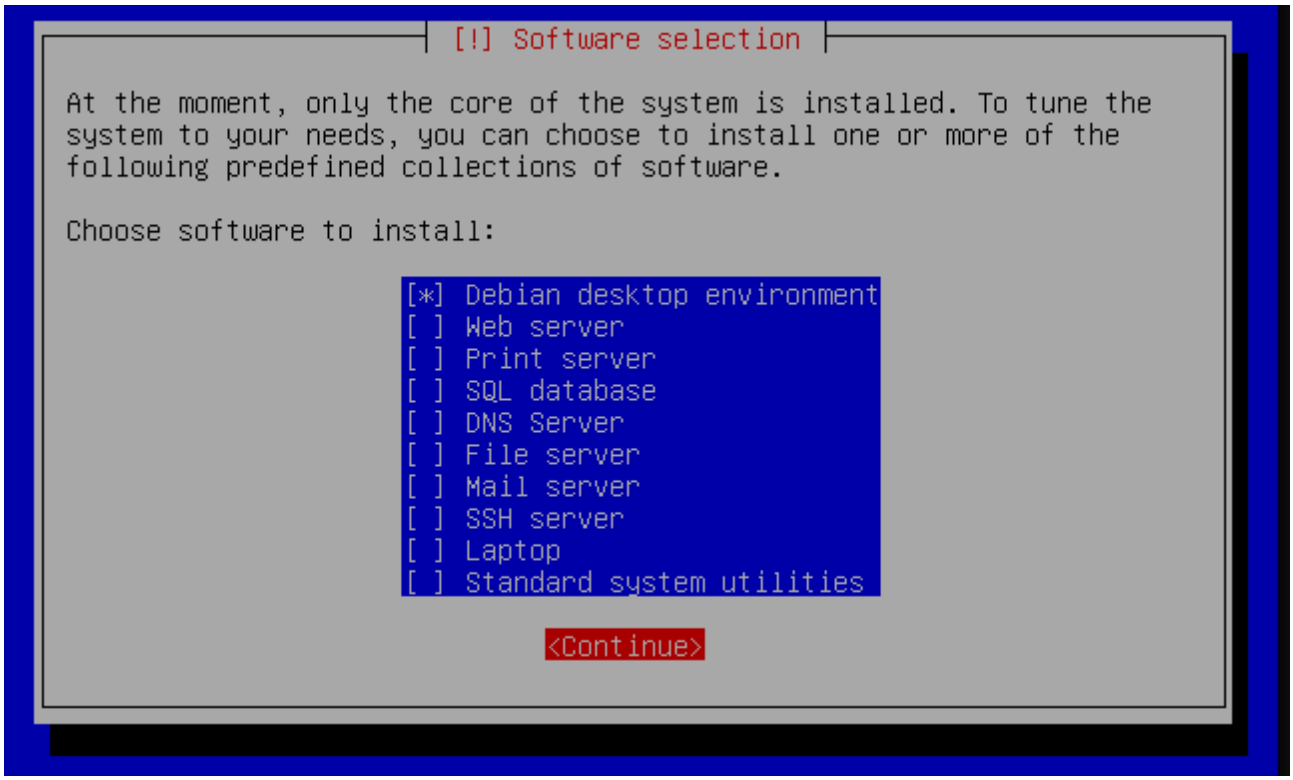
9. The next screen will ask if you want to write the changes to disks. Select “yes” and press “enter.”



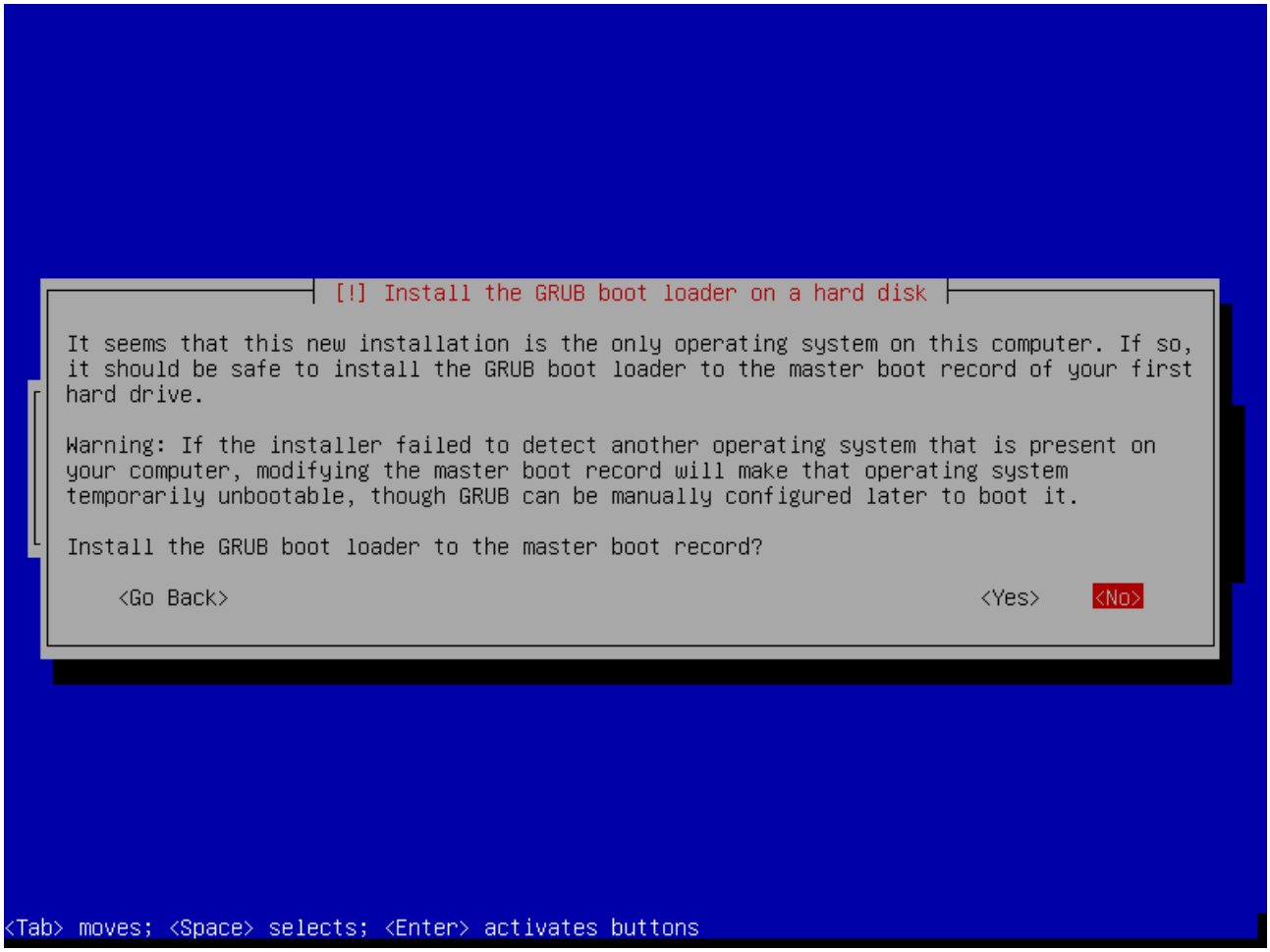
10. The installer will now begin “retrieving files” and installing the required packages for the OS. At the next prompt, it will ask you if you want to “participate in the package usage survey.” Select “no” and press “enter.”



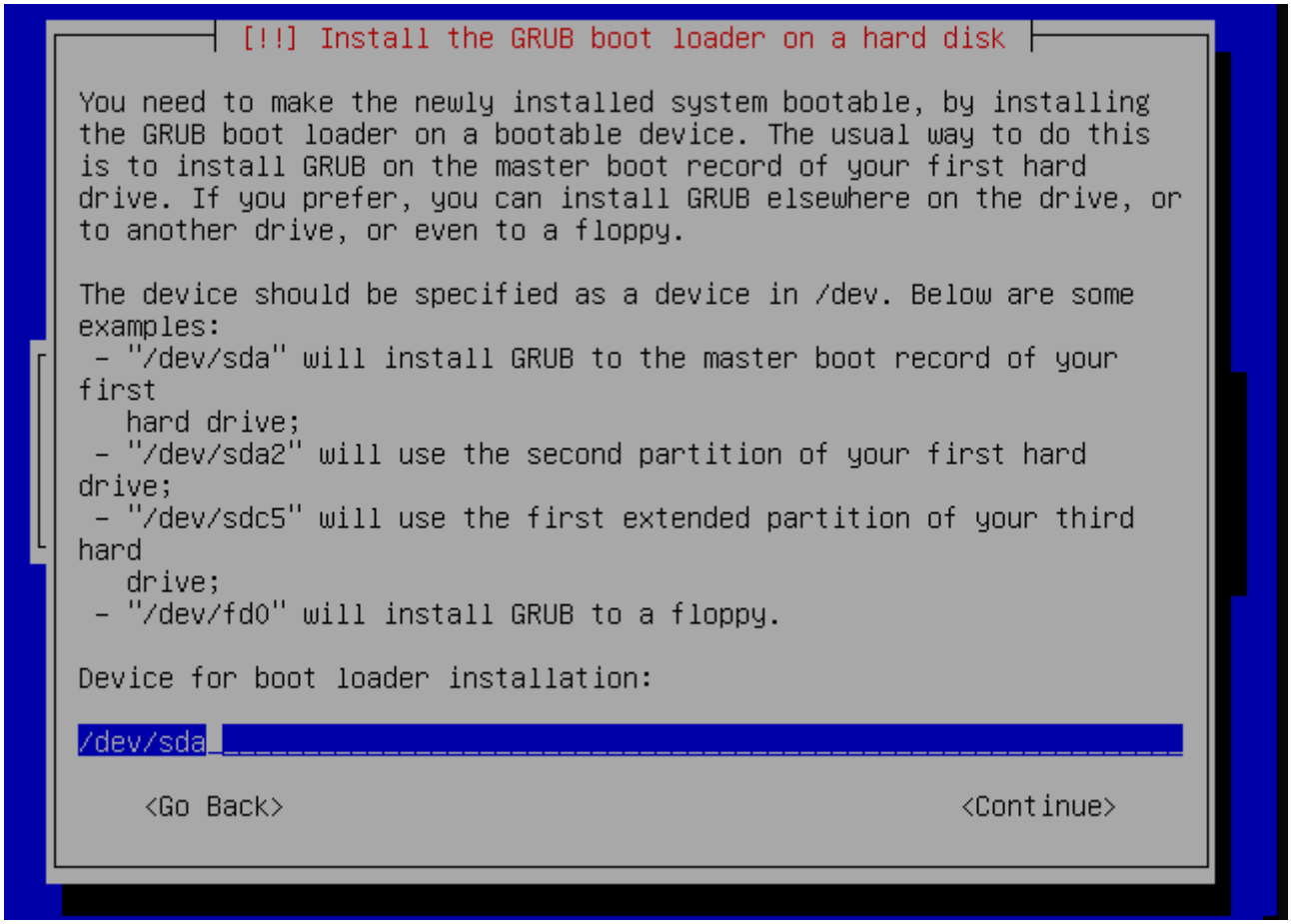
11. The installer will again perform some tasks until it prompts you to “choose software to install.” You only need to install the “Debian Desktop Environment.” Unselect the other chosen items by moving the arrow key until they are highlighted and pressing the space bar. When the “*” disappears, the item is unselected. When your screen looks like the screen shot below, press “enter” to continue.



12. The installer will now begin retrieving files and will then install them. This will take a long time. Eventually, you will be asked if you want to “Install the GRUB boot loader to the master boot record.” The screen shot below will not likely look the same as your's, as it will probably have discovered additional operating systems. This is not something you need to be concerned about. Select “no” and press “enter.”

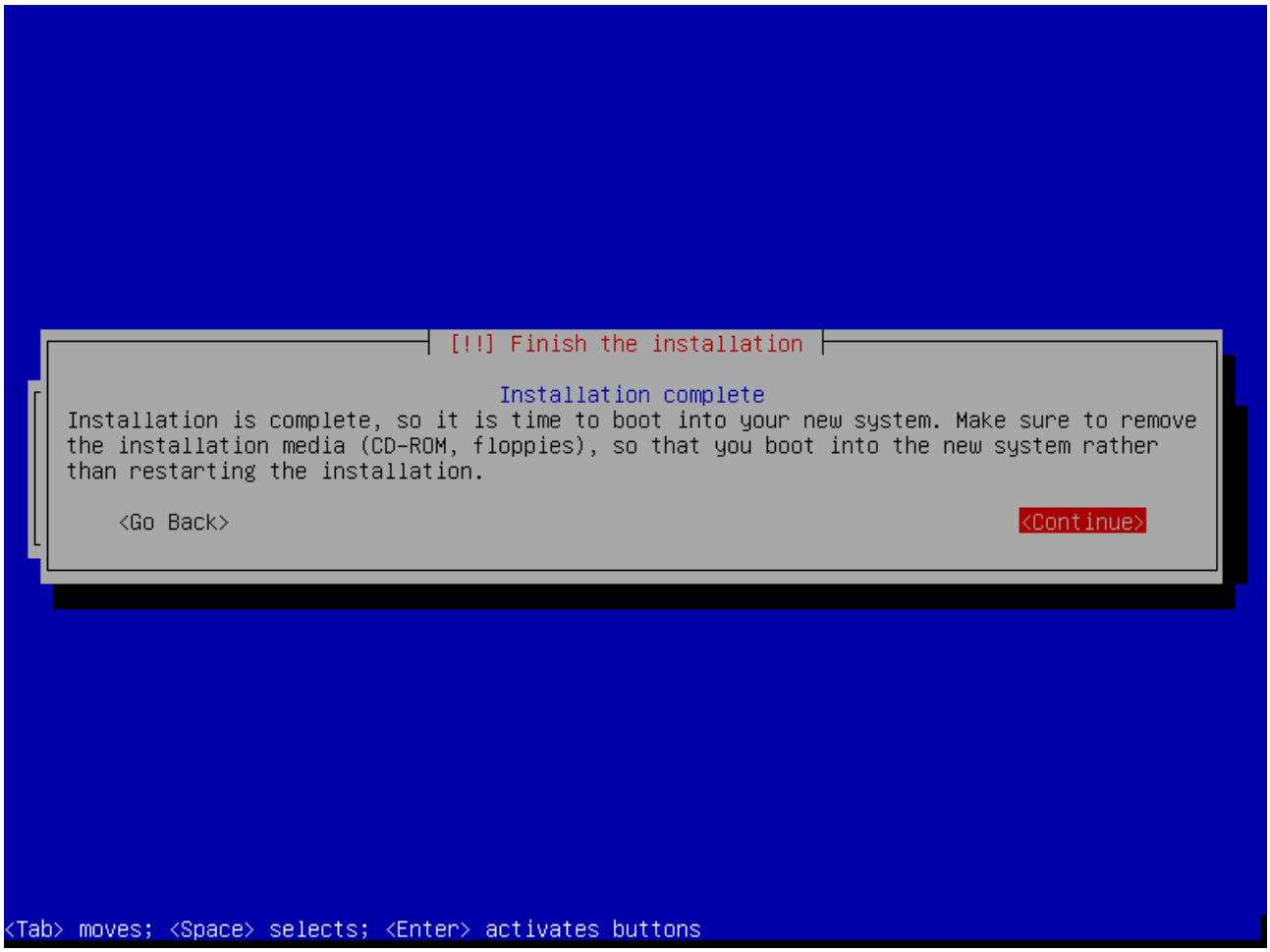


13. The next screen will ask you to type the “Device for boot loader installation.” In step 2 of this chapter, you were instructed to make a note of the device name that was the USB flash drive where you were installing Debian. The example used in this tutorial was “sda.” You need to enter the device name for your USB flash drive. However, the name needs to be preceded by “/dev/”. Thus, in the example in this tutorial, the entry would be “/dev/sda”. You need to enter the name of your device which will be in the format of “/dev/YourDeviceName” and press “enter.”

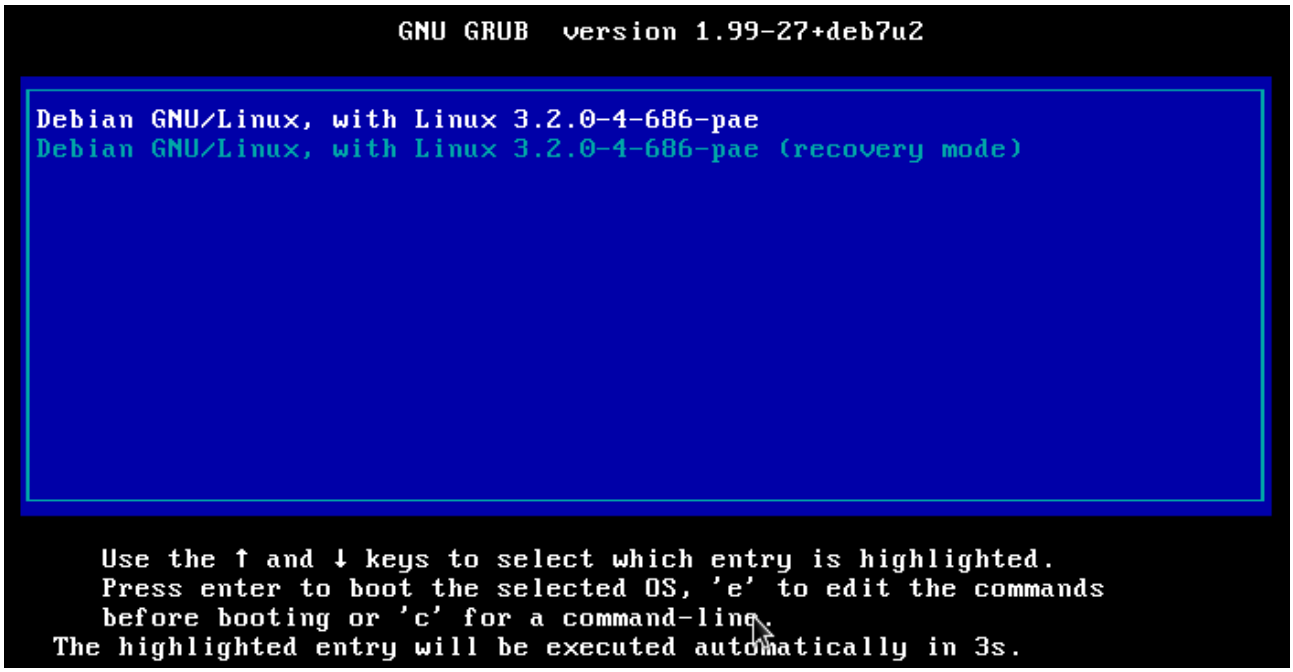


14. Now the installer will go through the process of finishing the installation. You will eventually be informed that the installation is complete. Select “continue” and press “enter.”

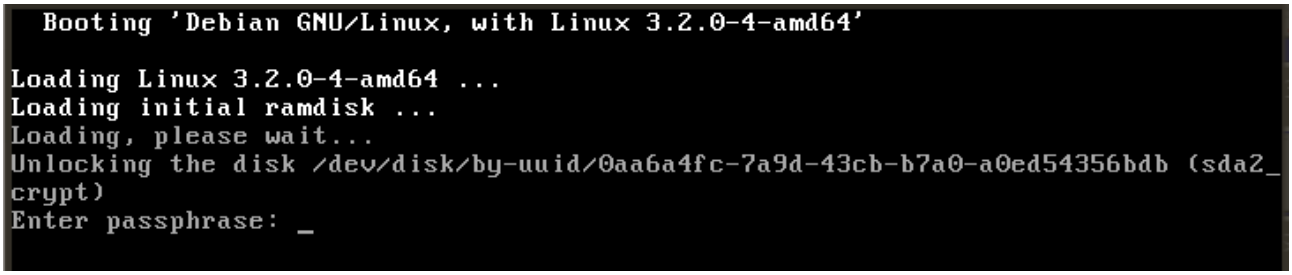
    NOTE: If the installation process took long enough to make you run out of time, you can shut down your computer at this point after the installer goes through the clean up process and restarts the machine. You can then continue from step 15 at a later time.



15. The installer will eventually reboot your computer. As your computer restarts, you need to get into a boot menu again in the same manner the you did in step 4 of chapter 1. When you activate the boot menu, choose your USB flash drive on which you installed Debian. Eventually, you will be prompted to choose a boot selection. It will default to Debian and, thus, you can either press “enter” or wait for the timer to run out. The example screen below may not look exactly the same as your's. But, it is essentially the same thing.



16. The next screen will prompt you to “enter passphrase.” This is the encryption passphrase you created in step 6 of this chapter. You will not see any symbols on your screen when you type your password. While this may seem odd, it is for security reasons. Someone watching your screen won't be able to determine the length of your passphrase. Type your passphrase and press “enter.”



17. Debian will now go through its boot process. Eventually you will reach the login window. When you reach the login window, press “enter” or click on “user.”

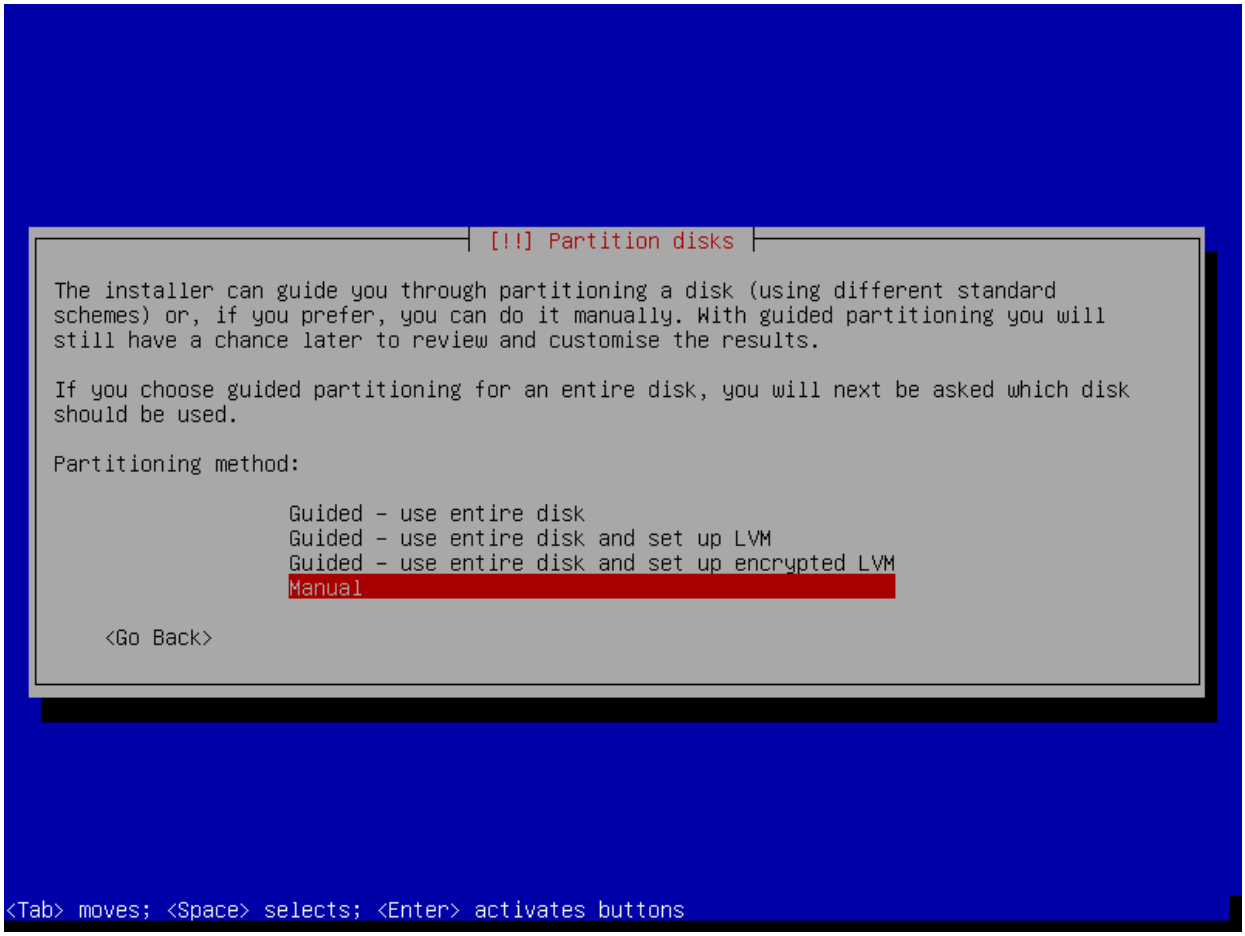
18. On the next screen, you will be prompted for your password. Before typing your password, click on the pull down menu that says “system default” and select “GNOME Classic.” Then, type the password you created for “user” in step 19 of chapter 1 and press “enter.” Debian will use “GNOME Classic” for every other login until you choose something different.

Congratulations! You now have a fully functional encrypted USB flash drive running Debian. At this point, continue the tutorial starting from Chapter 3 at page 124.

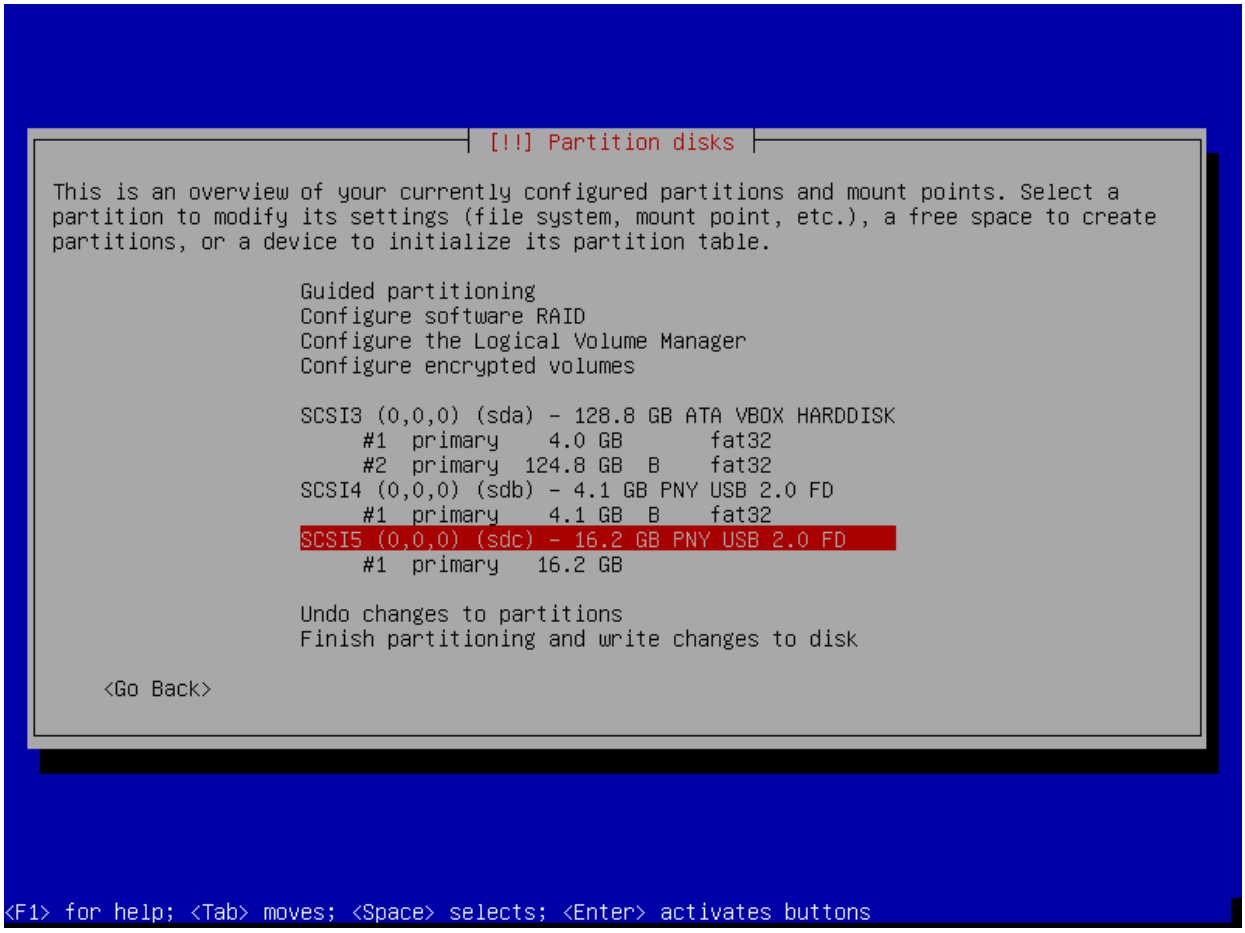
Chapter 2B. Installing the Operating System on an Encrypted Internal Hard Drive Partition with a USB Flash Drive Boot Key

As was stated earlier, if you have any sensitive files you may be worried about losing, **please back them up before beginning this process if you haven't already**. While it is unlikely that anything bad will happen, since you will be resizing an existing partition on your hard drive, there is a chance of data loss. With that out of the way, let's begin.

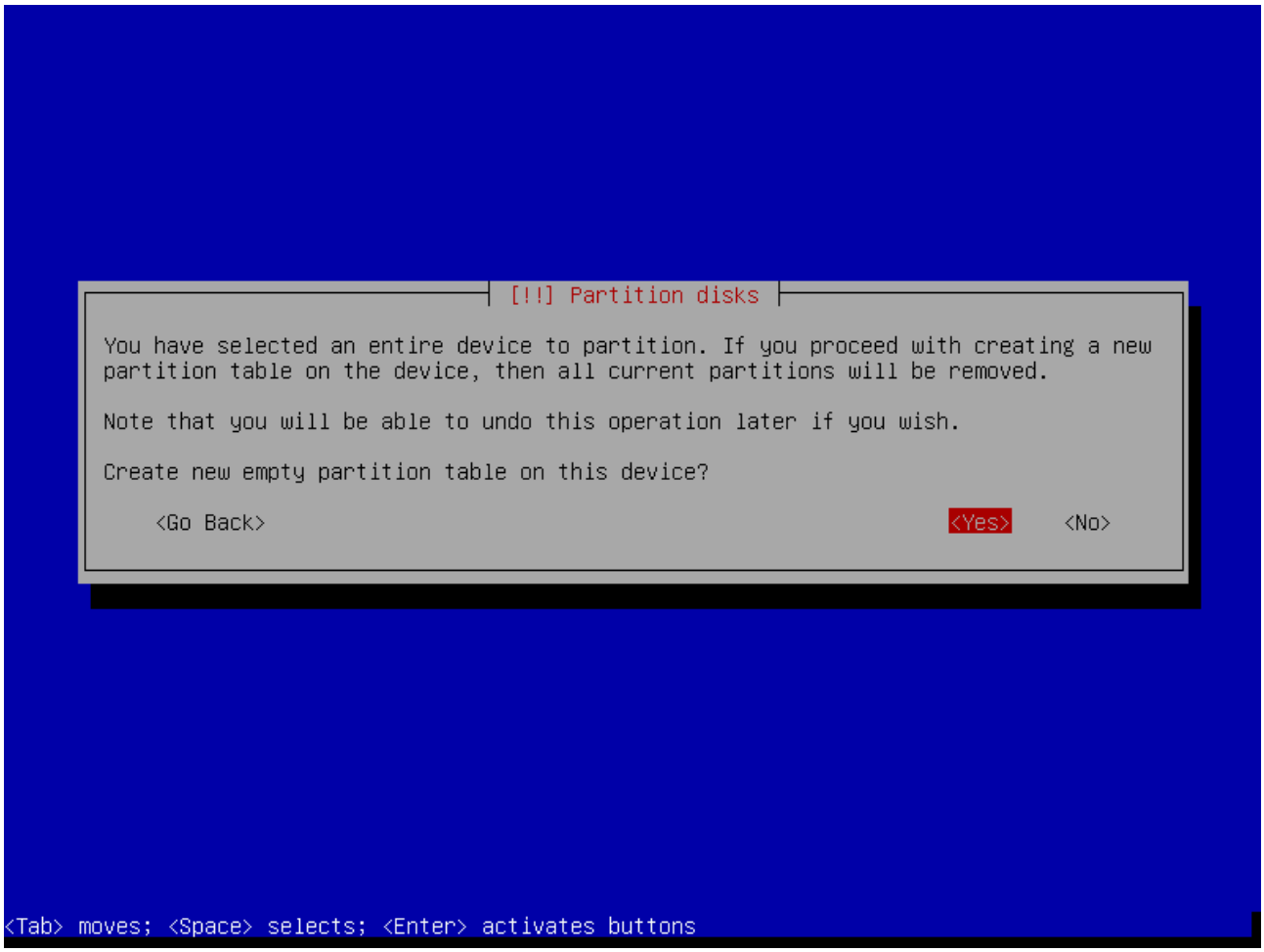
1. When prompted to select a “partitioning method.” Choose “manual” and press “enter.”



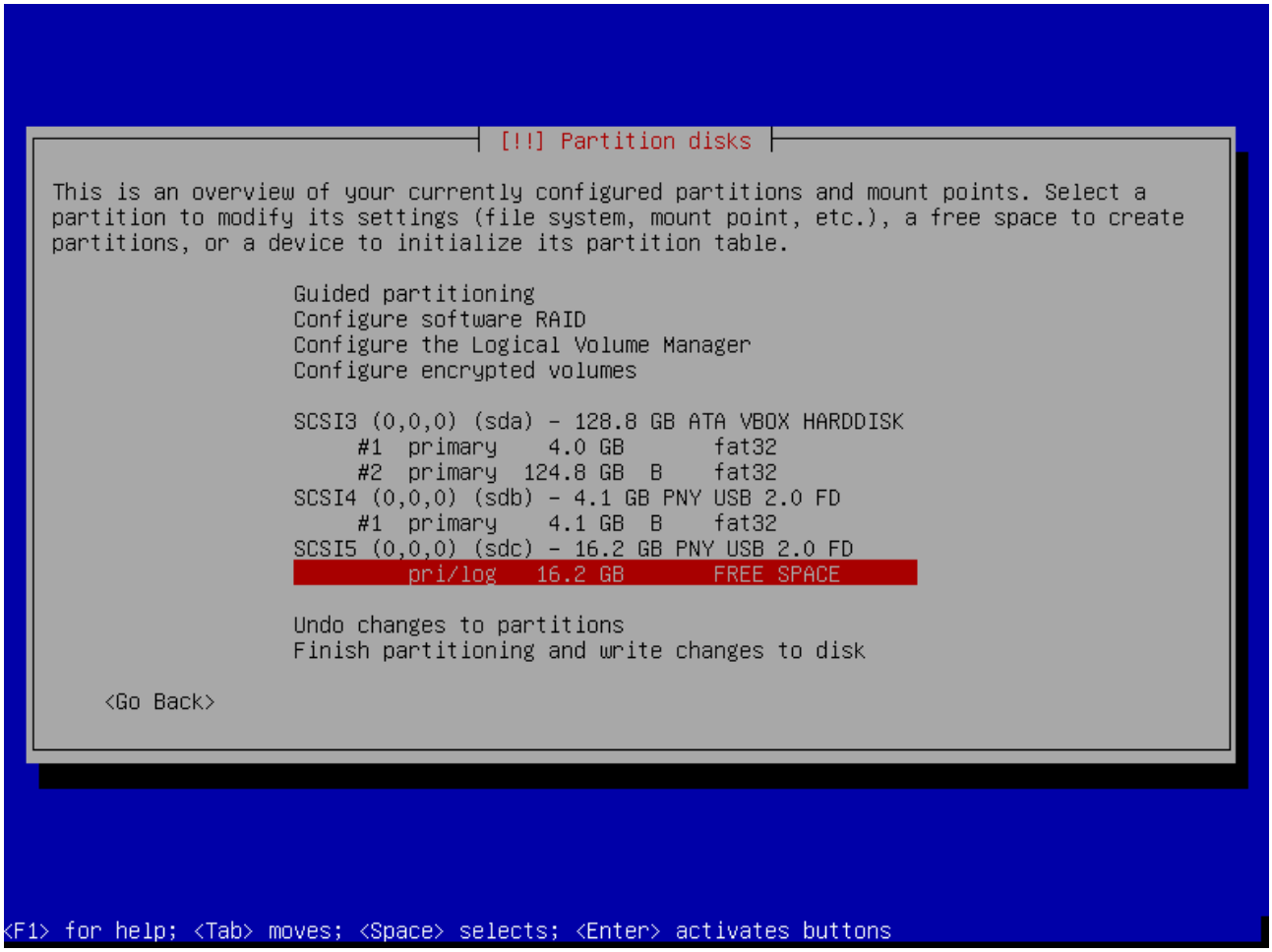
2. First, you need to prepare the USB Flash Drive to use as the Boot Key Disk in addition to making a note. In the image below, the USB Flash Drive I want to use as the Boot Key Disk is displayed as “SCSI1 (0,0,0) (**sdc**)” and the internal hard drive where the Debian root system will be installed is “SCSI3 (0,0,0) (sda).” Of particular importance is the device name of the flash drive which will be your Boot Key Disk. In the example below, it is “**sdc**.” However, it will likely be different on your computer. **Make note of your USB Flash Drive's device name and save it for later**. **You will need to know it later in this tutorial.** Select the flash drive you desire to use as the Boot Key Disk and press “enter.”



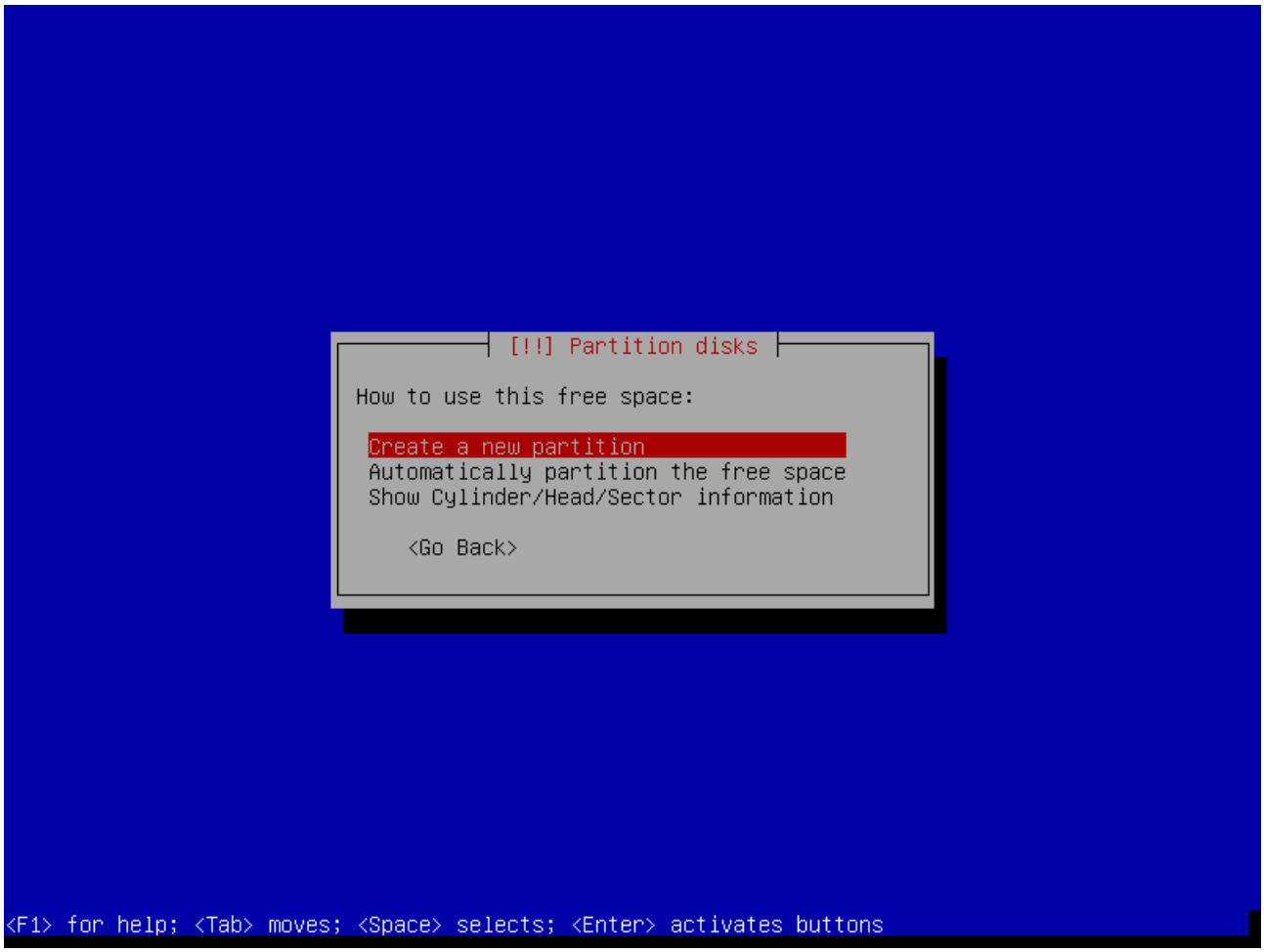
3. On the next screen that appears, choose “yes” and press “enter.”



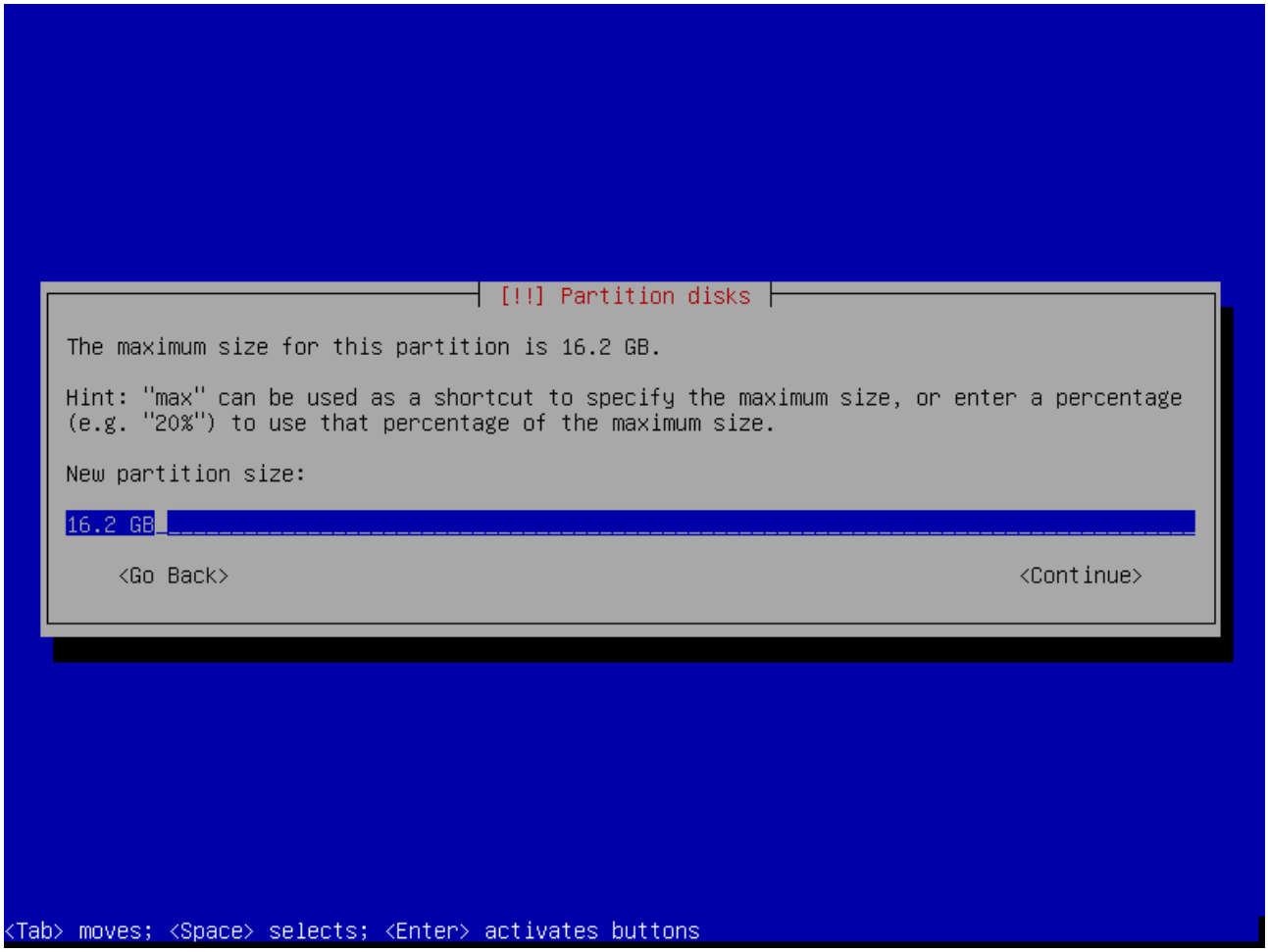
4. On the next screen, you will now see an entry labeled as “FREE SPACE.” Select that entry and press “enter.”



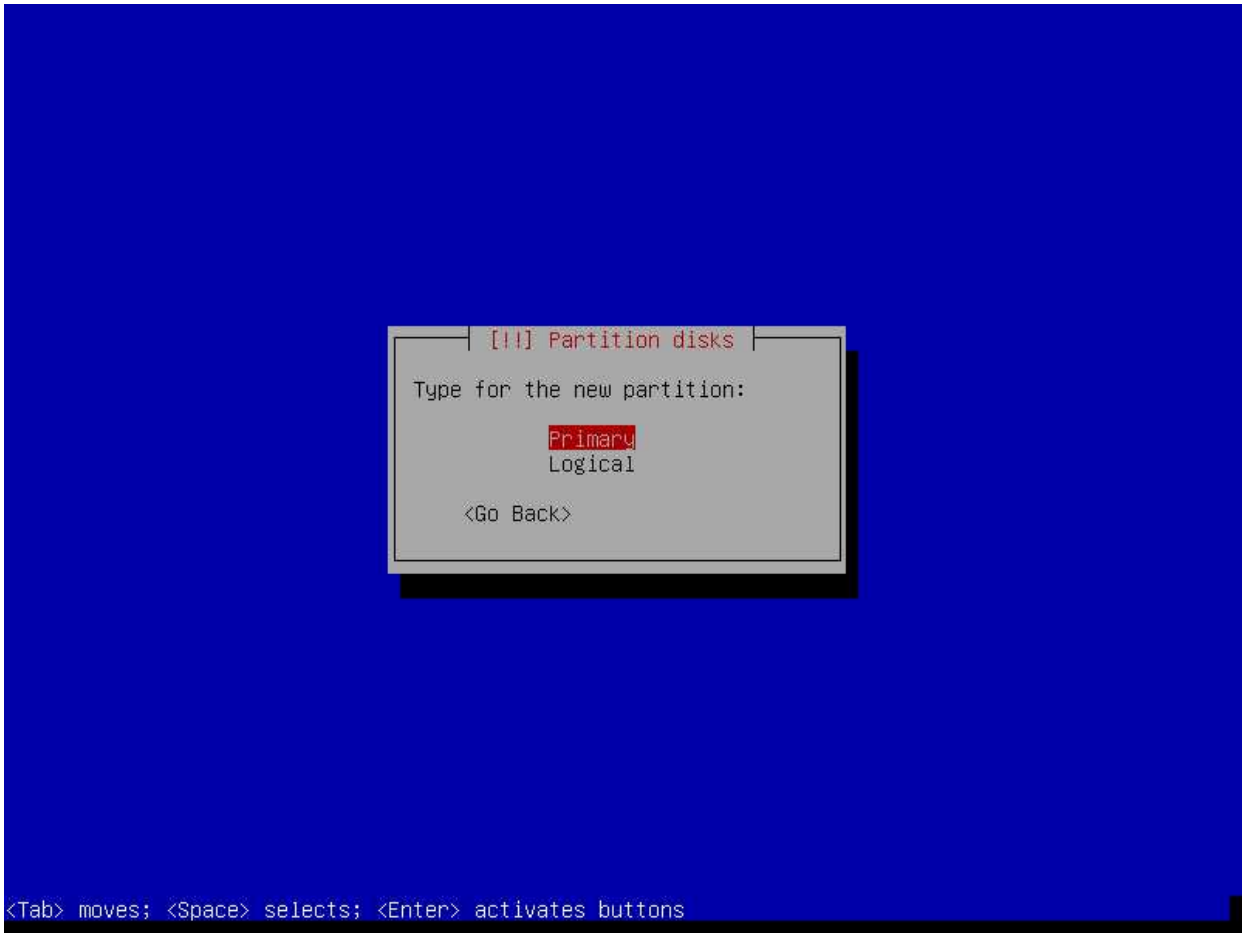
5. On the next screen, choose “Create a new partition” and press “enter.”



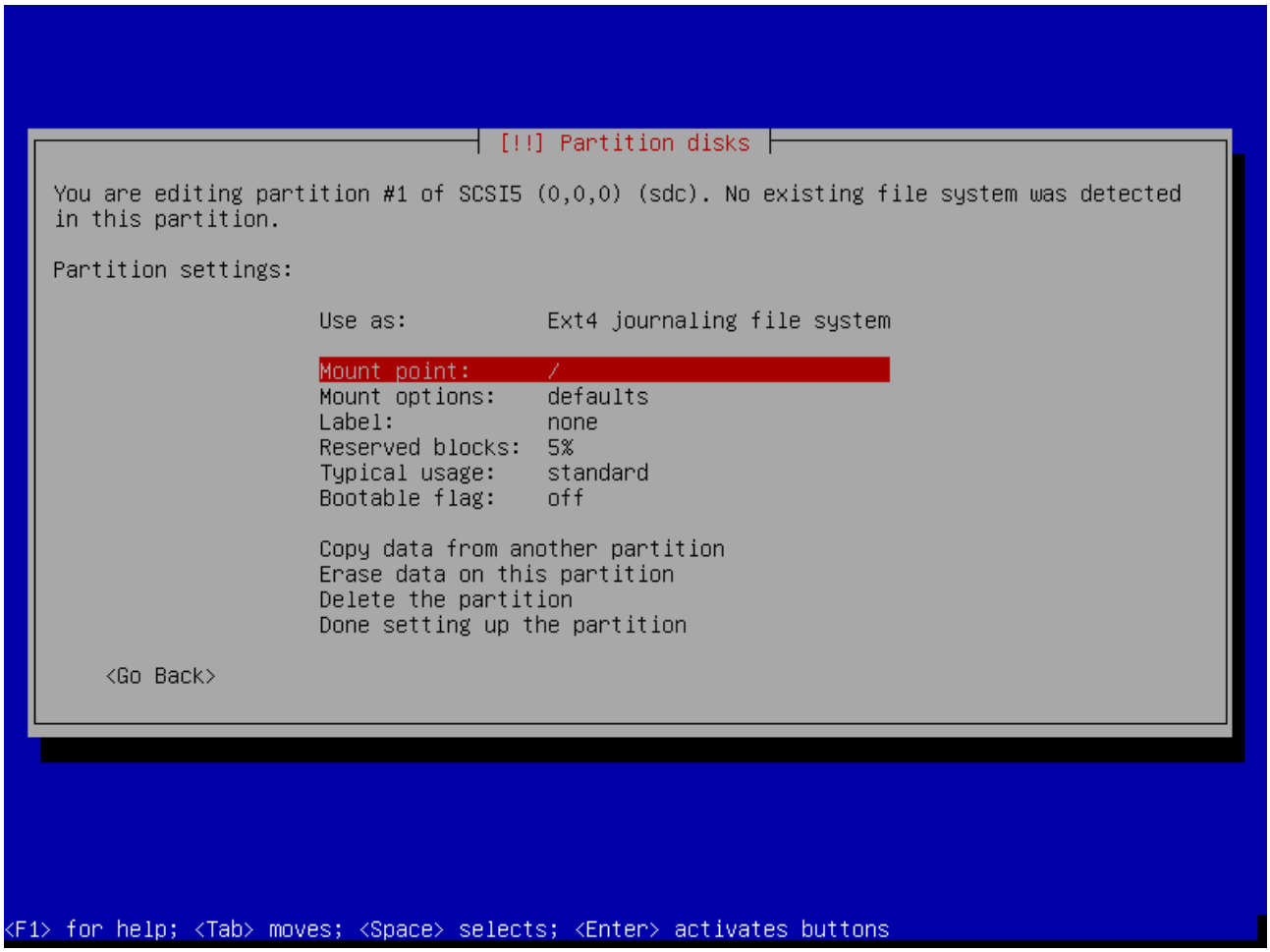
6. In the next screen, you will be asked to choose a new partition size. You can accept what is already selected by the installer. Simply press “enter” to continue.



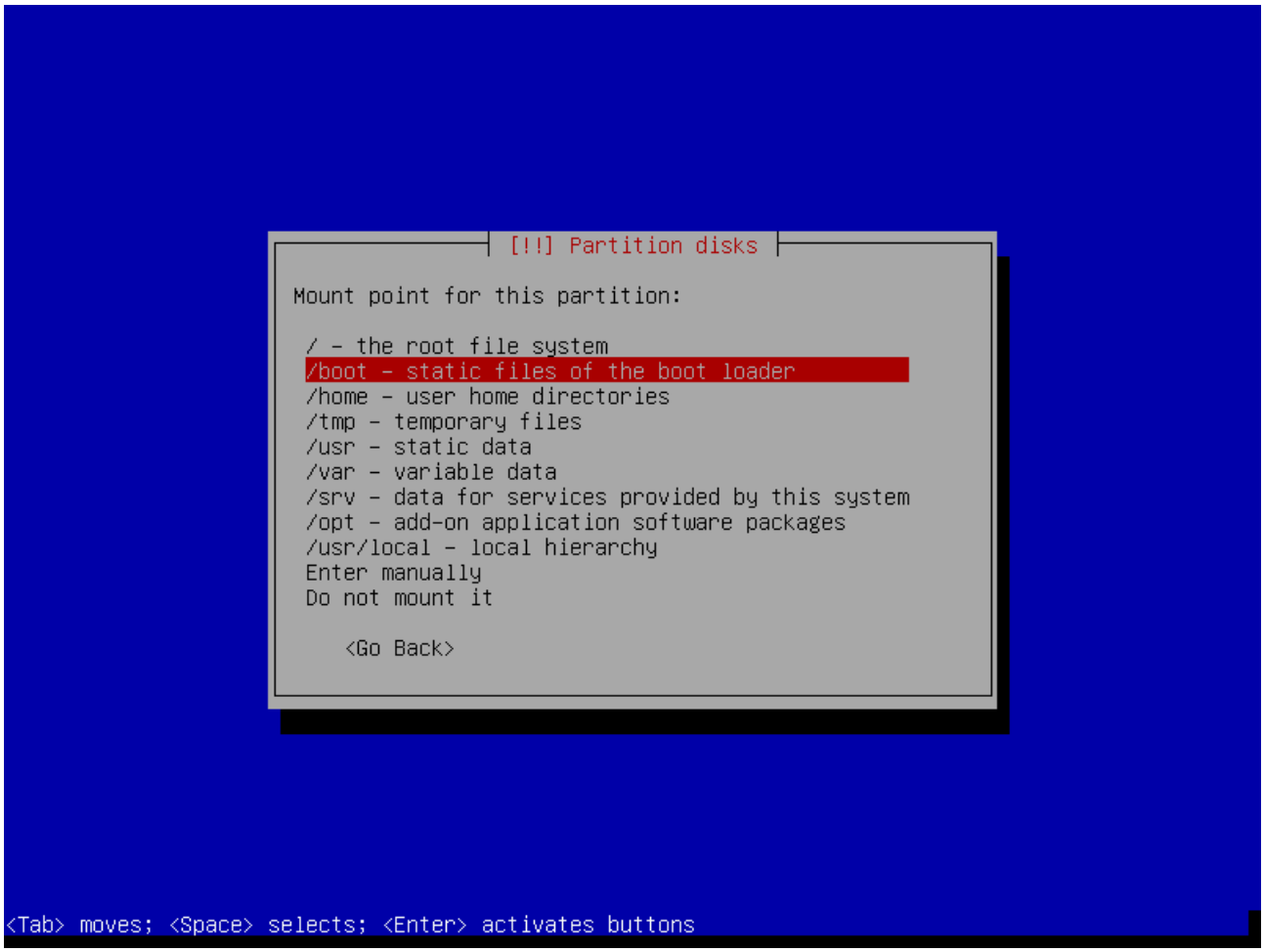
7. The next screen will ask you to choose the “type for the new partition.” Choose “Primary” and press “enter.”



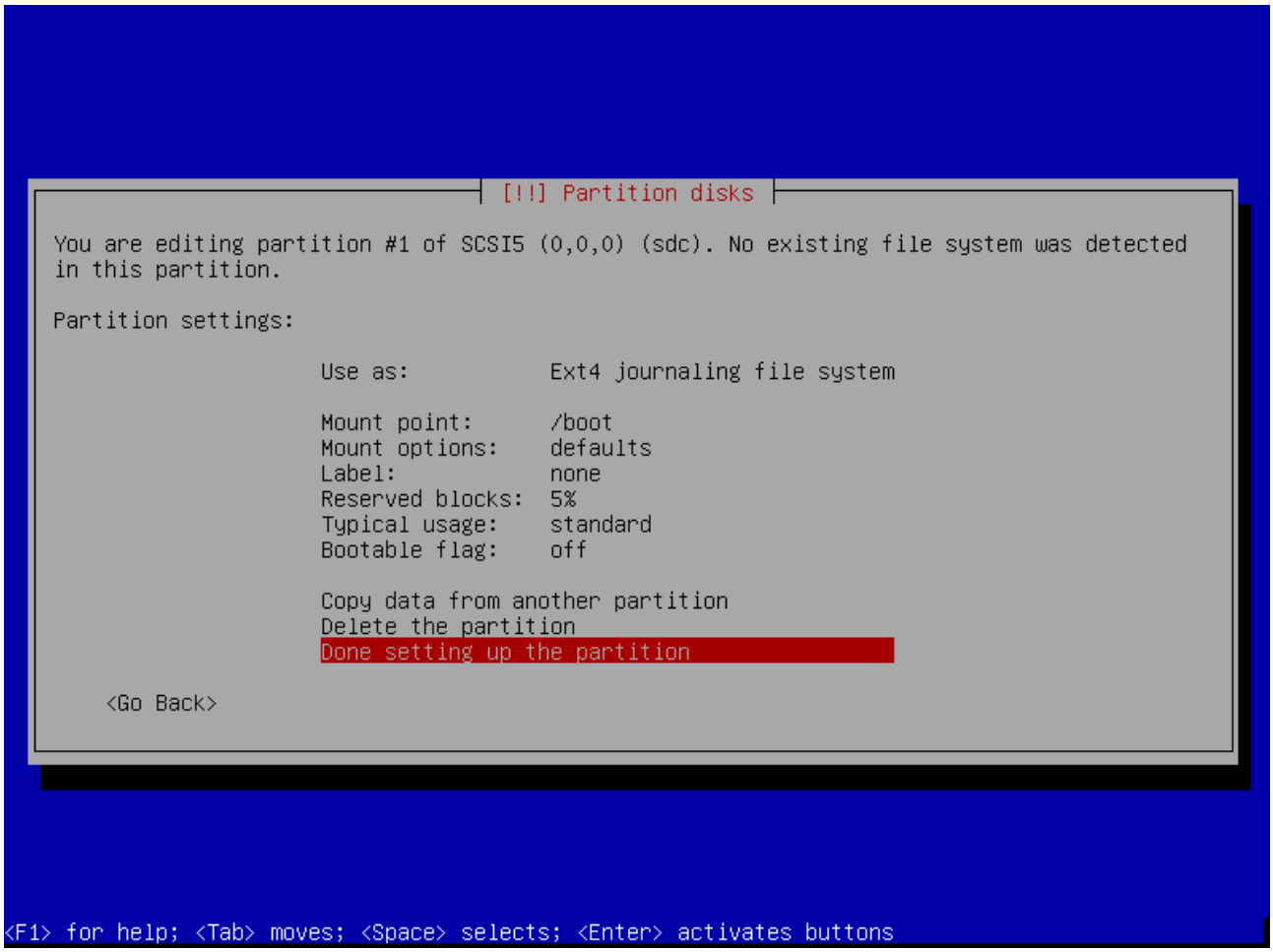
8. The next screen is for choosing your partition settings. There are many options here. However, in this step, you only need to concern yourself with one. You need to change the mount point to “/boot.” So, choose “Mount point” and press “enter.”



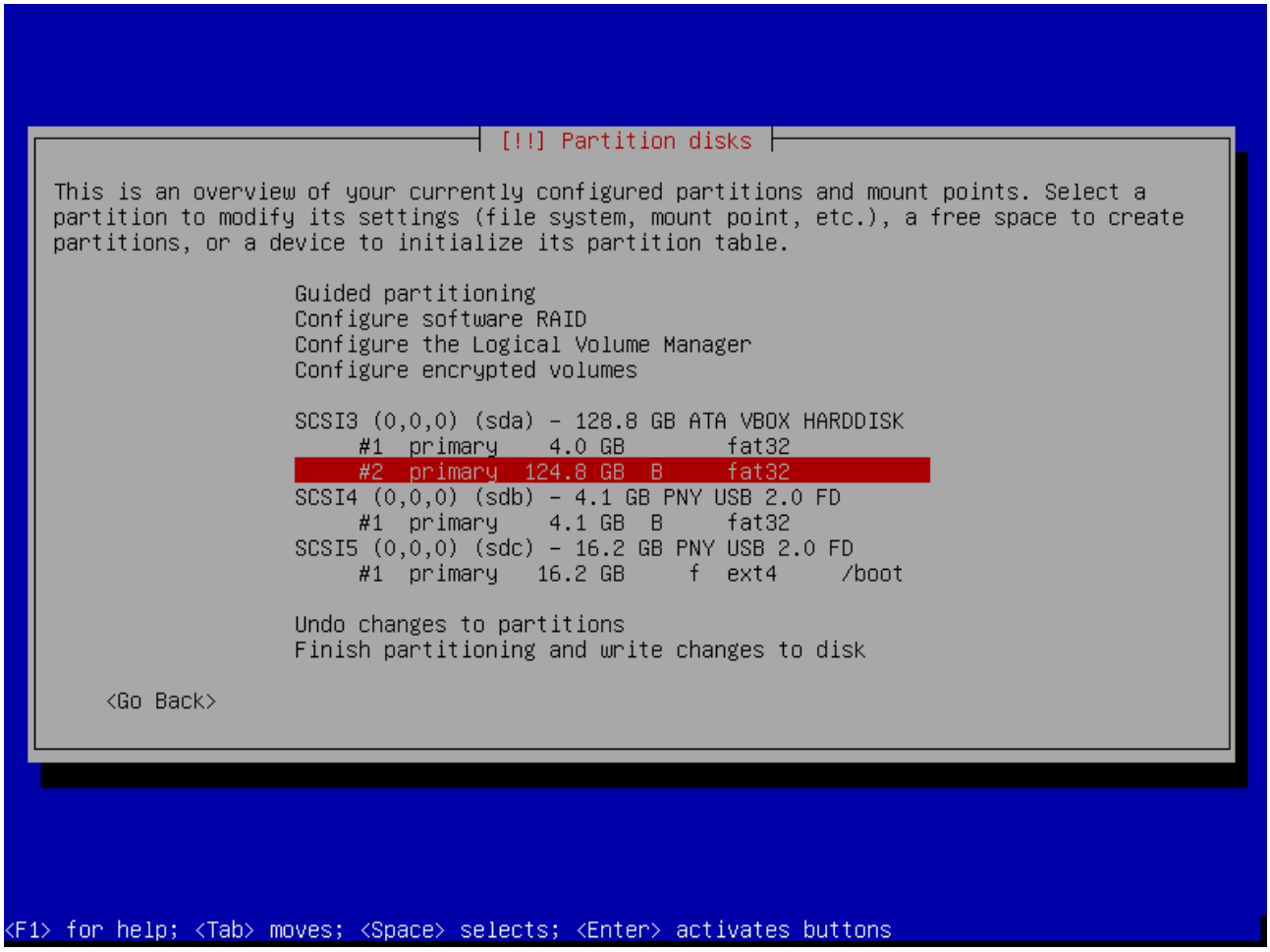
9. On the next screen, choose “/boot – static files of the boot loader” and press “enter.”



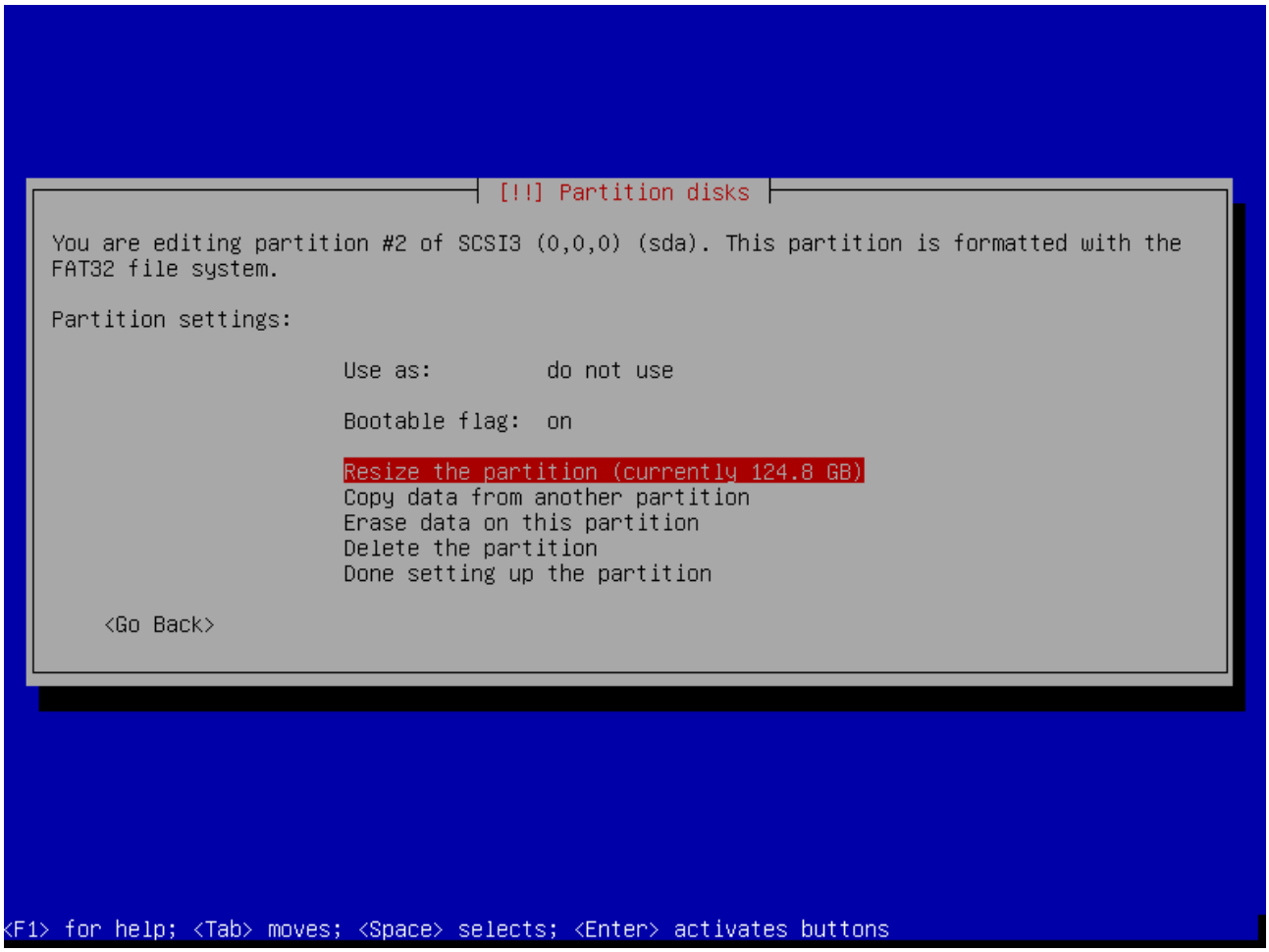
10. On the next screen, choose “Done setting up the partition” and press “enter.”



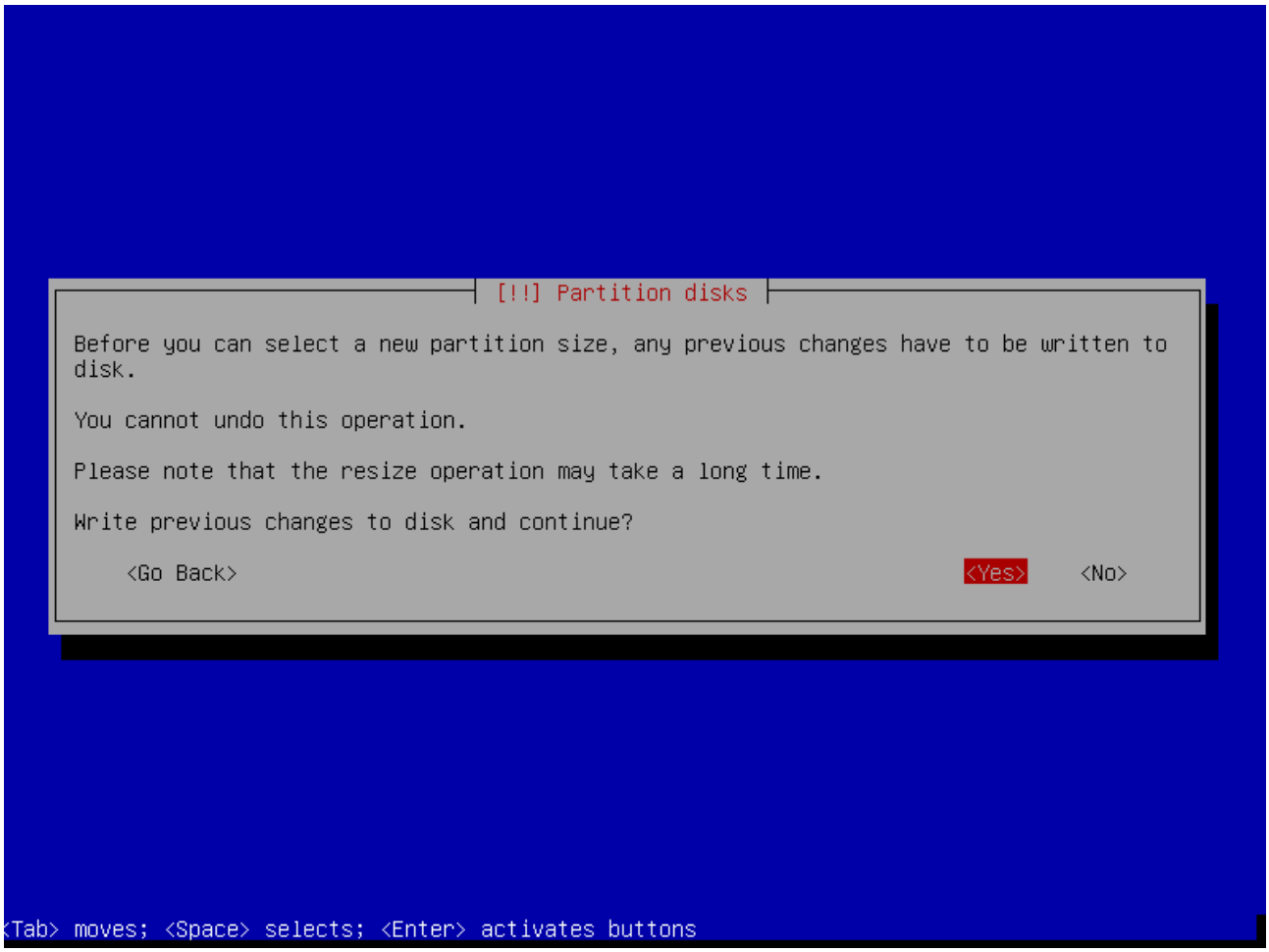
11. In the next step, you will begin the process of resizing the partition on your internal hard drive so you can create an encrypted partition for the Debian operating system. In this tutorial, the internal hard drive is “sda.” On your computer, the device name for your internal hard drive may be different. You may already have a number of partitions residing on “sda.” Choose the largest one and shrink it by the size you wish to allow for Debian. However, before doing this, **make sure there is enough free space on the drive to allow you to shrink it.** Select the drive to resize and press “enter.”



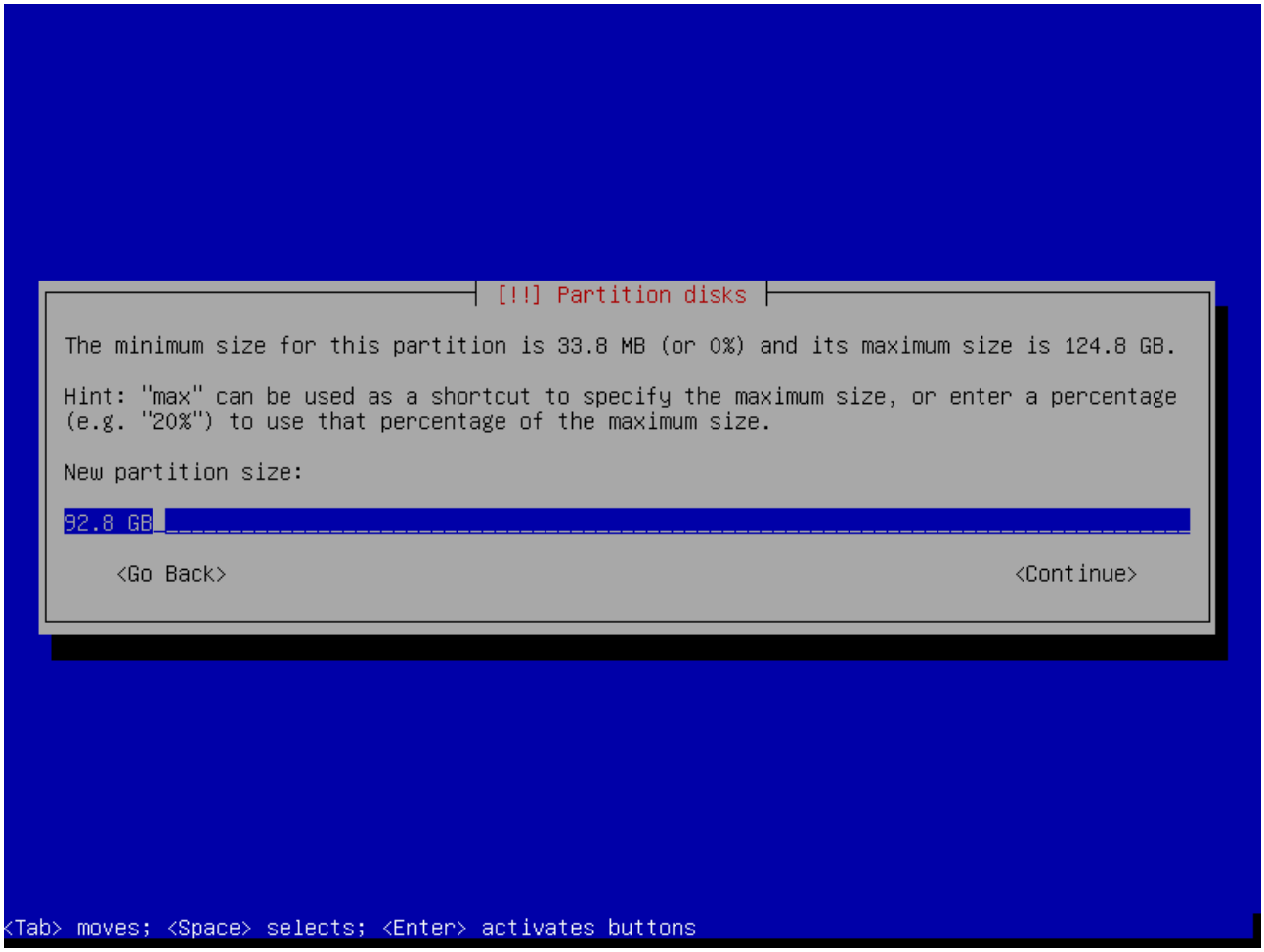
12. On the next screen, select the “resize the partition” option and press “enter.”



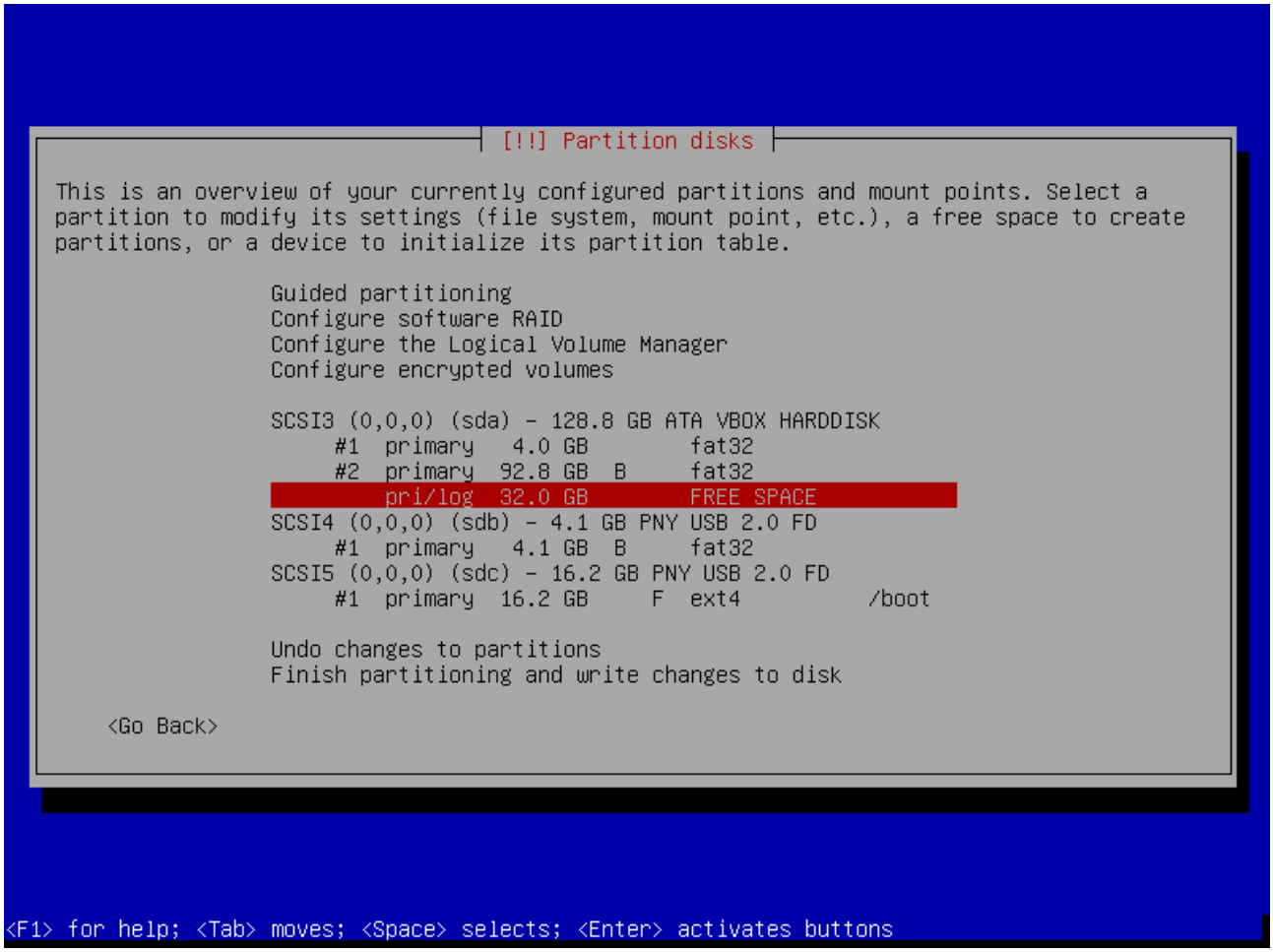
13. On the next screen, choose “yes” and press “enter.”



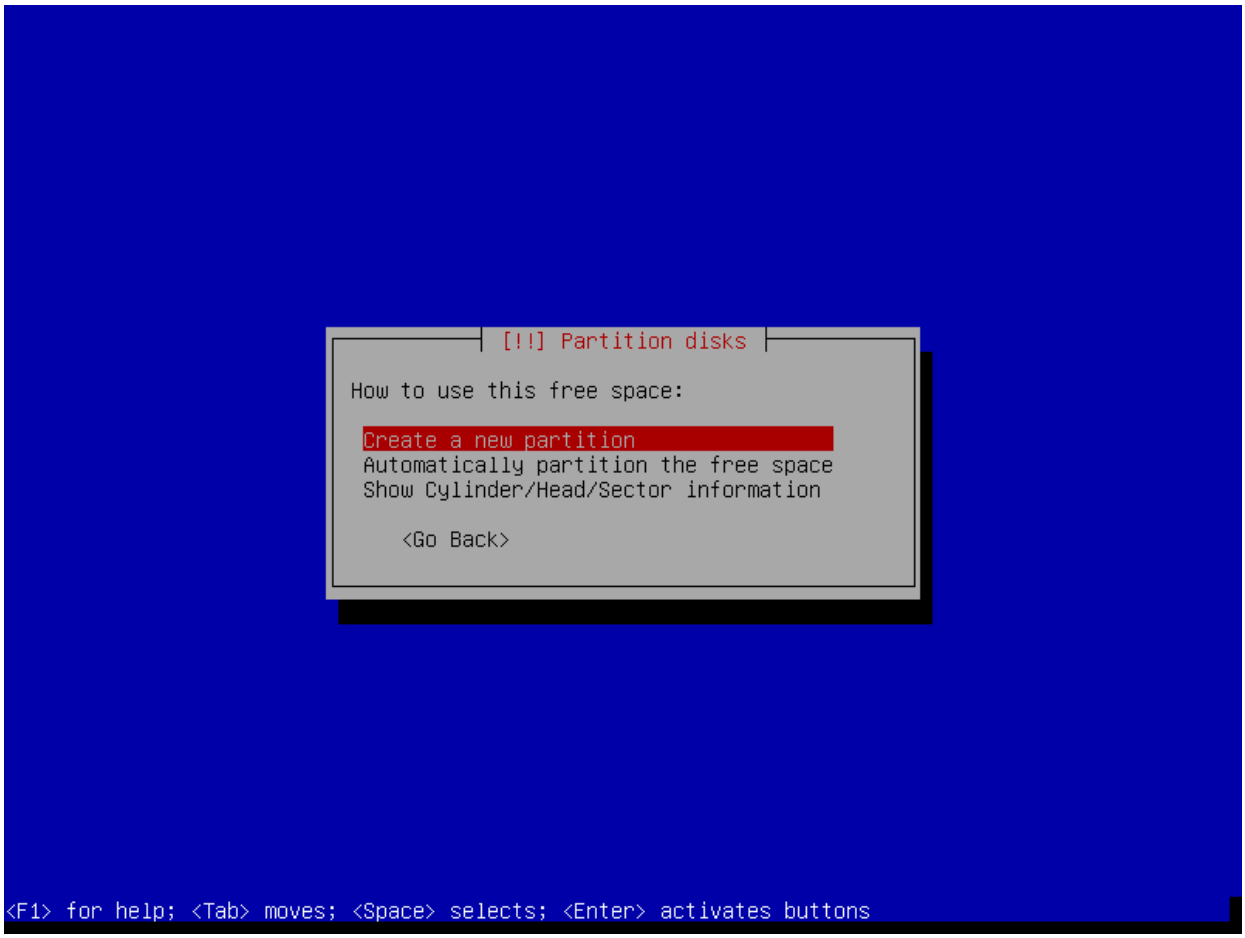
14. On the next screen, you will be prompted to enter a new partition size. 32 gigabytes will be sufficient for your purposes. However, if you wish to make it larger and have the space, feel free to do so. In the example below, 32 gigabytes is chosen for what will be our encrypted operating system disk. Since the maximum size of the disk in the example is 124.8 GB, subtracting 32 GB results in 92.8 GB. Use the same math to determine what you should type in the field for the new partition size and press “enter” when done. This process may take a bit of time.



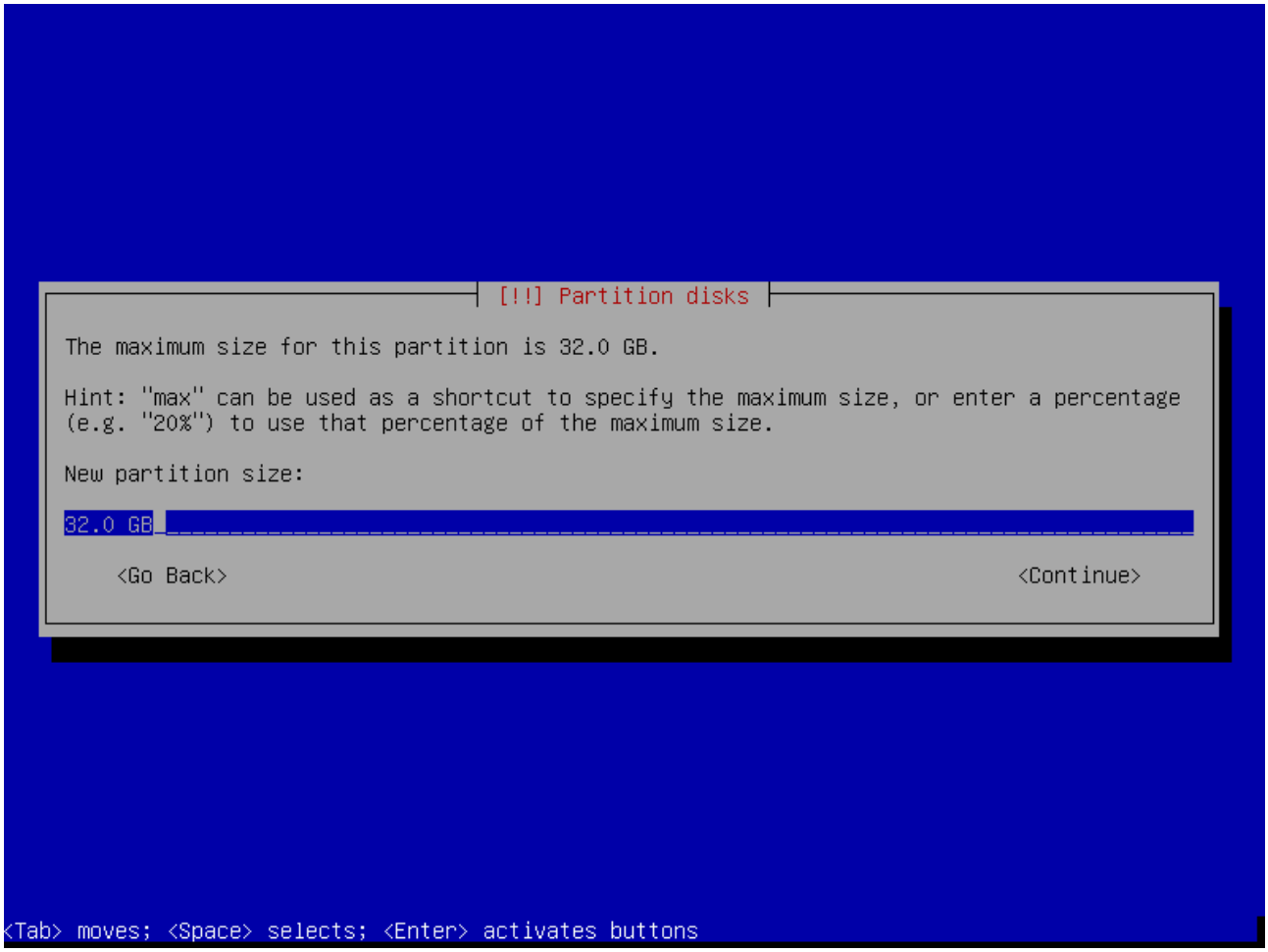
15. On the next screen, you will see a new entry marked “FREE SPACE” under (sda) with the size you chose for your encrypted disk. Select it and press “enter.”



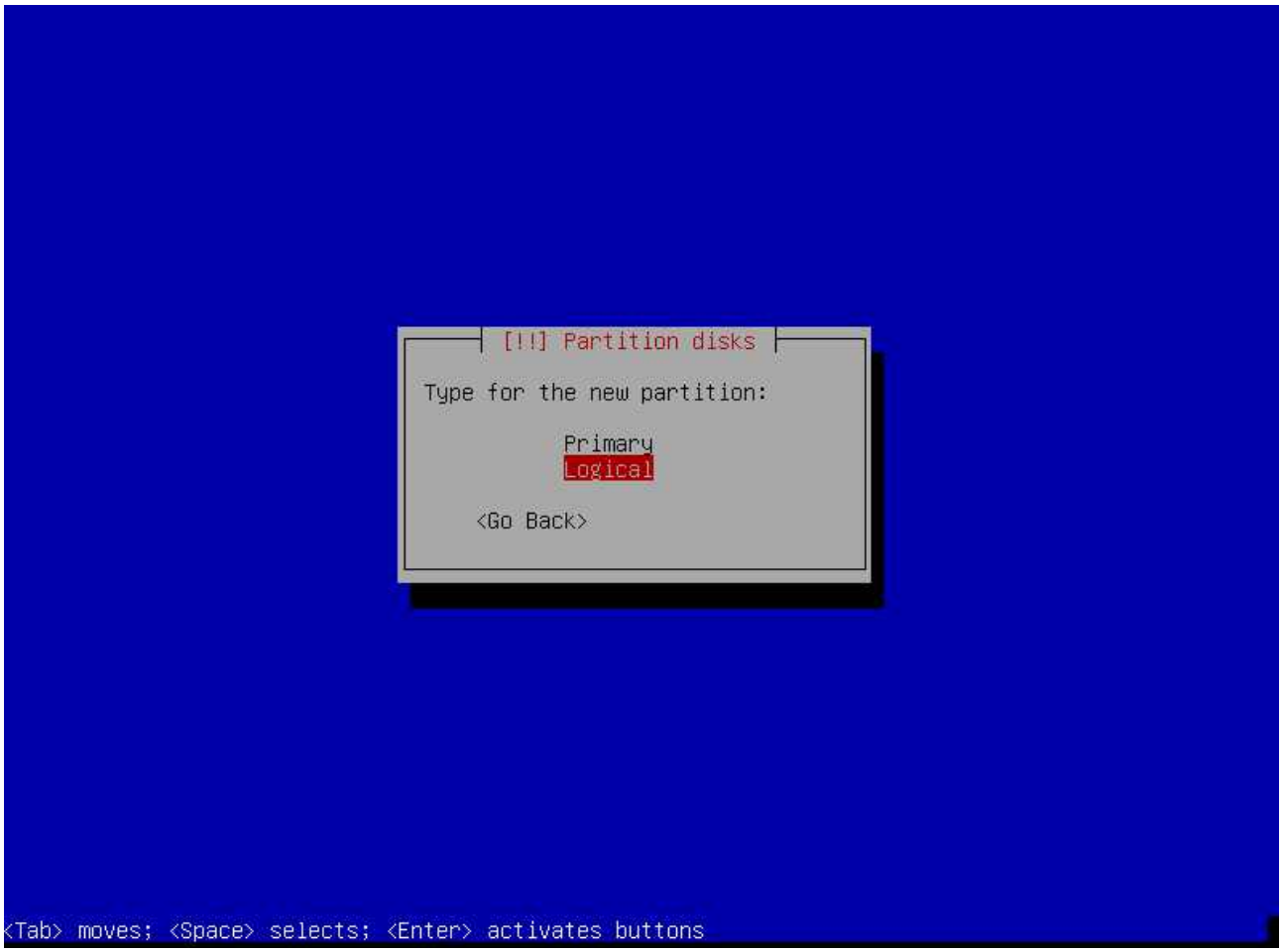
16. On the next screen, select “Create a new partition” and press “enter.”



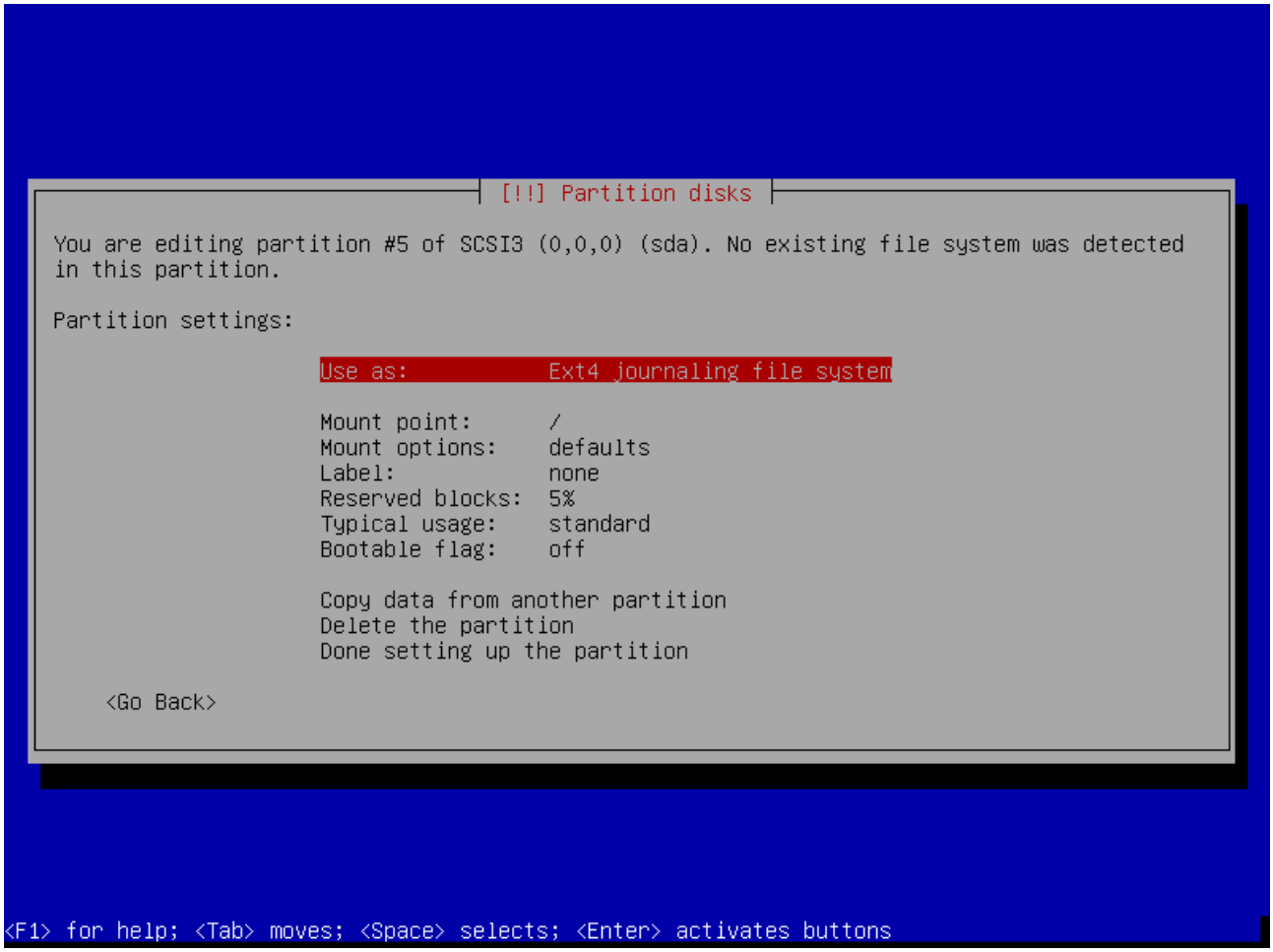
17. On the next screen, the maximum size for the disk will already be selected. Press “enter” to continue.



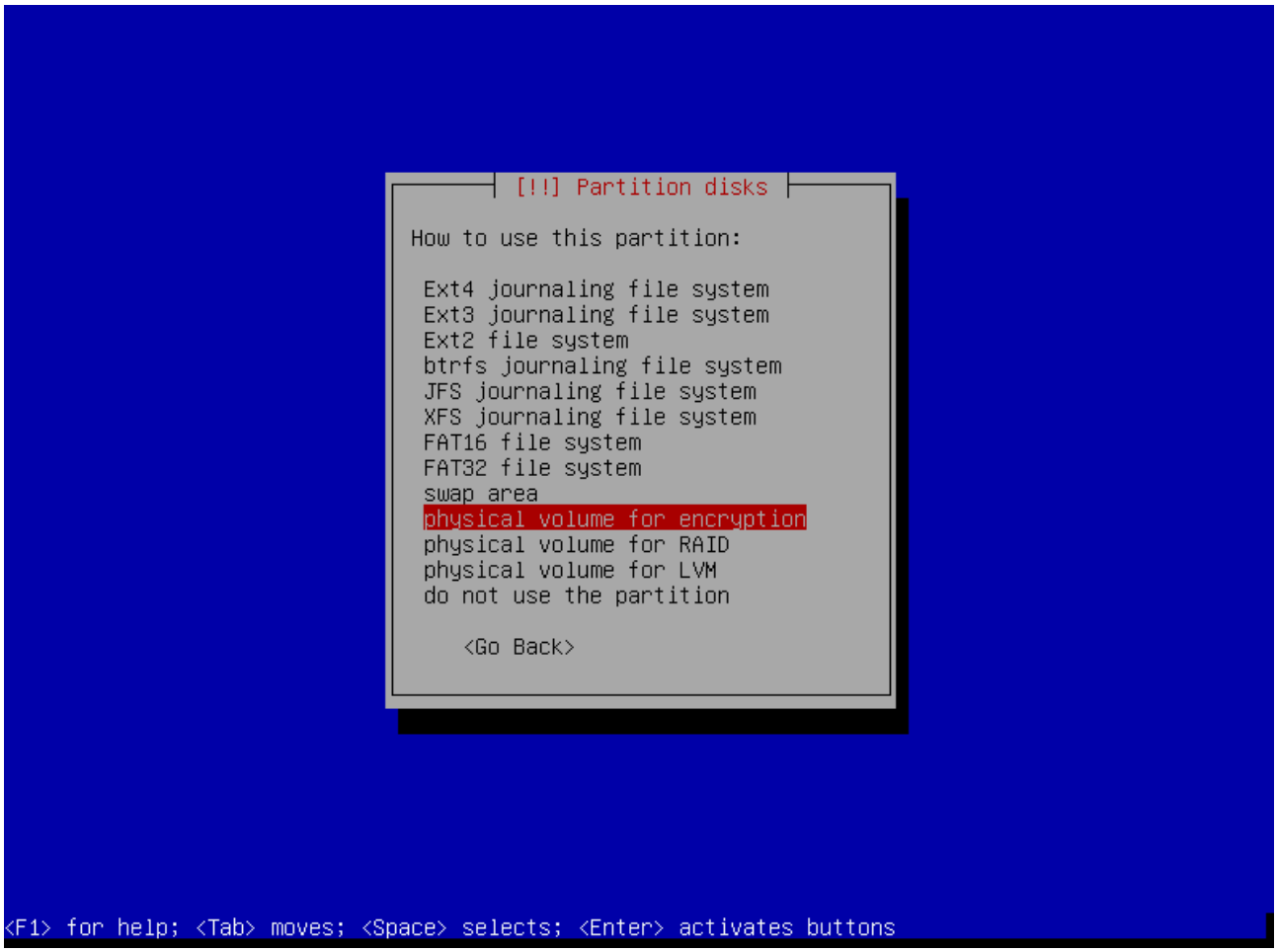
18. On the next screen, select “Logical” and press “enter.”



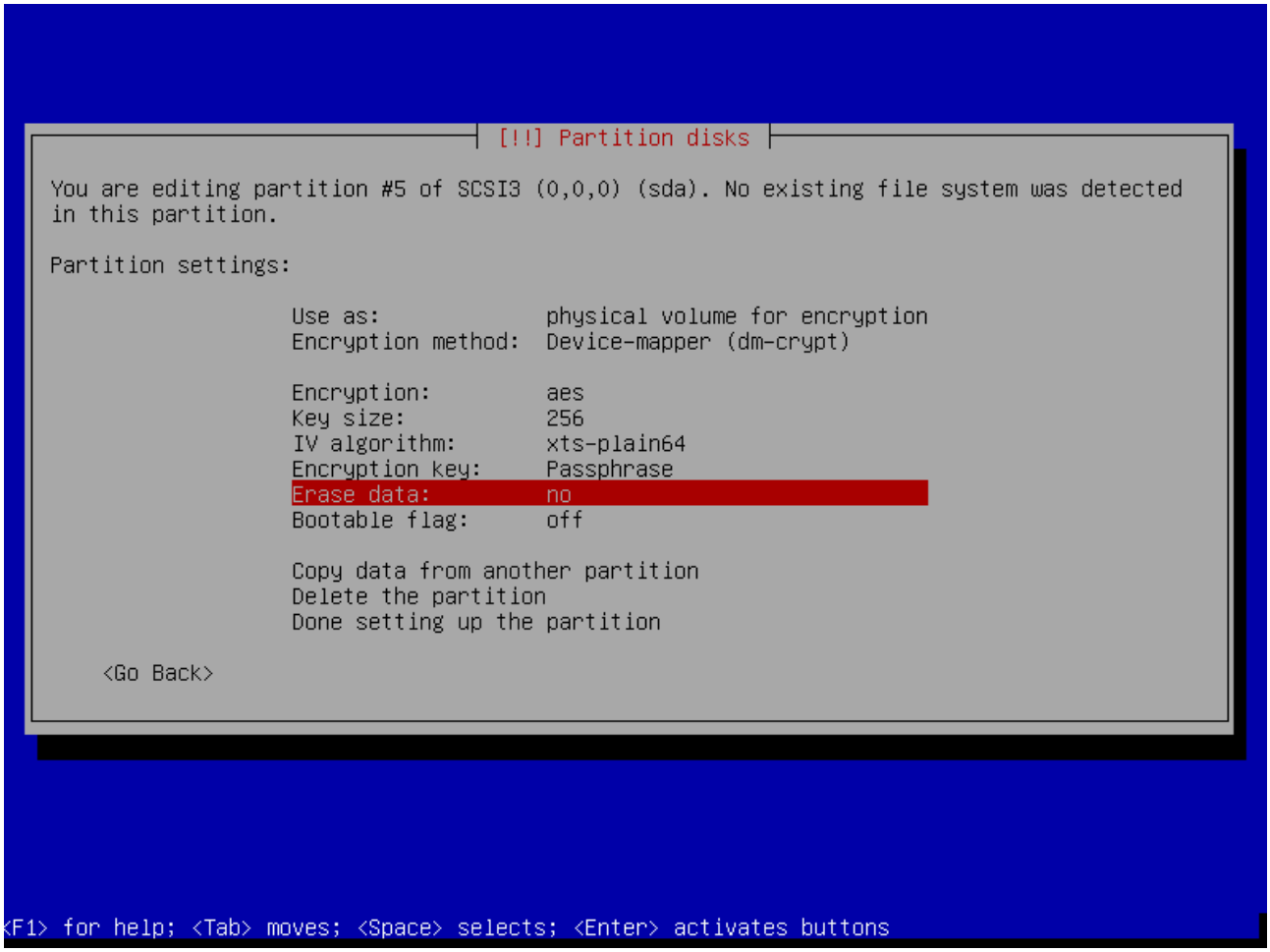
19. On the next screen, we need to set this partition to be used for encryption. Select the “Use as: Ext4 journaling file system” entry and press “enter.”



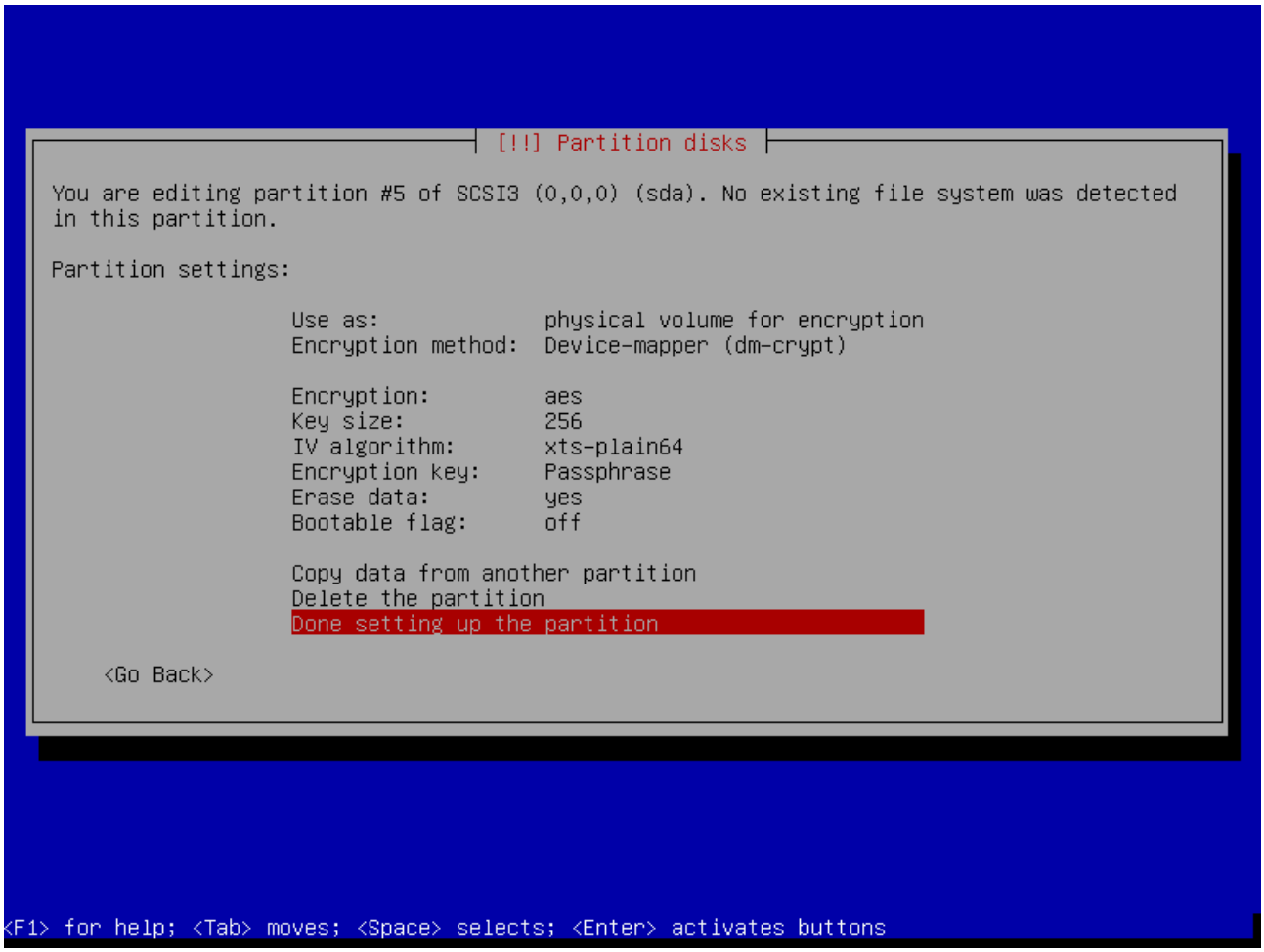
20. On the next screen, choose “physical volume for encryption” and press “enter.”



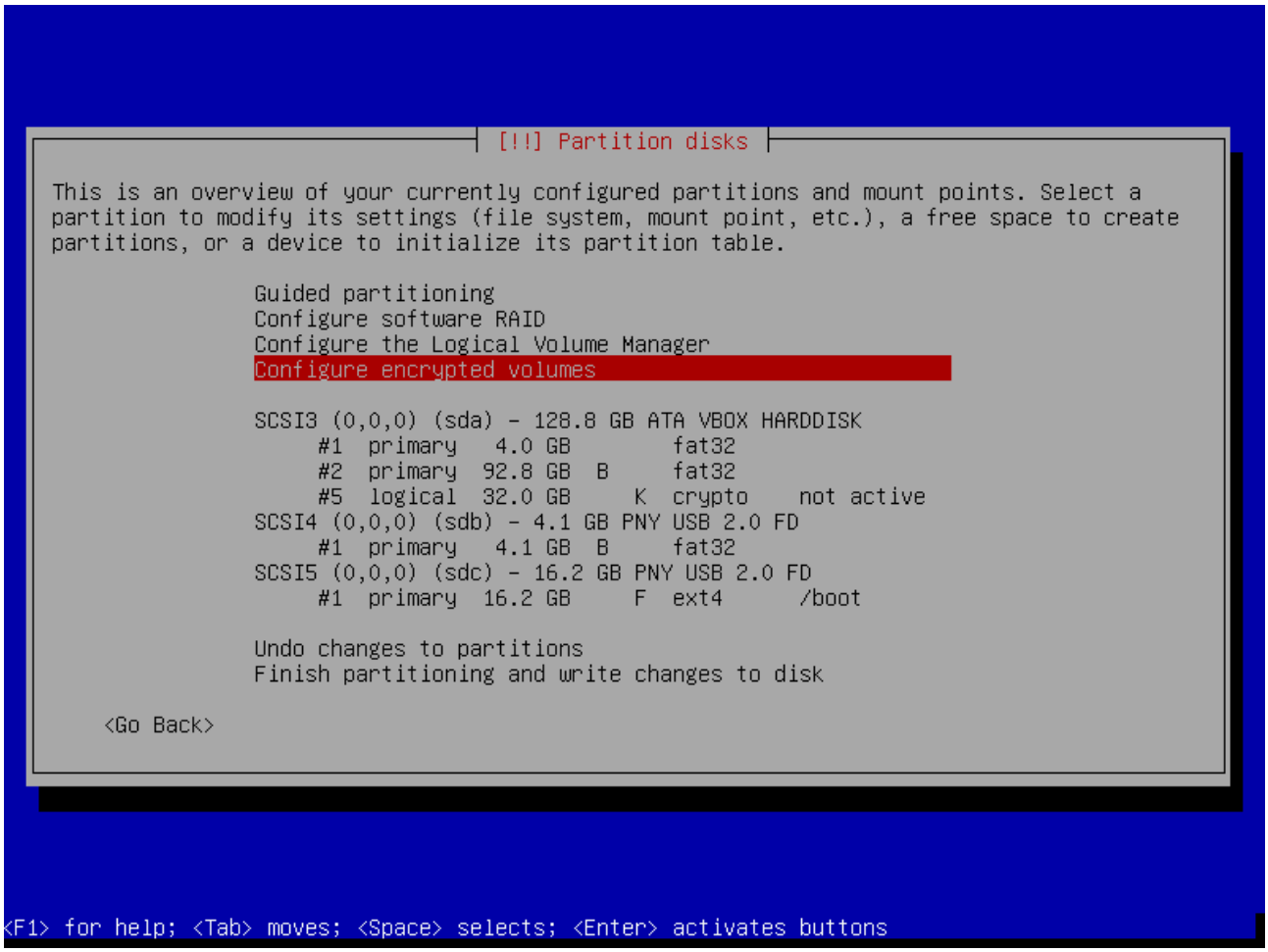
21. This step is optional. In the next screen, there is an option to “erase data” which is set to “yes” by default. If you choose to erase data, the installer will overwrite the full partition with pseudo-random data. If you want the tightest security, this is a wise step since it will be even more difficult for someone who has possession of your hard drive to successfully use forensics to decode it. However, this process can take a very long time. To skip erasing data, select “Erase data:” and press “enter.” The option will change to “no.” If you wish to erase data, skip this step and proceed to step 22.



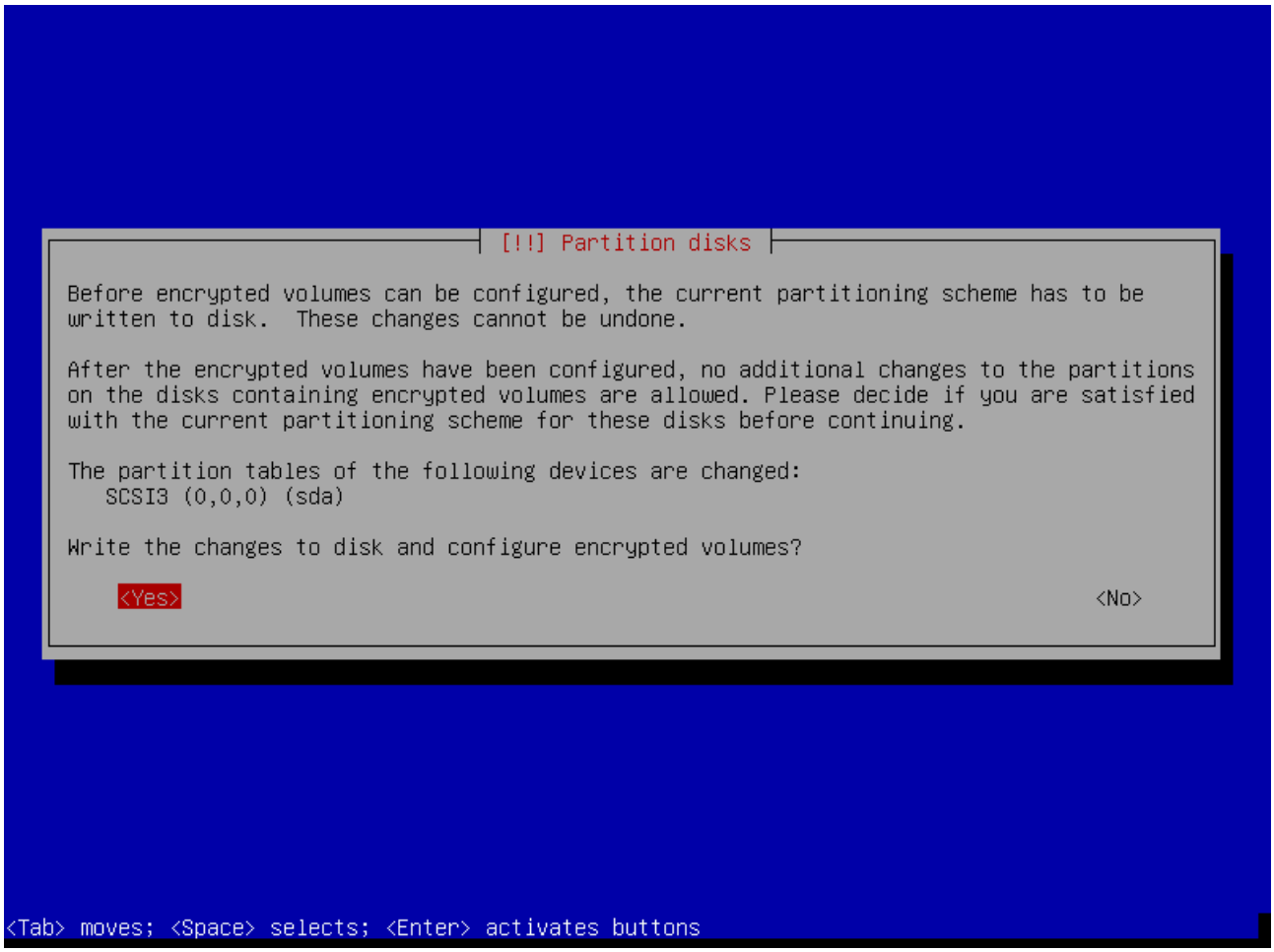
22. In this step, select “done setting up the partition” and press “enter.”



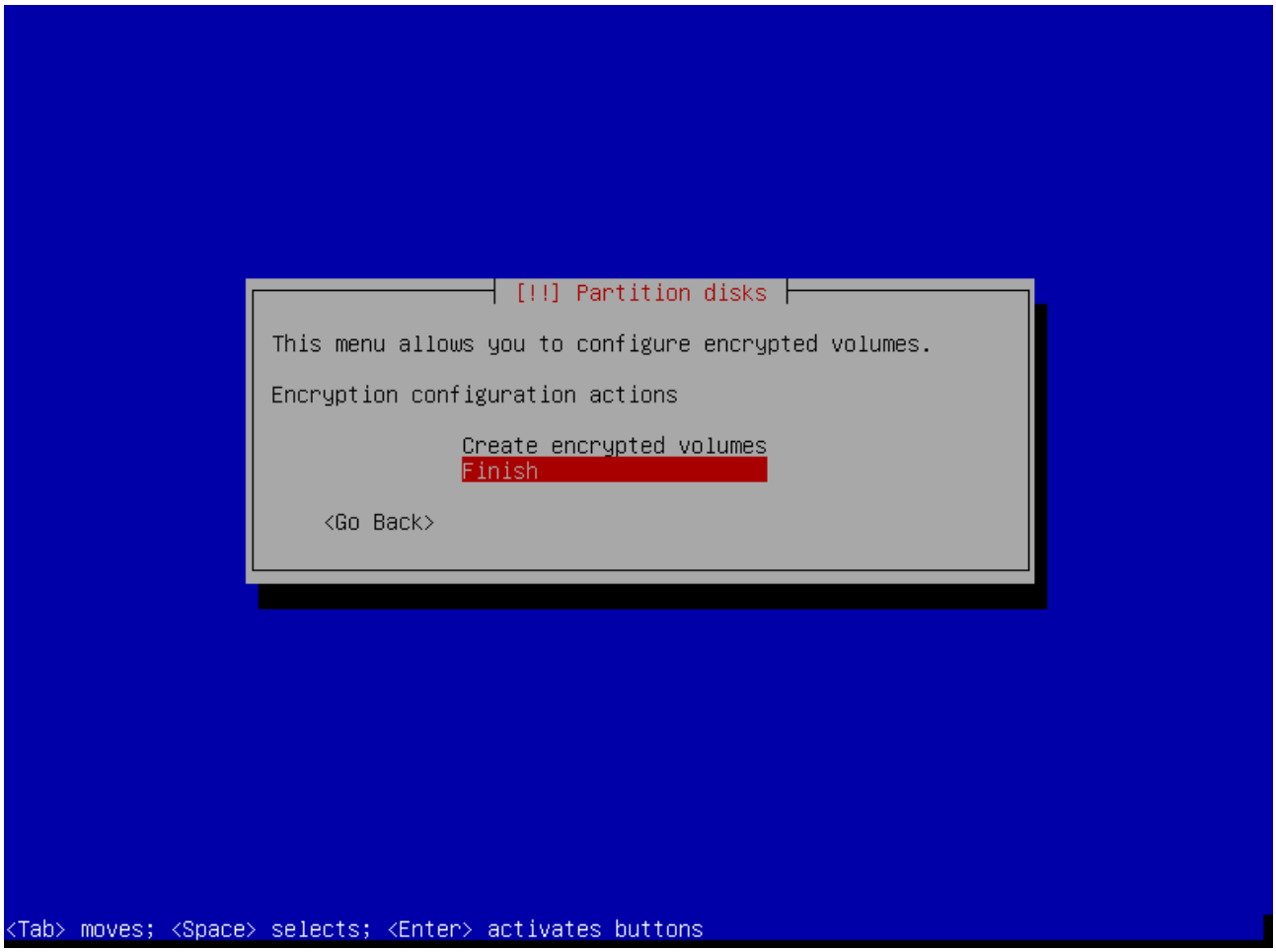
23. On the next screen, select “configure encrypted volumes” and press “enter.”



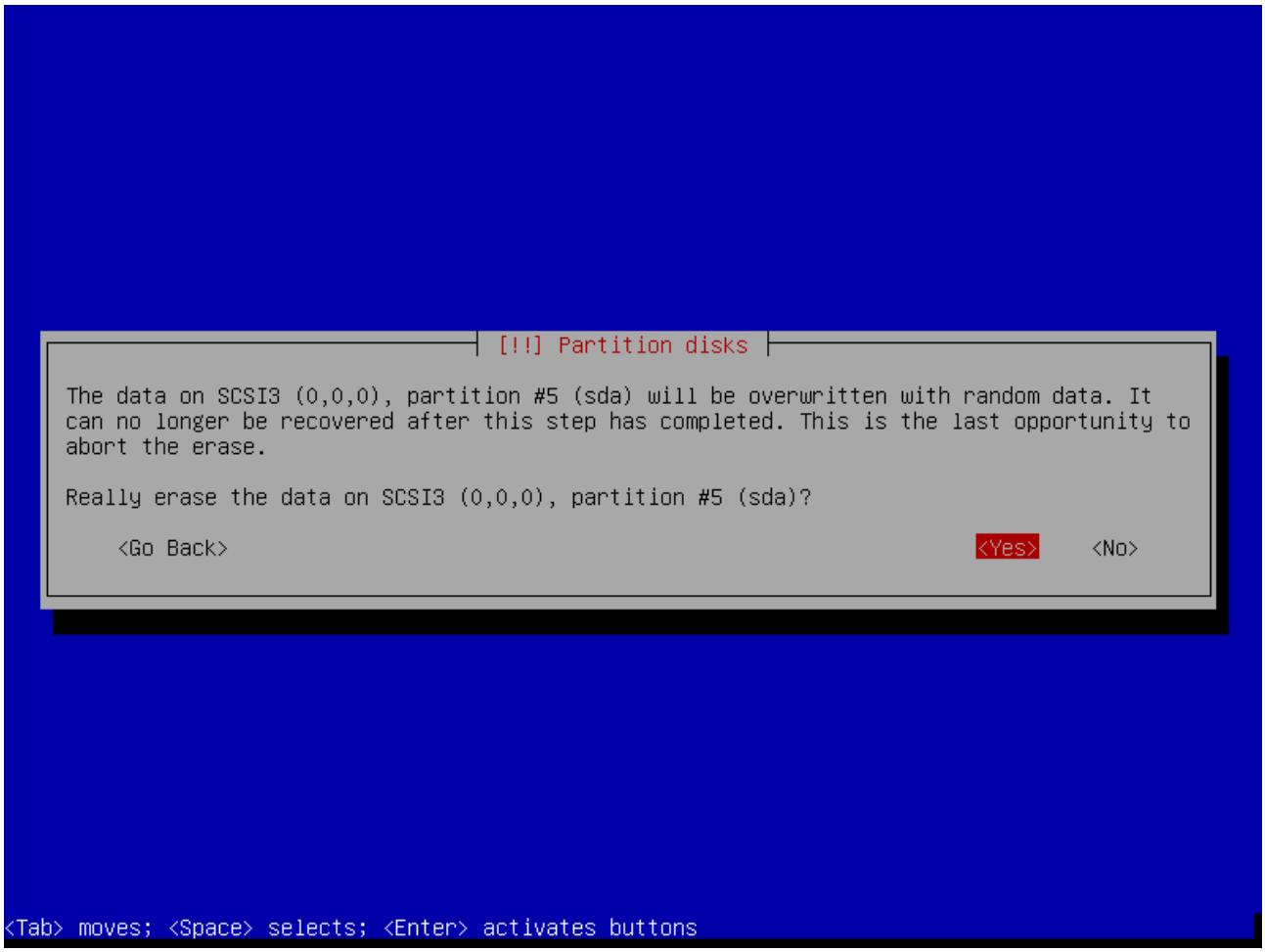
24. On the next screen, choose “yes” and press “enter.”



25. On the next screen, select “finish” and press “enter.”



26. If you opted to “erase data” when you set up the encrypted partition in step 21, you will be asked again if you want to erase the data. Choose “yes” if you do and press “enter.” This process can take hours. If you opted to not erase data, this screen will not appear and you can continue to step 27.



27. On the next screen, you will be prompted for your encryption passphrase. **It is imperative that you choose a very strong passphrase! Otherwise, encrypting your hard drive will simply amount to a waste of time!** As was discussed earlier in step 19 of chapter 1, an 8 character password is never a good passphrase. Since the Debian Installer is making use of the cryptsetup program and the LUKS encryption system, the following breakdown of the importance of a strong passphrase comes from the developer.

    "First, passphrase length is not really the right measure, passphrase entropy is. For example, a random lowercase letter (a-z) gives you 4.7 bit of entropy, one element of a-z0-9 gives you 5.2 bits of entropy, an element of a-zA-Z0-9 gives you 5.9 bits and a-zA-Z0-9!@#$%^&:-+ gives you 6.2 bits. On the other hand, a random English word only gives you 0.6...1.3 bits of entropy per character. Using sentences that make sense gives lower entropy, series of random words gives higher entropy. Do not use sentences that can be tied to you or found on your computer. This type of attack is done routinely today. To get reasonable security for the next 10 years, it is a good idea to overestimate by a factor of at least 1000.

    Then there is the question of how much the attacker is willing to spend. That is up to your own security evaluation. For general use, I will assume the attacker is willing to spend up to 1 million EUR/USD. Then we get the following recommendations:

    LUKS: Use > 65 bit. That is e.g. 14 random chars from a-z or a random English sentence of > 108 characters length.

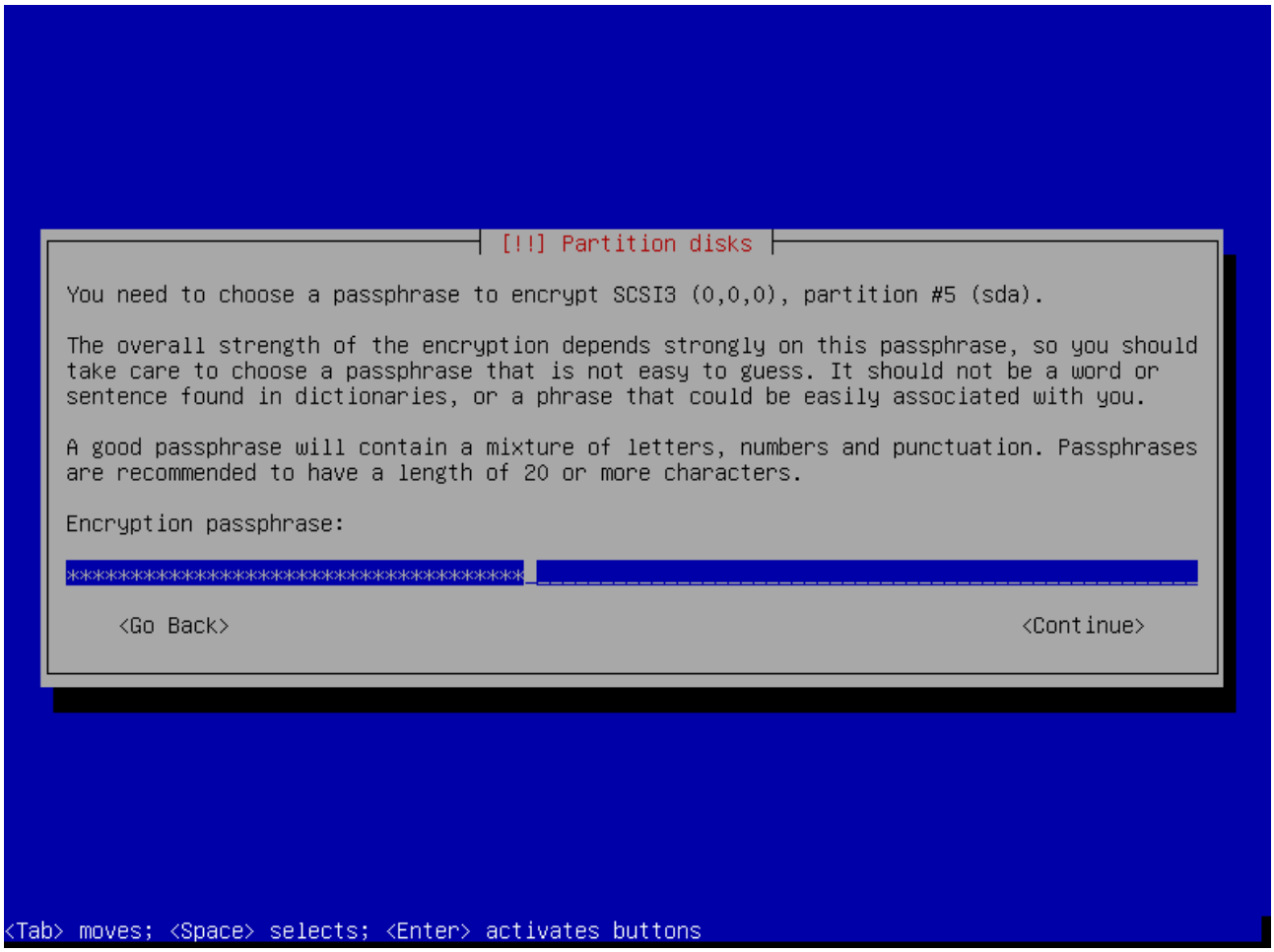
    If paranoid, add at least 20 bit. That is roughly four additional characters for random passphrases and roughly 32 characters for a random English sentence."

    https://code.google.com/p/cryptsetup/wiki/FrequentlyAskedQuestions#5._Security_Aspects

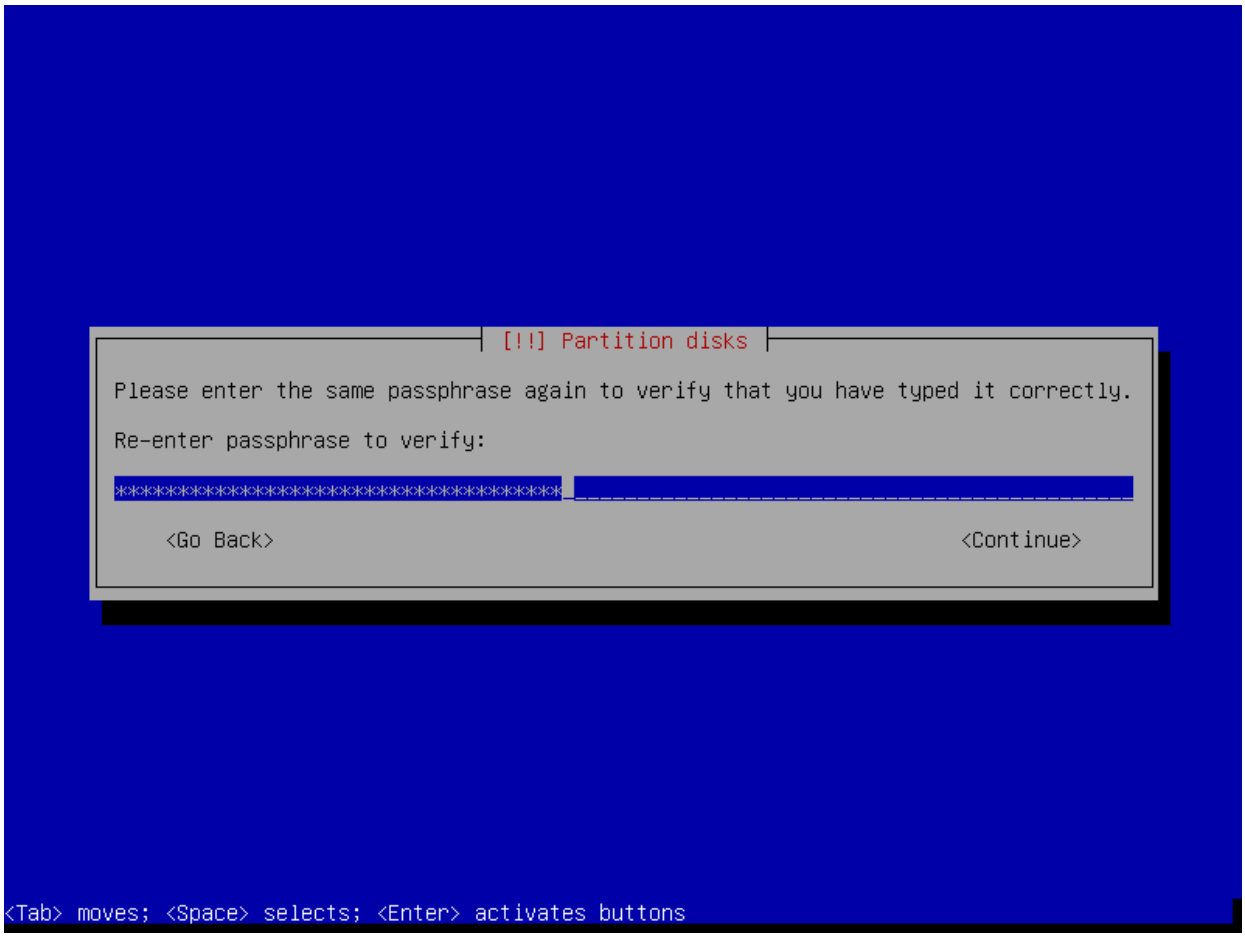
    Not in the mood to do math? The lesson to take away is that length, randomness and nonsense matter. They will get you more entropy. There are many tricks people use to come up with a nonsensical passphrase that they remember. For example, you could use a play on a favorite line from a movie you enjoy combined with a date you would remember like "If My Calculations Are Proper, When This Baby Hits 88 Miles Per Hour, You're Going 2 See Some Serious Business! January-1-2013?". This is a very secure type of passphrase that has plenty of entropy per the suggested numbers by the developer of cryptsetup.

    For further discussion of strong passphrases, go to https://www.grc.com/haystack.htm.

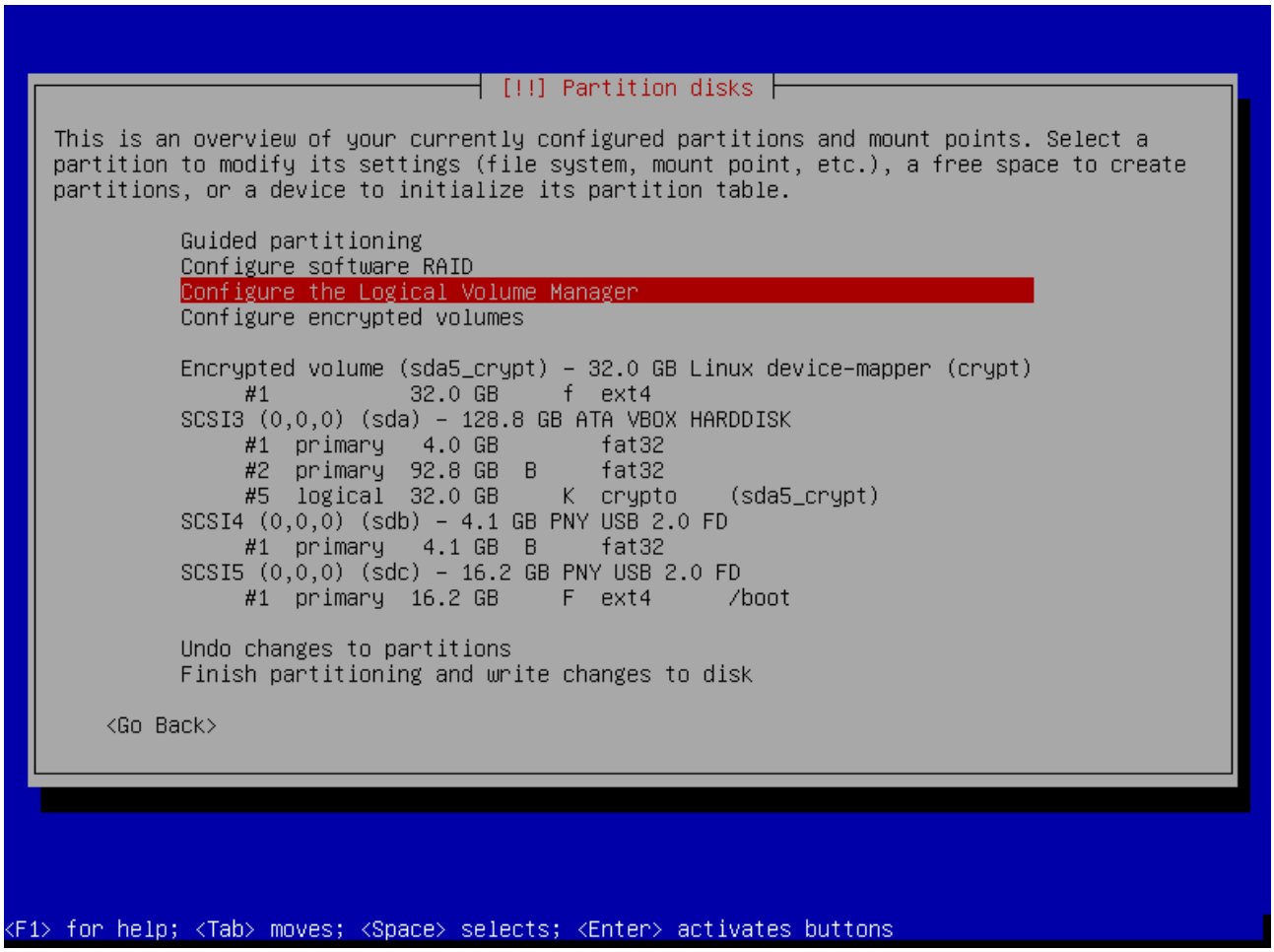
Once you have decided upon a strong passphrase, type it into the “encryption passphrase” field and press “enter.” **Remember, if you forget this passphrase, you have lost everything on your disk! Make sure you remember it! It cannot be recovered!**



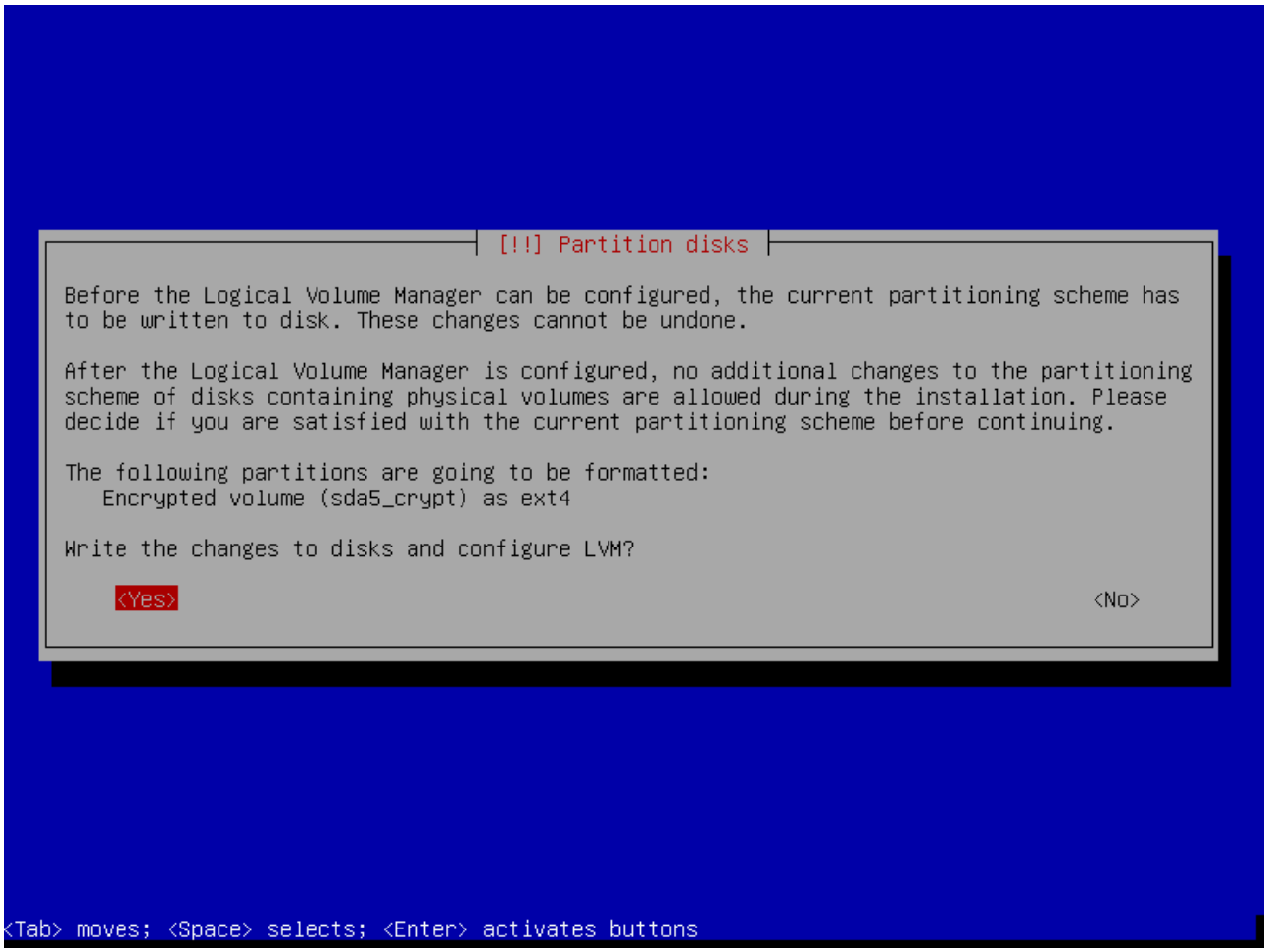
28. On the next screen, type your passphrase again to confirm it and press “enter.”



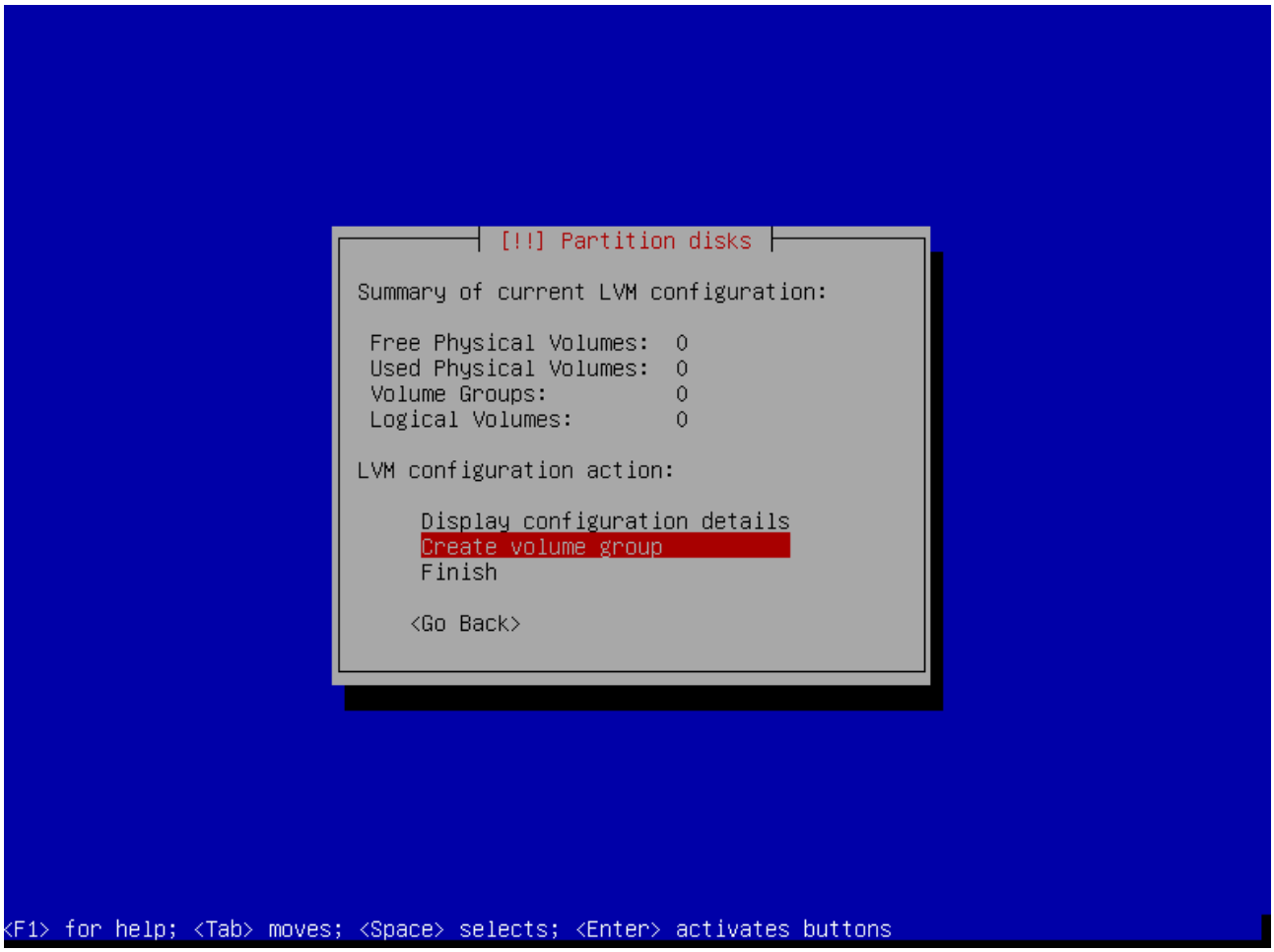
29. On the next screen, choose “Configure the Logical Volume Manager” and press “enter.”



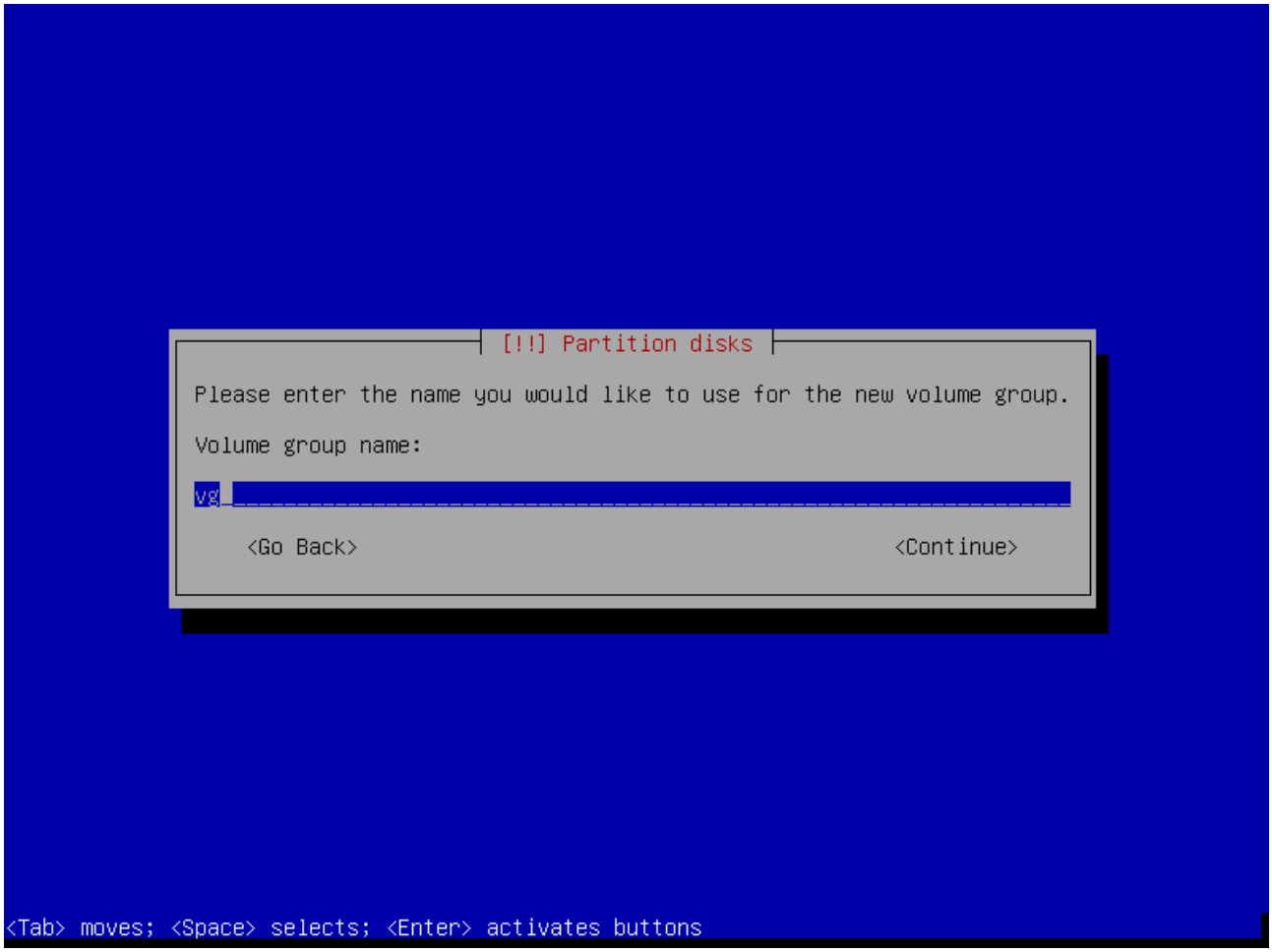
30. On the next screen, choose “yes” and press “enter.”



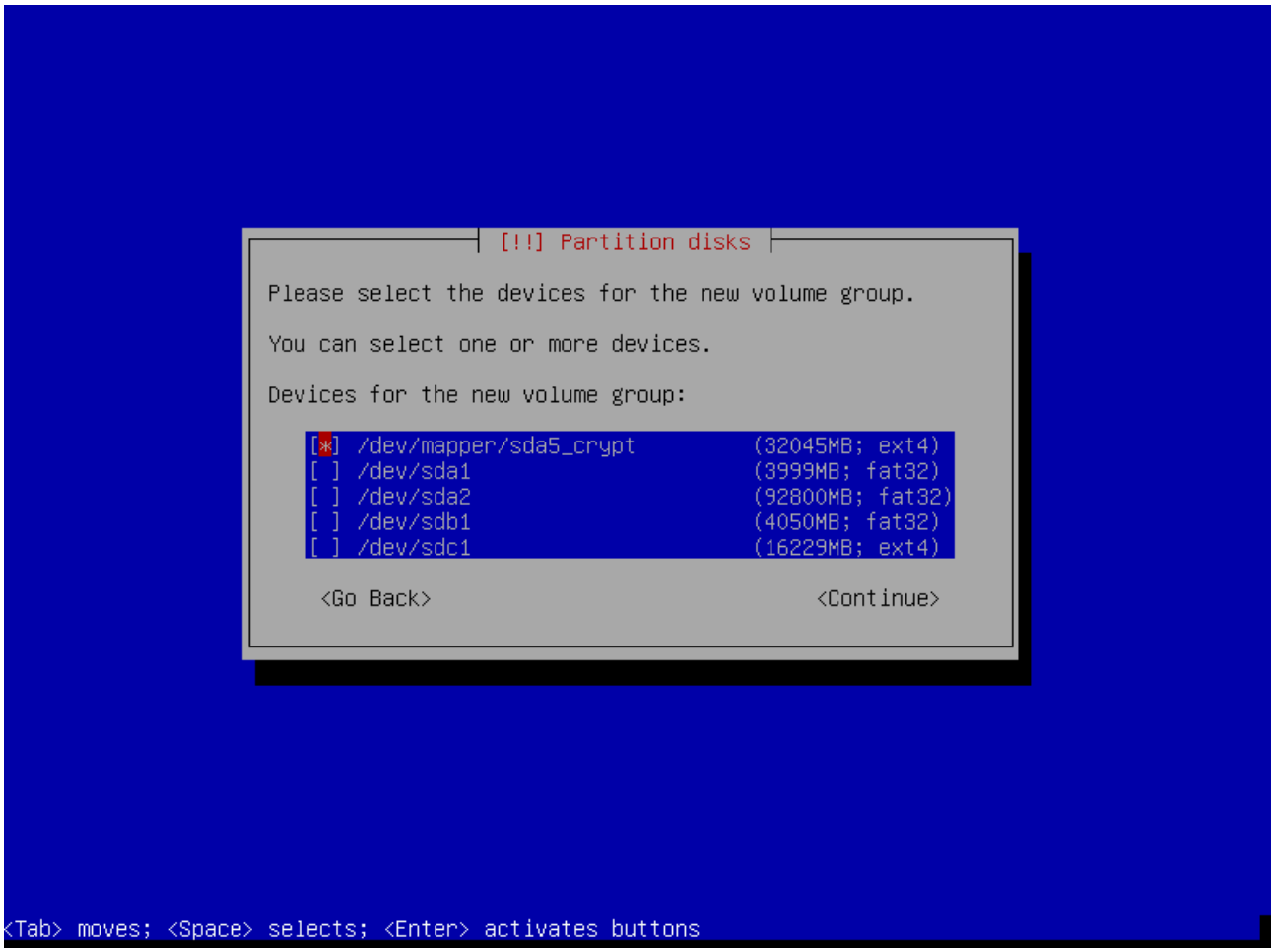
31. On the next screen, choose “create volume group” and press “enter.”



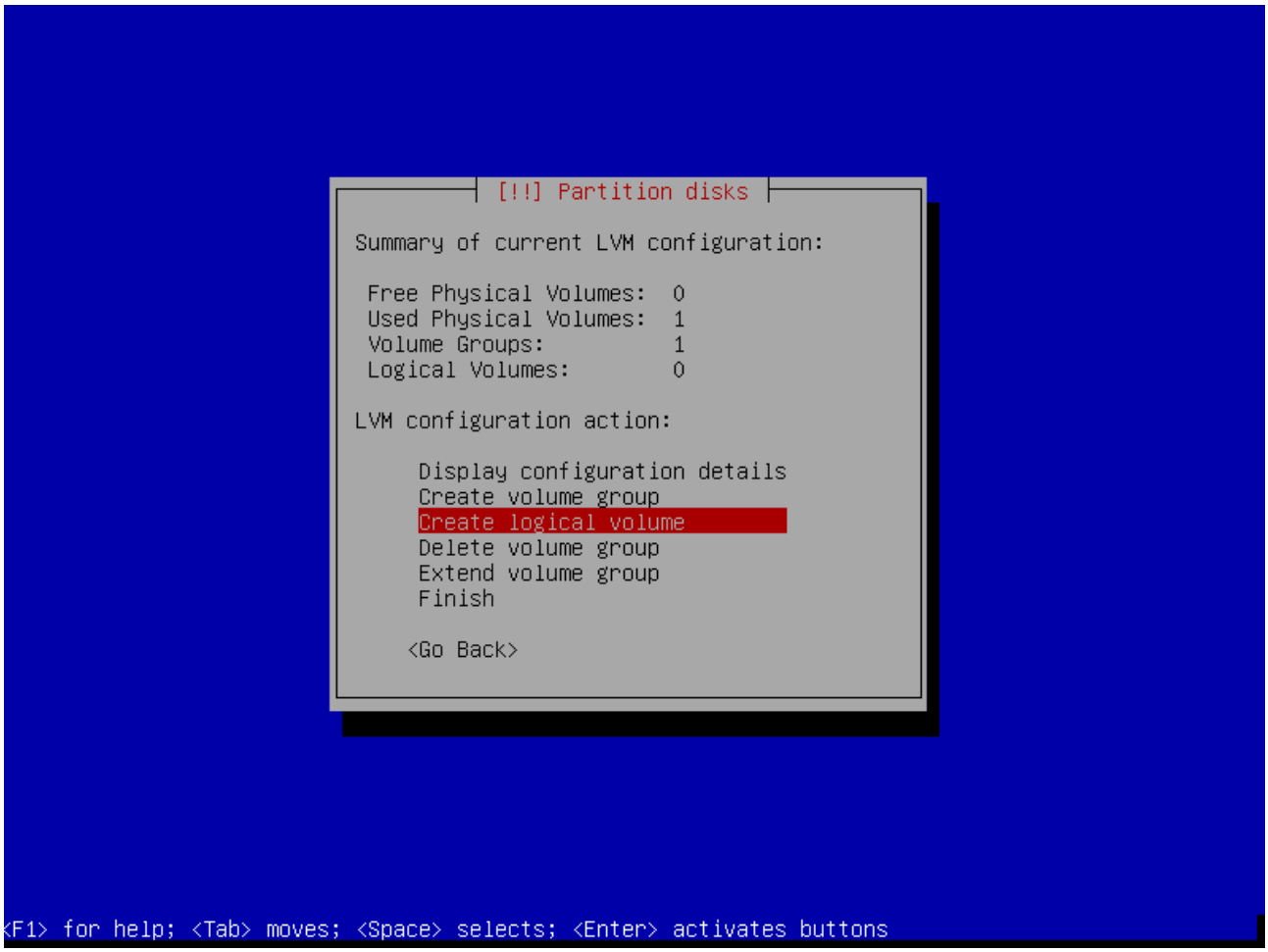
32. At the next screen, you will be asked to choose a “volume group name.” Type “vg” and press “enter.”



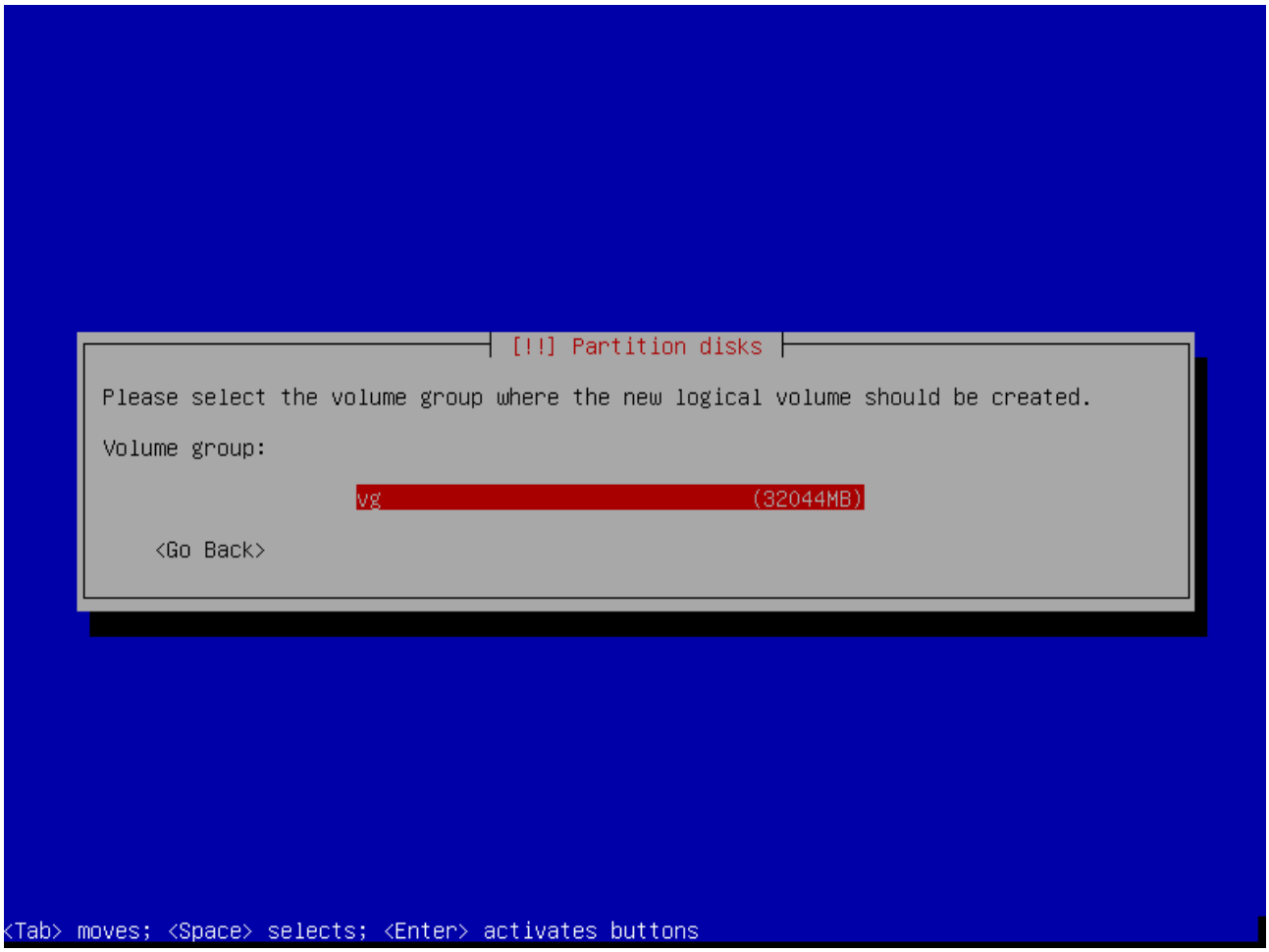
33. On the next screen, you will be asked to choose devices for the new volume group. You want to choose your encrypted partition. It will appear as "/dev/mapper/PartitionDeviceName_crypt". In the example below, it is "/dev/mapper/sda5_crypt." Select the box next to that entry and press the space-bar to enable it. When you enable it, an "*" will appear in the box. Then press "enter" to continue.



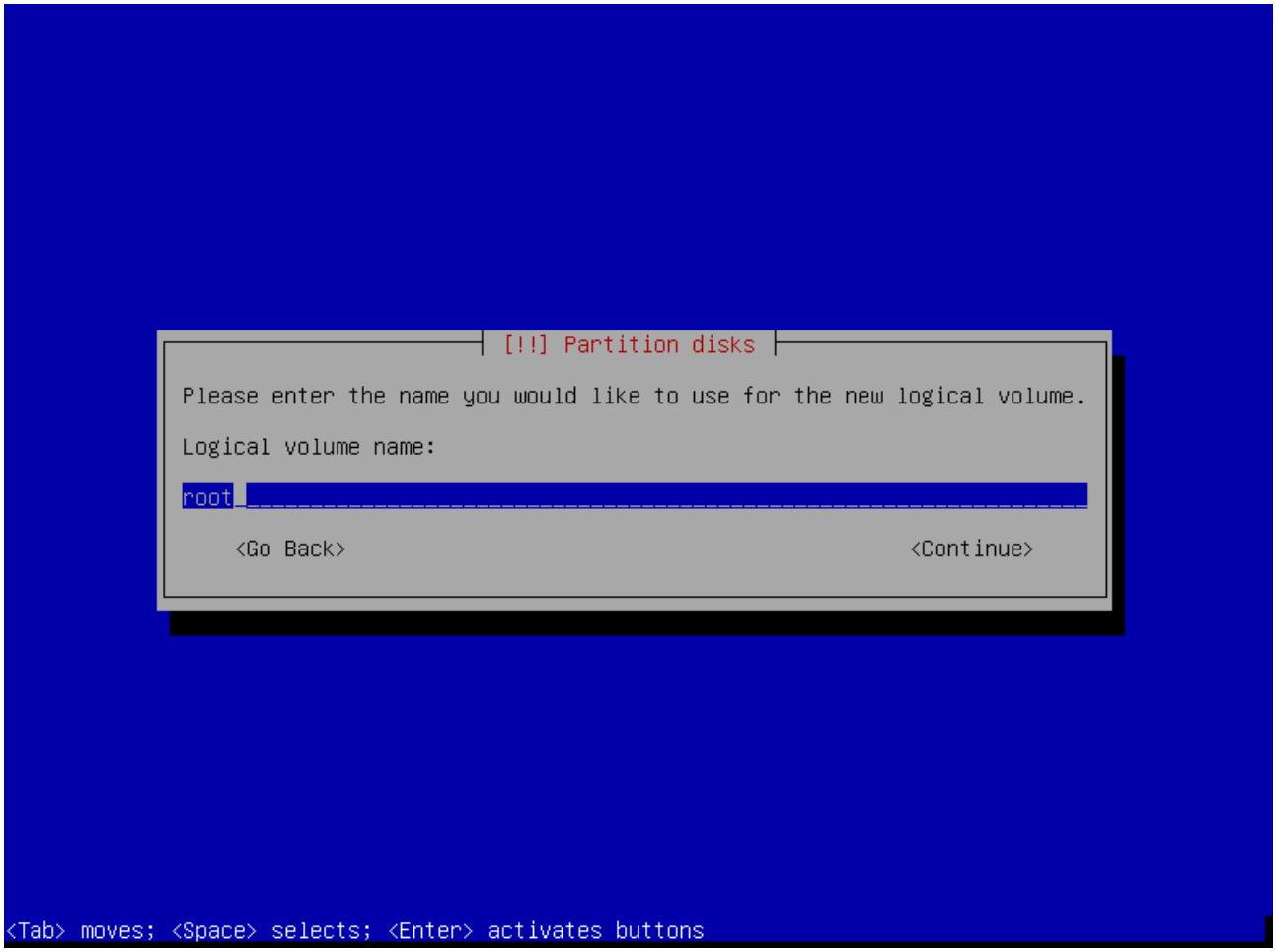
34. On the next screen, select “create logical volume” and press “enter.”



35. On the next screen, press “enter” to select “vg” and continue.

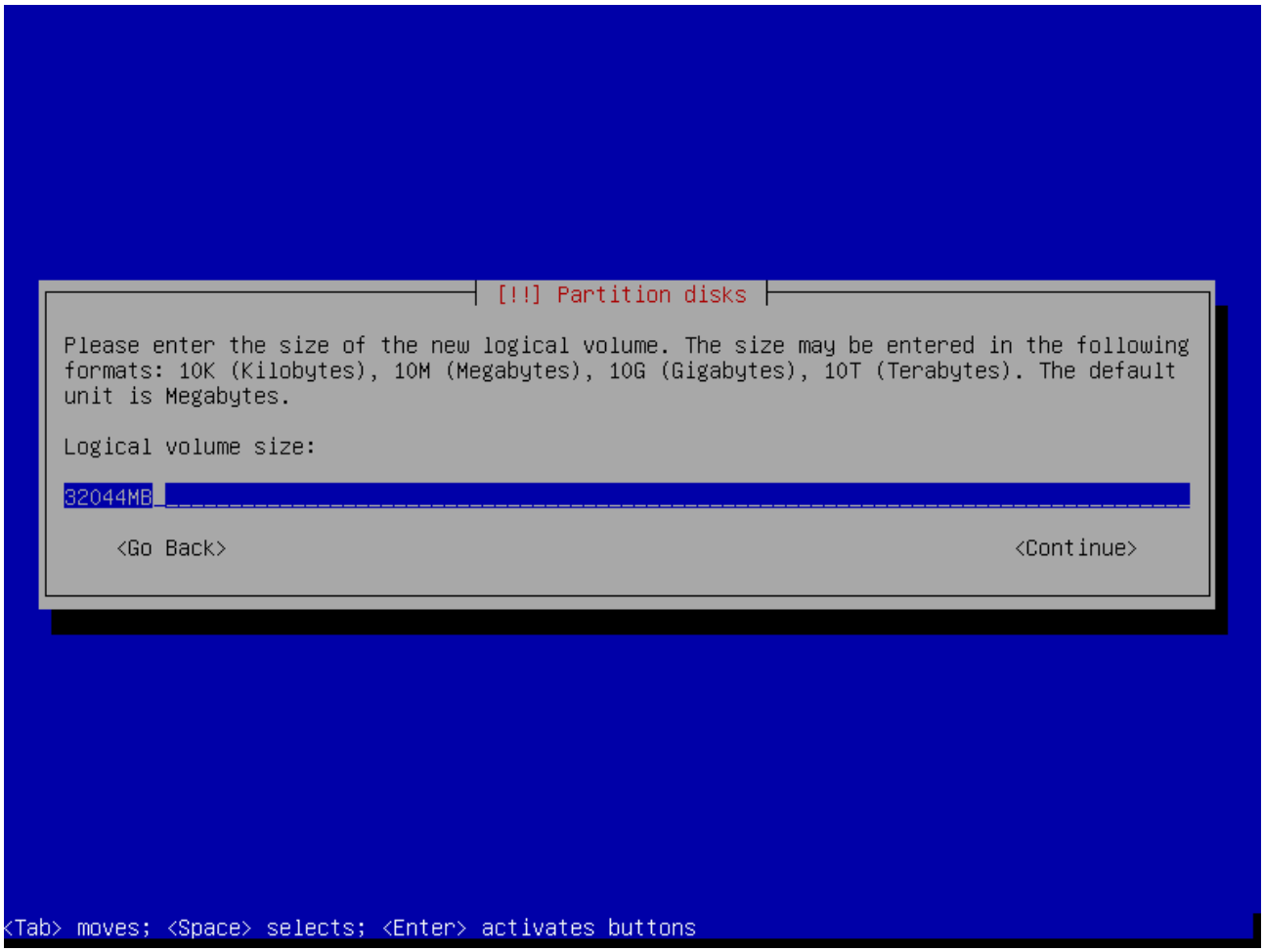


36. At the next screen, you will be prompted to create a logical volume name. Type “root” and press “enter.”

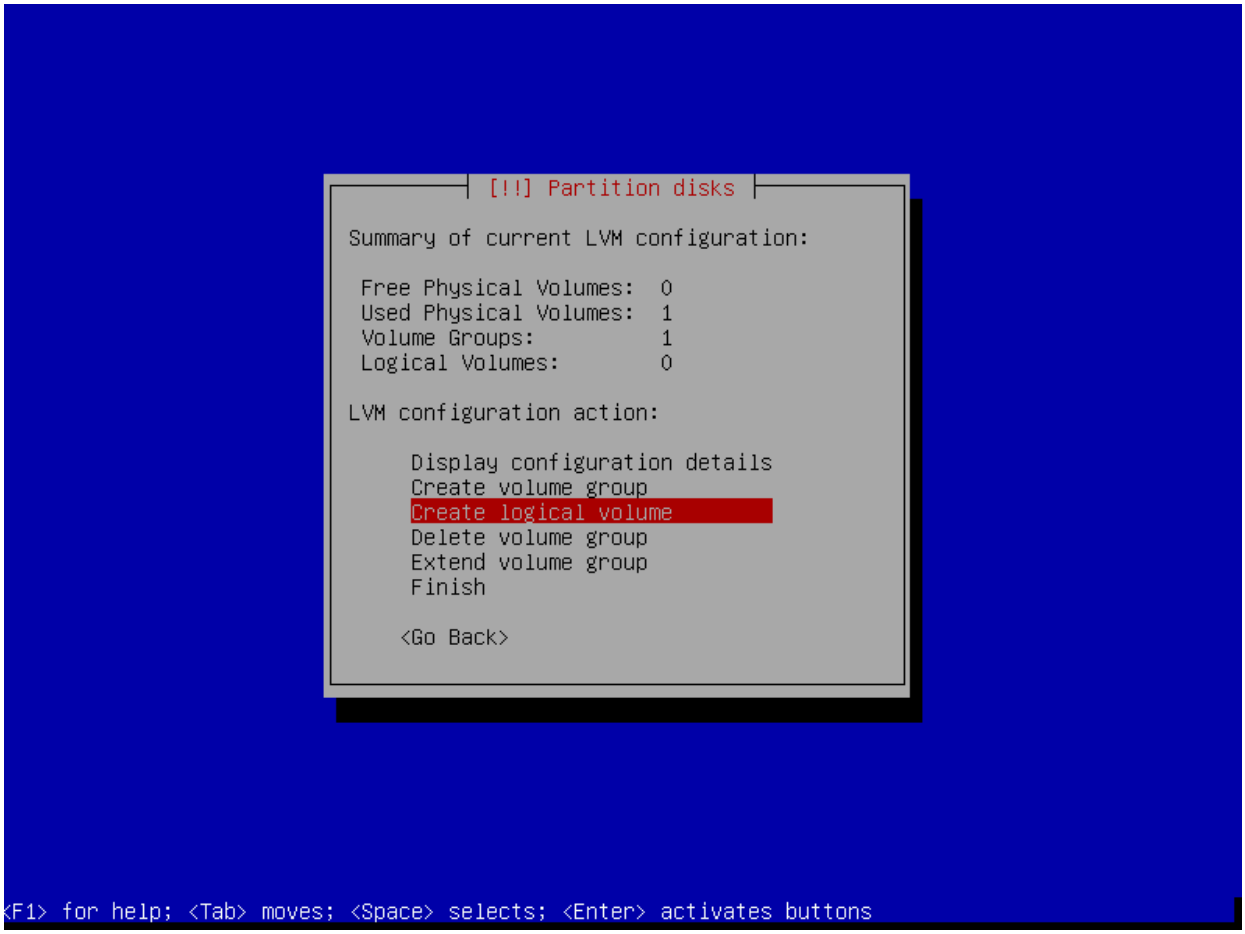


37. At the next screen, you will be asked to enter the logical volume size. **If you are installing this on a computer with less than 2 gigabytes of RAM, you will need to create an appropriately sized swap partition or the system will not work!** If you need a swap partition, a roughly 2 gigabyte partition will be more than safe (but, you may choose a smaller swap size depending on how much RAM is in your computer). Subtract 2 gigabytes from the default logical volume size and enter that number for your logical volume size. In the example below, the number would be changed from “32044” to “30044.” After you have entered the new size, press enter to continue.

    If you do not need a swap partition, accept the default entry. Press “enter” and continue to step 42.



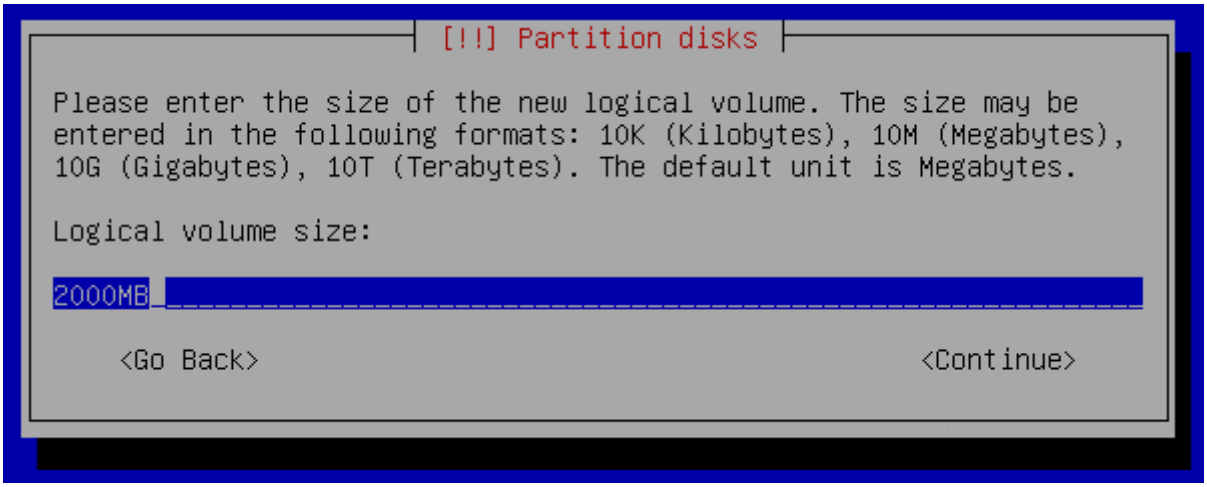
38. **You only need to do this step if you need a swap partition. If you do not need a swap partition, skip to step 42.** Select “create logical volume” and press “enter.”



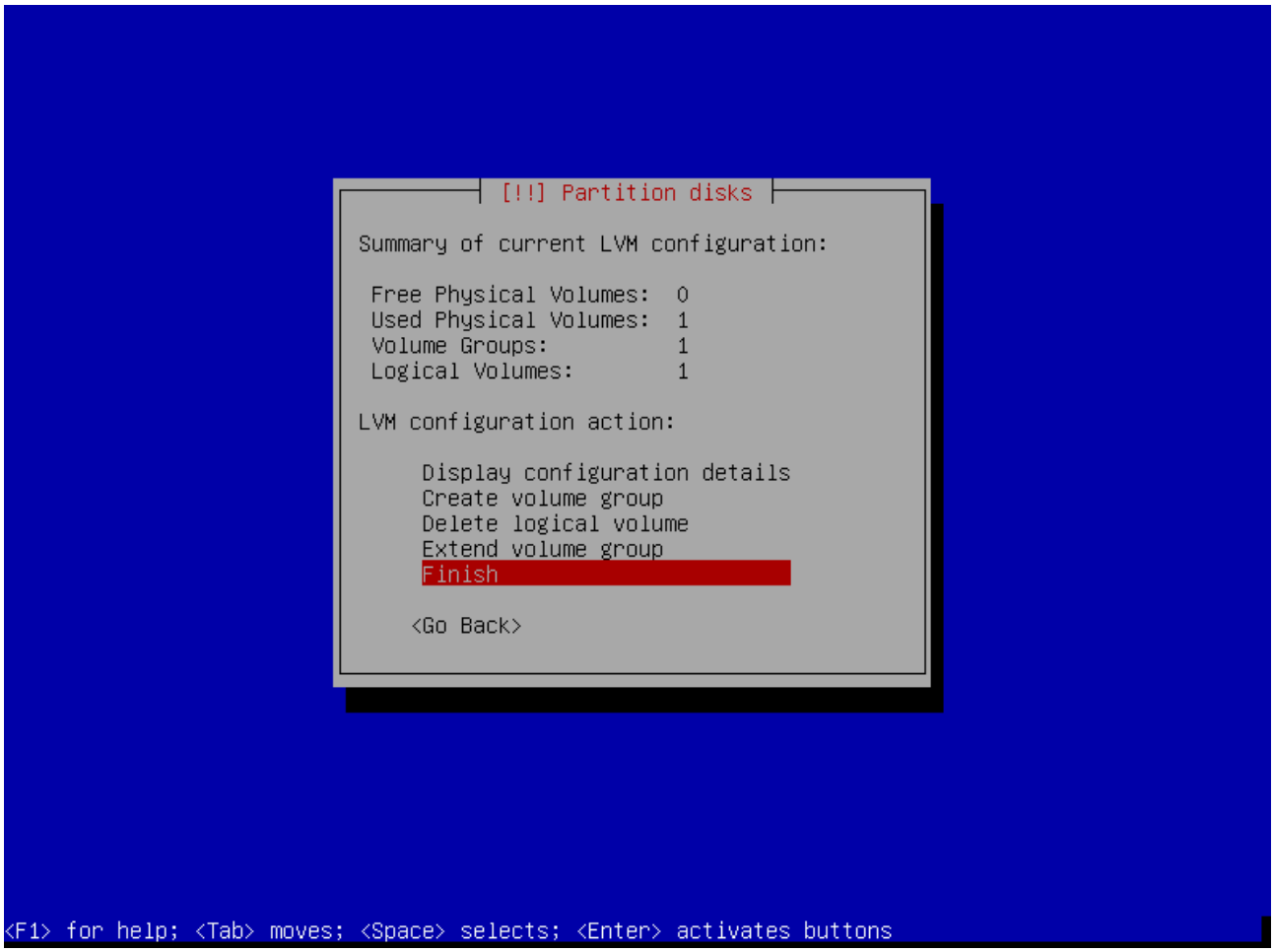
39. **You only need to do this step if you need a swap partition. If you do not need a swap partition, skip to step 42.** On the next screen, press “enter” to select “vg” and continue.

40. **You only need to do this step if you need a swap partition. If you do not need a swap partition, skip to step 42.** At the next screen, you will be prompted to create a logical volume name. Type “swap1” and press “enter.”

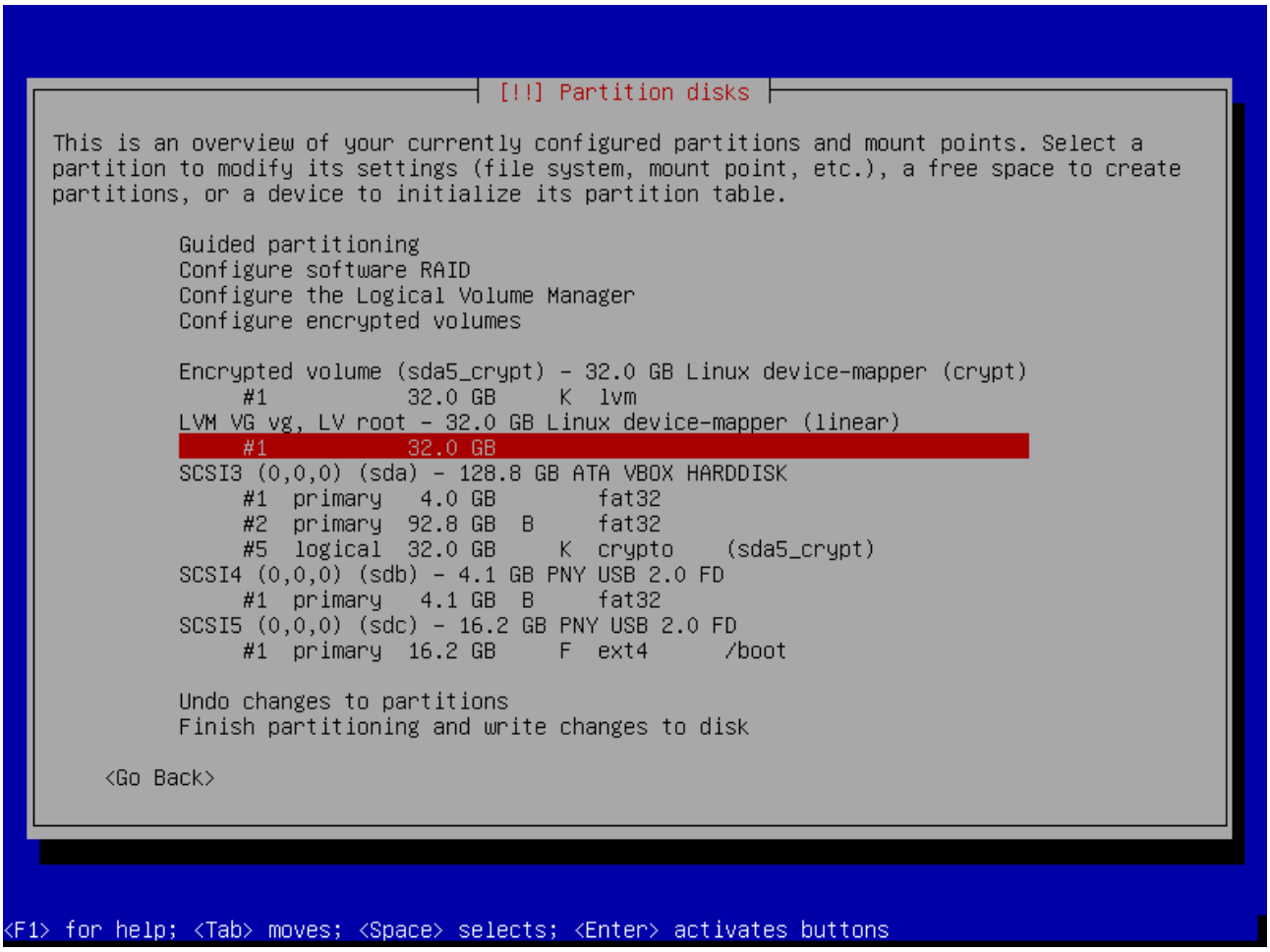
41. **You only need to do this step if you need a swap partition. If you do not need a swap partition, skip to step 42.** Next, accept the default size and press “enter.”



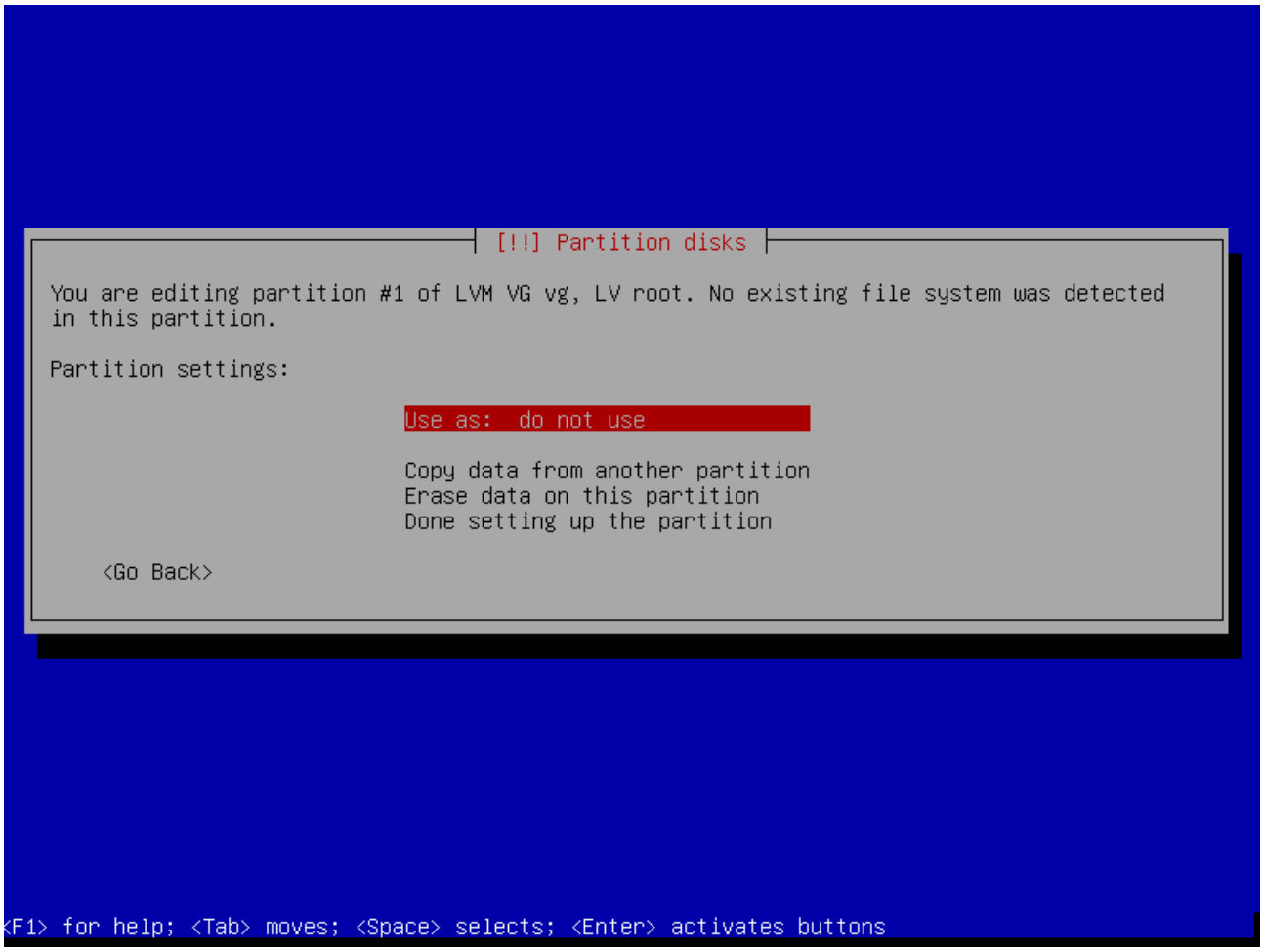
42. On the next screen, select “finish” and press “enter.”



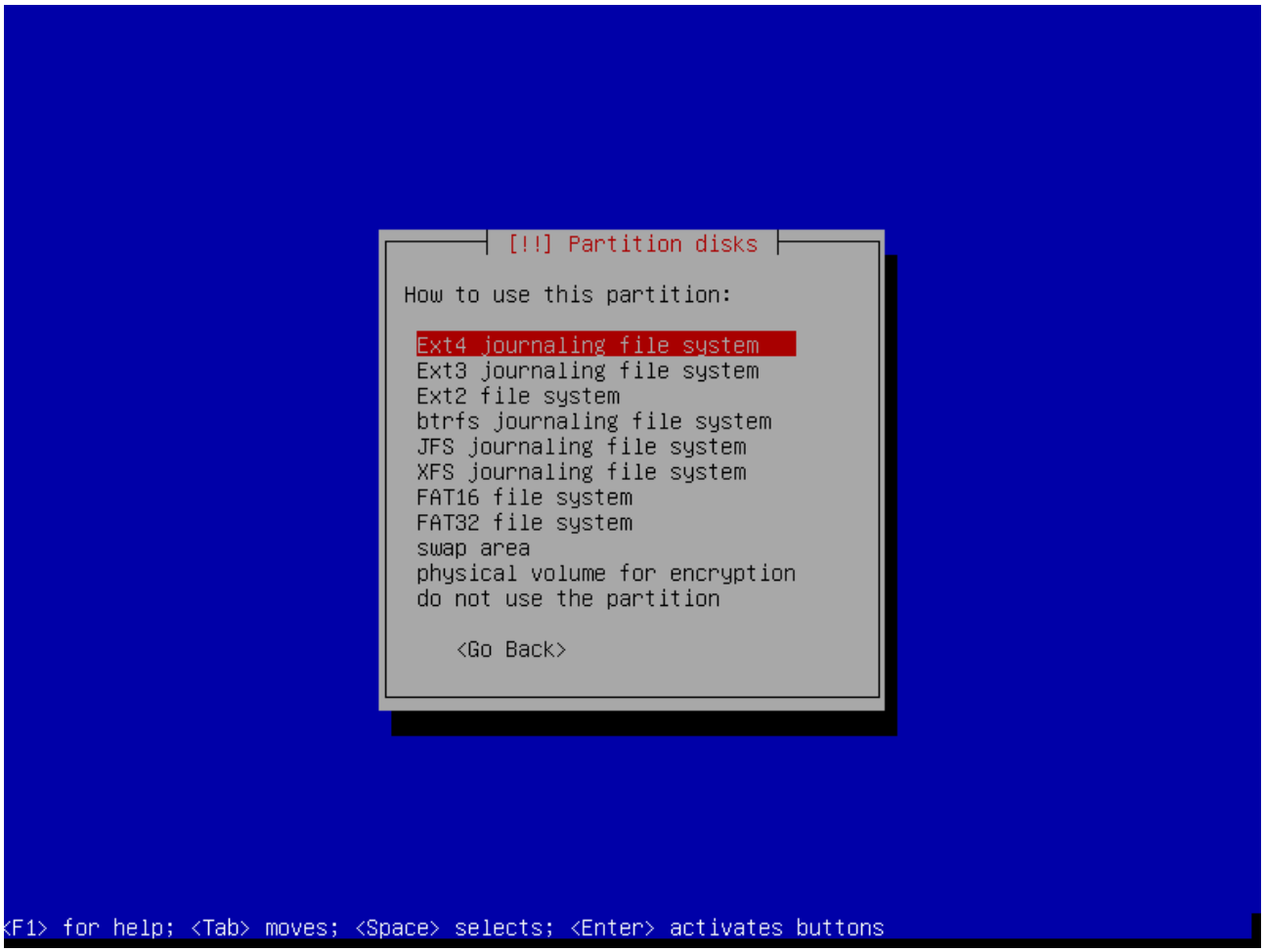
43. On the next screen, you will see a new entry for “LVM VG vg, LV root.” Choose the entry directly beneath it and press “enter.”



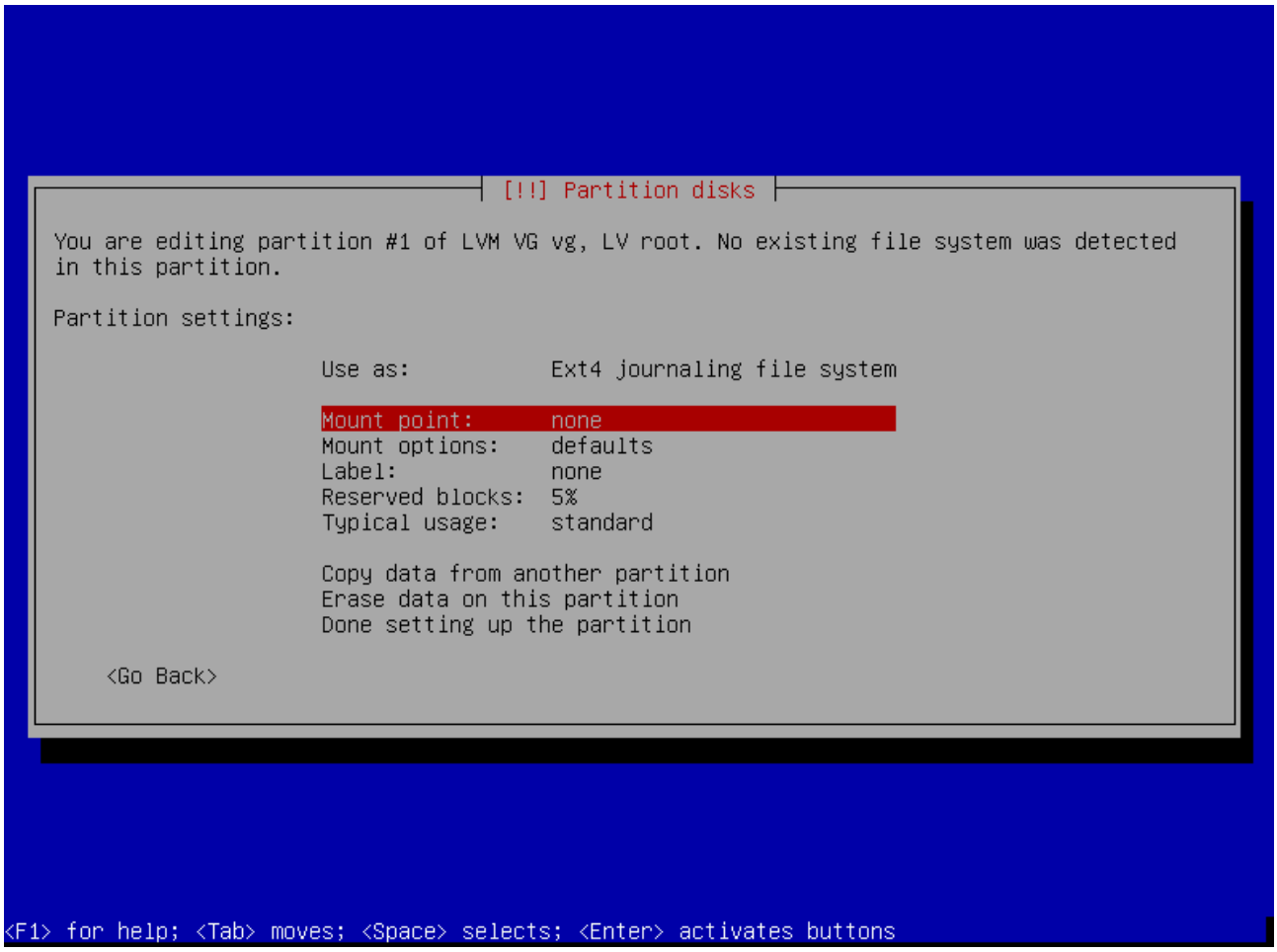
44. On the next screen, select “Use as: do not use” and press “enter.”



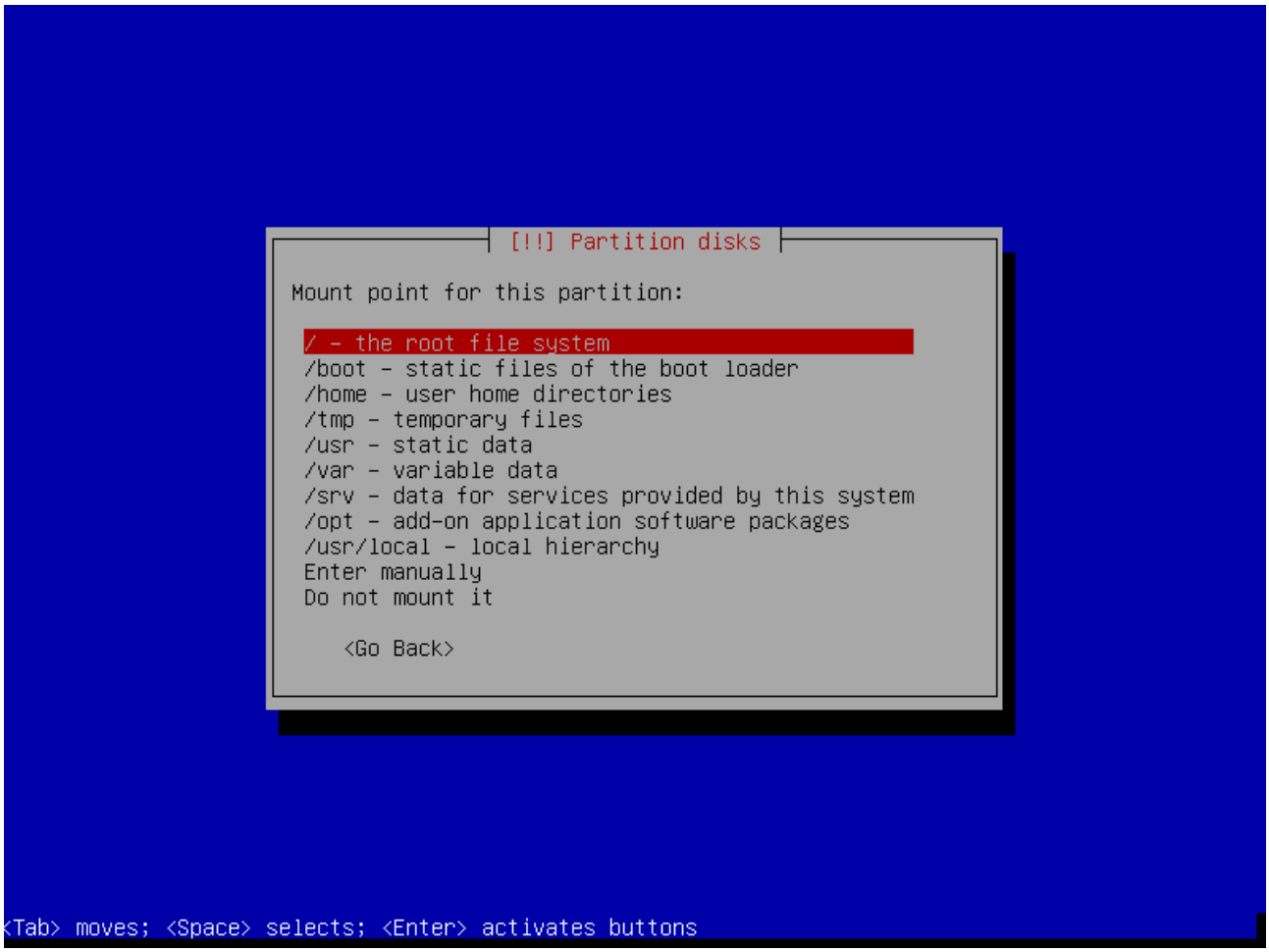
45. On the next screen, select “Ext4 journaling file system” and press “enter.”



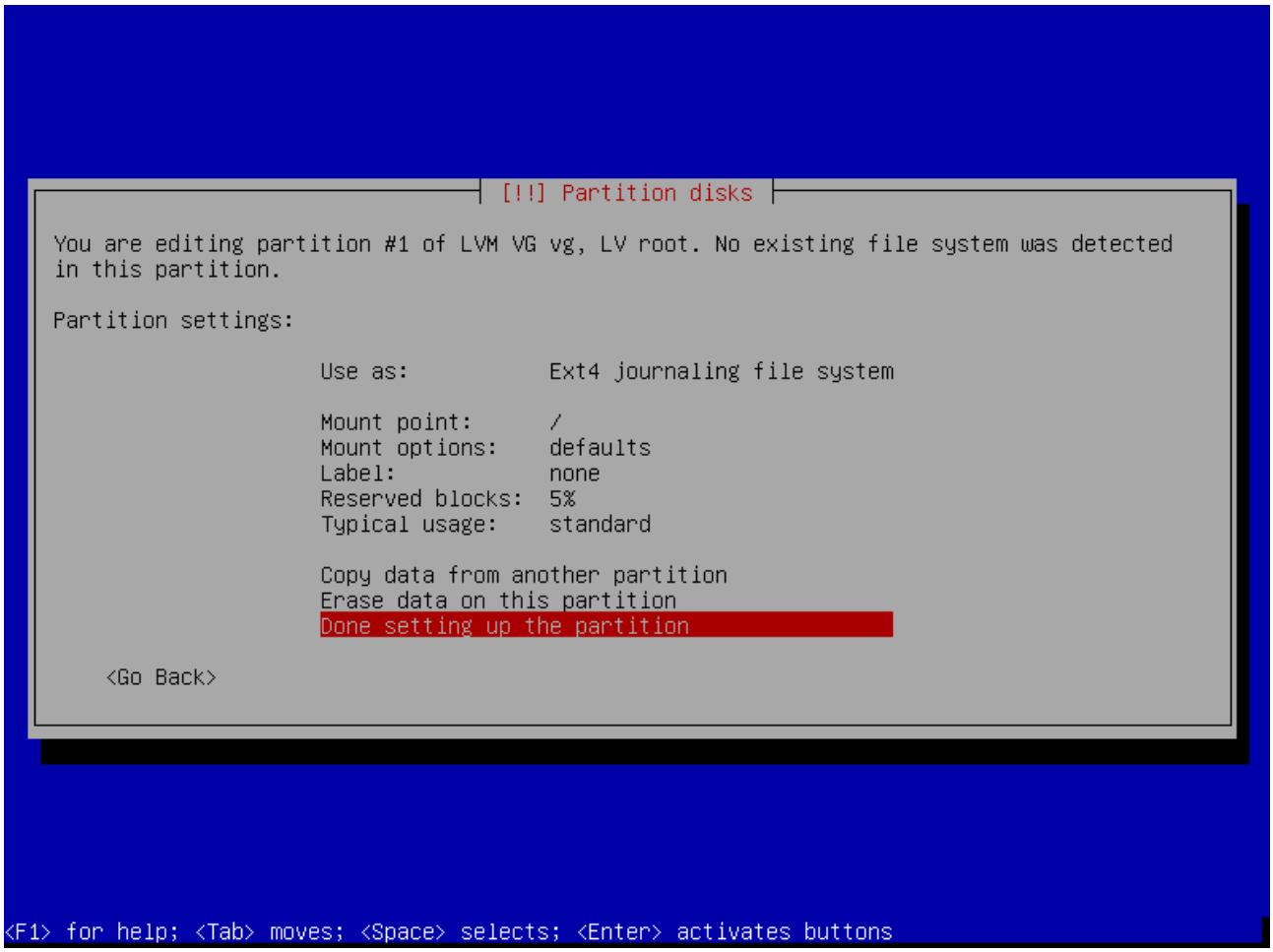
46. On the next screen, select “Mount point: none” and press “enter.”



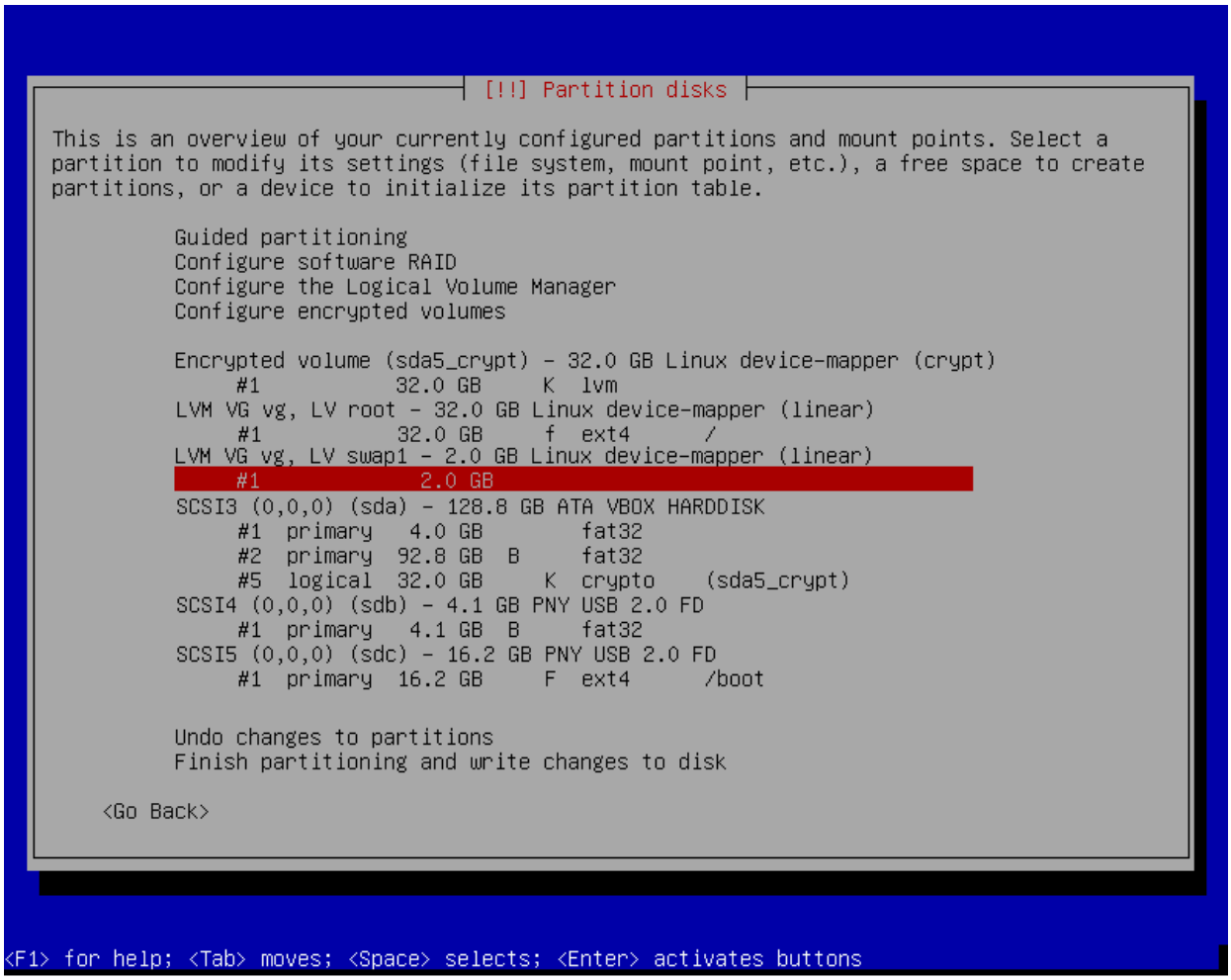
47. At the next screen, select “/ - the root file system” and press “enter.”



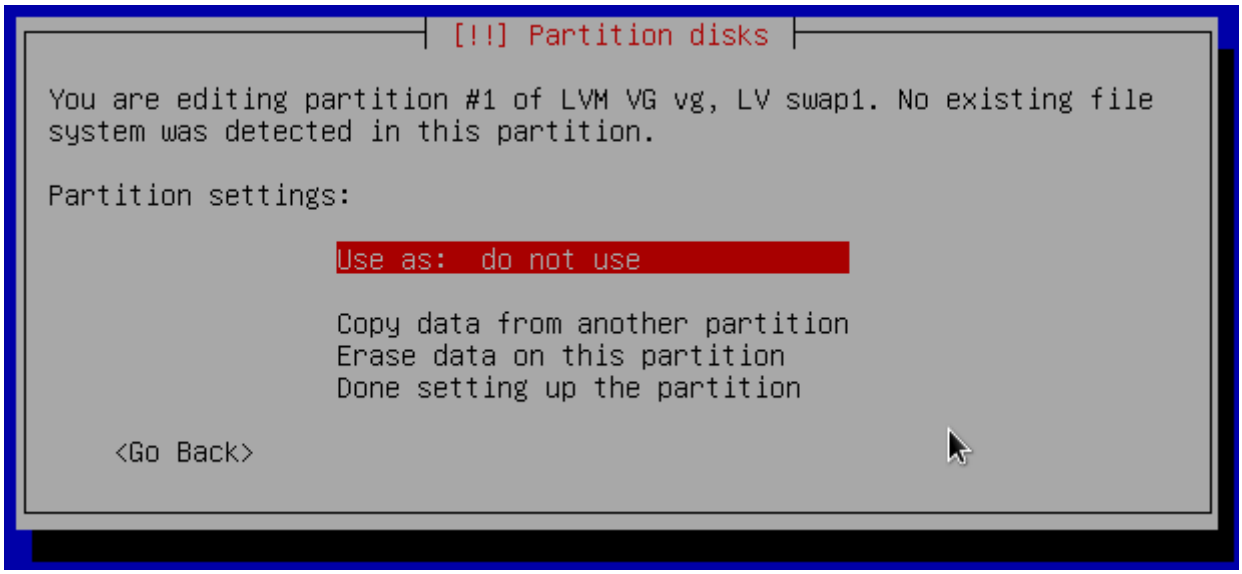
48. At the next screen, select “done setting up the partition” and press “enter.”



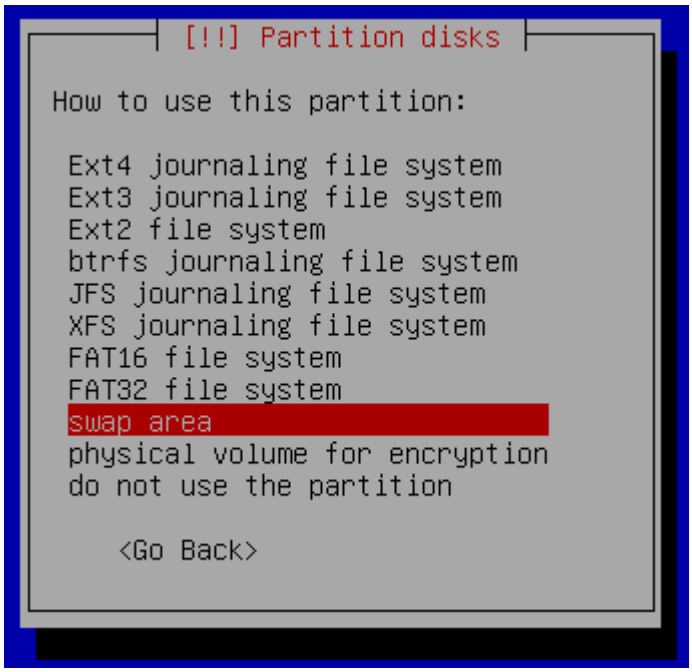
49. **You only need to do this step if you created a logical volume for a swap partition. If you did not create a logical volume for a swap partition, skip to step 53.** If you created a logical volume for your swap space, you will also see a new entry entitled “LVM VG vg, LV swap1.” Choose the entry directly beneath it and press “enter.”



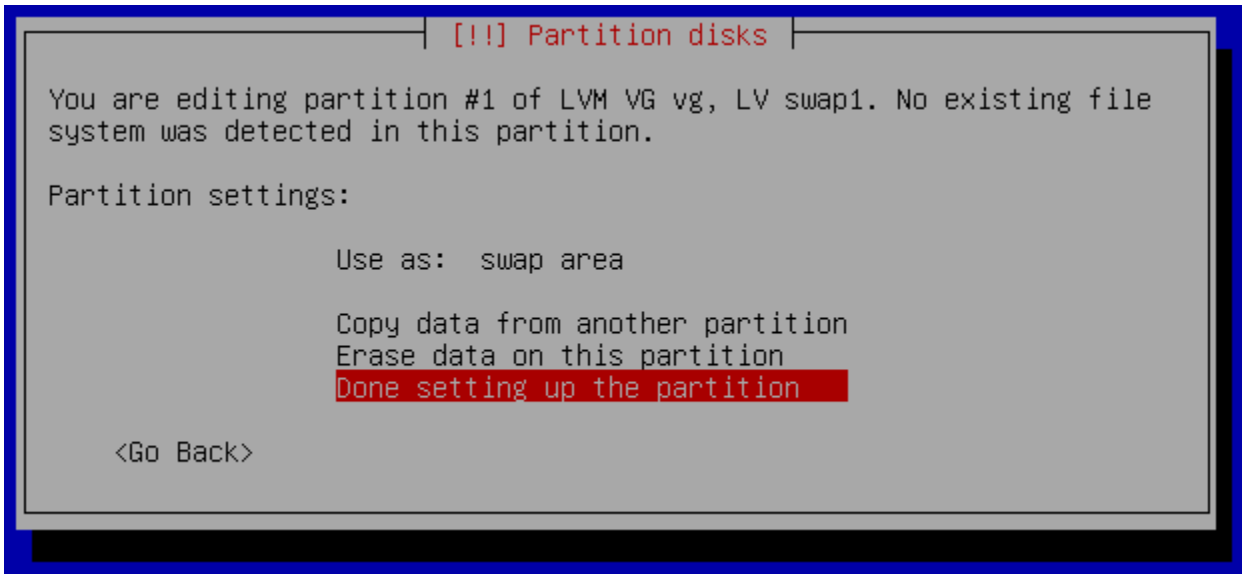
50. **You only need to do this step if you created a logical volume for a swap partition. If you did not create a logical volume for a swap partition, skip to step 53.** On the next screen, select “Use as: do not use” and press “enter.”



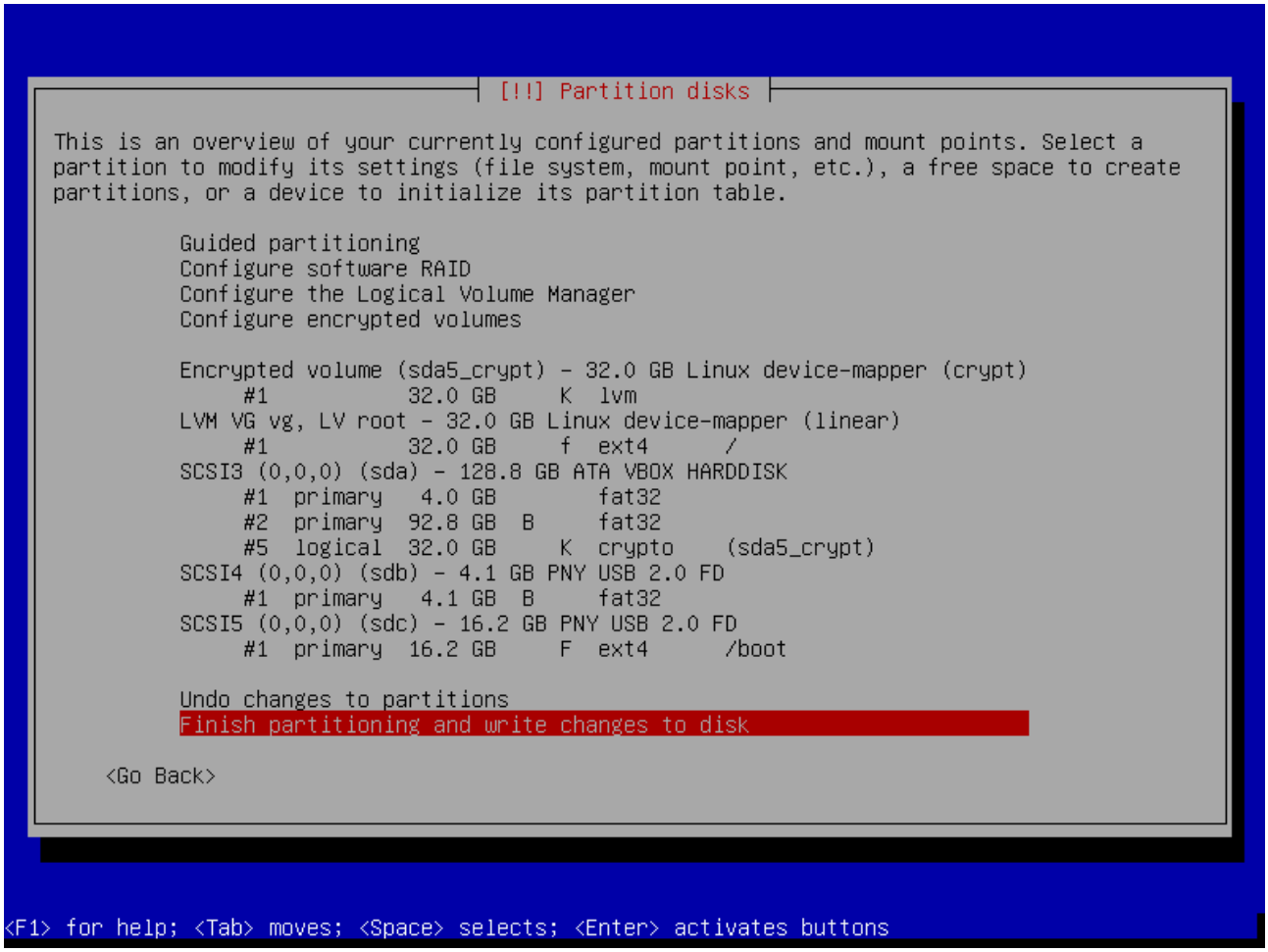
51. **You only need to do this step if you created a logical volume for a swap partition. If you did not create a logical volume for a swap partition, skip to step 53.** On the next screen, select “Swap area” and press “enter.”



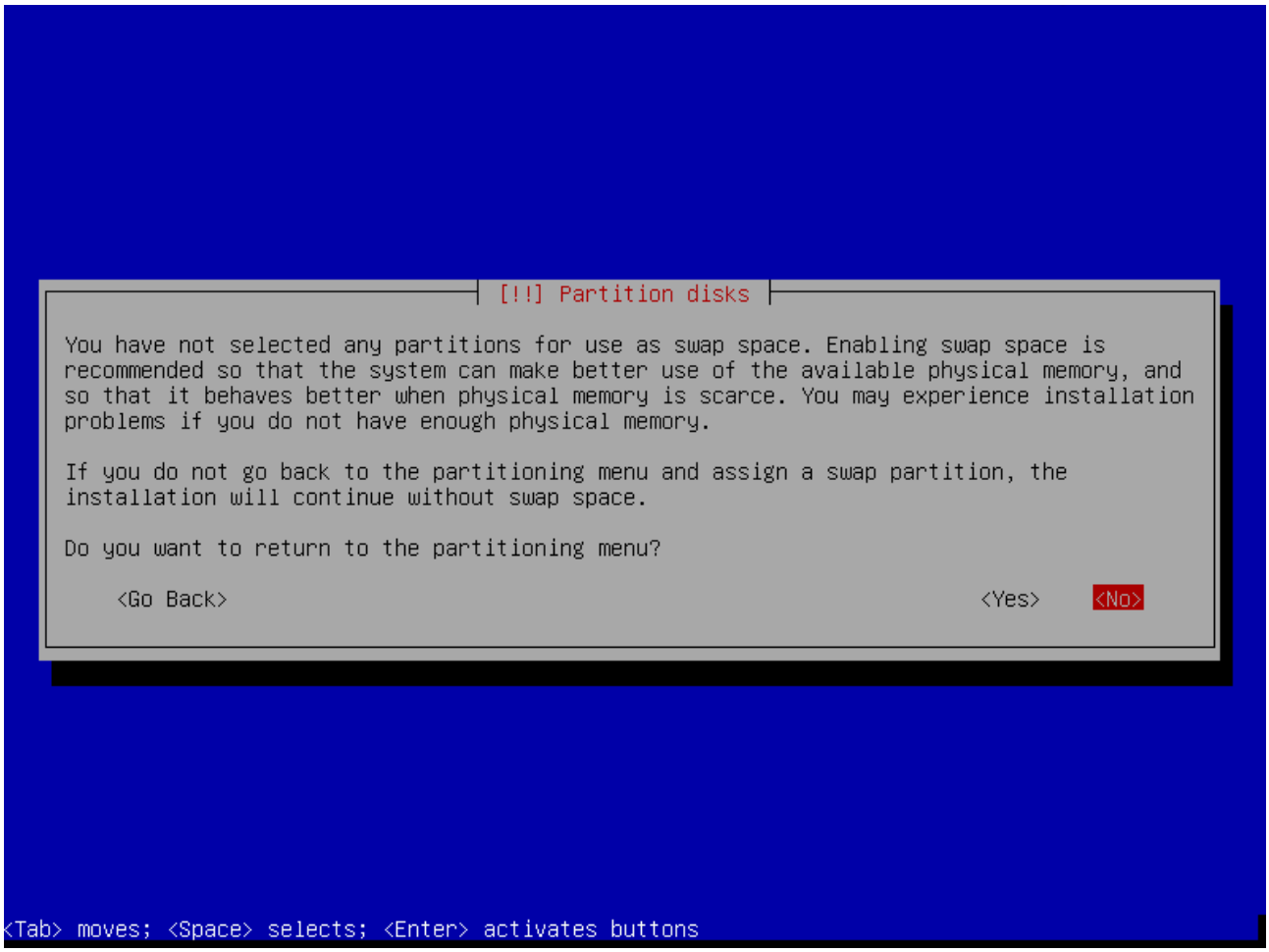
52. **You only need to do this step if you created a logical volume for a swap partition. If you did not create a logical volume for a swap partition, skip to step 53.** At the next screen, select “done setting up the partition” and press “enter.”



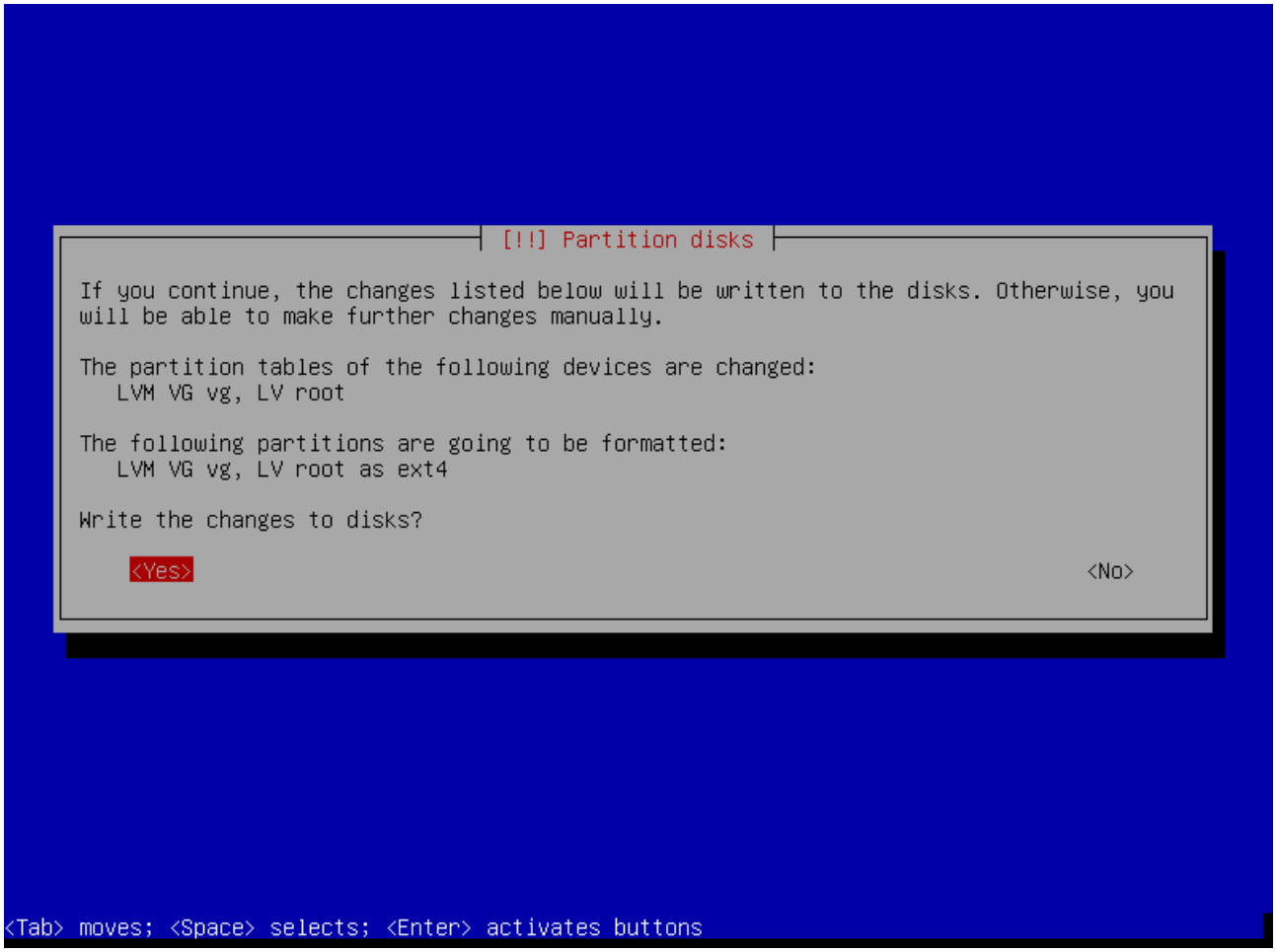
53. On the next screen, select “finish partitioning and write changes to disk” and press “enter.”



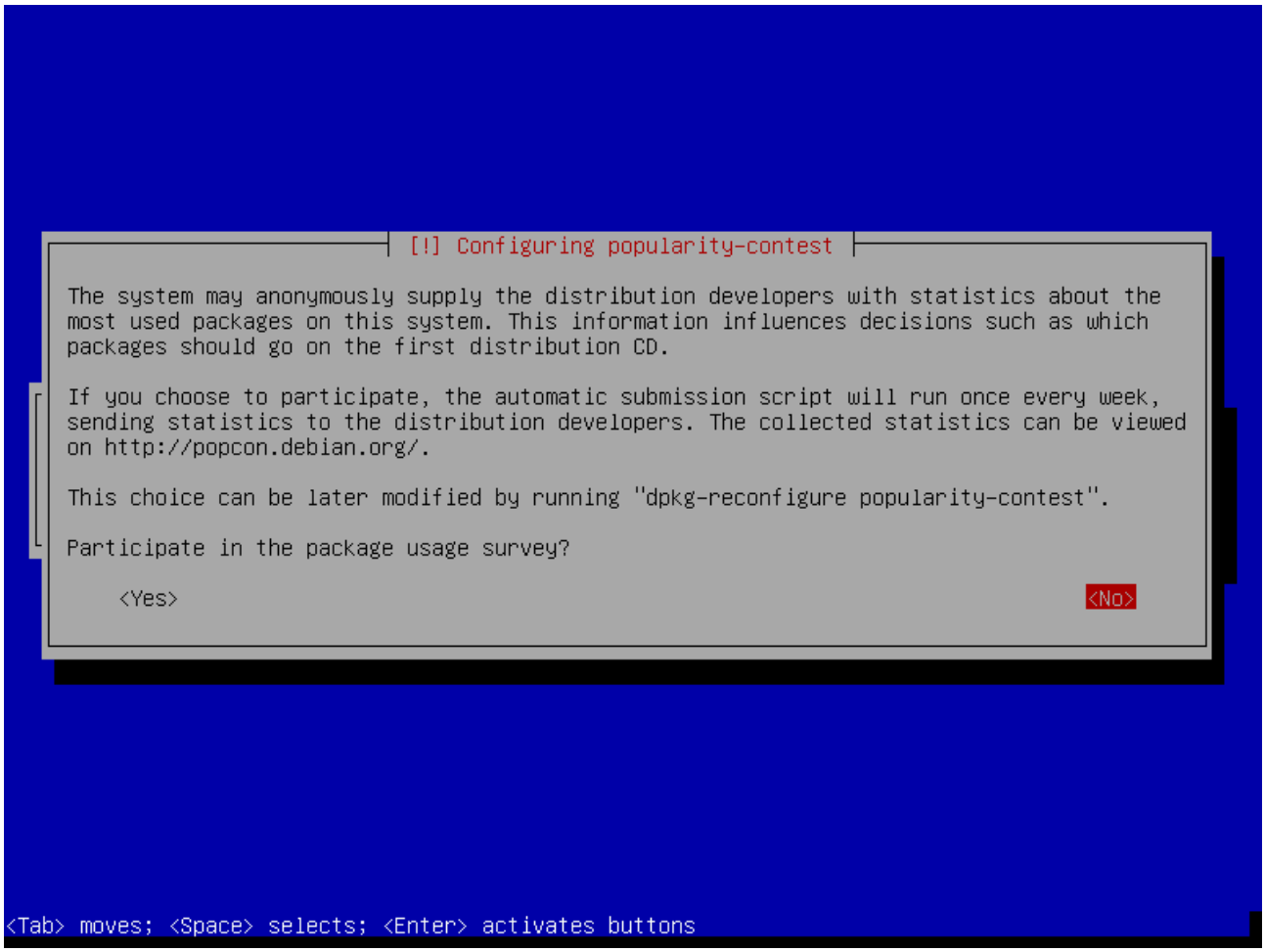
54. If you decided you did not need a swap partition, the next screen will inform you that you haven't selected a partition for swap space and ask if you want to return to the partitioning menu. Select “no” and press “enter.”



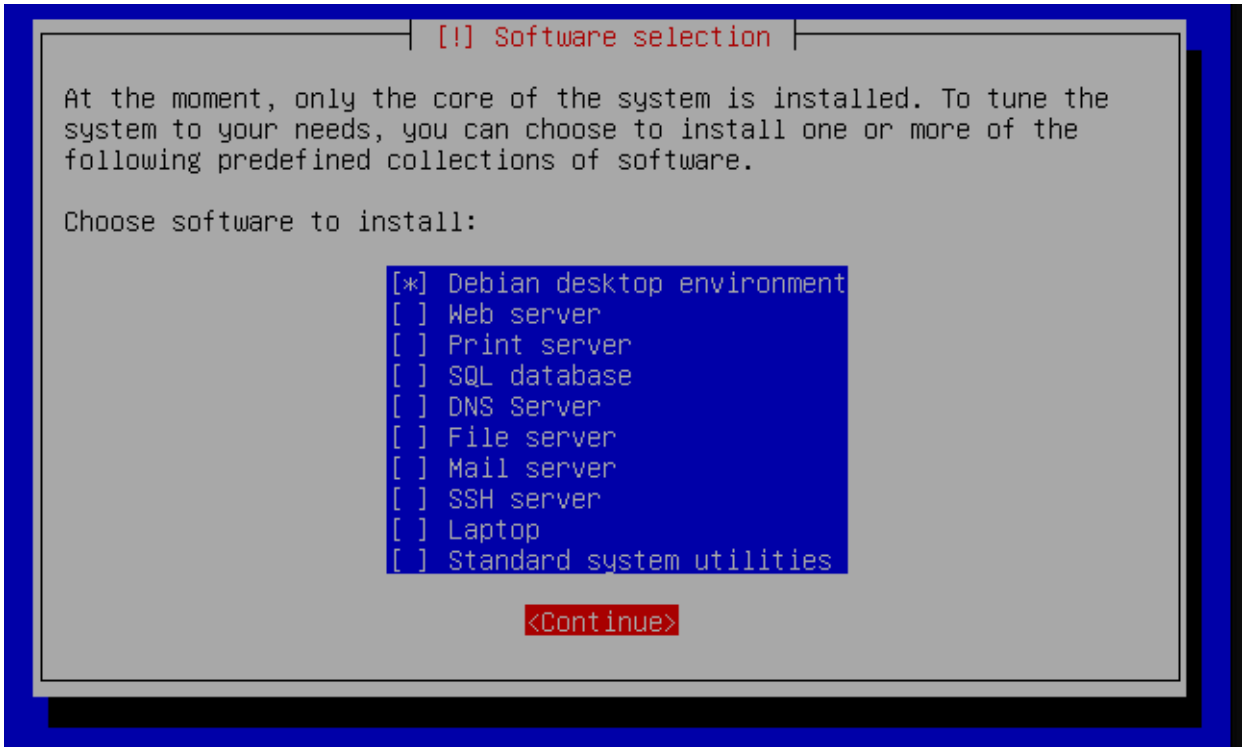
55. The next screen will ask if you want to write the changes to disk. Select “yes” and press “enter.”



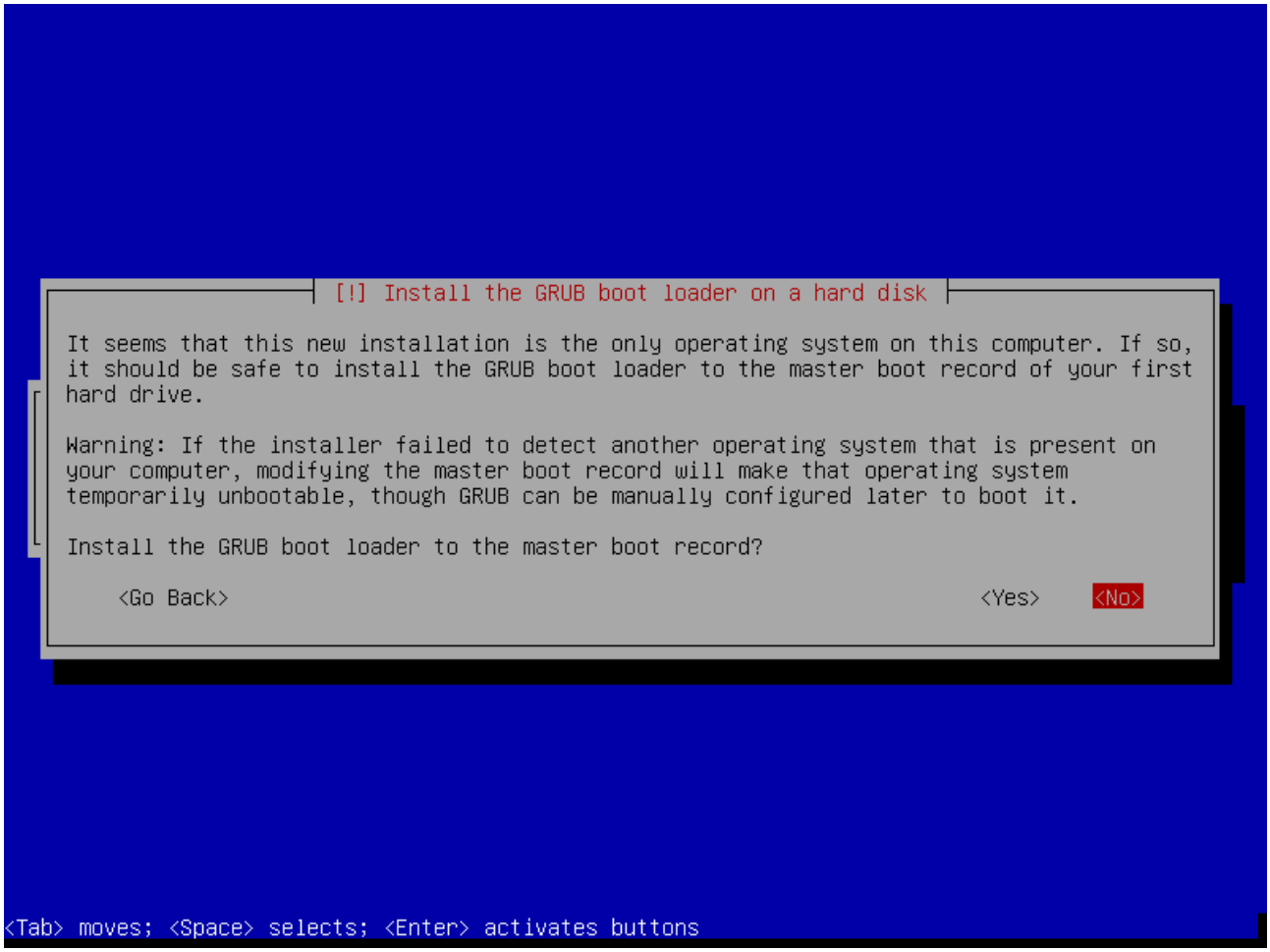
56. The installer will next go trough the process of “configuring apt” and installing various software. At the next prompt, you will be asked if you want to “participate in the package usage survey.” Select “no” and press “enter.”



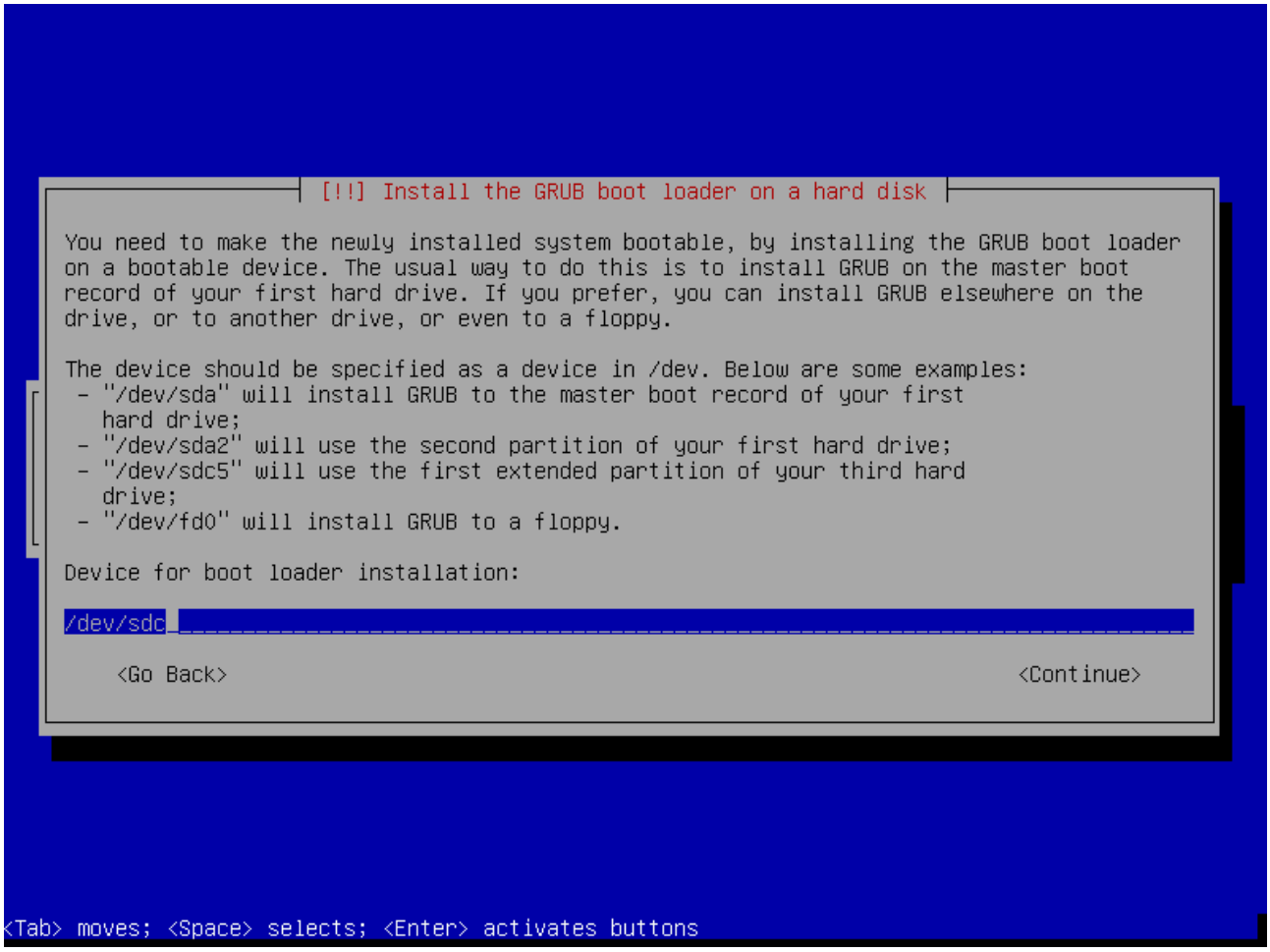
57. The installer will again perform some tasks until it prompts you to “choose software to install.” You only want to install the “Debian Desktop Environment.” Unselect the other chosen items by moving the arrow key until they are highlighted and pressing the space bar. When the “*” disappears, the item is unselected. When your screen looks like the screen shot below, press “enter” to continue.



58. The installer will now begin retrieving files and will then install them. This will take a long time. Eventually, you will be asked if you want to “Install the GRUB boot loader to the master boot record.” The screen shot below will not likely look the same as your's, as it will probably have discovered additional operating systems. This is not something you need to be concerned about. Select “**no**” and press “enter.”

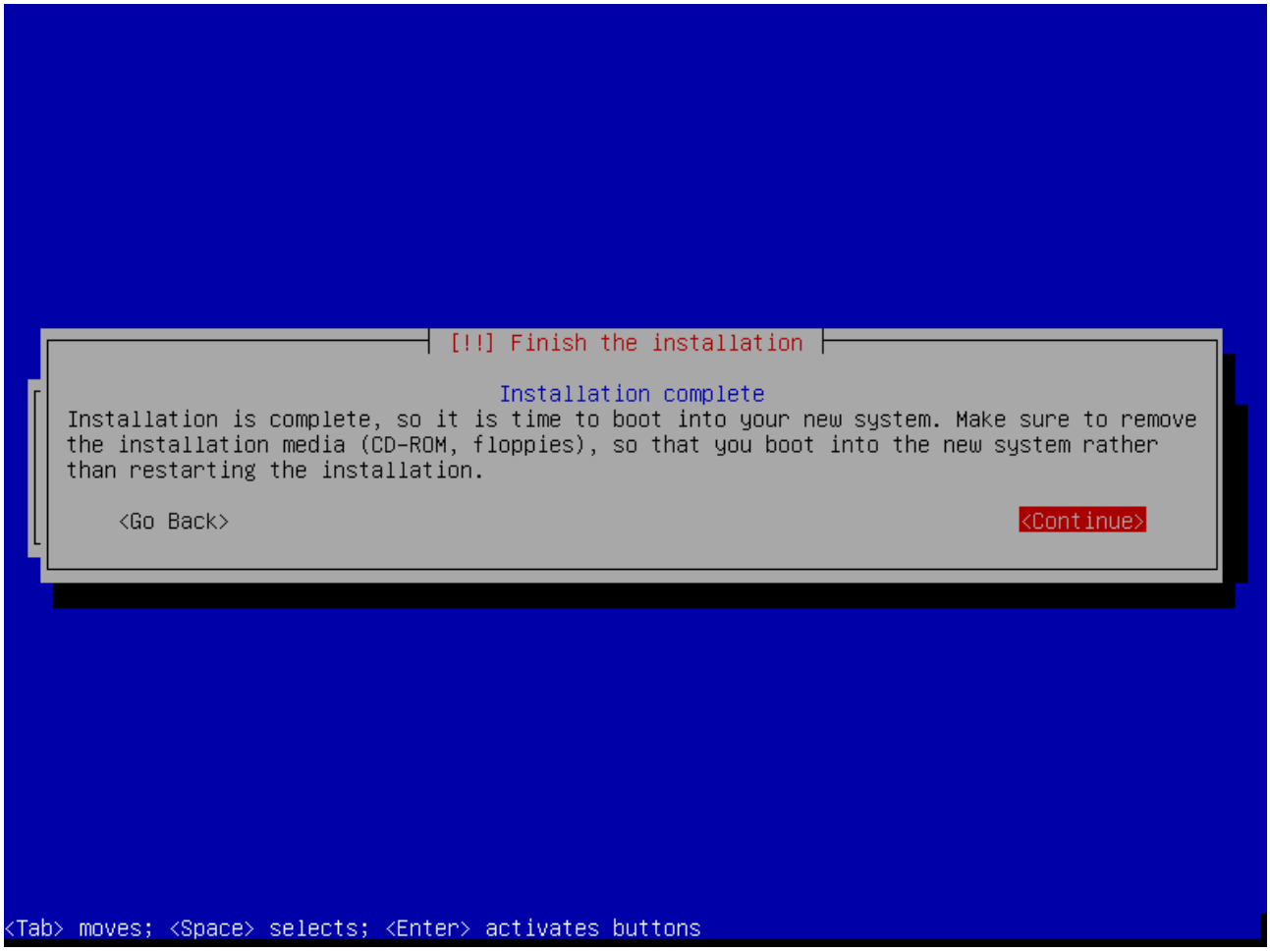


59. The next screen will ask you to type the “Device for boot loader installation.” In step 2 of this chapter, you were instructed to make a note of the device name that was the USB flash drive where you were installing Debian. The example used in this tutorial was “sdc.” You need to enter the device name for your USB flash drive. However, the name needs to be preceded by “/dev/”. Thus, in the example in this tutorial, the entry would be “**/dev/sdc**”. You need to enter the name of your device which will be in the format of “/dev/YourDeviceName” and press “enter.”

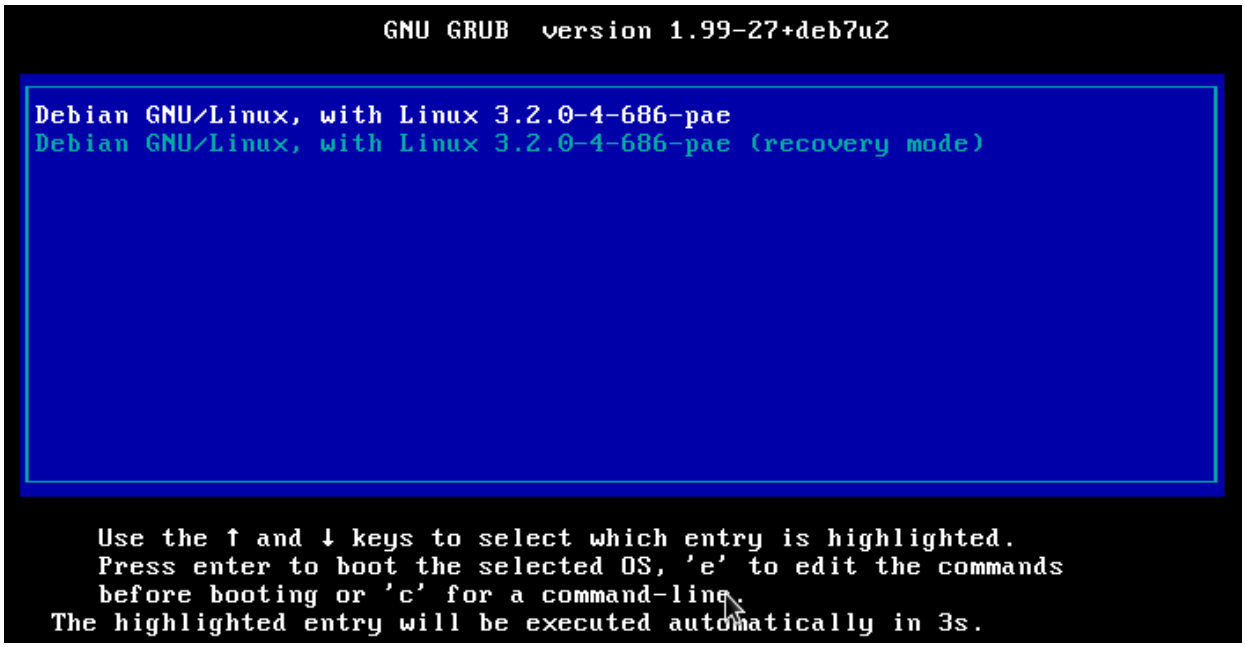


60. Now the installer will go through the process of finishing the installation. You will eventually be informed that the installation is complete. Remove the Debian Install Disk and press “enter.”

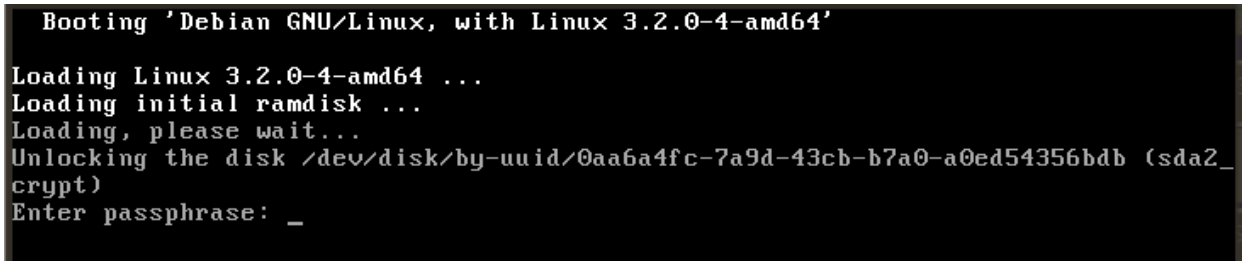
    NOTE: If the installation process took long enough to make you run out of time, you can shut down your computer at this point after the installer goes through the clean up process and restarts the machine. You can then continue from step 61 at a later time.



61. The installer will eventually reboot your computer. As your computer restarts, you need to get into a boot menu again in the same manner the you did in step 4 of chapter 1. When you activate the boot menu, choose your USB flash drive on which you installed Debian. Eventually, you will be prompted to choose a boot selection. It will default to Debian and, thus, you can either press “enter” or wait for the timer to run out. The example screen below may not look exactly the same as your's. But, it is essentially the same thing.



62. The next screen will prompt you to “enter passphrase.” This is the encryption passphrase you created in step 27 of this chapter. You will not see any symbols on your screen when you type your password. While this may seem odd, it is for security reasons. Someone watching your screen won't be able to determine the length of your passphrase. Type your passphrase and press “enter.”

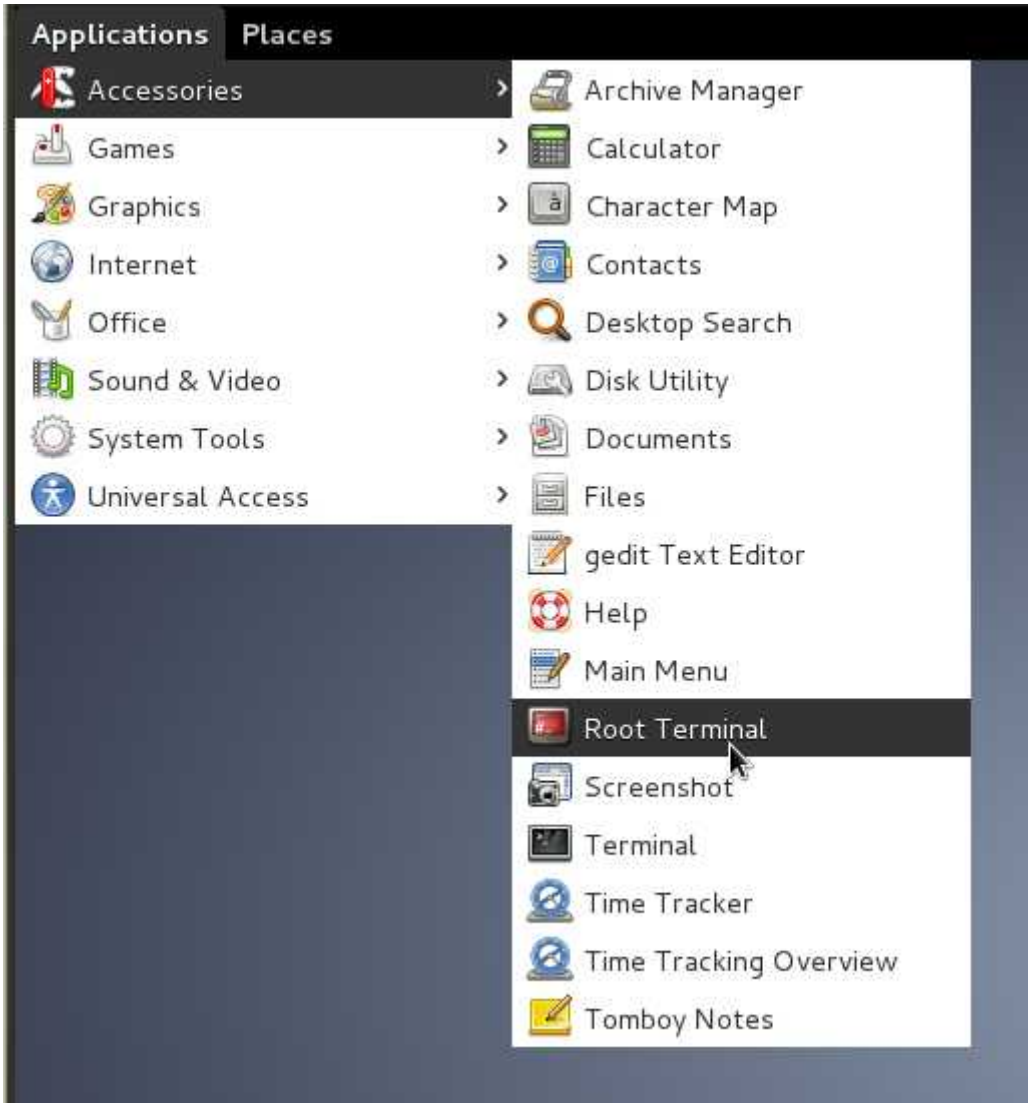


63. Debian will now go through its boot process. Eventually you will reach the login window. When you reach the login window, press “enter” or click on “user.”

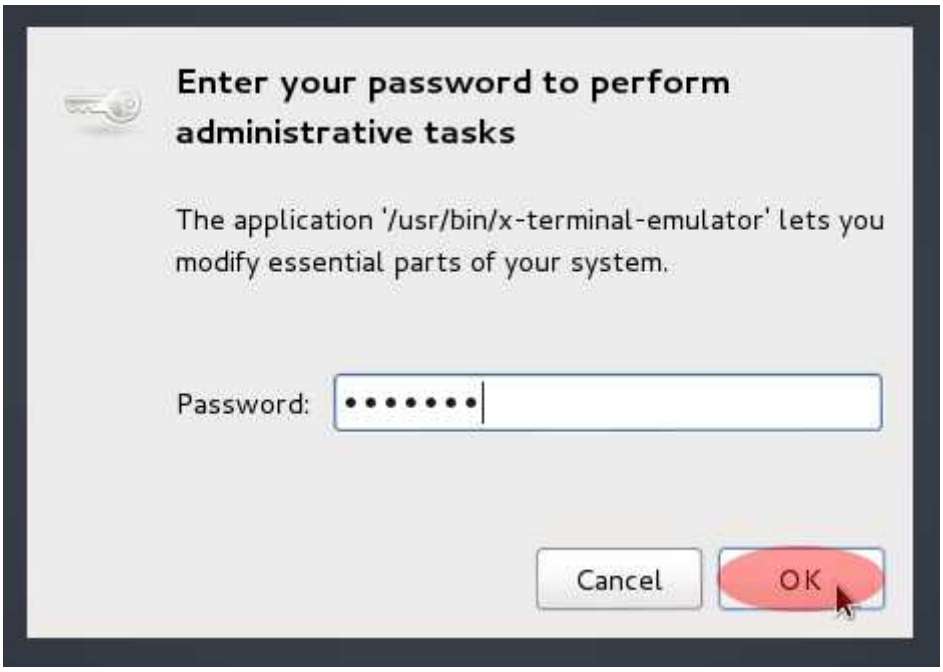
64. On the next screen, you will be prompted for your password. Before typing your password, click on the pull down menu that says “system default” and select “GNOME Classic.” Then, type the password you created for “user” in step 19 of chapter 1 and press “enter.” Debian will use “GNOME Classic” for every other login until you choose something different. You won't ever need to.

65. When you reach the Debian desktop, click on Applications in the upper right corner, then choose “Accessories → Root Terminal.”

    NOTE: Whenever you use this command, **you will have full root/administrative access until you “exit” the session.** Thus, **be extra cautious** in your session whenever you decide to use this command. **The changes you make can be damaging and permanent if you do something wrong.**



66. You will next be prompted to enter your password to perform administrative tasks. This is the same password you chose for “user” in step 19 of chapter 1. Type your password and click “ok.”

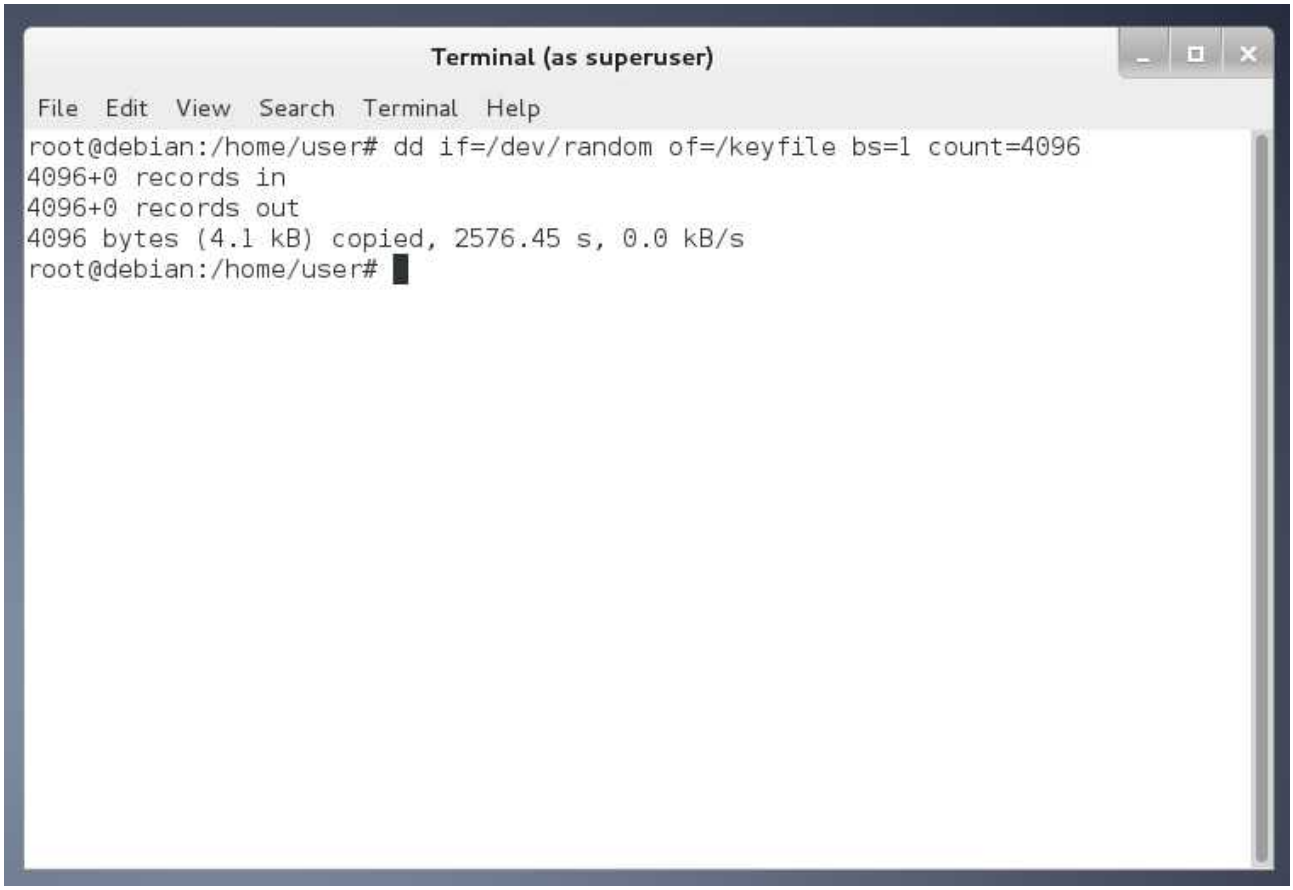


67. You will now be at a shell prompt as superuser (aka 'root') in a terminal program. Now you need to create your key file to unlock your hard drive in the future. Type the following line into the terminal:

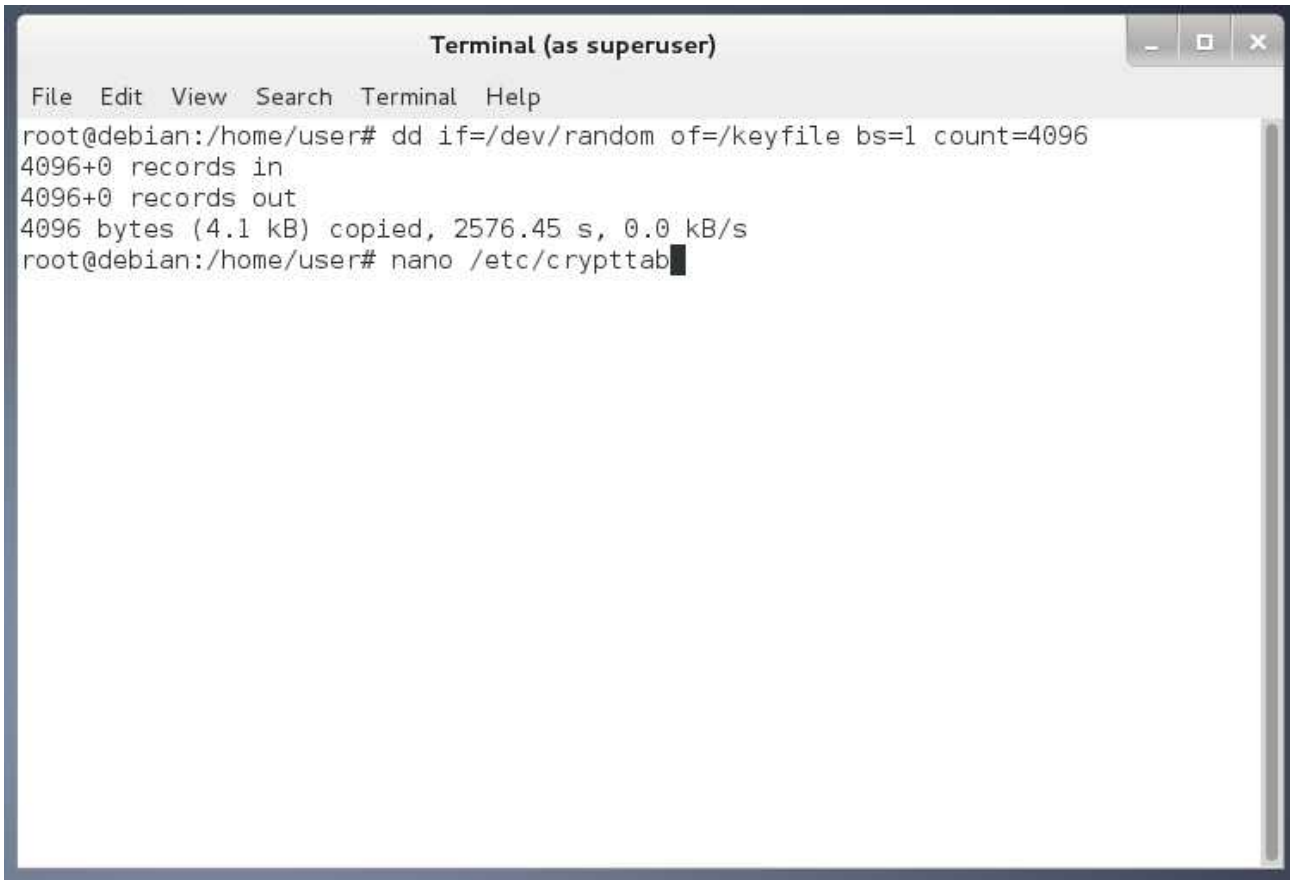
    dd if=/dev/random of=/keyfile bs=1 count=4096

    This will create a 4 kilobyte key file of entirely random data. The process may take awhile. In order to create more entropy for /dev/random and speed up the process, consider playing the included games from the Applications menu. /dev/random will create entropy from your mouse gestures and clicks in those games. When the process for generating the key file finishes, a cursor will appear next to a new prompt.

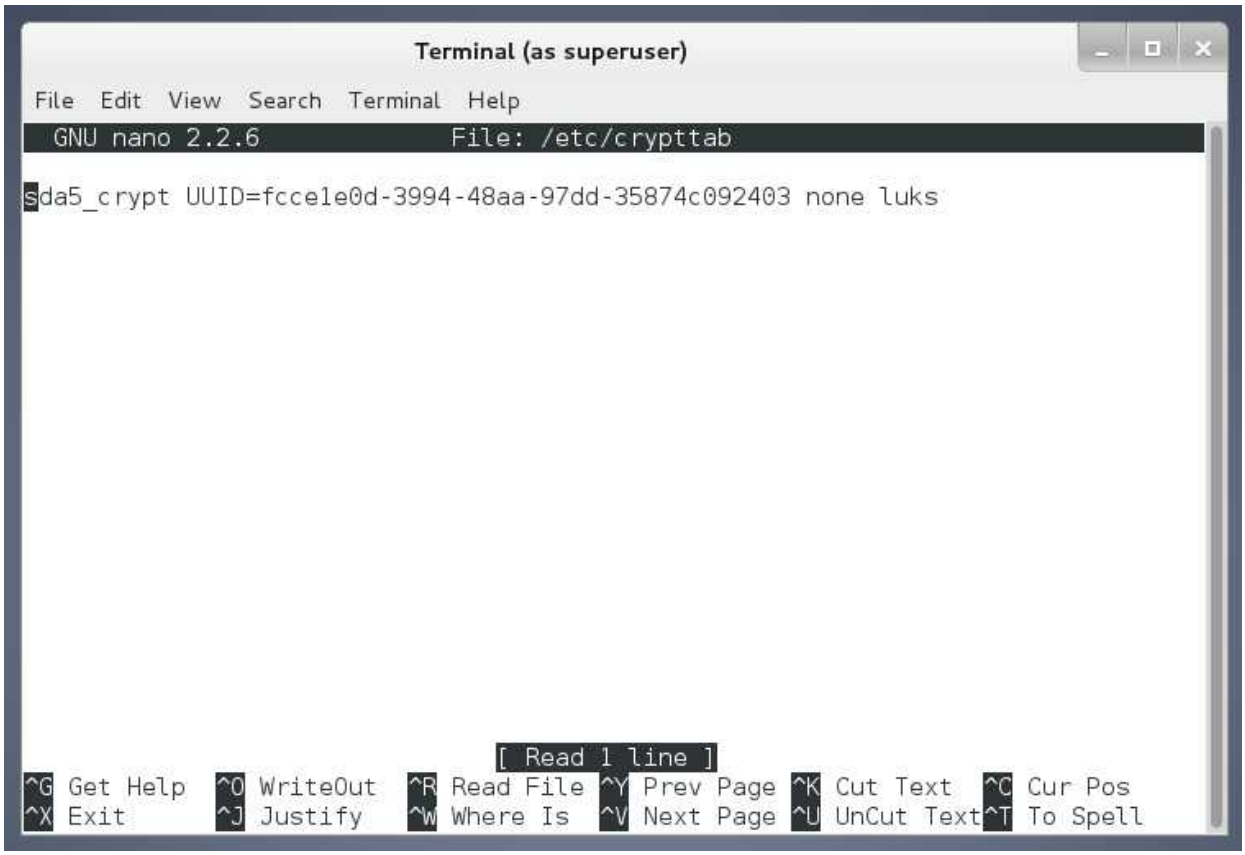
    NOTE: If you wish to use "copy and paste" throughout the guide for any terminal commands in the Debian Host OS, press "**CTRL-SHIFT-V**" to paste what you copied from this guide into a terminal session.



68. When your key file is created, now you can edit your /etc/crypttab file. This is a file that tells Debian how to handle encrypted drives on boot. Type "**nano /etc/crypttab**" in your terminal window.



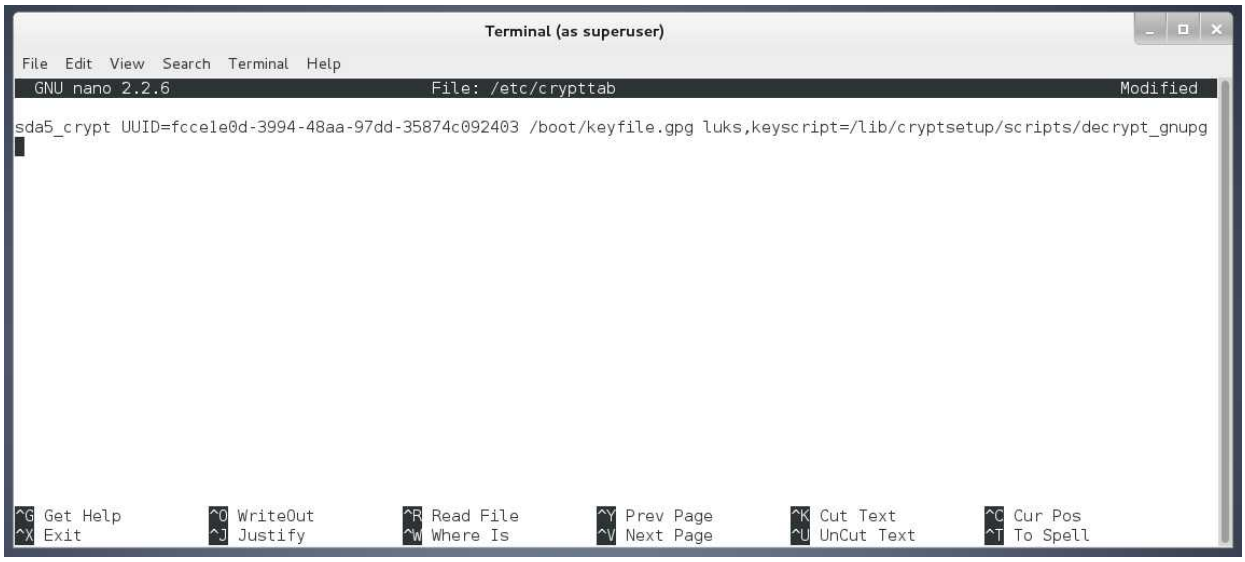
69. Now you need to change the existing line in /etc/crypttab to handle your future encrypted key file. When you open /etc/crypttab, you will see something similar to the screen shot below:



Make note of the section called “sda5_crypt” in the above example. “sda5” is the device name for the encrypted hard drive. It may be something different for your computer (for example, “sda6”). **You will need this information steps in 70 and 81**.

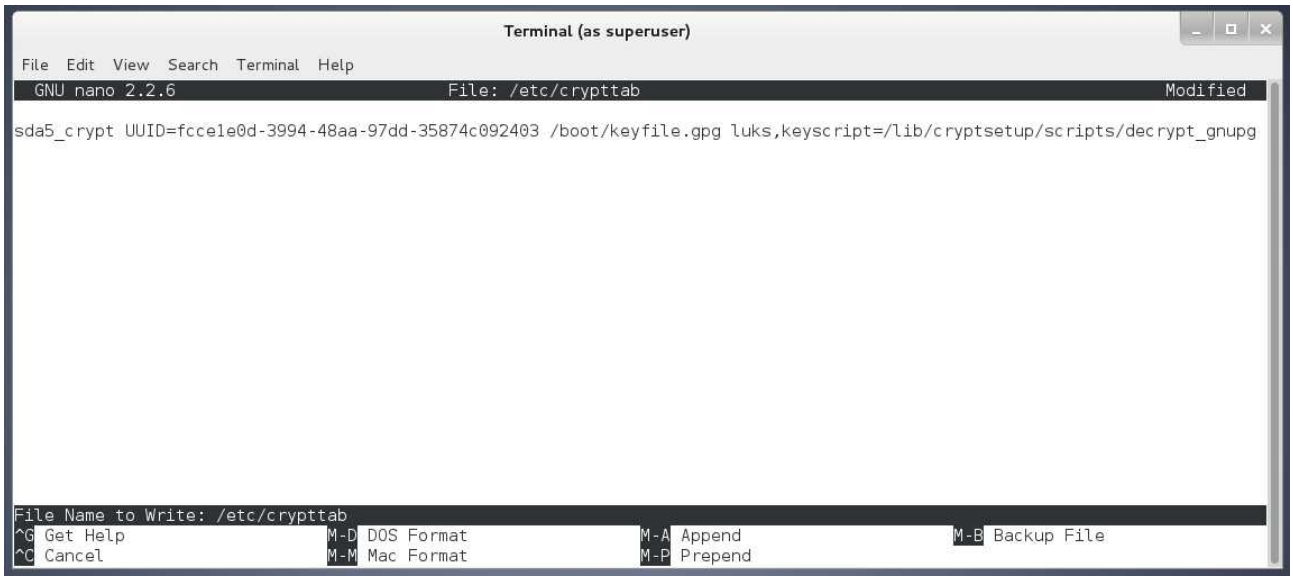
Move the cursor to the far right with your arrow keys and then erase “none luks” with the backspace key. Then add:

/boot/keyfile.gpg luks,keyscript=/lib/cryptsetup/scripts/decrypt_gnupg



Press the “Control” and “X” key at the same time. When prompted to “save modified buffer,” type “y” and press the enter key.

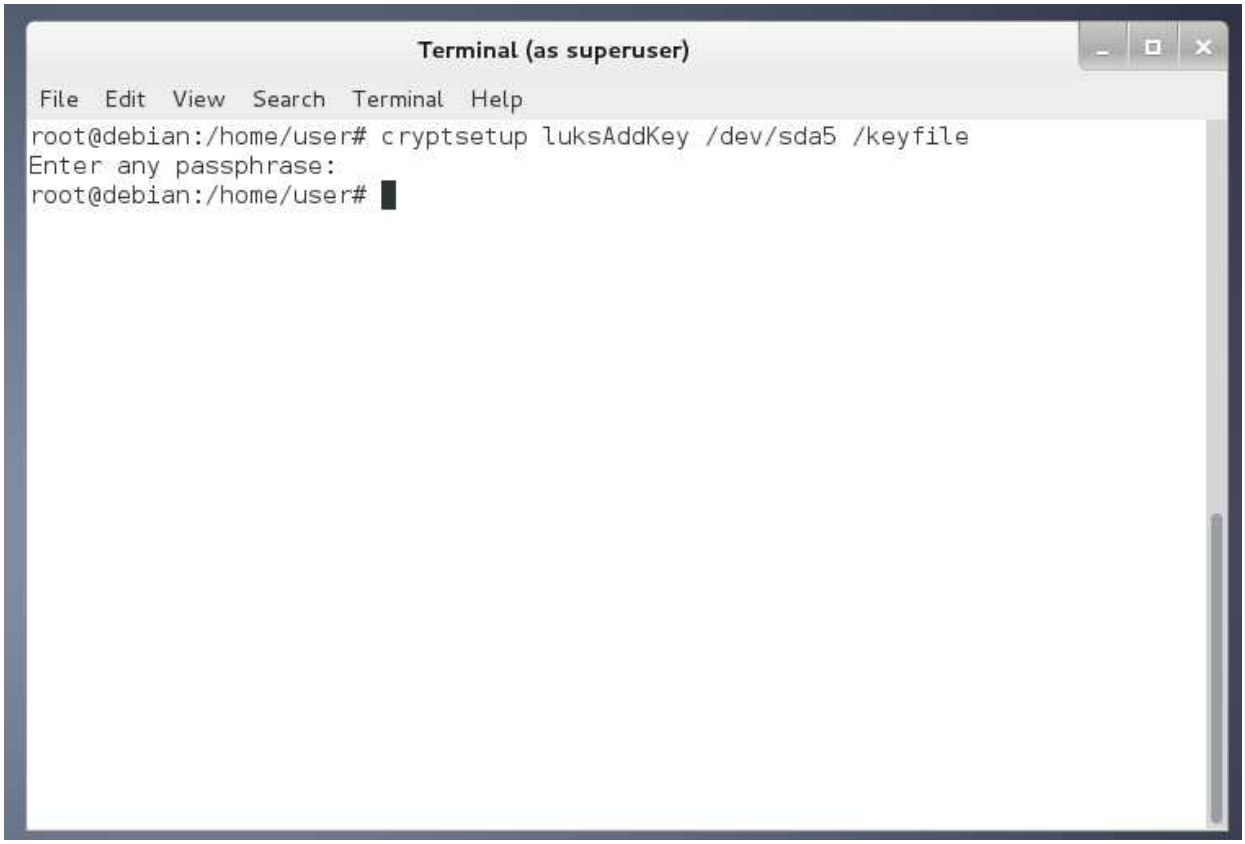
Press “enter” when prompted with “File Name to Write: /etc/crypttab”.



70. Now you need to add your key file to your LUKS keyring. You will need the device name for your encrypted hard drive that I told you to make note of in step 69. In my case, it is "sda5." Type the following in your terminal window and press "enter":

    cryptsetup luksAddKey /dev/*YourDeviceName* /keyfile

    When prompted to "Enter any passphrase," type the passphrase you created for your encrypted hard drive in step 27 of this chapter and press "enter." If the process was a success, you will return to the command prompt.



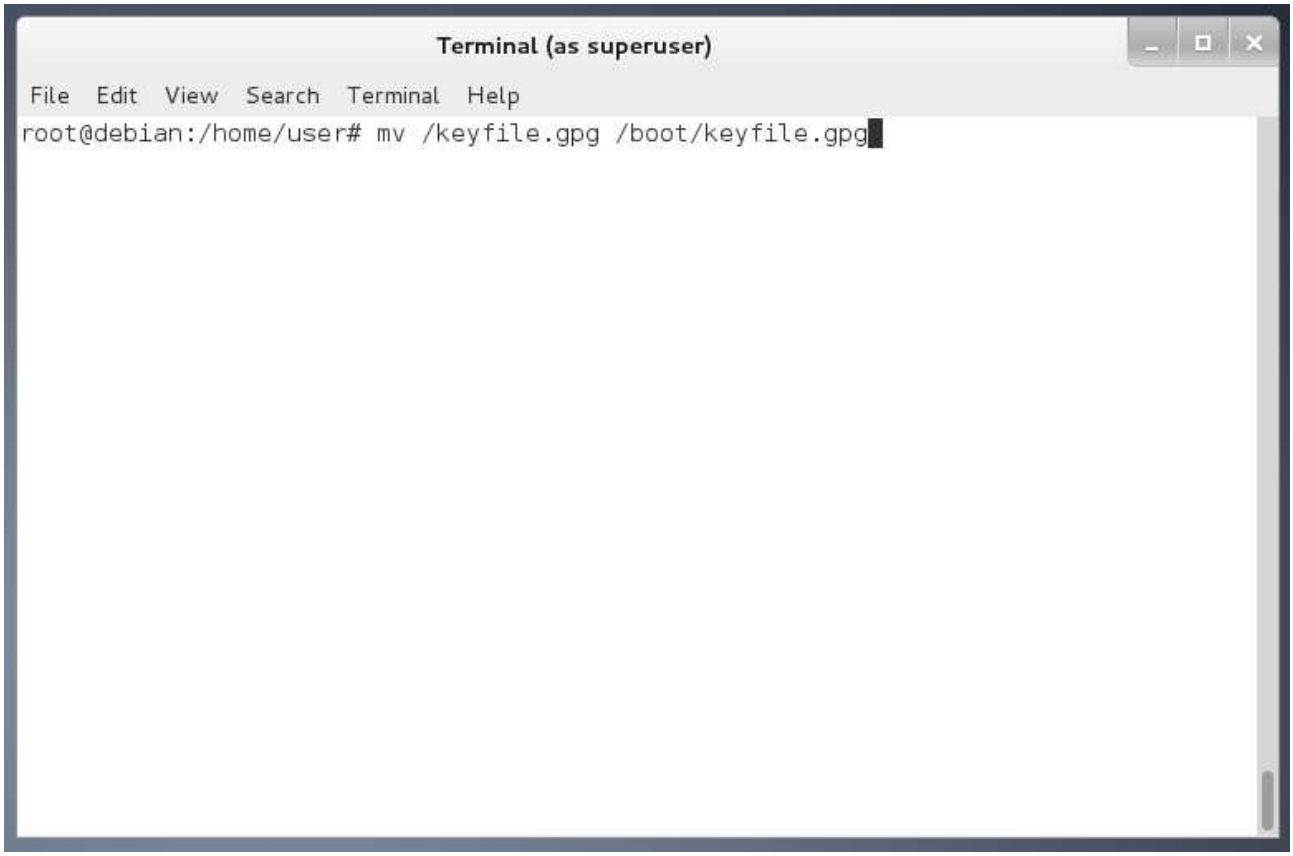
71. Now you need to encrypt your key file with the “gpg” program. Type the following line at your command prompt and press “enter”:

    gpg -c --cipher-algo AES256 /keyfile

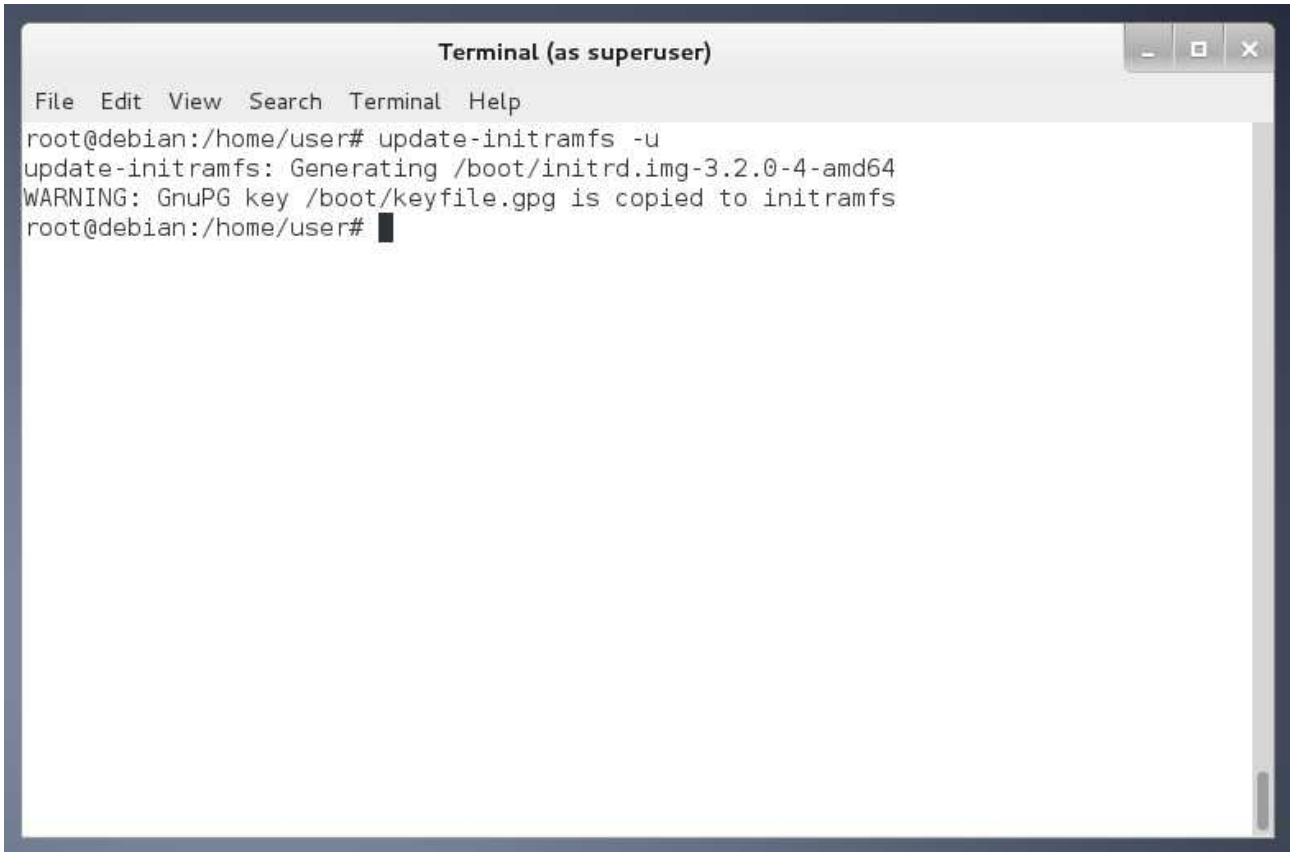
    When prompted to “Enter passphrase,” either use the same passphrase you chose in step 27 of this chapter or create something new that is just as long and random. Retype your passphrase to confirm it when prompted. **This will now be the passphrase you need to enter when you boot up Debian in the future.**

    If all went successfully, you will be returned to a command prompt with no error message.

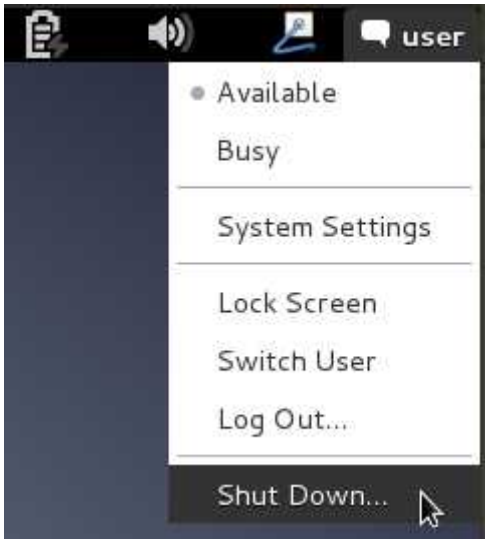
72. Next, type "**mv /keyfile.gpg /boot/keyfile.gpg**"and press "enter." This will move a copy of your encrypted key file to your USB Boot Key if you ever need it in the future.



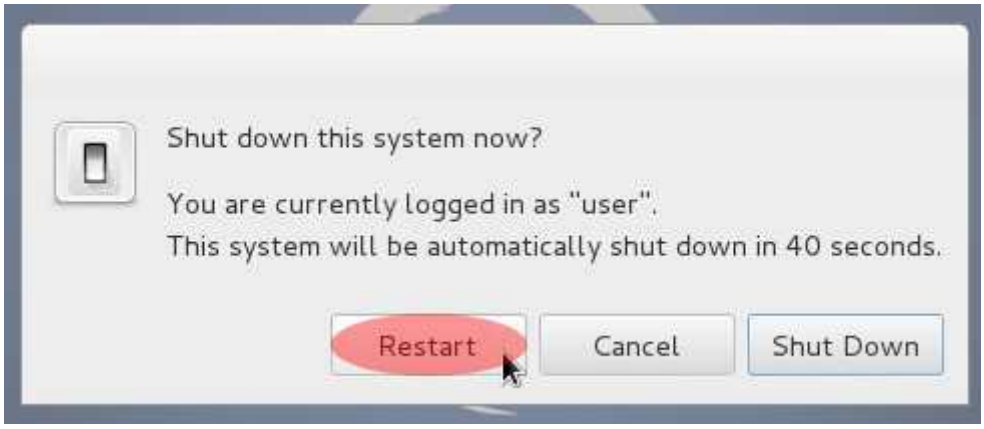
73. Now you need to update your boot process to actually use the encrypted key file. Type "**update-initramfs -u**" and press "enter." If all goes well, you will be returned to a command prompt with no error messages and your screen will look similar to the shot below. Do not worry about the "Warning: GnuPG key /boot/keyfile.gpg is copied to initramfs" message. That is supposed to happen.



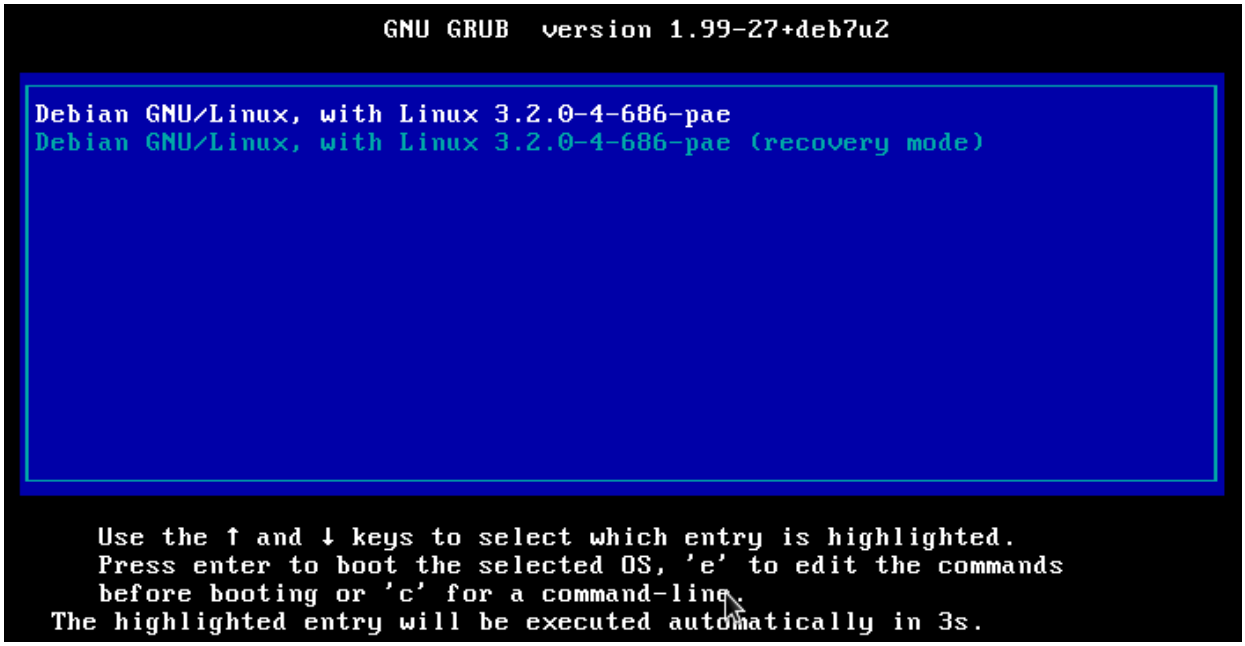
74. Now it is time to restart your computer. Click on “user” in the top right corner of your desktop and select “Shut Down.”



In the window that appears, click on “Restart.”



75. As your computer restarts, you need to get into a boot menu again in the same manner the you did in step 4 of chapter 1. When you activate the boot menu, choose your USB flash drive on which you installed Debian. Eventually, you will be prompted to choose a boot selection. It will default to Debian and, thus, you can either press “enter” or wait for the timer to run out.



76. Eventually you will be prompted to enter your passphrase. Enter the passphrase you chose in step 71 of this chapter and press “enter.”

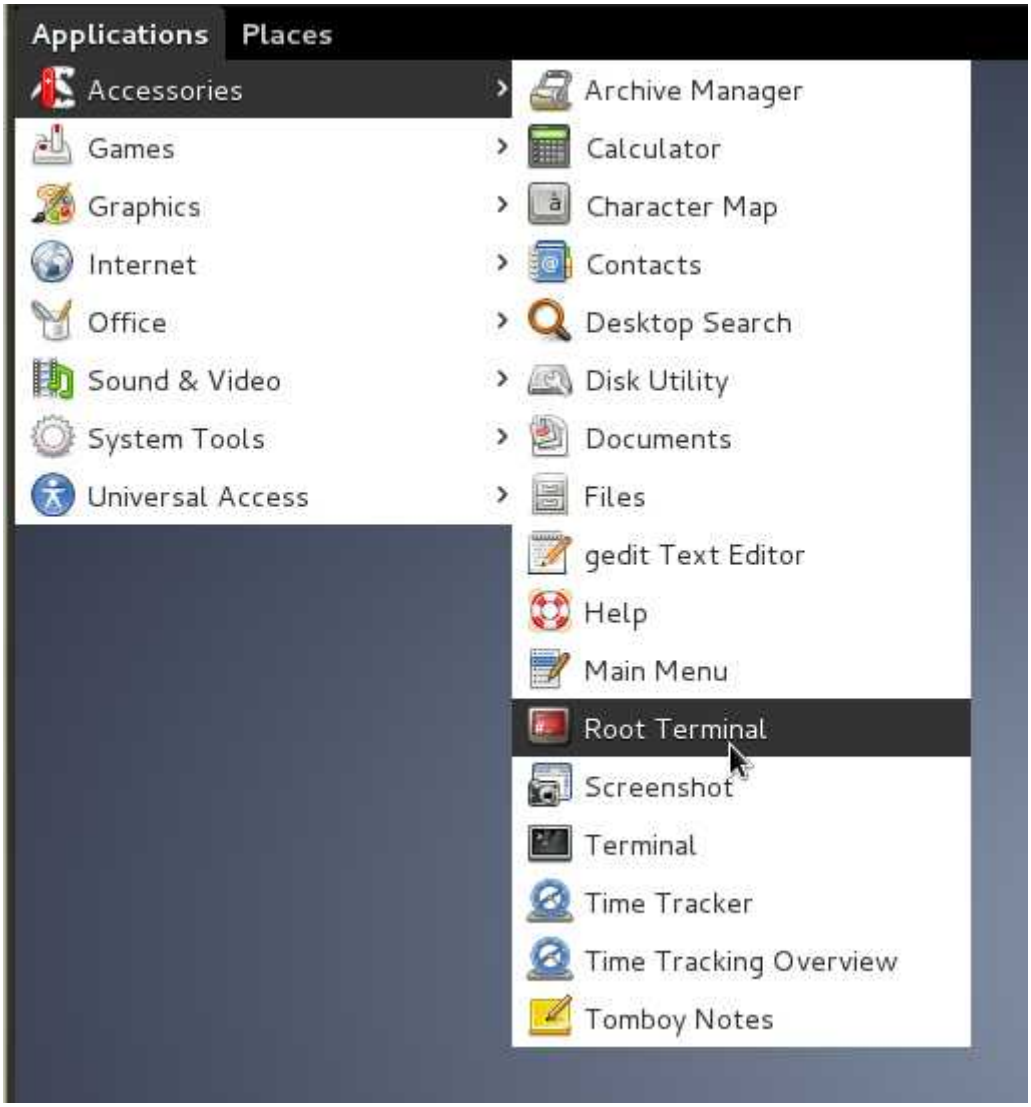
```
  Booting 'Debian GNU/Linux, with Linux 3.2.0-4-amd64'

Loading Linux 3.2.0-4-amd64 ...
Loading initial ramdisk ...
Loading, please wait...
  Volume group "vg" not found
  Skipping volume group vg
Unable to find LVM volume vg/root
Performing GPG key decryption ...
Enter passphrase for key /boot/keyfile.gpg: _
```

77. Debian will now go through its boot process. Eventually you will reach the login window. When you reach the login window, press “enter” or click on “user.”

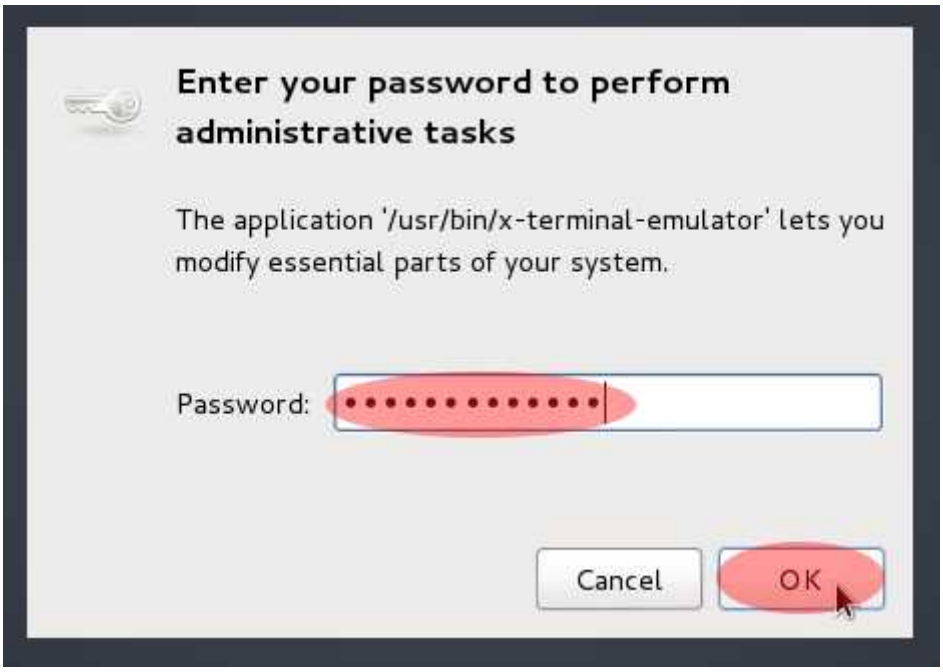
78. On the next screen, you will be prompted for your password. Type the password you created for “user” in step 19 of chapter 1 and press “enter.”

79. When you reach the Debian desktop, click on Applications in the upper right corner, then choose “Accessories → Root Terminal.”

    NOTE: Whenever you use this command, **you will have full root/administrative access until you “exit” the session.** Thus, **be extra cautious** in your session whenever you decide to use this command. **The changes you make can be damaging and permanent if you do something wrong.**



80. You will next be prompted to enter your password to perform administrative tasks. This is the same password you chose for “user” in step 19 of chapter 1. Type your password and click “ok.”



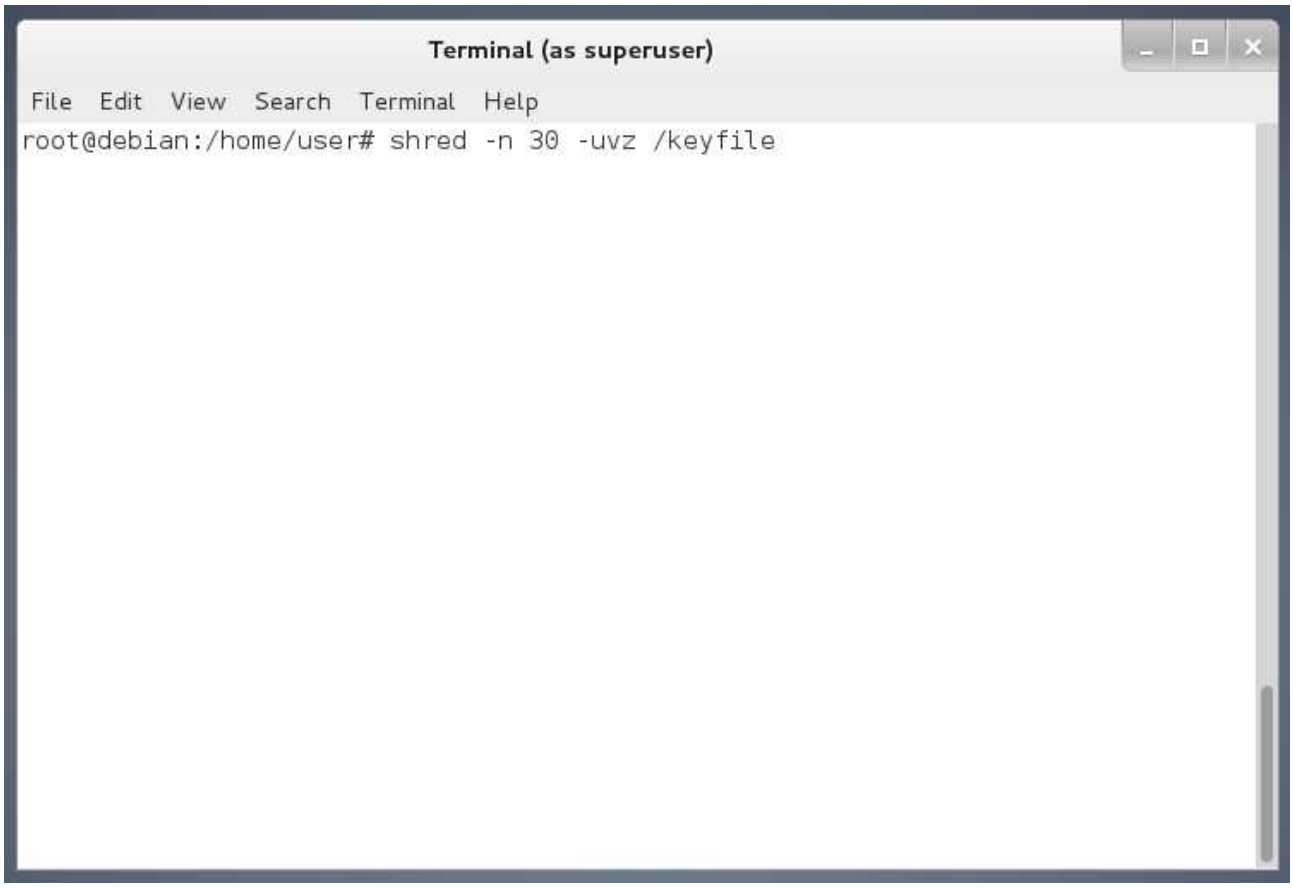
81. Next, you need to remove the initial passphrase you created for your encrypted hard drive partition in step 27 of this chapter. The LUKS encryption system uses what is called a keyring. At this point, you have two keys in your keyring: one containing the passphrase you chose when installing Debian in step 27 of this chapter and one containing the key file you created and added to the keyring in steps 67-73 of this chapter.

    Removing the passphrase you created in step 27 will make it so that your key file is the only means to unlock your encrypted hard drive. This provides strong security since you will never know the contents of the key file. As a human, it's unlikely that you could remember 4096 bytes of random characters. Thus, if you lose or destroy your USB flash drive boot key, the data on your hard drive is irrecoverable. **You will need the device name for your encrypted hard drive that I told you to make note of in step 69**. In my case, it is "sda5." Type the following and press "enter":

    cryptsetup luksKillSlot /dev/*YourDeviceName* 0 --key-file /keyfile

    If the process is successful, you will be returned to a command prompt with no error message.

82. Now it is time to securely remove your unencrypted key file from your hard drive. This further minimizes the risk of a potential attacker ever discovering it. If you ever need access to your unencrypted key file in the future, remember that you have an encrypted version of it stored on your boot key as “keyfile.gpg.” Type “**shred -n 30 -uvz /keyfile**” and press “enter.” When the process is over, type “exit” and press the “enter” key, or click on the “x” in the upper right corner to c lose the window.



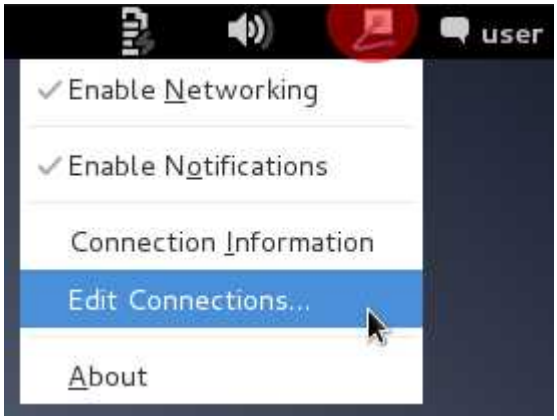
Congratulations! You have finished up the lengthy process of installing Debian onto an encrypted hard drive with a secure USB boot key. Continue on to the next chapter for the final steps of installing Debian and Whonix.

Chapter 3. Final Debian Tweaks and Whonix Installation

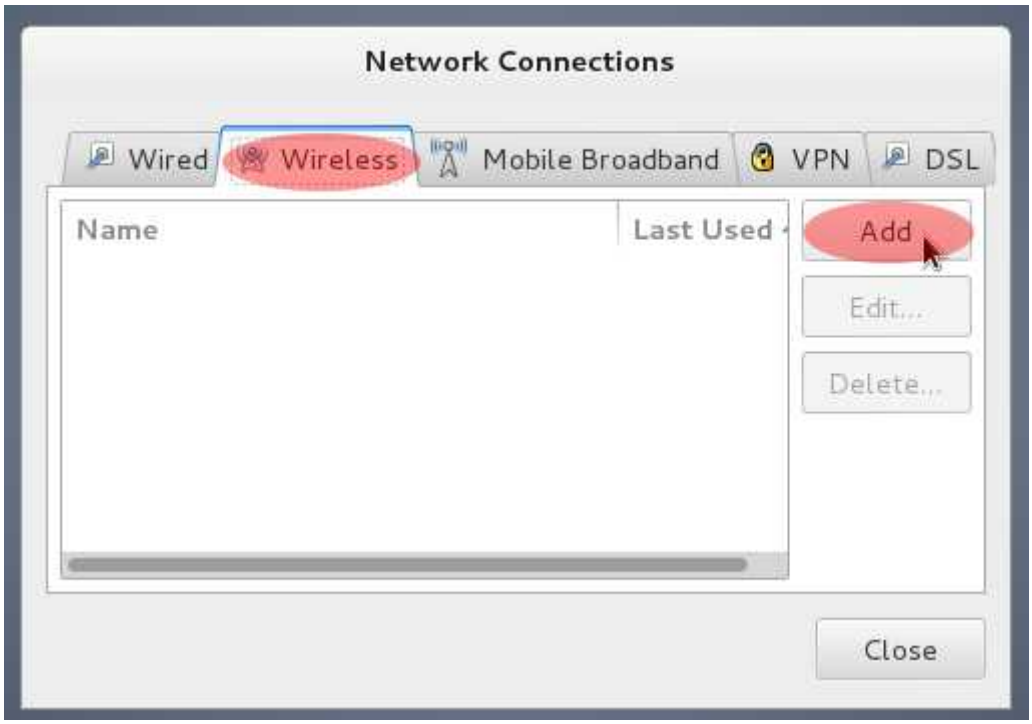
You are almost done with the Debian install! There are now only a few more steps you need to take. If you desire, you can take a break here and start from this chapter at another time. But, if you're ready to go, let's get started.

1. First, let's set up your networking connection. It is ideal to use a wired network connection for security reasons. If you left your wired connection plugged in, Debian's network manager should automatically detect it and connect to the Internet. **If you prefer to remain using a wired connection only, you can skip to Step 5.** But, if you prefer to use a wireless connection, or if you used one during the initial install in chapters 1 and 2, do a right-click (or Control-Key + Click if on a Mac) on the Gnome Network Manager icon in the upper right hand corner. The Gnome Network Manager icon will look like either of the following icons:

Then, click on “Edit Connections.”

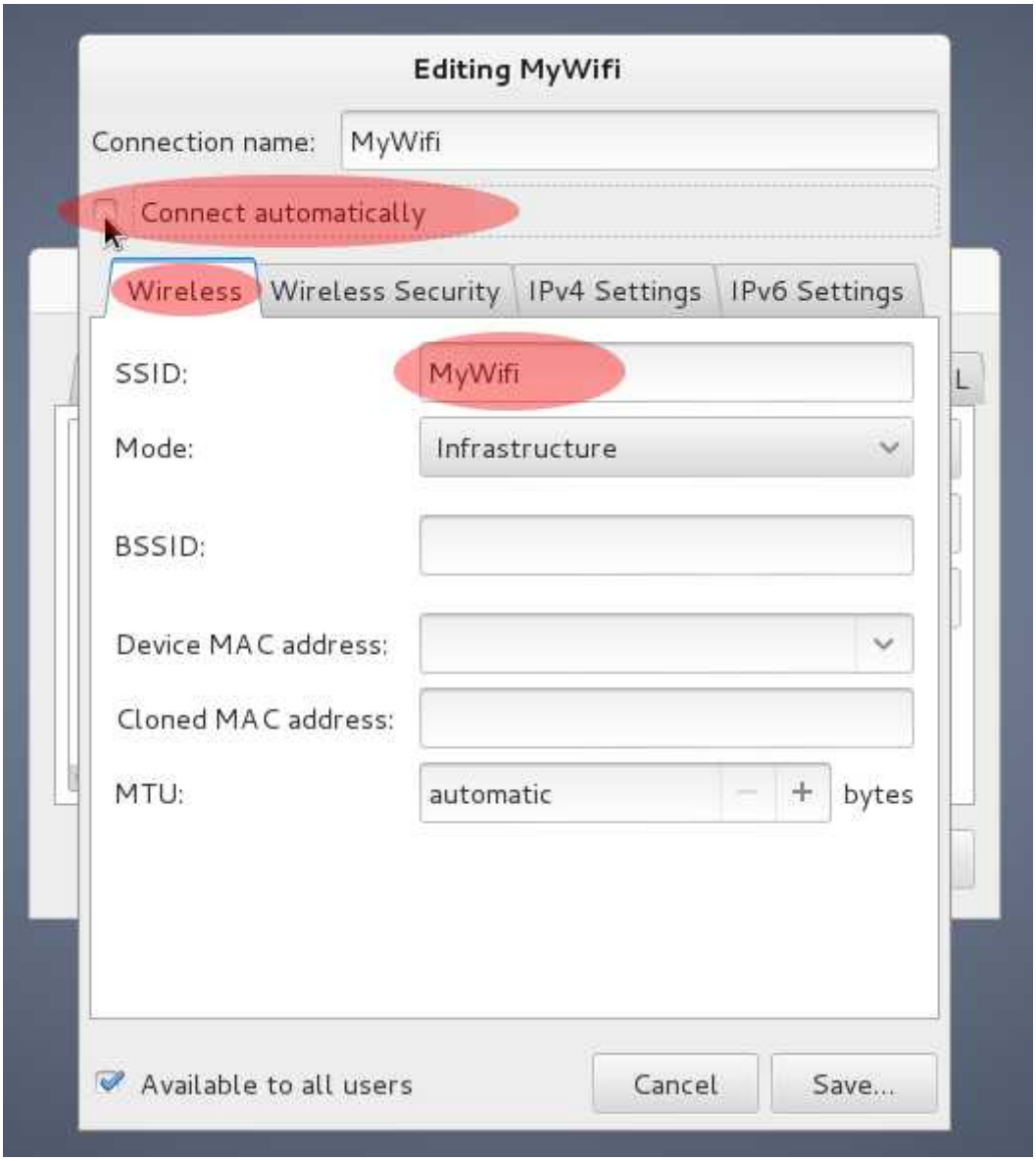


2. When the Network Manager window appears, click on the “Wireless” tab and click “add.” **If you configured a wireless connection during the install phase, click on your existing wireless connection and select “edit.”**



3. If you are setting up your wireless connection for the first time, type the name for your wireless connection in the spaces next to “connection name” and “SSID.” Then, uncheck the checked box next to “connect automatically.” Allowing your computer to automatically connect to your wireless connection opens up an opportunity for an attacker to compromise your security.

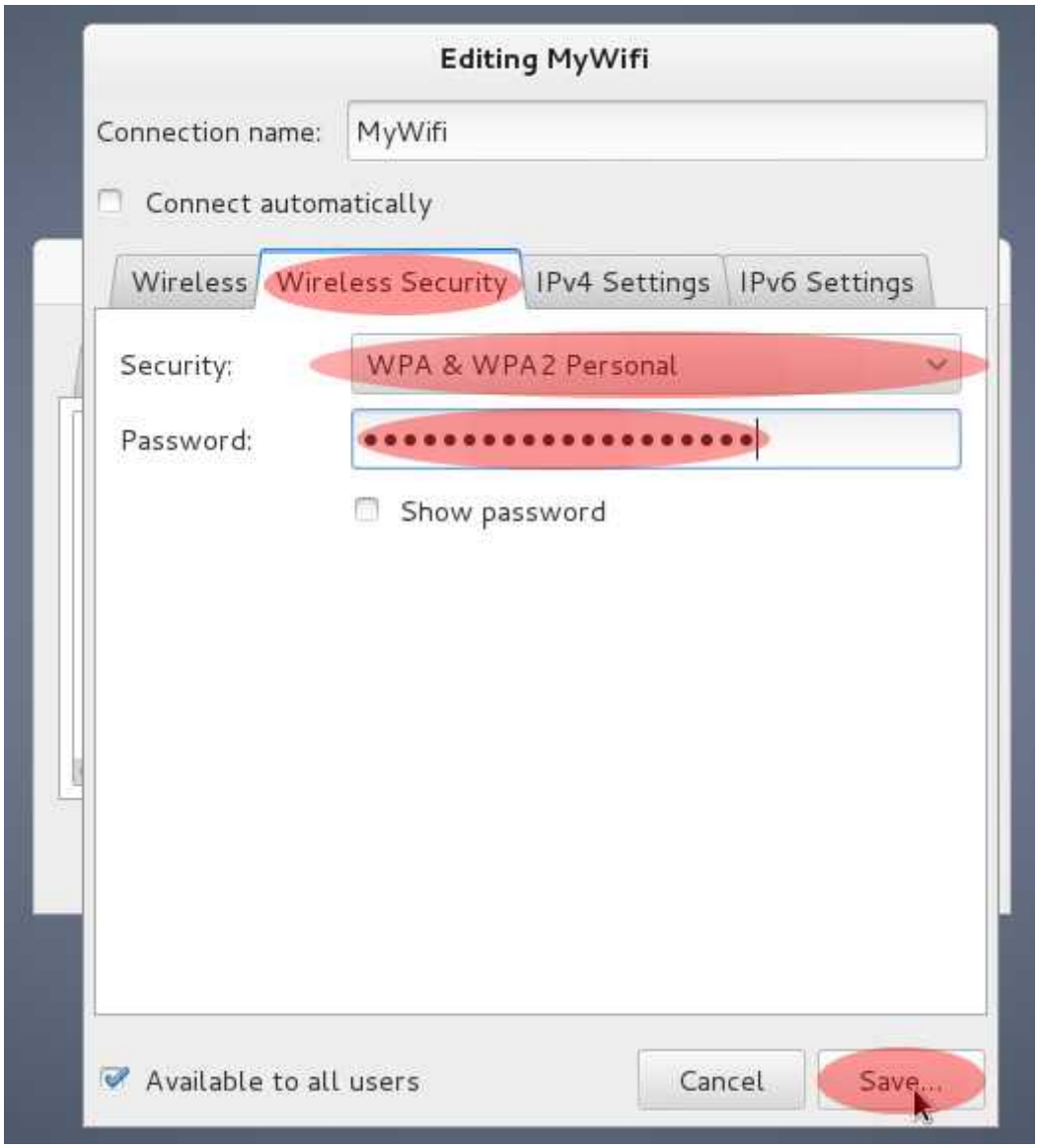
   If you are editing an existing connection, uncheck the checked box next to “connect automatically,” click “save,” close the Connection Manager window and continue to step 5.



4. Next, click on the “Wireless Security” tab. Select “WPA & WPA2 Personal” for “Security.” Then type the password for your wireless router in the “Password” field. Then click “Save.”

   If your router is still configured to use WEP for security, you should change it immediately. WEP is notoriously insecure and can often be cracked in less than 1 minute.

   When this process is finished, click the “X” in the upper corner of the Gnome Network Manager at the main screen to close the window. To connect to your wireless connection now and in the future, simply click on the Gnome Network Manager icon in the upper right corner and choose the network profile you created.



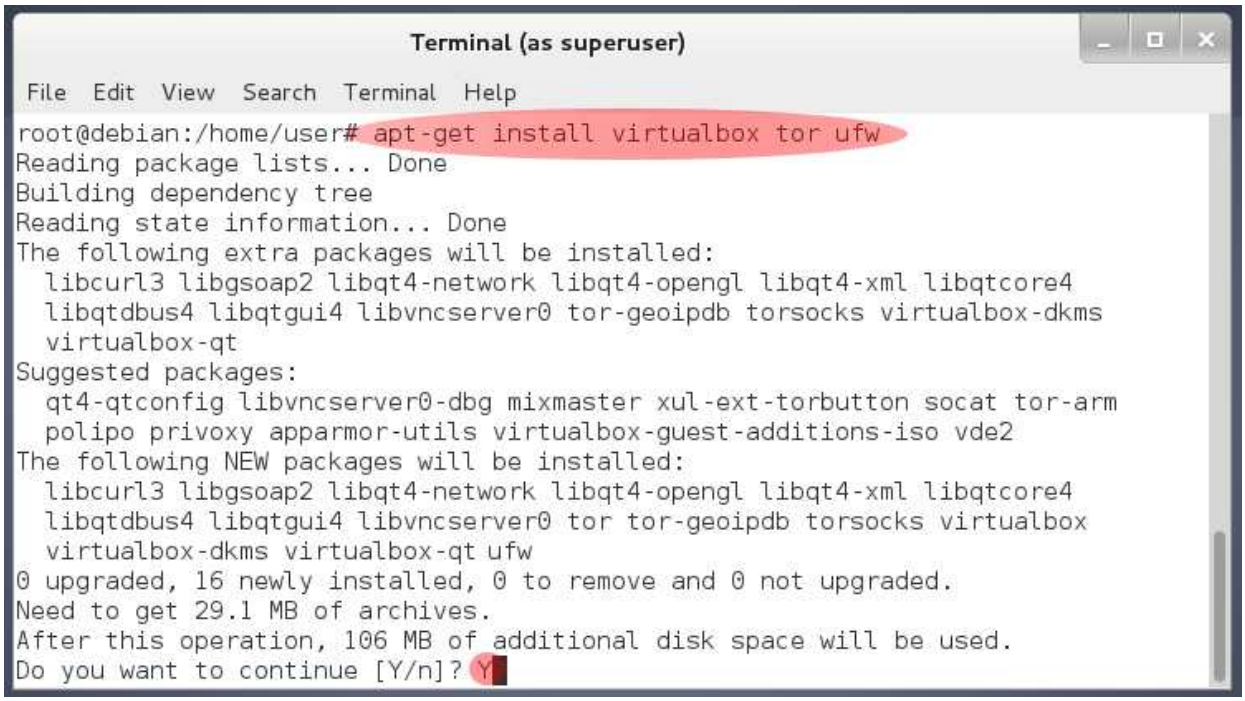
5. Next, click on “Applications” in the upper left hand corner of your desktop and select “Accessories → Terminal.”

6. Next, you need to give yourself root/administrative privileges to install additional software. Type "**sudo -i**" at the command prompt. When prompted for your password, type the same password you chose for "user" in step 19 of chapter 1.

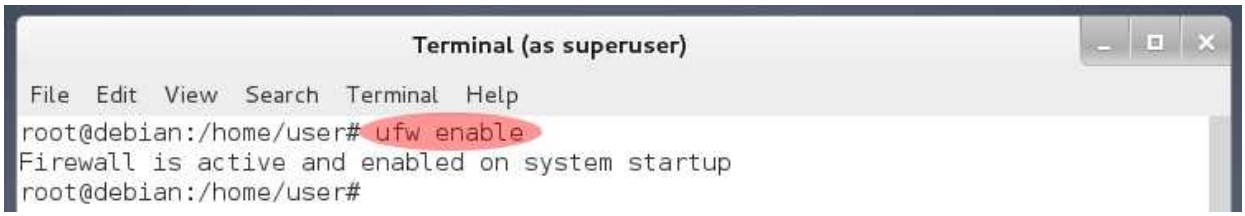
   NOTE: Whenever you use this command from a terminal session, **you will have full root/administrative access until you "exit" the session.** Thus, **be extra cautious** in your session whenever you decide to use this command. **The changes you make can be damaging and permanent if you do something wrong.**

   ADDTIONAL NOTE: If you wish to use "copy and paste" throughout the guide for any terminal commands in the Debian Host OS, press "**CTRL-SHIFT-V**" to paste what you copied from this guide into a terminal session.

7. Now you need to install VirtualBox, Tor and ufw. VirtualBox is the software that will run the Whonix virtual machines. Tor is a strong anonymizing proxy service that will enable you to download Whonix anonymously. Ufw is a software that will configure firewall rules for your OS. At the command prompt, type "**apt-get install virtualbox tor ufw**" and press "enter." When asked if "you wish to continue," type "**Y**" and press "enter."



8. Next, enable your firewall. Type "**ufw enable**" at the command prompt and press "enter." UFW should inform you that it is active. It will remain active through every reboot.



After you have enabled ufw, **you need to "exit" your root/administrative privileges.** Type "**exit**" at the command prompt and continue to the next step.

9. Next, type "**cd Downloads**" to change your directory to the Downloads directory. You are going to download all of the Whonix related files here.

10. Now you are going to download the Whonix-Gateway virtual machine. You will use a program called “wget” to download the file. If the connection gets interrupted for any reason, using the following command will continue downloading the Whonix-Gateway anonymously over the Tor Network from where you left off. Type “**torsocks wget -c http://mirror.whonix.de/9.6/Whonix-Gateway-9.6.ova**”and press “Enter.”

11. When you have successfully downloaded the Whonix-Gateway, it is time to download the Whonix-Workstation. Type “**torsocks wget -c http://mirror.whonix.de/9.6/Whonix-Workstation-9.6.ova**” and press “enter.”

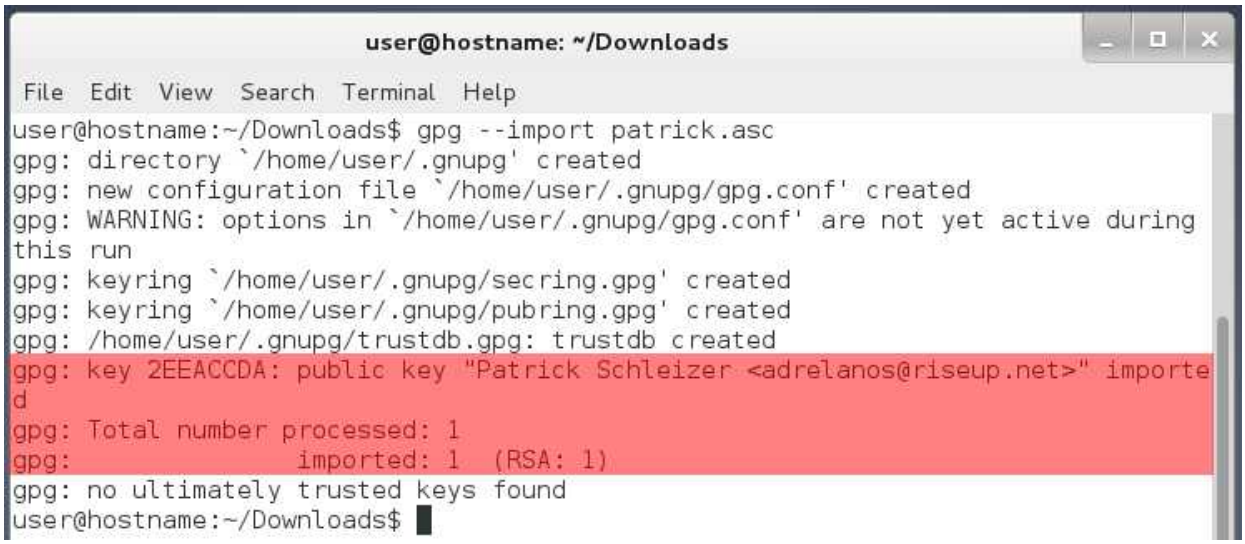
12. Now, download the verification signatures for the Whonix virtual machines. The verification signatures will allow you to test if the virtual machines have been tampered with. First, download the Whonix Gateway OpenPGP Signature. Type “**torsocks wget -c https://www.whonix.org/download/9.6/Whonix-Gateway-9.6.ova.asc**” and press “enter.”

13. Next, download the Whonix Workstation OpenPGP Signature. Type “**torsocks wget -c https://www.whonix.org/download/9.6/Whonix-Workstation-9.6.ova.asc**” and press “enter.”

14. Now, download the Whonix Signing Key. Type "**torsocks wget -c https://www.whonix.org/patrick.asc**" and press "enter."

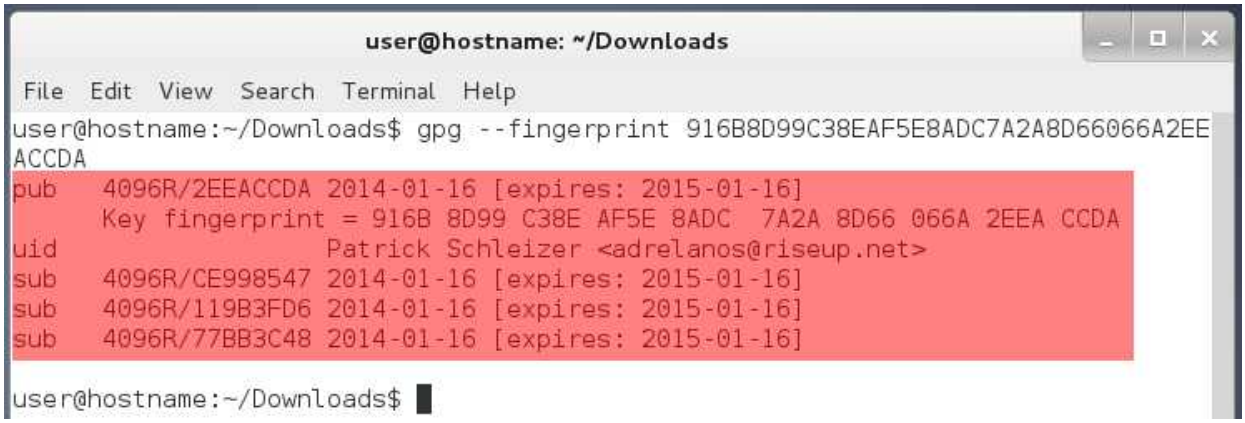
15. Now, import the developer's signature key by typing "**gpg --import patrick.asc**" and pressing "enter."

When finished, your screen should look similar to the one below. You may see some various errors or warnings. None of these are usually of any significance and will likely relate to the fact that you haven't used GPG to create your own key yet. The output of importance to you is highlighted in red below.



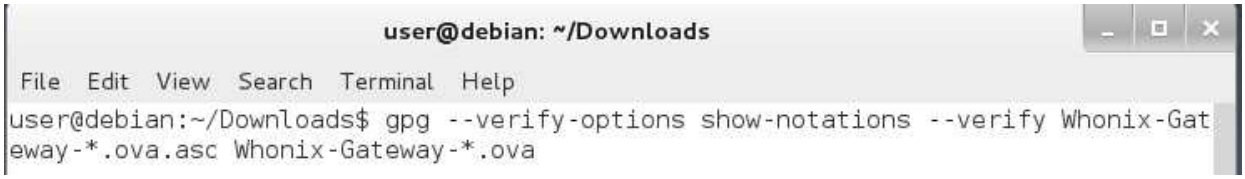
16. Next, verify the signature key using its fingerprint. Type "**gpg --fingerprint 916B8D99C38EAF5E8ADC7A2A8D66066A2EEACCDA**" and press "enter."

When finished, your screen should look the same as the one below. If it does not, you may have a bad signature. Download it again as described in step 14.

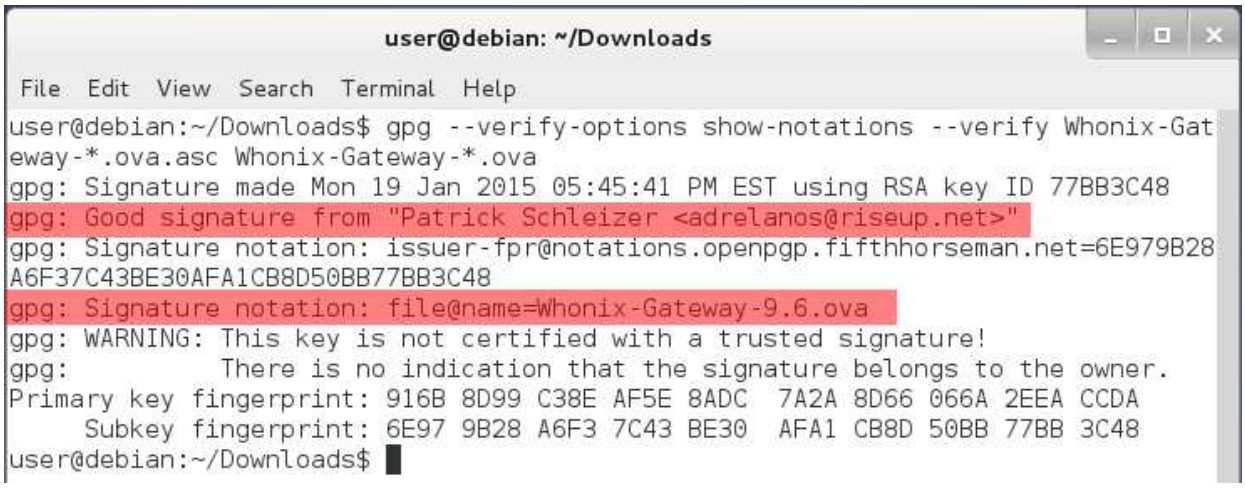


17. Next, test the integrity of Whonix-Gateway-9.6.ova by typing:

    "**gpg --verify-options show-notations --verify Whonix-Gateway-*.ova.asc Whonix-Gateway-*.ova**" and then press "enter." This may take a short while.



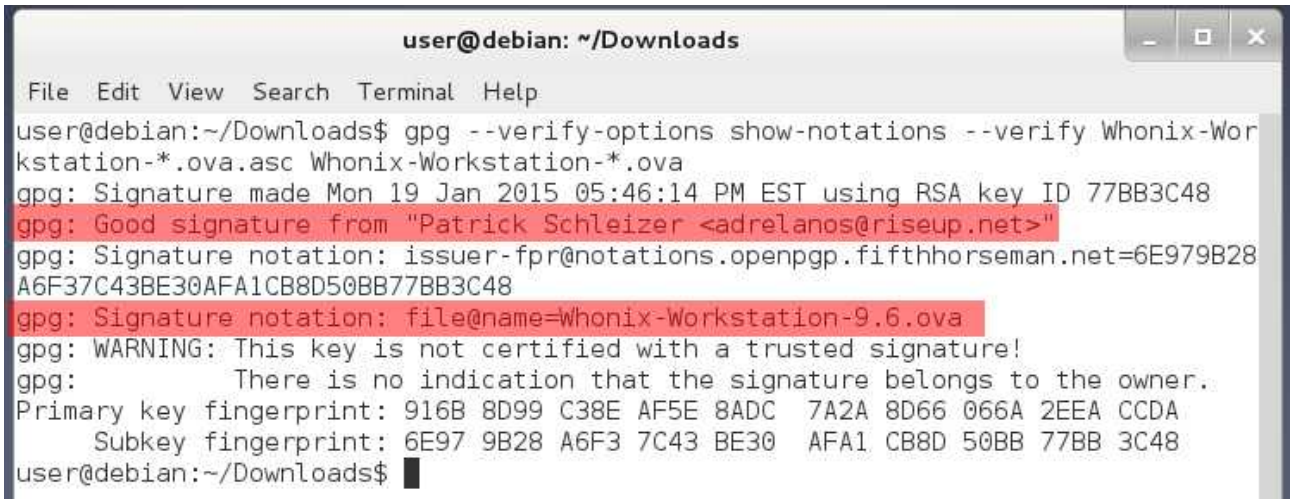
    When the verification is done, your screen should look similar to the screen shot below. If you see "**gpg: Good signature from "Patrick Schleizer <adrelanos@riseup.net>**"" and "**gpg: Signature notation: file@name=Whonix-Gateway-9.6.ova**" on your screen, then you have successfully verified the integrity of the image. The warnings that appear after that line can be ignored. **However, if you see "gpg: BAD signature from "Patrick Schleizer <adrelanos@riseup.net>"" or a file@name that is different than "Whonix-Gateway-9.6.ova" on your screen, delete the image and do not use it.** This means the image has probably been tampered with or got corrupted during the download process. Try downloading the image again at a later time.



18. Now, test the integrity of Whonix-Workstation-9.6.ova by typing:

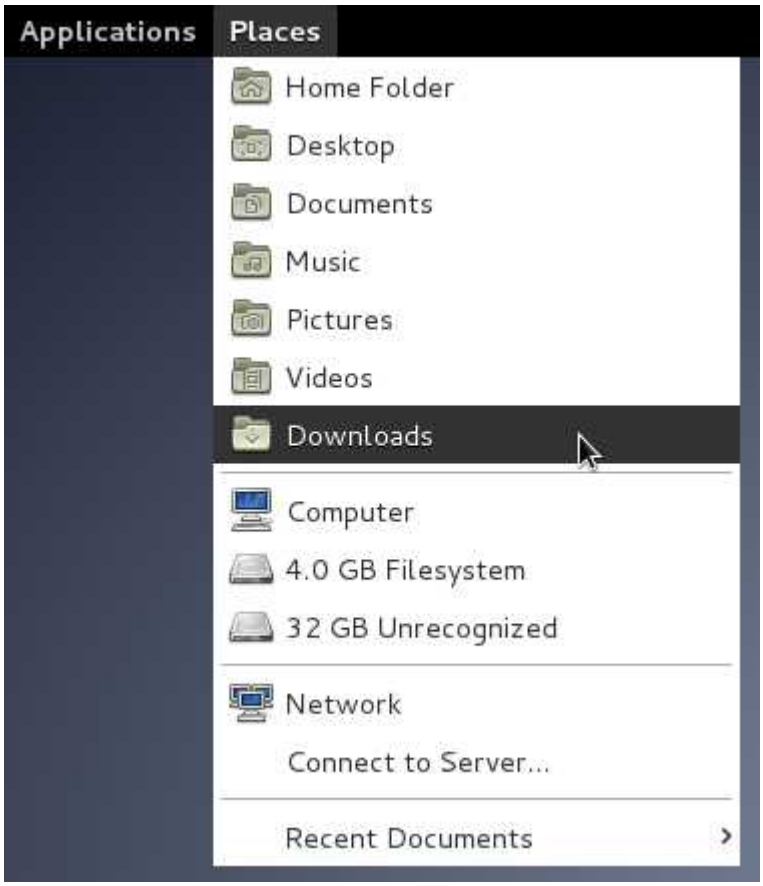
    "**gpg --verify-options show-notations --verify Whonix-Workstation-*.ova.asc Whonix-Workstation-*.ova**" and then press "enter." This may take a short while.

    When the verification is done, your screen should look similar to the screen shot below. If you see "**gpg: Good signature from "Patrick Schleizer <adrelanos@riseup.net>""** and **"gpg: Signature notation: file@name=Whonix-Workstation-9.6.ova**" on your screen, then you have successfully verified the integrity of the image. The warnings that appear after that line can be ignored. **However, if you see "gpg: BAD signature from "Patrick Schleizer <adrelanos@riseup.net>"" or a file@name that is different than "Whonix-Workstation-9.6.ova" on your screen, delete the image and do not use it.** This means the image has probably been tampered with or got corrupted during the download process. Try downloading the image again at a later time.



When this step is over, type "**exit**" and press "enter" or click on the "x" in the upper right corner when this step is done. You will not need the terminal again.

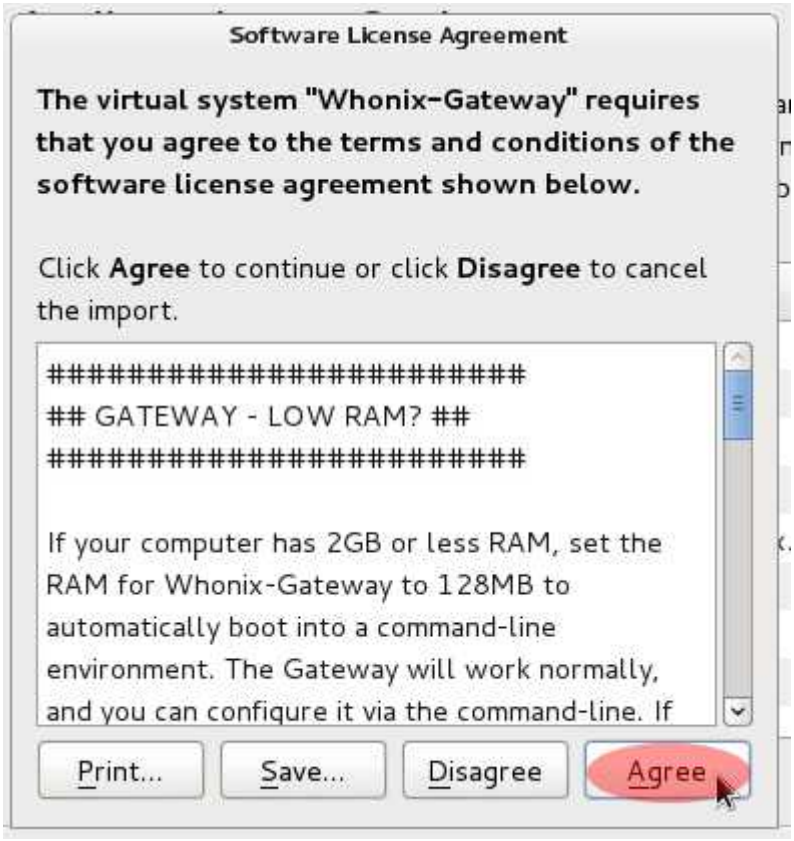
19. Now it's time to import the Whonix images into VirtualBox. Click on “Places” in your upper left hand screen and select “Downloads.”



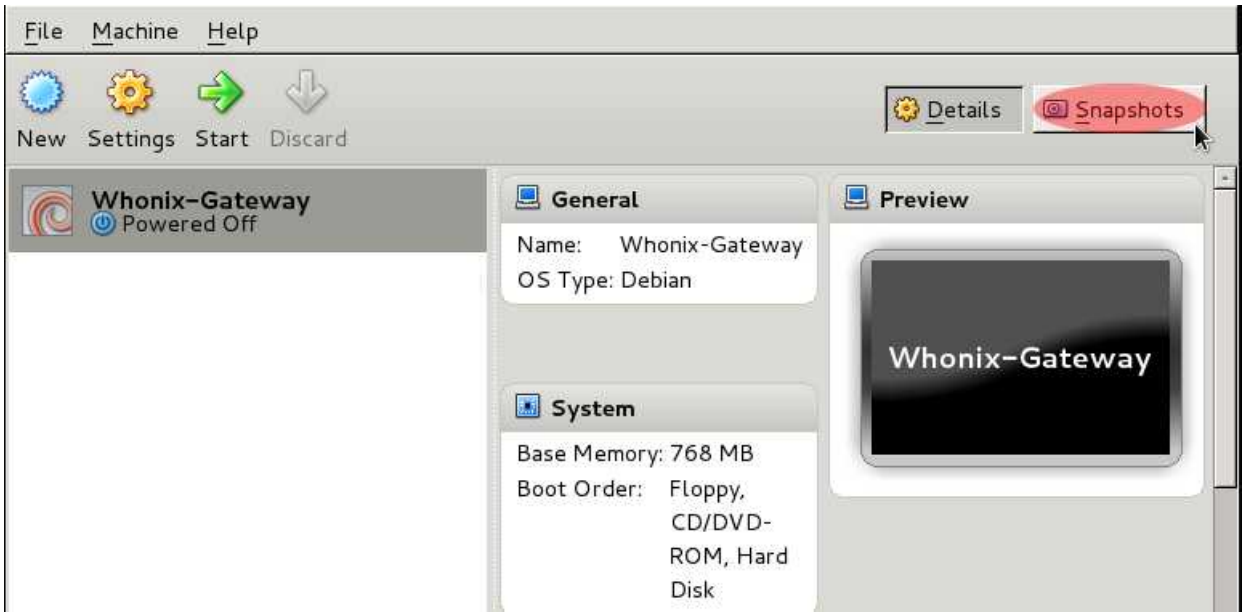
20. In the window that appears, double click on the file named “Whonix-Gateway-9.6.ova.”

21. VirtualBox will now open automatically. Eventually, it will open then “Appliance Import Wizard.” Click on “Import.”

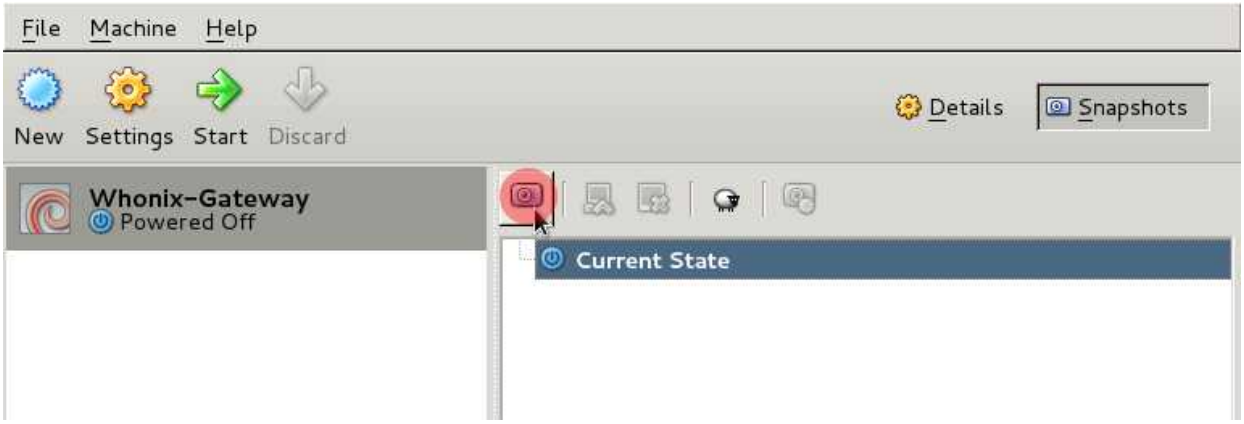
22. A “Software License Agreement” window will pop up informing you of various information, including what to do if you intend to run the Whonix Gateway on low RAM systems. Click “Agree” to continue.



23. When the import process is complete, make a snapshot of the Whonix Gateway virtual machine. This will provide you with an easy back up to restore from in case your virtual machine ever has problems. Click on the button that says “Snapshots” in the upper right corner of the VirtualBox Manager.



24. Click on the icon that looks like a camera located above “Current State.”



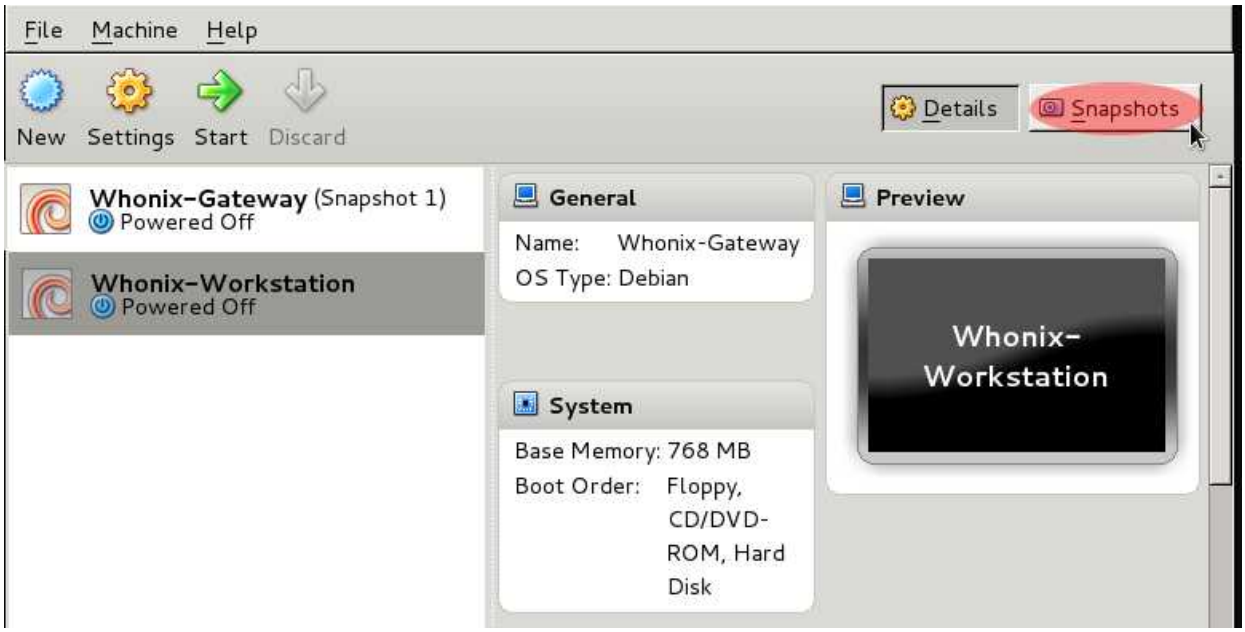
25. A window will pop up entitled “Take a Snapshot of Virtual Machine.” Choose an appropriate label for your snapshot, or just accept the default, and click “OK.”

26. Close the “VirtualBox Manager” and go back to the window displaying your Downloads Folder. It is now time to install the Whonix Workstation. Double click on “Whonix-Workstation-9.6.ova.”

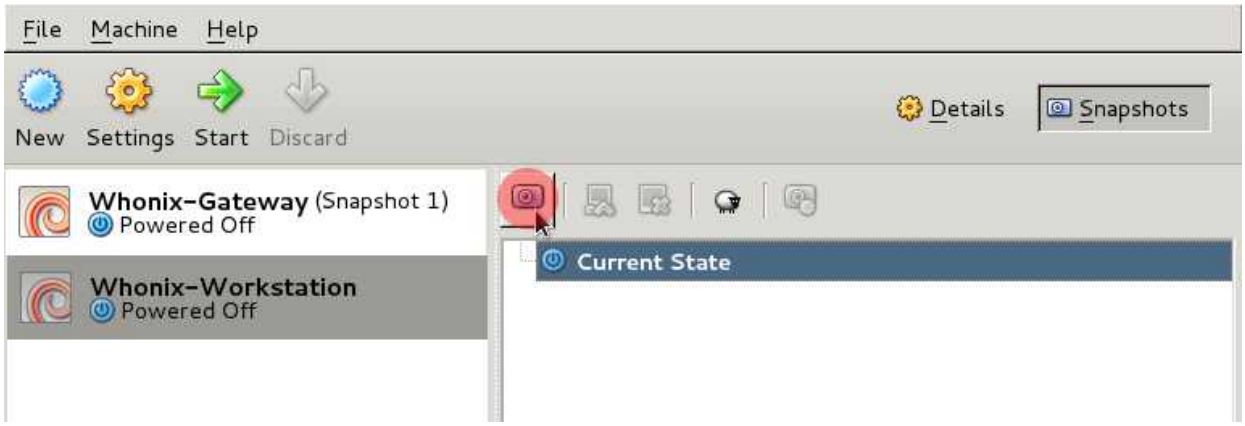
27. VirtualBox will now open automatically. Eventually, it will open then “Appliance Import Wizard.” Click on “Import.”

28. A “Software License Agreement” window will pop up informing you of various information, including what to do if you intend to run the Whonix Gateway on low RAM systems. Click “Agree” to continue.

29. When the import process is complete, make a snapshot of the Whonix Workstation virtual machine. This will provide you with an easy back up to restore from in case your virtual machine ever has problems. Click on “Whonix-WorkStation” and then click on the button that says “Snapshots” in the upper right corner of the VirtualBox Manager.

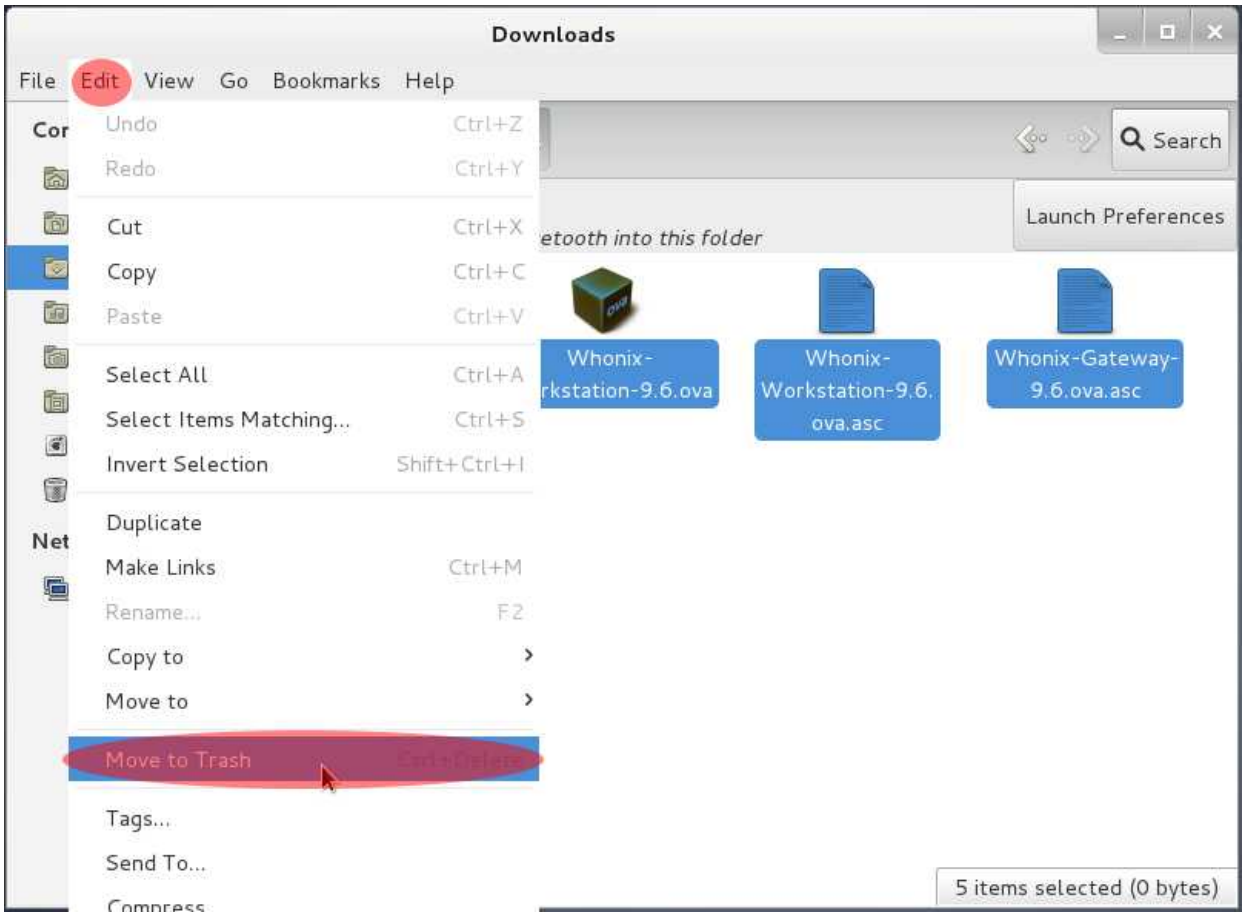


30. Click on the icon that looks like a camera located above “Current State.”

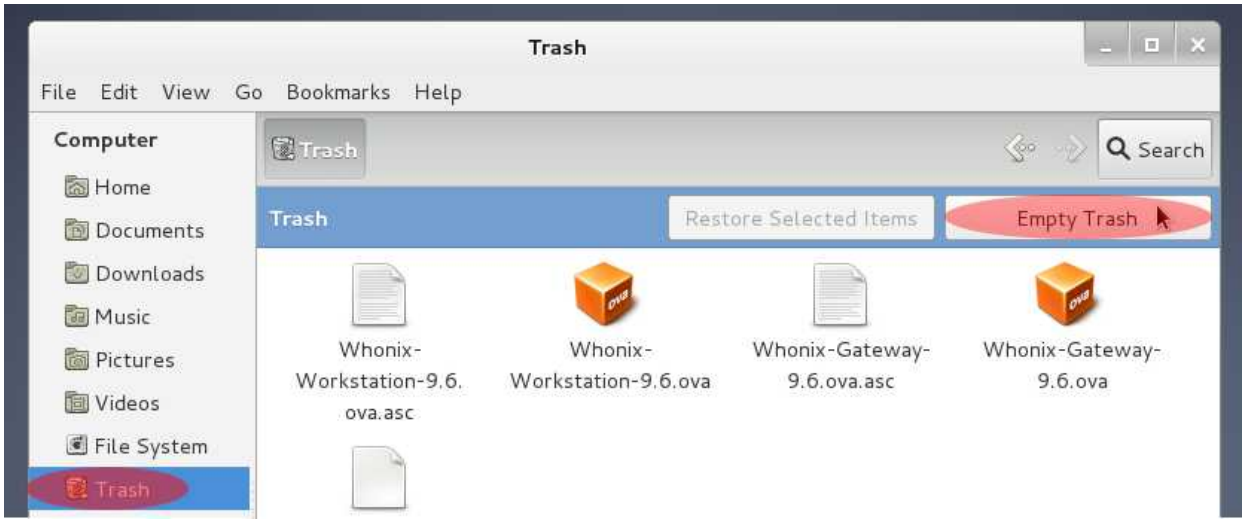


31. A window will pop up entitled “Take a Snapshot of Virtual Machine.” Choose an appropriate label for your snapshot, or just accept the default, and click “OK.”

32. To conserve space, you can now delete the Whonix files you downloaded. Go back to your “Downloads Folder” window and select all the files. Then, click on the “Edit” menu in the upper left area of the window and choose “Move to Trash.”



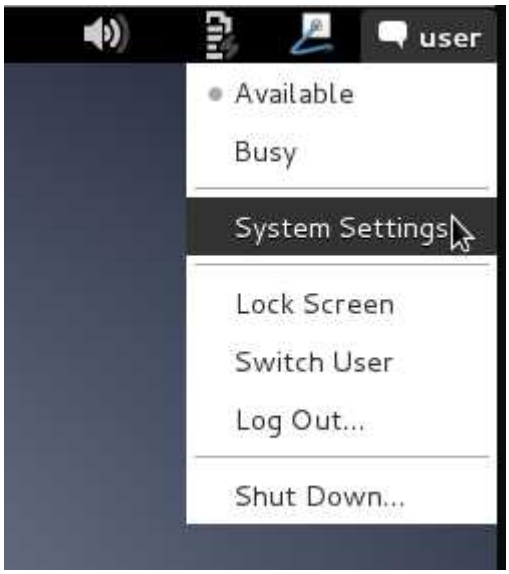
33. Next, click on the “Trash” icon towards the lower left side of the “Downloads Folder” window and click “Empty Trash.”



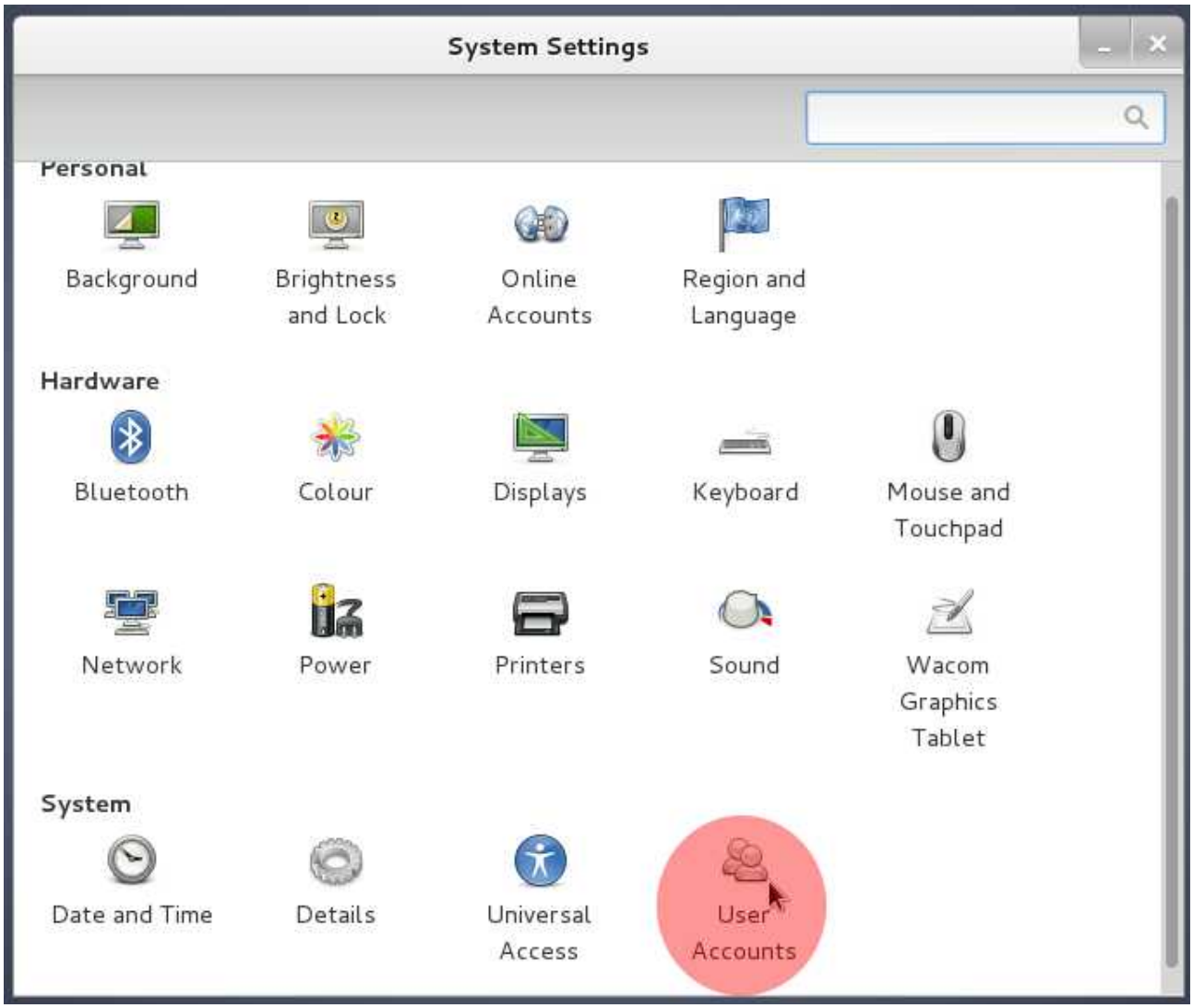
34. When asked if you wish to “empty all items from Trash, “click on “Empty Trash.” This will free roughly 3.3 gigabytes of hard drive space.

After you have emptied the Wastebasket, you can close the file explorer window.

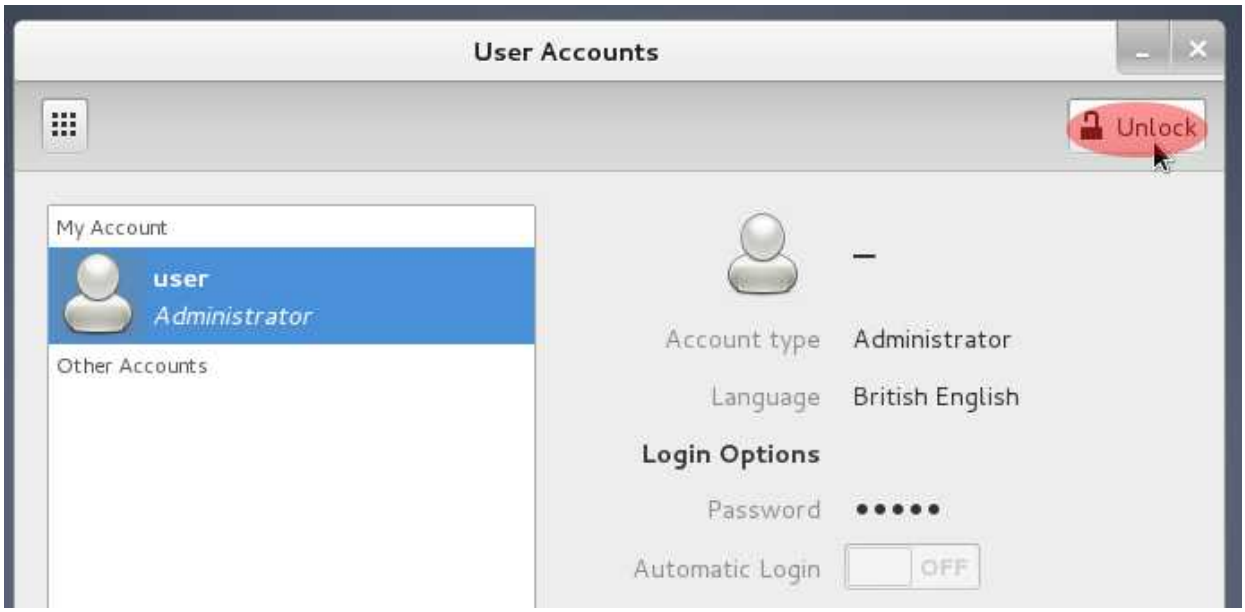
35. Now you should tweak a couple settings in Debian. Click on “user” in the upper right corner and then click on “System Settings.”



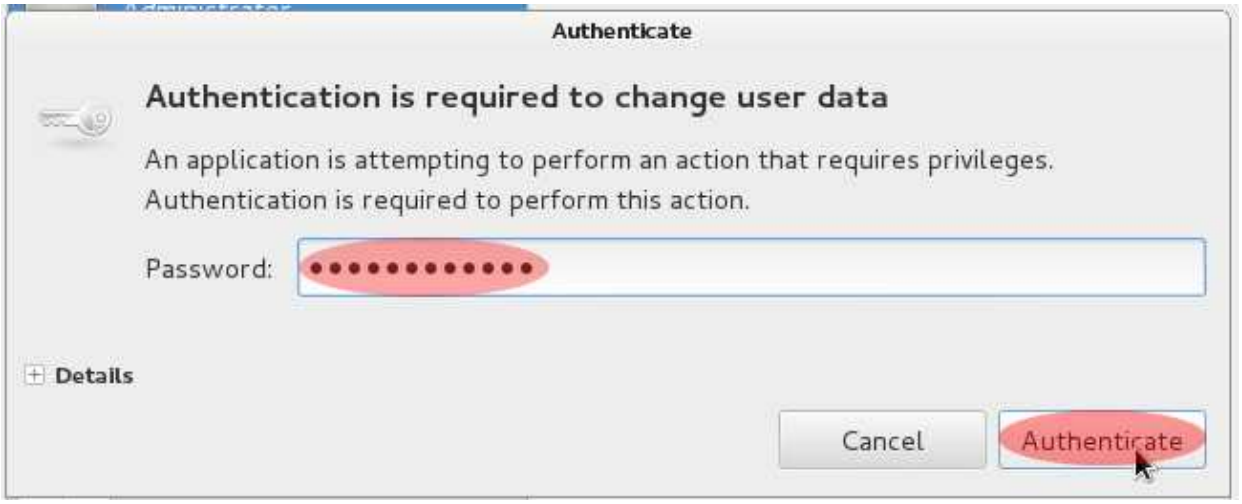
36. In the window that appears, click on “User Accounts” which is towards the bottom.



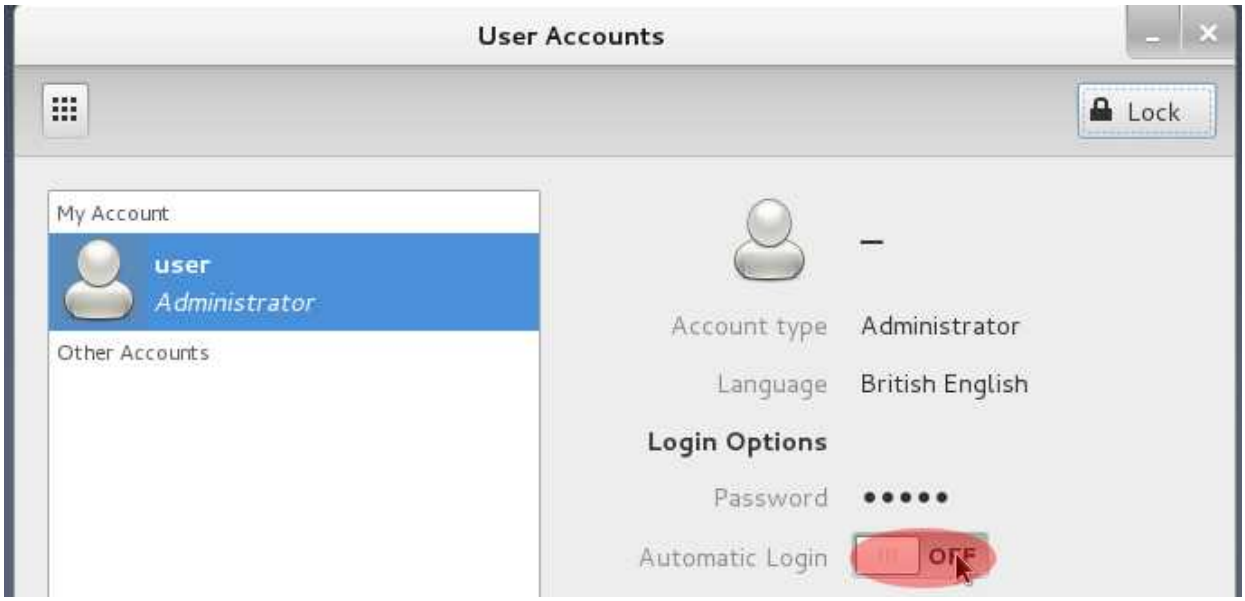
37. In the next screen, click on the “unlock” button in the upper right corner.



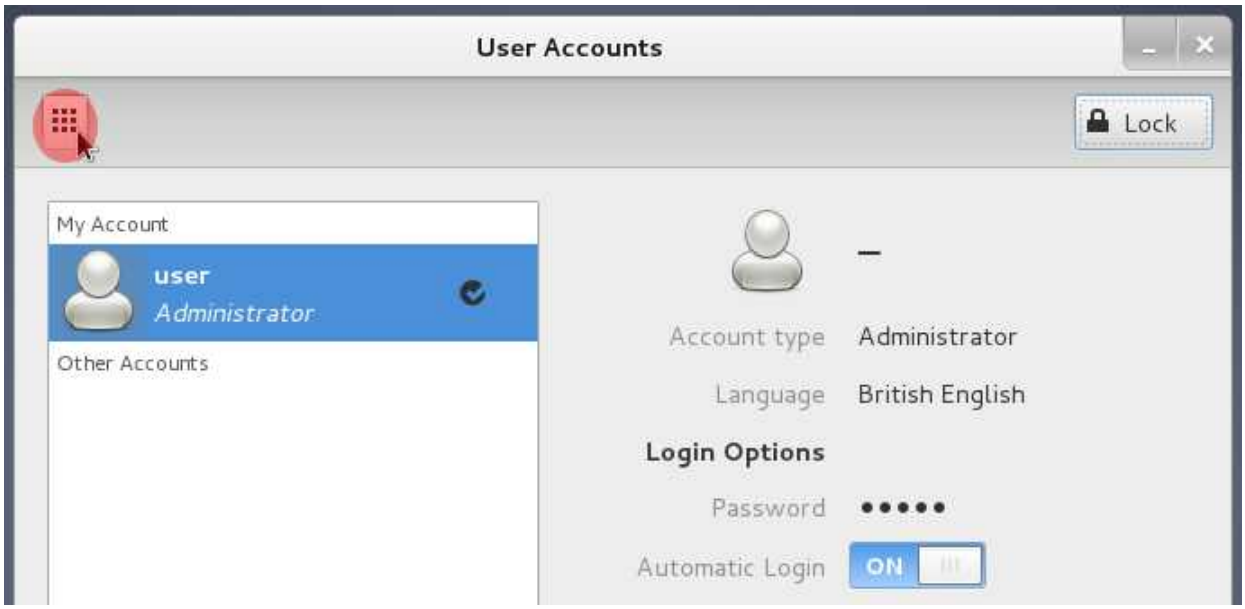
38. You will be prompted for your user password. Type it and click “authenticate.”



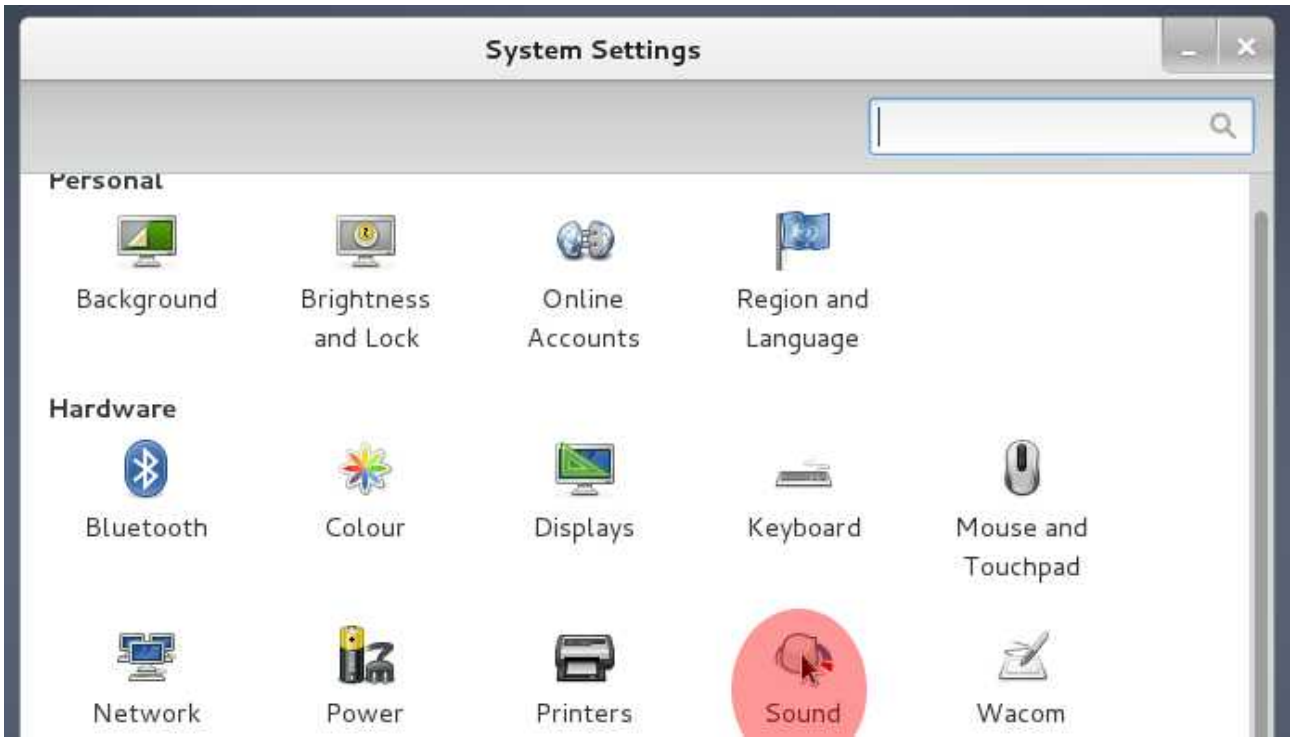
39. Click on the button that is in the “OFF” position next to “Automatic Login.” When switched “ON,” this will remove the requirement to type your user password to login to Debian on boot. Since you have an encrypted hard drive with a passphrase, this extra login check is not necessary.



40. Next, click on the button in the upper left corner with the six squares on it. This will take you back to the main system settings screen.

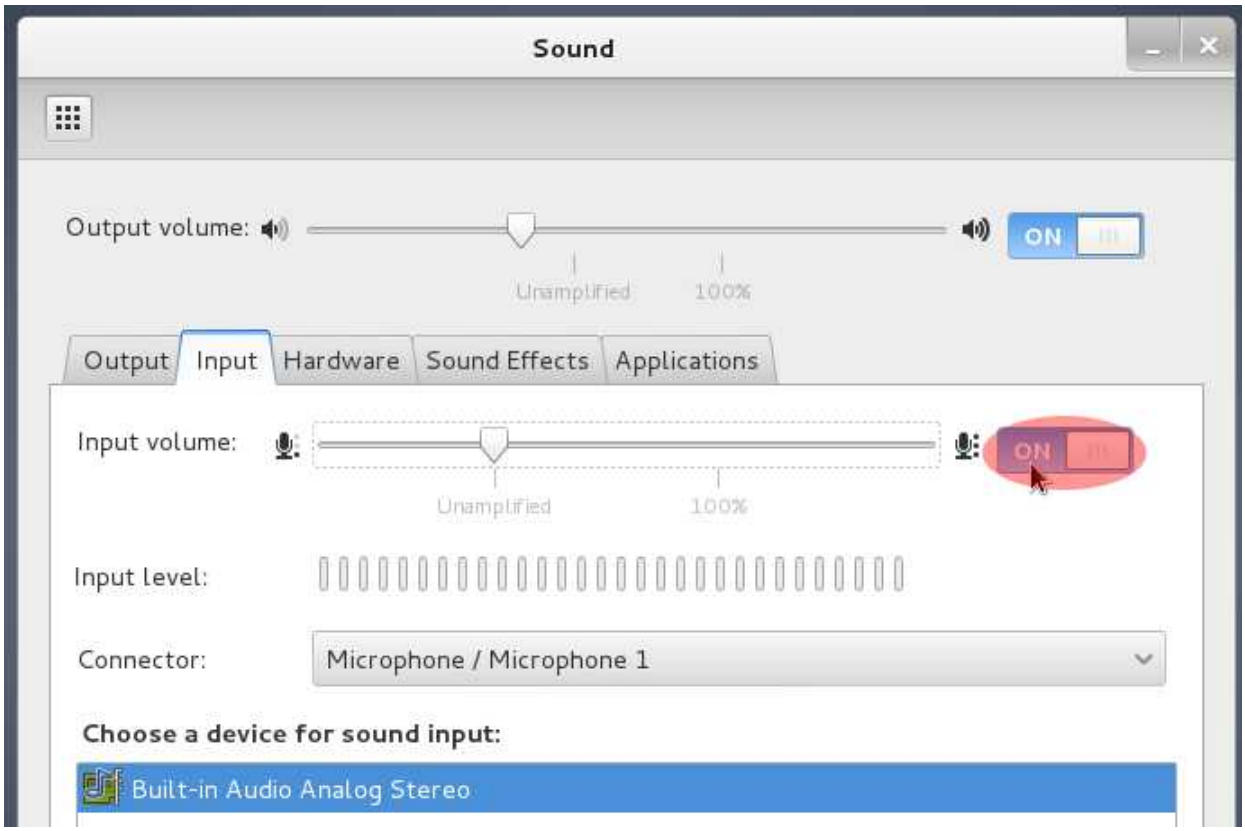


41. Next, you need to disable all of your microphone/sound inputs. VirtualBox does not currently have a setting to disable sound input in its current version. As a result, booting a virtual machine can enable your microphone (if you have one) which is a security hazard. Click on the “Sound” icon in system settings.

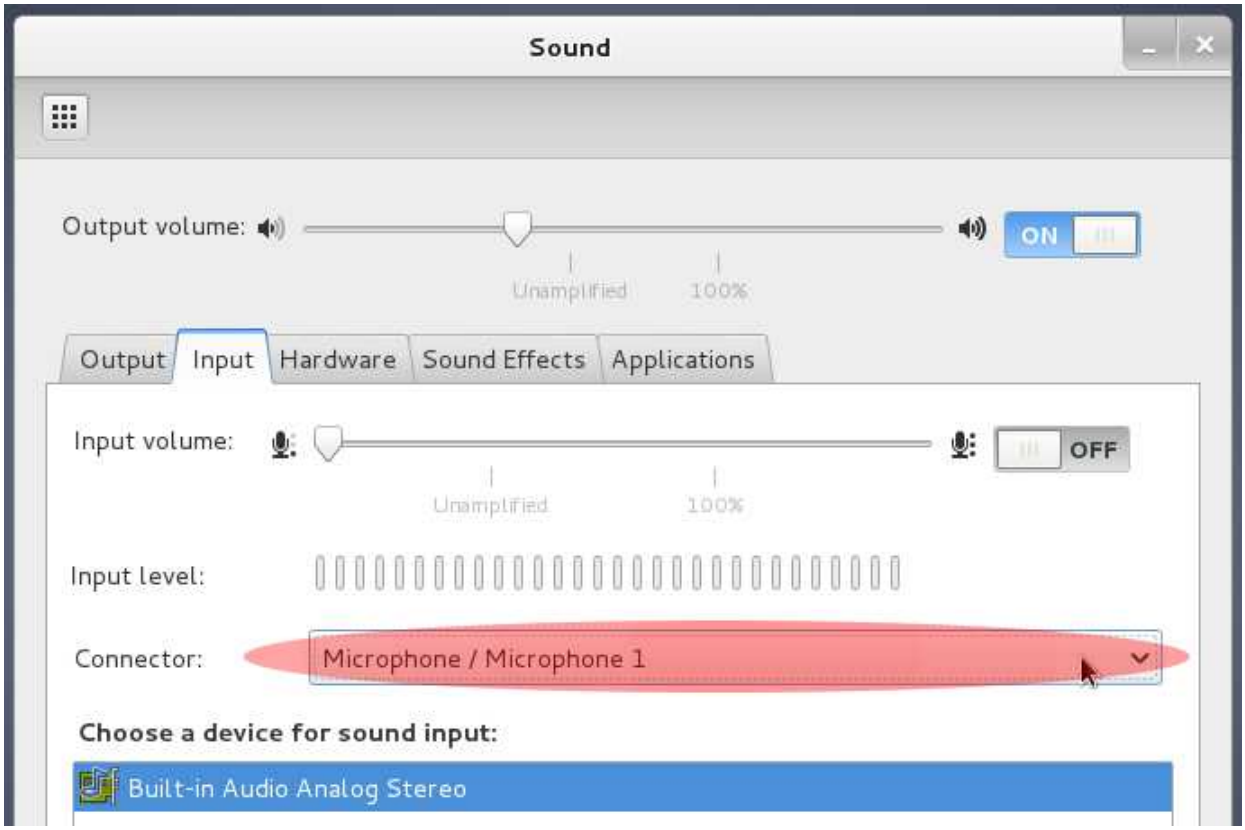


42. In the next screen, click on the “Input” tab.

43. Click on the “ON/OFF” button next to the Input Volume bar to set the device to “OFF.”



44. Click on the pull down menu next to “Connector.” Go through each device that is listed and set them all to “OFF” as you did in step 43. When you have finished, close the window.



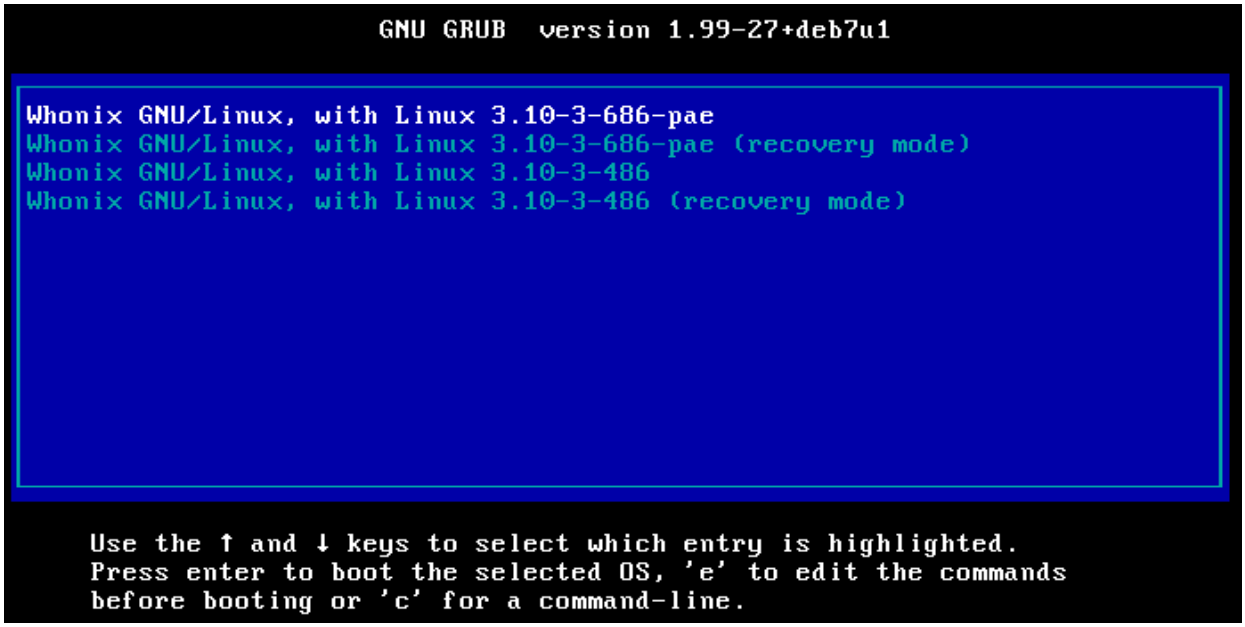
When you boot any virtual machine in the future, a microphone icon may appear in your status bar. In the example below, the icon appears towards the far left. If it looks like the following, grayed out with an “x” in the corner, it is muted.

However, if the microphone icon looks remotely similar to the one pictured below, then your microphone is on. Right click on it and choose “mute.”

45. Now you are ready to run Whonix for the first time. In the "Oracle VM VirtualBox Manager," click on "Whonix Gateway" and click "Start." **Since this might be your first time using VirtualBox, there is an issue that may confuse.** When you click on any running Virtual Machine (whether Whonix-Gateway or Whonix-Workstation), it will auto capture your mouse. This is by design. However, your mouse may appear to get stuck inside the virtual machine if you try to get to another window running outside your virtual machine. If you experience your mouse getting stuck, simply press the "Right Control Key" and VirtualBox will release your mouse.

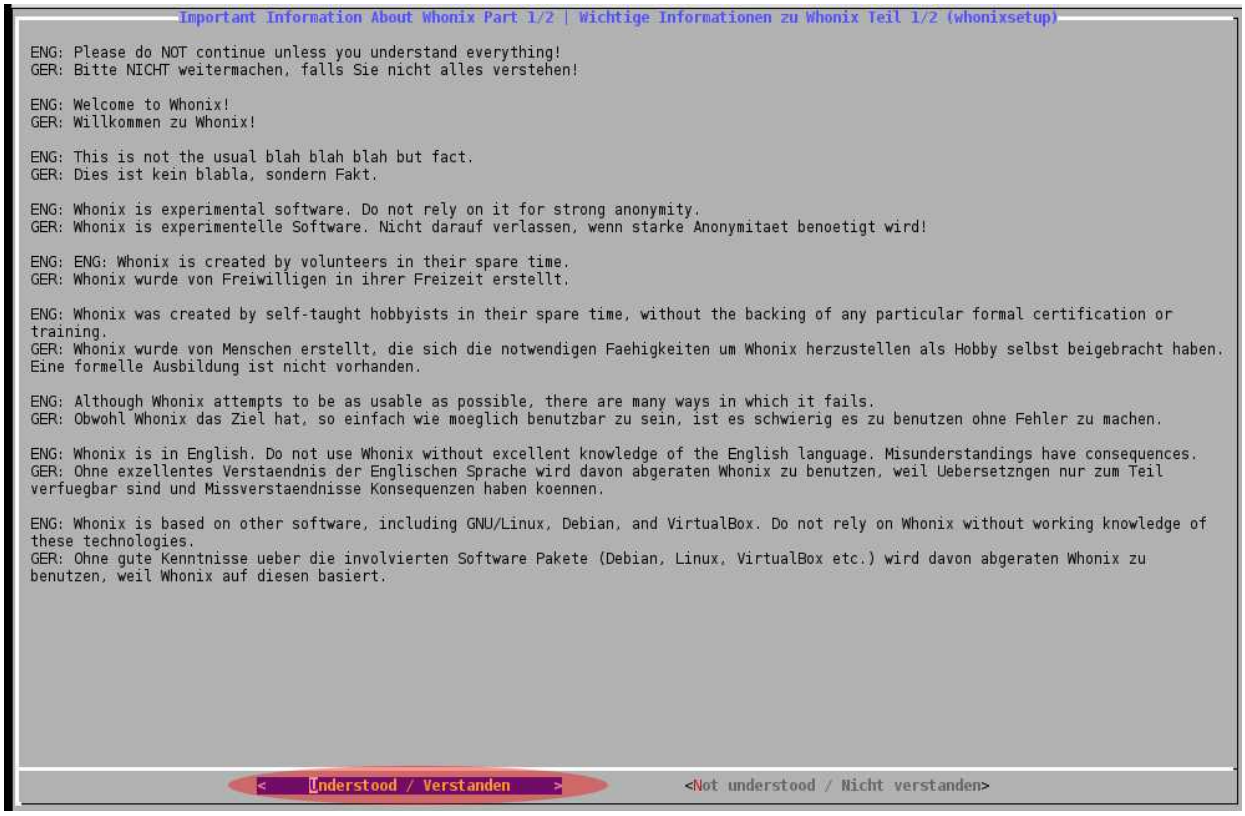
    Note: Depending upon the size and resolution of your monitor, you may discover that the Whonix Gateway window cannot display everything and, as a result, has scrollbars. To work around this, you can either run the Whonix Gateway in "Scaled Mode" by pressing "**RIGHT-CTRL C**" or in "Full Screen Mode" by pressing "**RIGHT-CTRL F**." If you wish to exit either mode, you simply press the same keys used to enable them.

46. A window will appear to start the Whonix Gateway boot sequence. You'll first see the GRUB menu. You can let it automatically boot with the default.

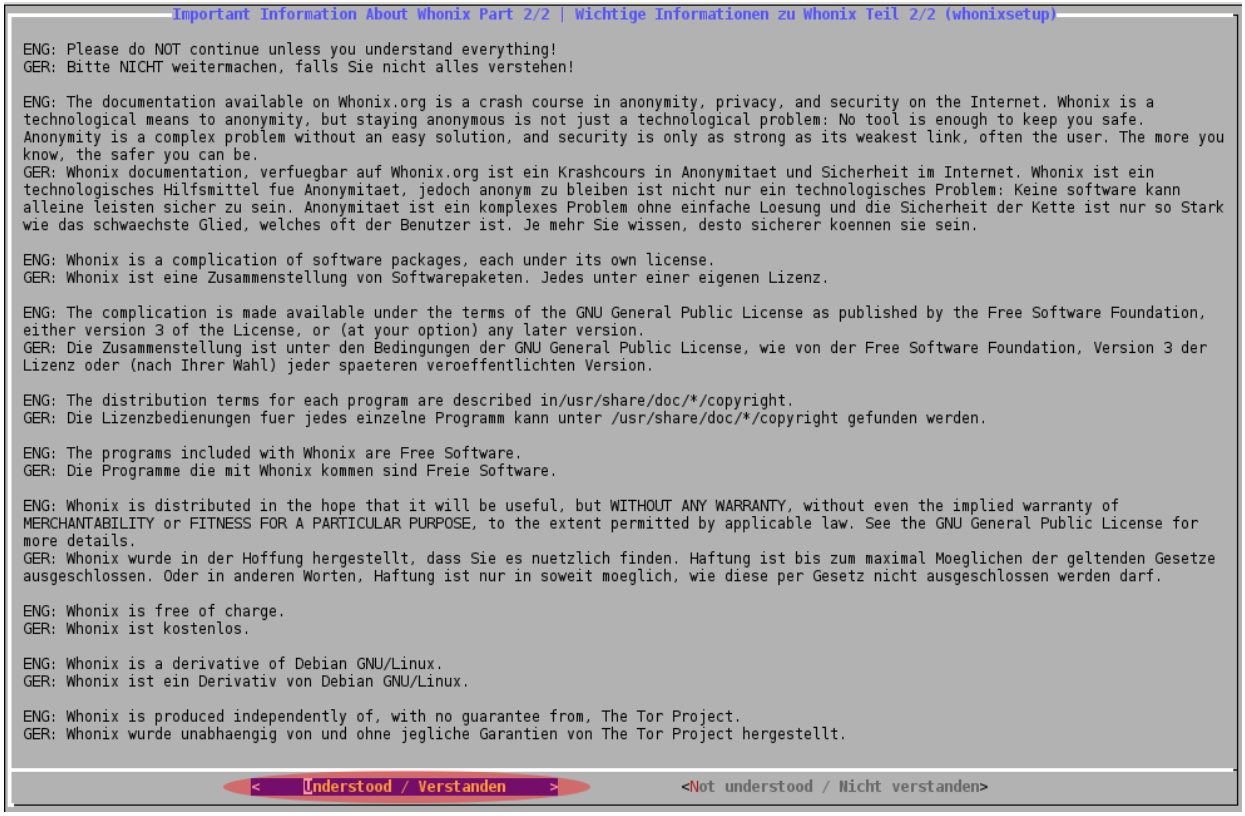


47. Since it is your first time running the Whonix Gateway, it is going to run through a number of procedures and reboot once. Eventually, when it finishes its boot process, a window will appear entitled “First Boot Notice.” After reading it, click the “No” button to prevent from reappearing on boot.

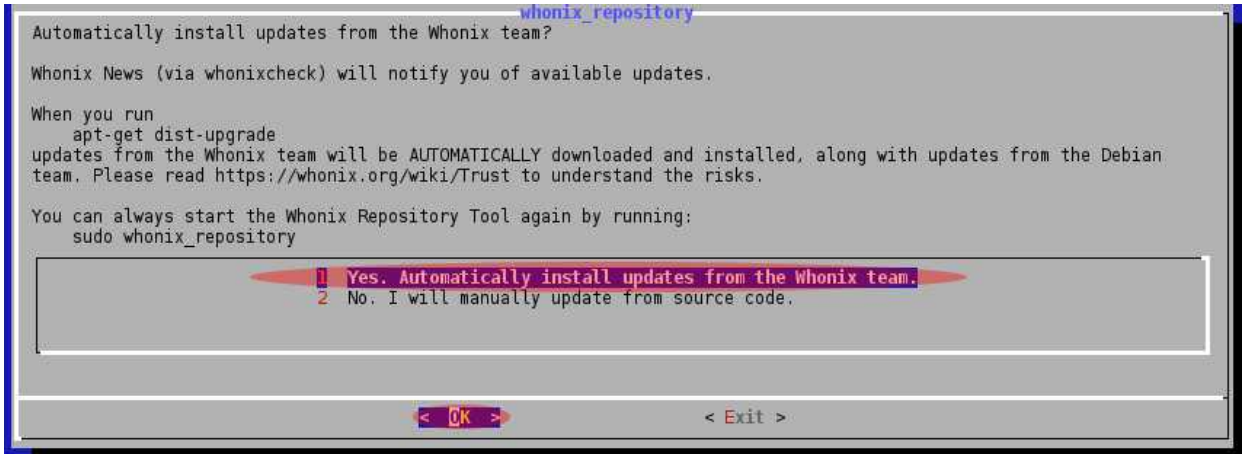
48. Next, the “Important Information About Whonix” will be present.. Click on “Understood/Verstanden” to continue.



49. Next, an additional “Important Information About Whonix” window will appear. Click on “Understood/Verstanden” to continue.

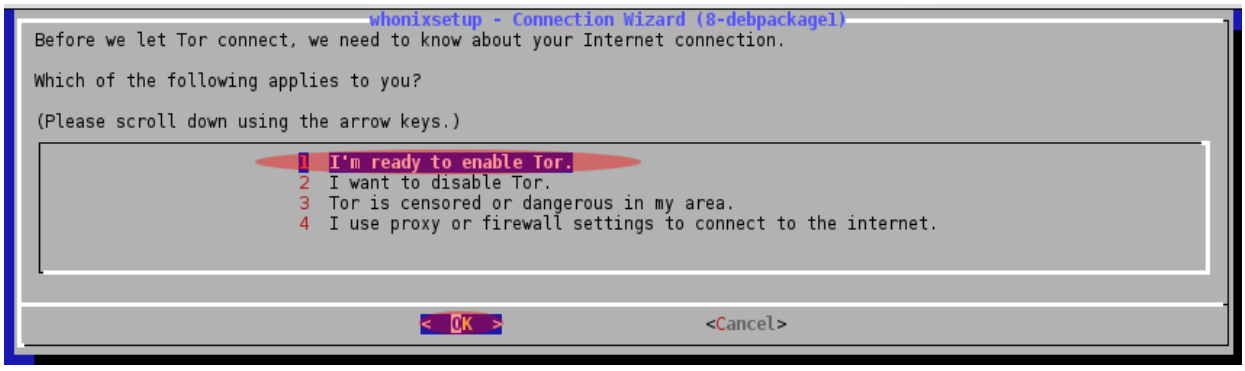


50. The next window will ask if you wish to automatically install updates from the Whonix Team. Choose “Yes” and click “OK.”

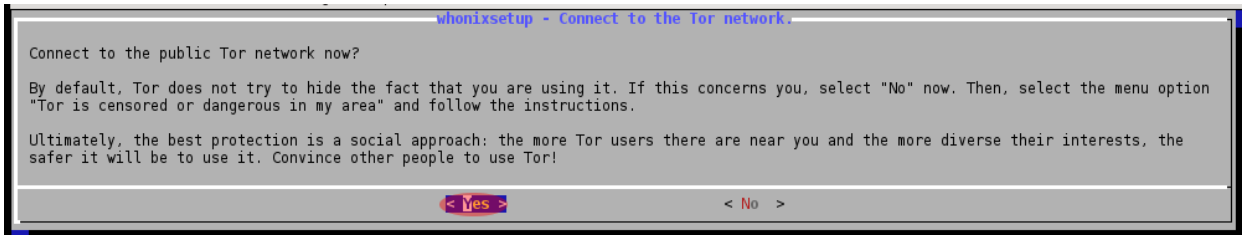


51. Next, you will be asked which repository you'd like to receive updates from. Choose “Whonix Stable Repository” and click “OK.”

52. The next screen will ask you how you want to connect to the Tor Network with a “which of the following applies to you” prompt. For the purposes of this tutorial, it is assumed that you live in a jurisdiction where connecting to the Tor Network is not something that has any legal consequence. However, **this is not the case in all jurisdictions throughout the world.** Please make sure that connecting to the Tor Network is something that is safe in your locale. If you are confident that using the Tor Network is safe in your locale, select option #1 and press “enter” or click on “< OK >.”

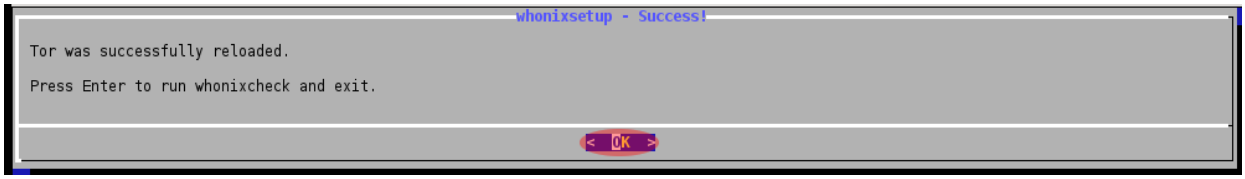


53. The next screen will as if you wish to “connect to the Tor network now.” Press “enter” or click “< Yes >” to continue.

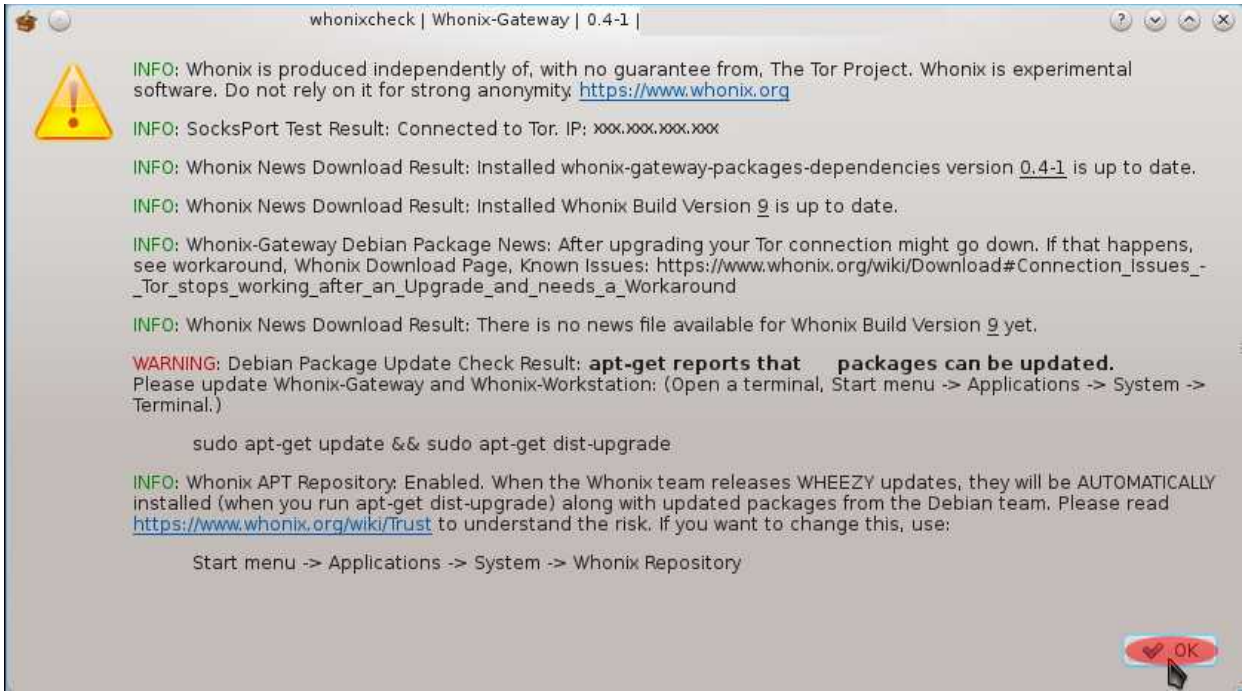


54. At the next screen, press “enter” or click “< OK >” to reload Tor and check its status.

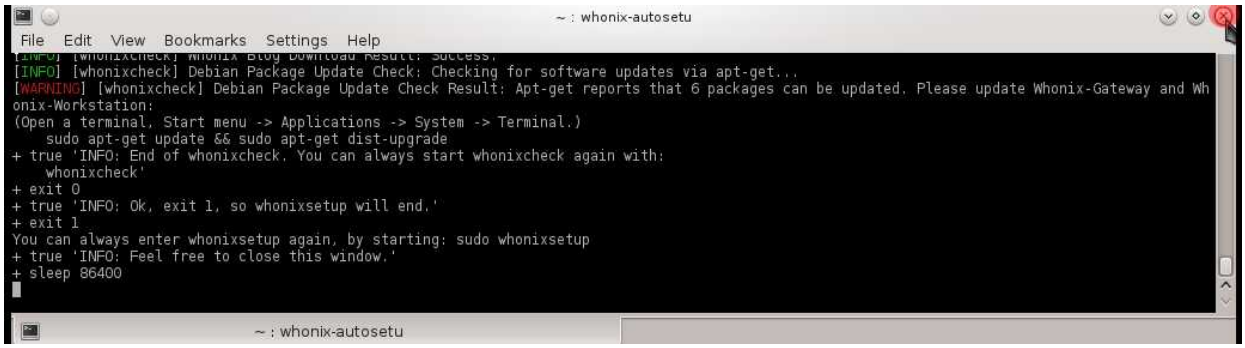
55. At the next screen, you should be informed that “Tor was successfully reloaded.” Press “enter” or click on “< OK >” to continue.



56. The Whonix Gateway will now go through a secure time synchronization procedure, in addition to checking the status of the connection and checking for software updates. When it finishes, you will see a window appear similar to the screen shot below. Click on the “OK” button if visible, or the “x” in the upper right corner of the results window to close it.

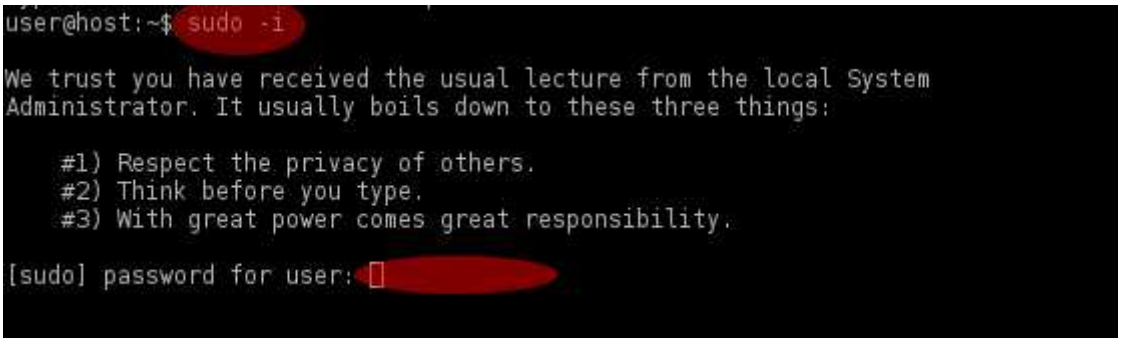


57. Click on the “X” in the upper right corner of the “whonix-autosetup” window to close it.



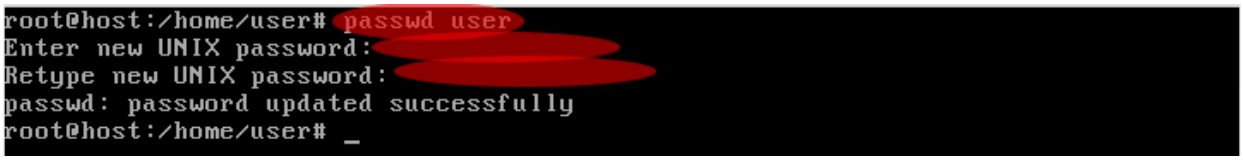
58. Now you should be at the Whonix Gateway Desktop. It's time to change the default passwords and install the latest updates to the Whonix Gateway. Double click on the “Konsole” icon to get to a command prompt.

59. Eventually you will come to a command prompt. At the command prompt, type "**sudo -i"** and type "**changeme**" when prompted for "password for user."



60. Now you need to change the default passwords. Again, don't choose a password that's easy for a machine or human to guess. Type "**passwd**" and press "enter." You will be prompted to enter a new password. You will then be asked to confirm it. If the process is successful, your screen will look like the screen shot below.

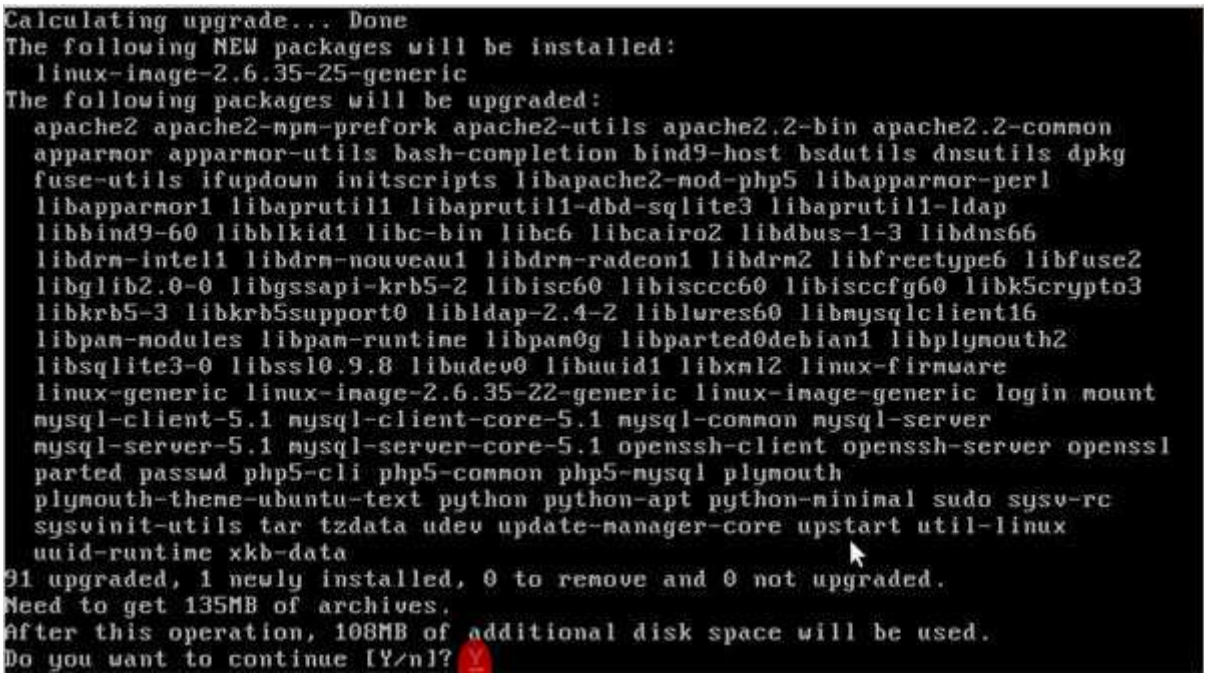
61. Next, change the password for the "user" account on the Whonix Gateway. Type "**passwd user**" and press "enter." You will be prompted to enter a new password. You will then be asked to confirm it. If the process is successful, your screen will look like the screen shot below.



62. Now it is time to update the Whonix Gateway with any recent patches or software upgrades. Type "**apt-get update && apt-get dist-upgrade**" and press "enter."

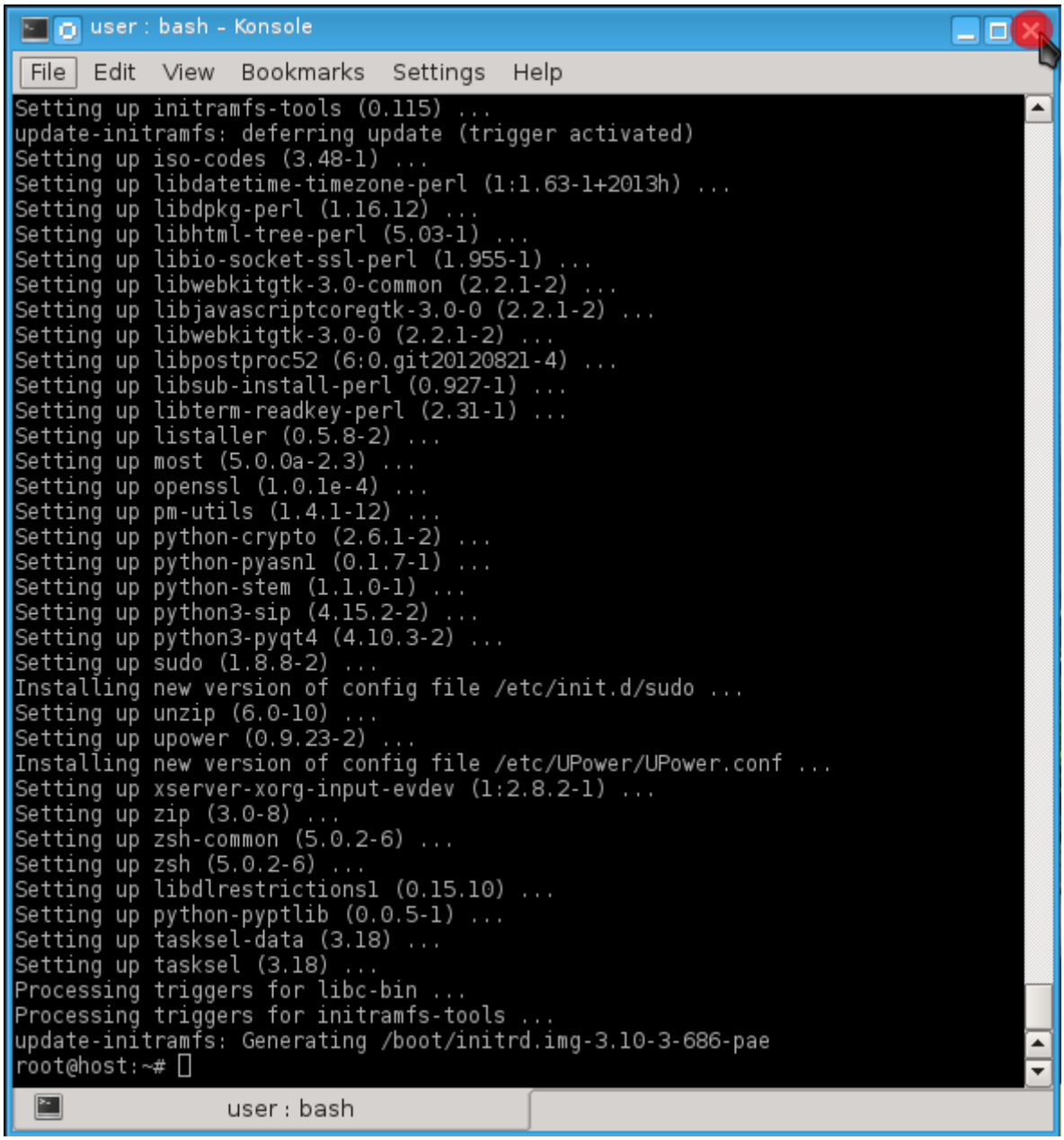
```
root@host:/home/user# apt-get update && apt-get dist-upgrade_
```

Apt-get will download the most current list of packages and patches. When asked if you want to continue, type "**y**" and press "enter." Since this is your first time doing a system upgrade, it is likely that you will have a large amount of data to download. Thus, this process may take some time.



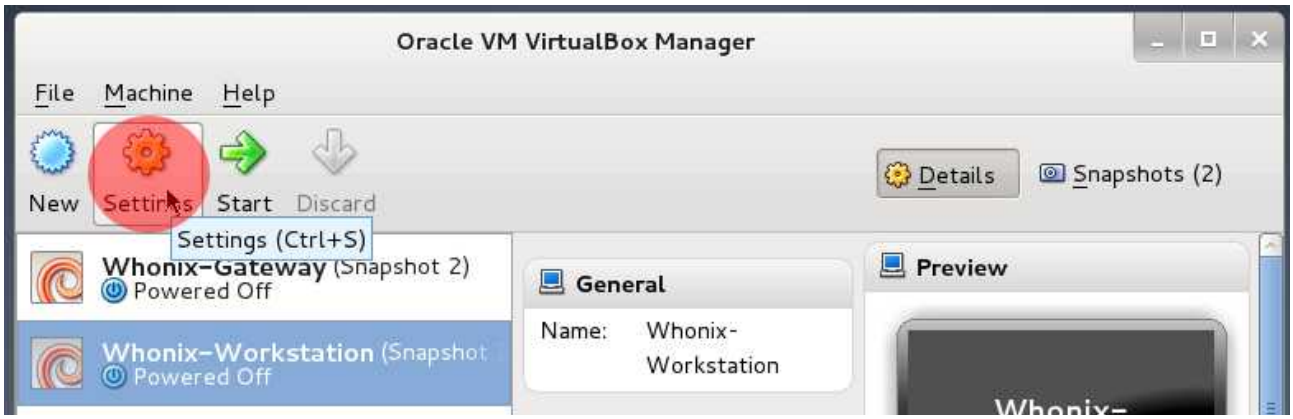
Note: During the distribution upgrade process, you may be prompted to select various options. It is generally best to simply go with the defaults. If, however, you are ever prompted to overwrite a file, choose the option that keeps the original "local version" instead unless the new file has "**.whonix**" as a filename extension.

63. When the process finishes and you are returned to the command prompt, click on the “x” to close the window.

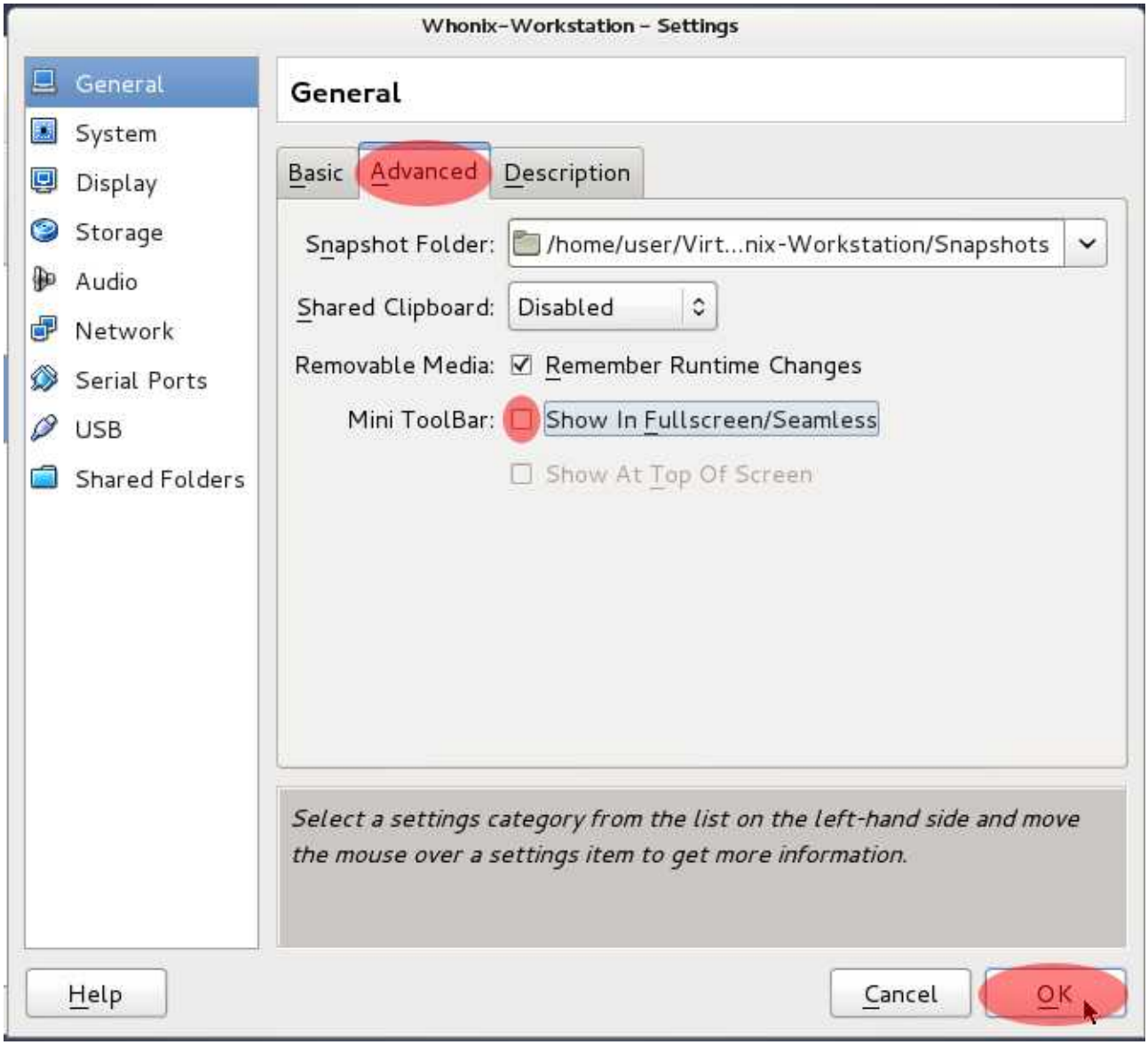


64. Now it is time to prepare to start the Whonix Workstation. You need to get back to the VirtualBox Manager. However, when moving your mouse around, you'll probably notice that it is stuck inside the Whonix Gateway virtual machine window. This is by design. To release the mouse from the Whonix Gateway (or any virtual machine in the future), press the "**right-ctrl**" key (or the equivalent key if you use an Apple computer).

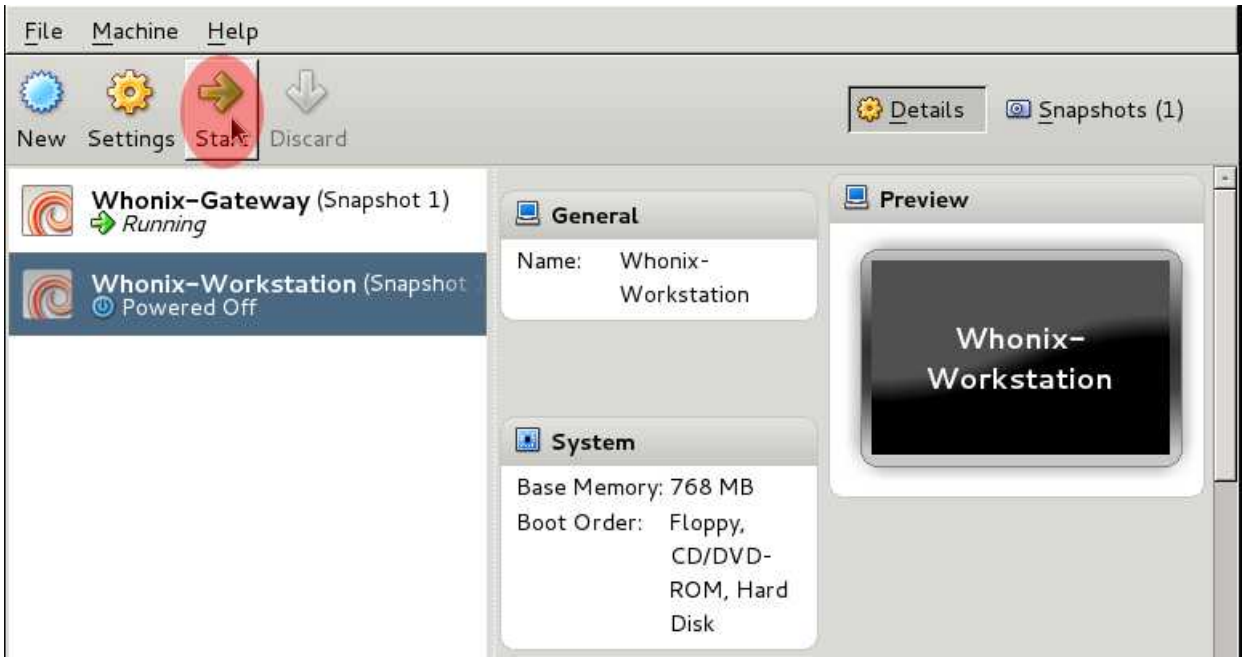
    It will probably be more user friendly for you to run the Whonix Workstation in "Full Screen Mode." Unfortunately, a "Mini Toolbar" is present in VirtualBox's "Full Screen Mode" by default, which can cause the mouse pointer to seem sluggish when used near the bottom of the screen on a number of computers. Before starting the Whonix Workstation, let's address that. Click on "Whonix Workstation" in the VirtualBox Manager and then click the "Settings" button.



64b. Next, click on the “Advanced” tab. Then, click on the check box next to “Mini Toolbar” so it is unmarked. Then, click the “OK” button.

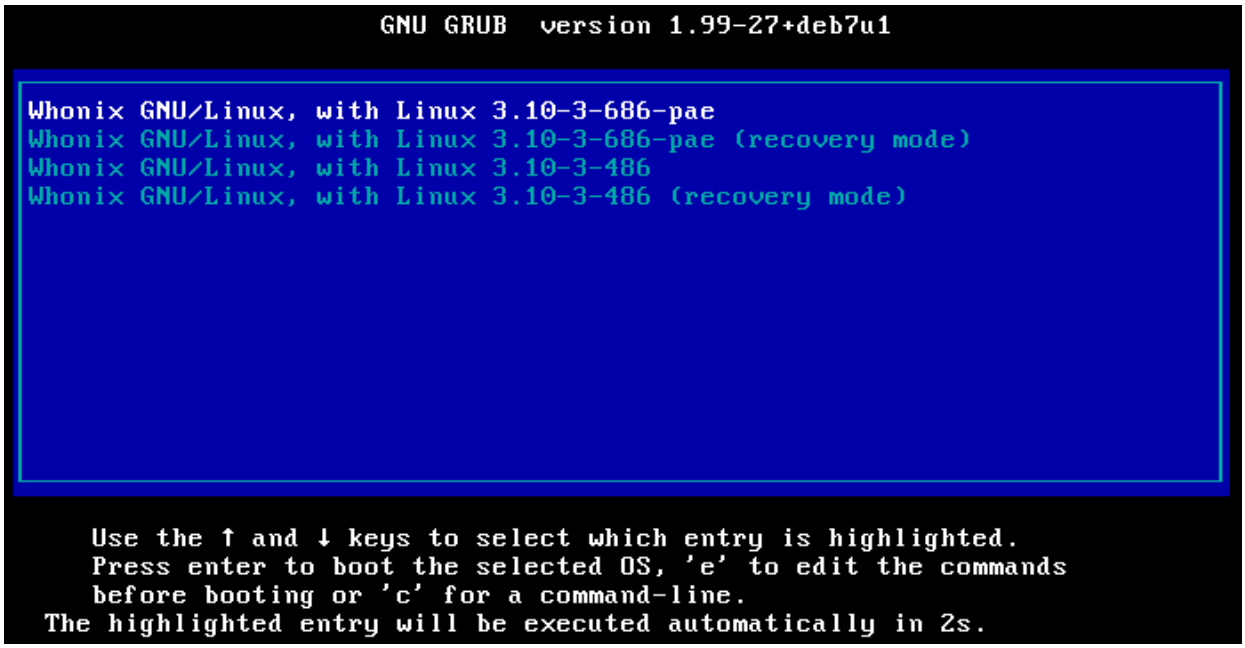


64c. Now, with the “Whonix-Workstation” selected, click the “Start” button.

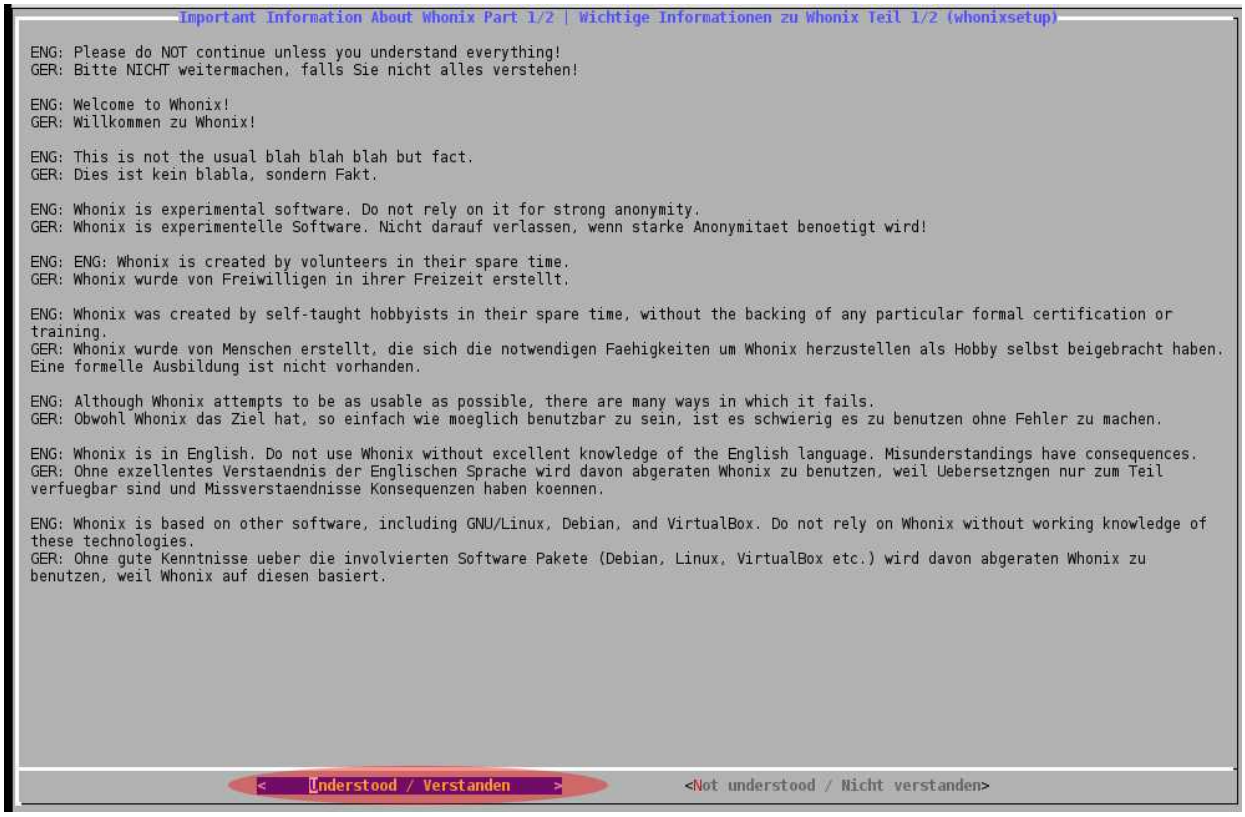


65. A window will appear to start the Whonix Gateway boot sequence. You'll first see the GRUB menu. You can let it automatically boot with the default.

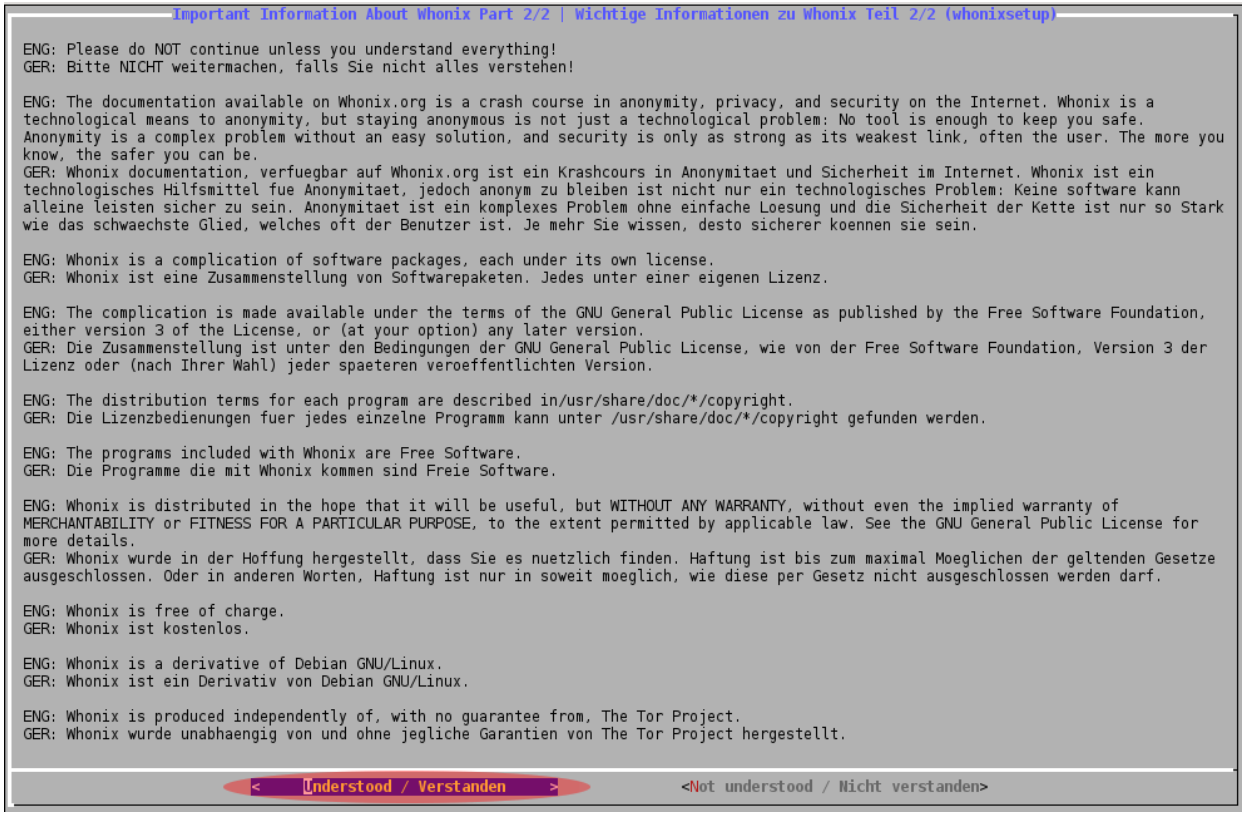
    NOTE: At this point, you will probably enjoy "Full Screen Mode" more. Press "**RIGHT-CTRL F**" to run it in "Full Screen Mode." If you wish to exit "Full Screen Mode," simply press "**RIGHT-CTRL** F" again.



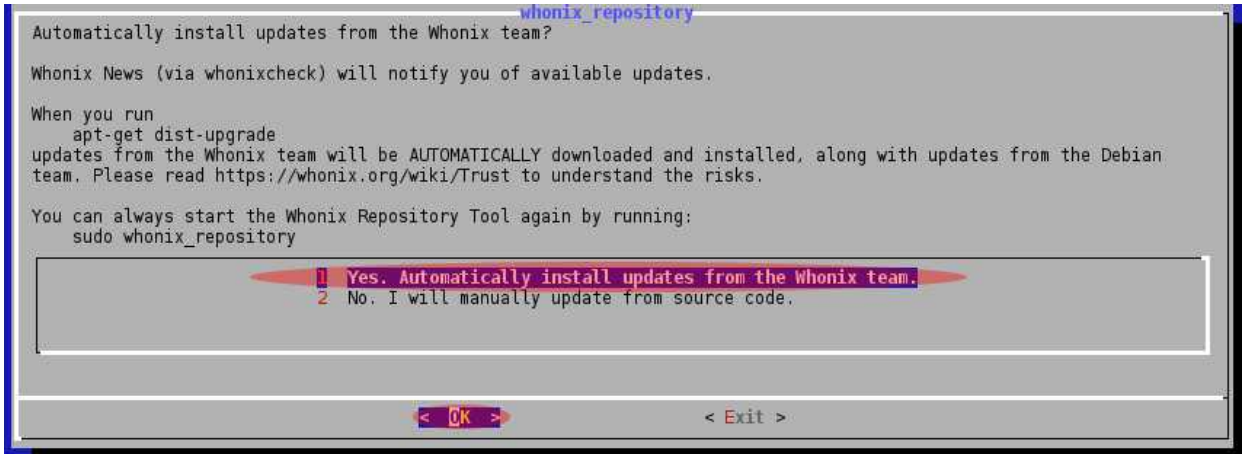
66. Since it is your first time running the Whonix Workstation, it is going to run through a number of procedures and reboot once. Eventually, when it finishes its boot process, the “Important Information About Whonix” window will appear. Click on “Understood/Verstanden” to continue.



67. Next, an additional “Important Information About Whonix” window will appear. Click on “Understood/Verstanden” to continue.



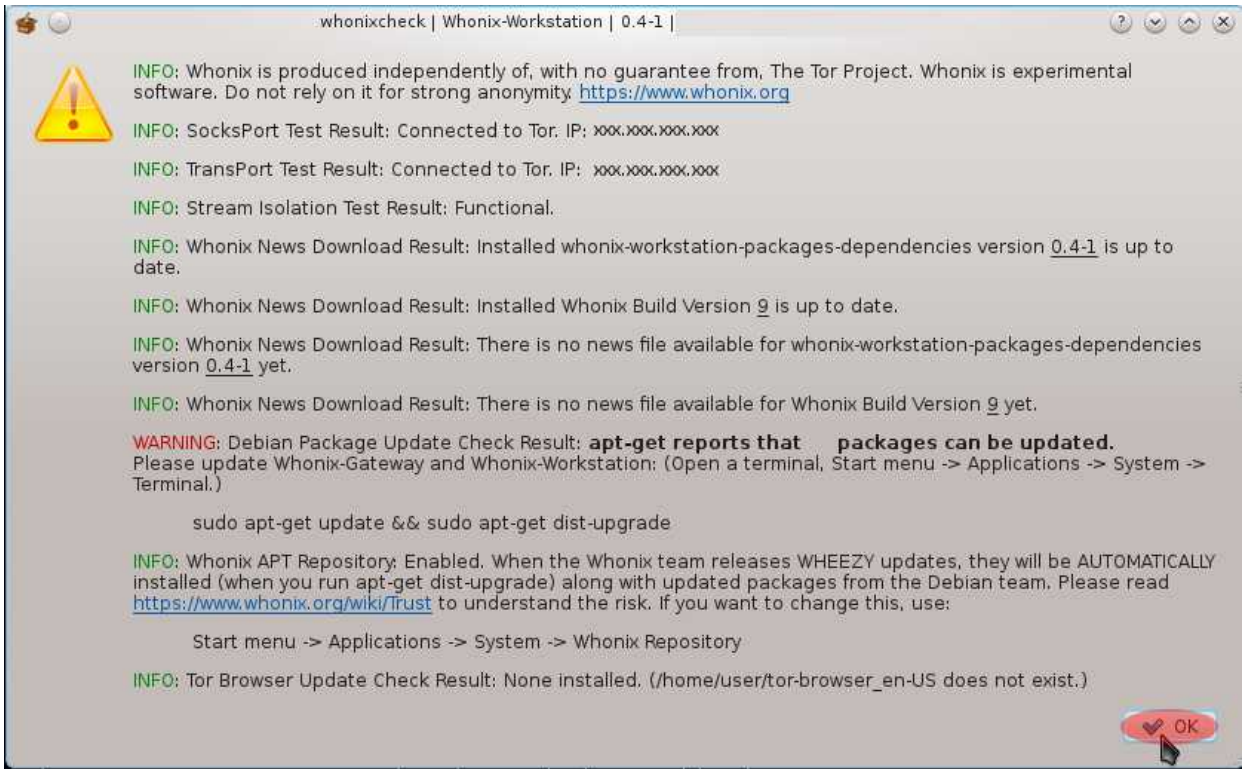
68. The next window will ask if you wish to automatically install updates from the Whonix Team. Choose “Yes” and click “OK.”



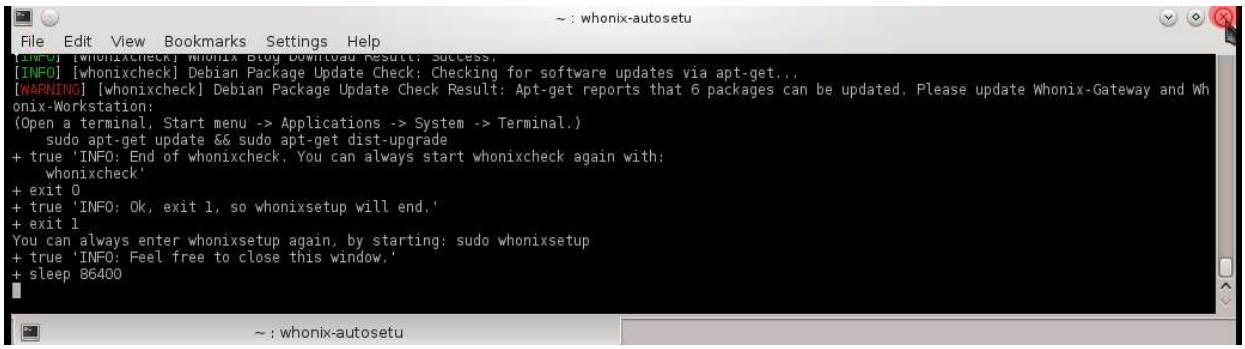
69. Next, you will be asked which repository you'd like to receive updates from. Choose “Whonix Stable Repository” and click “OK.”

70. At the next screen, press “Enter” to continue.

71. The Whonix Workstation will now go through a secure time synchronization procedure, in addition to checking the status of the connection and checking for software updates. When it finishes, you will see a window appear similar to the screen shot below. Click on the “OK” button if visible, or the “x” in the upper right corner of the results window to close it.

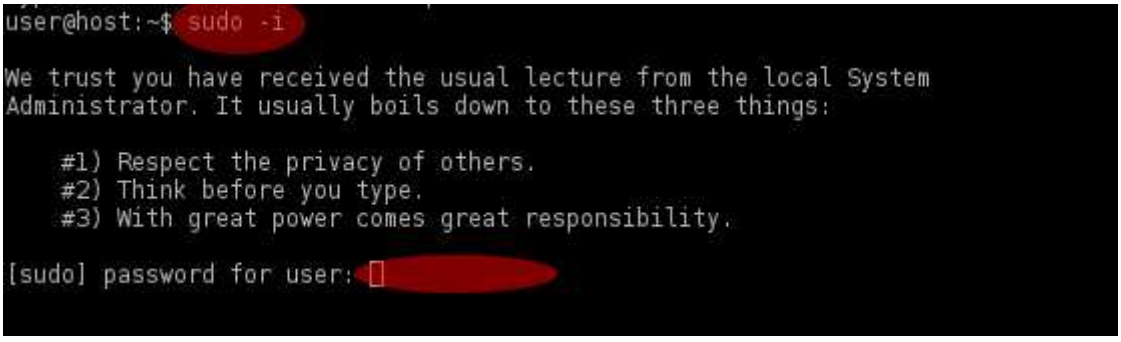


72. Click on the “X” in the upper right corner of the “whonix-autosetup” window to close it.



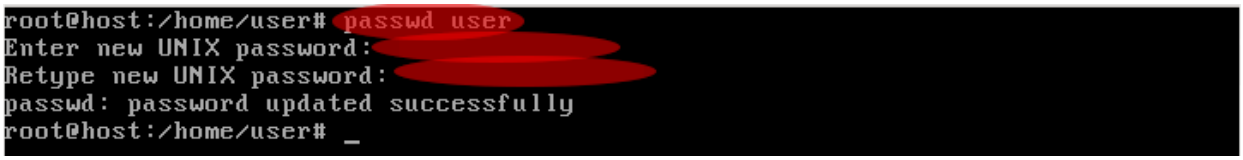
73. Next, you need to get to a shell prompt. Double click on the “Konsole” icon to open up a terminal and reach a shell command prompt.

74. You need to reset the default passwords for the Whonix Workstation as well. Type “**sudo -i**”and press “enter.” When prompted to enter “password for user,” type “**changeme**” and press “enter.”



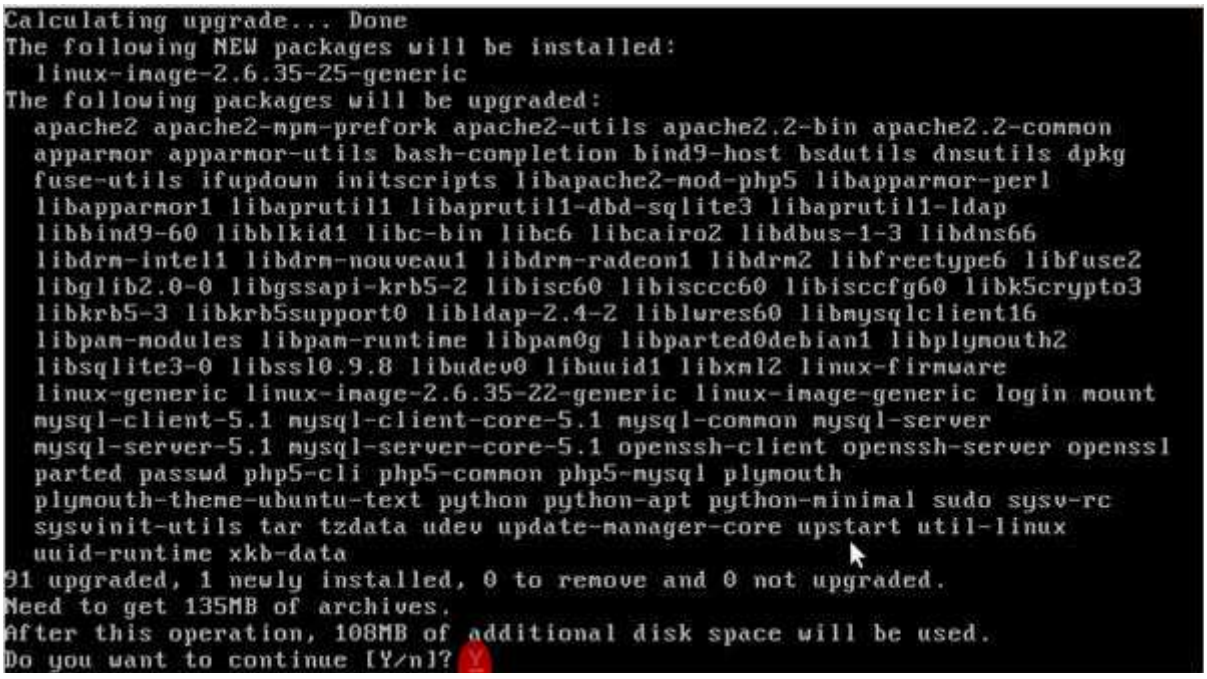
75. Now you need to change the default passwords. Again, don't choose a password that's easy for a machine or human to guess. Type “**passwd**” and press “enter.” You will be prompted to enter a new password. You will then be asked to confirm it. If the process is successful, your screen will look like the screen shot below.

76. Next, change the password for the “user” account on the Whonix Workstation. Type “**passwd user**” and press “enter.” You will be prompted to enter a new password. You will then be asked to confirm it. If the process is successful, your screen will look like the screen shot below.



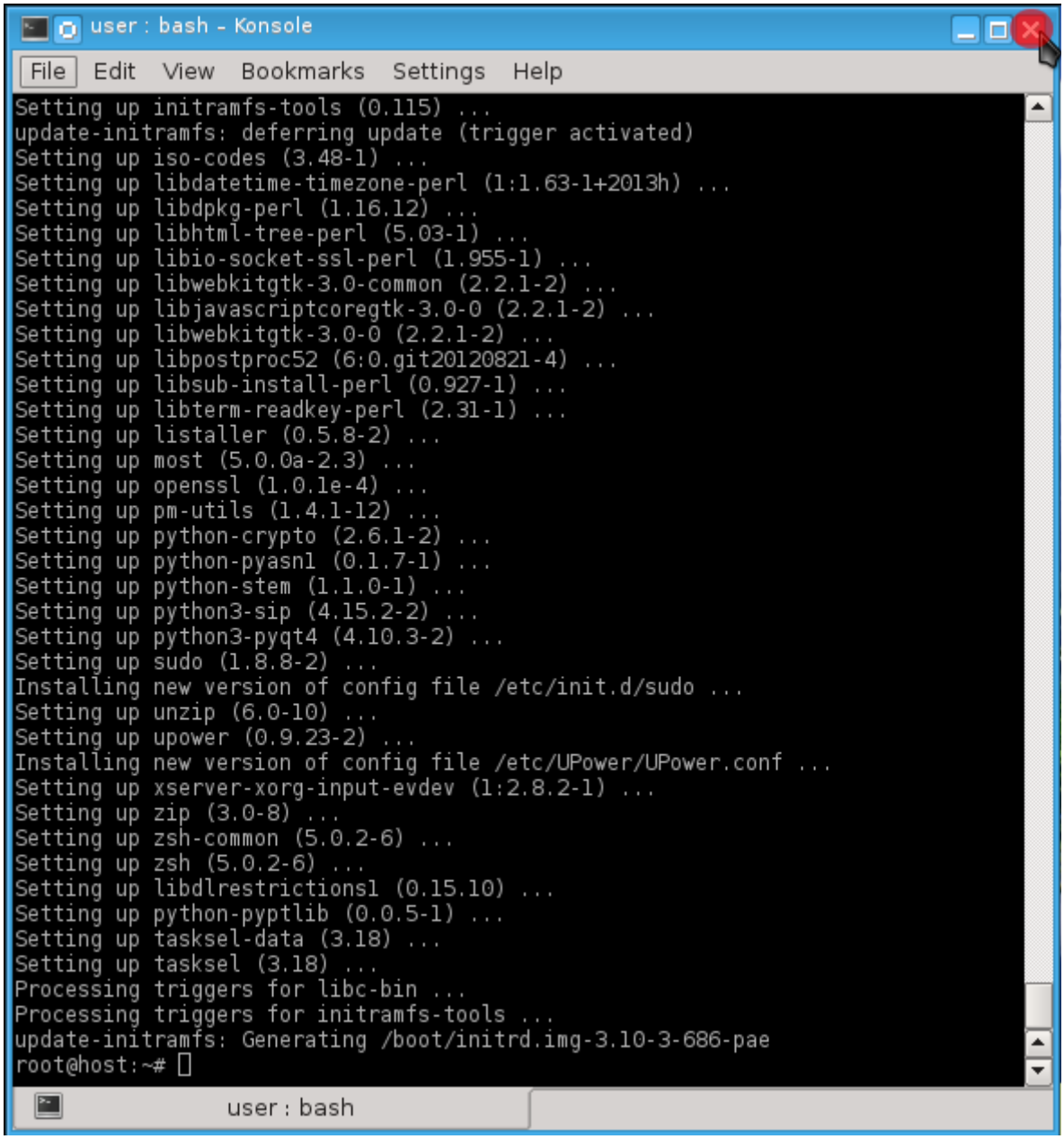
77. Now, update the Whonix Workstation with any recent patches. Type “**apt-get update && apt-get dist-upgrade**” and press “enter.”

Apt-get will download the most current list of packages and patches. When asked if you want to continue, type “**y**” and press “enter.” Since this is your first time doing a system upgrade, it is likely that you will have a large amount of data to download. Thus, this process may take some time.



Note: During the distribution upgrade process, you may be prompted to select various options. It is generally best to simply go with the defaults. If, however, you are ever prompted to overwrite a file, choose the option that keeps the original “local version” instead unless the new file has “**.whonix**” as a filename extension.

78. When the process finishes and you are returned to the command prompt, click on the “x” to close the window.



Congratulations! You have finished installing the “operating system” relating to the “Safer Anonymous OS.” Feel free to take a break here. The next chapters will deal with installing and/or using software in a secure and anonymous fashion over the Internet. You can take a break from here if you like.

Chapter 4. Using Whonix Securely and Anonymously

If you made it this far, you're now ready to begin using Whonix. This tutorial is not intended to be a full manual for everything involving Whonix or security and anonymity. However, you will be given the basics on installing and using a number of very good tools. Additionally, unless otherwise specified, all instructions are intended to be executed in the Whonix Workstation. To learn more about Whonix and its various uses, **it is strongly recommended that you visit and read the following links**:

- https://www.whonix.org/wiki/Documentation [Whonix Documentation]
- https://www.whonix.org/wiki/Security_Guide [Whonix Security Guide]
- https://www.whonix.org/wiki/Warning [Warnings Guide & Behavior to Avoid]

If you need any support or troubleshooting for using Whonix, please go to https://www.whonix.org/forum.

As the first rule (or advice) going forward from this point, **do not use Whonix to login to any accounts that you have used without Whonix and can be traced to your identity. Consider everything you do from here forward the creation of a new identity.**

Additionally, when using this set up in the future, always boot the Whonix Gateway virtual machine first in VirtualBox. If you boot the Whonix Workstation first, it won't work.

Finally, **do not use the main Debian host operating system that you installed on your computer for surfing the web or engaging in other net related activities!** The goal is to keep Debian as clean as possible. Surfing the web with the Debian host operating system opens up greater possibilities that your machine may be infected with malware. If your Debian host operating system becomes infected with malware, then your Whonix virtual machines are compromised as well. Therefore, **use Whonix Workstation for all your networking activities.**

Chapter 4a. Proper Start Up and Shut Down Procedures for Whonix

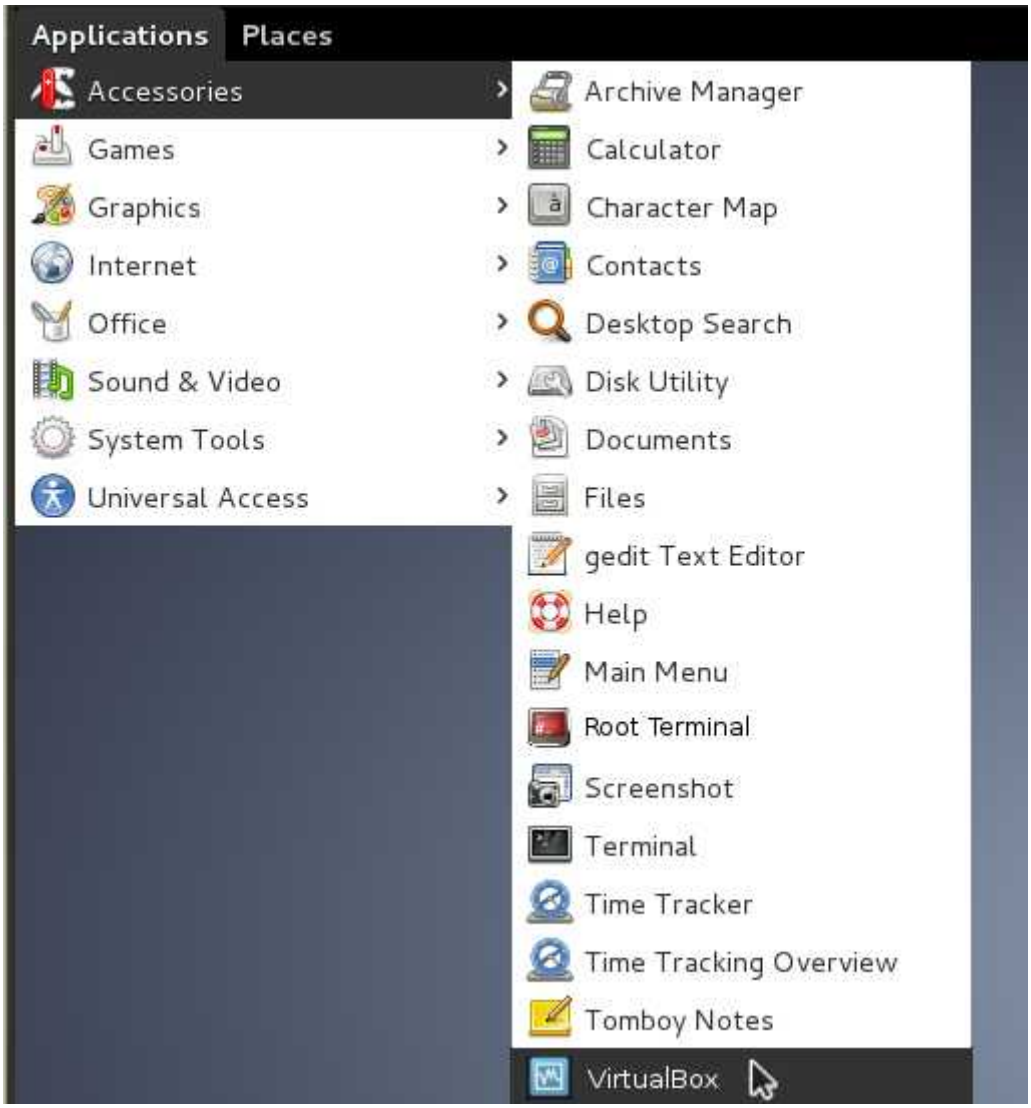
In order for Whonix to function as intended, there is a specific start up and shut down procedure that you need to follow in the future. This chapter will explain how to do just that.

For an easy quick reference, here is the procedure:

1. Boot the **Whonix Gateway** first.
2. Boot the Whonix Workstation second.
3. Shutdown the **Whonix Workstation** first.
4. Shutdown the Whonix Gateway second.
5. Shutdown Debian last.

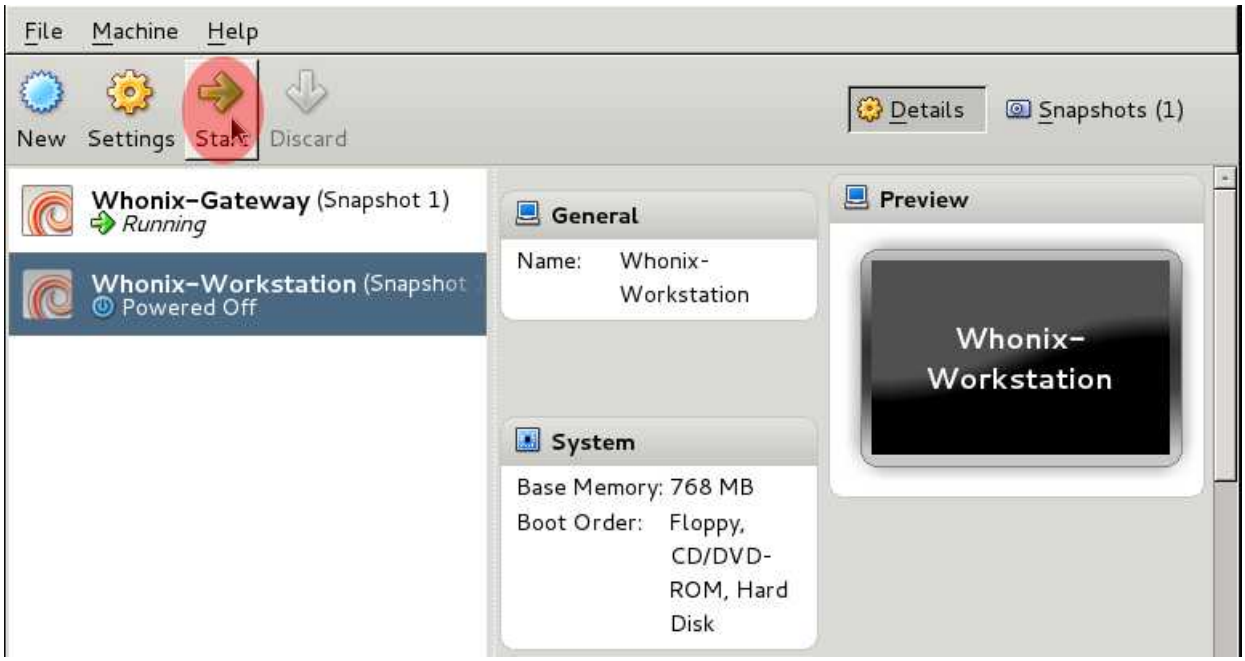
Below are the slightly more detailed instruction.

1. When you have booted into Debian from your USB Flash Drive and reach your Dekstop, click on “Applications → Accessories → VirtualBox” to open the VirtualBox Manager.



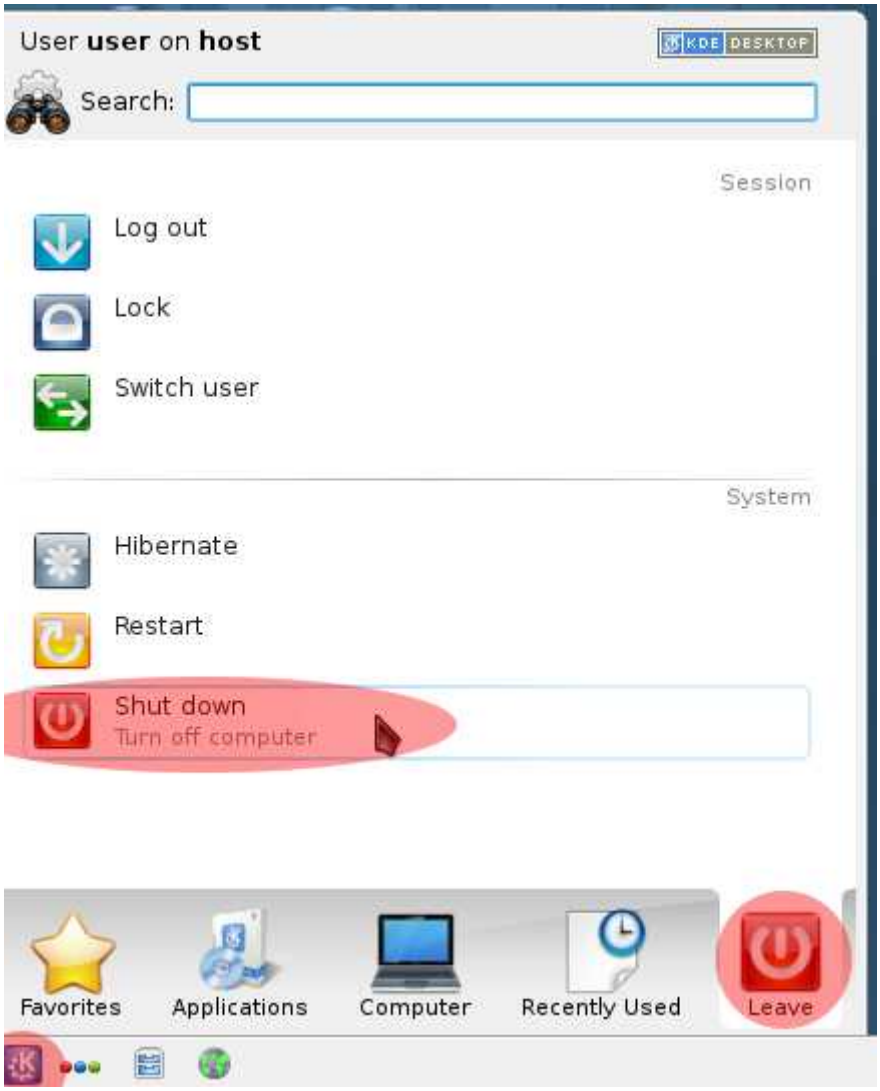
2. In the VirtualBox Manager, click on “Whonix-Gateway” and click “Start.” **Whonix Gateway must always be run first or the system won't work.**

3. When you reach the Desktop of the Whonix Gateway, go back to the VirtualBox Manager, click on “Whonix-Workstation” and click “Start.” If your mouse is stuck in the Whonix Gateway, remember you need to press the “**right-ctrl**” key to release it.



When you reach the Desktop of the Whonix Workstation, you are ready to being using it as you usually would any other computer.

4. **When you are ready to shut down your computer**, first make sure you have saved all your work in the Whonix Workstation and closed the programs. Then, shut down the Whonix-Workstation. Then, click on the "K" start button in the lower left corner of your screen, hover the mouse over the "Leave" icon that appears in the right side of the Start Menu and then click on "Shut down."

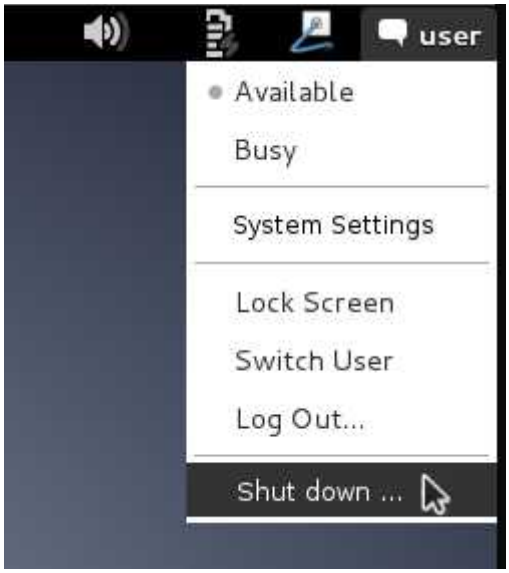


5. In the next window that appears, click on "Turn Off Computer."

6. The next screen will prompt you to close “Abort active sessions.” Click on “OK” to continue.

7. When the Whonix Workstation window closes from view, it is shut down. You can now close the Whonix Gateway. To close the Whonix Gateway, **switch over to the Whonix Gateway window and repeat the choices made in steps 4-6 above.** It is the exact same process for shutting down the Whonix Gateway as it is for shutting down the Whonix Workstation.

8. When the Whonix Gateway window closes from view, it is shut down. **Now you can shut down Debian.** Click on the “user” menu in the upper right corner of your screen and click “Shut Down.”



9. In the window that pops up, click “Shut Down.” Eventually your computer should power off.

Once your computer is powered off, you are finished. **This is how you should start up and shut down your system every time in the future.**

Chapter 4b. Using the Tor Browser.

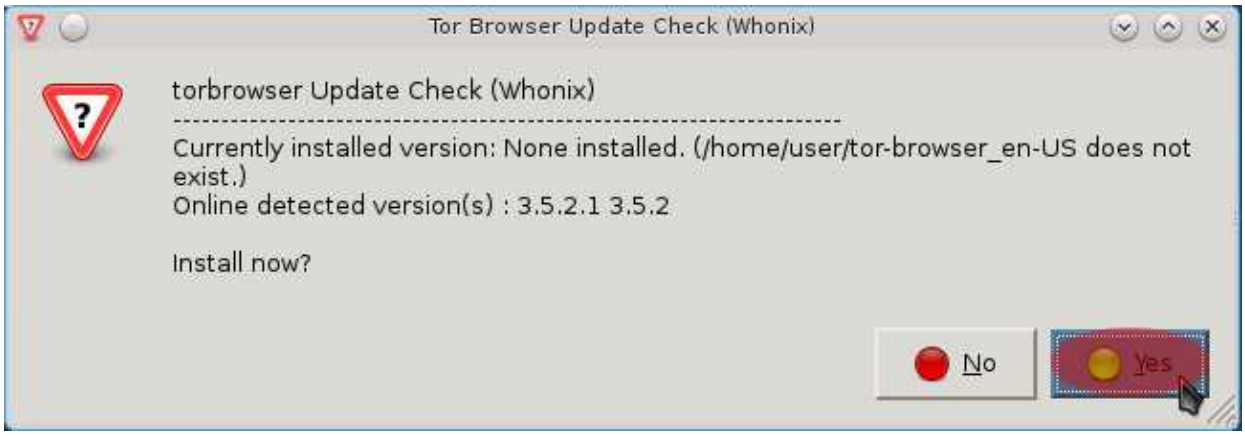
It may seem redundant to have an instructional section on something as simple to use as a web browser. However, your web browser is often the most common piece of software that attackers will manipulate to exploit you. The Tor Project has done a very good job in making the Tor Browser as secure as possible. However, due to a debate about the trade off between usability and security, the Tor Browser is currently set to allow all javascript to run.

The debate on the enabling or disabling of javascript is a fair one. Many web sites now make use of multitudes of javascript to deliver their service or data. If javascript is disabled, then the web sites often appear to be broken which will frustrate less patient users. However, javascript is often a vulnerable vector that is leveraged by attackers, with one of the most notorious recent examples involving infecting everyone who visited any server hosted by "Freedom Networking" on the Tor Hidden Network with malware that exposed their real IP address. Whonix provides a very good safe guard against leaking one's real IP address. But, there is no good reason to leave a door open for malware infections. This chapter will instruct you on how to install the Tor Browser in Whonix and how to make the most of the "NoScript" plugin, which will disable all javascript by default, that comes pre-installed in the Tor Browser.

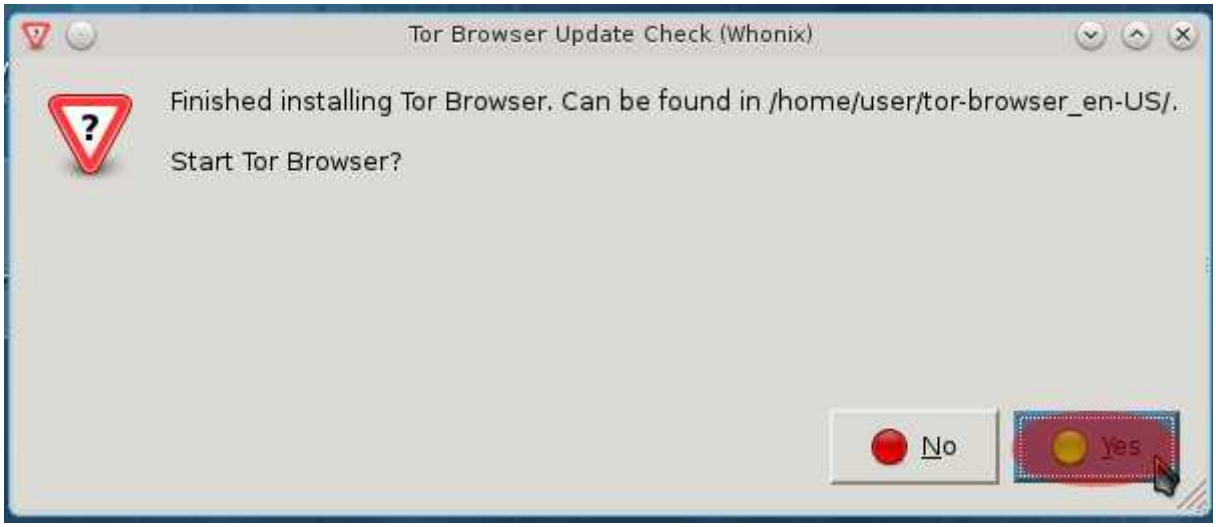
1. The Tor Browser does not come pre-installed on Whonix by default. However, the Whonix Team has included a script on the Desktop that will install the Tor Browser. Thus, you first need to double click on the "Update Tor Browser" icon on your desktop.

   NOTE: As of time of publication, a bug is resulting in the installation of an Alpha version of Tor Browser rather than the stable version. Alpha versions of software are not as tested as the stable versions and are considered less secure as a result. If you wish to install the stable version, please follow the alternative instructions at https://www.whonix.org/wiki/Manually_Updating_Tor_Browser. For more info on this bug, follow the forum post at https://www.whonix.org/forum/index.php/topic,939.0.html.

2. A window will pop up a couple times informing you that it is checking for updates. Eventually you will come to a window which will ask you if you want to install the Tor Browser. Click on “yes.”



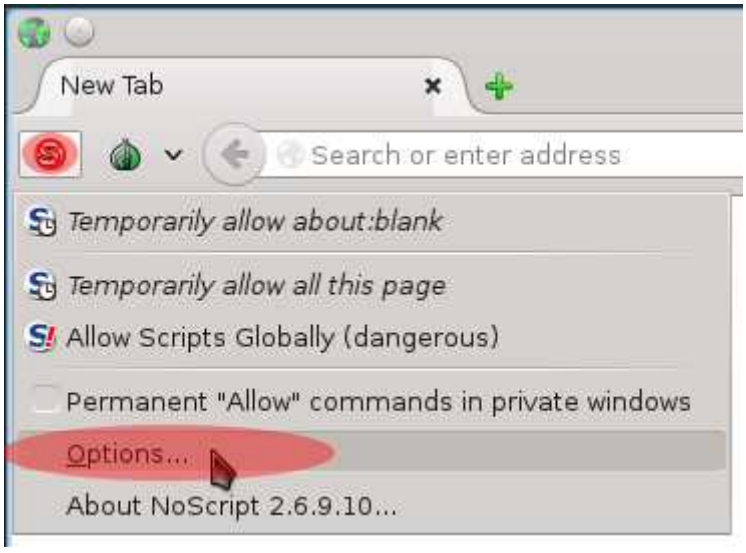
3. A new window will eventually appear informing you that you are downloading the Tor Browser. This process may take a few minutes. When it finishes, you will eventually come to a window which asks if you want to run the Tor Browser. Click on “yes.”



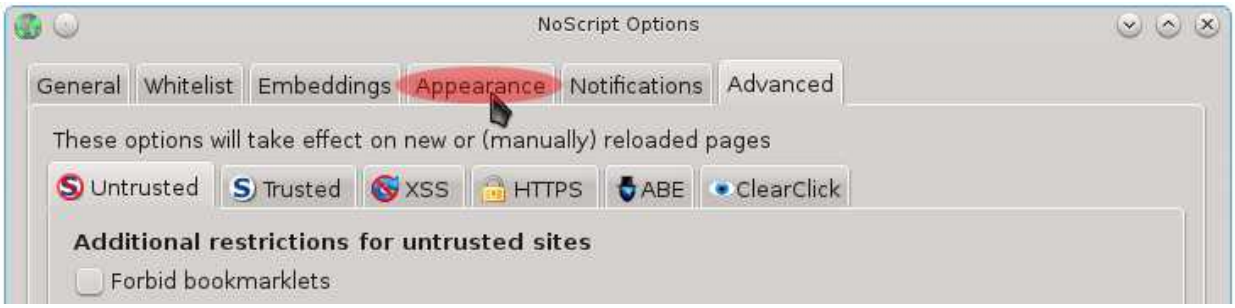
4. In the next window that appears, you need to disable javascript via the NoScript plugin. The NoScript icon will be to the left of the location bar in the browser and will look like the icon below.

Click on the icon and select “Forbid Scripts Globally (advised)”.

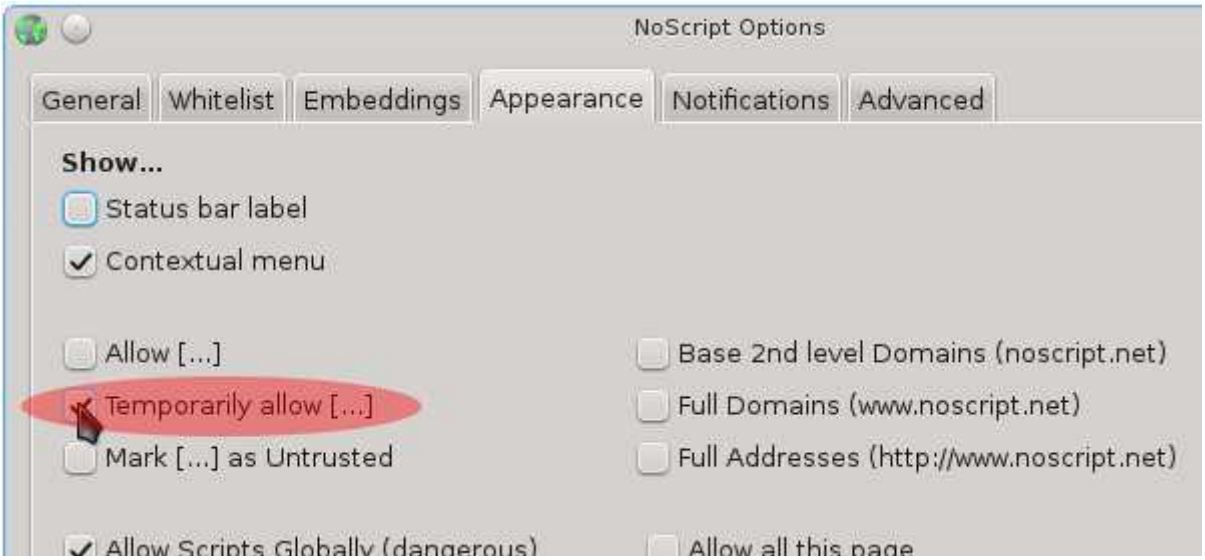
5. Now, click on the NoScript icon again and select “options.”



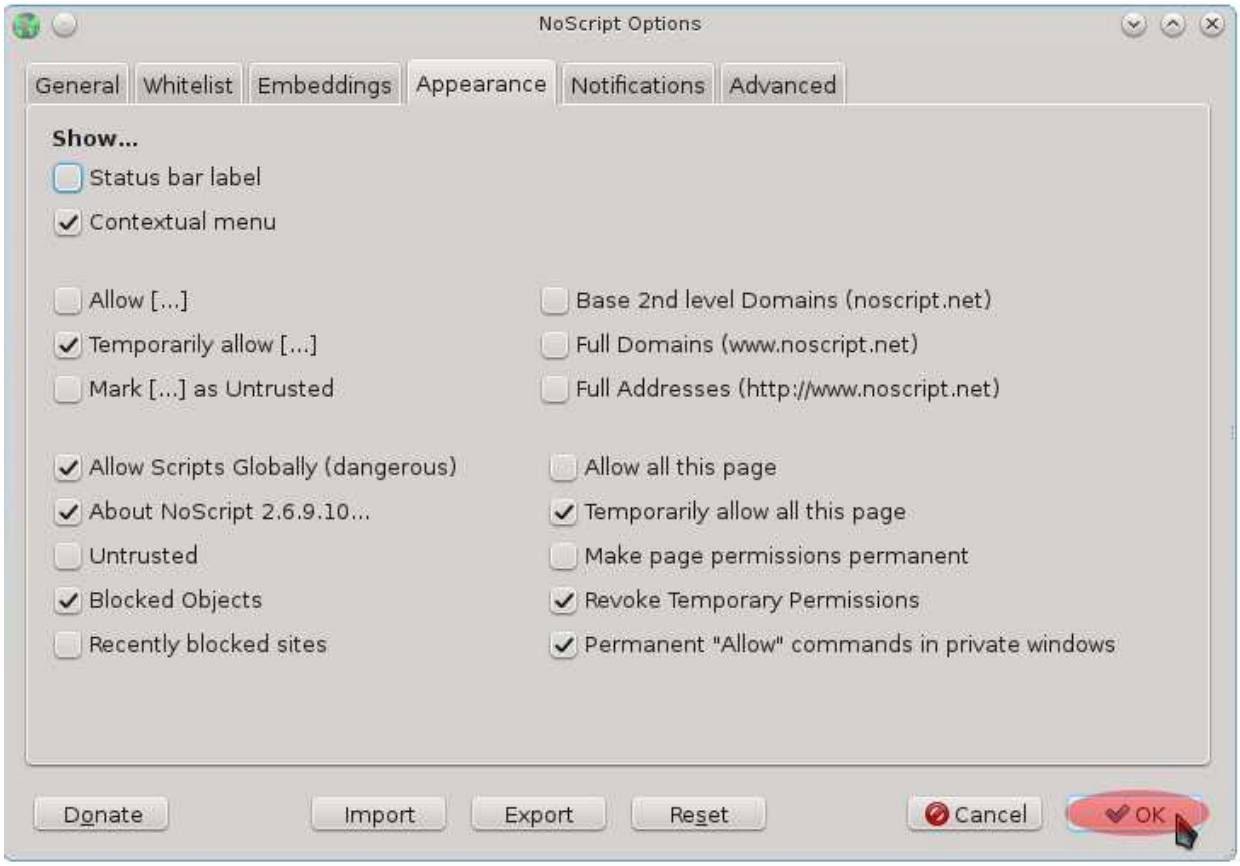
6. In the next window that appears, click on the “Appearance” tab.



7. Click on the box next to “Temporarily Allow [...]” so that a check mark appears in it. You want to enable this option.



8. Next, click the “OK” button to close the window.

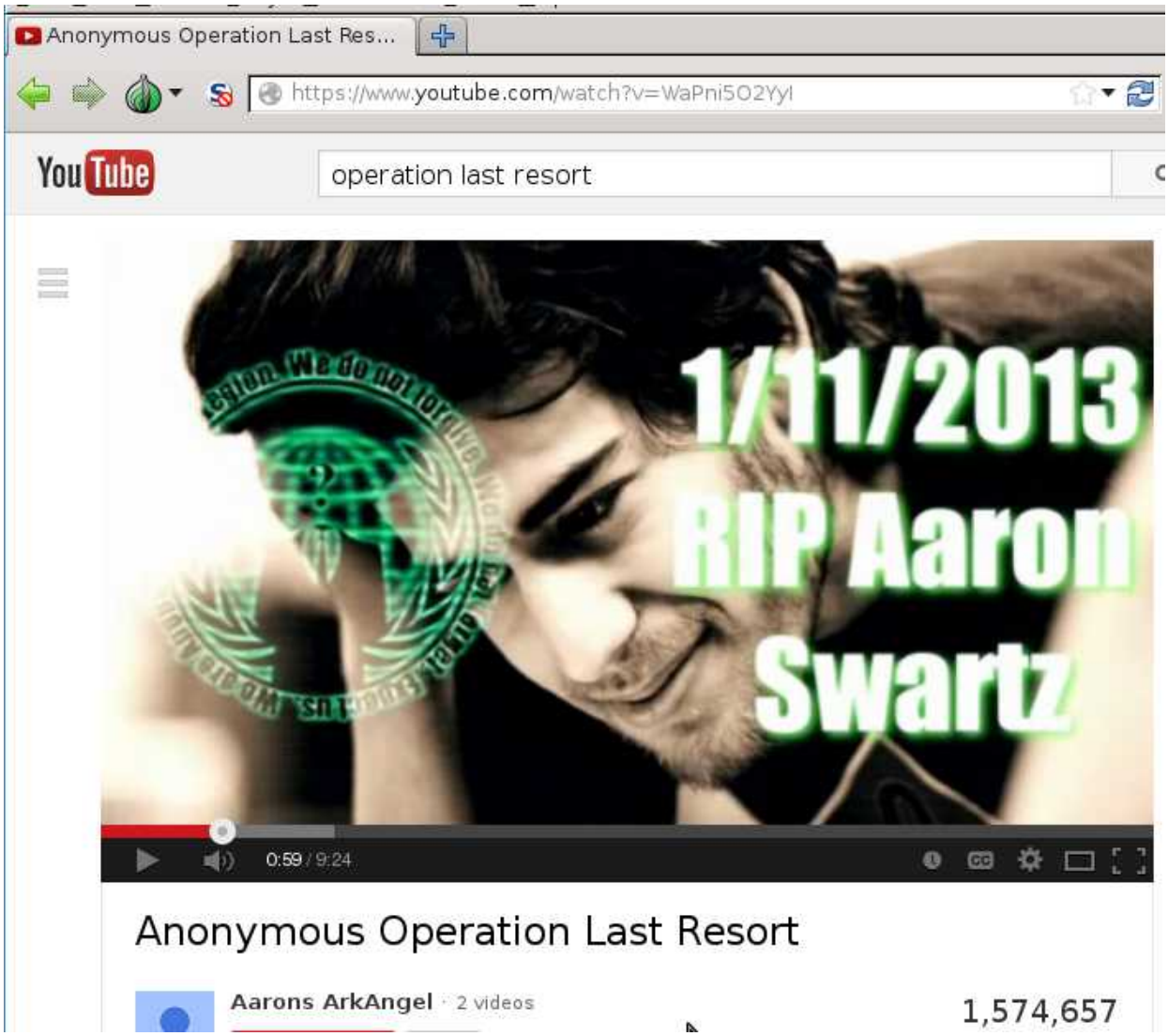


From now on, javascript, and other scripting, is disabled by default for every site you visit. Additionally, you will have the option to temporarily allow individual scripts to run on various sites. **However, whenever you update the Tor Browser, NoScript will be reset to enable all scripts. Thus, each time you update the Tor Browser, remember to disable all scripting again in NoScript and configure as described in the steps above.**

9. Now, try an example to get the feeling for how NoScript will work while you browse the web. By default, most browser scripting is disabled. This provides protection against various drive-by infections from sites hosting malware, obnoxious banner ads from advertisers, etc. At the same time, it will require you to take some additional steps to get web pages that rely on javascript to function properly. In Tor Browser, go to https://www.youtube.com/watch?v=WaPni5O2YyI

10. Notice that, aside from having a blank Youtube screen, you don't even see any player controls. This is due to the fact that NoScript has blocked scripting. Thus, you need to enable scripting from Youtube.com. Click the NoScript icon and click on “Temporarily allow https://www.youtube.com.”

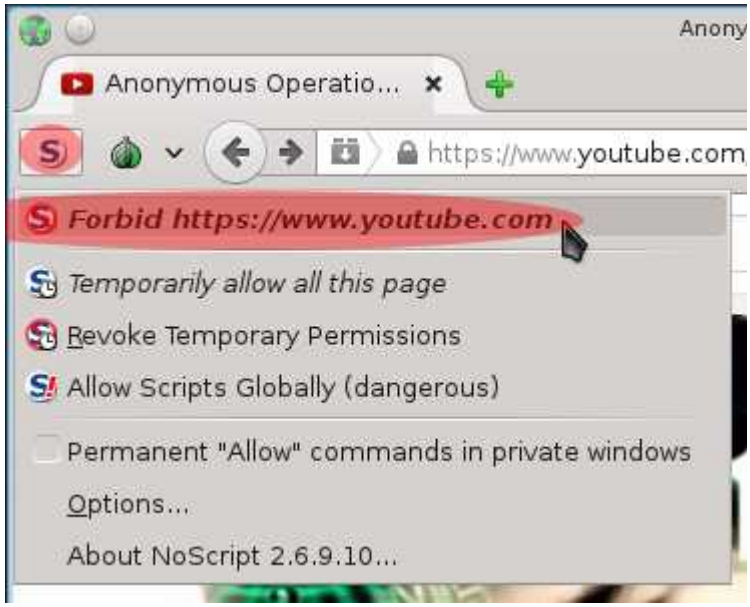
11. When the page reloads, eventually the video will begin to play.



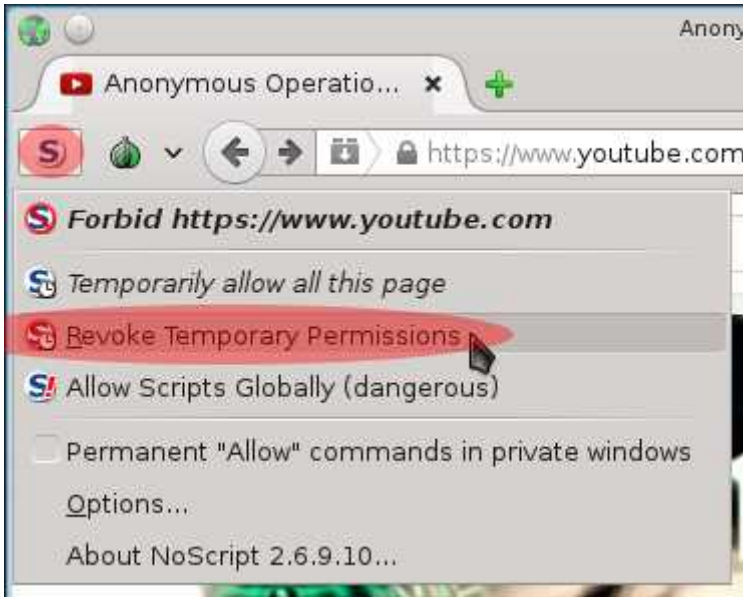
While the above example is specific to youtube.com, a similar process will apply to every other web page you use. If you browse to a site and find that it is broken in a way that makes it unusable, follow the steps you learned above with the quick reference below.

1. Be patient when learning what scripts need to run on various sites. **Start by only temporarily allowing the main domain name of the website in NoScript.**
2. When the page reloads, if it works the way you like, you are done. If not, enable other scripts that appear related to reload the page reload again with the additional chosen scripts allowed. Do this until you find a combination that works.
3. If you completely run out of patience, use the “Temporarily allow all this page” option in NoScript.

12. When you are done using the web page for which you temporarily allowed scripts to run, the safest and most secure thing to do is close the Tor Browser and open it again if you wish to continue using it. This will clear all of the temporary permissions you allowed in NoScript, in addition to clearing all cookies, temporary browser data, etc. However, if you prefer not to close the browser, you can disable the script permissions in NoScript the same way you enabled them. Click on the "NoScript" icon in your browser. Then, for every script that is enabled click the option to "forbid" it.



If that option is too tedious under the circumstances, there is also the option to revoke all temporary script permissions you've granted by clicking on "Revoke Temporary Permissions."



13. Once you have revoked the temporary permissions that you allowed for a site, you can either browse to a new site or close the tab. **The scripts will no longer be able to run on any new web page you visit.**

That's all there is to it. Keep in mind that, the less scripts you allow, the better. A solid majority of scripts serve no extra purpose other than for various online entities to send you ads or collect data about your browsing session. In the worst case scenario, it opens a vector to infect your computer. While Whonix provides protections against some of the pitfalls that come with being exploited by scripts, there is no reason to test fate. Thus, learn to live without scripting where possible. To run the Tor Browser in the future, there is both a “Start Tor Browser” icon on your Desktop, in addition to a quick launch icon next to the Start Button.

Chapter 4c. Using a Password Manager

Some of the most common mistakes people make involve the choice of a weak and easily crackable password and/or reusing the same password for multiple accounts. It can be a frustrating task for many people to choose different and complex passwords for every online account they use. However, without doing that, if one of their accounts gets compromised, the attacker will very likely have access to all of their accounts and will discover them shortly. Additionally, As of this writing, CNET has reported that both the United States NSA and FBI have been asking service providers for anything from individual user passwords to entire password databases.

No longer can the difficulty of remembering multiple complex passwords be an excuse for dangerous behavior. The simple solution to the problem is a password manager. In this chapter, you will install, and learn how to use, KeePassX, a secure and encrypted offline password generator and manager.

1. First, double-click on the “Konsole” icon on your Desktop.

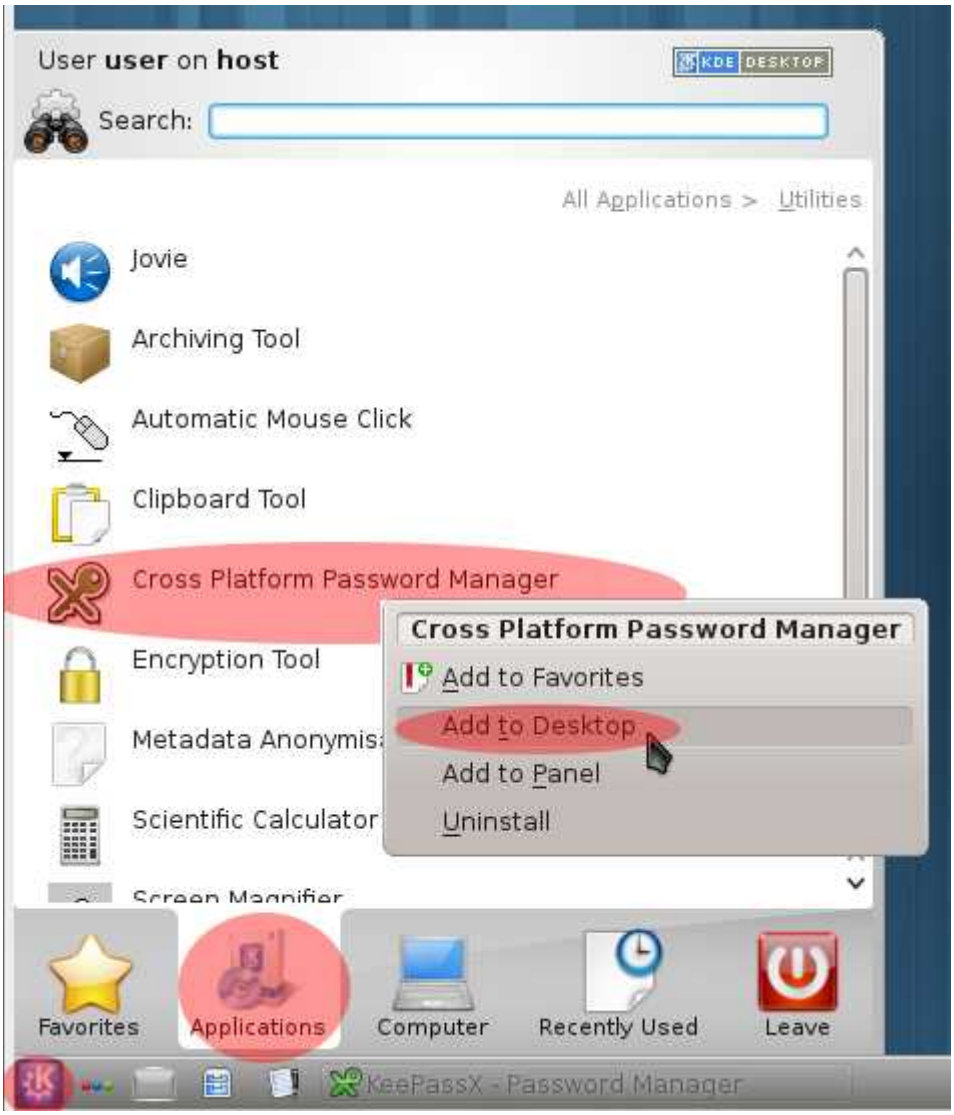
2. At the command prompt, type “**sudo apt-get install keepassx**” and press “enter.” Type your user password and press “enter” when prompted.

   NOTE: If you wish to use “copy and paste” throughout the guide for any terminal commands in the Whonix Workstation, and you are viewing this guide from within the Whonix Workstation, press “**LEFT-CTRL+SHIFT+V**” to paste what you copied from this guide into a terminal session.

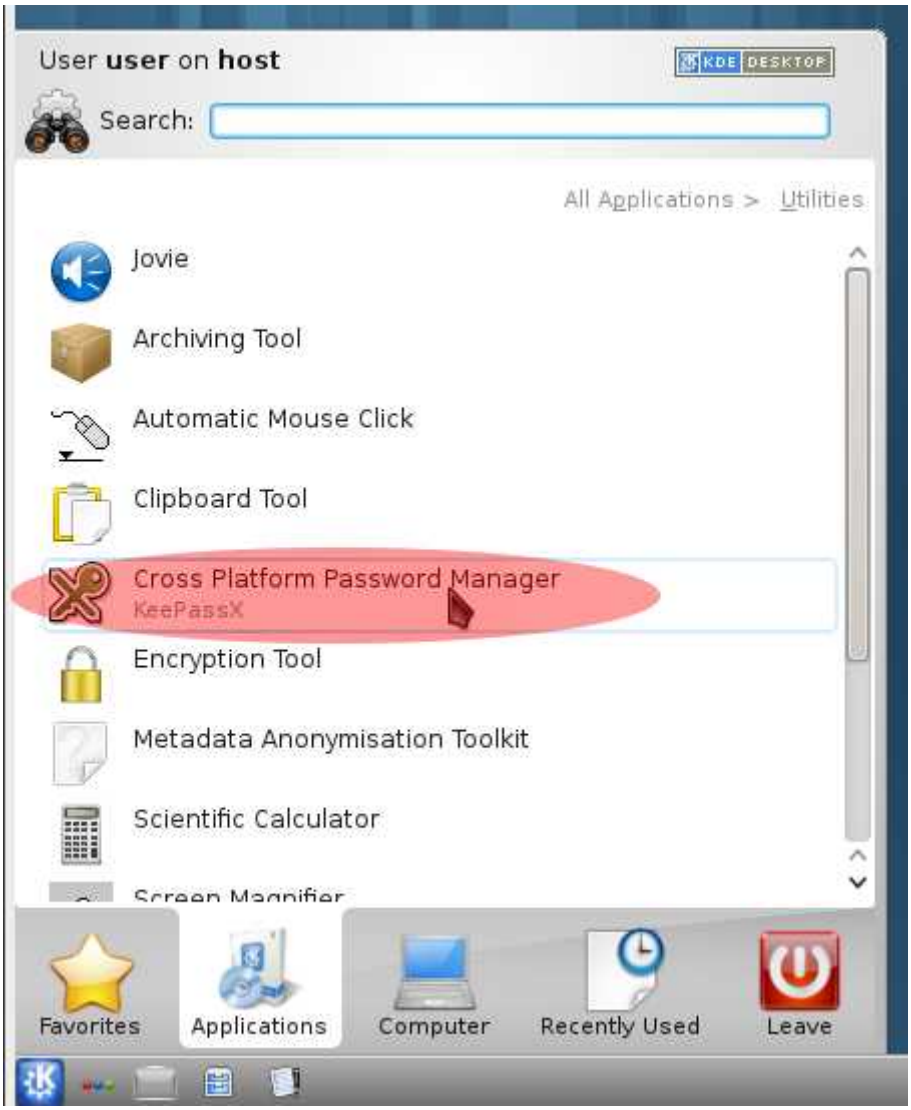
```
user@host:~$ sudo apt-get install keepassx
[sudo] password for user:
```

   When the install process finishes and you have a command prompt, you can close the Konsole terminal by typing “**exit**” and pressing “enter” or clicking on the “x” in the upper right corner.

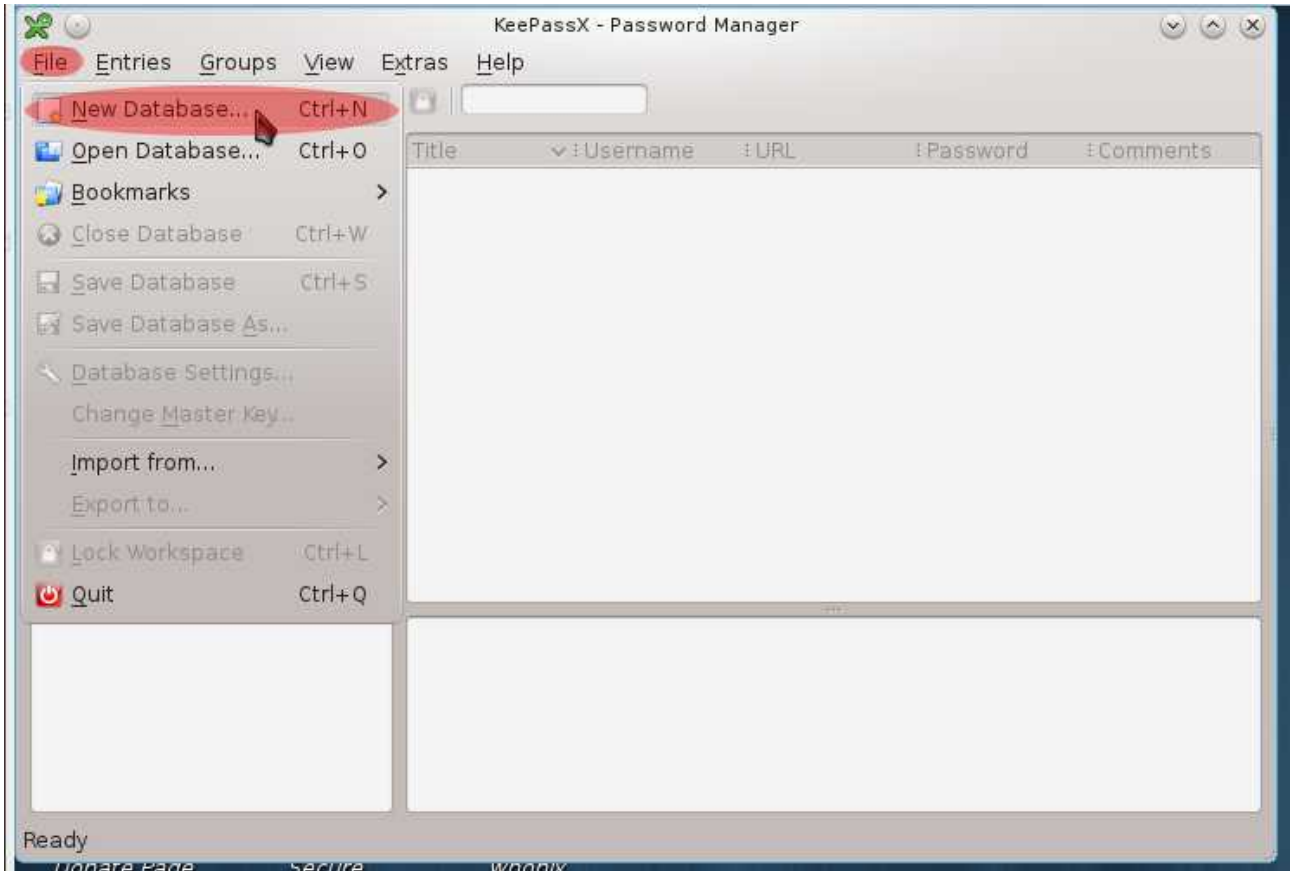
3. For simplicity, now add a shortcut for KeePassX to your desktop. Click on the K start button and go to "Applications → Utilities." Right-click on "Cross Platform Password Manager" and select "Add to Desktop." A shortcut to "KeePassX" will now be on your desktop.



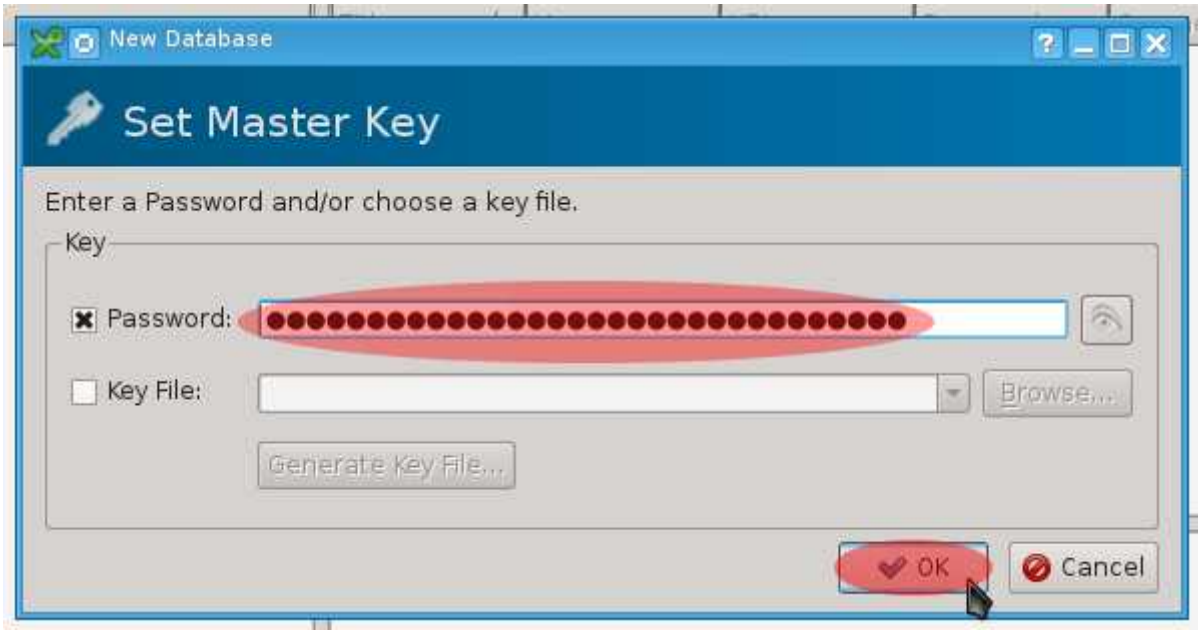
4. After you add the icon to the Desktop, the Start Menu will still be open. Click on "Cross Platform Password Manager" to open KeePassX.



5. When KeePassX opens, click on "File → New Database" to create your password database.

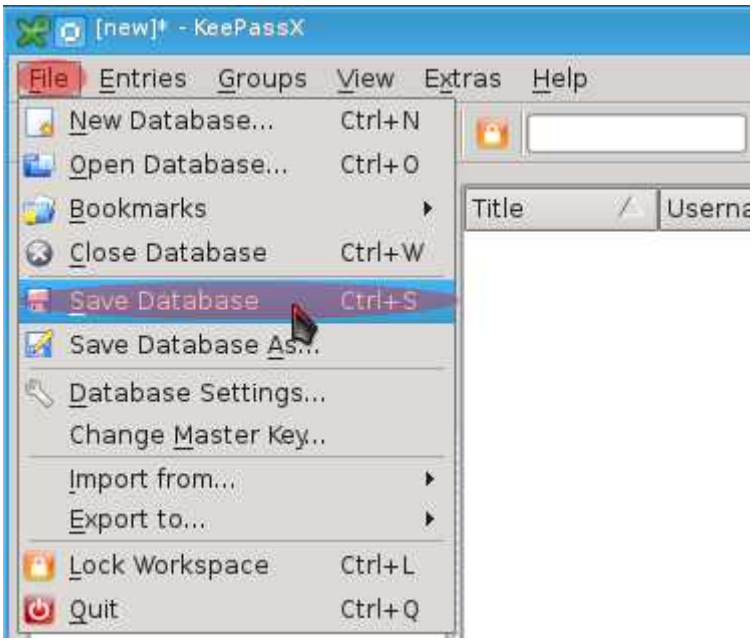


6. You will now be prompted to choose a password for your database. Choose something secure in a similar manner to how you chose passwords earlier in this tutorial and click "OK." **Remember that if you forget this password, you will not be able to access any of the passwords you store in the database.**

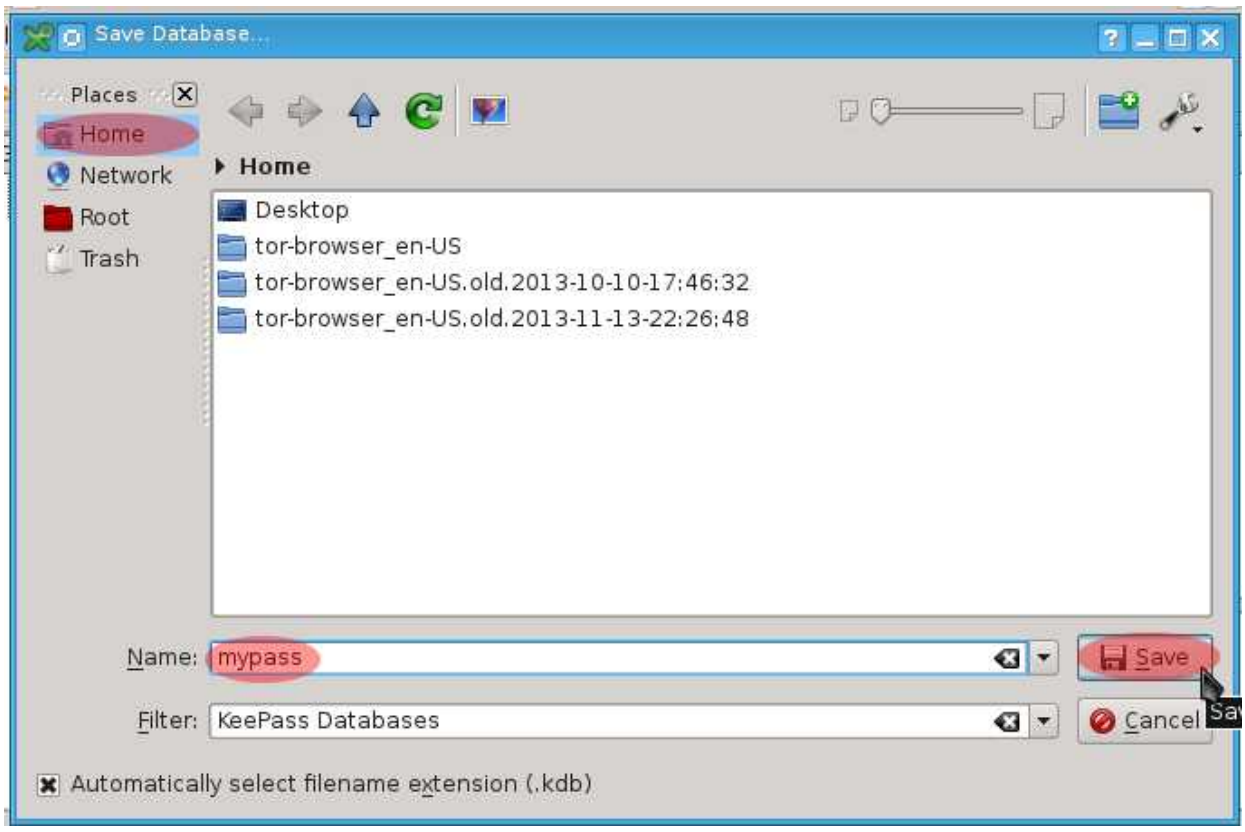


7. When prompted to confirm your password, re-enter what you chose in step 6 and click "OK."

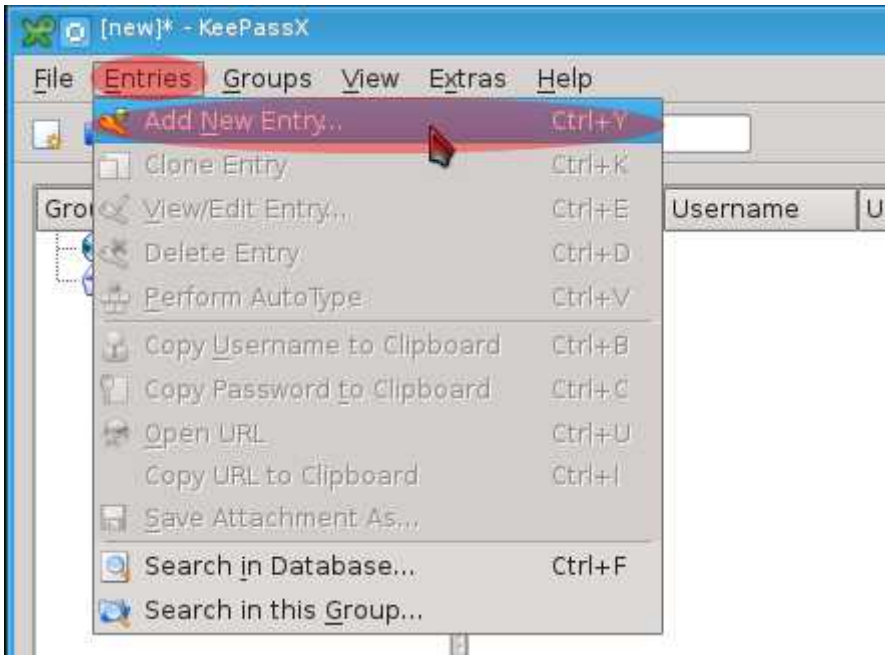
8. Next, save the database to create your database file. Click on “File → Save Database.”



9. Now, choose a safe location and file name for your password database. When you have chosen the location you want, click “Save.” In the example below, the database will end up being saved as “mypass.kdb” in the “home” folder. This database will open automatically the next time you open KeePassX.

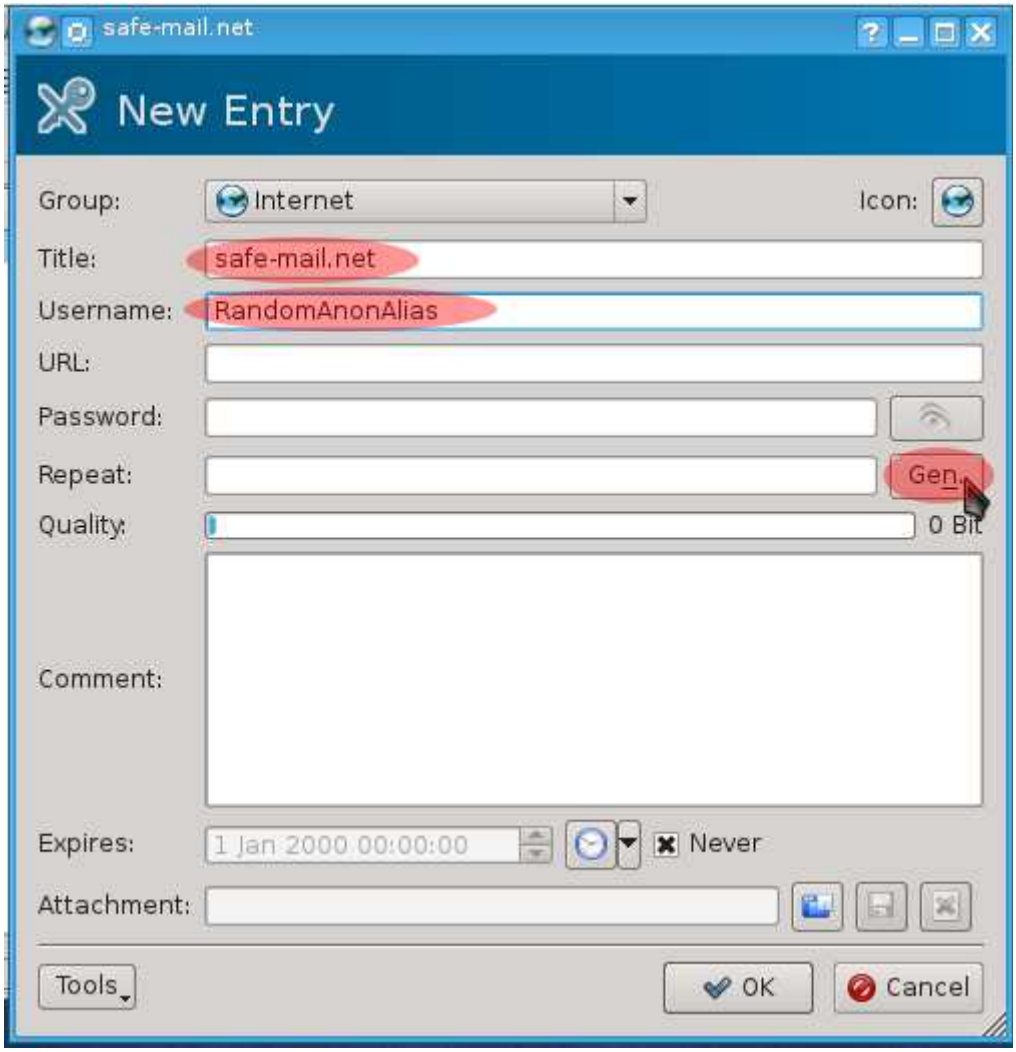


10. Create a new account entry in the password manager. Click on “Entries” in the menu bar and then click “Add New Entry.”



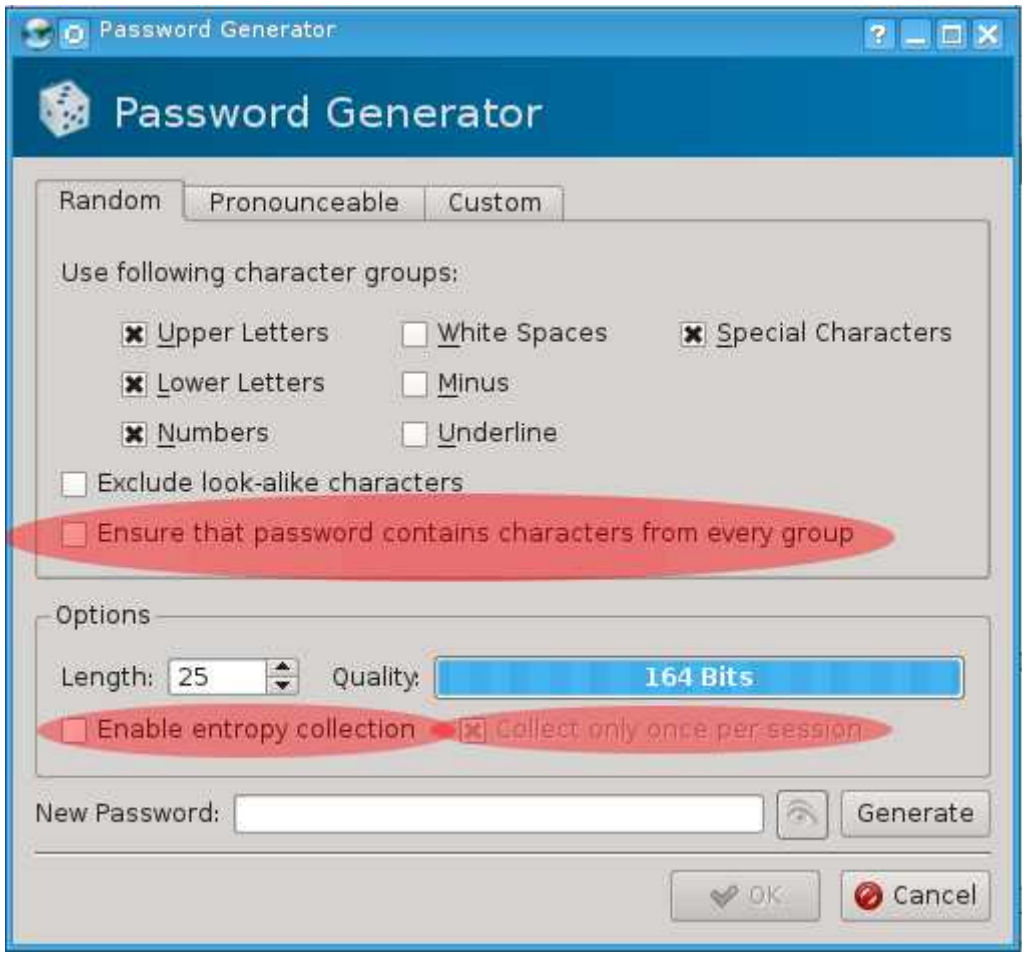
From this point forward, it may be easier to create a dummy account to learn how to use KeePassX. Open up Tor Browser and choose a site where you wish to create an account and use it where appropriate with these steps. An easy and quick one to use is “safemail.net.”

11. In the window that appears, type the name of the site/service in the field called “Title” and the username that you register with the Internet service/web-page in “username.” Then, click on “Gen” to go to the password generation screen.



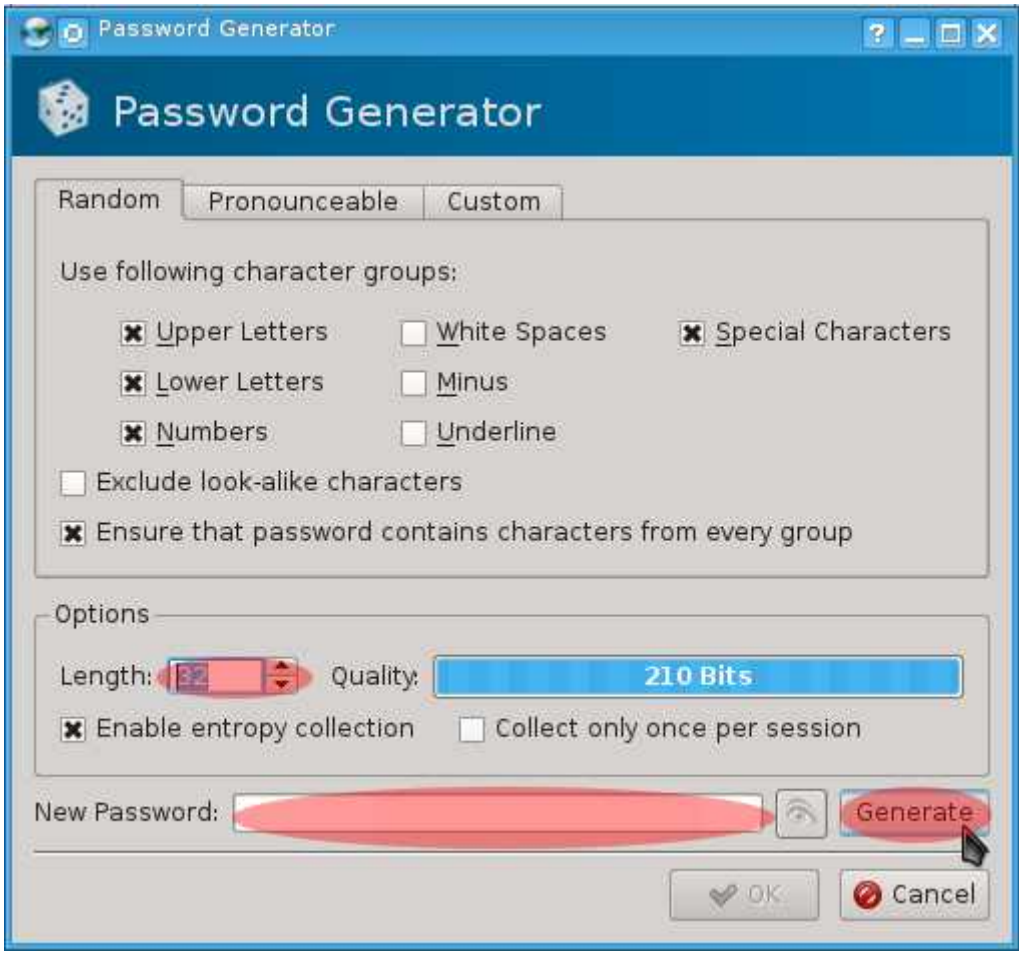
12. The “Password Generator” window will now appear and look like the one below.

    Click on the boxes next to “Ensure that password contains characters from every group” and “Enable entropy collection” so that those options are enabled. When it appears, uncheck the box next to “Collect only once per session” so that this option is disabled. These options will remain the way you set them for each additional use.

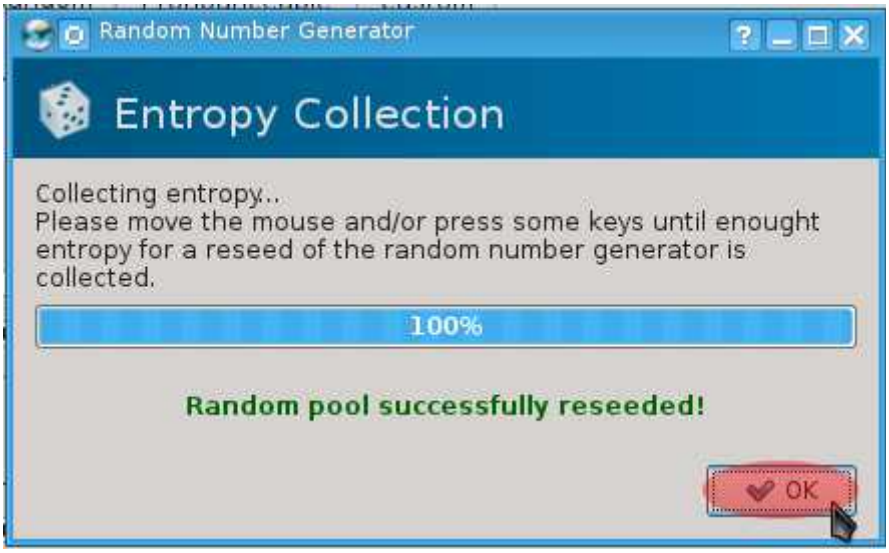


If your Password Generator now looks exactly like the one below, continue to the next step.

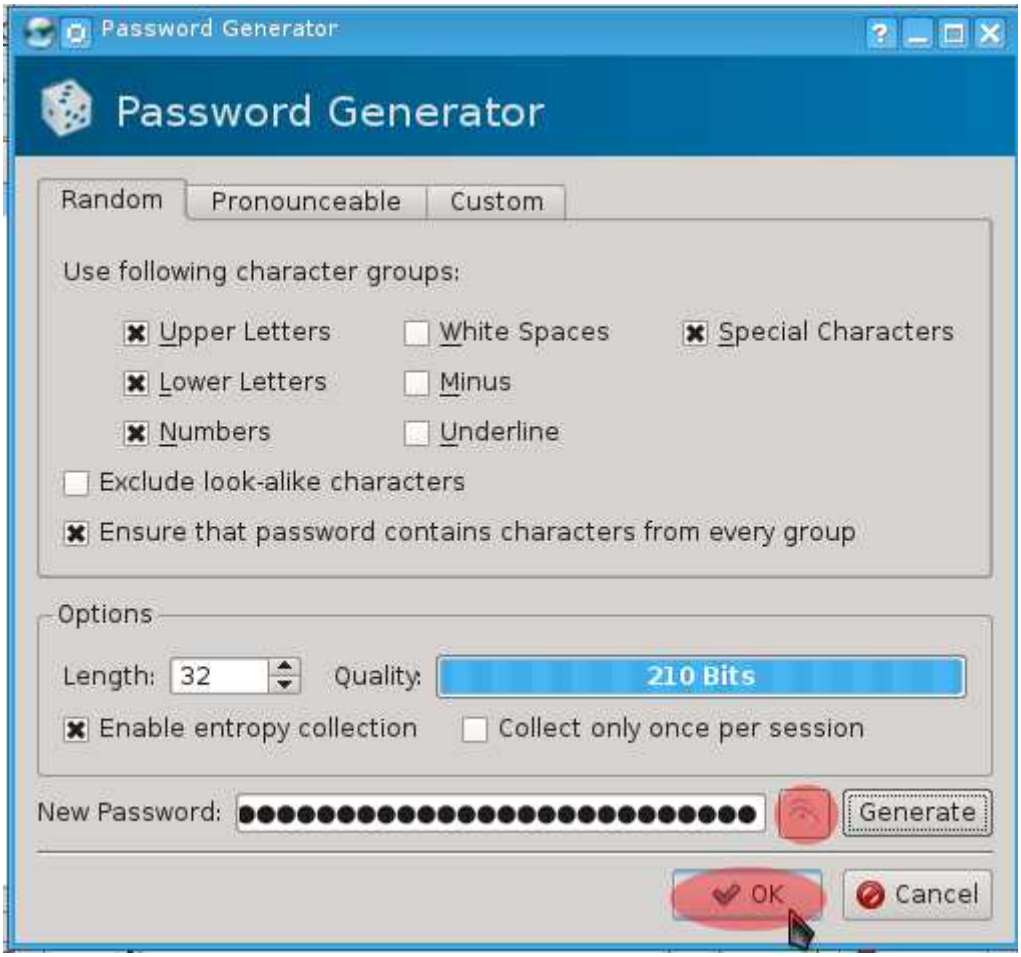
13. Next, select the length of your password. Since you do not need to remember your password (and may very well not want to ever remember it), you should ideally set the password to the maximum length that the service allows. However, to prevent against brute force guessing attacks, the default length of 25 above should be sufficient. When you've settled on a password length, click on the “Generate” button.



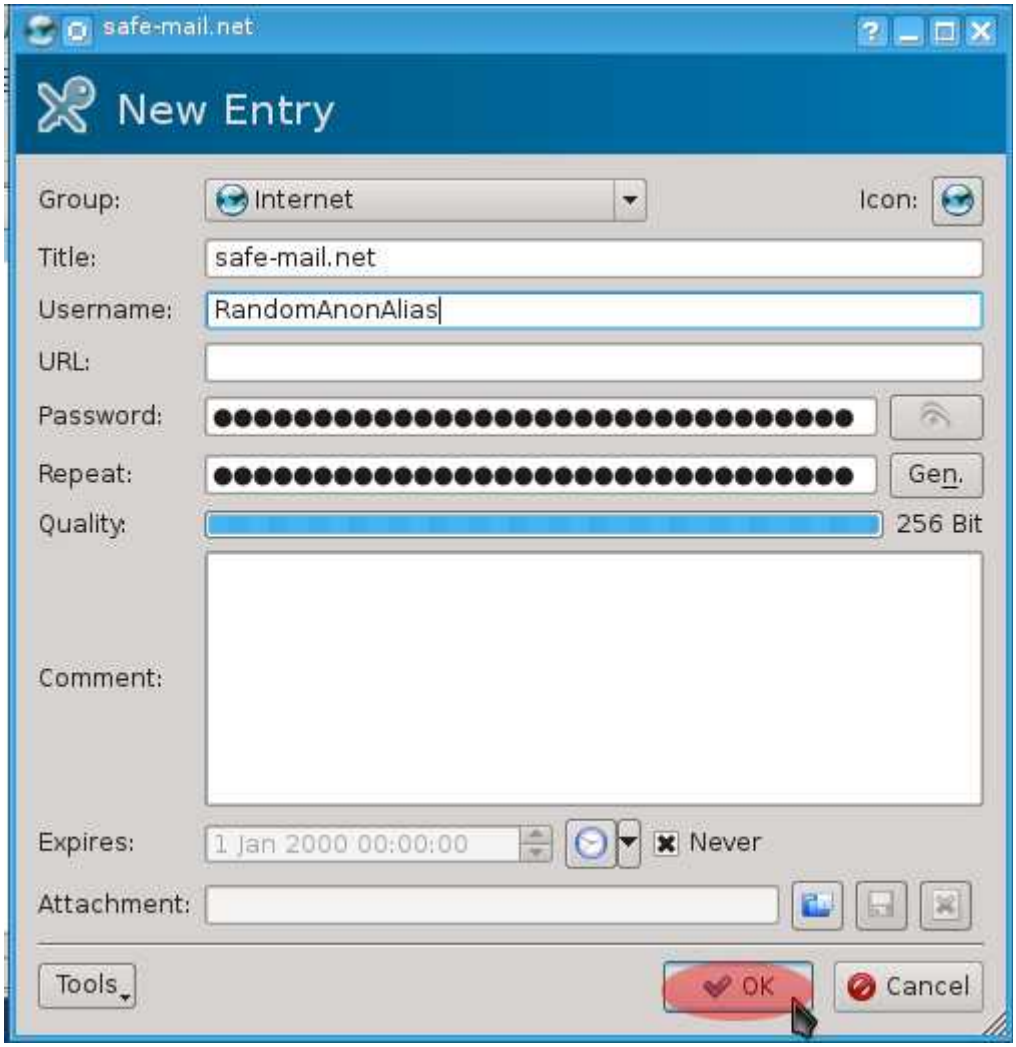
14. The “Entropy Collection” window will now appear. Move your mouse around and press random keys to generate an entropy pool for the password generator. When it is finished, click on the “OK” button.



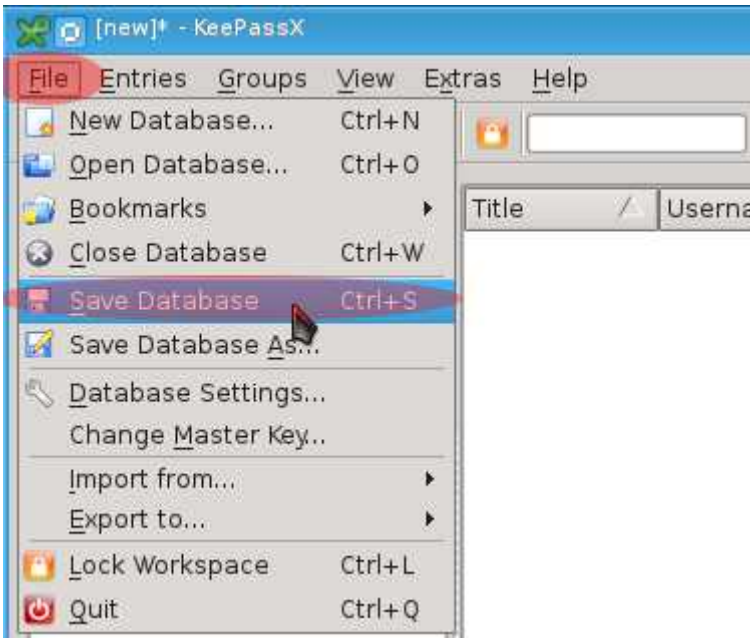
15. You will now be back at the Password Generator window. If you are curious to see what your password looks like, you can click on the eyeball button next to the “New password” field. Otherwise, click on “OK” to continue.



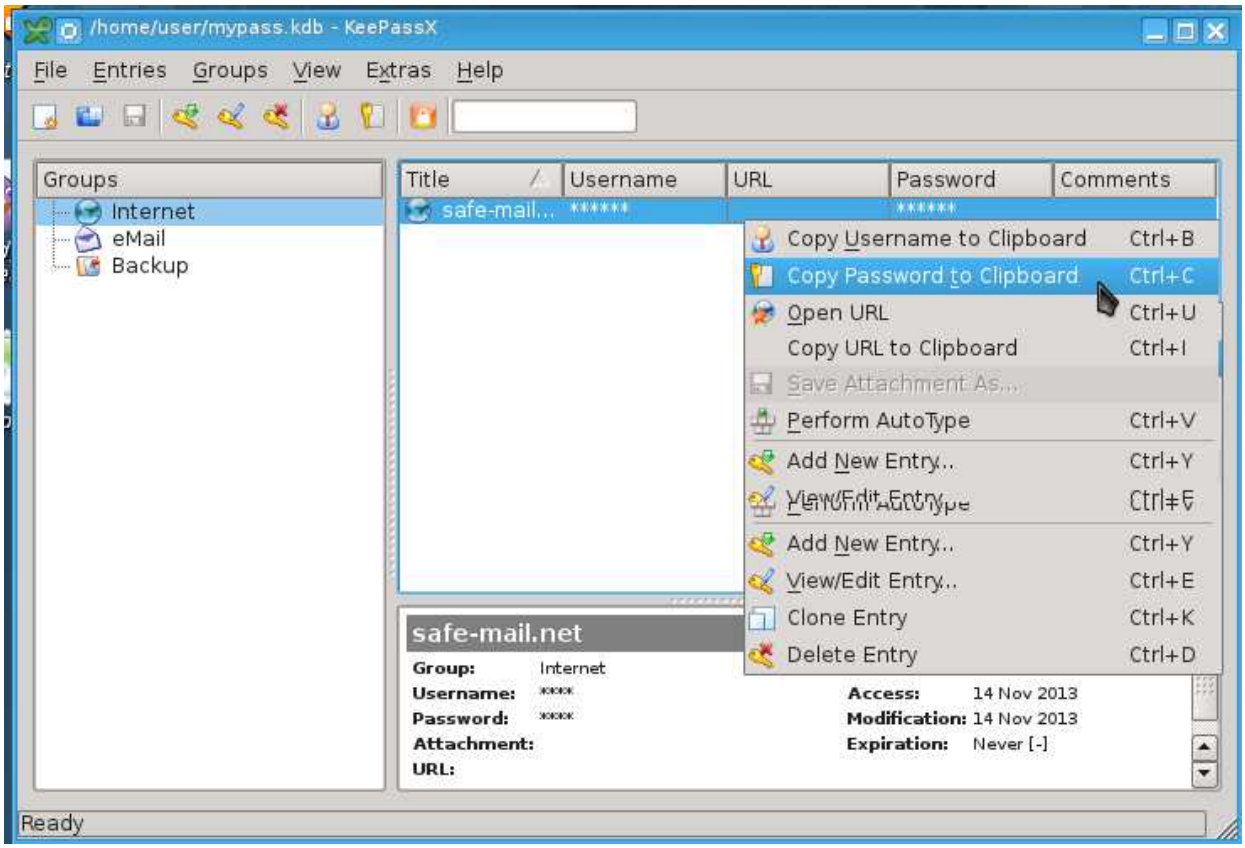
16. Now you will be back to the “New Entry” screen. Click on the “OK” button to continue.



17. You will now be returned to the main screen of KeePassX. It is a good practice to save your database whenever you add a new account and password to KeePassX. Thus, click on "File → Save Database."



18. Now, whenever you need the password for an account, you can highlight the entry in KeePassX and press "**LEFT-CTRL C**" or right-click on it and select "Copy Password to Clipboard." The password will be automatically cleared from your clipboard in 20 seconds.



If you were creating an account to follow along with these steps, now would be a good time to test out using the password on that site. To use the password on any service, simply click in the password field that it provides and press "**LEFT-CTRL V**" to paste the password in.

19. When you are finished using KeePassX, close it. There's no reason to leave it running the whole time.

This concludes the basic instructions on using KeePassX in a secure manner. Use of KeePassX as instructed above will result in passwords that are at low risk of being cracked by an attacker, while also being individually unique to every service you use. It greatly minimizes the fallout one can experience if an account they own is compromised and, thus, is one of the better models to use.

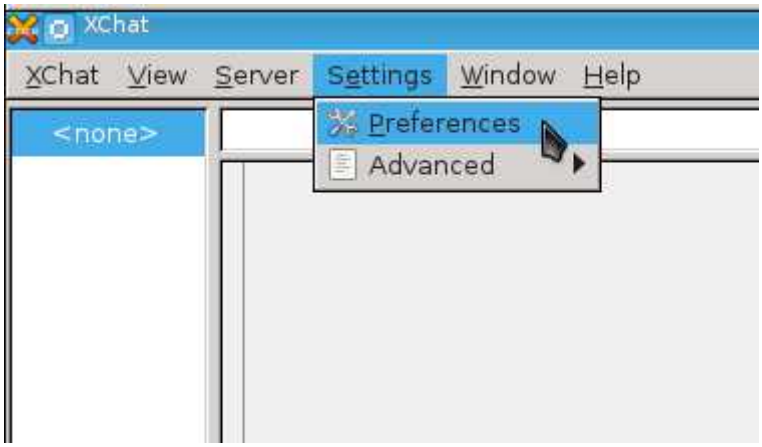
Chapter 4d. Using the IRC and XChat

The Internet Relay Chat (IRC) is one of the best available technologies for real time group conversations. Numerous different IRC networks exist that cater to multiple general interests to incredibly niche interests. However, it is also a technology where a number of people who are concerned about their privacy or anonymity have gotten exploited or have shot themselves in the foot. This chapter will give you basic instructions on how to get started safely using the IRC.

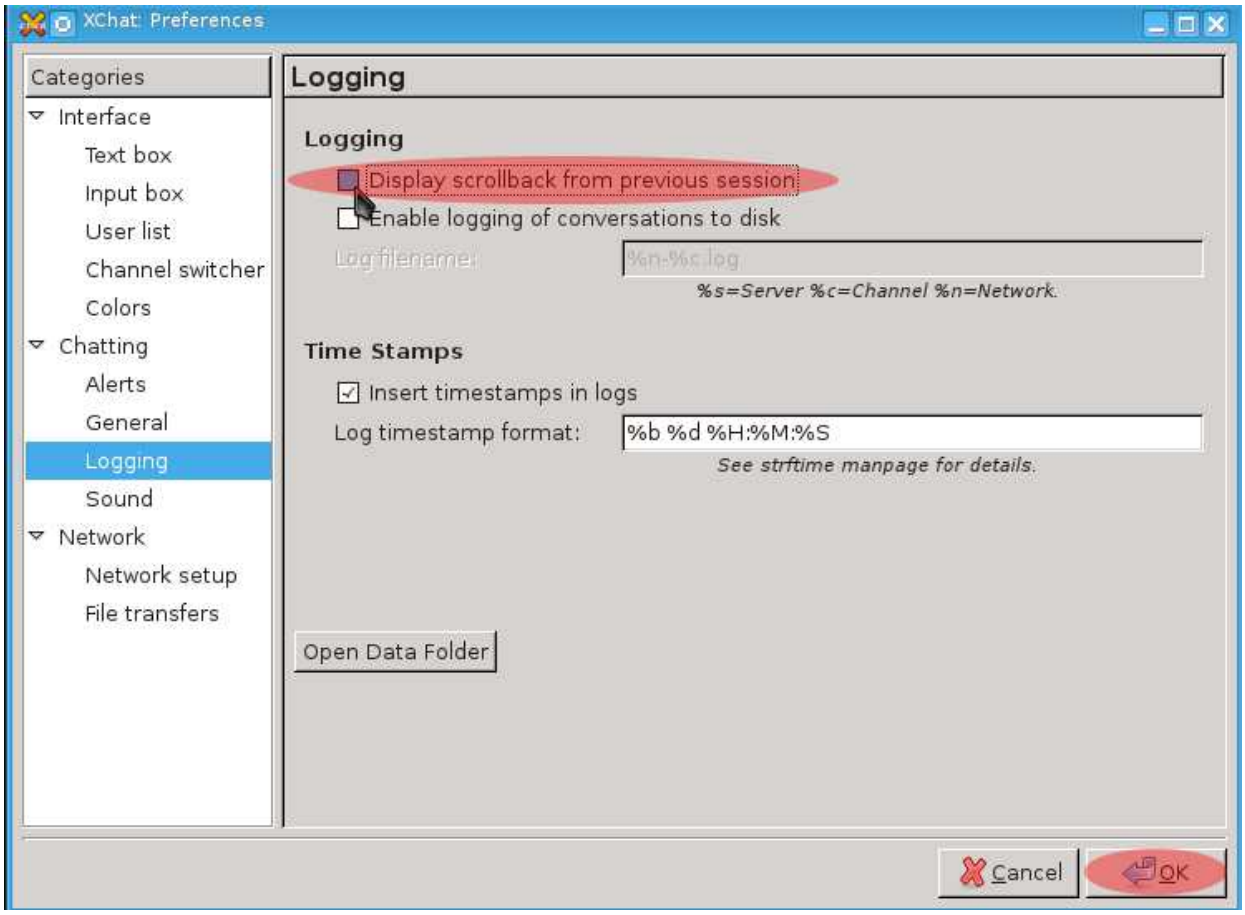
XChat is a graphical IRC client that comes pre-installed with Whonix. As a result, most of the settings that leave people vulnerable have been appropriately set by the Whonix developers. Additionally, since all of your traffic is routed through the Tor network, this adds another layer of security and anonymity to your IRC experience that simply didn't exist in the past. However, one down side is that a number of IRC servers have intentionally blocked any incoming connections from Tor. Circumventing the Tor blocking measures is a trivial task, but not a matter that will be covered in this chapter. Instead, let's get you on a server that welcomes and embraces the Tor Network where you can chat with us.

1. First, double-click on the “XChat IRC” icon on the Desktop.

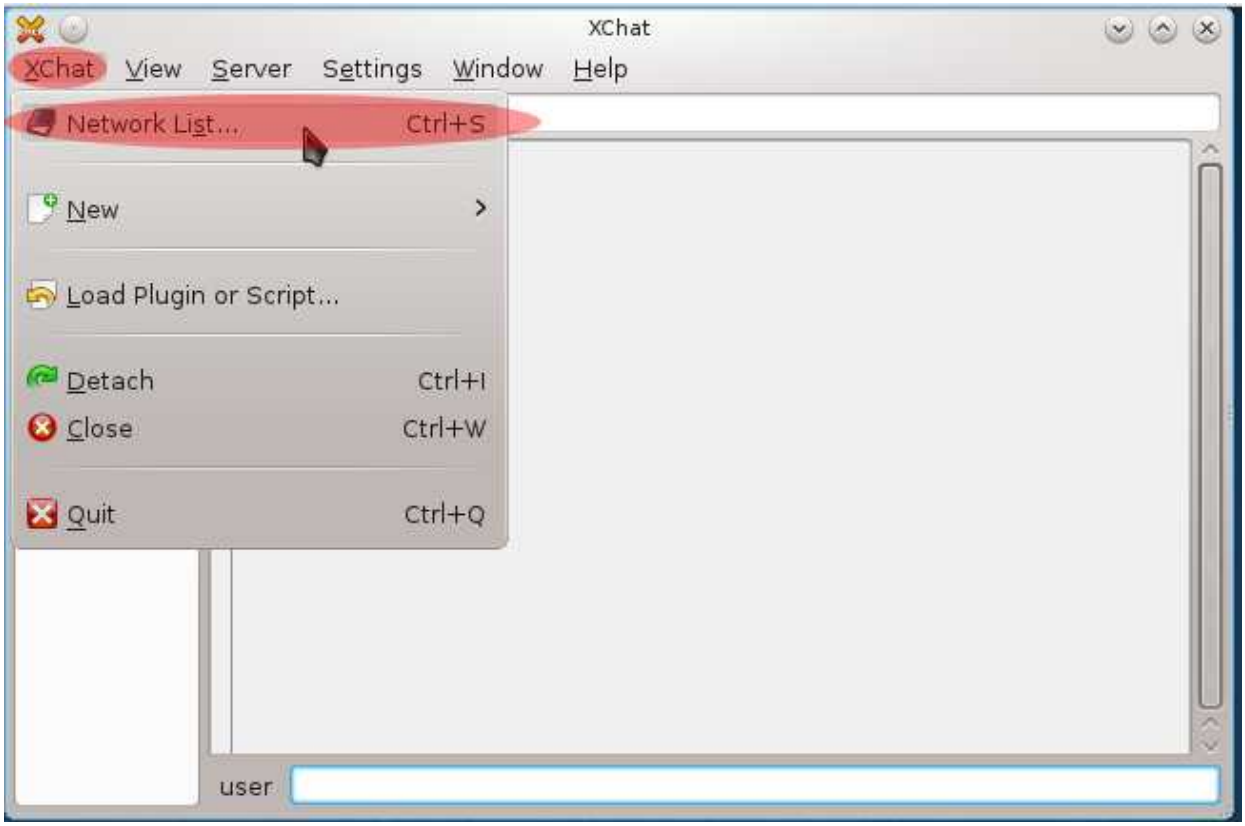
2. Now, you need to tweak one setting before doing anything. In the window that opens, click on “Settings → Preferences.”



3. Click on the “Logging” tab and uncheck the box next to “Display scrollback from previous session” and then click the “OK” button. If you do not do this, your system will log your previous sessions automatically. If your computer is ever compromised, this could be data that you would not want to be discovered.

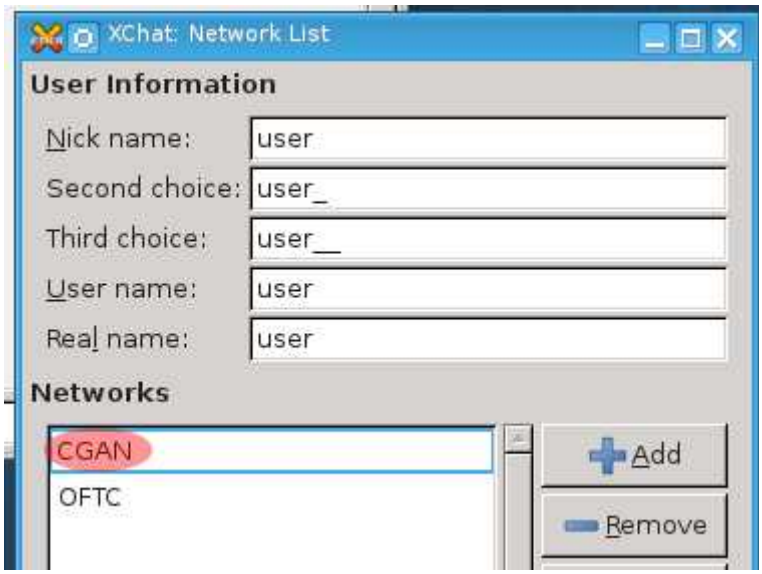


4. When you are returned to the main XChat screen, click on the “XChat” menu and then click “Network List.” This will open up the Network List window which stores profiles for any IRC server you desire to use.

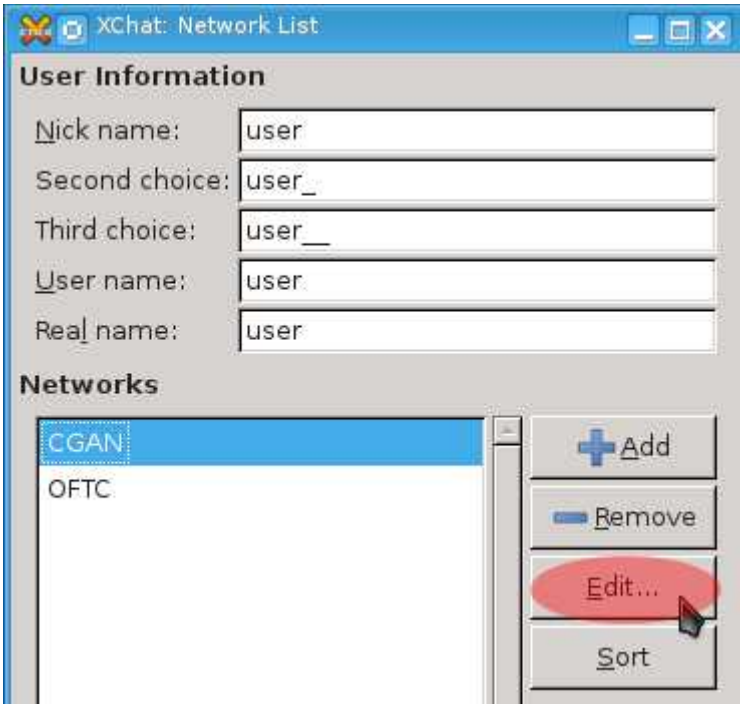


5. In the “Network List” window that appears, click on “Add.”

6. A “New Network” profile will be created and highlighted in blue. In this example, type “**CGAN**” and press “enter.” This will be the profile for the Cyberguerrilla Anonymous Nexus.

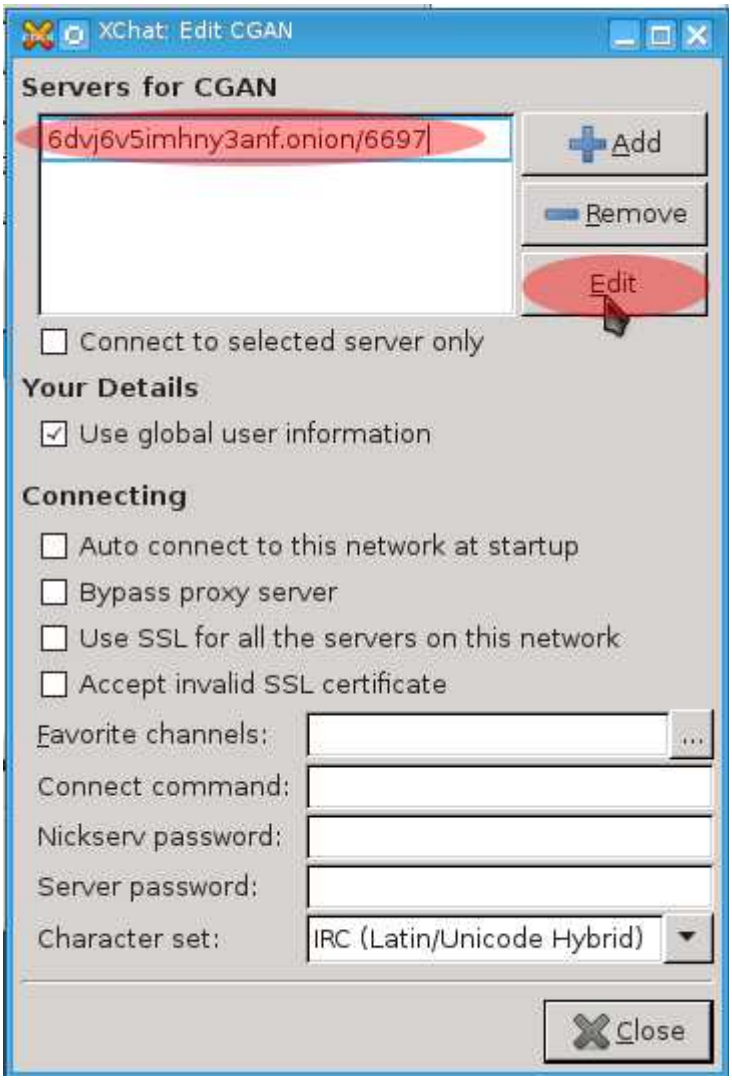


7. Next, click the “Edit” button.



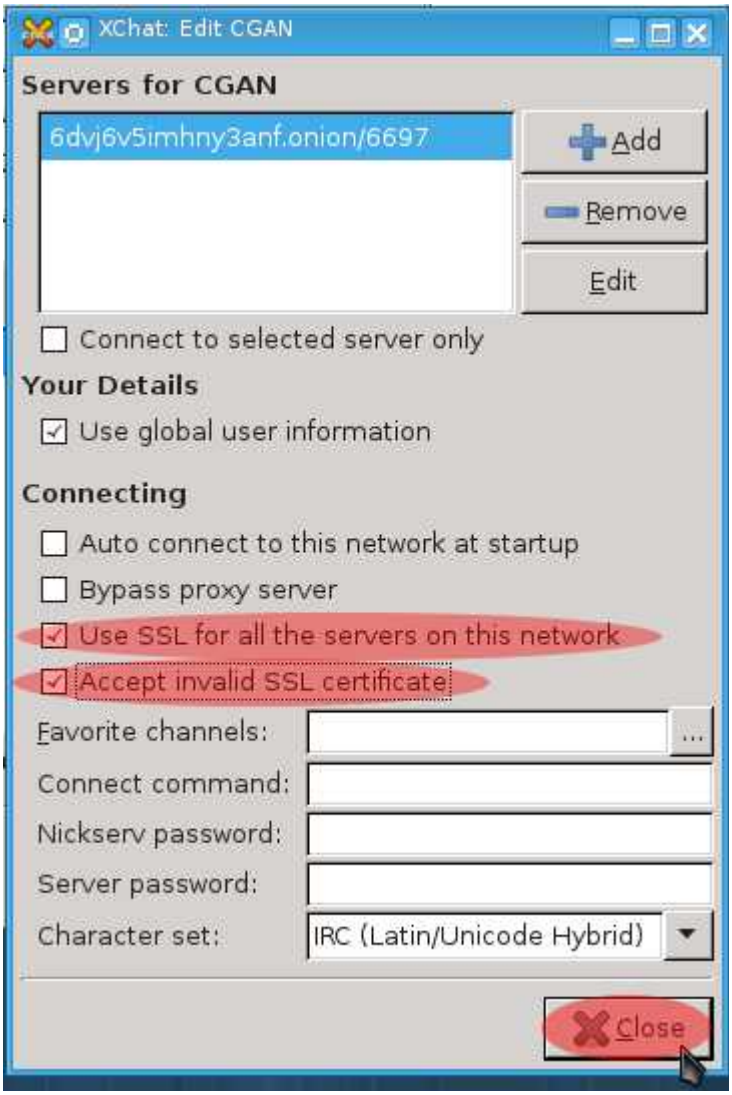
8. In the next window that appears, click on “Edit.” Then, type “**6dvj6v5imhny3anf.onion/6697**” and press “enter.”

   That address probably looks odd to you. This is a special address that is only available over the Tor network. When connecting to a server with a “.onion” address on the Tor Hidden Network, not only is your data connection encrypted between you and the server, you also get greater anonymity protections than you would by merely connecting to a standard Internet address like “cyberguerrilla.org.” **Whenever you have the option of connecting to a hidden service (a domain with a “.onion” suffix) for communication while using Whonix, , whether in IRC or for any other service, use it.**

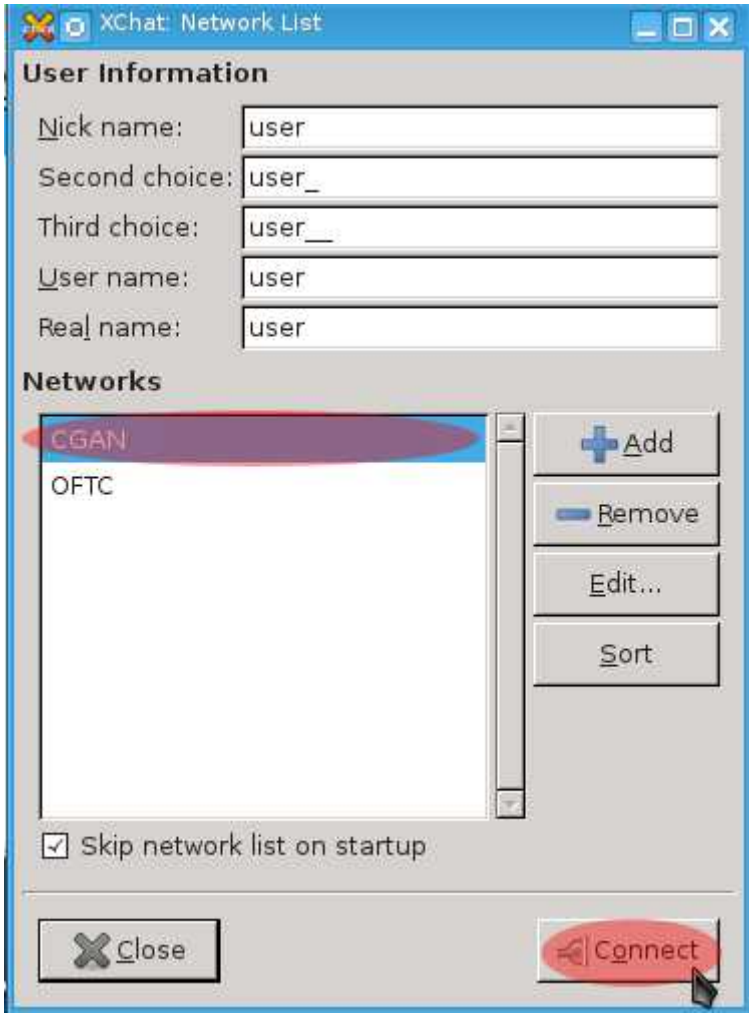


9. Now, click the check boxes next to “Use SSL for all the servers on this network” and “Accept invalid SSL certificate.” If your window looks like the screen shot below, click “Close.”

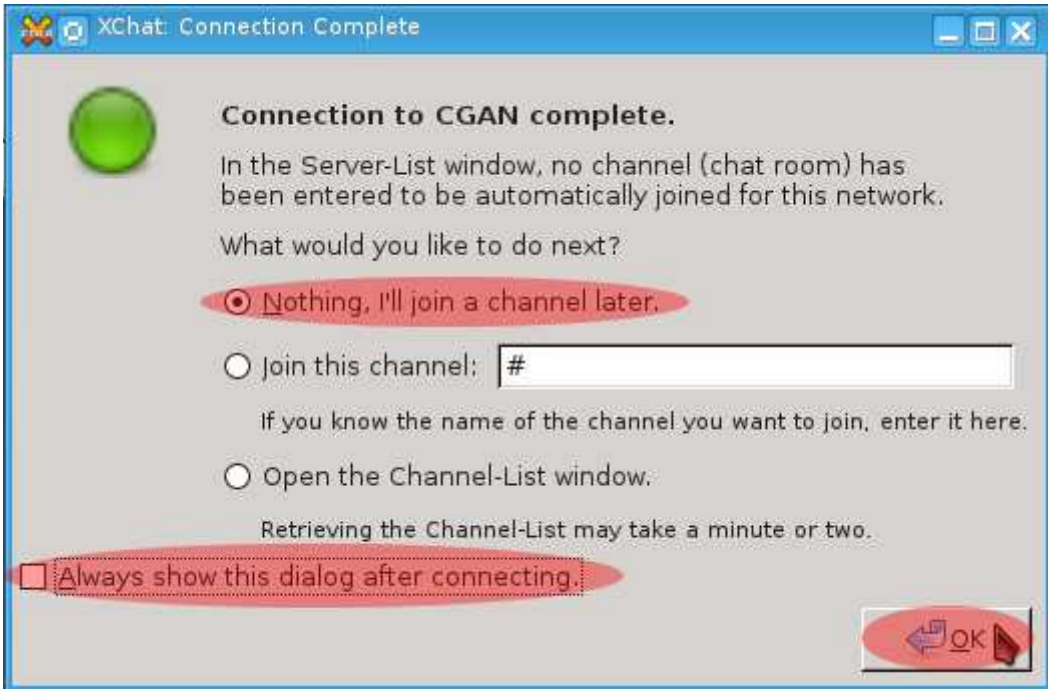
   Note: If possible, always enable the “Use SSL for all the servers on this network” option. This will encrypt the data between your computer and the IRC server. If XChat complains about the SSL certificate not being valid, this is either due to the IRC server being compromised or, in most cases, the IRC server using a self signed SSL certificate (which is not something you need to worry about). When connecting to a “.onion” address, lack of SSL encryption between you and the IRC server is not something that needs to concern you since the entire connection will be encrypted by the Tor Network.



10. Next, click on “CGAN” and then click on the “Connect” button. This will connect you to the CGAN IRC server.

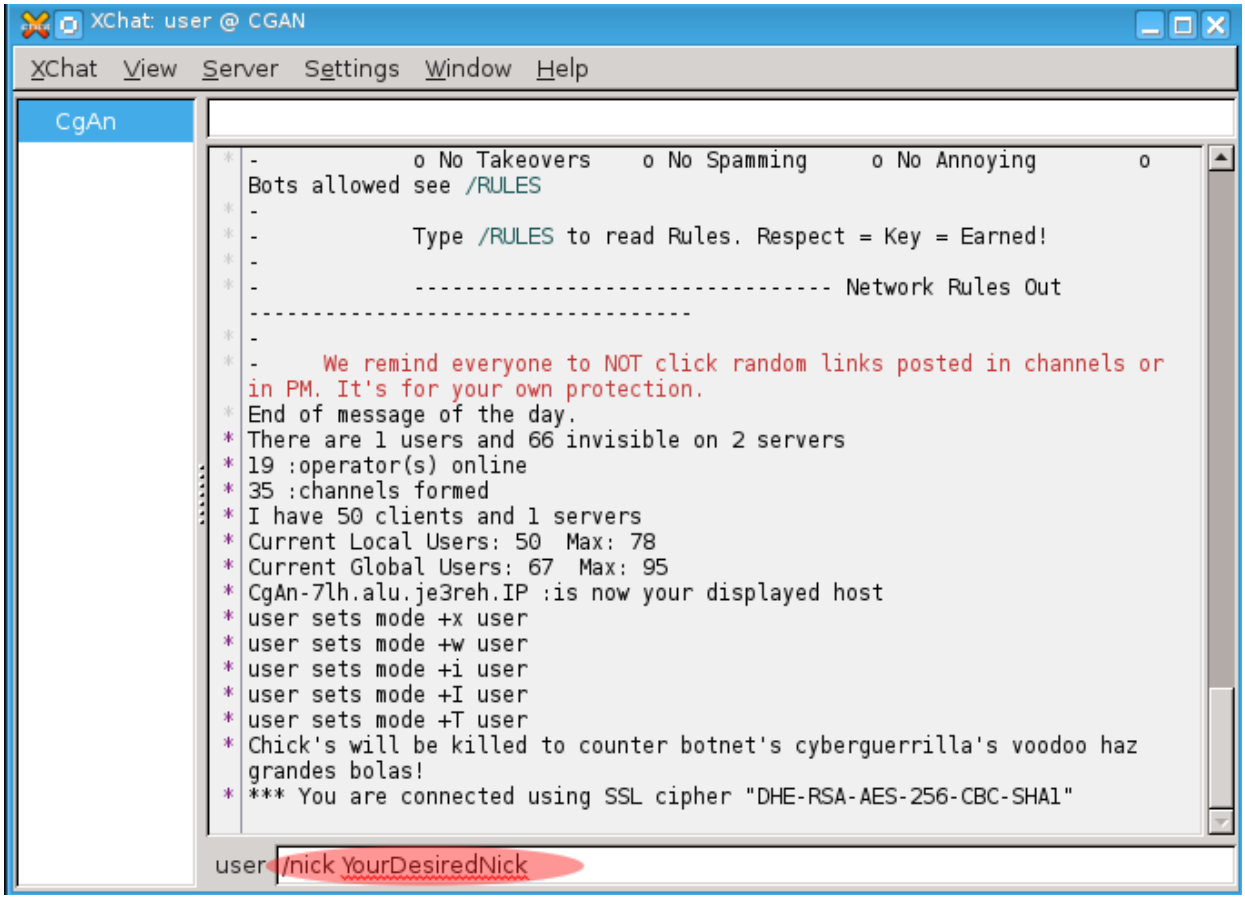


11. When you connect to the server, the “XChat: Connection Complete” window will appear. This window can be more of a nuisance since, due to the instructions provided here for using systems anonymously, it's of little use to you. Click on the circle next to “Nothing, I'll join a channel later.” Then, uncheck the box next to “Always show this dialog after connecting.” When the window looks like the one below, click the “OK” button to continue.



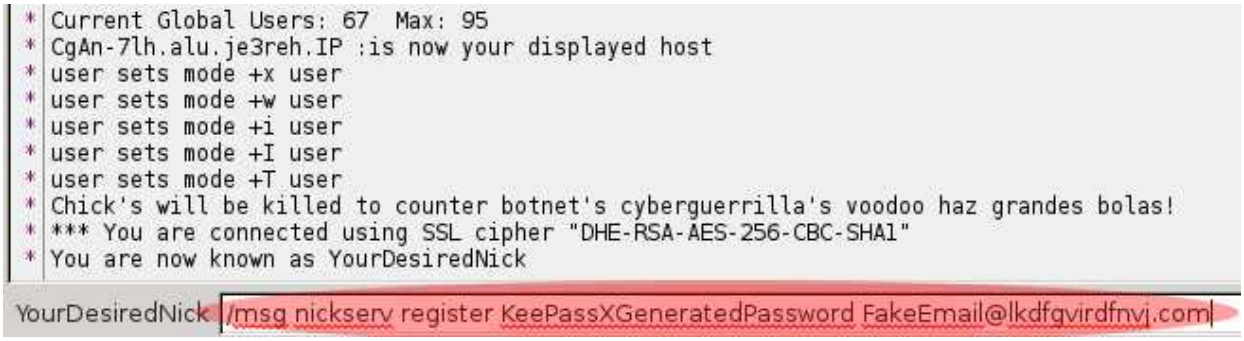
12. Now, change your nickname. It will default to “user.” To change your nick name, in the white bar next to “user” at the bottom of the window, type “**/nick YourDesiredNickname**” and press “enter.”

    Note: Never choose a nickname that can be correlated to your real identity! This means not to use any nickname which you've used or have been known by, whether it is something your parents or friends called you or an alias you used online.



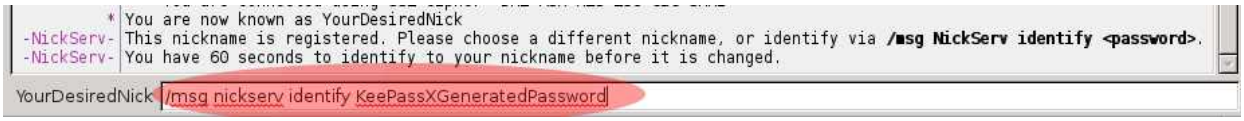
13. If you intend to use this nickname again in the future, or if you want to take advantage of additional identity masking by using a vhost (**which you should and which will be discussed in step 14**), you should now register your nickname. To do this, you need to send a specific message to the IRC server's "nickserv" service which will supply a password you wish to use and a fake email address. Type "**/msg nickserv register [Password made with KeePassX] FakeEmail@lkdfgvirdfnvj.com**"

    Note: Use KeePassX to create a password and save it in its database along with the nickname you chose.



    If you successfully registered your nickname, the server will send you a message stating "**YourDesiredNick** is now registered" as shown below.

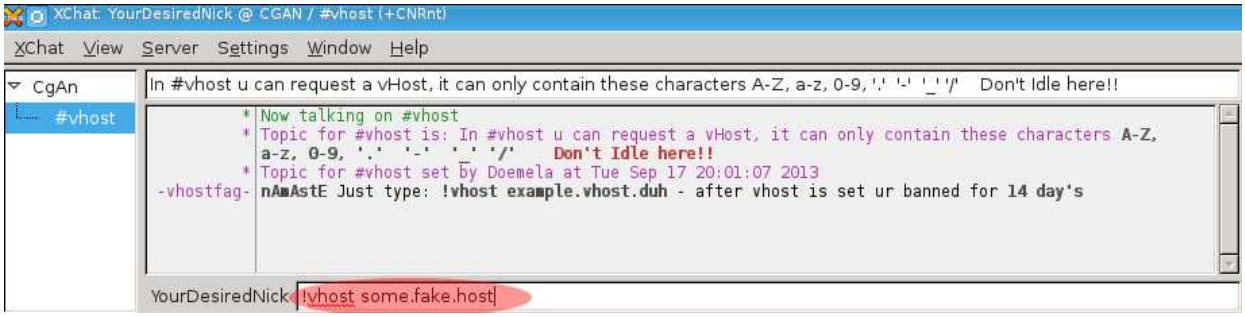
    In the future, when you choose the same nickname after connecting to the IRC server as you did in step 12, **you must supply the Nickserv with the password you set in the instructions above.** If you do not, the server will change your nickname to something else in a certain period of time. To let the server know that you are the owner of a nickname type "**/msg nickserv identify KeePassXGeneratedPassword**" and press "enter."



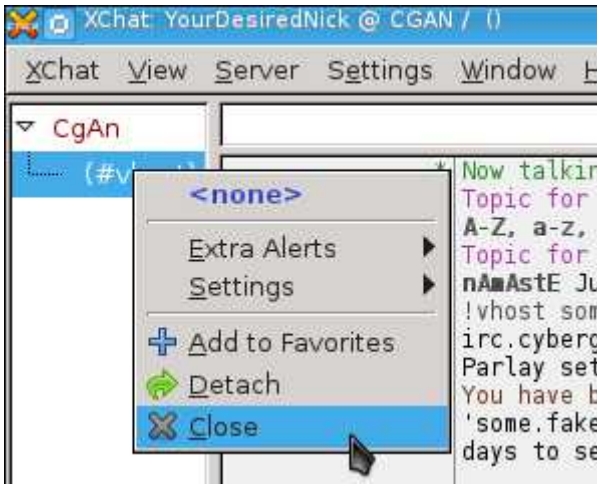
14. Now, set up a virtual host, or vhost, for yourself. While a vhost may seem like overkill under the circumstances since your IP address is already cloaked by Tor and probably the IRC server, the type of masking the IRC server uses may still allow an observer to know you are using Tor. There's no reason they need to know that. Thus, type "**/j #vhost**" to join the vhost channel.

15. In the next window that opens, type "**!vhost some.fake.host**" and press "enter" to set your virtual host. Different servers have different rules for how you can set a vhost. But, the syntax for setting it is usually the same. From this point on, every time you identify your nickname to the Nickserv, your vhost will be displayed. You do not need to create a vhost every time you log in to the IRC server.

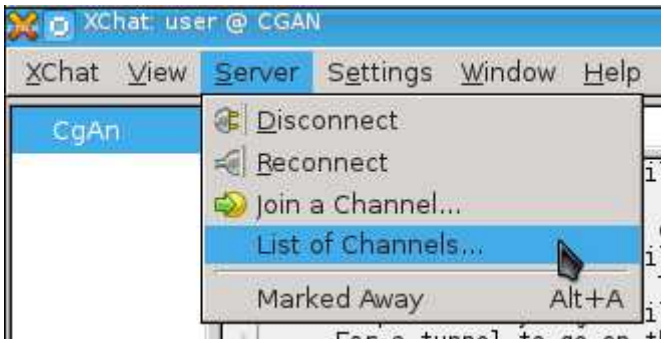
    Note: Do not choose any fake host name that can be correlated to your identity. That will include old inside jokes relating to gaming clans, old web forums where you were a member, etc.



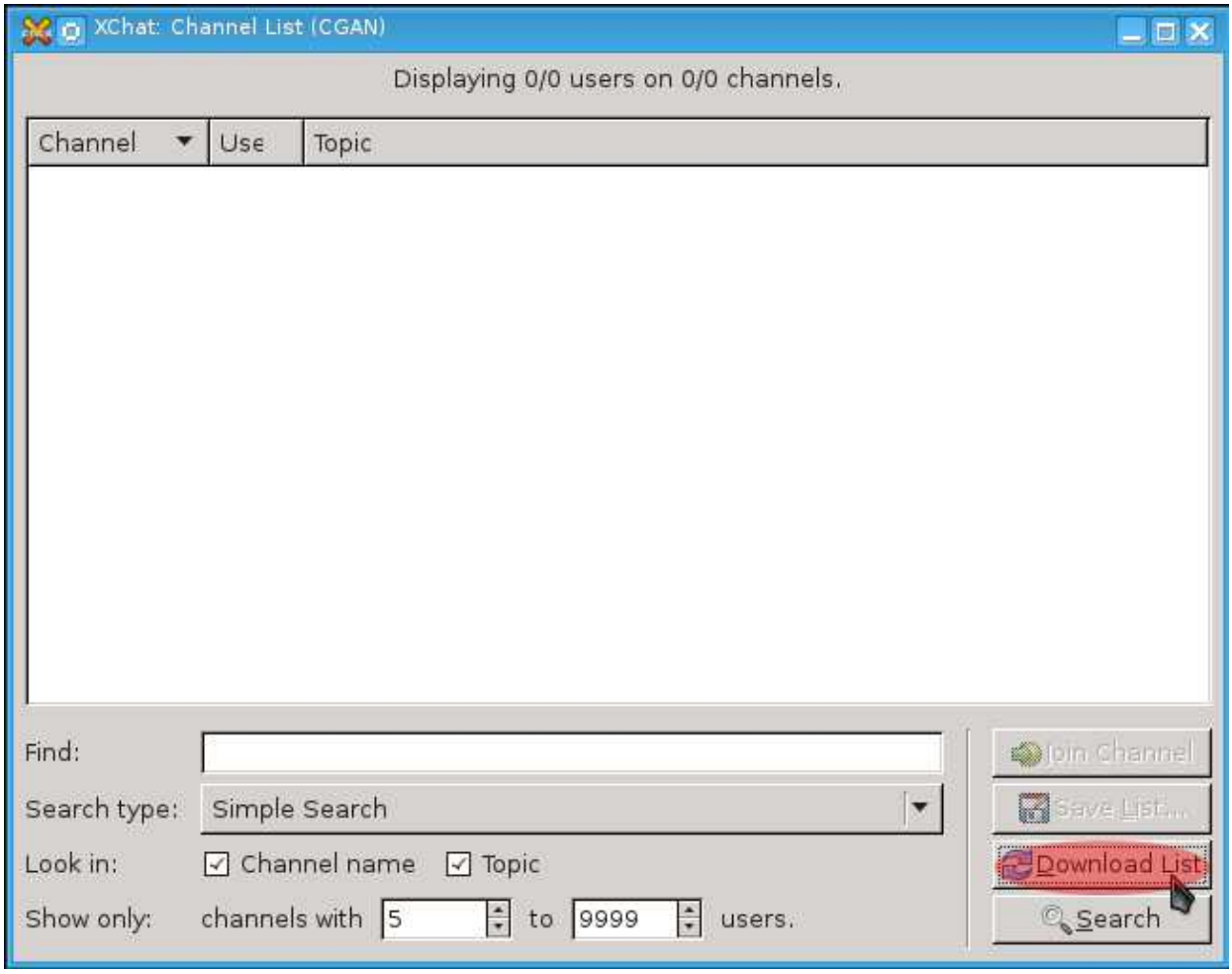
16. If you successfully set your vhost, the server will inform you that you've been banned from the channel. You can now close the channel window. Right-click on "#vhost" in the upper right side of the XChat window and click on "close." You can use this method to quit any IRC channel in the future.



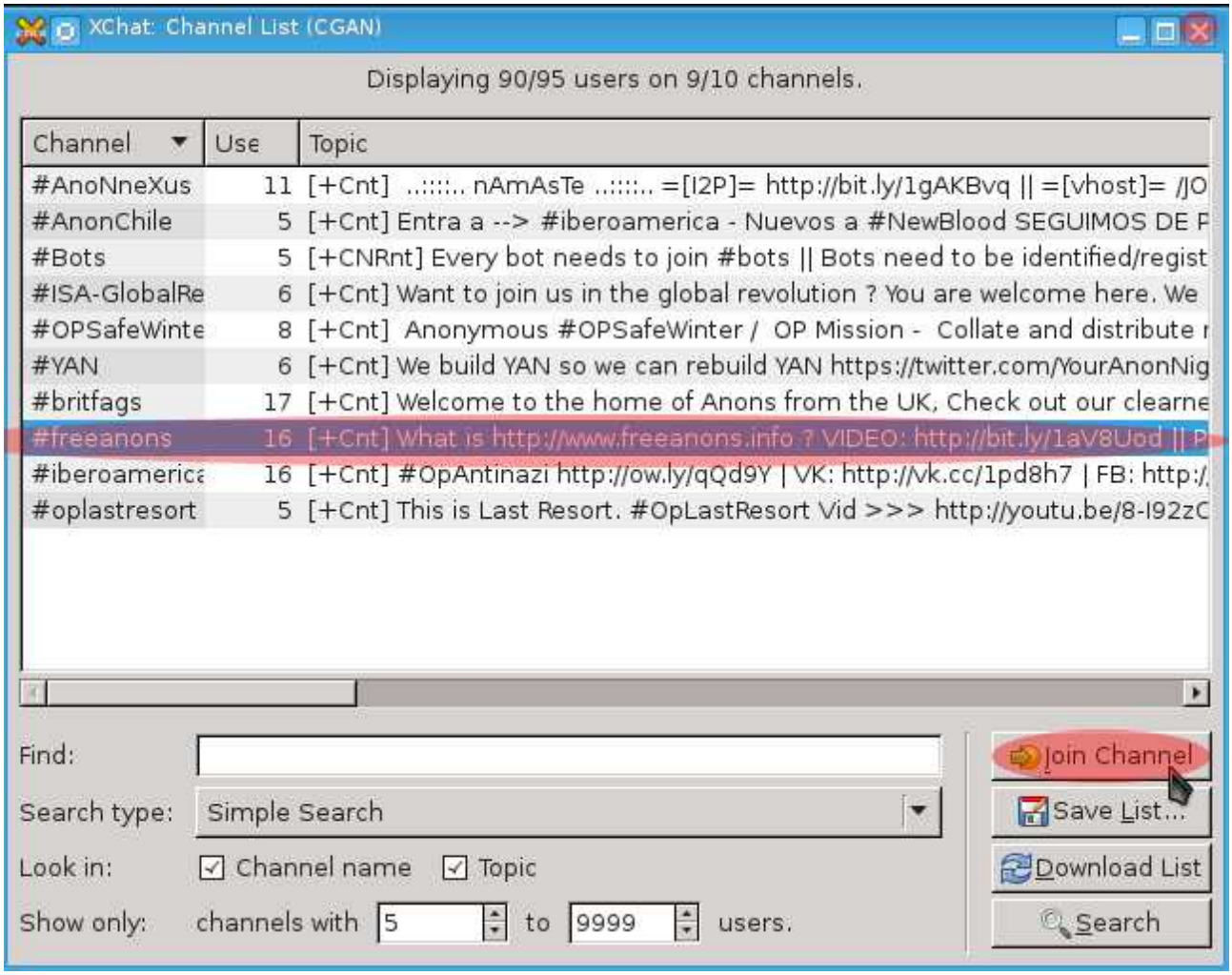
17. Next, come join a channel where you can chat. An easy way to find channels on any server is to use the "list" command. XChat provides a user friendly means of viewing the list. Click on "Server → List of Channels."



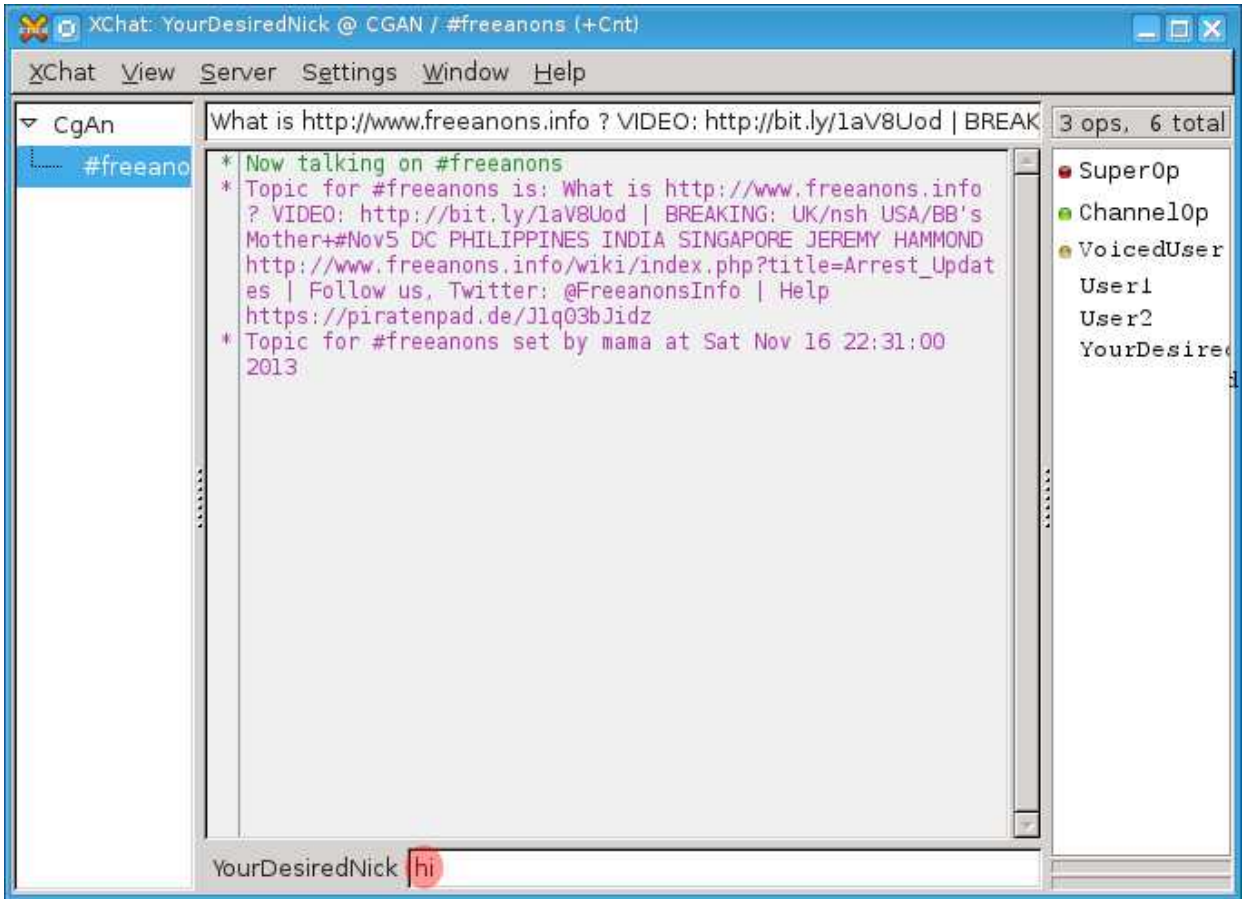
18. A window will appear that provides various options. By default, it will filter out the listing of any channel with less than 5 users present. You can change this if you desire. Otherwise, simply click on the "Download List" button.



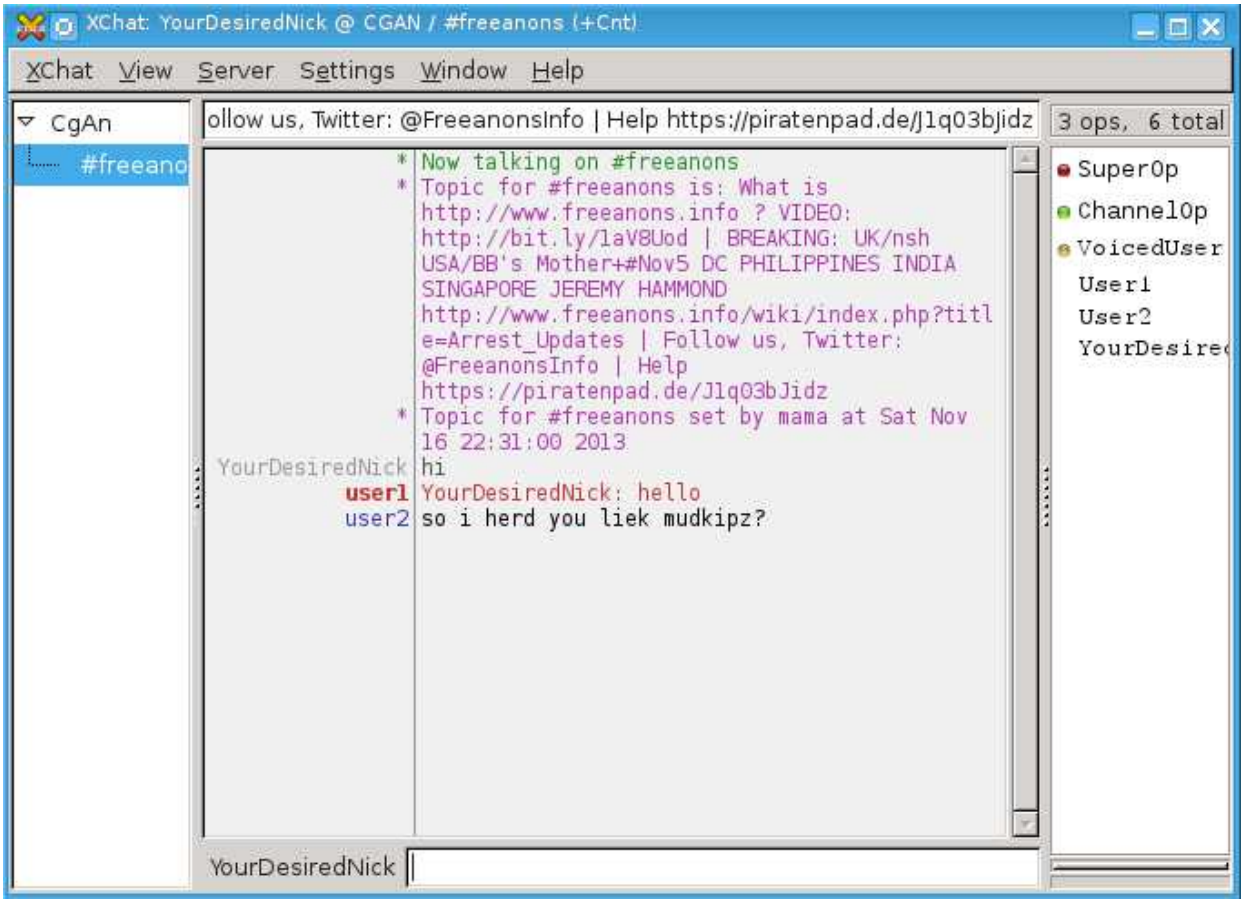
19. A list of available channels will now appear in your window. Join “#freeanons” to come and chat with some of us. Click on “freeanons” and then click the “Join Channel” button. You can then close the channel list window. In the future, if you already know a channel that you wish to join, you can do so by simply typing “**/j #YourDesiredChannel**” and pressing “enter.”



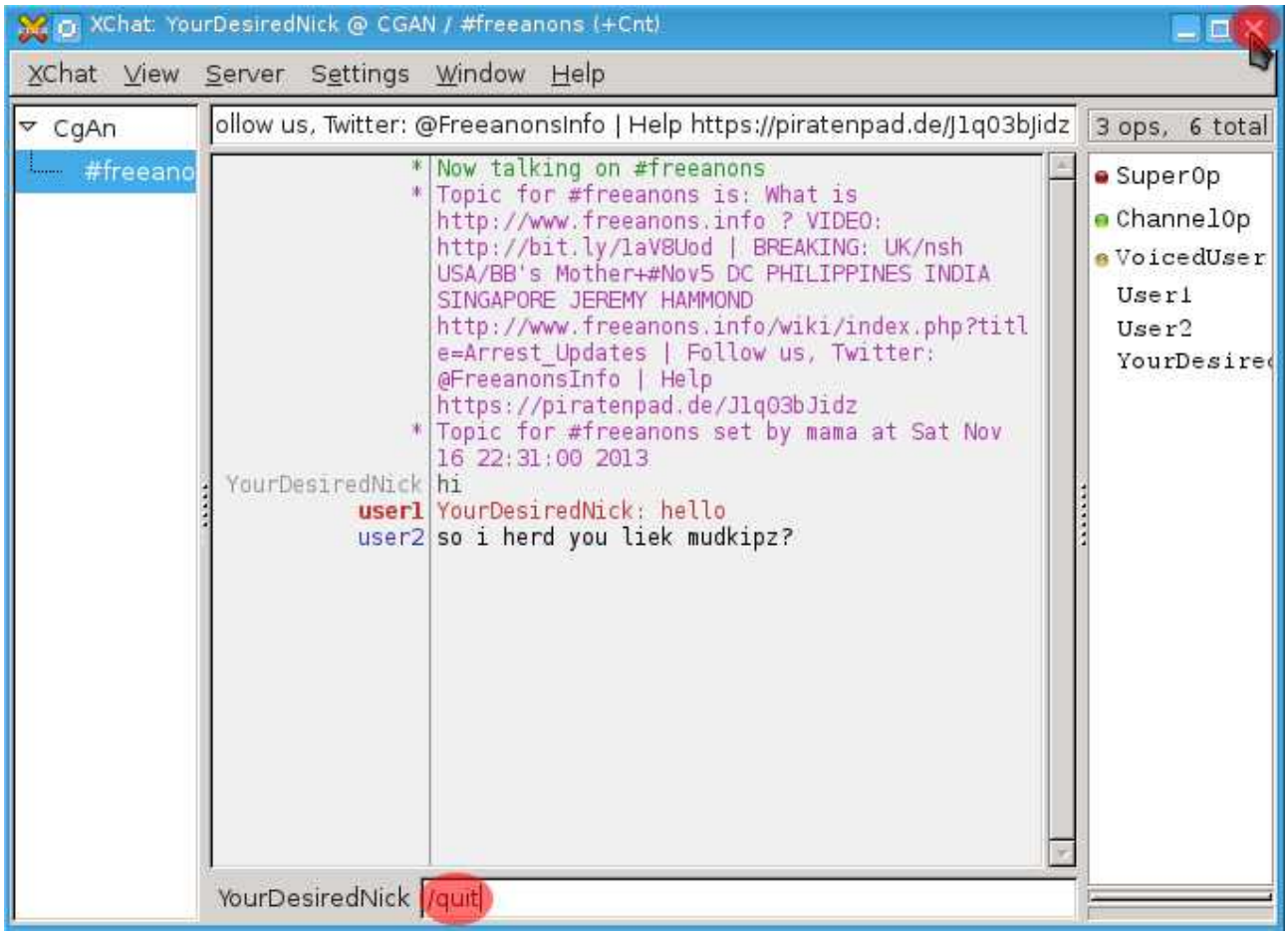
20. Next, announce your presence to the channel. A simple “hi” will do. To chat with others in the channel, simply type whatever you want to say in the section next to your nick name and press “enter.” The #freeanons channel is mirrored across multiple different IRC networks. While not always full of conversation, there are generally people around who will be eager to welcome you and chat.



The screen shot below is provided for reference. After you've typed something to be displayed in the channel, it will be displayed next your nickname in grey. Text from other users in the color red are messages intended for you. Text in regular black is general channel chatter. You will also see some colored circles in the right column in most channels. The more common ones are shown in the example. Anyone with a red circle next them is a Super Operator in a channel. Those with green circles are Channel Operators. Think of these people as administrators of the channel. They maintain control of the channel.



21. When you wish to disconnect from the server, there are two ways to do this. If you only want to disconnect from one server (it is possible to be connected to multiple servers at the same time in XChat), type "**/quit**" and press "enter." If you wish to disconnect from all the servers and close XChat, simply click on the "x" in the upper right corner.



This covers the basics of connecting to, and using, an IRC server. For the future, remember these important rules:

1. **Do not give any real personal information about yourself on the IRC if you wish to keep your anonymity. IRC channels can be logged by anyone.**
2. **Be wary of clicking on any links that have been sent to you or posted in channels. Various people may try to send you malware.**
3. **Do not ever use a nickname that you have used outside of Whonix. Additionally, do not choose a nickname that can be correlated to your identity.**
4. **Do not chose a vhost that can be correlated to your identity.**
5. **Enable SSL encryption for any IRC server you use if possible.**

Note: As you get more comfortable using XChat, you will probably notice that there are a number of ways to store nicknames, either globally or specifically for certain IRC servers, and passwords for various services, including Nickserv, on IRC servers. There is a reason you should consider against using those features in XChat. This is due to the fact that **XChat stores all of your nicknames and passwords in a configuration file that is not encrypted. If an attacker compromises your machine and views or copies your XChat configuration file, they will be able to see every nickname and password that you have stored within it.** Thus, it is safer to use KeePassX to store all of your IRC account related personal/sensitive details.

Chapter 4e. Using an Instant Messenger

This chapter will instruct you on how to use an instant messenger account with the Off-The-Record (OTR) plugin. OTR is a plugin that provides end-to-end encryption to instant messenger sessions, thus making the chats much more secure. Before using an instant messenger, understand the following issues with it, as detailed in the Whonix documentation at https://www.whonix.org/wiki/Chat:

"Most of instant messenger protocols are unsafe from a privacy point of view. This is not a Whonix specific problem. It is a general problem with instant messengers. [...]
Tor Exit Node eavesdropping can happen if no encryption to the server is enabled. Some protocols have encryption disabled by default, some do not support encryption at all. See also Overview about Pidgin protocols and their encryption features. If encryption to the server is enabled, the Tor Exit Node can no longer eavesdrop. One problem solved, another problem remains unsolved.
The server could still gather interesting information.

- Account names
- Buddy list (list of contacts)
- Log login dates and times
- Timestamp of messages
- Who communicates with whom
    - If the recipient knows the sender and the recipient uses a non-anonymous account or was ever logged in without Tor, this can be used as a hint who the sender is.
- Content of messages - Can be prevented using end-to-end encryption. This is covered [by] OTR.

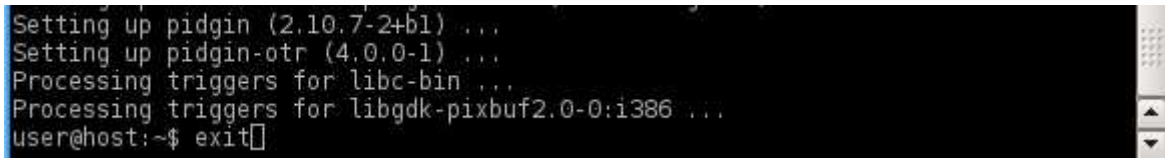
A server-based protocol designed with openness, security and privacy in mind is Jabber."

With that in mind, it is strongly recommended that you use a Jabber account. As of this writing, the most known Jabber server, Jabber.org, is not accepting new registrations. However, this is unimportant. If you create a jabber account with any Jabber server, you will be able to communicate with anyone who uses Jabber on any other server. Some Jabber servers offer different encryption services than others. In this tutorial, the Tor hidden service for jabber.calyxinstitute.org will be used as an example, which is a server with an A grade from the security rating system at https://xmpp.net/result.php?domain=jabber.calyxinstitute.org&type=client.

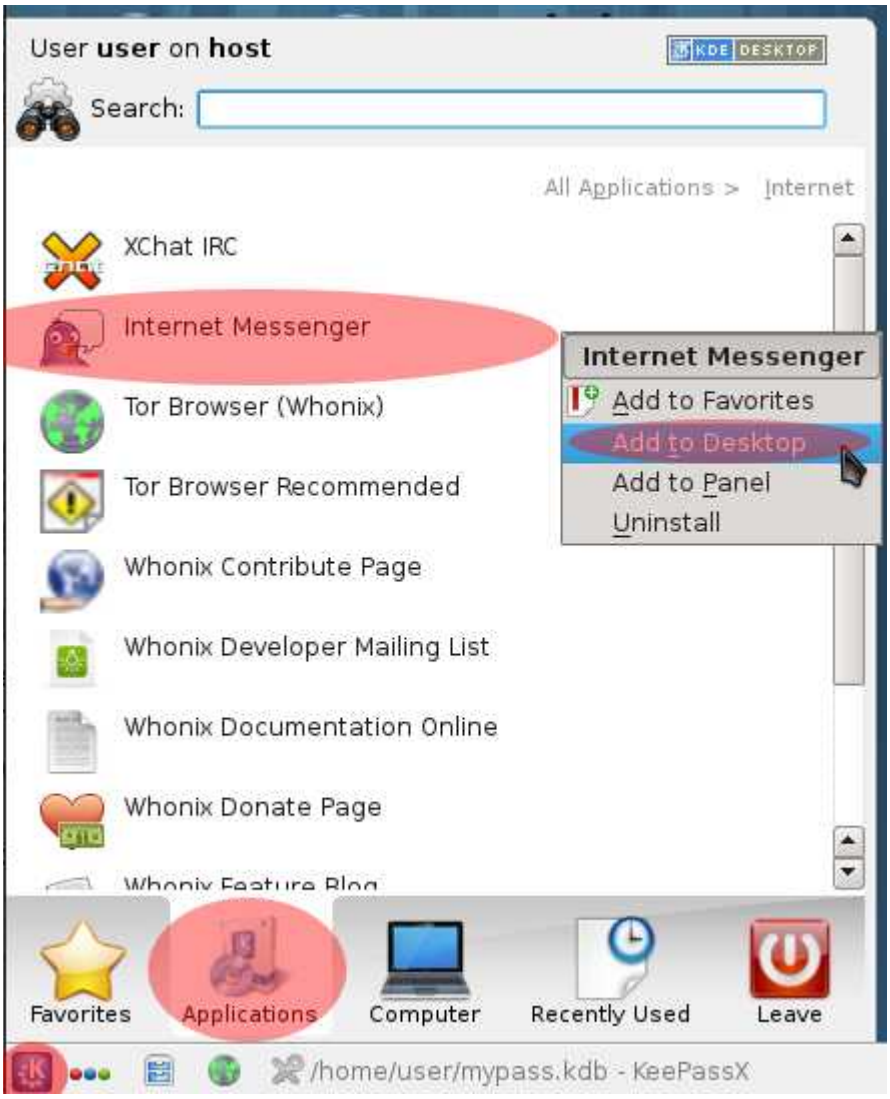
1. You first need to install two programs to use instant messaging, Pidgin and Pidgin-OTR. Pidgin is your instant messenger client. Pidgin-OTR is a plugin for Pidgin that provides end-to-end encryption between yourself and the person on the other side of your chat. **If you do not use Pidgin-OTR, assume that your communications can be intercepted and read.** To install these programs, first you need to open up a Konsole session. Double-click on Konsole on your Desktop.

2. At the command prompt in the window that appears, type "**sudo apt-get install pidgin pidgin-otr**" and press "enter." You may be prompted to enter your password. Type your password and press "enter." When asked "do you want to continue? [Y/n]?" type "**Y**" and press enter.

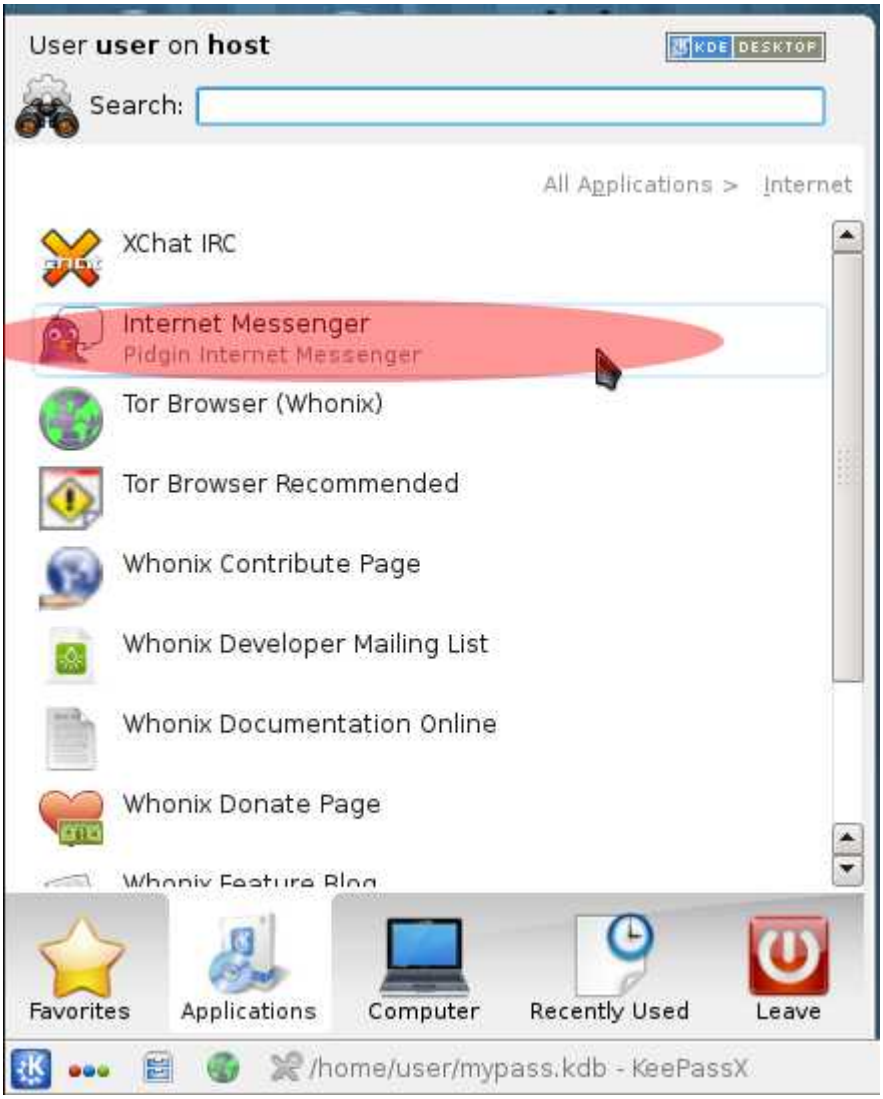
3. When the installation process is finished and you've returned to a command prompt, type "**exit**" and press "enter."



4. For simplicity, now add a shortcut for Pidgin to your desktop. Click on the K start button and go to "Applications → Internet." Right-click on "Internet Messenger" and select "Add to Desktop." A shortcut to "Pidgin Internet Messenger" will now be on your desktop.



5. After you add the icon to the Desktop, the Start Menu will still be open. Click on "Internet Messenger" to open Pidgin.



6. On the next window that appears, click on the “Add” button.

7. When the next window appears, open up an instance of KeePassX. Generate a password and anonymous account name for your instant messenger account in KeePassX and save it.

8. Return to the Pidgin window. Now, you need to choose the protocol for Jabber. Click on the pulldown menu next to “Protocol” and choose “XMPP.” XMPP is the protocol for Jabber. Then, type the user name you wish to use next to “Username” and type “jabber.calyxinstitute.org” next to “Domain.” Then, click on the checkbox next to “Create this new account on the server.” Finally, click on the “Advanced” tab.

9. Next, make sure the chosen option next to “Connection security” is “Require Encryption.” Then, to use the Tor hidden service, type “ijeeynrc6x2uy5ob.onion” in the field next to “Connect Server.” Then, uncheck the box next to “Show Custom Smileys.” Finally, click the “Add” button.

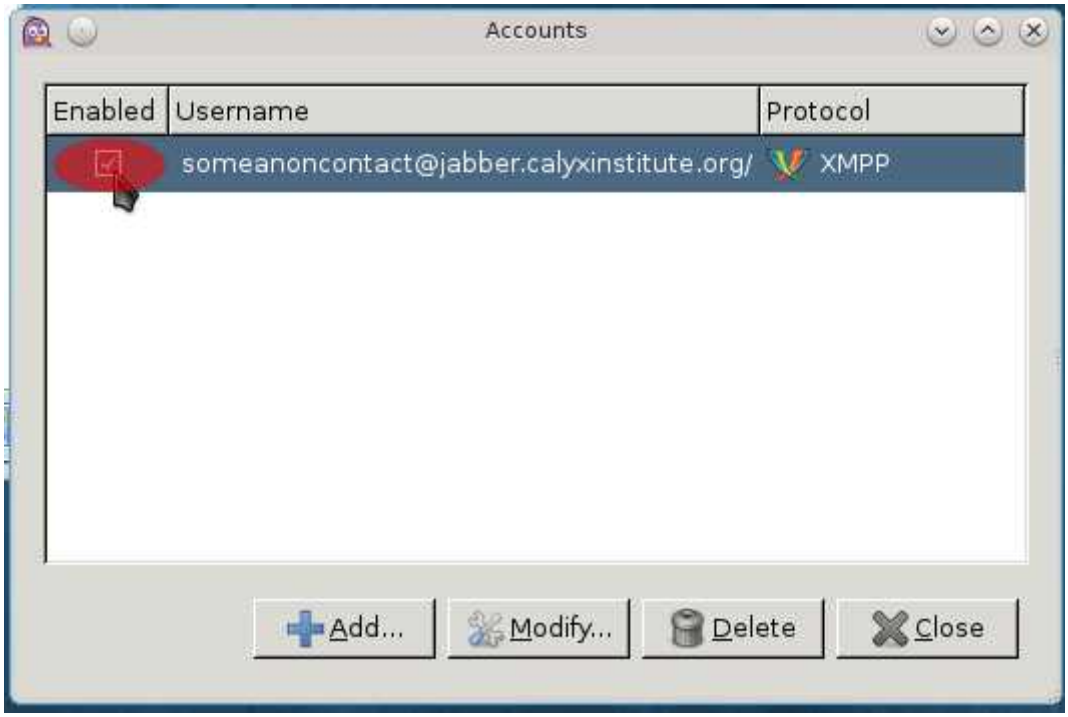
10. The next window that appears will inform you that the SSL certificate you received from ijeeynrc6x2uy5ob.onion belongs to “*.calyxinstitute.org.” Click the “Accept” button.

11. In the next window, enter the username you wish to use again in the “User” field and copy the password you created with KeePassX into the “Password” field. Finally, click the “OK” button.

12. If your account was successfully created, you will see the window below. Click on the “Close” button to continue.

Note: When you give out your Jabber screen name, it is similar to email. In this example, if you wanted to tell someone what your screen name was, it would be “**anonymousalias@jabber.calyxinstitute.org**”. All Jabber accounts follow the **username@jabberserverdomain** syntax.

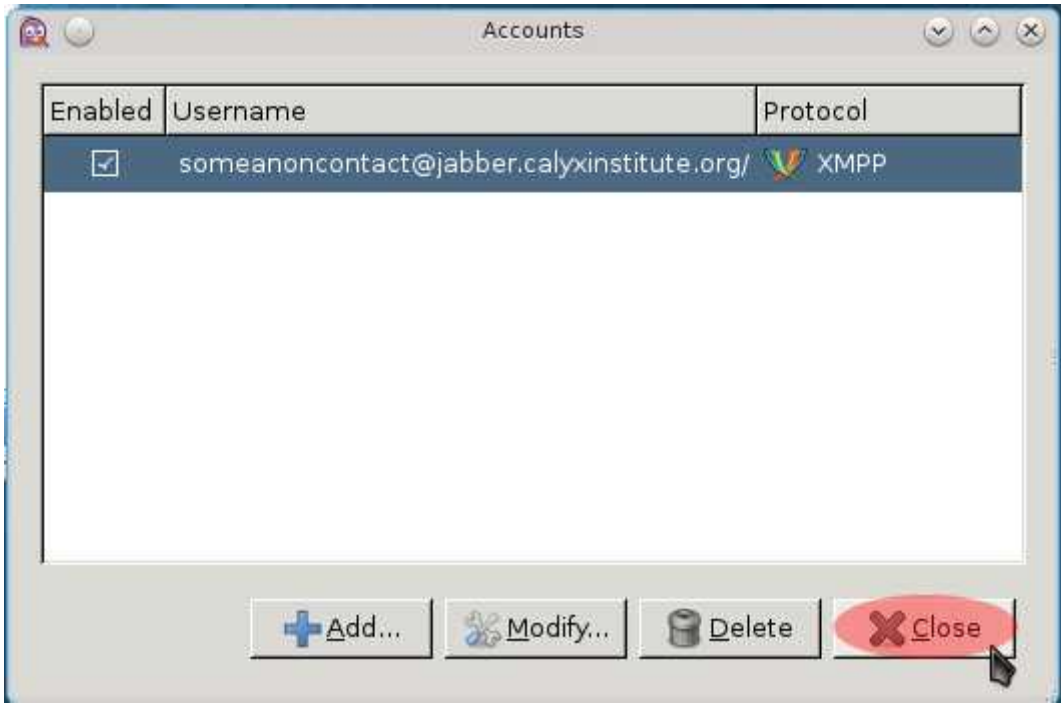
13. Now you need to enable your account to log in. Click on the checkbox under “Enabled” next to the Jabber account you created so the box is checked.



14. The next window that appears will prompt you for your password. Copy your password from KeePassX and enter it into the field next to “Enter Password.” Then, click on the “OK” button.

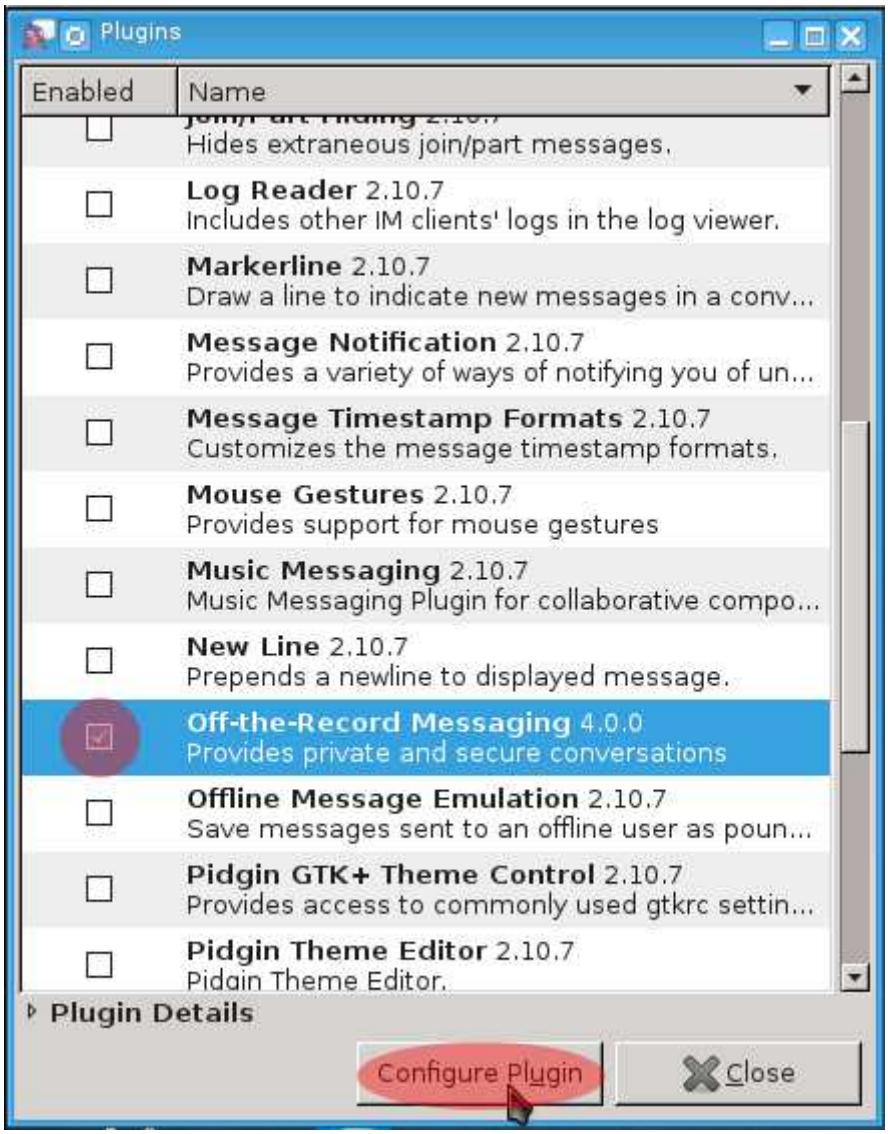
    Note: **Do not use the “Save Password” option. Pidgin does not store passwords and account details in an encrypted format. Thus, if an attacker compromises your machine and reads your Pidgin configuration file, they can get the password to your Jabber account.** The safest option is to use KeePassX to store your password and enter it into Pidgin when prompted as the program starts in the future.

15. You will next be returned to the the “Accounts” window. Click on the “Close” button.



16. Next, from the Pidgin “Buddy List” window, click on “Tools → Plugins.”

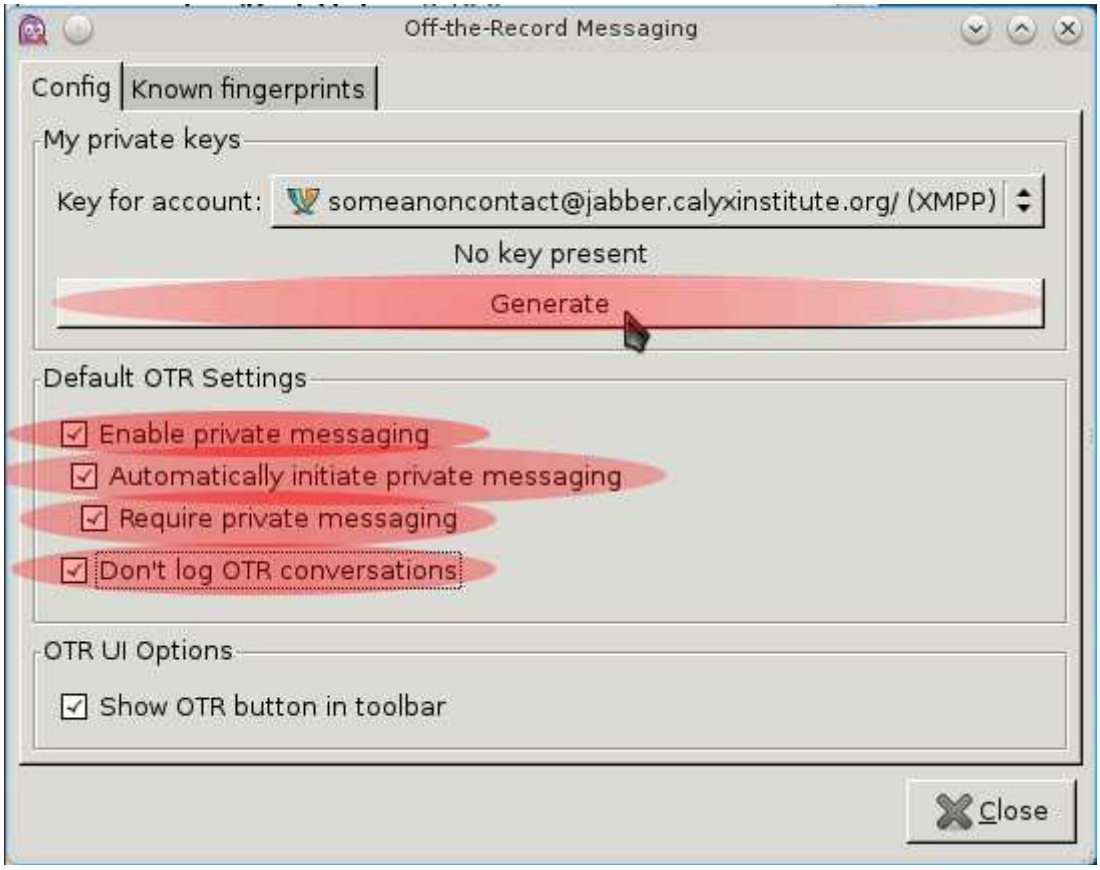
17. Now, you need to configure the OTR plugin for future use. Scroll down until you see “Off-the-Record Messaging.” Click the check box next to it so it is “enabled.” Then, click on “Configure Plugin.”



18. In the next window that appears, make sure every box is checked. Of particular importance is to mark the “Require private messaging” box. If someone does not have the option of chatting with you via an OTR encrypted session, then they aren't worth chatting with. **Using an instant messenger service without OTR will put both you and the person you are talking to at risk of having your communications intercepted.**

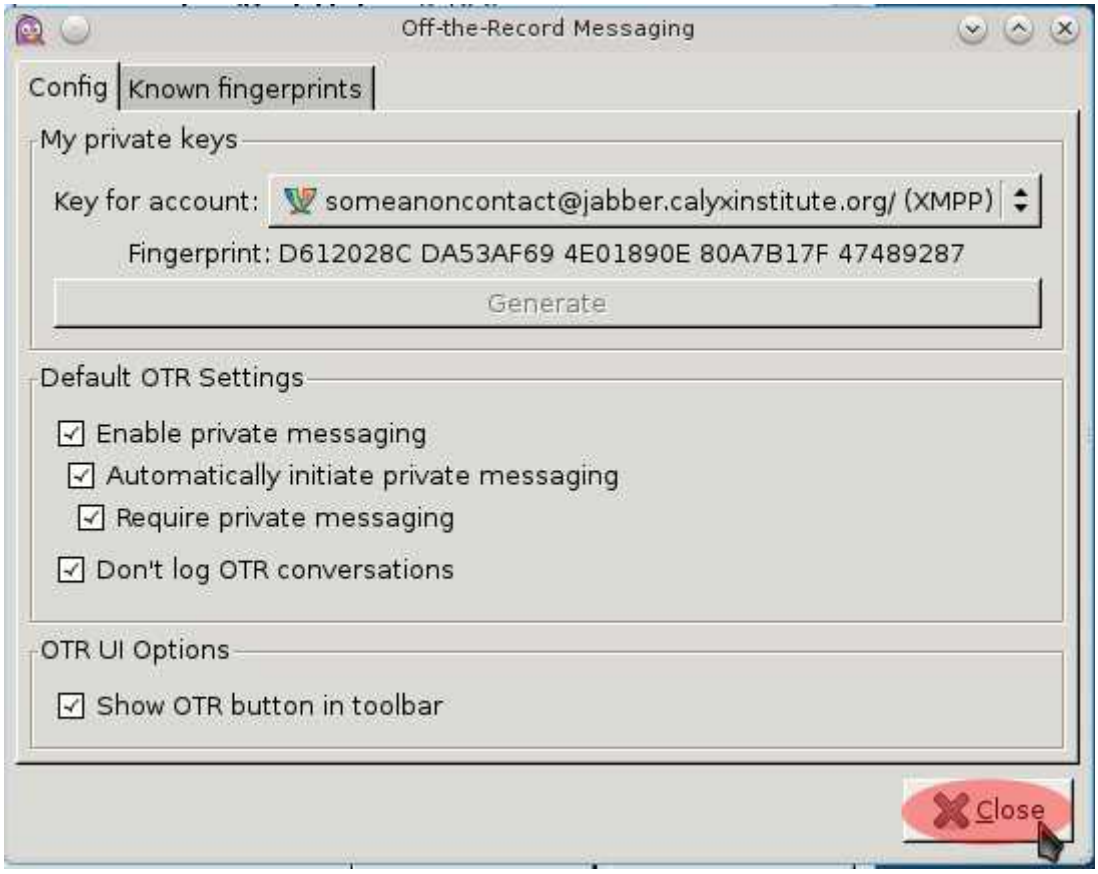
    When you are done marking the boxes, click on “Generate.” This will create your unique OTR private key for your account.

    Note: If you create more than one account, you will need to generate an OTR key for each.

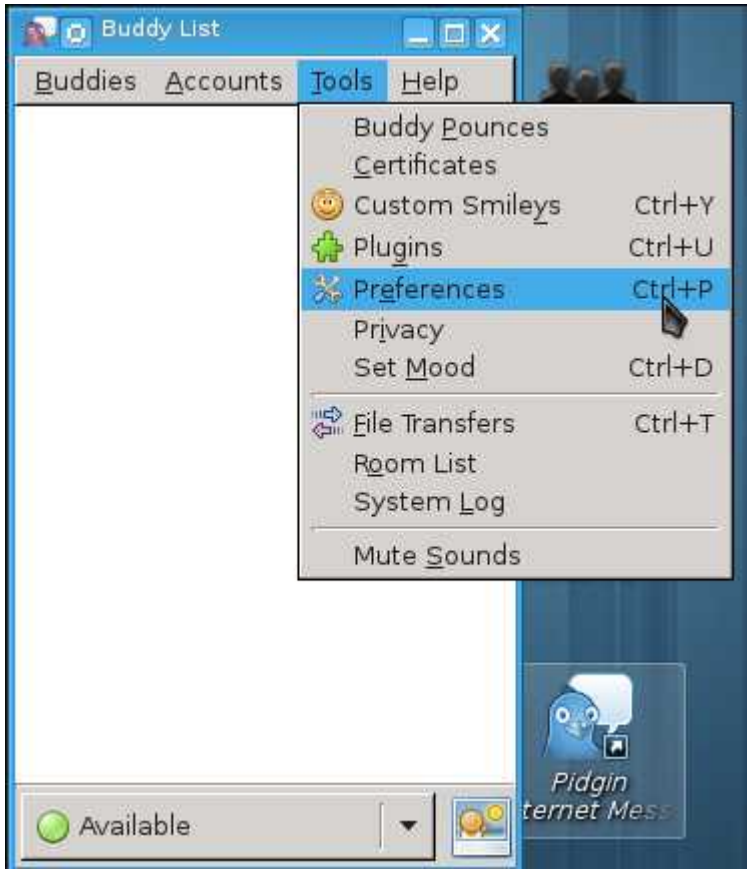


19. A “generating private key” window will next appear. When it says “done,” click the “OK” button.

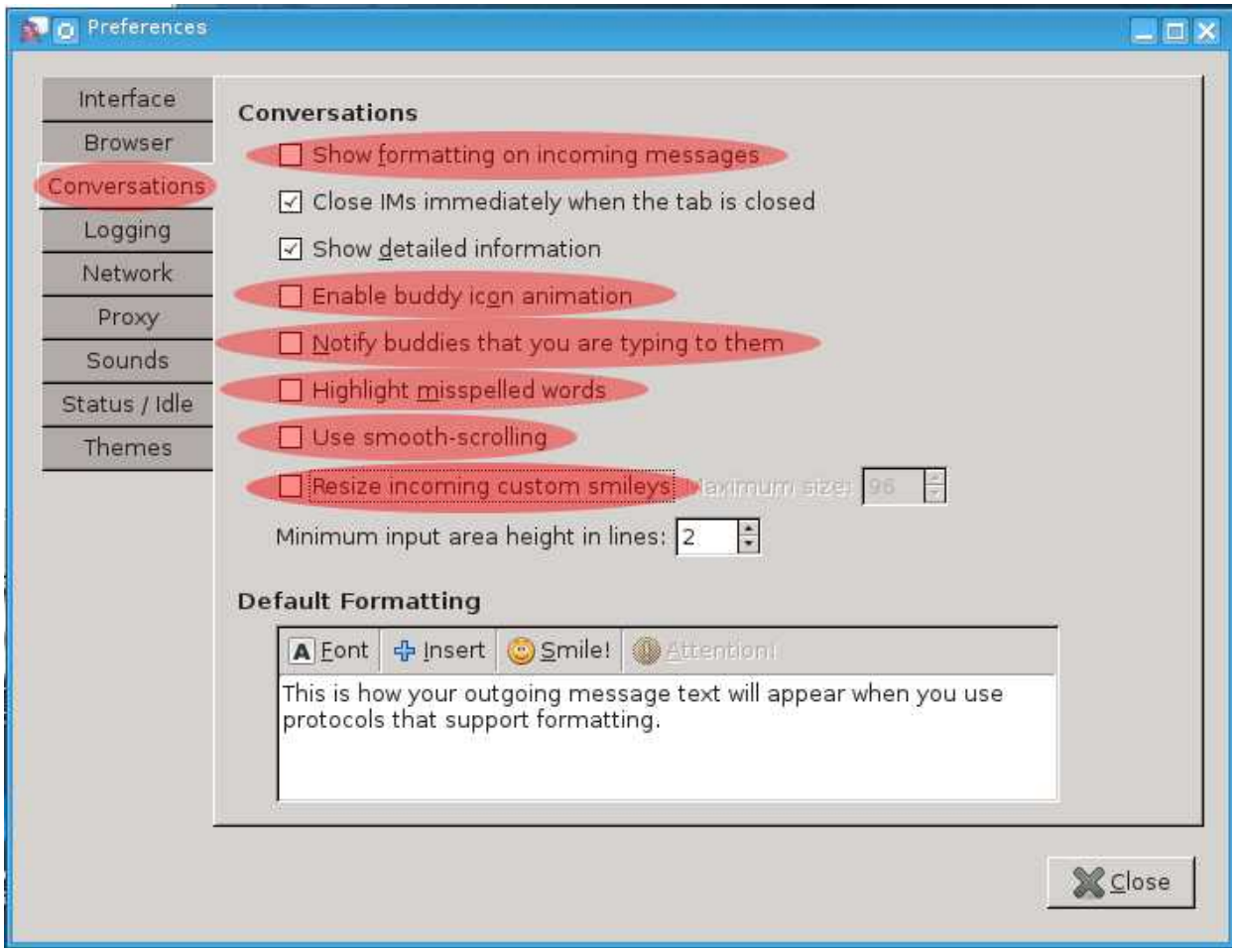
20. When you are returned to the previous “Off-the-Record Messaging” configuration window, click on the “Close” button.



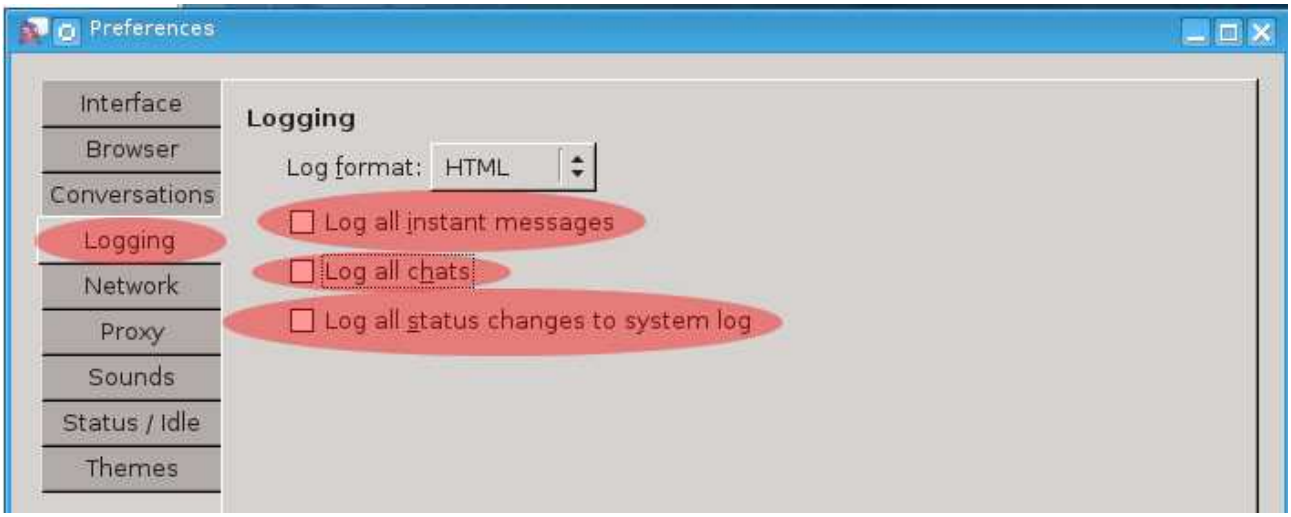
21. Next. Do the final configuration tweaks to Pidgin. Click on “Tools → Preferences.”



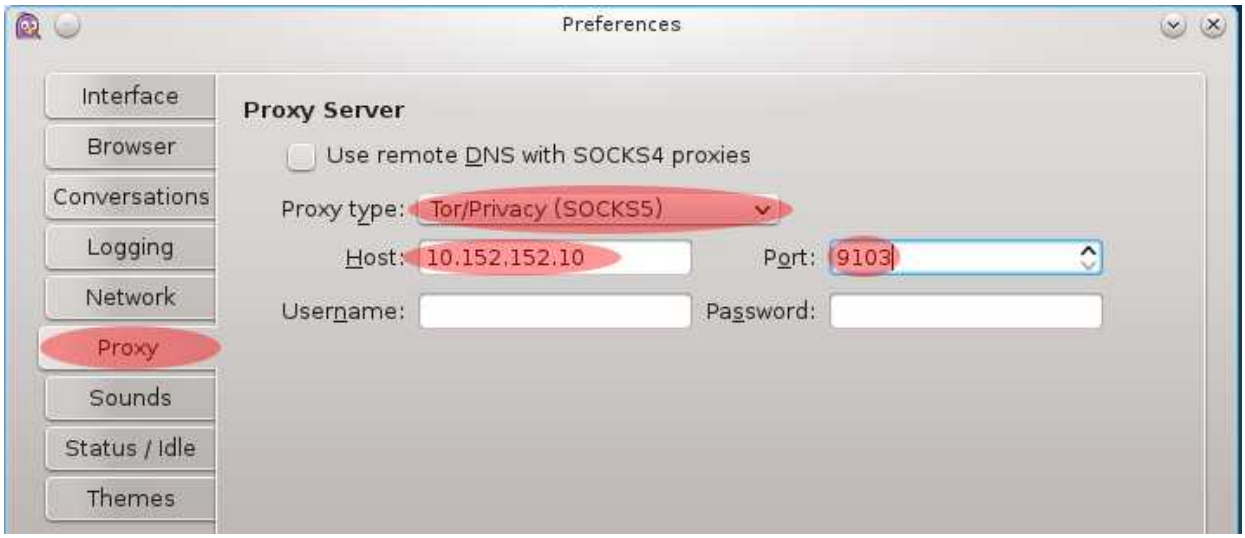
22. On the next window, click on the “Conversations” tab on the left side of the window. Then unmark the “show formatting on incoming messages,” “enable buddy icon animation,” “notify buddies that you are typing to them,” “highlight misspelled words,” “use smooth-scrolling” and “resize incoming custom smileys” options. When your window looks like the image below, continue to the next step.



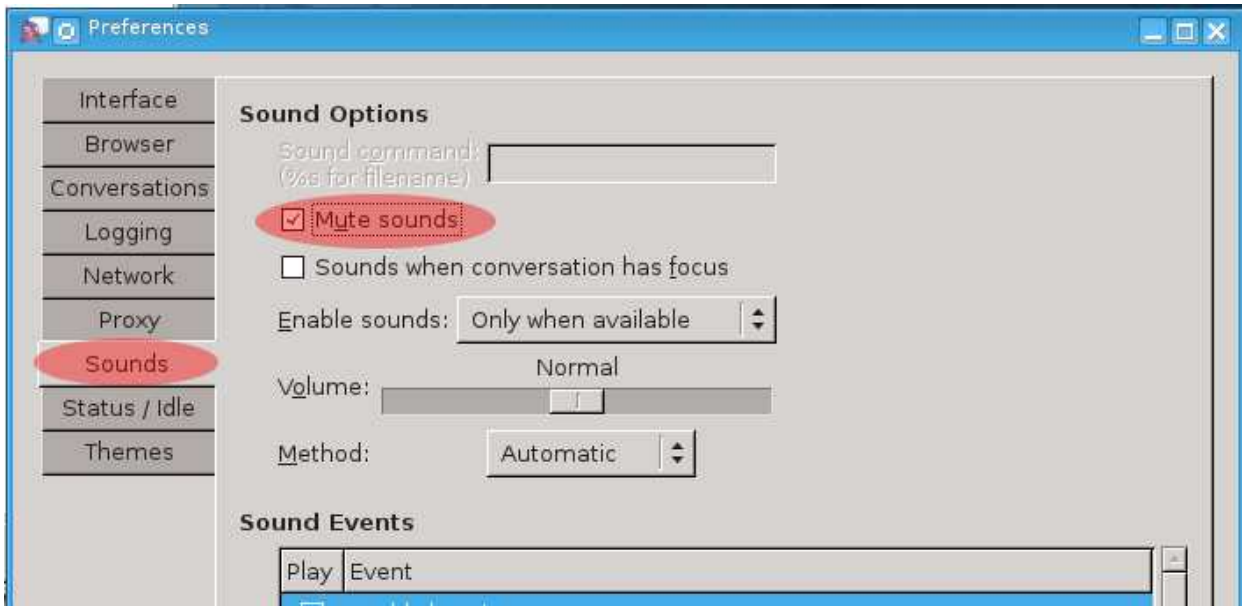
23. Click on the “Logging” tab on the left side of the window. Unmark every option here. When your screen looks like the image below, continue to the next step.



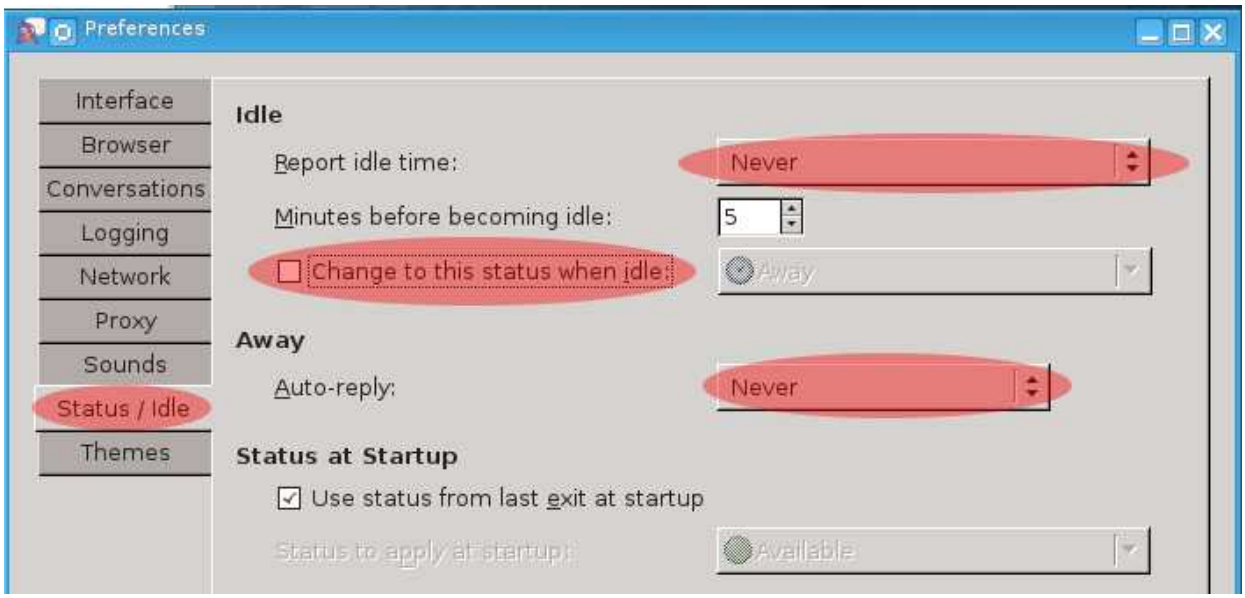
24. Next, Click on the “Proxy” tab on the left hand side of the window. Then, select “Tor/Privacy (SOCKS 5)” in the pull down menu next to “Proxy type.” Next, type “10.152.152.10” in the field next to “Host.” Then, type “9103” in the field next to “Port.”



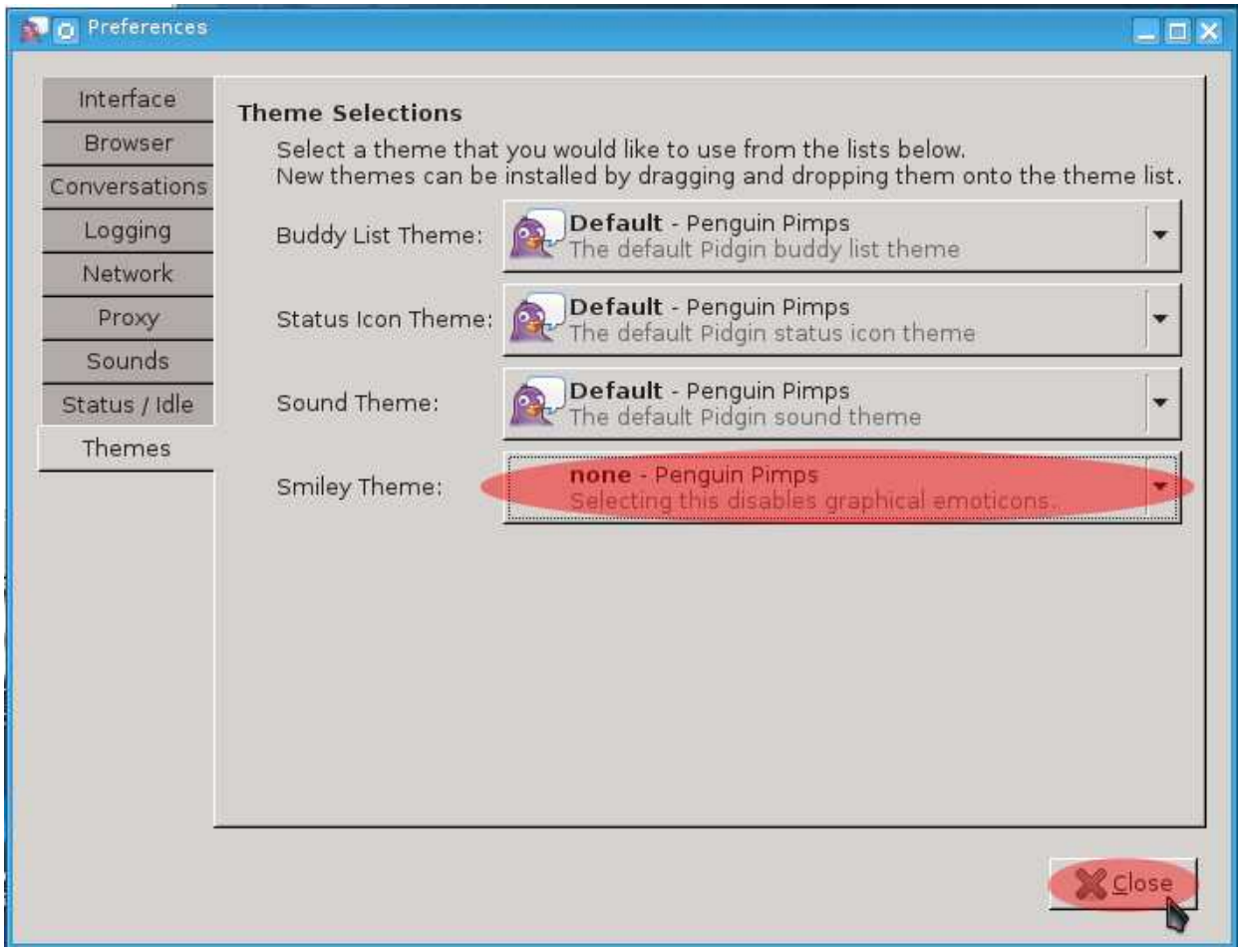
25. Click on the “Sounds” tab on the left side of the window. Enable the “mute sounds” option. When your screen looks like the image below, continue to the next step.



26. Click on the “Status / Idle” tab on the left side of the window. Then, click on the pull down options next to “Report idle time” and select “Never.” Next, unmark the box next to “change to this status when idle.” Finally, click on the pull down options next to “Auto-reply” and select “Never.” When your screen looks like the image below, continue to the next step.



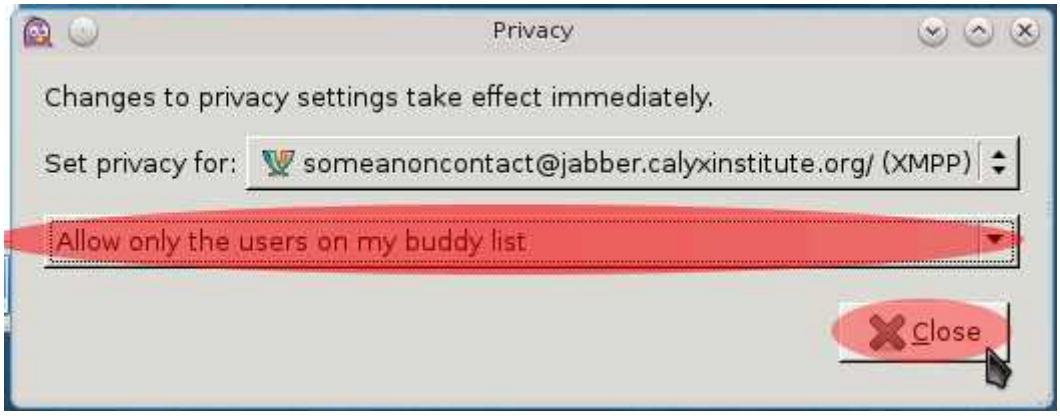
27. Click on the “Themes” tab on the left side of the window. In the pull down options next to “Smiley Theme,” select “none.” Then, click on the “close” button.



28. Next, when you have returned to the “Buddy Icons” window, click on “Tools → Privacy.”

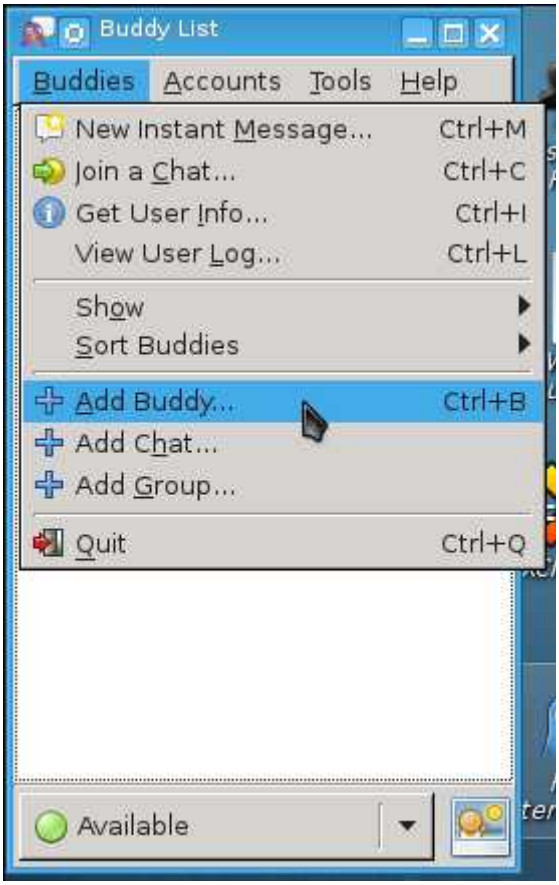
29. In the pull down option field beneath the “Set privacy for: {your nickname},” select “Allow only the users on my buddy list.” Then click “Close.”

    Note: In the future, **only users on your buddy list will be able to send you messages**. There are trade-offs here. On one hand, you will be creating a buddy list that will be stored on the Jabber server you use. If an attacker gains access to the server, whether through an exploit or legal process, they will be able to access your buddy list and possibly profile you based on who it contains. On the other hand, this also weakens the abilities of random attackers to exploit vulnerabilities in your client by directly sending you a message before you've authorized them to be in your buddy list.

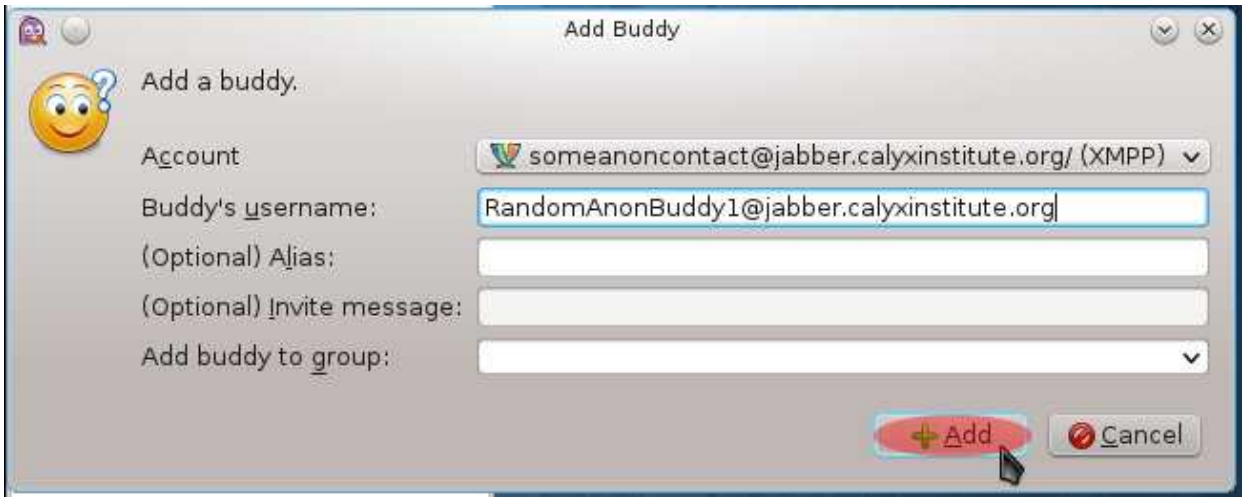


Congratulations. You have now installed and configured Pidgin for general use in Whonix. The remainder of this chapter will instruct you on how to chat with others using Pidgin with OTR.

30. To initiate a chat with someone, first add them to your Buddy List. From the “Buddy List” window, click on “Buddies → Add Buddy.”



31. In the next window, type the contact address of the person you wish to chat with in the field next to “Buddy's username.” This will be in the format of **username@JabberServerDomain.** Then, click on the pull down menu next to “add buddy to group” and select the group you wish to add the contact to. When finished, click the “Add” button.

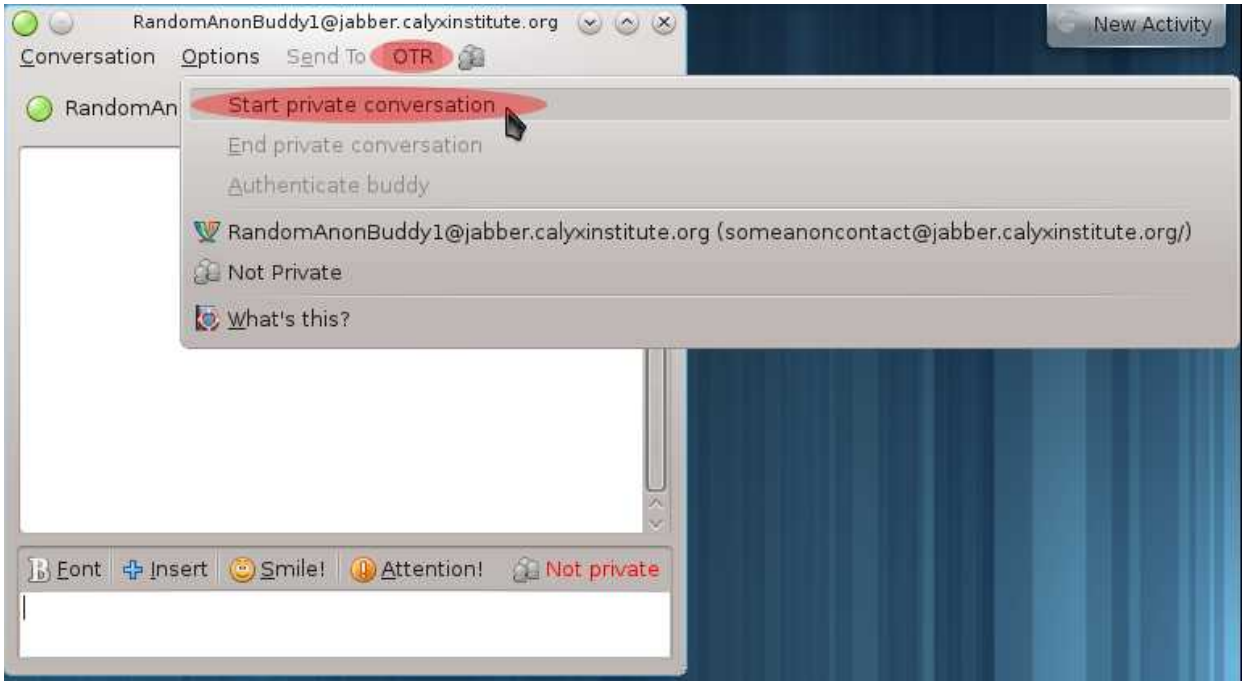


Note: **The contact you add will not appear in your Buddy List immediately at this point.** This is due to the fact that your contact must authorize you to add them to your Buddy List and, after you are authorized, must be online.

32. When your newly added contact has authorized you to add them to your Buddy List, you will see their screen name appear in your Buddy List if they are online. You will also be prompted by Pidgin to authorize them to add you to their Buddy List. If it is someone you contacted, or someone you wish to chat with, click on the “Authorize” button.

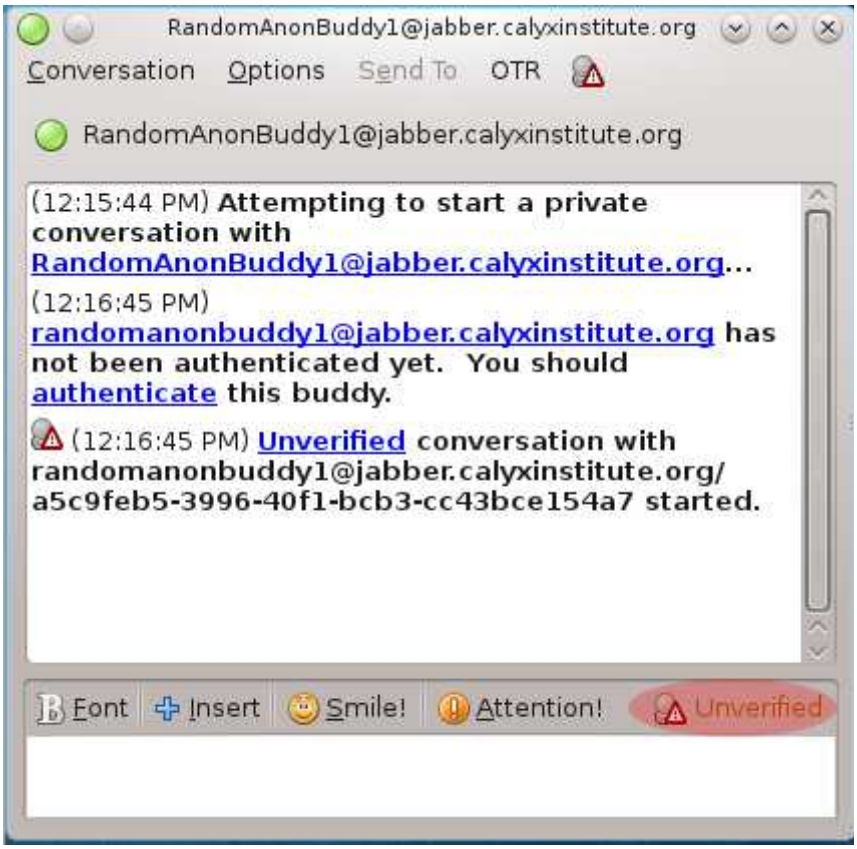
33. Next, to chat with a contact in your Buddy List, double-click on their screen name.

34. In the next window that appears, you need to start an OTR “private conversation.” Click on “OTR → Start private conversation.”



Note: Since you set private conversations as “required” in the OTR configuration, simply typing some text and sending it will also start a private conversation. However, until the private conversation handshake is completed between you and the other user, anything that you've typed will not be seen by them. Thus, it's better to use the method above and wait for the confirmation that the private conversation has started.

35. Eventually, you will receive a message that your “private conversation” has started. However, note the “Unverified” status message. Also, notice the “Unverified” icon towards the lower right corner that is highlighted in red in the image below. These inform you that you haven't verified the identity of the person your are chatting with yet.



For future security purposes, you need to verify the identity of the sender. Click on the “Unverified” icon highlighted in red in the image above and select “Authenticate buddy.”

36. On the next screen, click on the pull down menu under “how would you like to authenticate your buddy” and choose “manual fingerprint verification.” The contact's fingerprint will be listed directly below your's, and is a series of five strings of random letters and numbers.

    If you currently have the ability to communicate with your contact in real time by another channel, such as IRC, have them repeat what their OTR fingerprint is. If it matches up, you are safe. If not, you may be experiencing a man-in-the-middle attack and, thus, may have an unsafe communication session. If the contact asks for your fingerprint, supply them with what is shown as your OTR fingerprint in this window by the same means.

    If you have no way to initially authenticate your contact in real time, find a means to confirm it with them later outside of Jabber. Other options may exist for this, such as an encrypted email signed with a corresponding GPG key (which will be discussed in the next chapter), Twitter, or some other communication service.

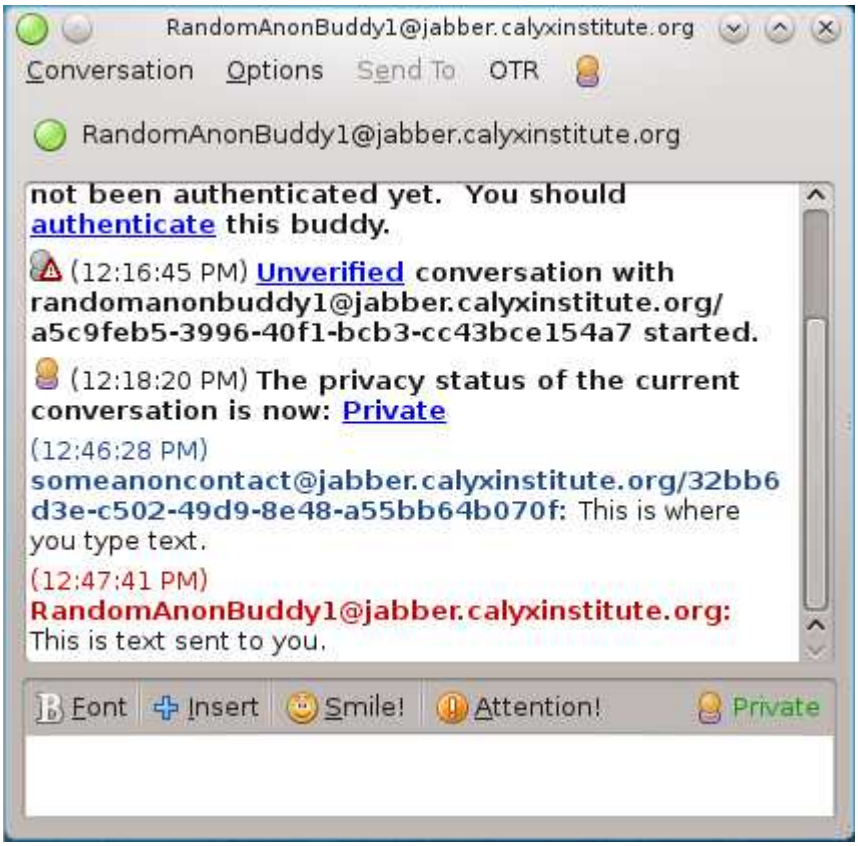
    If you choose to authenticate the contact without actually verifying their fingerprint, be wary of discussing anything sensitive in the Pidgin chat until you have confirmed that you are indeed chatting with the contact you want.

    Once you have finished the manual verification procedure (or have concluded that you can't), select “I have” in the pull down menu preceding “verified that this is in fact the correct fingerprint for [contact name]”and click on the “Authenticate” button.

37. Notice how the status of the conversation has changed to “Private,” which is highlighted in red in the image below. For all future conversations with this contact, if their OTR key has remained the same, the status will always be marked as private. **IMPORTANT: If the status ever reverts to “Unverified,” you may not be talking to the contact. It could be that someone has hacked his Jabber account or that a server somewhere in the middle has meddled with the encryption process. Be very wary if a contact who you've verified reverts to an unverified status.**

    Sending messages at this point is straightforward. In the section of the screen shot below where you see “this is where you type text,” that is where you type messages to be sent to your contact. When you are ready to send it, press the “enter” key.

The message you sent will show up next to your name which will be blue. Messages you receive will show up next to the contact's name which will be red.



38. Pidgin is also controlled by an icon that sits in the lower right corner of your Taskbar. It is highlighted in red in th image below.

First, enable the icon to blink when you receive new messages. This will make it easier for you to know someone has sent you a message if you are using other windows in Whonix. Right-click on the Pidgin related icon in your Taskbar and select “Blink on New Message.”

Finally, to quit Pidgin, you need to do more than close your message windows or Buddy List window. Right-click on the Pidgin related icon in your Taskbar and select “Quit.”

You've reached the end of the chapter on Pidgin and OTR. For future reference, remember these points.

1. Do not ever use a screen name that you have used outside of Whonix. Additionally, do not choose a screen name that can be correlated to your identity.
2. Make sure the Jabber provider you uses implements the proper encryption protocols at every level. Resources on the net will tell you if it does or does not. (calyxinstitute.org currently passes the test).
3. If you aren't using Off-The-Record encryption during your chat sessions, **assume that they are being logged and that anyone can read them.**
4. Just because you are using Off-the-Record encryption, **don't assume that the person you are chatting with isn't logging your conversation.** As with any other communication technology, do not share any real information about yourself which could identify you.
5. **If anyone you've ever chatted with via Off-the-Record encryption changes from a "Verified" to an "Unverified" status, assume you are talking to an impostor.**
6. **DO NOT USE PIDGIN TO STORE PASSWORDS!** All passwords and account details stored by Pidgin are unencrypted. If your machine is compromised by an attacker, they could gain access to your screen name by viewing Pidgin's configuration files if you use Pidgin to store passwords. Only use KeePassX to store your passwords.

Now you are ready to continue on to the next chapter that deals with one of the more underused technologies by beginners, anonymous email and GPG encryption.

Chapter 4f. Encrypted email with Icedove and Enigmail

Due to the complexity of the software in the past, one of the most underutilized forms of protection for users is email encryption. However, with the use of Icedove (the Debian Project's email client) and Enigmail (a graphical front-end for using the GnuPG [“GPG”] encryption program), taking advantage of encrypted email is now much easier. This is not the same as online services that promise “encrypted email” in transit or storage such as Lavabit. Those types of systems can still be broken by an attacker if the system cooperates. Rather, the email encryption discussed here involves direct end-to-end encryption that can only be read by the intended recipient and, thus, is much more secure.

Be aware that e-mail is a very insecure system by design when it comes to privacy and anonymity and, thus, must be used with great discipline and caution. For example, even if you encrypt all of the email that you send to a recipient, if they reply to your email and don't encrypt it, then they have just sent an email that contains their message, and likely a quote of the one you typed, which can be viewed by numerous different attackers. Furthermore, the names of email recipients and the subject line of your email cannot be encrypted and, thus, are always viewable to an attacker. Additionally, there is a number of different types of metadata that can be harvested from email, depending on how it is used. **Therefore, please be careful if you use email to engage in sensitive communications.**

With that out of the way, let's proceed.

1. First, open a Konsole session. Double-click on the Konsole icon on your Desktop.

2. Next, install the Icedove email client and the Enigmail GPG encryption add-on. Type “**sudo apt-get install icedove enigmail**” and press “enter.” You may be prompted to enter your password. Type your password and press “enter.” When asked “do you want to continue? [Y/n]?” type “**Y**” and press enter.

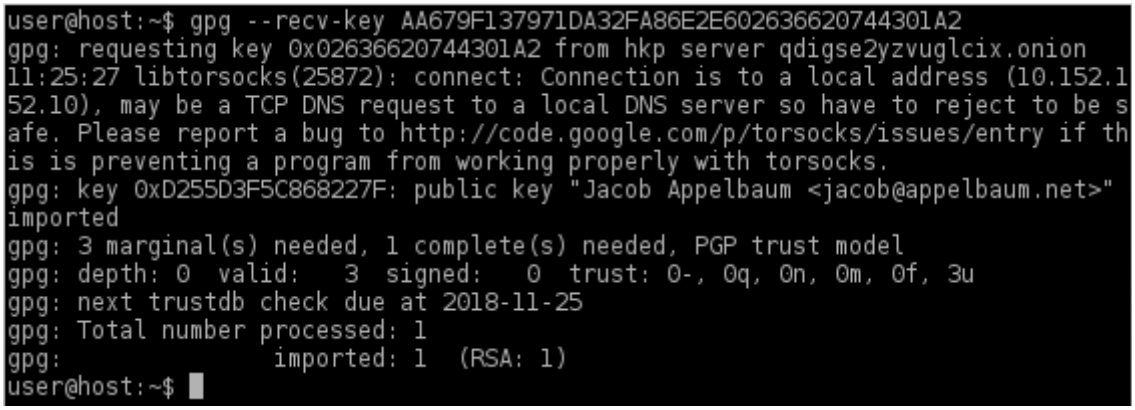
```
Type: "whonix" <enter> for help.
user@host:~$ sudo apt-get install icedove enigmail
```

3. Next, download “TorBirdy.” This is a plugin for Icedove created by the Tor Project to further anonymize Icedove.
   Type “**wget https://www.torproject.org/dist/torbirdy/torbirdy-current.xpi**” and press “enter.”

4. The following steps are optional but **strongly recommended**. Next, download the necessary files to verify the integrity of the TorBirdy installer.
   Type "**wget https://www.torproject.org/dist/torbirdy/torbirdy-current.xpi.asc**" and press "enter." If you wish to skip the verification procedure, proceed to step 7.

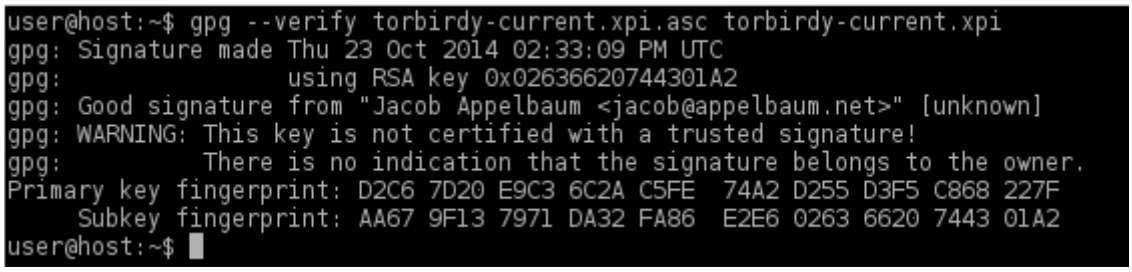
5. Now, download the GPG signature of Jacob Appelbaum, one of the developers of TorBirdy.
   Type "**gpg --recv-key AA679F137971DA32FA86E2E602636620744301A2** and press "enter."

   When you have imported the key, your screen will like the screen shot below. You can safely ignore the "libtorsocks" error. This is a bug in the current version of Torsocks that will be addressed in the soon to be released new version. It does not affect the ability to import keys from a key server, nor does it jeopardize your anonymity.



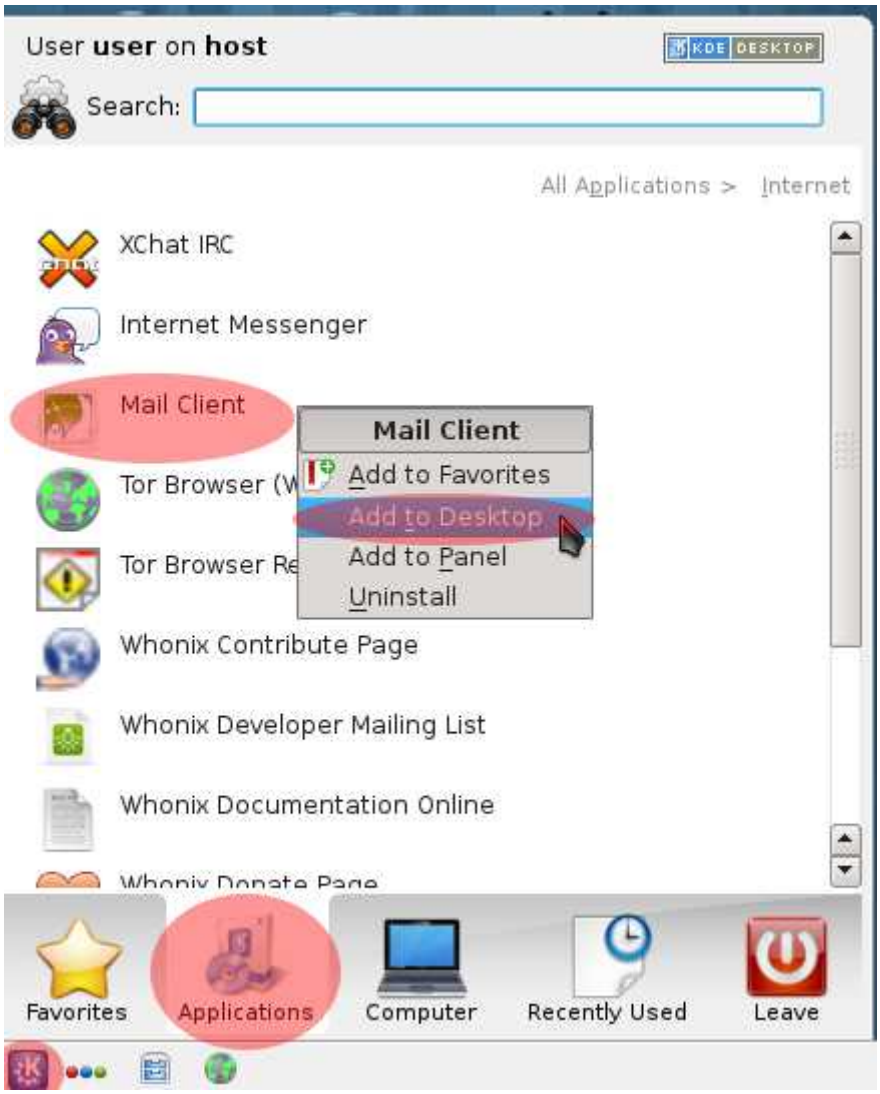
6. Next, it is time to verify the integrity of TorBirdy. Type "**gpg --verify torbirdy-current.xpi.asc torbirdy-current.xpi**" and press "enter."

When the verification is done, your screen should look similar to the screen shot below. If you see "**gpg: Good signature from "Jacob Appelbaum (offline long term identity key) <jacob@appelbaum.net>"**" on your screen, then you have successfully verified the integrity of the program installer. The warnings that appear after that line can be ignored. **However, i**f **you see "gpg: BAD signature from "Jacob Appelbaum (offline long term identity key) <jacob@appelbaum.net>"" on your screen, delete the image and do not use it.** This means the image has probably been tampered with or got corrupted during the download process. Try downloading the image again at a later time.

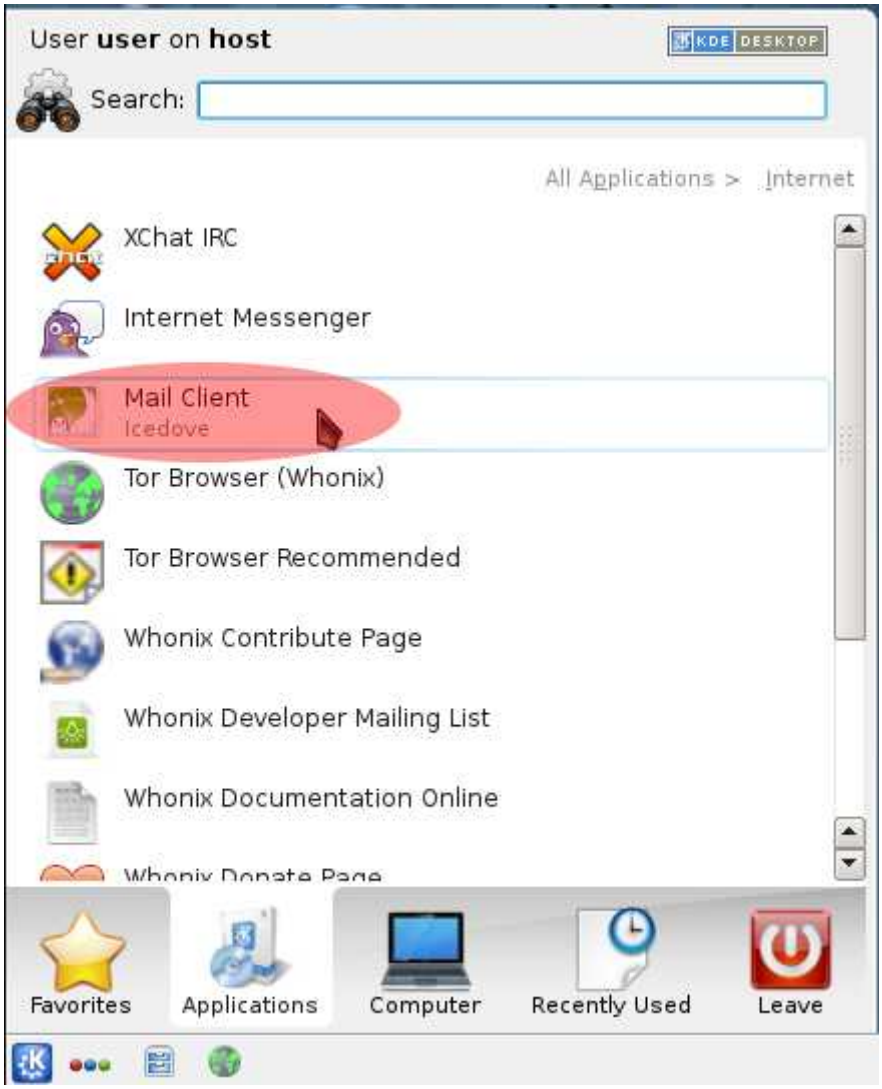


7. Now, you can close your Konsole session. Type "**exit**" and press "enter."

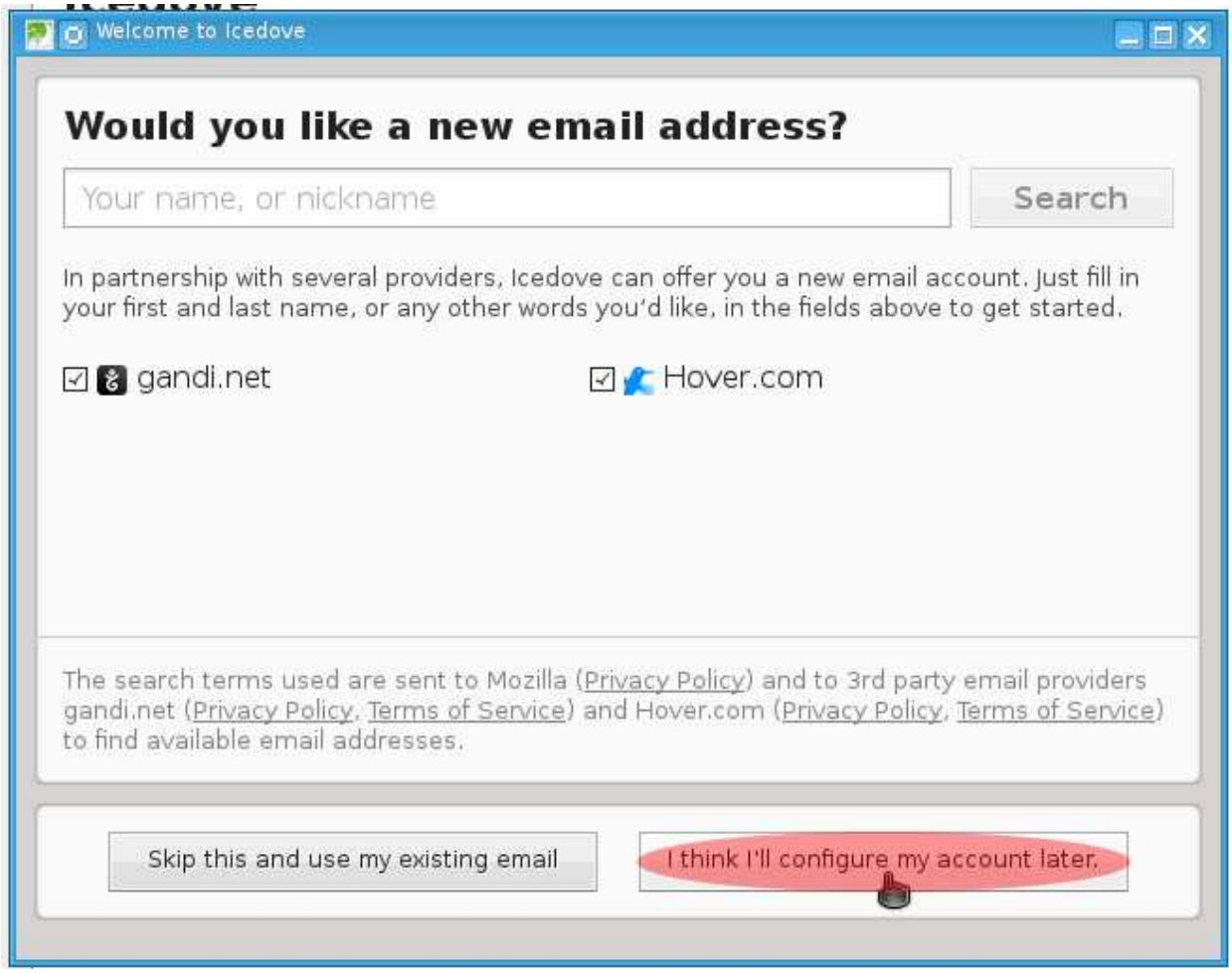
8. For simplicity, now add a shortcut for Icedove to your desktop. Click on the K start button and go to "Applications → Internet." Right-click on "Mail Client" and select "Add to Desktop." A shortcut to "Icedove" will now be on your desktop.



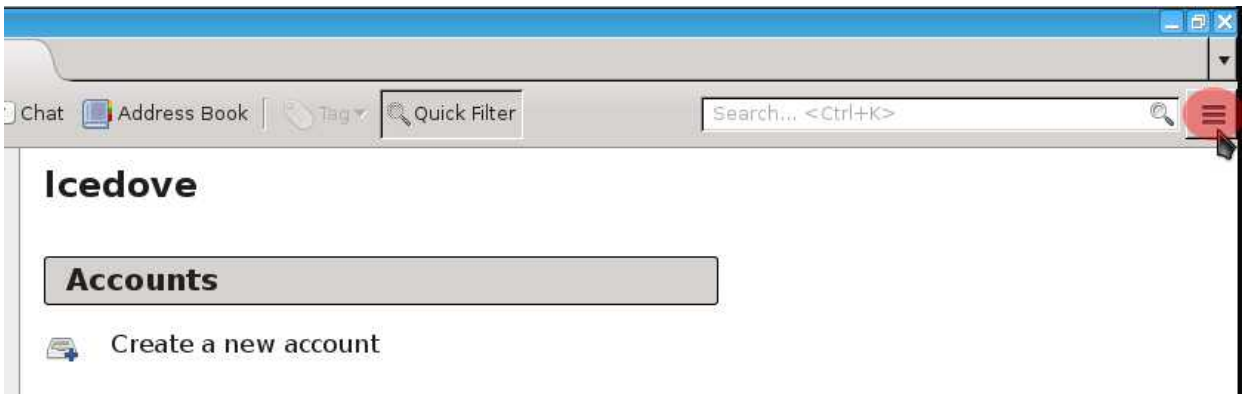
9. After you add the icon to the Desktop, the Start Menu will still be open. Click on "Mail Client" to open Icedove.



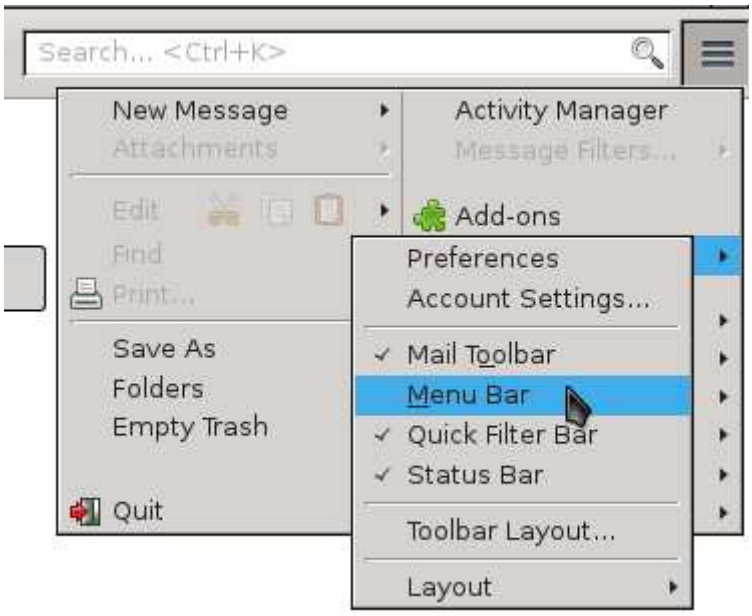
10. The first window that will appear on running Icedove for the first time will ask you if you "would like a new email address." Click on "I think I'll configure my account later."



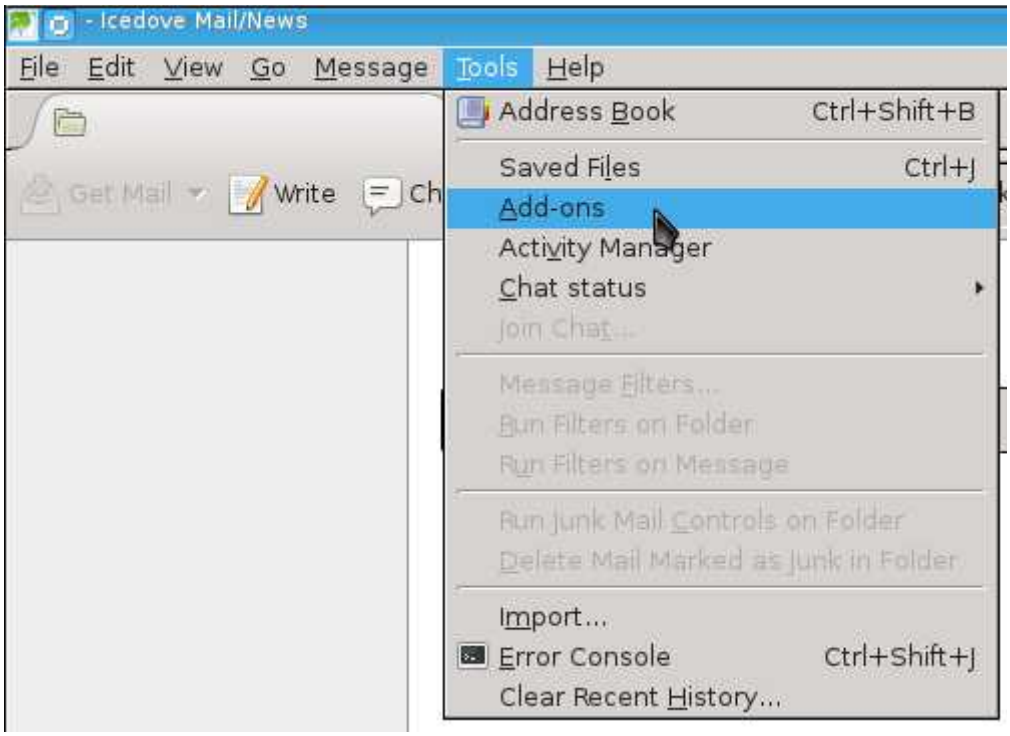
11. When you reach the main Icedove window, click on the icon that has the 3 horizontal bars towards the upper right corner.



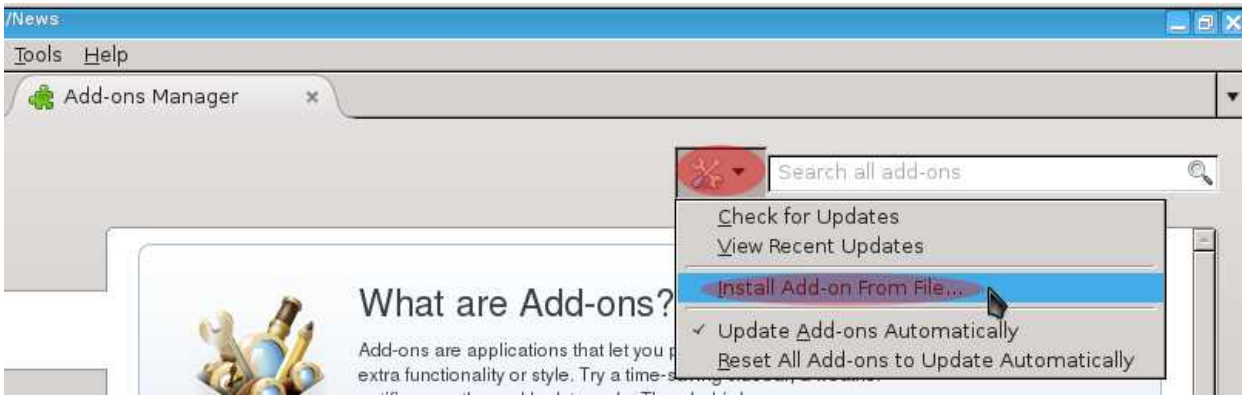
12. In the menu that appears, click on “Preferences → Menu Bar.”



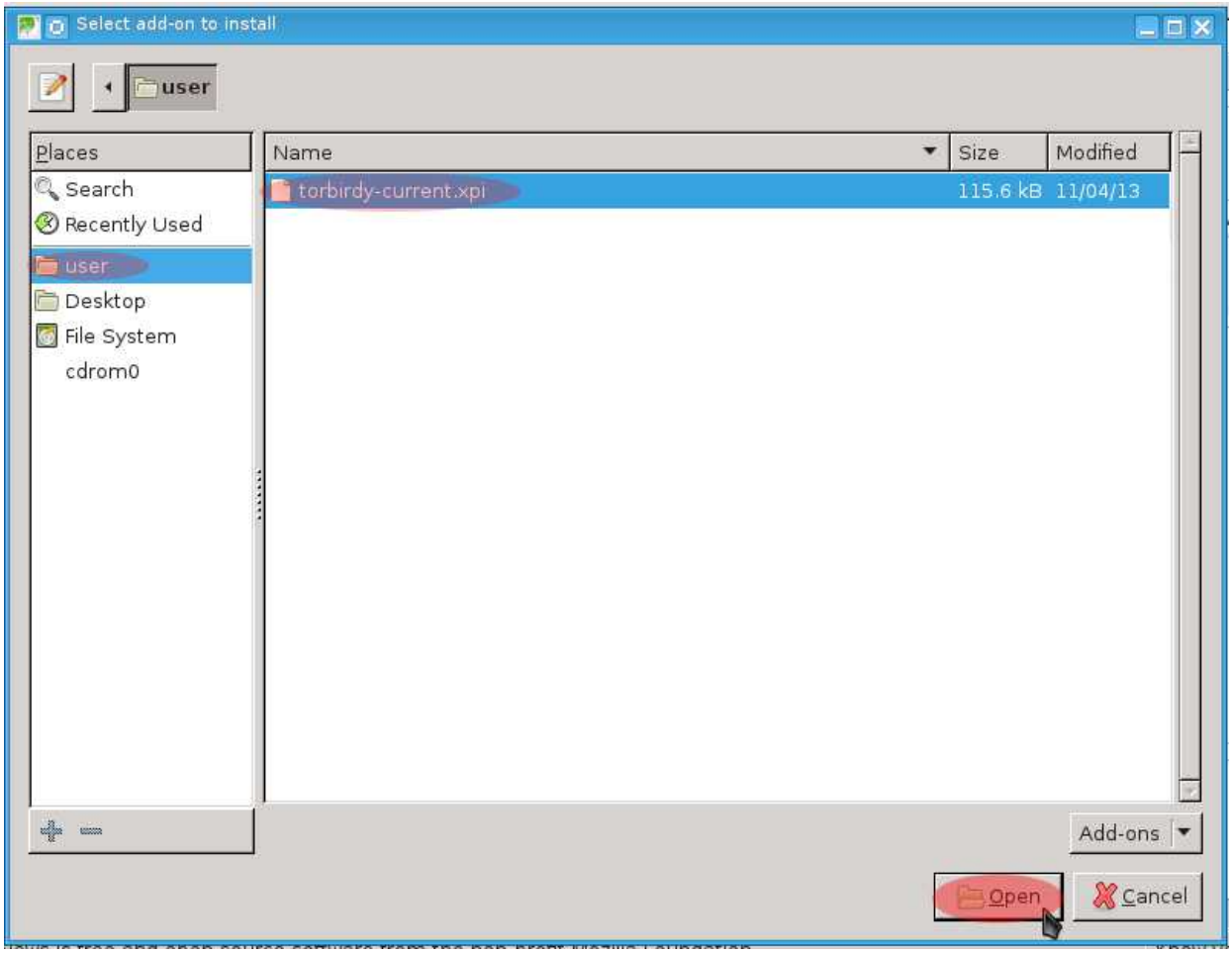
13. A menu bar will now appear towards the top of the Icedove window.
Click on “Tools → Add-ons.”



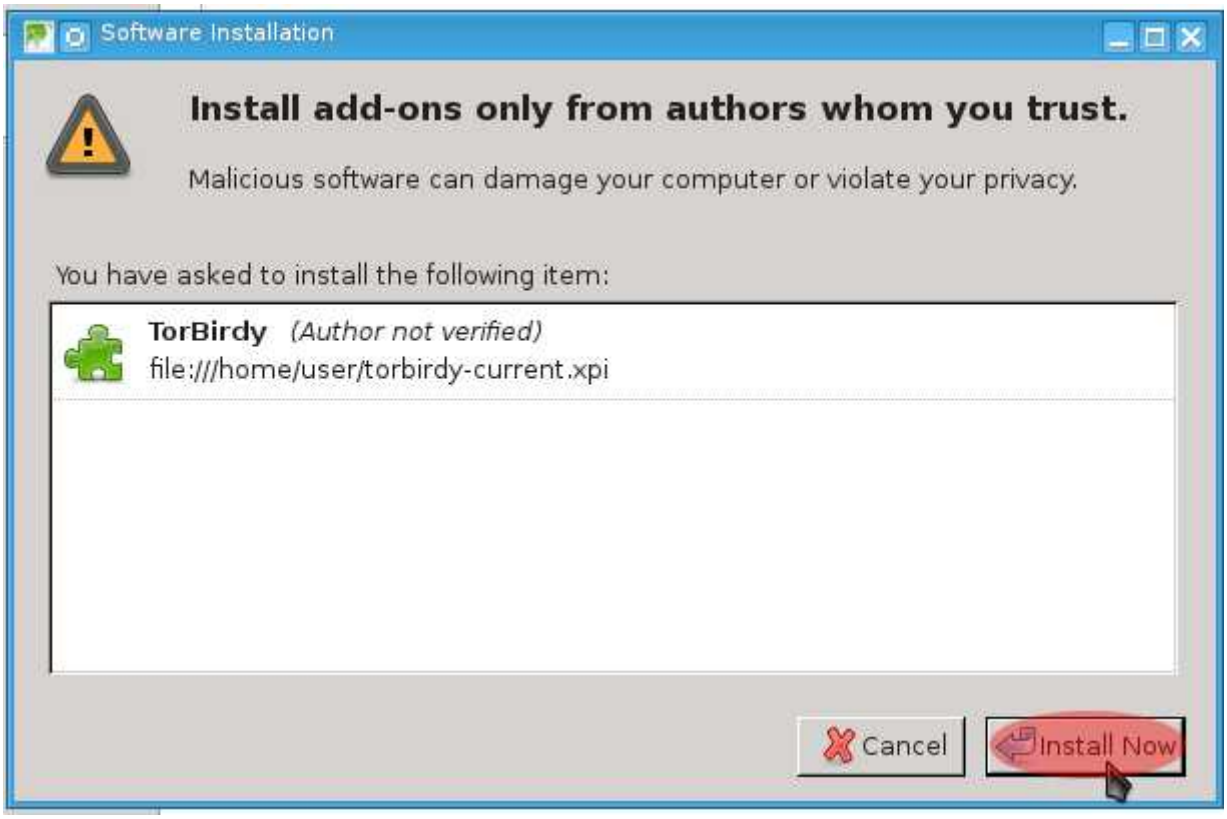
14. On the next screen, you will see an icon towards the upper right side that resembles a wrench and a screwdriver in an X formation. Click on that icon and choose “Install Add-on From File.”



15. In the next window that appears, click on the “user” icon in the left side column. Then, click on “torbirdy-current.xpi” and click on the “Open” button.

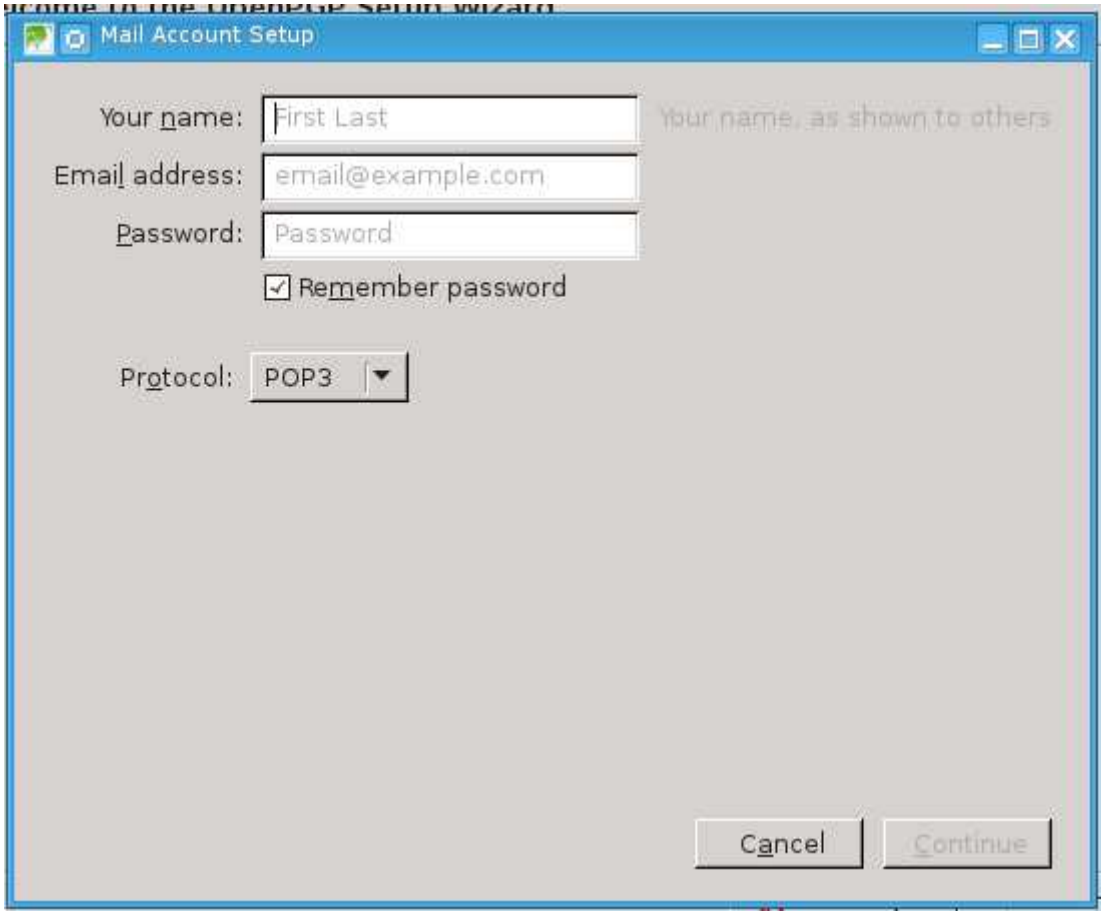


16. In the “Software Installation” window that appears, you will first be asked to wait a few seconds. When the wait timer finishes, click on the “Install Now” button.



17. When you are returned to the main Icedove screen, click on the button towards the upper right side of the window that says “Restart Now.”

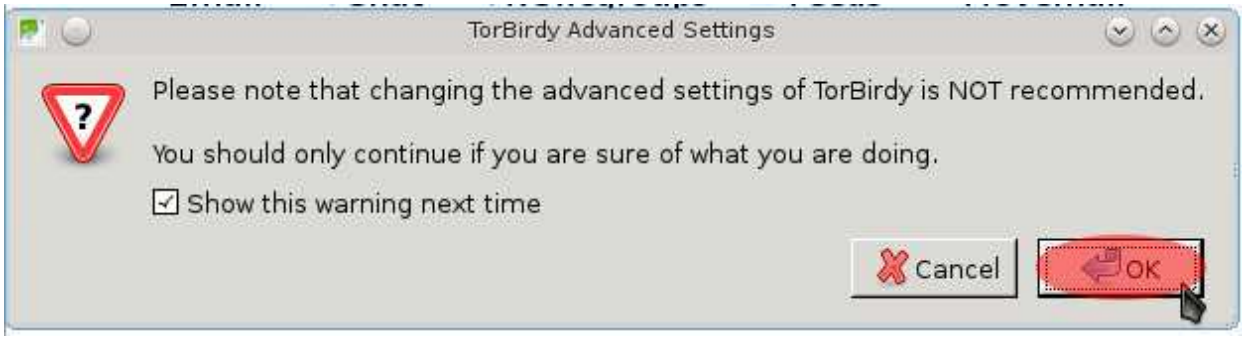
18. When Icedove restarts. You will be presented with a screen to setup your new email account that will look like the screen below.



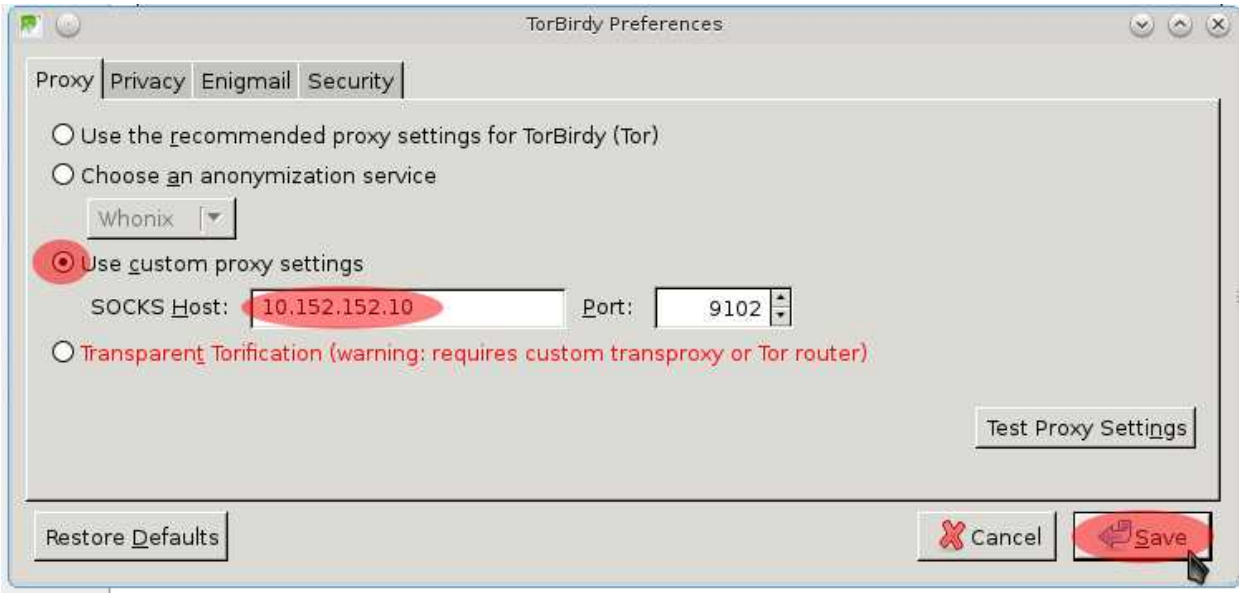
You are going to leave this window alone for now. Before entering any info, you need to manually configure TorBirdy to make full use of the protections it offers.

18b. Click on the words that say “TorBirdy Enabled” in the lower right-hand corner of the Icedove window and select “Open TorBirdy Preferences.”

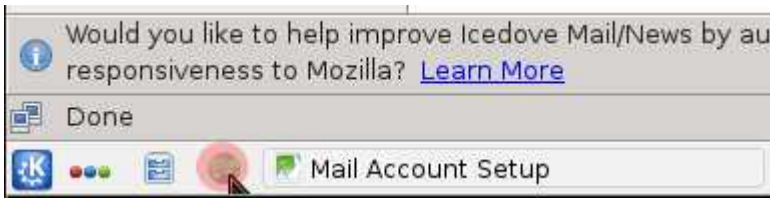
18c. A window will appear stating that changing the advanced settings of TorBirdy is not recommended. Click the “OK” button to continue.



18d. On the next screen, click on the radio button to select “Use custom proxy settings.” Then type “**10.152.152.10**” in the field next to “SOCKS Host” and click the “Save” button.



18e. Now you you need to create a new email account. So, while leaving Icedove running, click on the Tor Browser icon located near the K Start Button towards the lower left side of your screen.



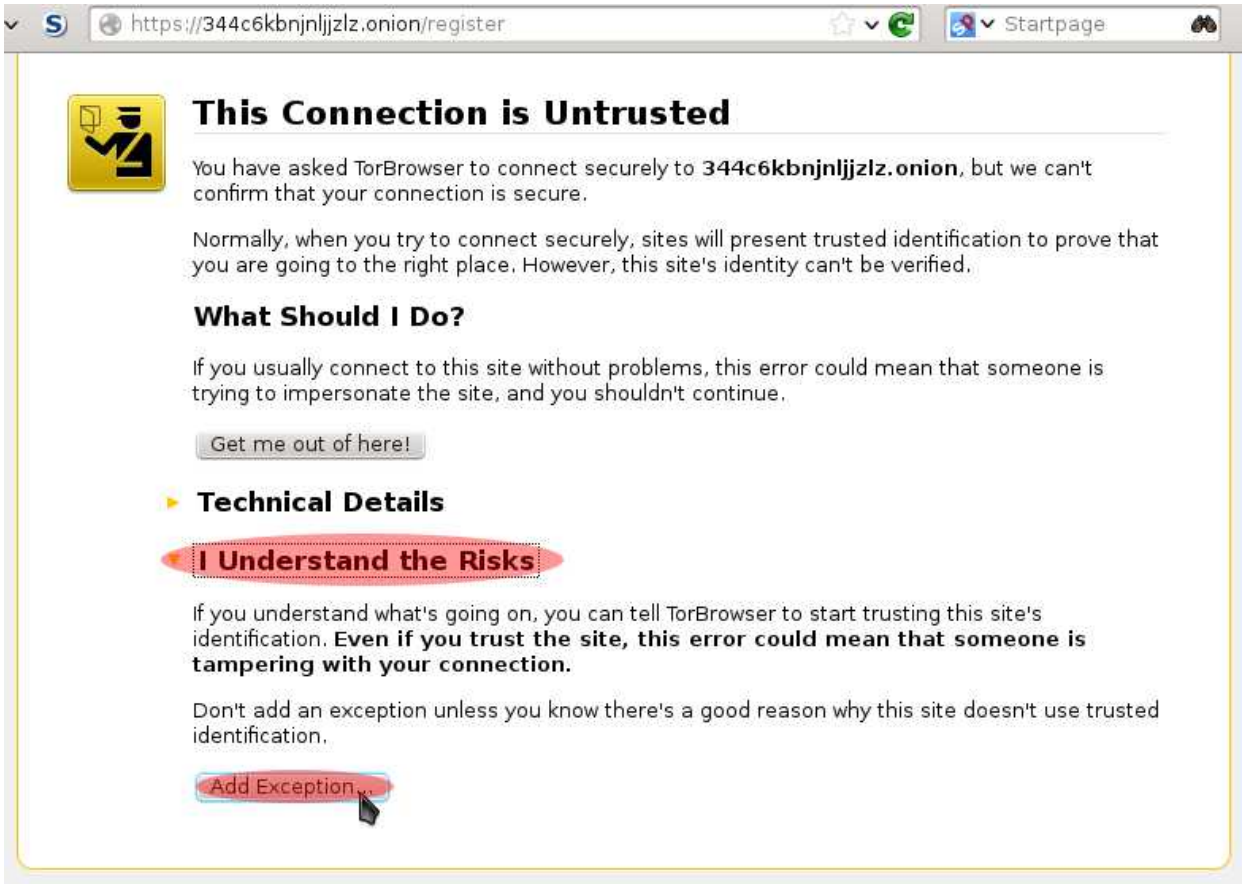
19. First and foremost, there are multiple email providers that you have the option to choose from. For the purposes of this tutorial, the example used will be vfemail.net. **This is not to be confused with an endorsement of vfemail.net as the best or most secure email provider.** In fact, vfemail.net leaves a lot to be desired. As a commercial service, vfemail.net can place text ads in the footers of your outgoing mail and has a hard limit of 50 megabytes of bandwidth per month. However, at the time of this publication, vfemail.net is one of the few free regularly available email providers offering POP3 email access through a .onion address in the Tor Hidden Network. To learn more details regarding the features and offerings of vfemail.net, go to **https://344c6kbnjnljjzlz.onion/faq.php**.

    If used properly with GPG encryption, vfemail.net's Tor Hidden email service will provide you with strong anonymity and privacy. **However, remember that this is a Tor Hidden Service which means you have no way of ever determining who is running it. Thus, if you do not use GPG to encrypt your e-mail, and the people who send you e-mail do not encrypt it with GPG either, it can be easily read by the e-mail service provider, random computers on the internet that relay a sent email message, or anyone who manages to gain access to your account!**

    When Tor Browser opens, type "**https://344c6kbnjnljjzlz.onion/register**" in your location bar to go to the vfemail.net Tor hidden service web page and press "enter."

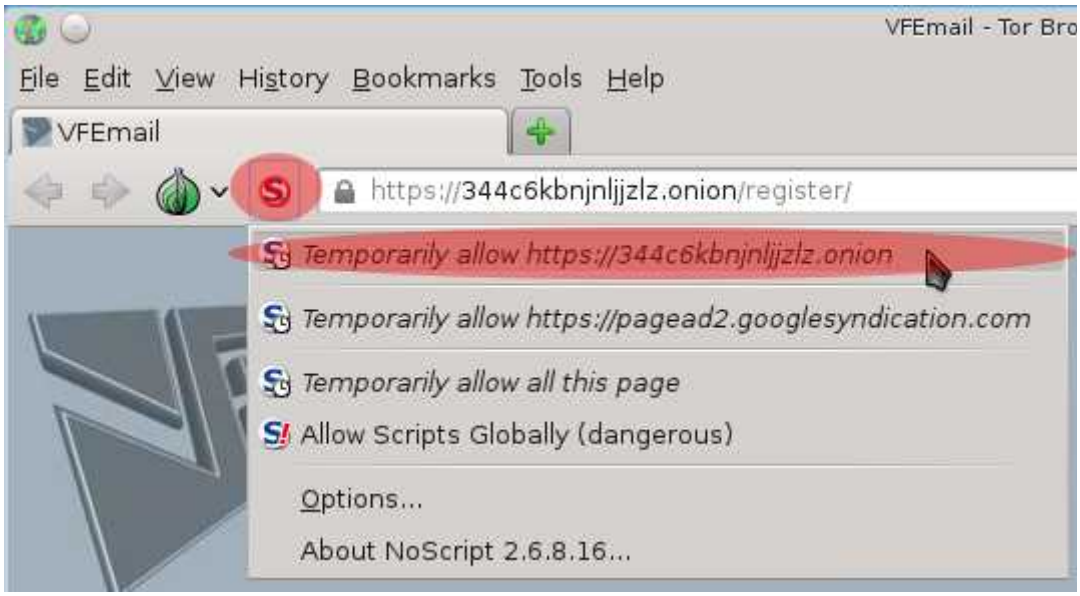
    If you wish to use another email provider, go to its registration page, create your new account with them, use KeePassX to generate your password for it, and continue to step 26.

20. Next, the Tor Browser will warn you that the web page's “connection is untrusted.” This is expected. The warning is due to the fact that the SSL certificate you received is from vfemail.net, but the domain you are connecting to is 344c6kbnjnljjzlz.onion. Click on the text that says “I understand the risks” and then click on the “add exception” button that will appear beneath it.



21. Next, a window prompting you to “add security exception” will appear. Click on the “Confirm Security Exception” button.

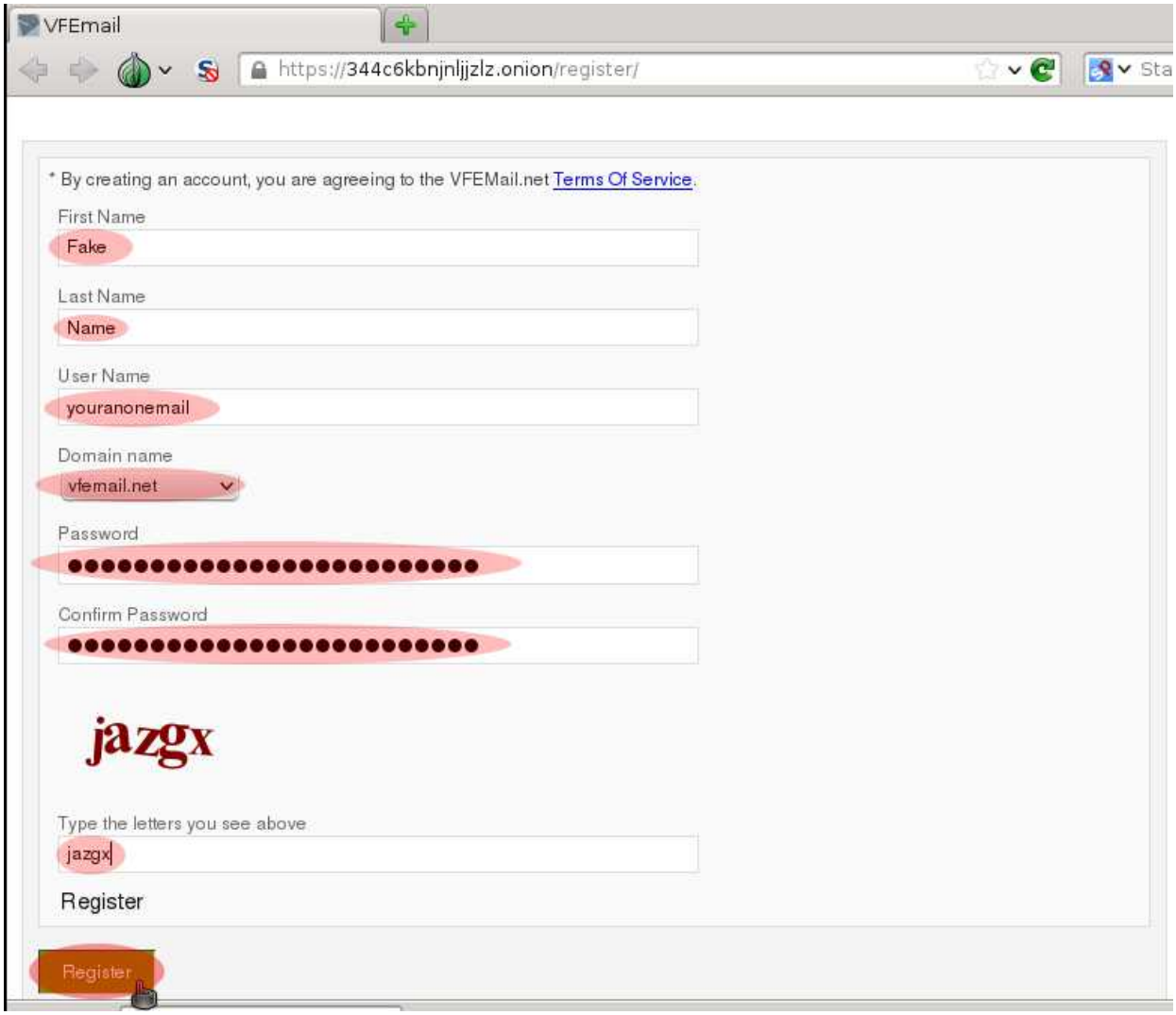
22. The registration screen for vfemail will now load. As of this publication, javascript is required for the registration process. Thus, click on the NoScript icon to the left of the browser location bar and select “temporarily allow https://344c6kbnjnljjzlz.onion.”



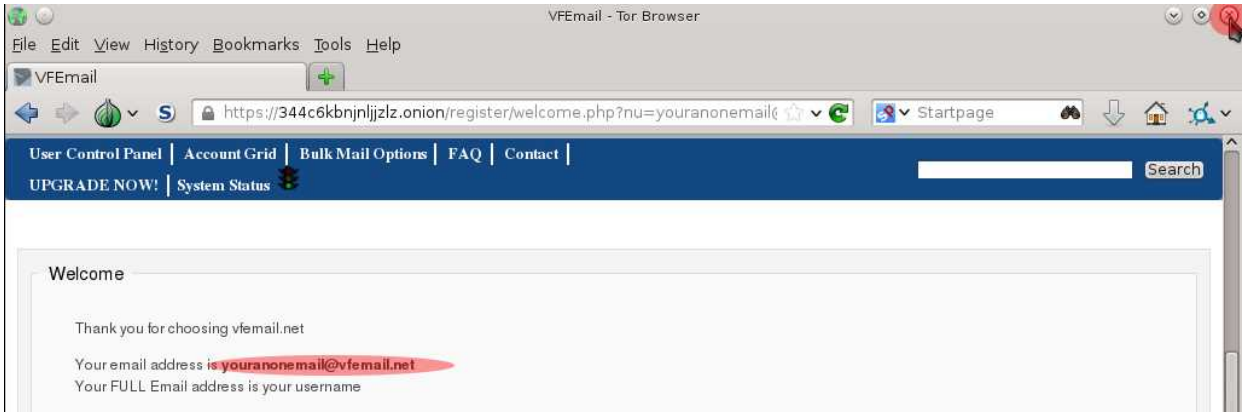
23. Now, you need to reload the page in order for the javascript to load. Click on the green icon in the far right of your browser location bar to reload the page.

24. When the page reloads, you will need to create your email account name and password. Open up KeePassX and create a password as instructed in Chapter 4b.

    When finished, creating your password in KeePassX, type fake information into the fields under “First Name” and “Last Name.” Then, type the email name you wish to use in the field under “User Name.” Next, select “vfemail.net” in the pull down menu under “Domain name.” Then, copy the password you created in KeePassX and paste it into the fields under “Password” and “Confirm Password.” Finally, type the letters that appear in the CAPTCHA puzzle in the field under the “Type the letters you see above” heading and click on the “Register” button.

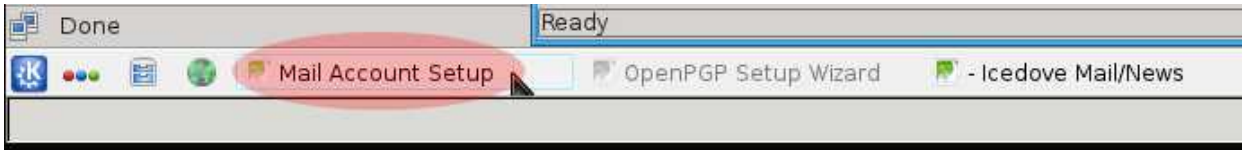


25. The next screen will confirm that you have created an account. The email address you selected will be displayed on the page. **Copy that address and paste it into the "description" or "username" fields of KeePassX that are associated with your password immediately. Then, save your KeePassX database**. Then, click the X button to close Tor Browser and continue to the next step.

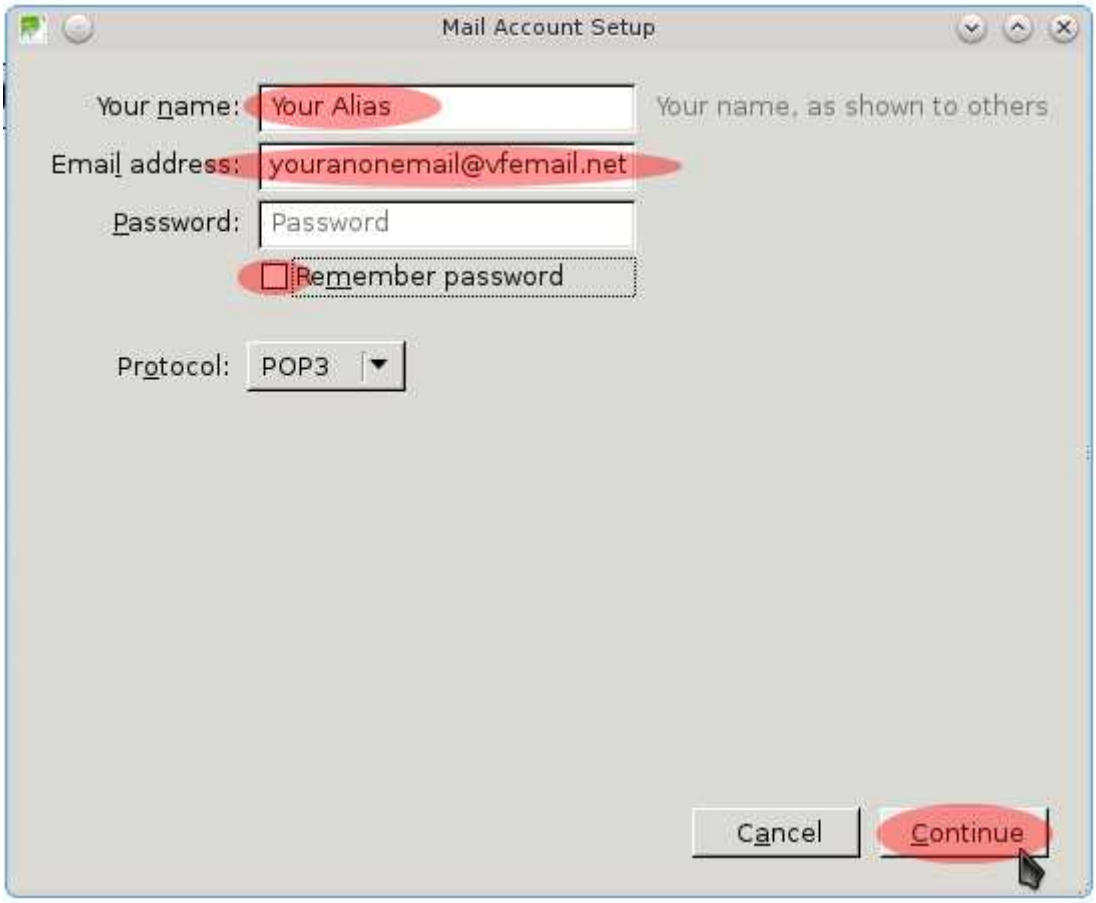


26. Now, return to your Icedove "Mail Account Setup" window by clicking on the "Mail Account Setup" button in your taskbar at the bottom of the screen. It is highlighted in red in the image below.

    From this point forward,if you did not choose the vfemail.net hidden server as your email provider, you will need to use the appropriate server name/domain name where "**344c6kbnjnljjzlz.onion**" is instructed as the entry in this tutorial.

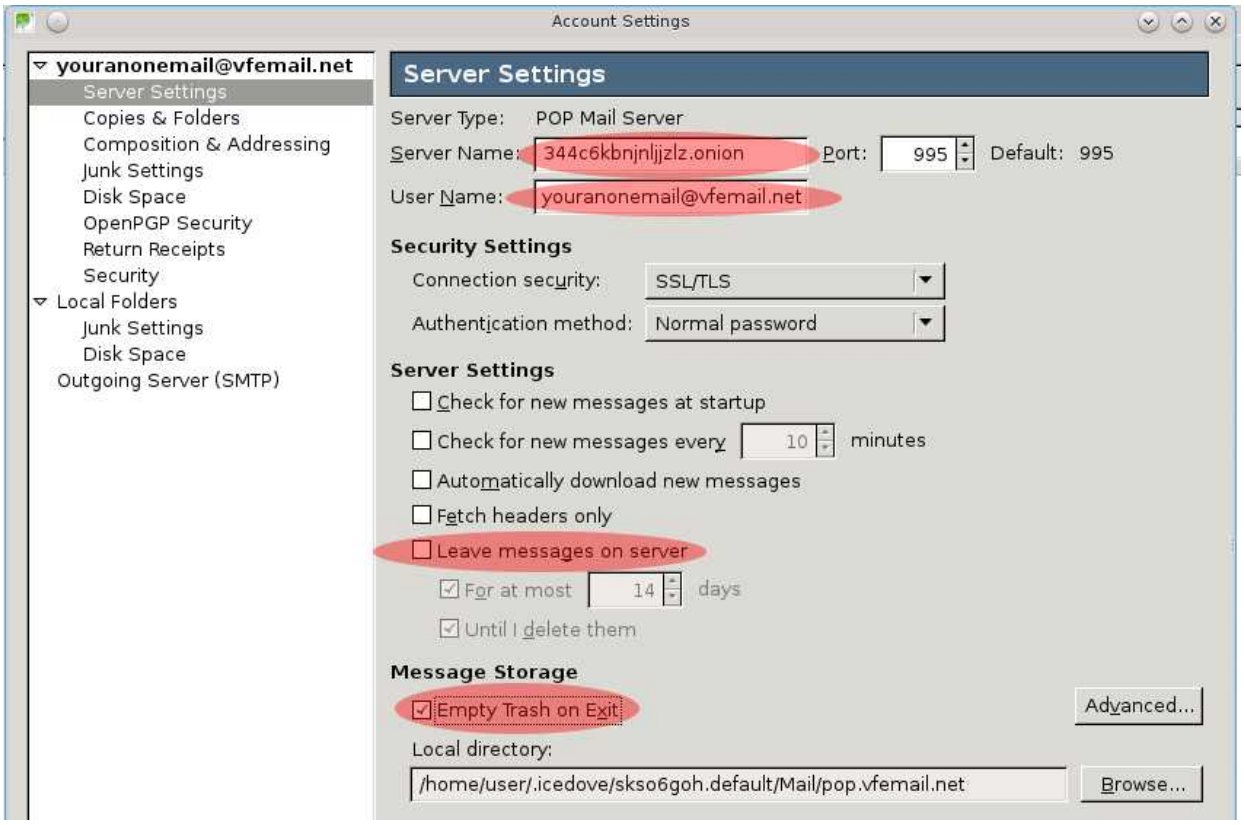


27. When you are returned to the “Mail Account Setup” window, type the alias that you wish to use in the field next to “Your name.” This will appear next to your email address in emails you send to others. Then, type the vfemail.net email address you just created into the field next to “Email address.” Finally, uncheck “remember password” and click the “Continue” button.

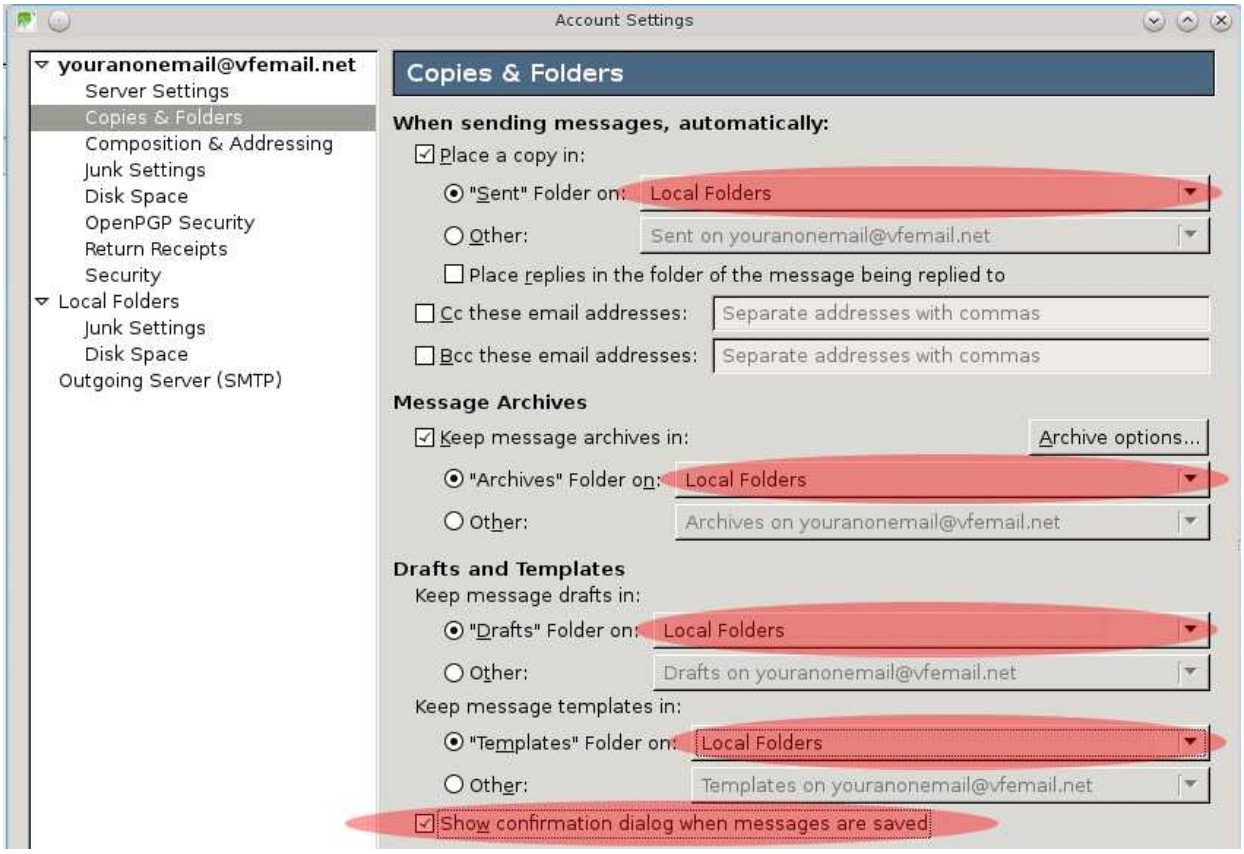


28. The next window that appears will inform you that Torbirdy has blocked the automatic configuration process to protect your anonymity. Click on the “OK” button to continue.

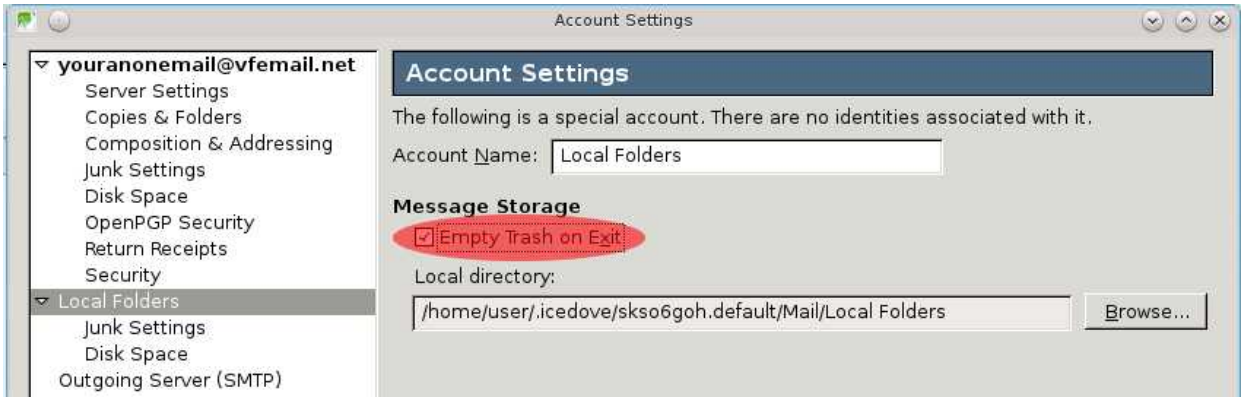
29. In the next window, you need to configure Icedove to connect to the hidden server of vfemail.net. The fields you need to change are highlighted in red. Type "**344c6kbnjnljjzlz.onion**" in the field next to "Server Name." Then, type your **complete email address** into the field next to "User Name." Additionally, **unmark the box** next to "Leave messages on server." Finally, mark the box next to "Empty Trash on Exit" and continue to the next step.



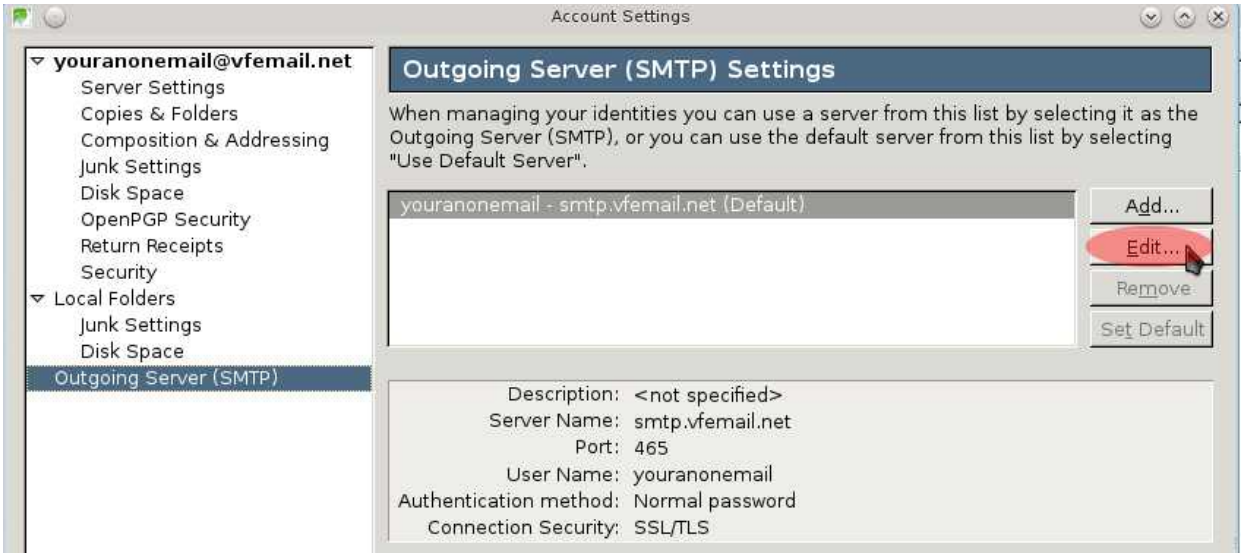
30. Next, click on “Copies and Folders” in the left column. Each option you will need to change is highlighted in red below. In the pull down menu next to “'Sent' Folder on,” select “Local Folders.” Next, in the pull down menu next to “'Archives' Folder on,” select “Local Folders.” Additionally, in the pull down menu next to “'Drafts' Folder on,” select “Local Folders.” Now, in the pull down menu next to “'Templates' Folder on,” select “Local Folders.” Finally, mark the box next to “show confirmation dialog when messages are saved.” When finished, continue to the next step.



31. Next, click on “Local Folders” in the left column. Then, click on “Empty trash on exit.” When finished, continue to the next step.

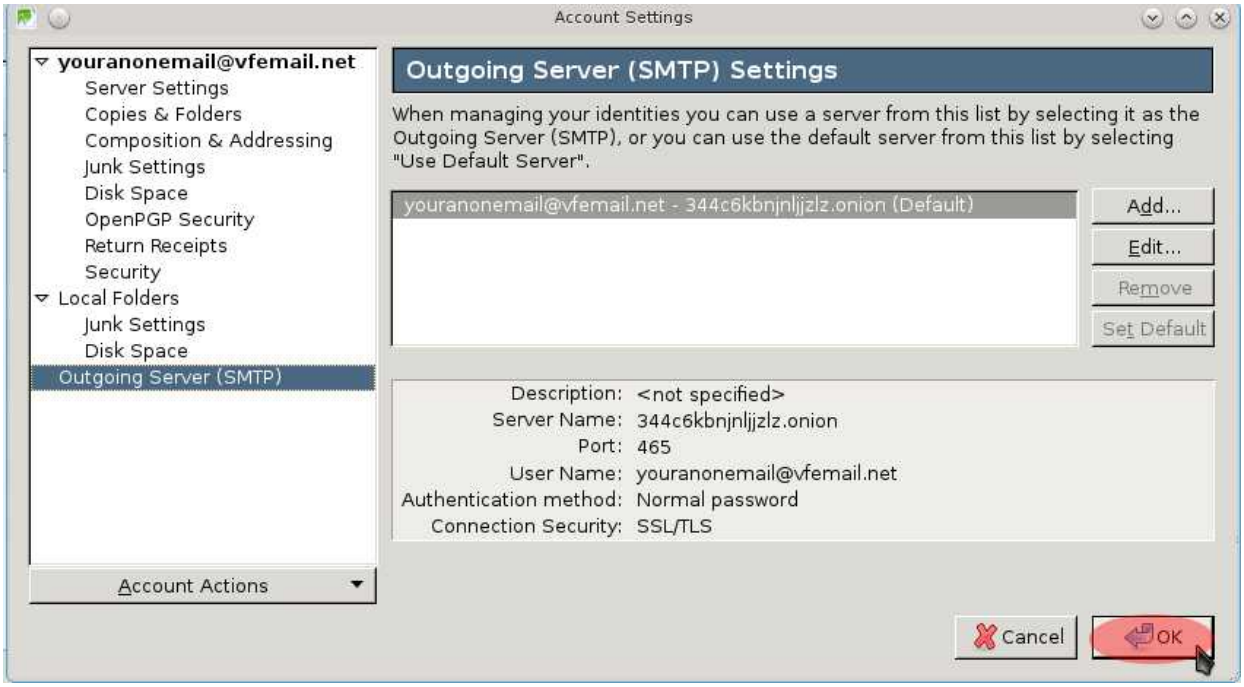


32. Now, click on “Outgoing Server (SMTP)” in the left column. Then, click on the “Edit” button.



33. In the next window that appears,type “**344c6kbnjnljjzlz.onion**” in the field next to “Server Name.” Then, type your **complete email address** into the field next to “User Name.” Finally, click on the “OK” button.

34. When you are returned to the “Account Settings” window, click on the “OK” button.

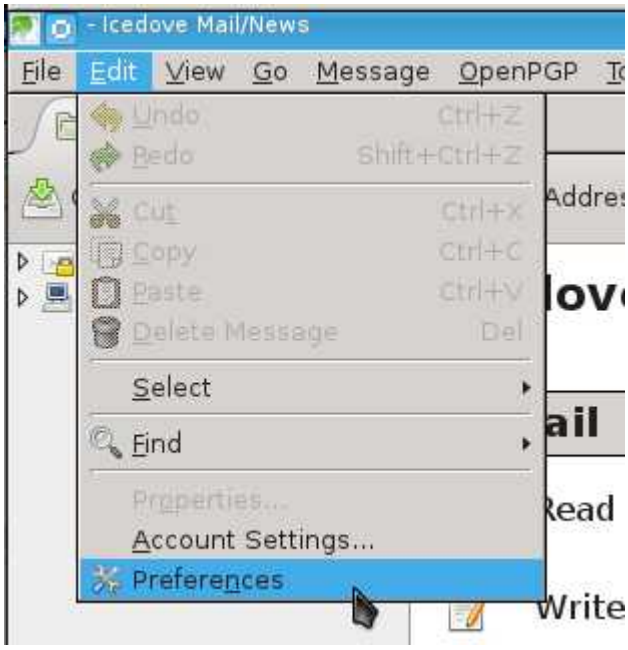


35. Icedove will now attempt to connect to 344c6kbnjnljjzlz.onion. When it connects, the “Add Security Exception” window will appear informing you that there is an issue with with the SSL certificate. This is expected. The warning is due to the fact that the SSL certificate you received is from vfemail.net, but the domain you are connecting to is 344c6kbnjnljjzlz.onion. Click on the “Confirm Security Exception” button.

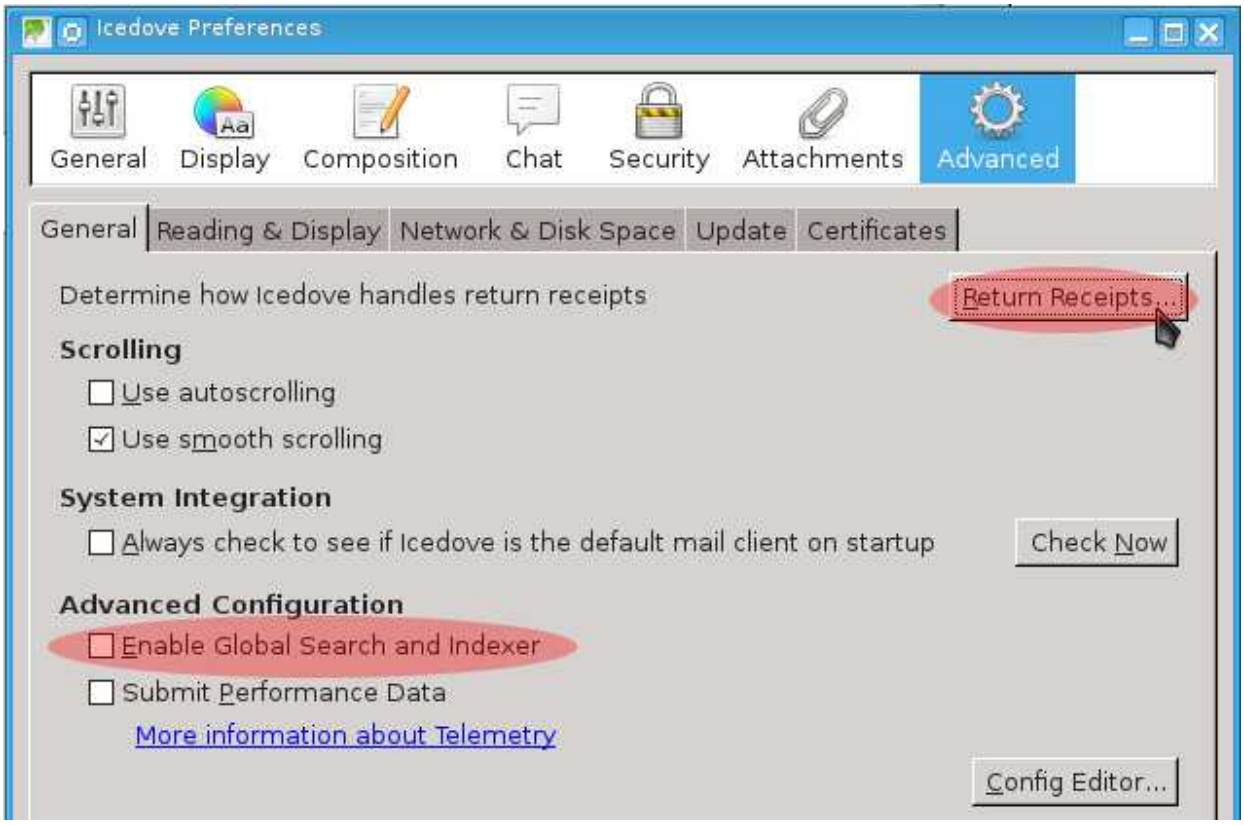
36. You will now be returned to the “Add-ons Manager” tab in the main Icedove window. At the bottom of your screen, Icedove will likely be asking you if you wish to help improve Icedove by sending various data to Mozilla. Click “No.”

37. Next, close the “Add-ons Manager” tab. Click on the “x” in the tab.

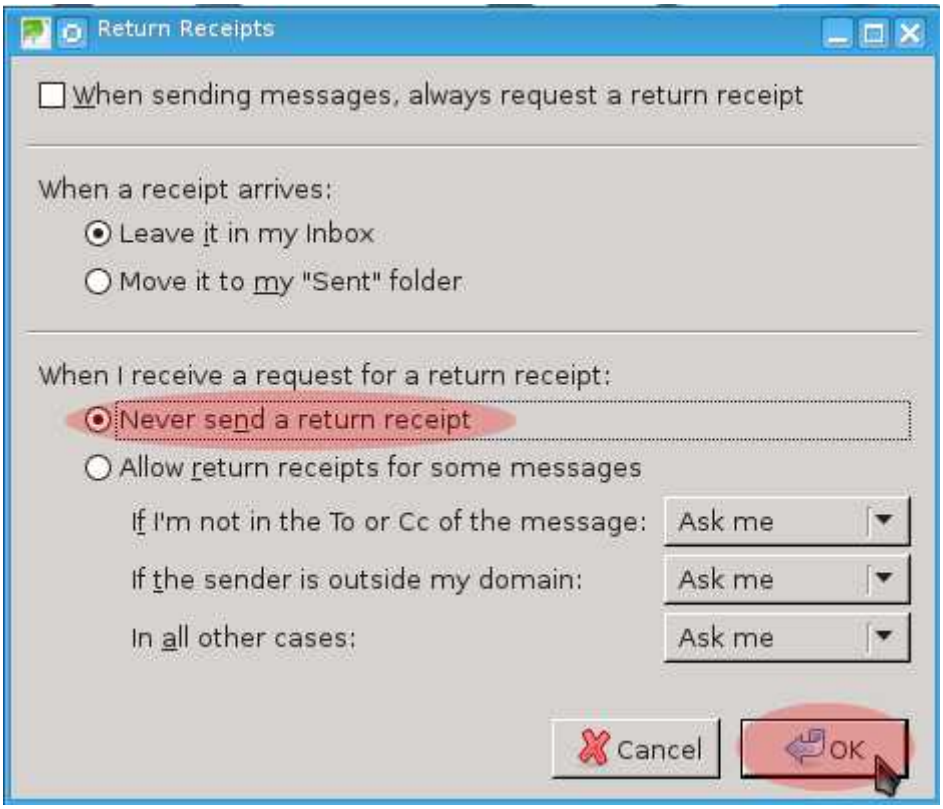
38. You will now be returned to the main Icedove window. Click on “Edit → Preferences.”



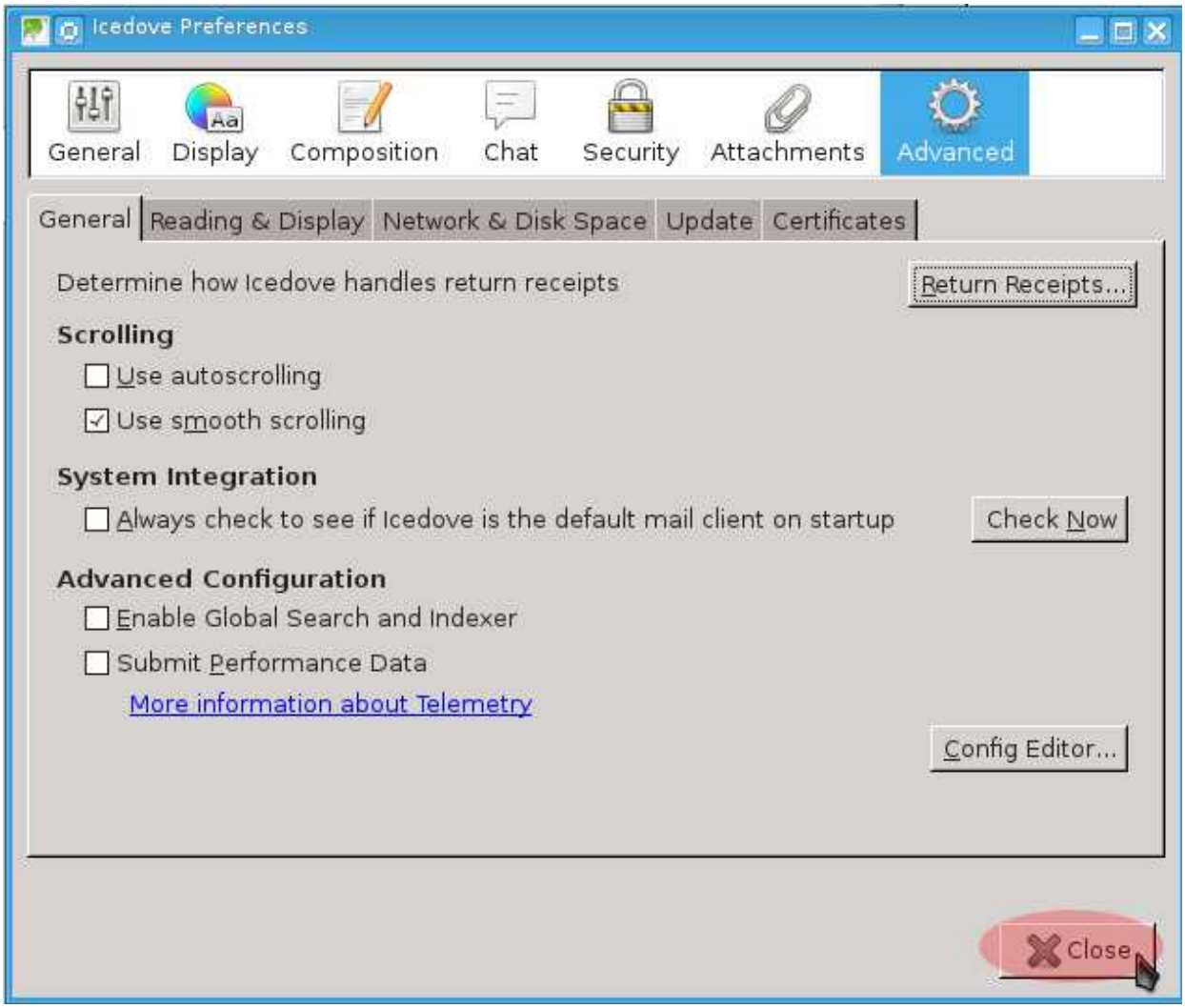
39. In the window that appears, click on the “Advanced” tab. Unmark the box next to “Enable Global Search and Indexer.” Then, click on the “Return Receipts” button.



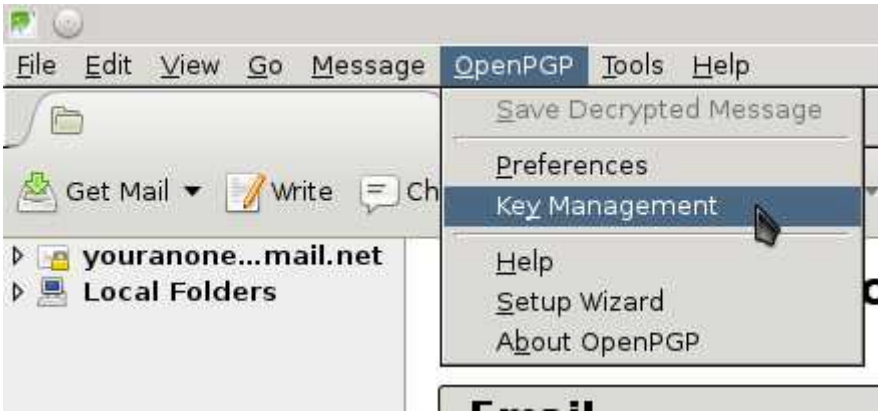
40. In the next window that appears, mark the circle next to “Never send a return receipt.” Then, click the “OK” button.



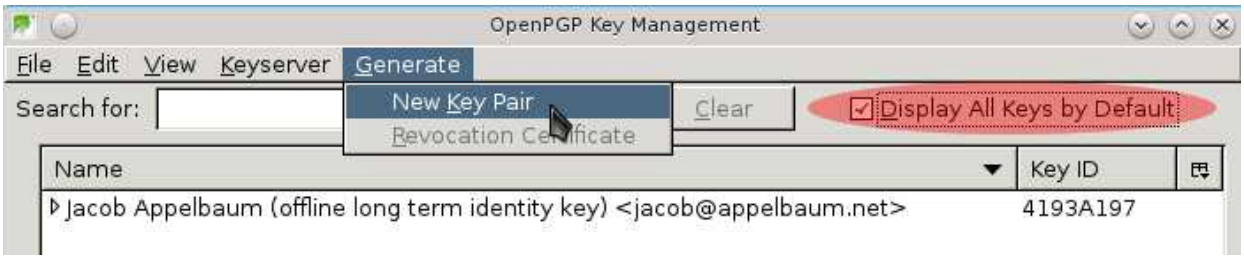
41. When you are returned to the “Icedove Preferences” window, click the “Close” button.



42. Next, you will be returned to the main Icedove window. Click on “OpenPGP → Key Management.”

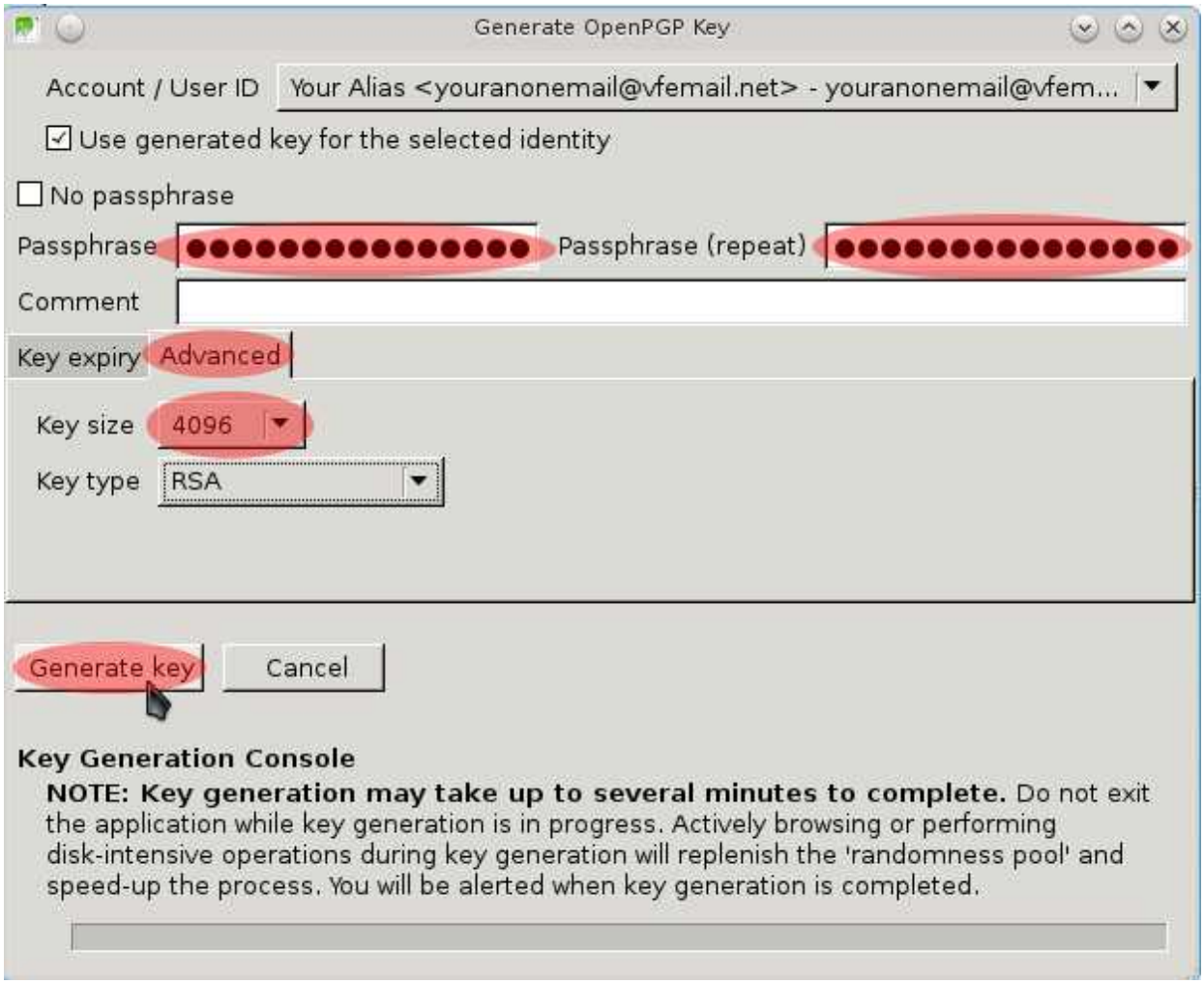


43. In the next window that appears, mark the box next to “Display All Keys by Default.” You will now see the public GPG key you imported earlier for Jacob Appelbaum. Then, click on “Generate → New Key Pair” to begin the process of creating your personal GPG keys.



44. In the next window that appears, choose a strong passphrase and input it into the fields next to “Passphrase” and “Passphrase (repeat).” Create your passphrase using the same methodology that you used for the passphrase to encrypt your hard drive in the beginning of this tutorial. You will need your passphrase to sign messages with GPG or to decrypt messages sent you. With a strong passphrase, if your machine is ever compromised and someone steals your GPG Secret Key, you won't have to worry about them being able to read your encrypted emails or being able to impersonate you.

    After you have entered your passphrase in the appropriate fields, click on the “Advanced” tab. Click on the pull down menu next to “Key size” and select “4096.” Then, click on the “Generate Key” button.

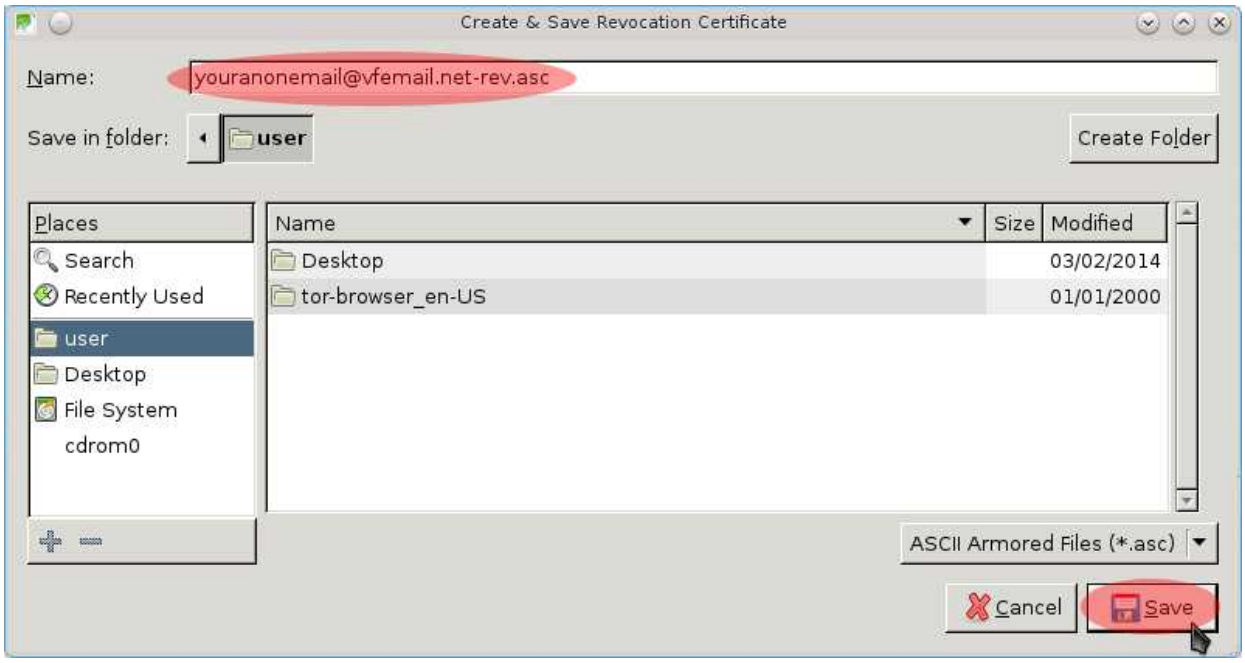


45. When the next window appears, click the “Generate Key” button.

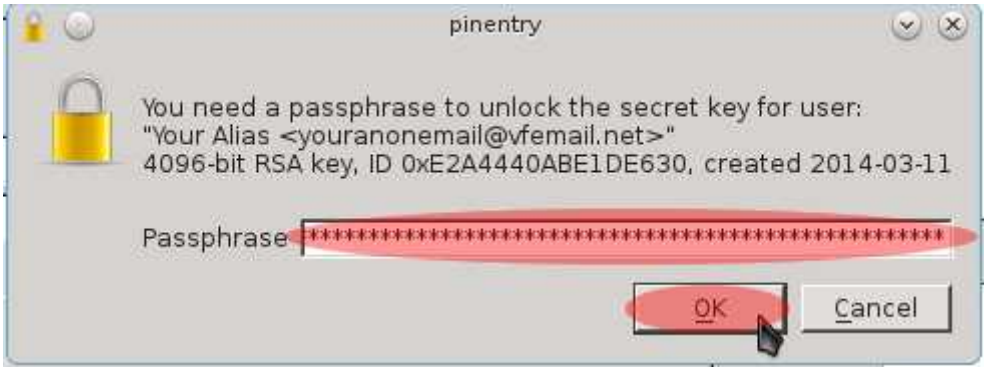
46. You will now be returned to the “Generate OpenPGP Key” window. However, this time you should notice a progress bar moving on the bottom of the window. The key generation process needs to collect entropy in order to generate the keys. Thus, either move your mouse around in a random manner or open a copy of Tor Browser and browse to random sites.

    When the key generation process has completed, on the window that appears, click on the “Generate Certificate” button.

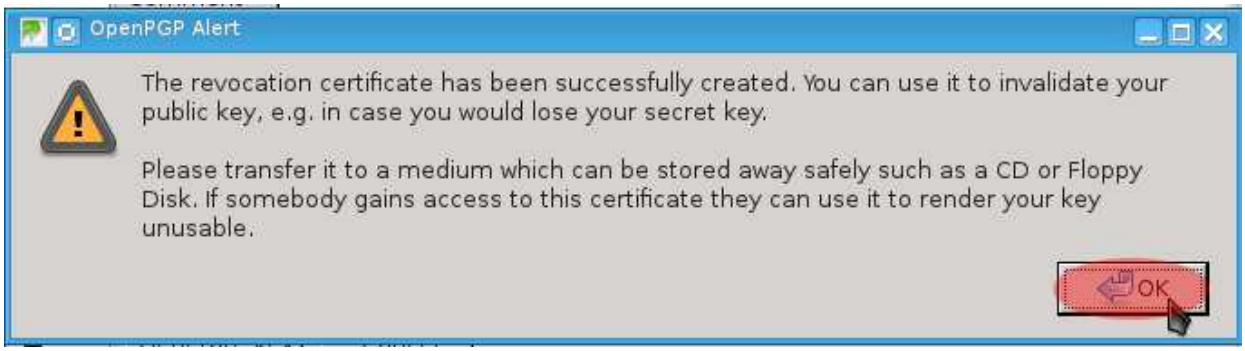
47. The next window will ask you where you want to store your GPG Revocation Certificate. Click on “user” in the left column. Then, choose a filename other than the default for your GPG Revocation Certificate. The default name uses spaces which can make a step later in this guide trickier for you. Finally, click the “Save” button.



48. You will next be prompted for your GPG passphrase to create and save the GPG Revocation Certificate. Type you GPG passphrase you created in the steps above and click the “OK” button.

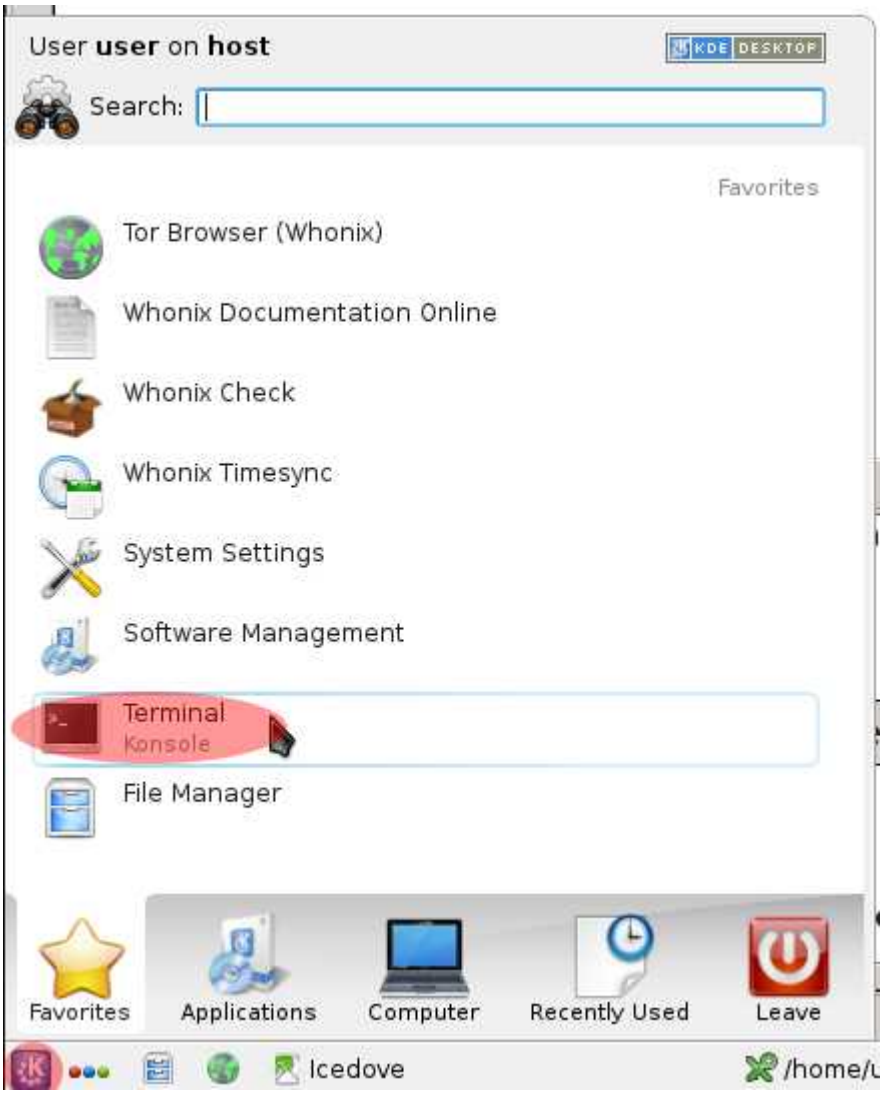


49. Next, you will be informed the the GPG revocation certificate was successfully created. Click the “OK” button.



50. **Note:** The following steps are optional, but recommended. Before continuing with Icedove, take the time to encrypt your revocation certificate. Your GPG revocation certificate can be used to revoke your public encryption key that you have added to key servers even if you no longer have access to your GPG Secret Key or have forgotten your password. If an attacker gets their hands on your GPG revocation certificate, they can revoke your keys. Encrypting the GPG revocation certificate with a passphrase you can remember will protect you against an attacker using it to revoke your keys if they manage to steal your revocation key. Open up a Konsole / Terminal session to get to a command prompt. Click the K start button and then click “Terminal.”

    If you wish to skip encrypting your revocation key, continue from step 56.

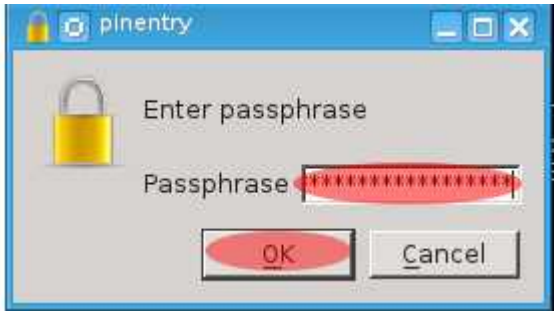


51. At the command prompt, type
"**gpg --cipher-algo --symmetric RevocationCertificateFileName**" and press "enter."

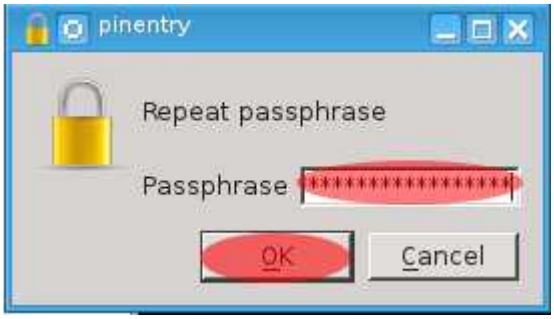
    Tip: If you included spaces in your file name, once you typed the first few letters of it, you can complete the rest of the file name by pressing the "Tab" key. This can save you time when typing any file name from the command prompt.

```
user@host:~$ gpg --cipher-algo AES256 --symmetric youranonemail@vfemail.net-rev.asc
```

52. You will be prompted to "Enter passphrase." Choose a secure passphrase and enter it into the passphrase field. Then, click the "OK" button. If you ever need to use your revocation certificate, this the passphrase you will use to decrypt it first.



53. You will be asked to re-enter your passphrase. Type it again into the passphrase field and click the "OK" button.



54. Eventually, you will be returned to the shell prompt. Type "**ls *.gpg**" and press "enter." If you see a file that has the same name as your revocation certificate ending with ".gpg," you have successfully encrypted your revocation certificate ad can continue to the next step. If you don't see such a file, start again from step 51.

```
user@host:~$ ls *.gpg
youranonemail@vfemail.net-rev.asc.gpg
user@host:~$
```

55. Now, securely delete your unencrypted revocation key.
    Type "**shred -n 30 -uvz RevocationCertificateFileName**" and press enter.

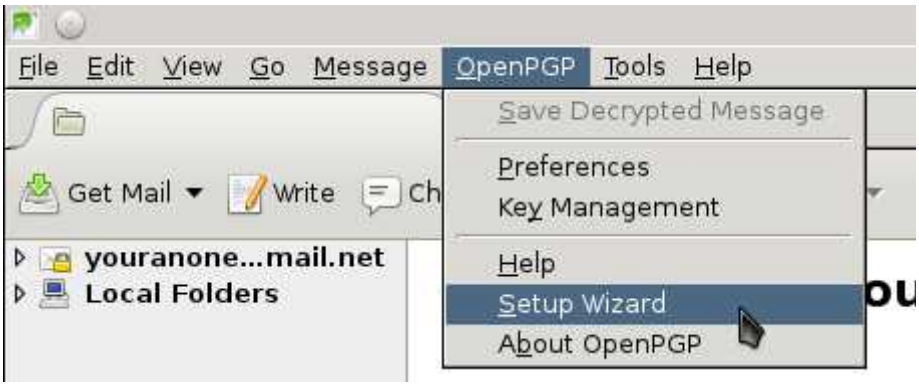
```
user@host:~$ shred -n 30 -uvz youranonemail@vfemail.net-rev.asc
```

    When the process completes, close the Terminal/Konsole window by clicking on the "x" in the upper right corner or typing "**exit**" and pressing enter. Then, go back to Icedove.

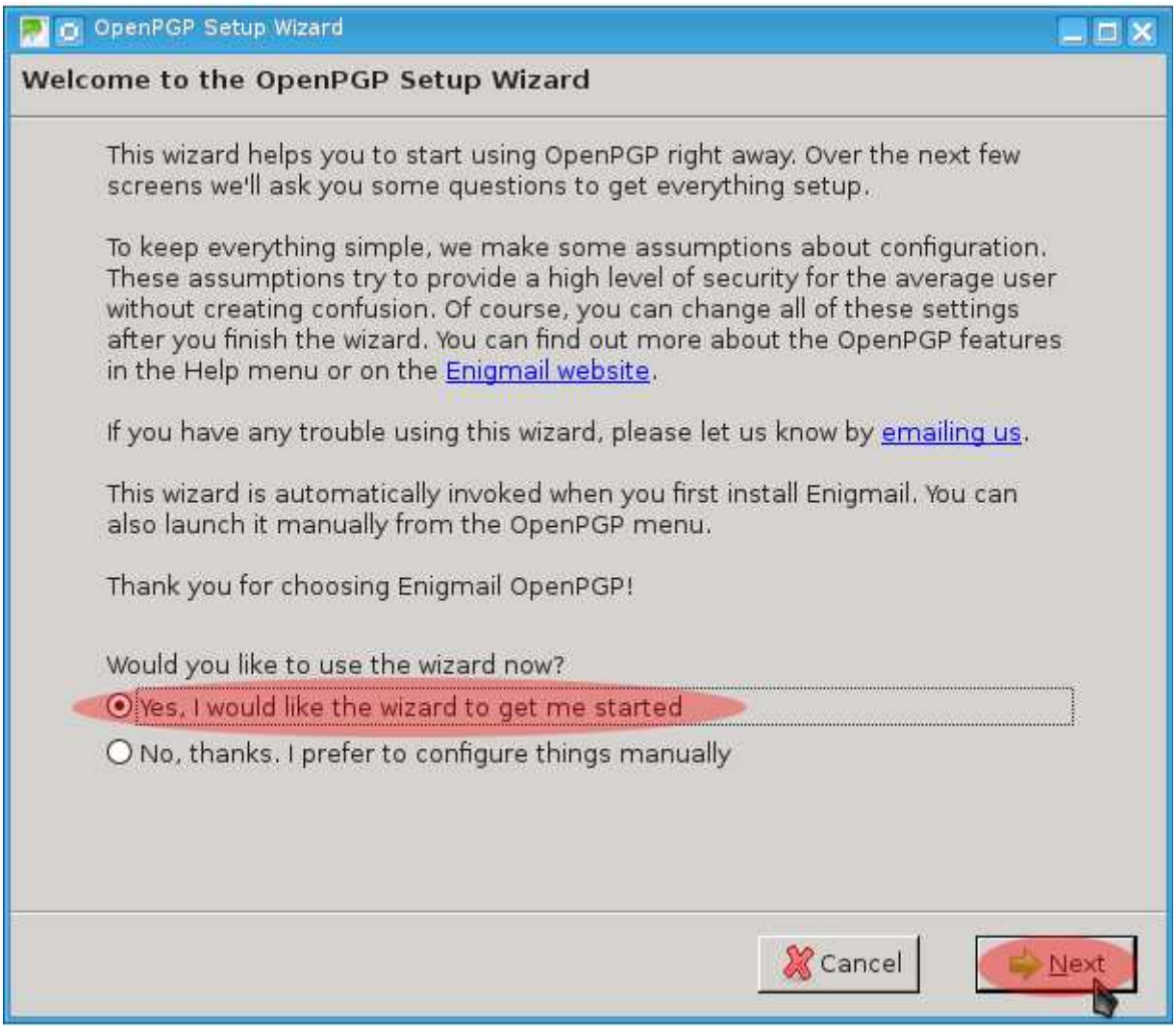
    In the future, if you ever need to use your revocation key, decrypt it by typing "**gpg -o RevocationCertificateFilename.asc -d RevocationCertificateFilename.gpg**".

56. In Icedove, the Key Manager window will now show your GPG key in your key library. It will appear in a bold font. You can now close this window.

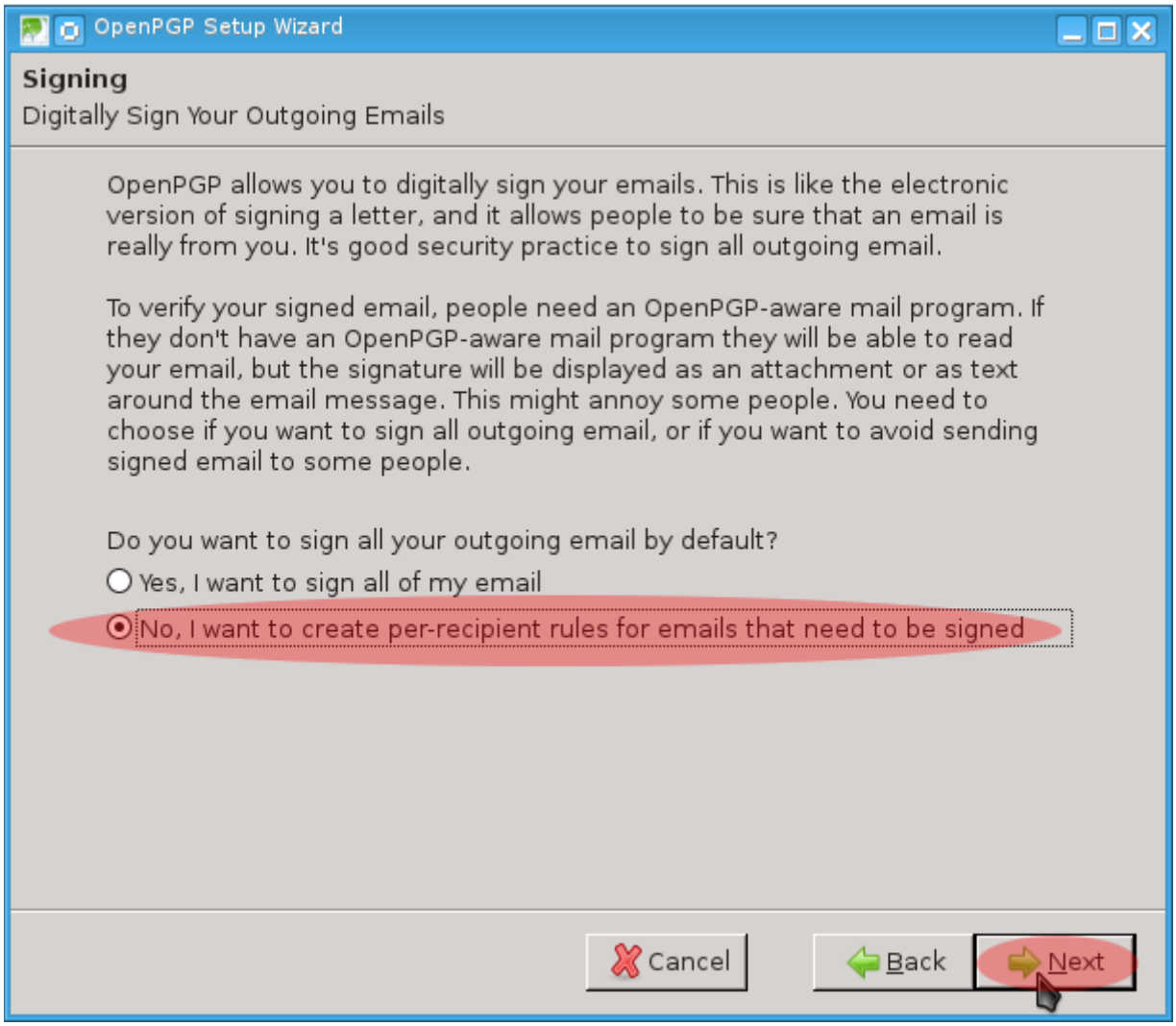
57. Next, in Icedove, click on "OpenPGP → Setup Wizard."



58. On the next window that appears, choose “Yes, I would like the wizard to get me started” and click the “Next” button.

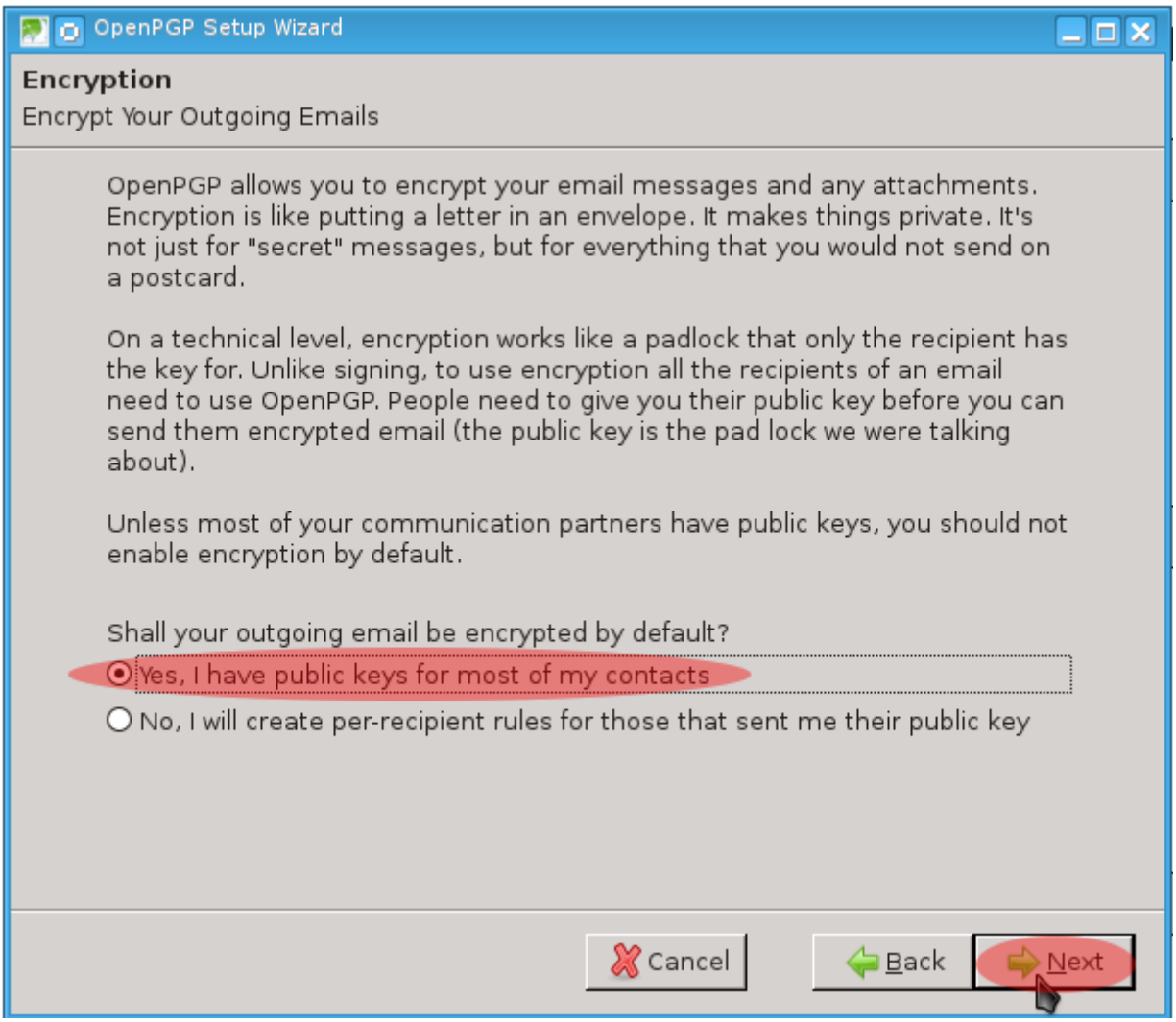


59. On the next screen, you will be asked if you want to “digitally sign all of your outgoing emails.” Select “No, I want to create per-recipient rules for emails that need to be signed.” Then, click the “Next” button.

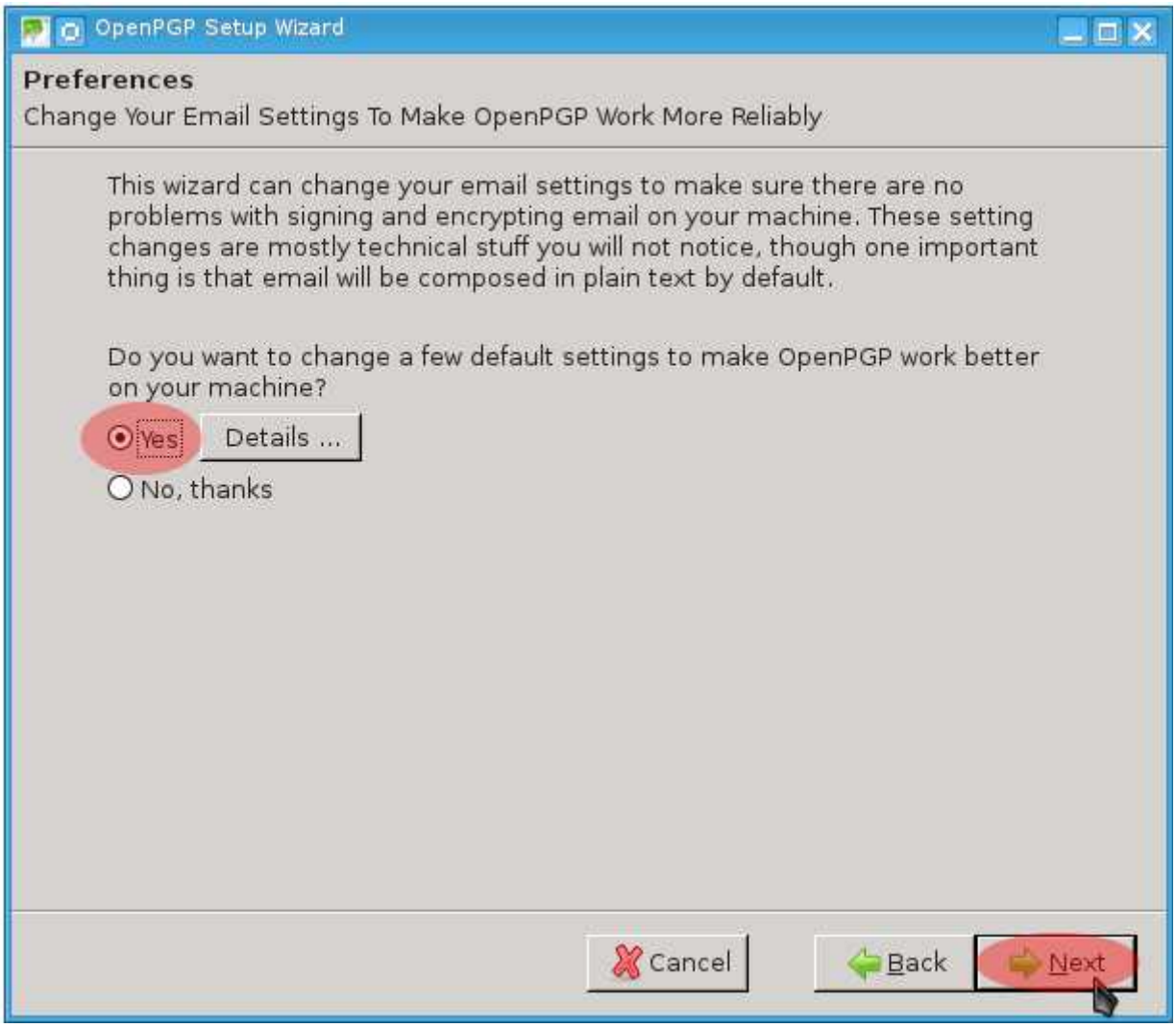


60. On the next screen, you will be asked if you wish to encrypt all outgoing emails. Choose “Yes, I have public keys for most of my contacts” and click the “Next” button.

    Note: You may read or hear elsewhere that this makes sending email to people who do not use GPG more stressful. Ignore such discussions. It is not more stressful than accidentally sending a message to someone unencrypted that should have been encrypted. The option you selected above makes such a scenario much less likely.

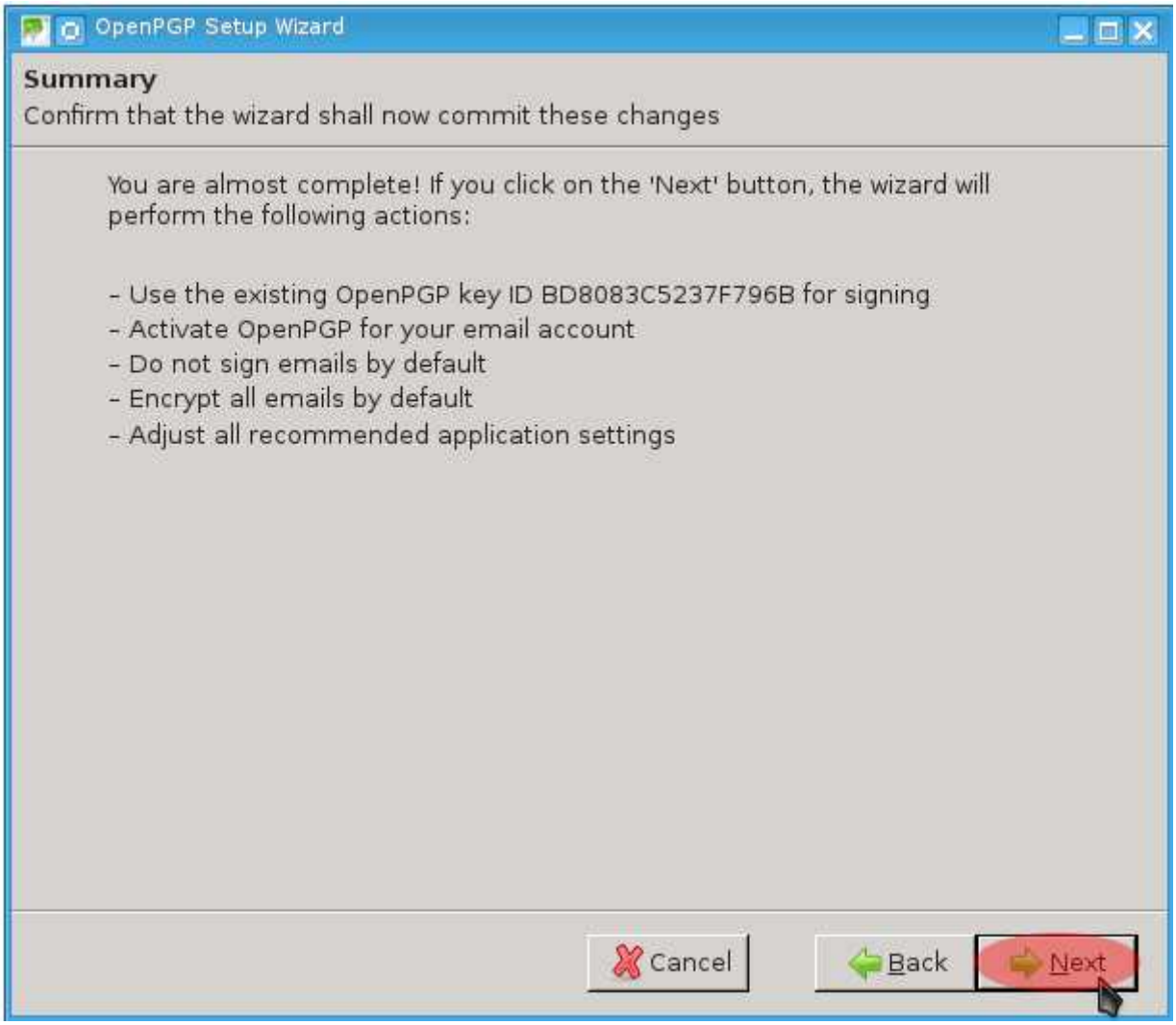


61. Next, you will be asked if you wish to change your email settings to make OpenPGP work more reliably. Choose “yes” and click the “Next” button.

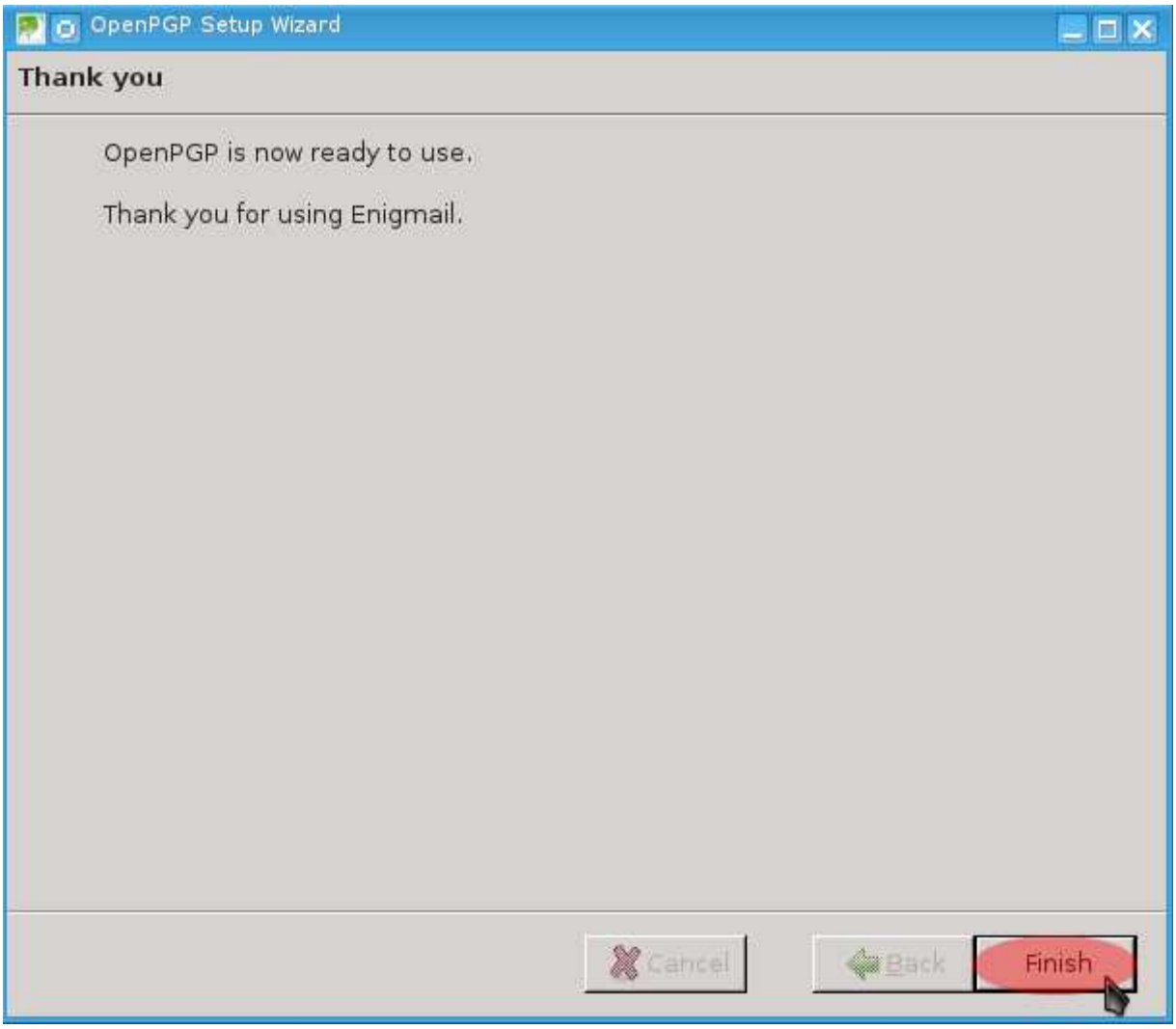


62. Now, chose the key pair that you created earlier for encrypting emails with Thunderbird. Select “I want to select one of the keys below for signing and encrypting my email.” Then, click on the corresponding “Account / User ID” that is shown in the window and click the “Next” button.

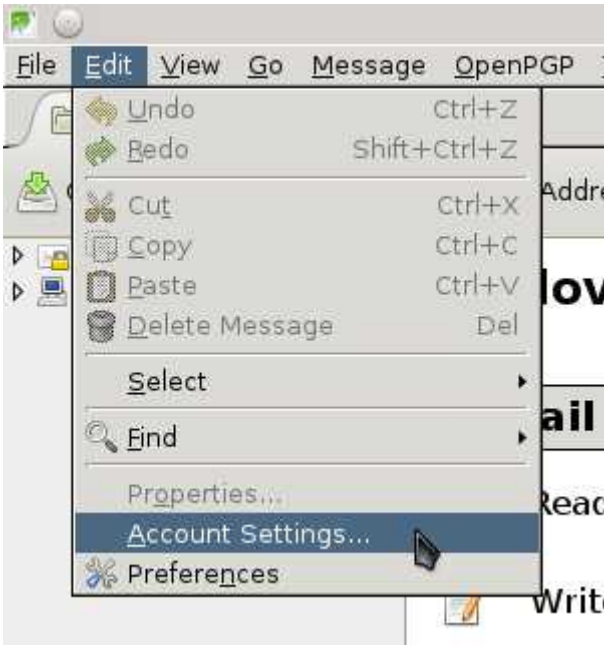
63. On the next screen that appears, click the “Next” button to continue.



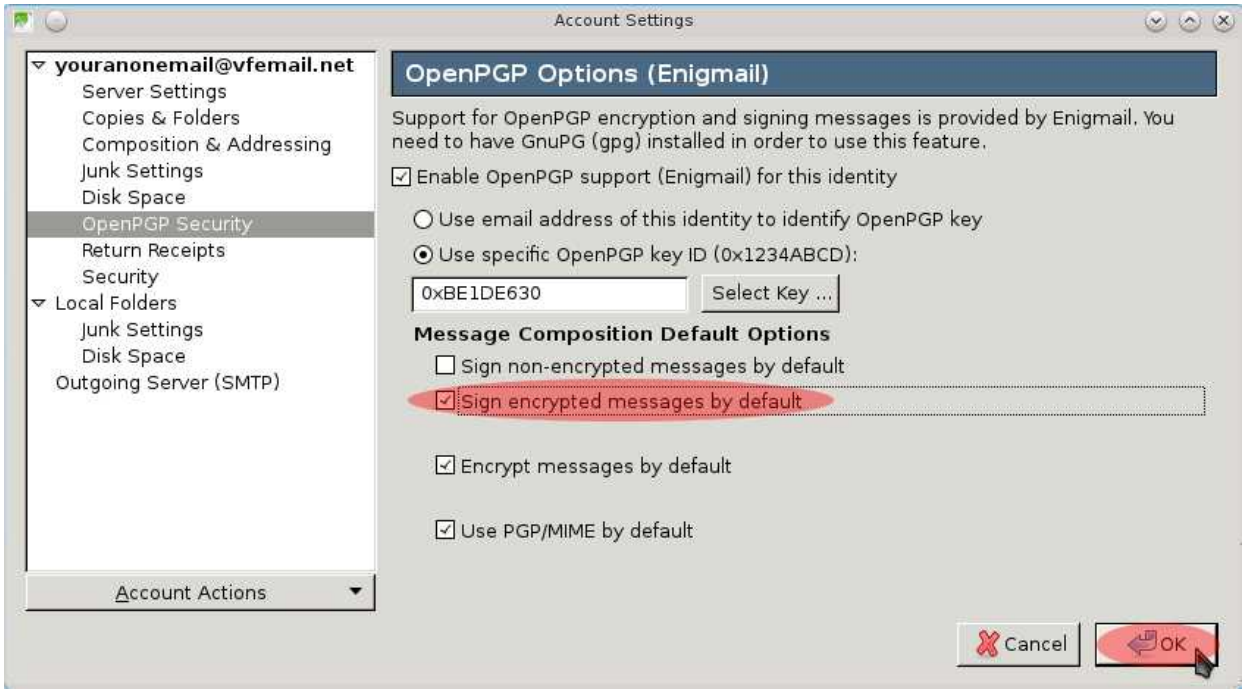
64. On the next screen that appears, click on the “Finish” button.



65. Next, you should change one setting that wasn't addressed by the OpenPGP Setup Wizard. At the main Icedove window, click on “Edit → Account Settings.”

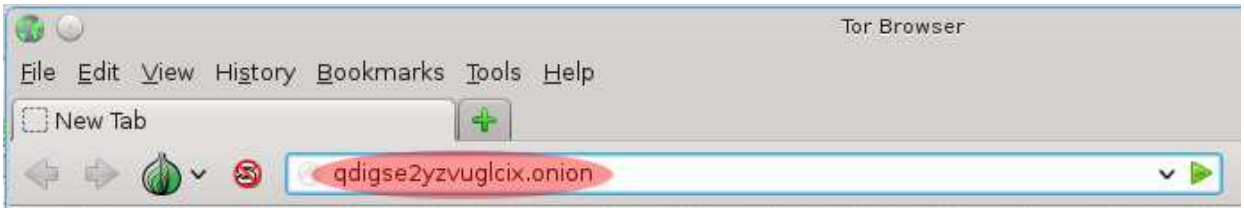


66. In the window that appears, click on “OpenPGP Security” in the left column. Then, mark the box next to “Sign encrypted messages by default” and click the “OK” button.



67. Next, this tutorial will walk you through importing the GPG public key for the email account affiliated with support for this tutorial. There are multiple ways to import keys into your GPG keyring. By far, the most common and easiest method is the use of a key server. Unfortunately, as of the time of this publication, there is an issue with TorBirdy that prevents Enigmail's key manager from importing keys directly from a keyserver. This is not a problem. In this case, you will use Tor Browser.

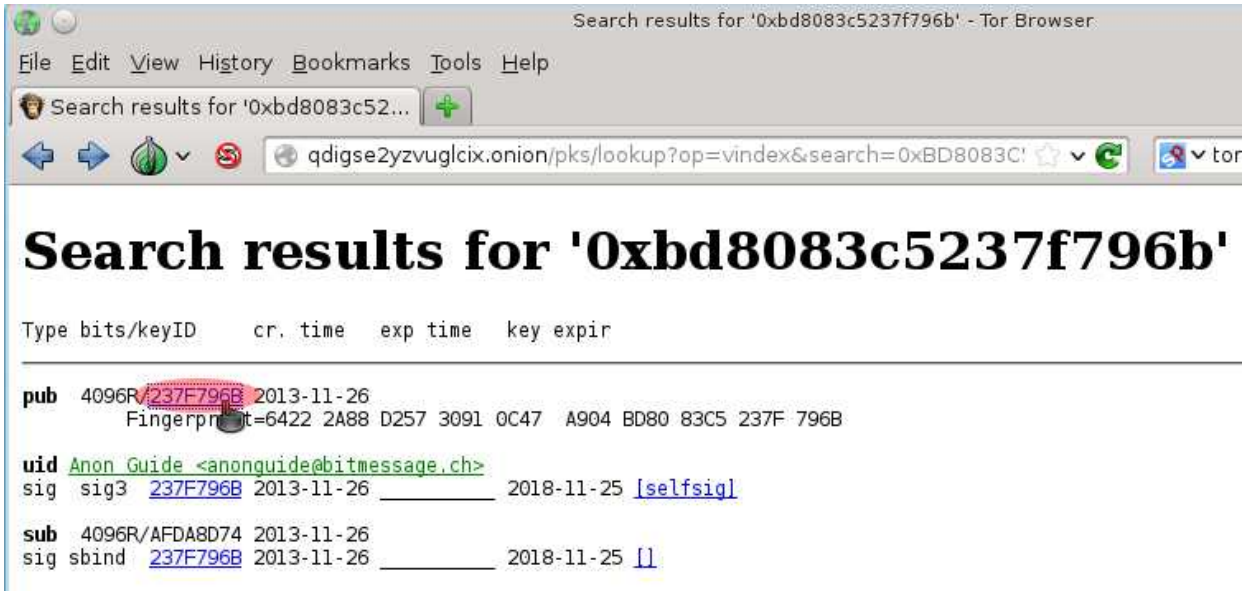
    Open up Tor Browser, type "**http://qdigse2yzvuglcix.onion**" in the location bar and press "enter." This is the Tor hidden service address for "zimmerman.mayfirst.org," a public GPG keys server.



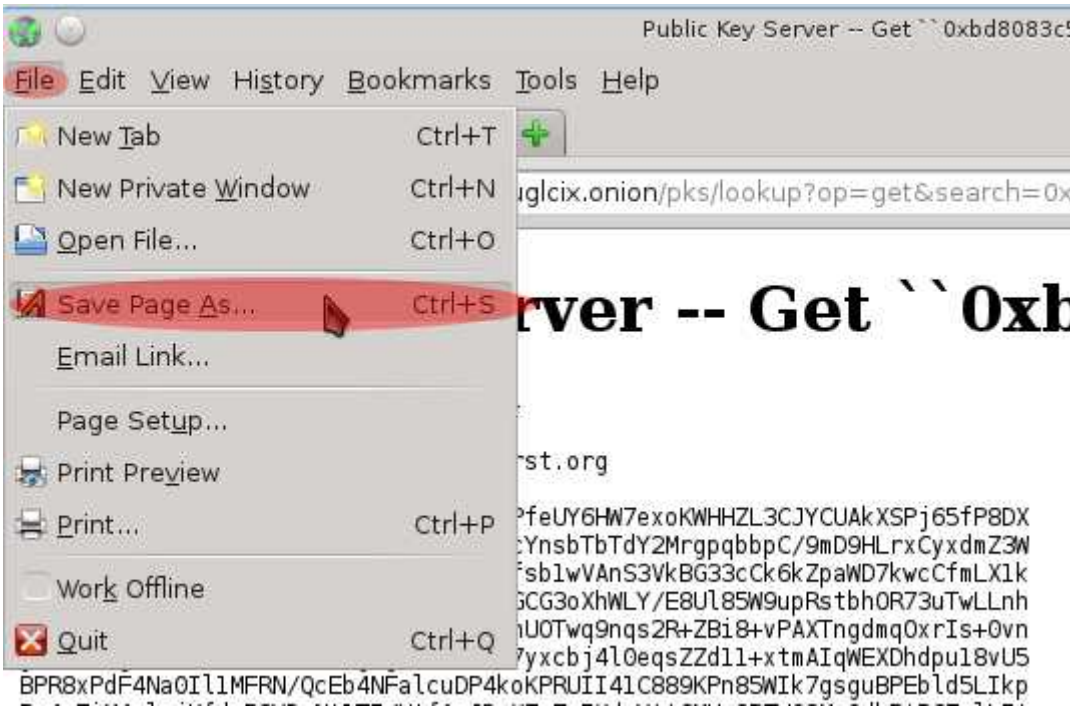
68. Next, in the field next to "Search String," type "**0xBD8083C5237F796B**" and then click on the "Search" button. 0XBD8083C5237F796B is the identification number associated with the public GPG key for anonguide@bitmessage.ch.

    Note: You can search for other peoples' public GPG keys on this server as well by entering their email address in the field next to "Search String" and clicking the "Search" button.

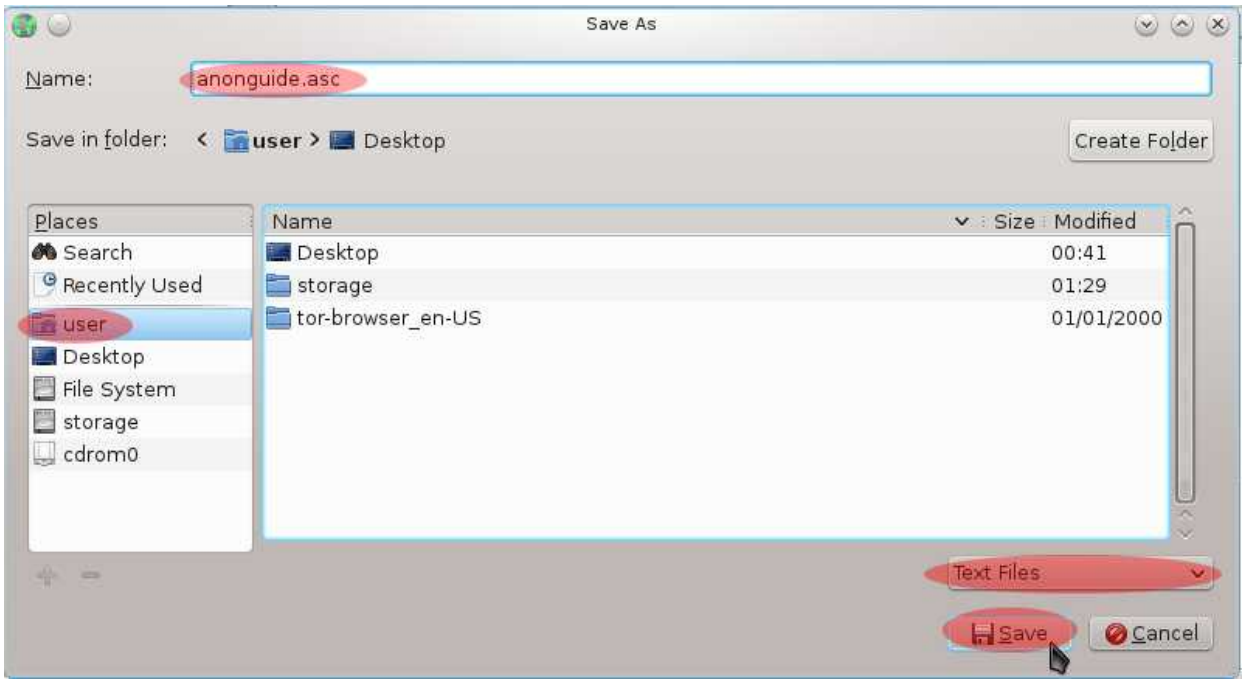
69. In the “search results” that appear, click on the link next to “pub” and above “fingerprint.” This will take you to the public GPG key for anonguide@bitmessage.ch.



70. The next web page you see will show the random text that is the public GPG key for anonguide@bitmessage.ch. Save this as a text file to your hard drive.
Click on “File → Save Page As.”

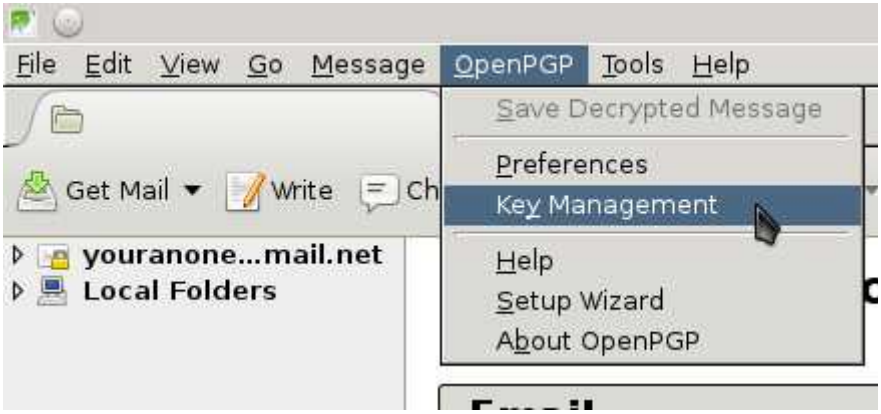


71. In the “Save as” window that appears, click on the “user” folder under “Places” towards the left side of the window. Then, in the field next to “Name,” type “**anonguide.asc**.” Next, click the pull down menu located towards the bottom right corner of the window and select “Text Files.” Finally, click on the “Save” button.

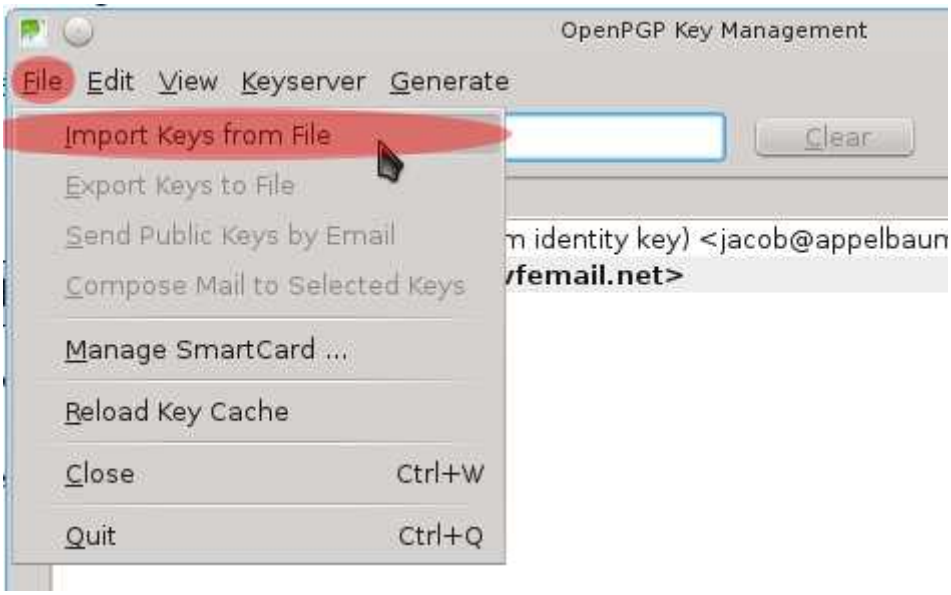


You will be using the same web page again to host your public GPG key. Thus, you may leave the browser open and continue to the next step.

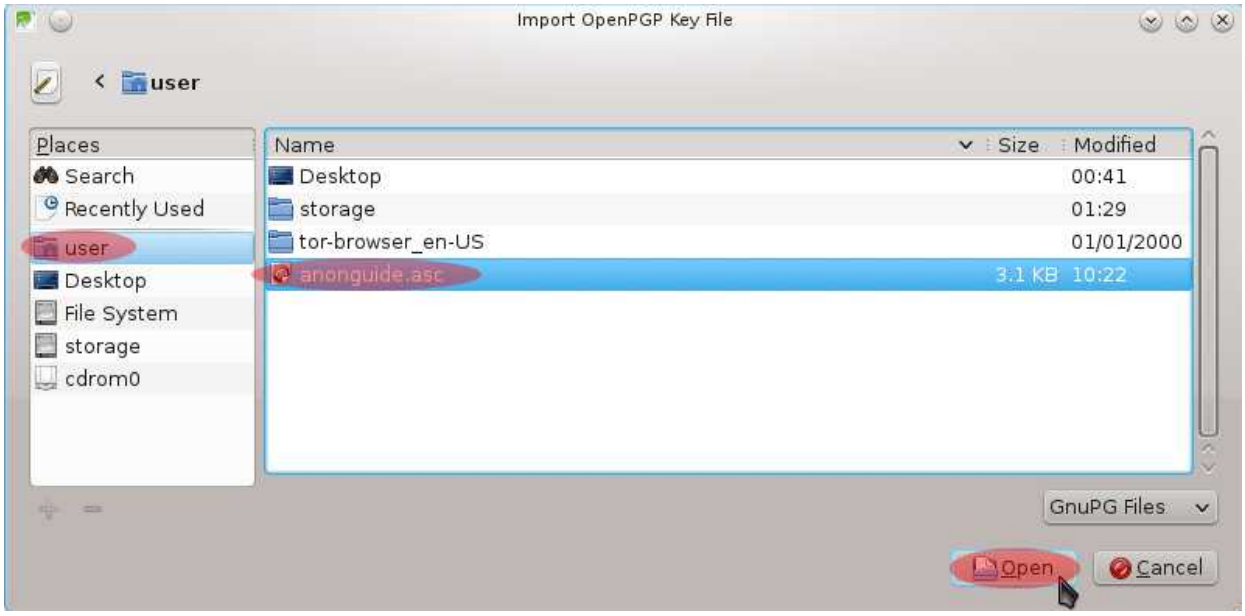
72. Next, return to Icedove and click on “OpenPGP → Key Management.”



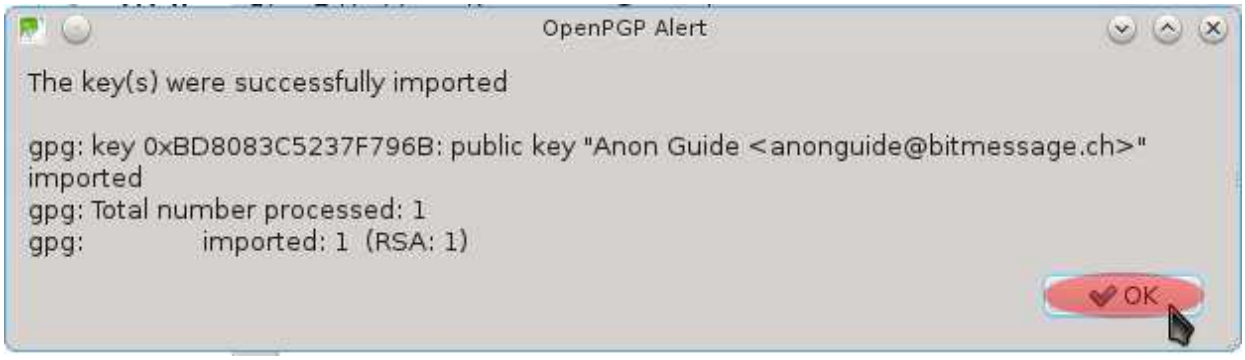
73. In the Key Management window, click on “File → Import Keys from File.”



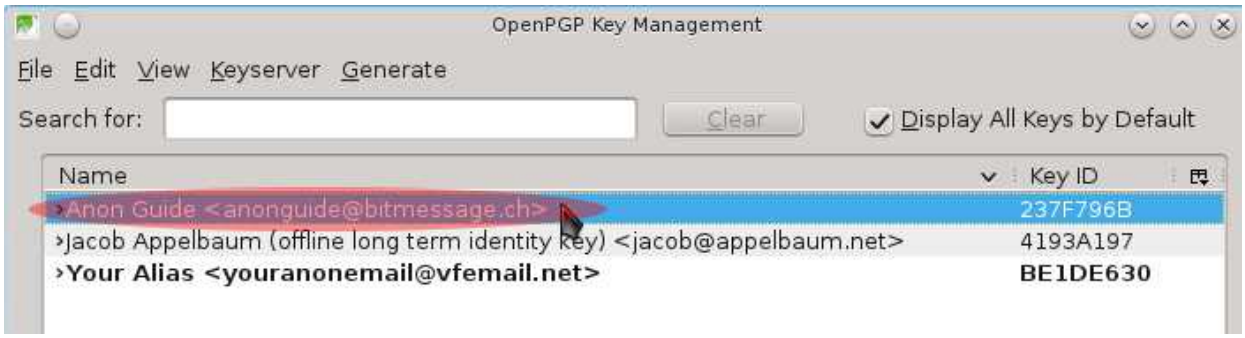
74. In the next window, click on the “user” folder under “Places” towards the left side of the window. Then, click on “anonguide.asc” and click on the “Open” button.



75. The next window that appears should inform you that the key was successfully imported. Click on the “OK” button to continue.



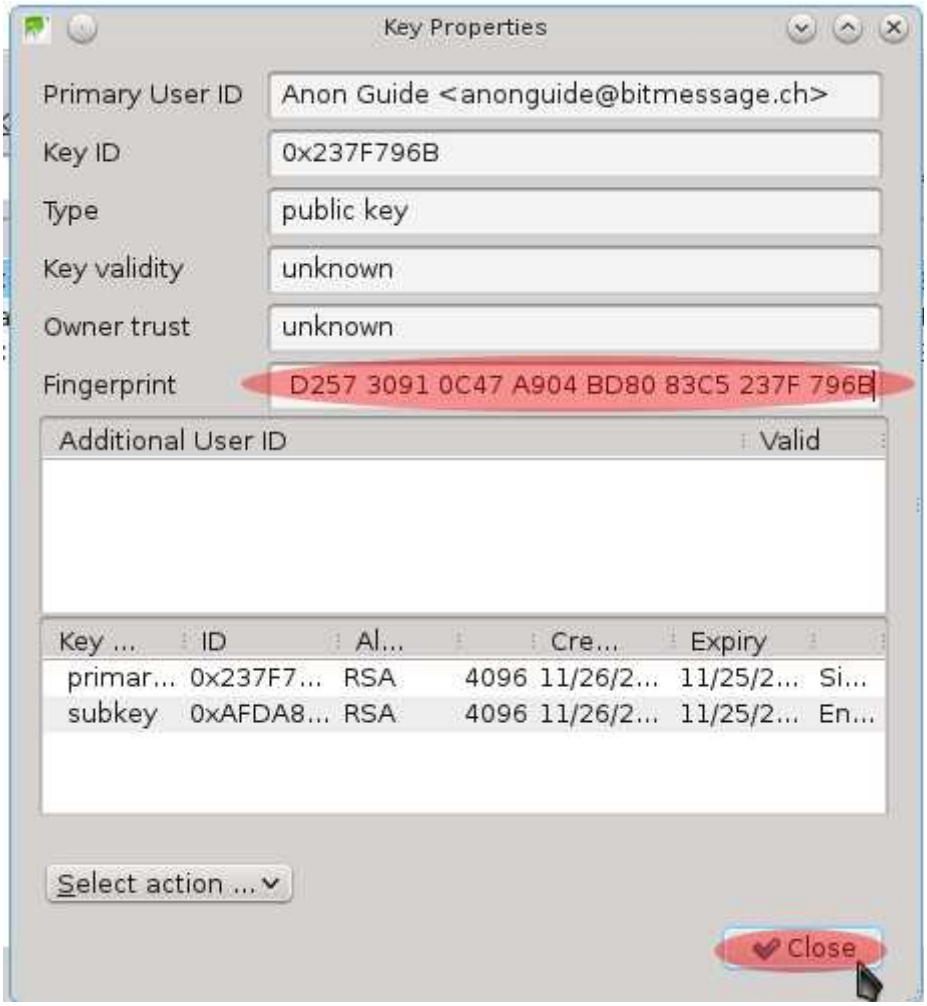
76. Now, verify the integrity of the newly imported key for “anonguide@bitmessage.ch.” Double-click on the key for “Anon Guide <anonguide@bitmessage.ch>” to open the “Key Properties” window.



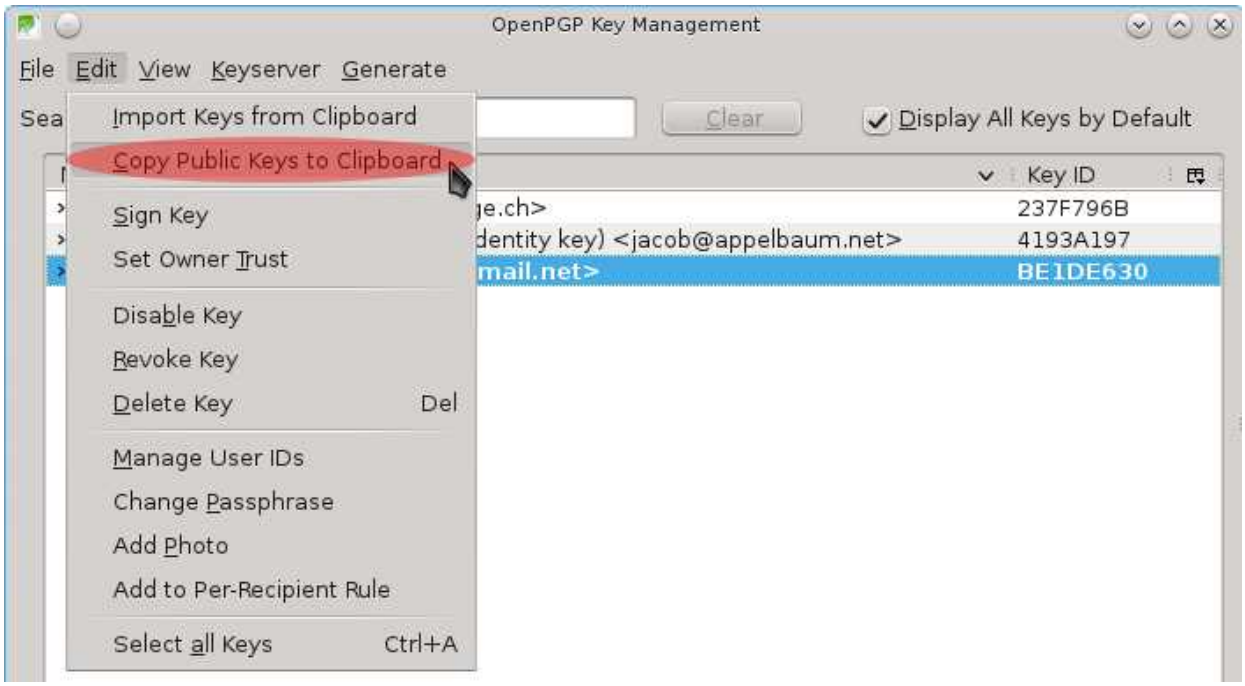
77. In the window that appears, note the fingerprint. It should be "**6422 2A88 D257 3091 0C47 A904 BD80 83C5 237F 796B**". The full fingerprint may not display in the Key Properties window. You can scroll through it by clicking in the field next to "Fingerprint" and using your arrow keys.

    If the fingerprint anything different, **assume the public key for this tutorial that you downloaded has been tampered with and do not use it.** When you have confirmed the fingerprint, click the "OK" button.

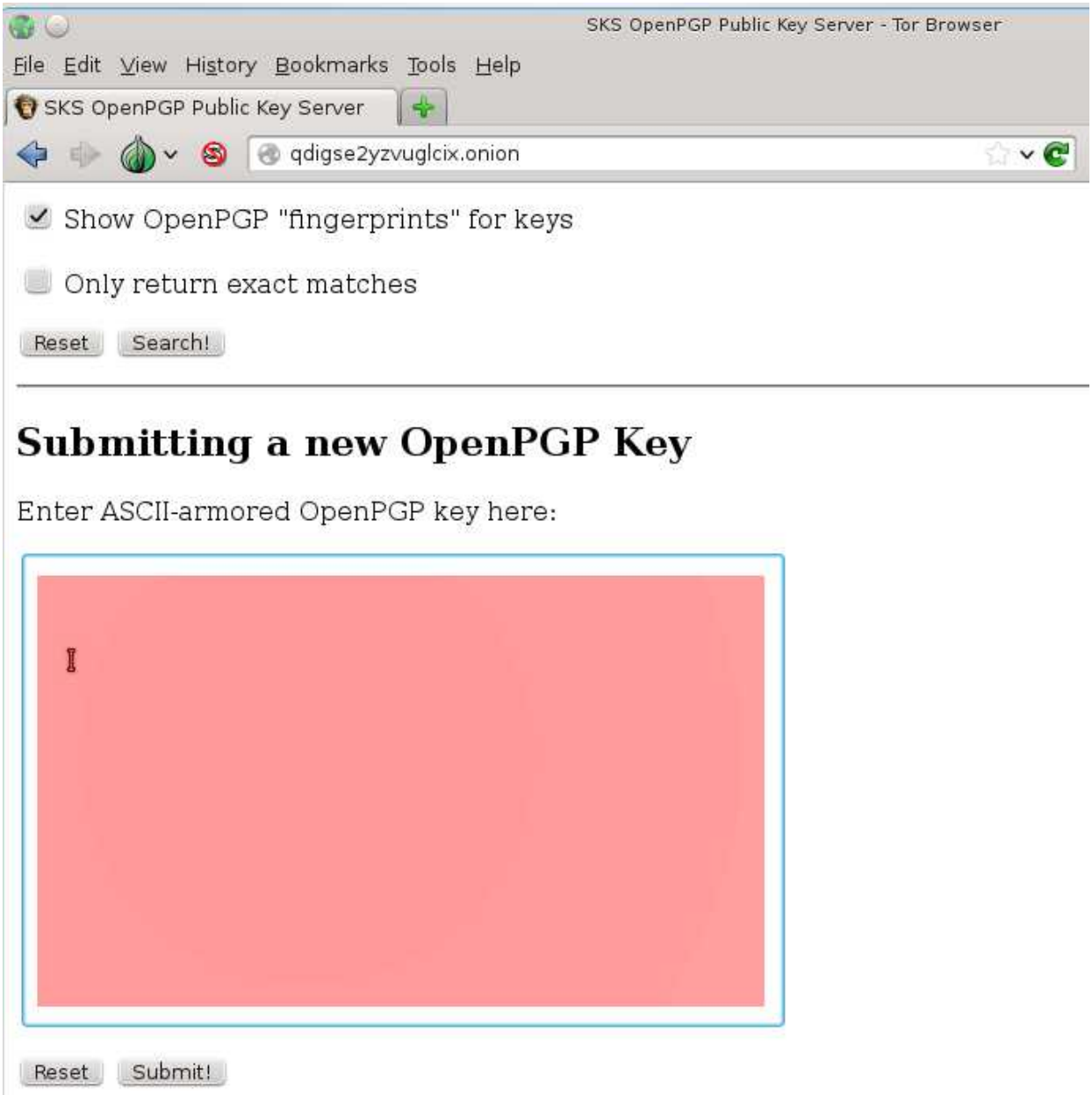
    Note: It is always important to verify any GPG public key you have added to your keyring with a fingerprint provided to you by the person you wish to communicate with. The reason for this is that anyone can add a GPG public to a key server that claims to belong to a certain email account. If an attacker is monitoring an email account through surveillance, and you use an encryption key that they created to falsely correspond to the person you wish to communicate with, the attacker will be able to read your email.



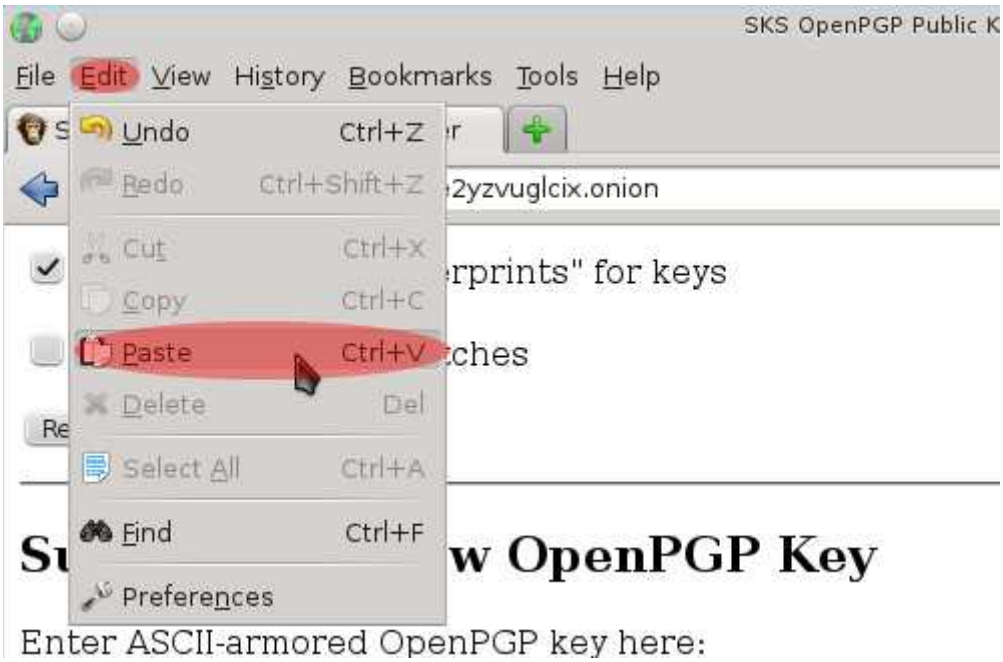
78. Now you should begin the process of exporting your public key to a GPG key server. Click on the entry for your email address in the Key Management window. Then, click on "Edit → Copy Public Keys to Clipboard."



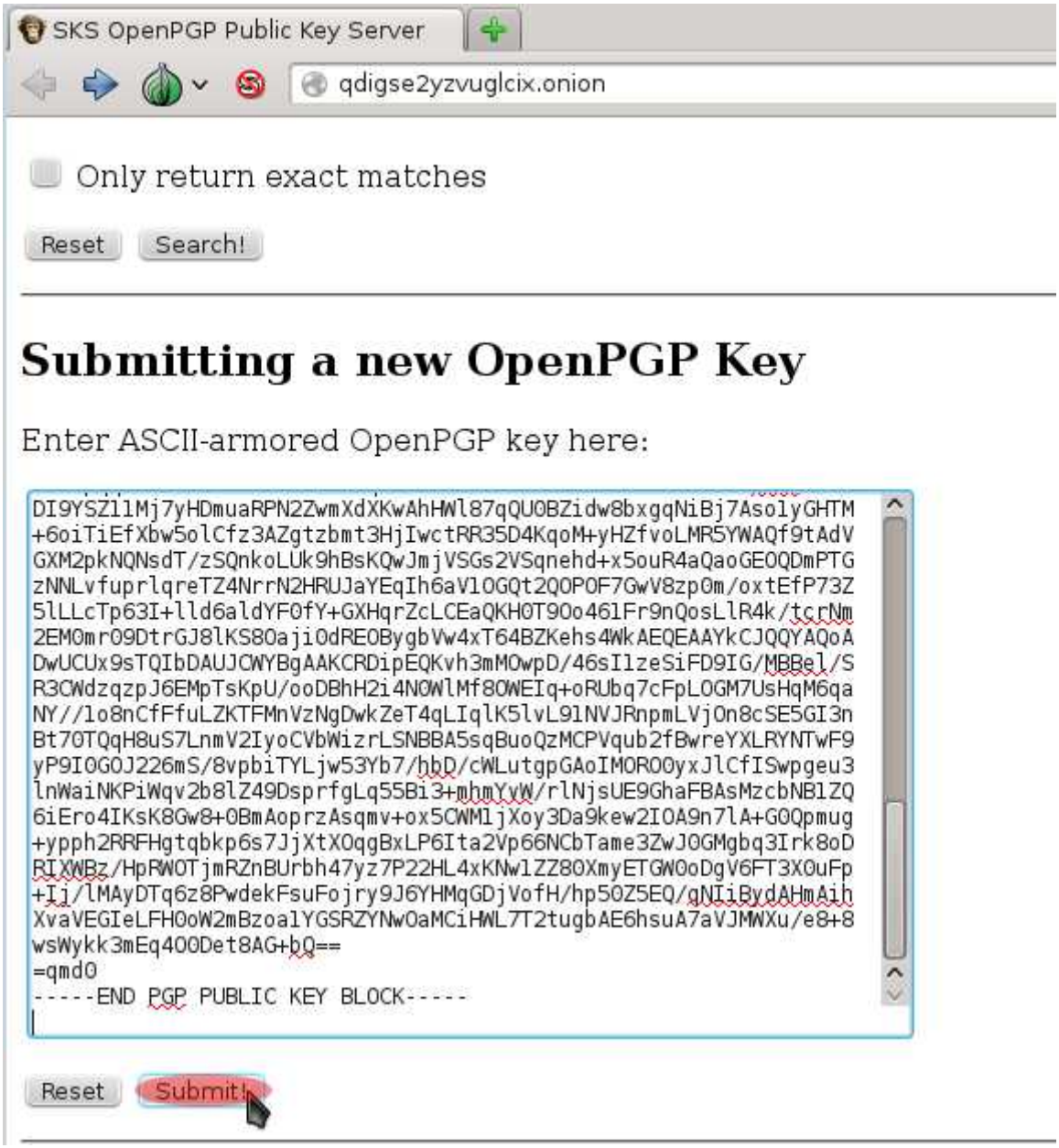
79. Now, go back to the Tor Browser and return to the opening page of **http://qdigse2yzvuglcix.onion** by either using the back buttons or entering it in the location bar and pressing “enter.” When you are back at the opening page, scroll down to the section entitled “Submitting a new OpenPGP Key.” Then, click in the text area directly underneath “Enter ASCII-armored OpenPGP key here.” You should see a cursor blinking in the text field.



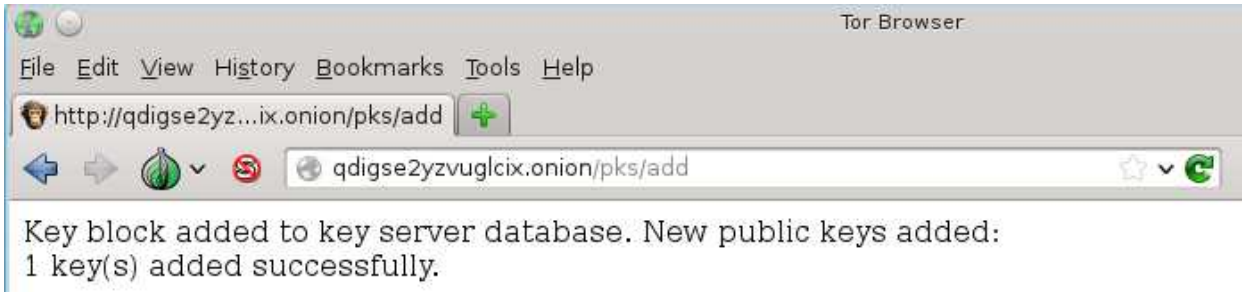
80. Next, click on “Edit → Paste” to paste the contents of your clipboard into the text field. The text you paste into the field will be random characters. If it is something else, go back to step 78 and copy your public key again.



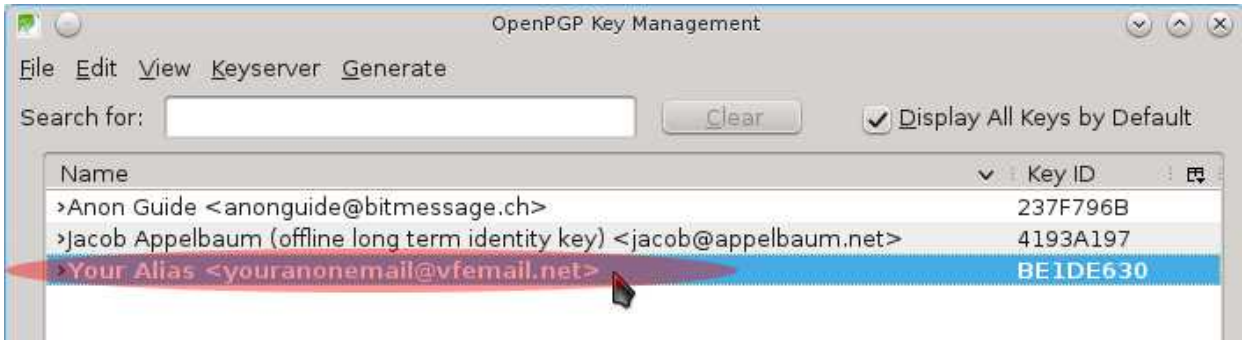
81. Now, click on the “Submit” button under the text field where you pasted your public GPG key.



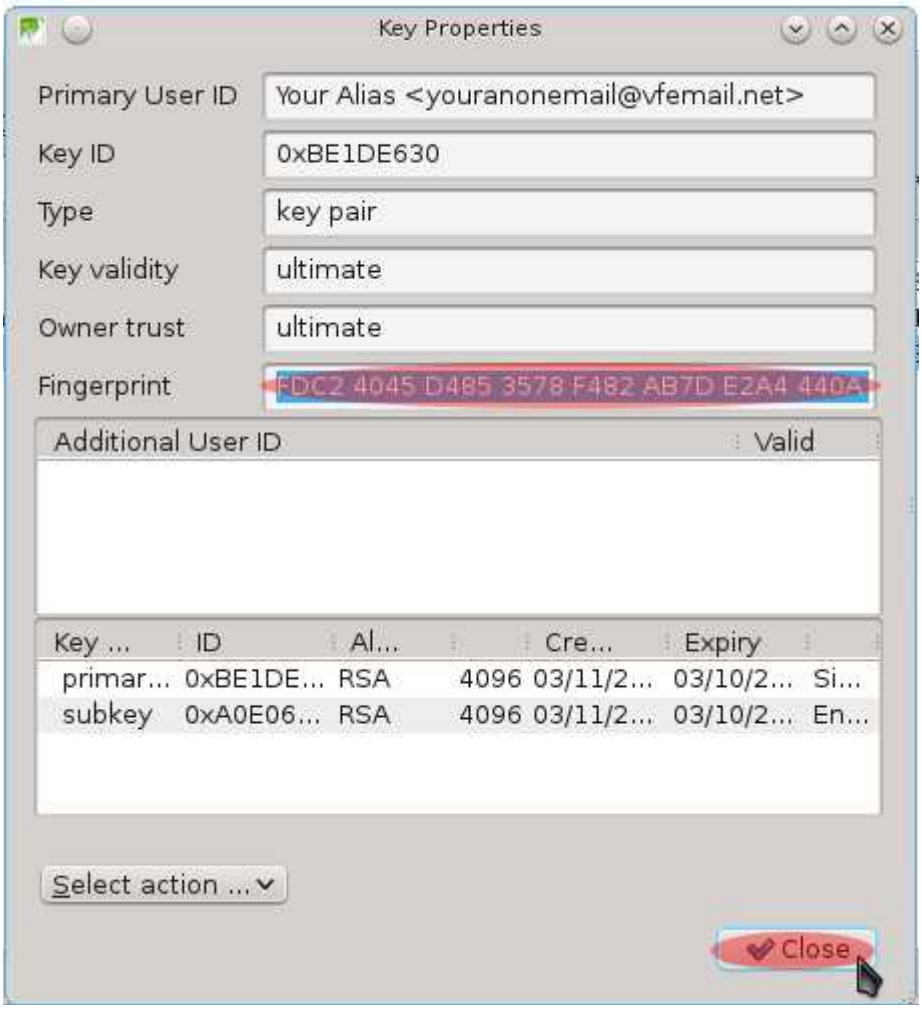
82. You should next see a screen confirming that your public GPG key has been “added successfully.” You may close the Tor Browser now if you wish.



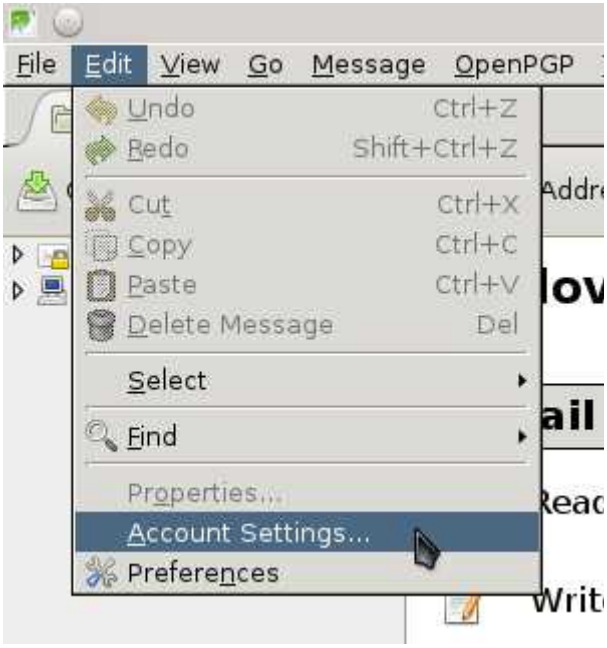
83. Now, let's prepare Icedove to inform people about your public GPG key through listing it in your email signature. Return the the “Key Management” window in Icedove and double-click on the key entry for your vfemail.net email address to open the “Key Properties” window.



84. In the window that appears, click in the field next to “Fingerprint.” Then, “select all” of the text in the field by typing either “**LEFT-CTRL A**” or doing a right-click and choosing “select all.” Next, copy the text to your clipboard by typing “**LEFT-CTRL C**” or doing a right-click and choosing “copy.” When you have copied the text to your clipboard, click the “Close” button.



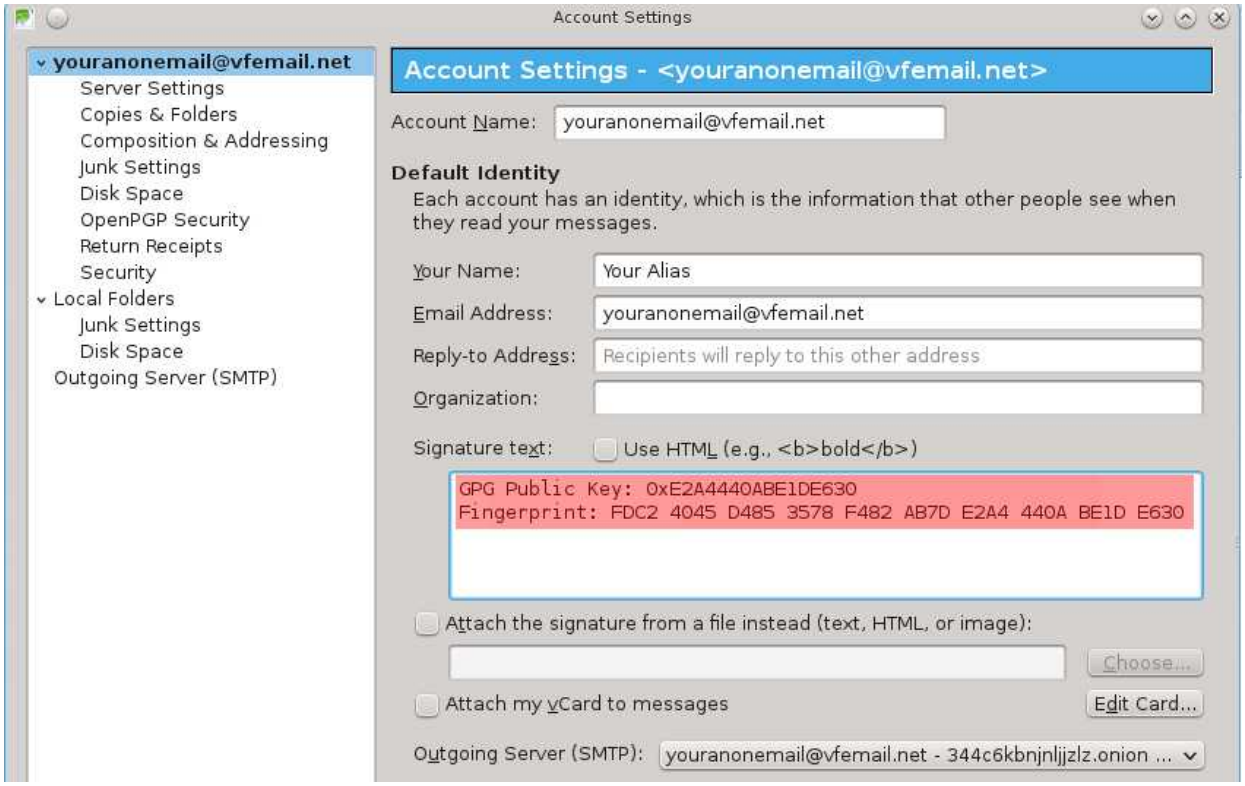
85. From the main Icedove window, click on “Edit → Account Settings.”



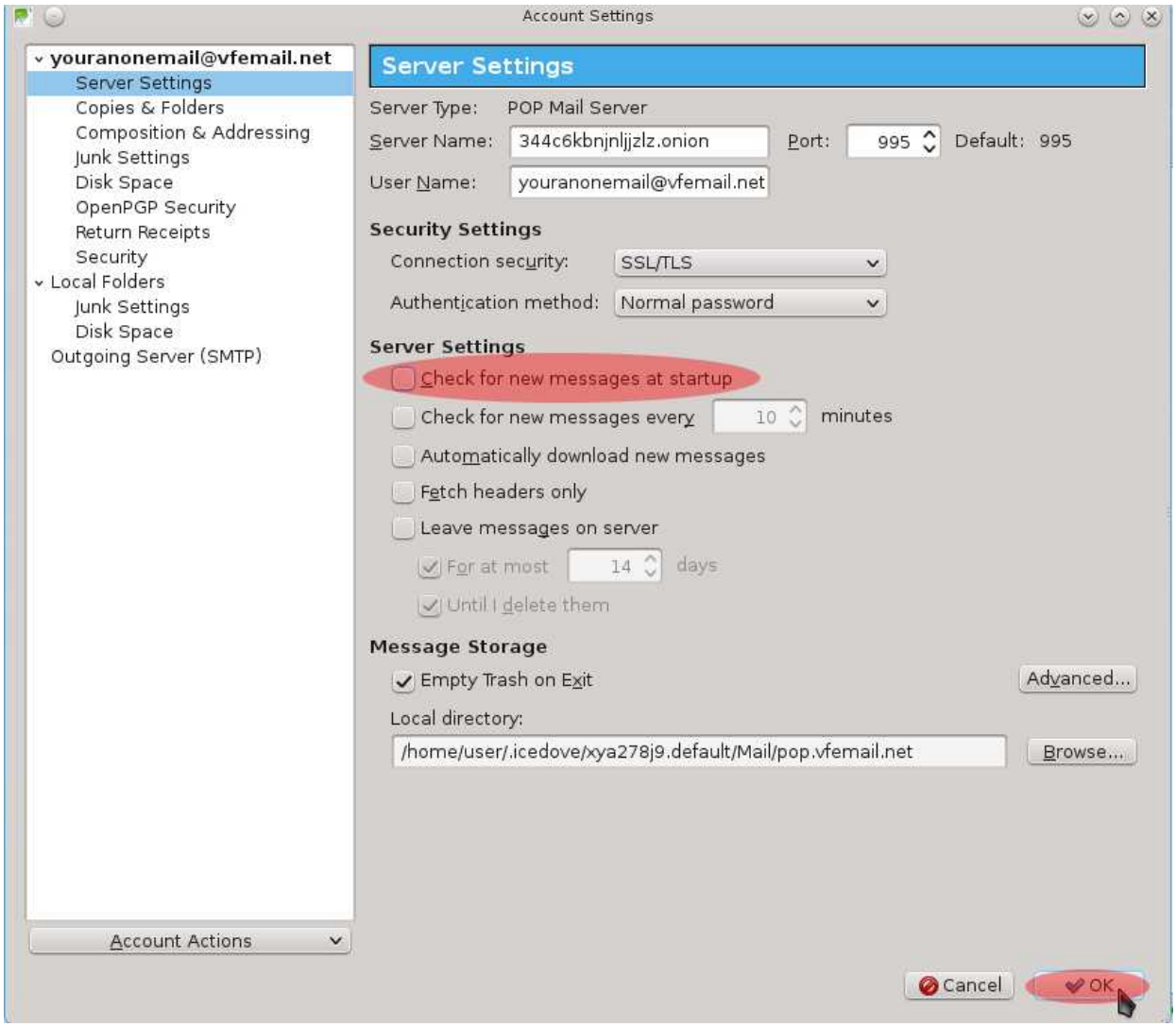
86. Now you are going to create a signature that will be included in all of your outgoing mail that will contain both your GPG public key ID and your GPG public key fingerprint. In the next window that appears, click in the text field located underneath “Signature text.” Then paste the contents of your clipboard on to two separate lines in the text field.

    On the first line, type “**GPG Public Key:**” before the fingerprint you just pasted. Then, delete all but the last 16 characters of the fingerprint from this line. If you look at the example below, you'll notice that your fingerprint consists of 10 groups of 4 characters. Delete the first six groups. Then, delete the spaces in between the remaining groups of characters. Finally, type “**0x**” (that is the numeral zero) directly in front of the remaining characters. In the example below, that results in “0xE2A4440ABE1DE630.” The end result of what you create here is your GPG public key ID number. People can enter that into various GPG key servers to find your public key and send you encrypted messages.

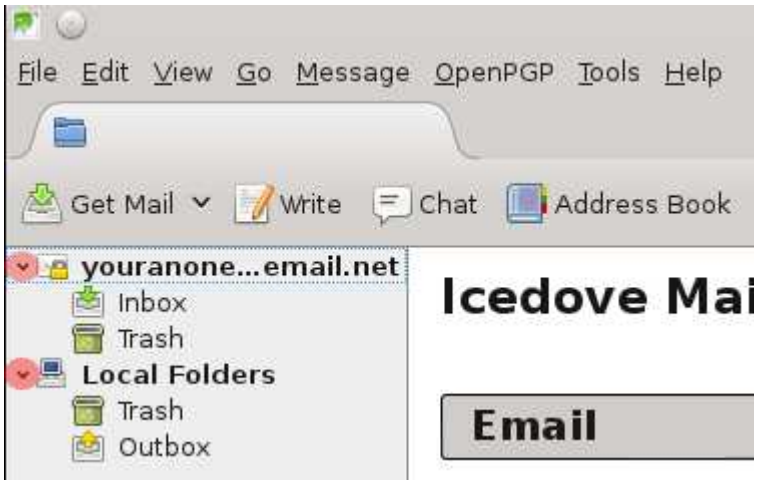
    On the second line, type “**Fingerprint:**” in front of the characters you pasted there. This will help enable people who download your GPG public key to verify that it is they key you wish them to use.



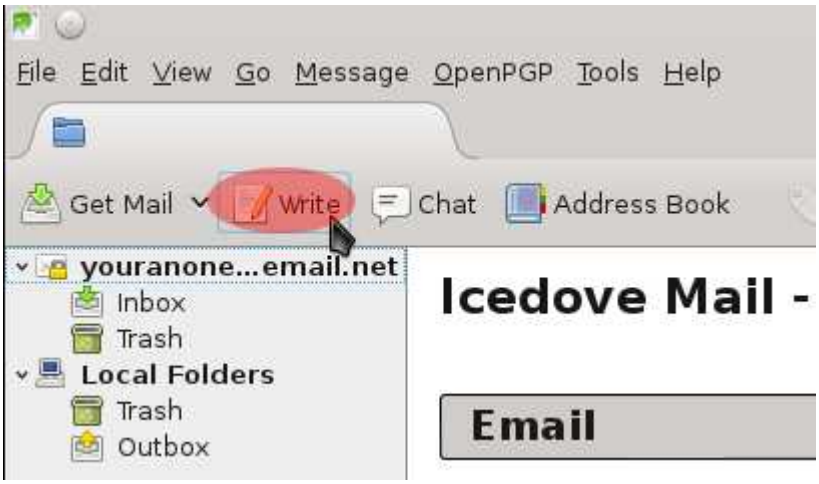
87. Next, click on “Server Settings” in the field to the left side of the “Account Settings” window. Due to a bug in either Icedove or Torbirdy, you may notice that “Check for new messages at startup” has been enabled. Uncheck the box next to “Check for new messages at startup” to disable the feature. Then, click on the “Close” button.



88. When you are returned to the main Icedove window, expand the folders for your newly created account. They will be located under the “Get Mail” button. Click on the “>” arrow signs to have them point downward and expand your folders.



89. Now you will be instructed on sending out your first test email to anonguide@bitmessage.ch. Click on the “Write” button located in the upper left region of the window.

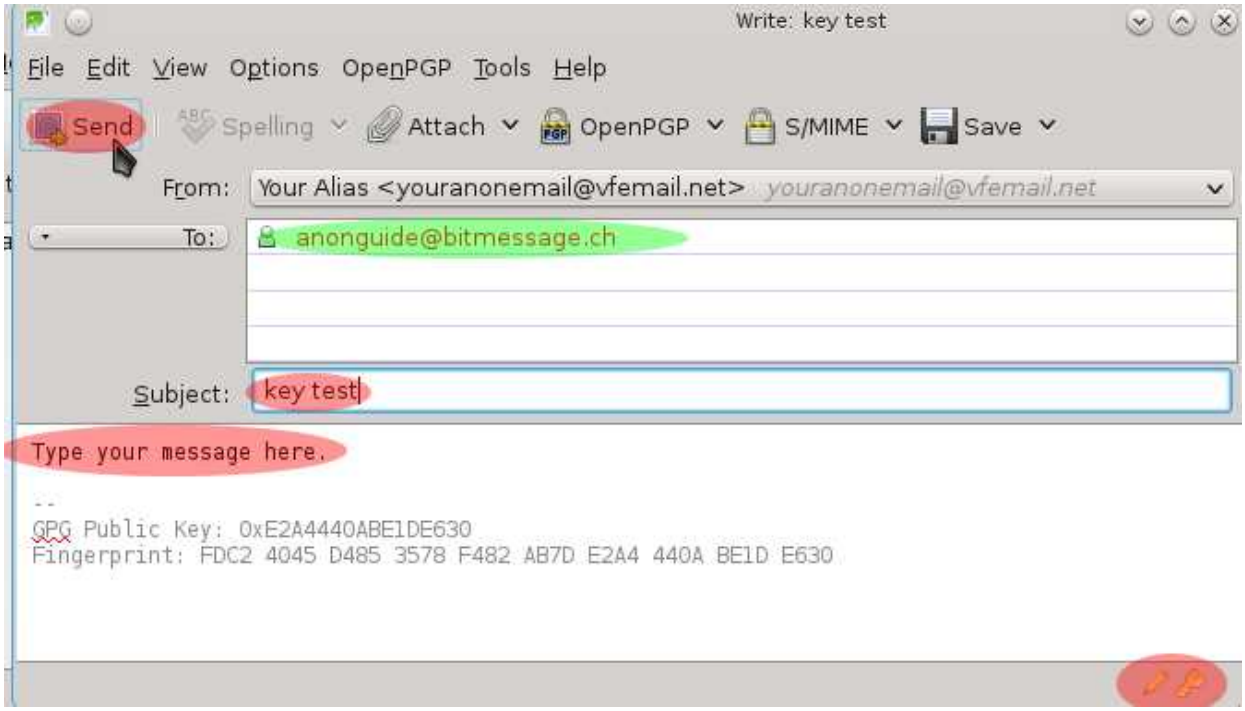


90. A new window will open for you to compose an email message. In the “To” field, type “**anonguide@bitmessage.ch**”. Then, type “key test” in the “Subject” field. Then, type whatever you wish into the message body. You do not need to go into great detail. The point of this email is to test your encryption key and get you familiar with a common encrypted email exchange.

    Notice the pencil and key icons in the lower right corner. These icons should be in a yellow color, which means your message will be signed and encrypted (if you have a corresponding public key). If they are grey, that means encryption and/or signing is disabled.

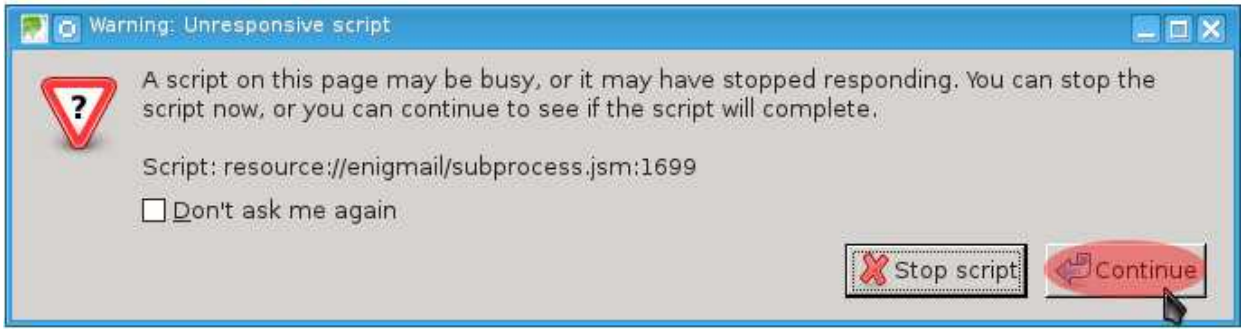
    Note: The Subject field is **NEVER ENCRYPTED**, even when you encrypt your message and attachments. Thus, **be wary of any information you put in a subject field.**

    When you are ready to send the message, click the “Send” button.



91. You will next be prompted to enter your GPG passphrase. This will enable you to sign the message you are sending to us. When you sign a message, this provides a mechanism which allows the recipient of an email to be confident that you actually wrote the email and not an impostor. Type your passphrase and click the “OK” button.

92. If you take too long to enter your GPG passphrase, the window imaged below may appear. Don't worry about that. Finish typing your GPG passphrase and, when you get to the “Warning: Unresponsive Script” window, click the “Continue” button. Your email will now be encrypted.

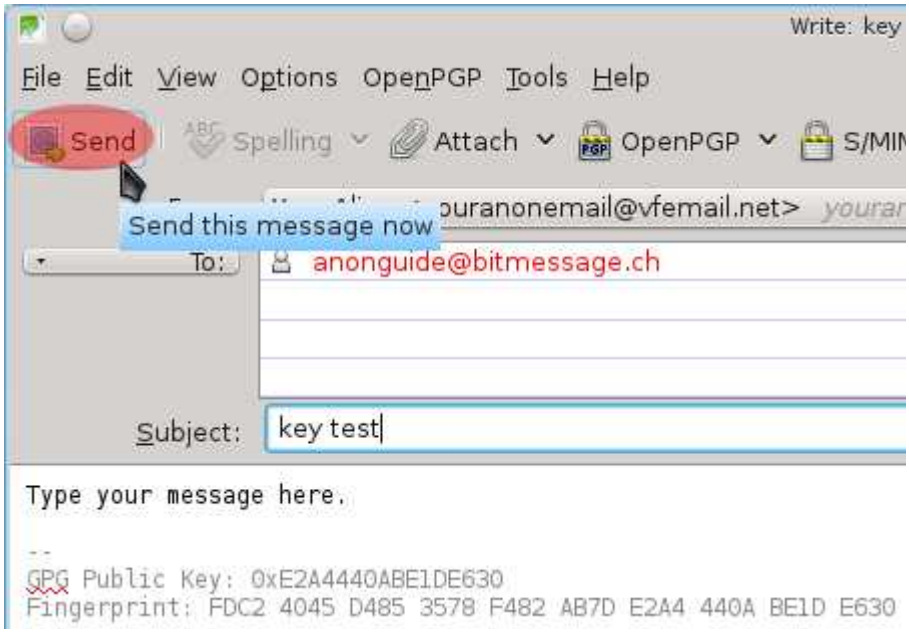


93. Since this is your first time sending an email, another “Add Security Exception” window will appear. This is expected. The warning is due to the fact that the SSL certificate you received is from vfemail.net, but the domain you are connecting to is 344c6kbnjnljjzlz.onion. Click on the “Confirm Security Exception” button. You won't have to do this again in the future.

94. As a result of the issue with the SSL certificate in the last step, the sending of your message will fail. Select the Icedove “Write: key test” window from your task bar.

Then, click the “OK” button in “Send Message Error” window that appears.

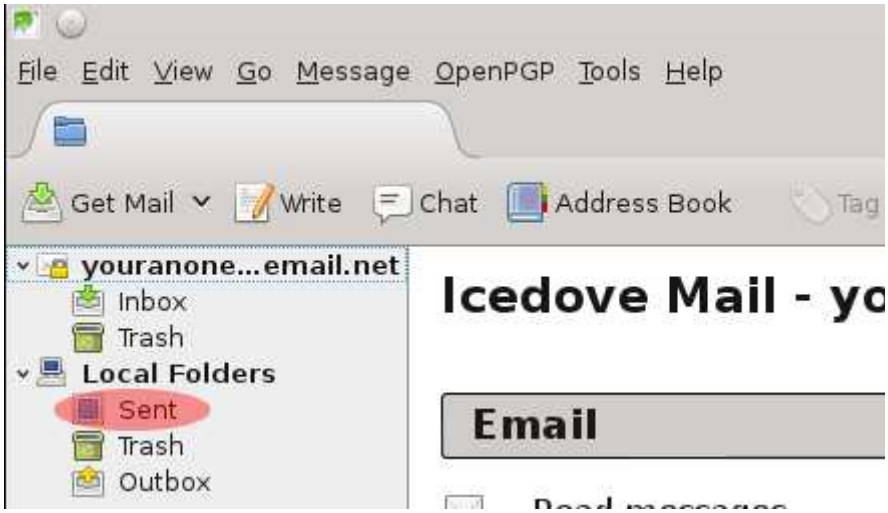
Finally, when you are returned to your email composition window, click on the “Send” button again.



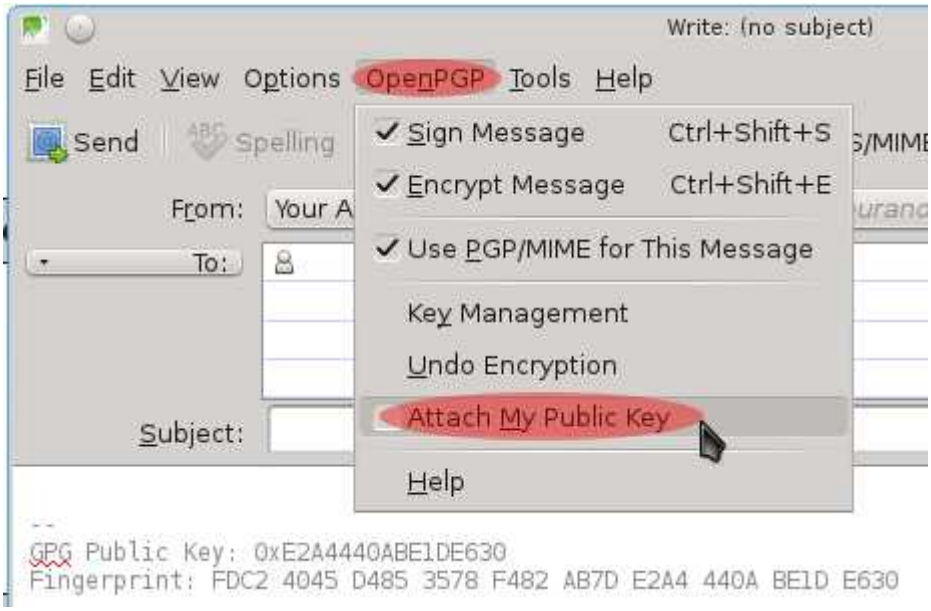
95. Next, you will be prompted to enter the password for your vfemail.net account. This will happen each time you start Icedove and send an email for the first time since your password is not stored by the program. However, once you have entered the password, Icedove will remember it for the session. The same process applies to receiving email. When asked to enter your password, copy it from KeePassX, paste it into the password field and click the "OK" button.

Note: Do not use Icedove's Password Manager to store your password. Icedove does not encrypt stored passwords by default. Thus, if an attacker compromises your machine and manages to access your Icedove folder, they will gain the password to your email account if you have stored it in Icedove.

96. You will now be returned to the main Icedove window. If you notice a new "Sent" folder in your Local Folders on the left side of the window, your email to anonguide@bitmessage.ch was sent.



97. In some instances, you may wish to send an email to an address for which you have no GPG public key in your keyring. When you reach a new mail composition window like you did in step 90, you have the option of sending your GPG public key to the recipient as an attachment. If you wish to do that, click on "OpenPGP → Attach My Public Key."



Once you have composed the message and click the "Send" button, you will see the window imaged below. Mark the box next to "Send mail unencrypted and unsigned." Then, click the "OK" button.

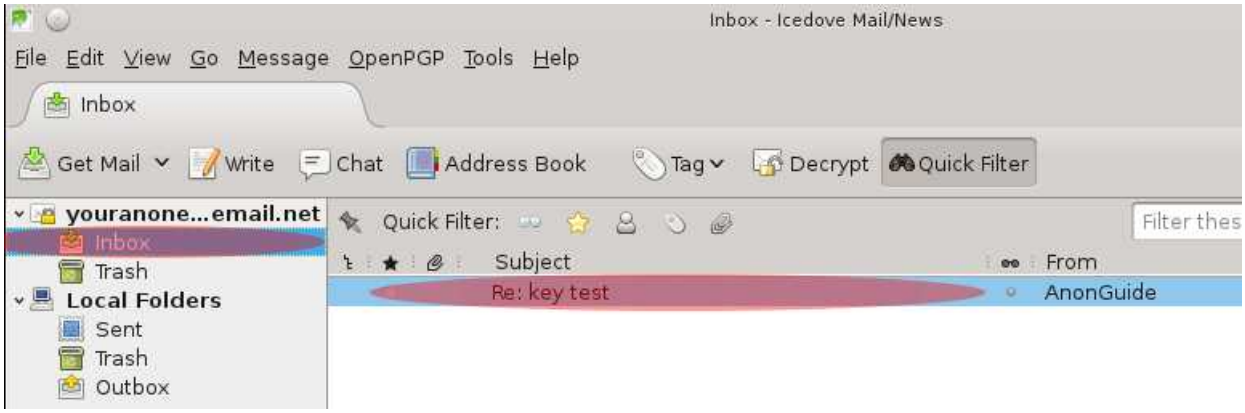
Note: Remember that this email is unencrypted. Thus, it is possible that, if someone intercepts your email at some point, it could be read. Be wary of what information you share in an unencrypted email.

The remainder of this chapter will discuss downloading and reading email.

98. In the near future, you will want to check your mail to see if you got a response from us or if anyone has sent you email messages. From the main Icedove, click on the “Get Mail” icon to check for any new email messages on the server and download them.

99. Next, you will be prompted to enter your password for your email account. Once you have entered the password, Icedove will remember it for the session. When asked to enter your password, copy it from KeePassX, paste it into the password field and click the “OK” button.

100. When you receive new emails, a counter will appear next to “Inbox” in the left column. Click on “Inbox” to go to the list of new emails. Then, click on the email that you wish to read.



101. If the message you received was encrypted with your public key, you will need to type your GPG passphrase to decrypt it. If a window like the one in the image below appears, type your GPG passphrase and click the “OK” button.

102. The email will next display in the lower portion of your Icedove window. From here, you have the option of replying, forwarding, deleting, etc. If you're reading the message sent to you by anonguide@bitmessage.ch, your encryption configuration is working.

Congratulations. You have reached the end of the Icedove and Enigmail email tutorial. It should be emphasized that **this is not meant to be an all inclusive tutorial on the safest way to use GPG/PGP encryption.** There are a number of other resources on the Internet, or people you can talk to, that can provide more tips that may be better for the perceived threat model you want to address. However, you now have a strong starting point that has laid down the basic fundamentals of using encryption over email. Remember the following tips regarding email:

- **Do not contact people you know in real life at non-anonymous email addresses with the email account you created here.** Do your best to keep your real world identity separate from your online identity in Whonix.

- **Be wary of what you share about yourself in email!** Just because your email is encrypted doesn't protect you if the person you are communicating with stores your emails in an unencrypted format. Nor does it protect you from someone receiving messages from you who desires to use the information you provide to exploit you.

- **Never include sensitive information in an email subject, EVEN IF THE EMAIL IS ENCRYPTED!** Subject headers in email are never encrypted, despite the fact that the rest of the message is.

- If you send email to a recipient without encryption, **assume it can be read by anyone!**

- Whenever you have the option to use a Tor hidden service, a domain name with a .onion extension, **use it!** If you can confirm it is controlled by the service you wish to use, it will give you greater protections.

Chapter 4g. Malware Mitigation.

One of the most common risks to a secure system that you will encounter is malware. Despite what some may say about Linux, it is not immune to the threat of malware. The standard approach for most users to prevent malware is a virus scanner. However, such a method is flawed since, once malware has found its way on to your computer, it's already been compromised. All a virus scanner can do is attempt to clean up the mess. Additionally, using a virus scanner only detects known malware. Any unknown malware will get past it and compromise your system undetected.

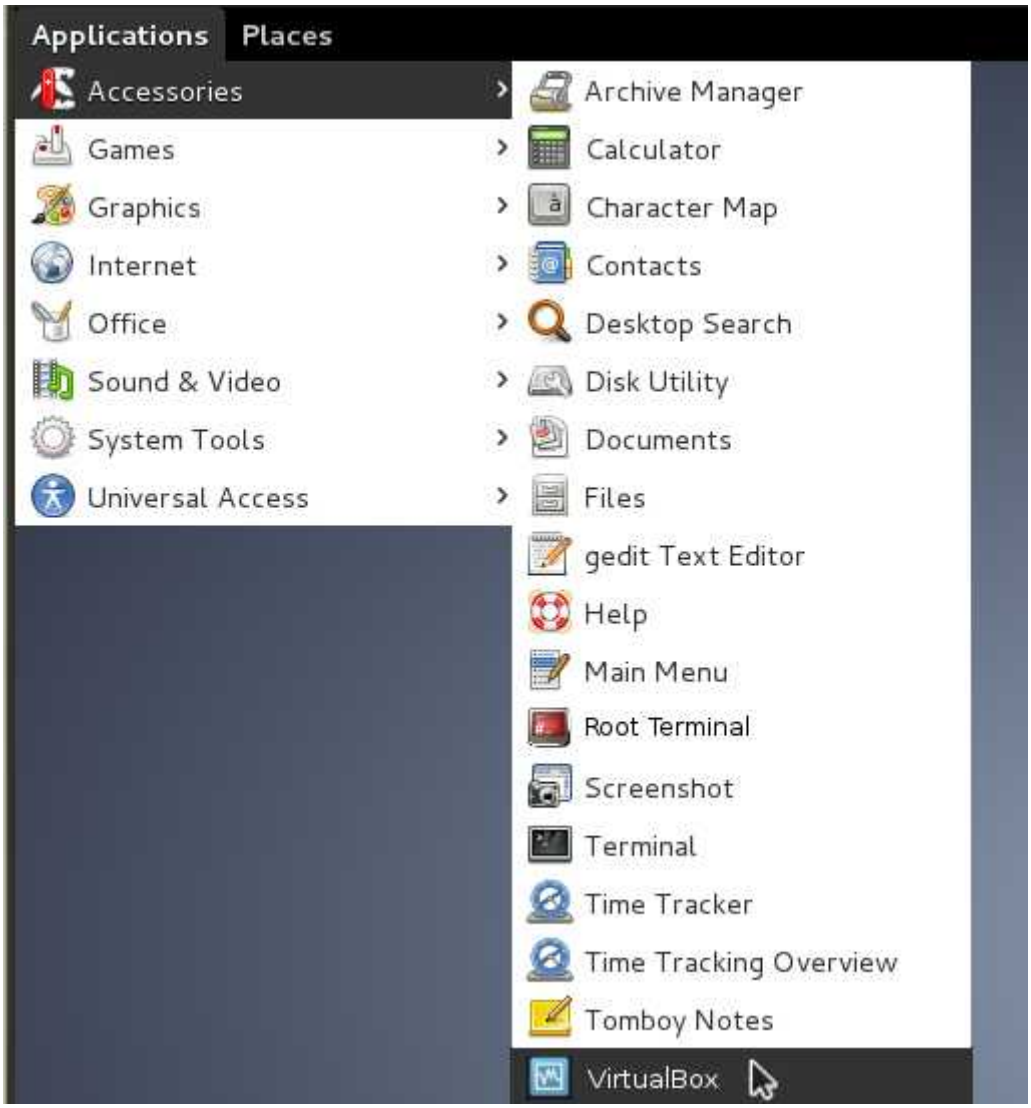
The method described in this chapter provides a means of limiting the risk of a lasting compromise of your Whonix Gateway and Whonix Workstation by malware. Rather than relying on a virus scanner, this method involves creating an additional virtual hard drive for persistant storage of various files and then restoring the Whonix Gateway and the Whonix Workstation from a snapshot after each use. The benefit of this method is that, if either the Whonix Gateway or the Whonix Workstation are compromised by malware during your session, it will simply be erased and gone the next time you use the Whonix Gateway or Whonix Workstation.

While this method provides a fairly good way to mitigate the risks associated with malware, do not become overconfident in it and get reckless with your networking habits. This method will only work against malware that is confined to the Whonix virtual machines. If the malware is advanced enough to break out of the restrictions of a virtual machine and compromises your host, then this method will no longer do you any good and your entire system will no longer be secure. Additionally, standard malware that infects your vm can still compromise communications that you believed to be encrypted, thus weakening a significant aspect of the security methods discussed earlier in this guide. Therefore, while this method will mitigate against a persistent install of malware in your Whonix Gateway or Whonix Workstation, remember that it is still best to avoid malware compromise entirely.

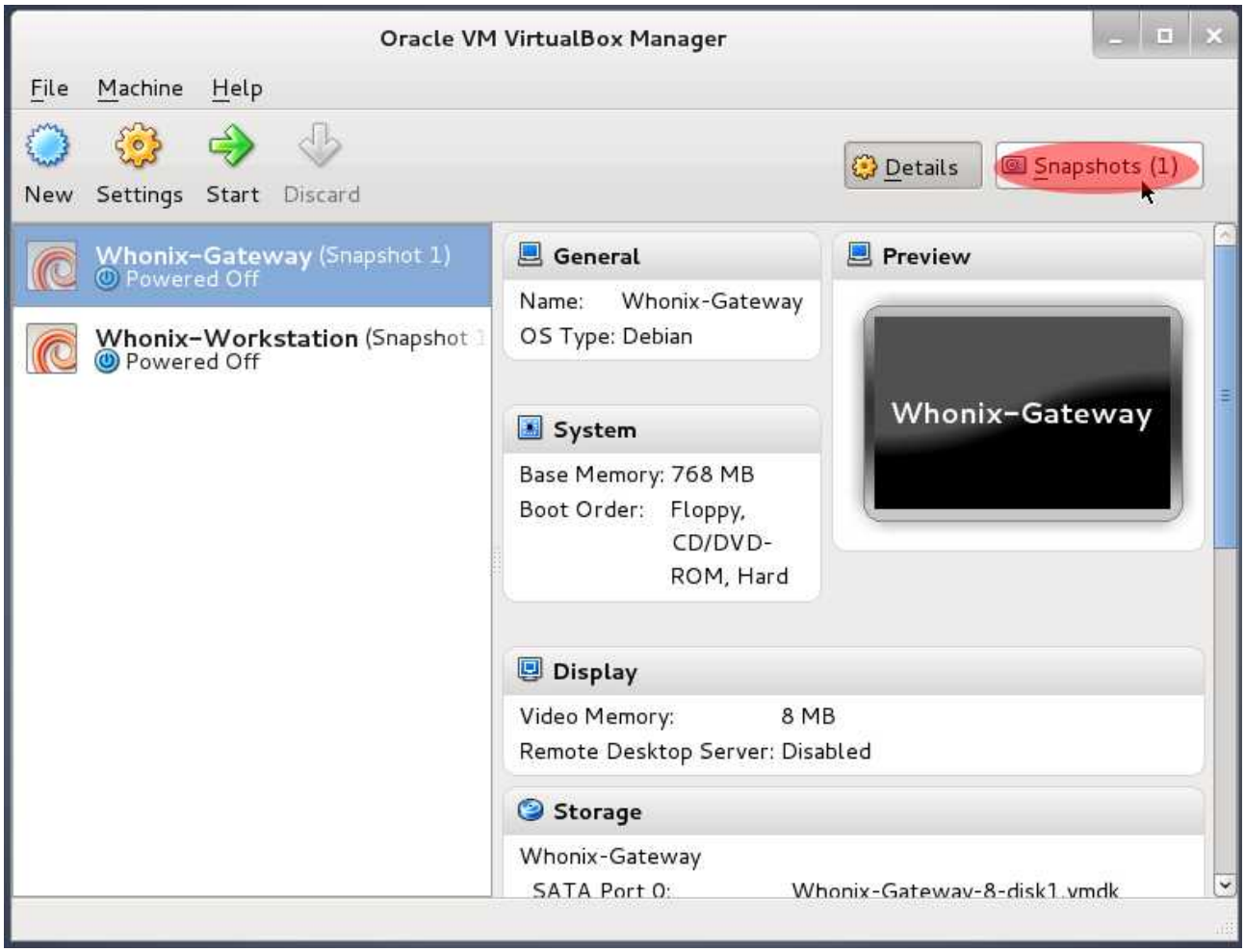
Also be aware that if you create a snapshot of a either the Whonix Gateway or Whonix Workstation after it has been compromised, and you are using that snapshot for this method, then the mitigation techniques described in this chapter will essentially be worthless. Thus, if you've already used the Whonix Gateway or Whonix Workstation to visit risky internet sites, consider doing a fresh install of Whonix as described in this guide before implementing the method in this chapter.

Let's begin.

1. **First and foremost, if your Whonix Gateway and Whonix Workstation are running, shut them down as described in steps 4-7 of Chapter 4a.** The first thing you need to do is create a new virtual hard drive to use with your Whonix Workstation. This is done from inside the VirtualBox Manager. If your VirtualBox Manager is not currently running in your Debian host OS, click on "Applications → Accessories → VirtualBox" to open the VirtualBox Manager.

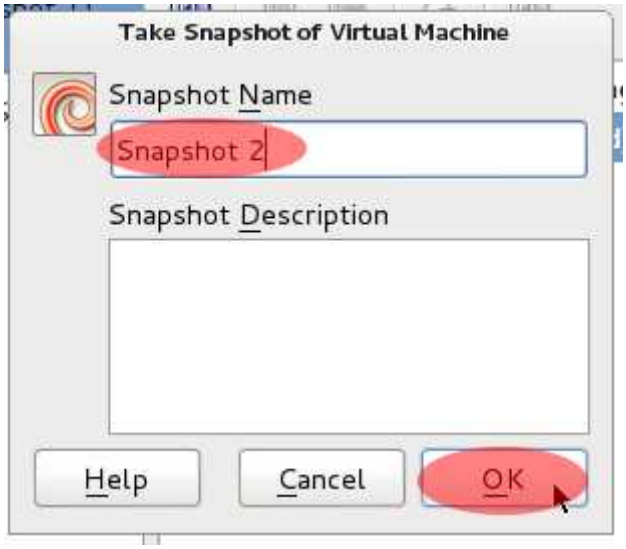


2. If you've made it this far, you've done some substantial work with your Whonix virtual machines. Take snapshots of them for backup purposes before proceeding. First, click on “Whonix Gateway” and then click on “Snapshots.”

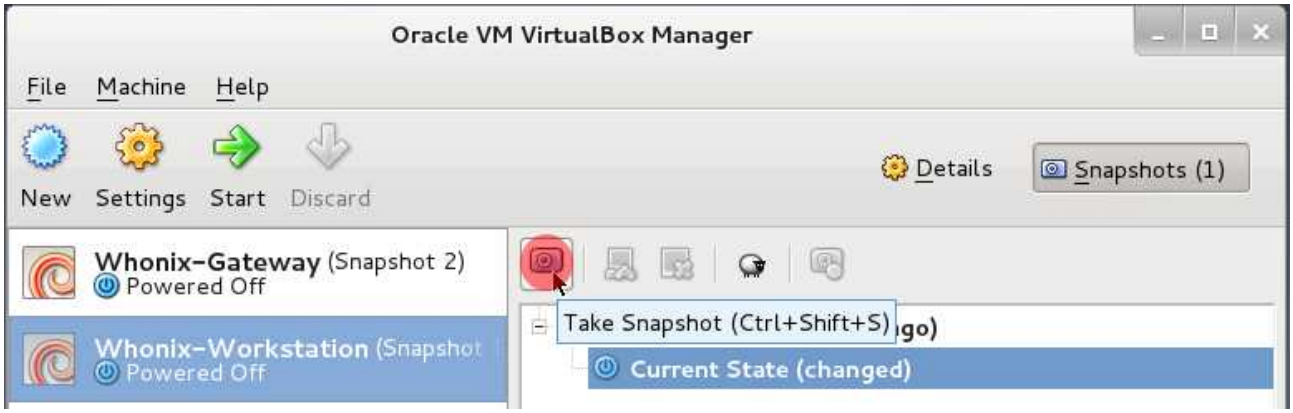


3. Next, click on the icon that looks like a camera towards the upper center of the screen to take a snapshot of your Whonix Gateway.

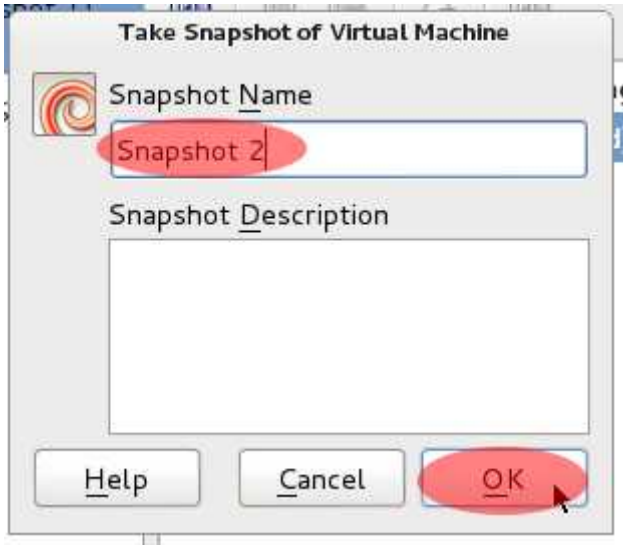
4. On the next screen that appears, choose whatever name you want for your snapshot and click the “OK” button.



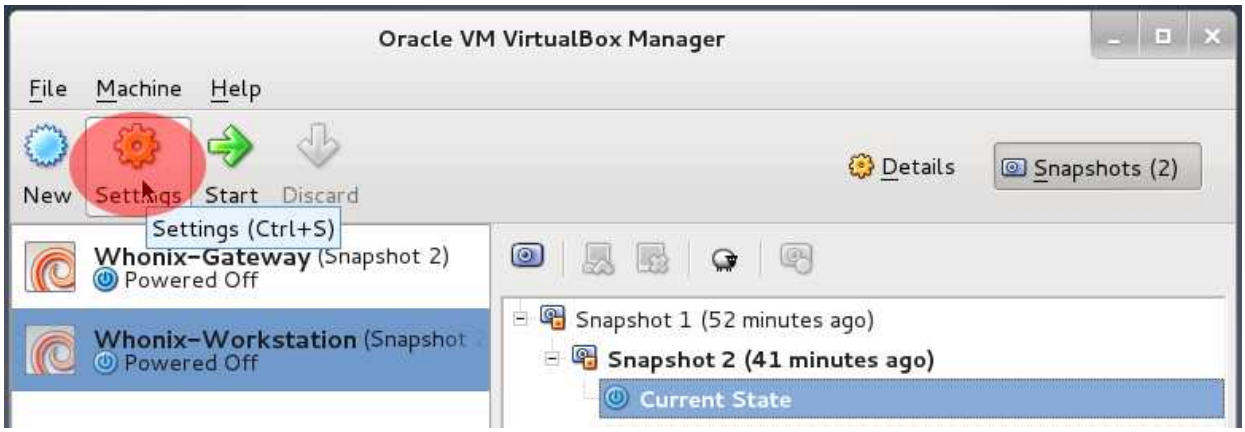
5. Next, click on the “Whonix Workstation” to select it and click on the camera icon towards the upper center of the screen to take a snapshot.



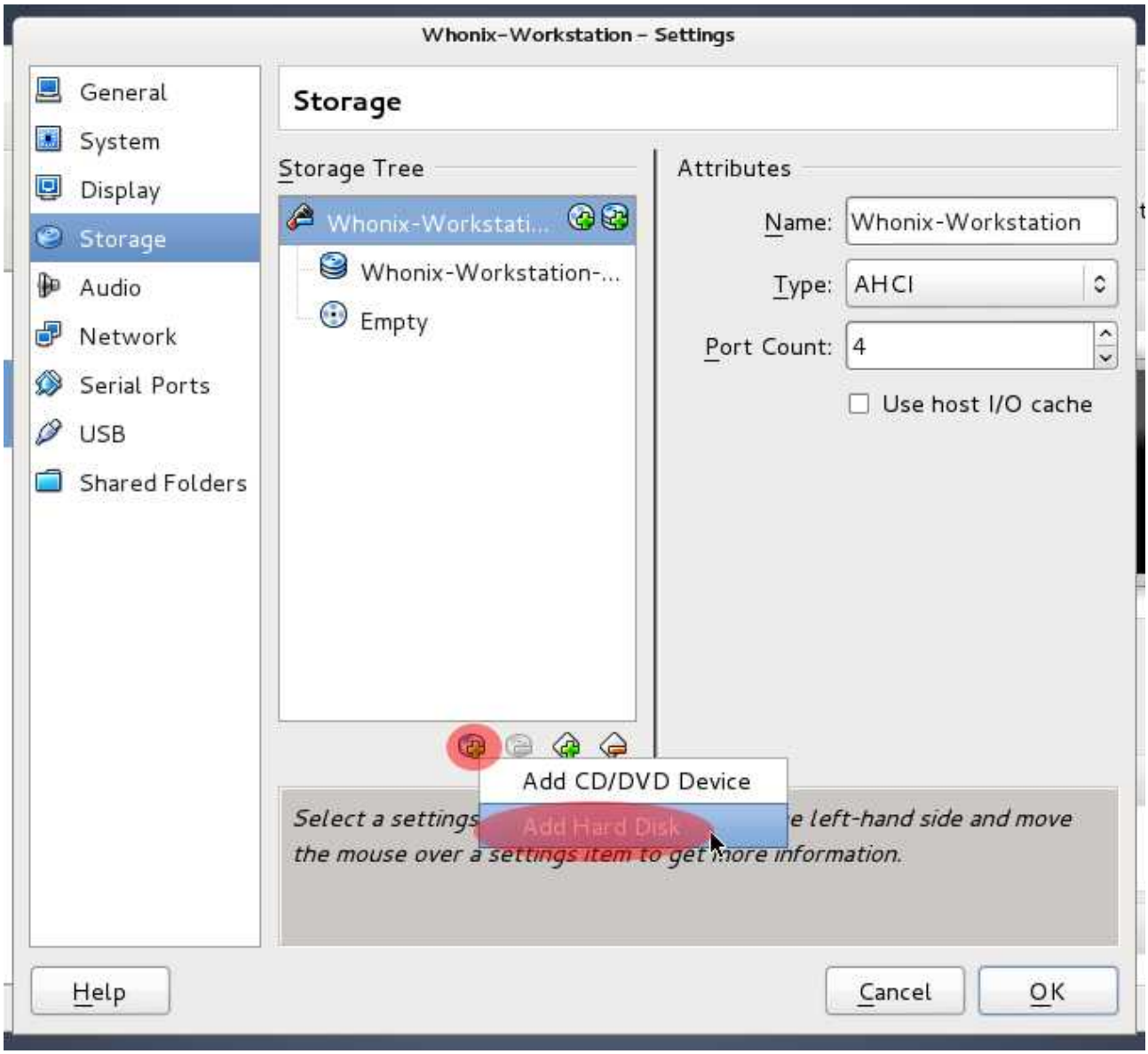
6. On the next screen, choose whatever name you want for your snapshot and click the “OK” button.



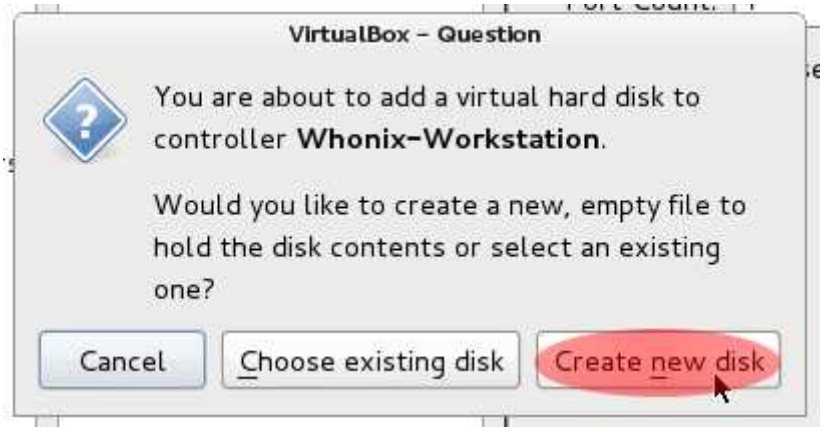
7. Next, with the “Whonix Workstation” still selected, click on “Settings.”



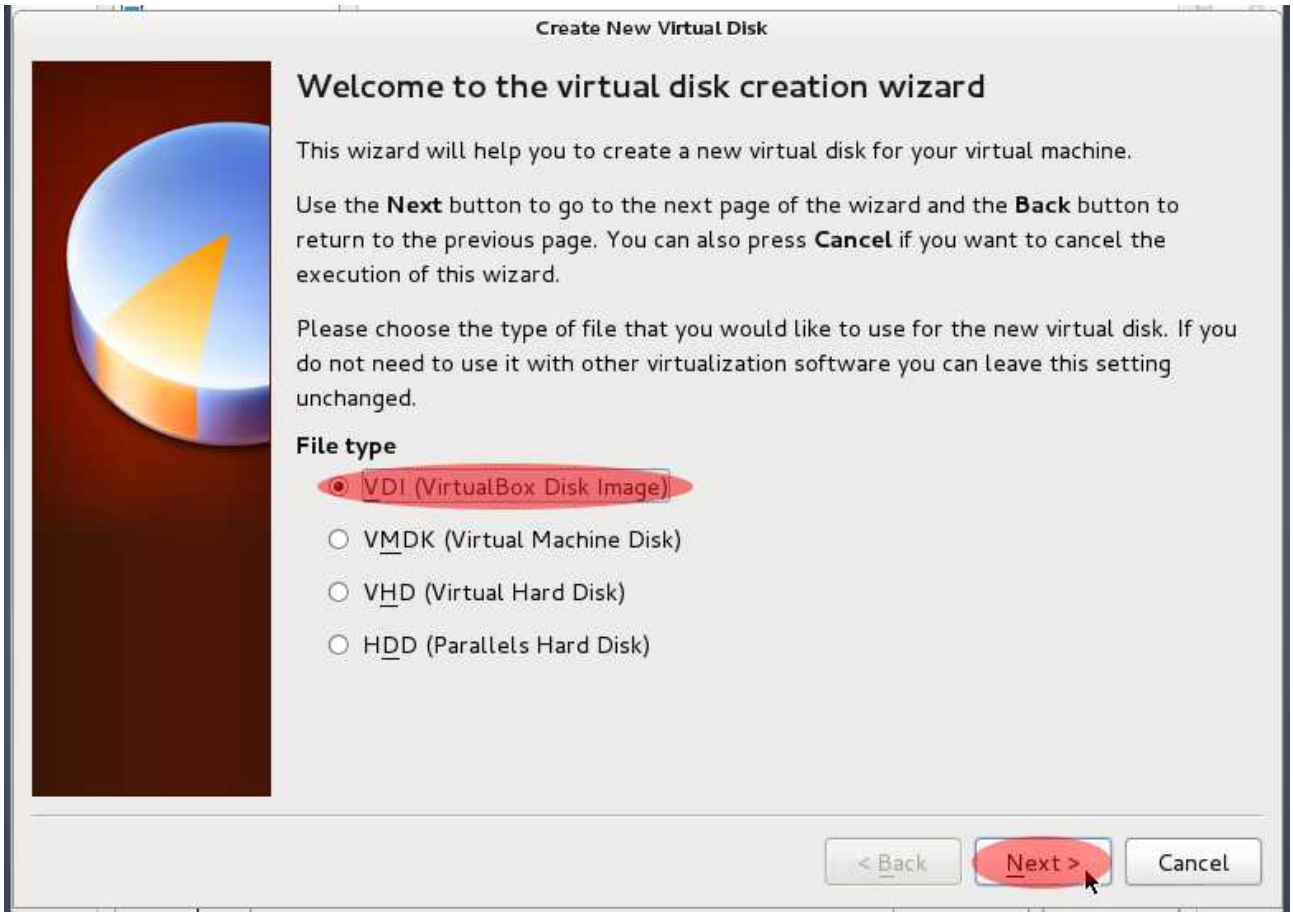
8. In the window that appears, click on “Storage” on the left side of the window. Then, click the small icon that looks like a circular disk with a “+” sign on it towards the bottom of the window and select “Add Hard Disk.”



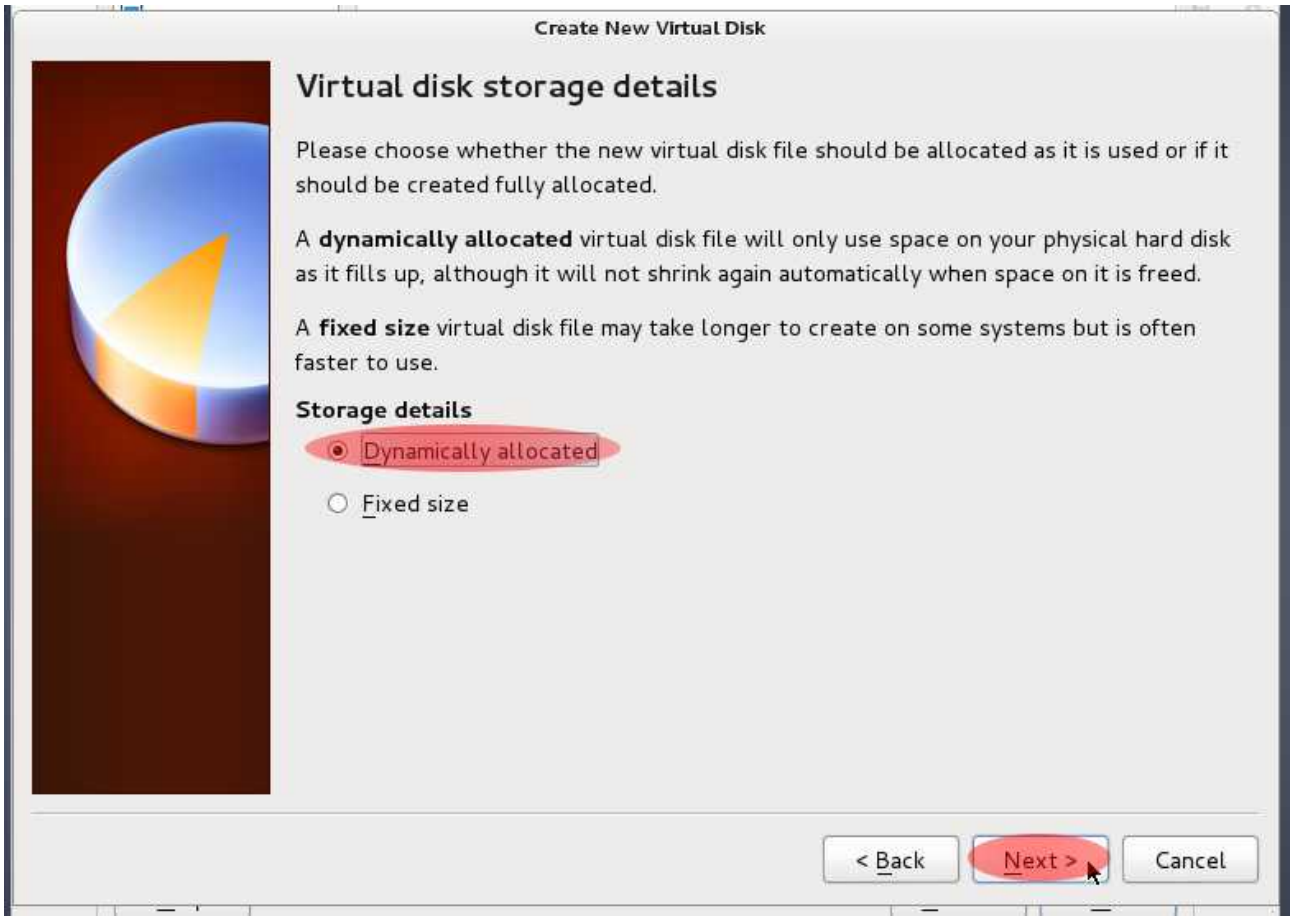
9. In the next window that appears, click on the “Create new disk” button.



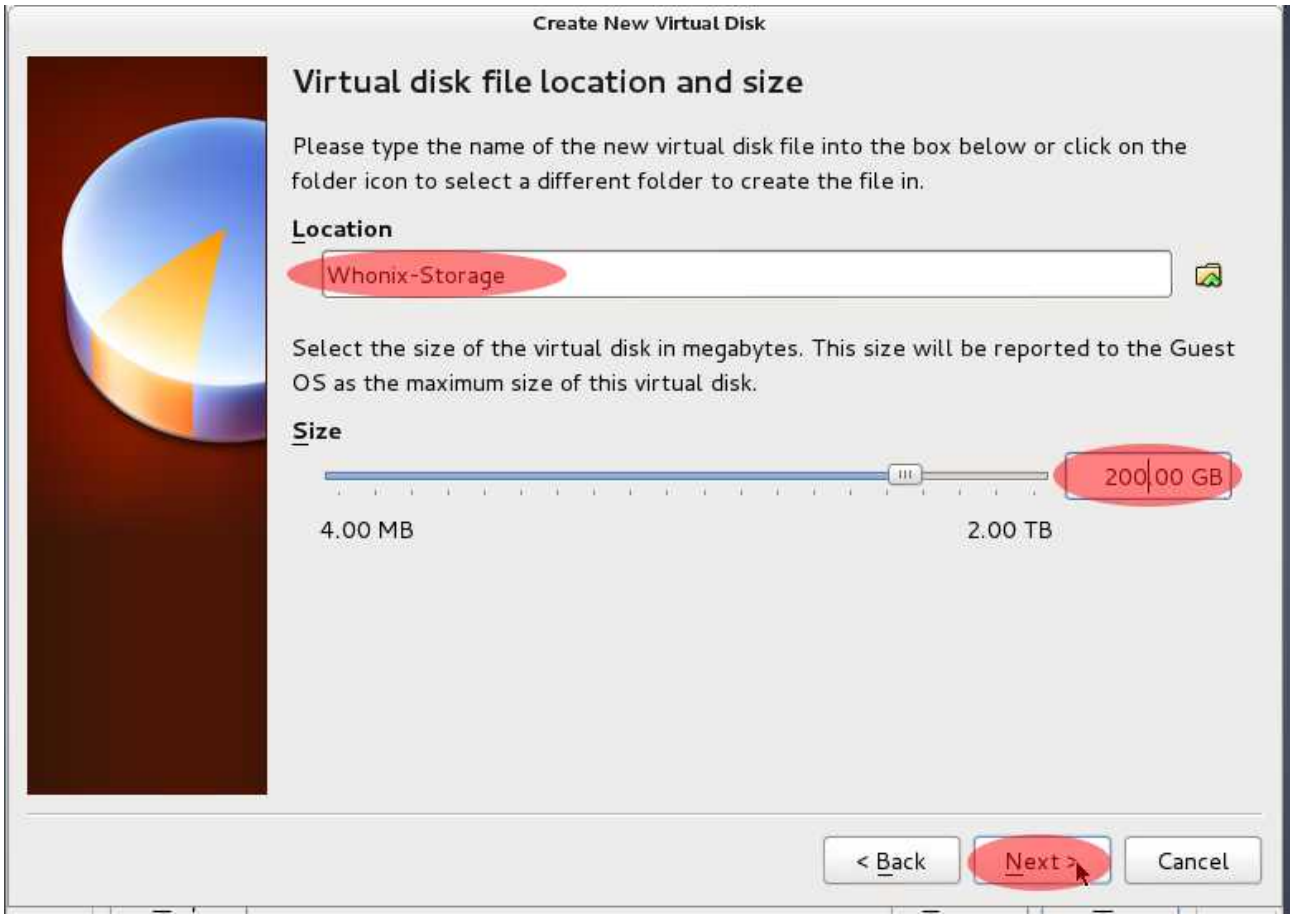
10. In the window that appears, choose “VirtualBox Disk Image” and click “Next.”



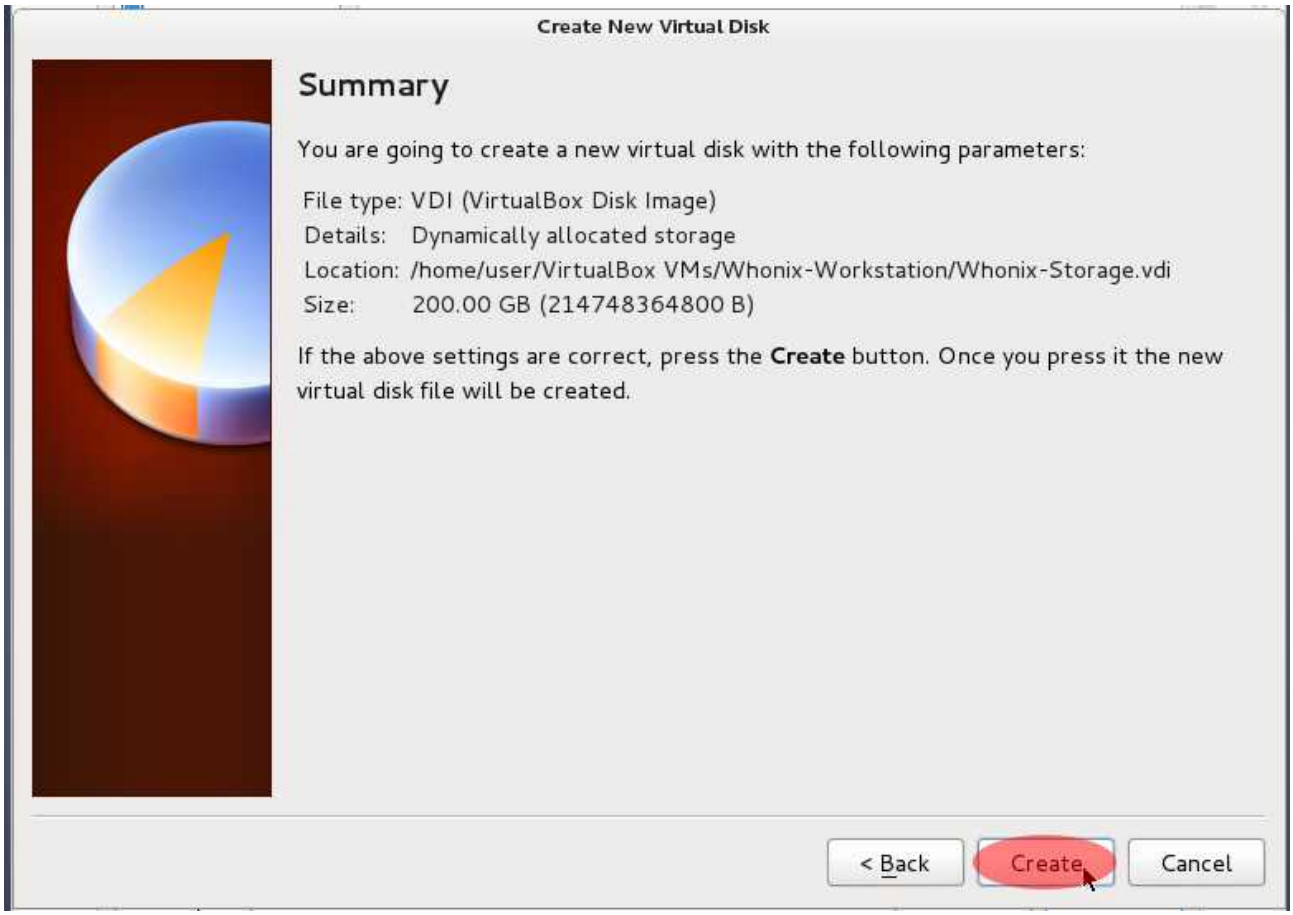
11. On the next screen, select “dynamically allocated” and click on the “Next” button.



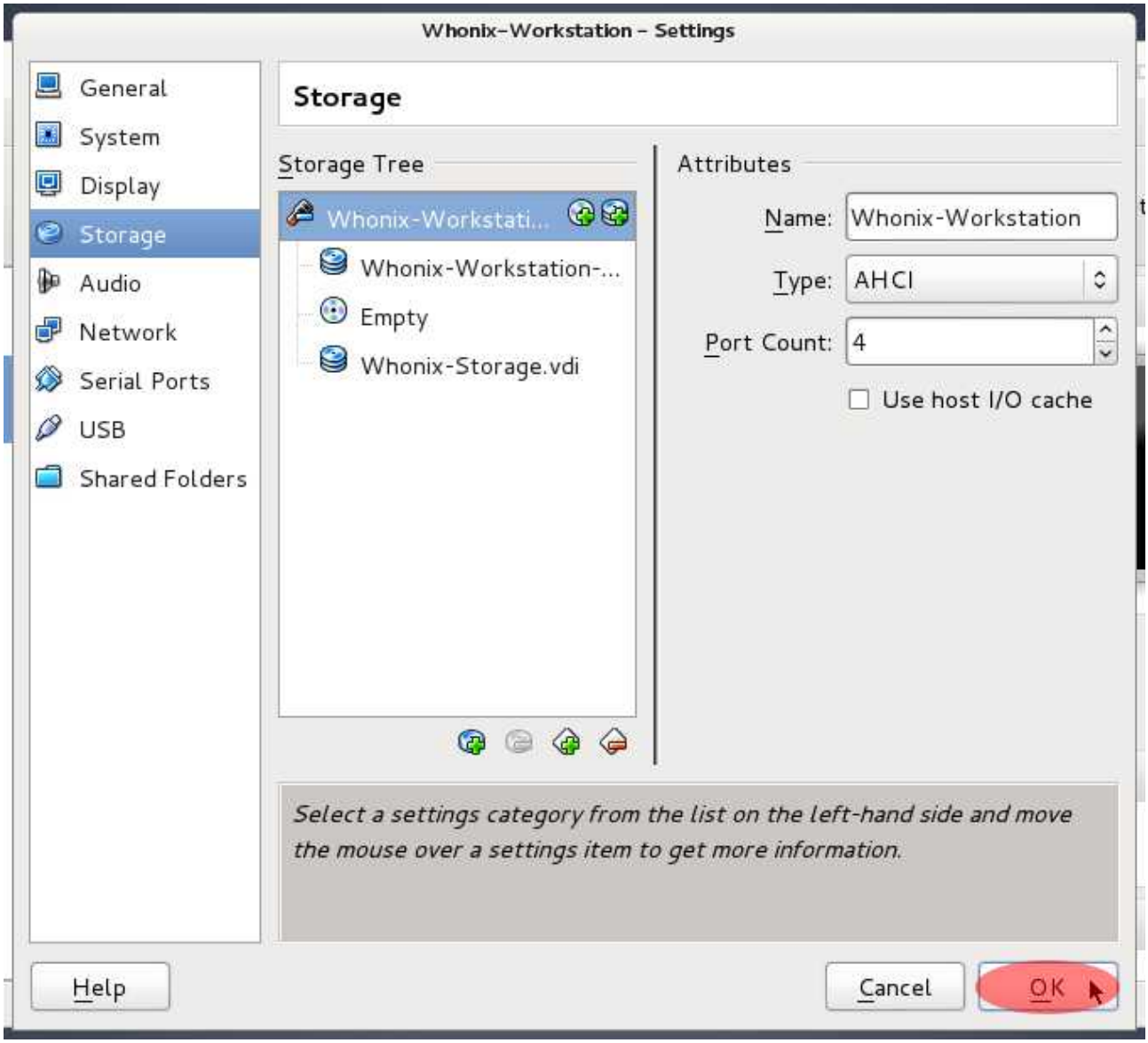
12. Now, choose a name for your new virtual hard disk in the field under “Location.” Then, choose the maximum amount of data you want the drive to be able to hold by either adjusting the slider under “Size” or typing in the size you prefer in the field next to the slider. If you believe there is ever a chance that you will be storing a lot of data on your new hard drive, choose a larger size. Since the virtual hard disk is “dynamically allocated,” a larger size won't instantly take up more disk space on your local hard drive. Rather, the virtual hard drive will only increase in size as data is written to it. Finally, when you are ready to proceed, click the “Next” button.



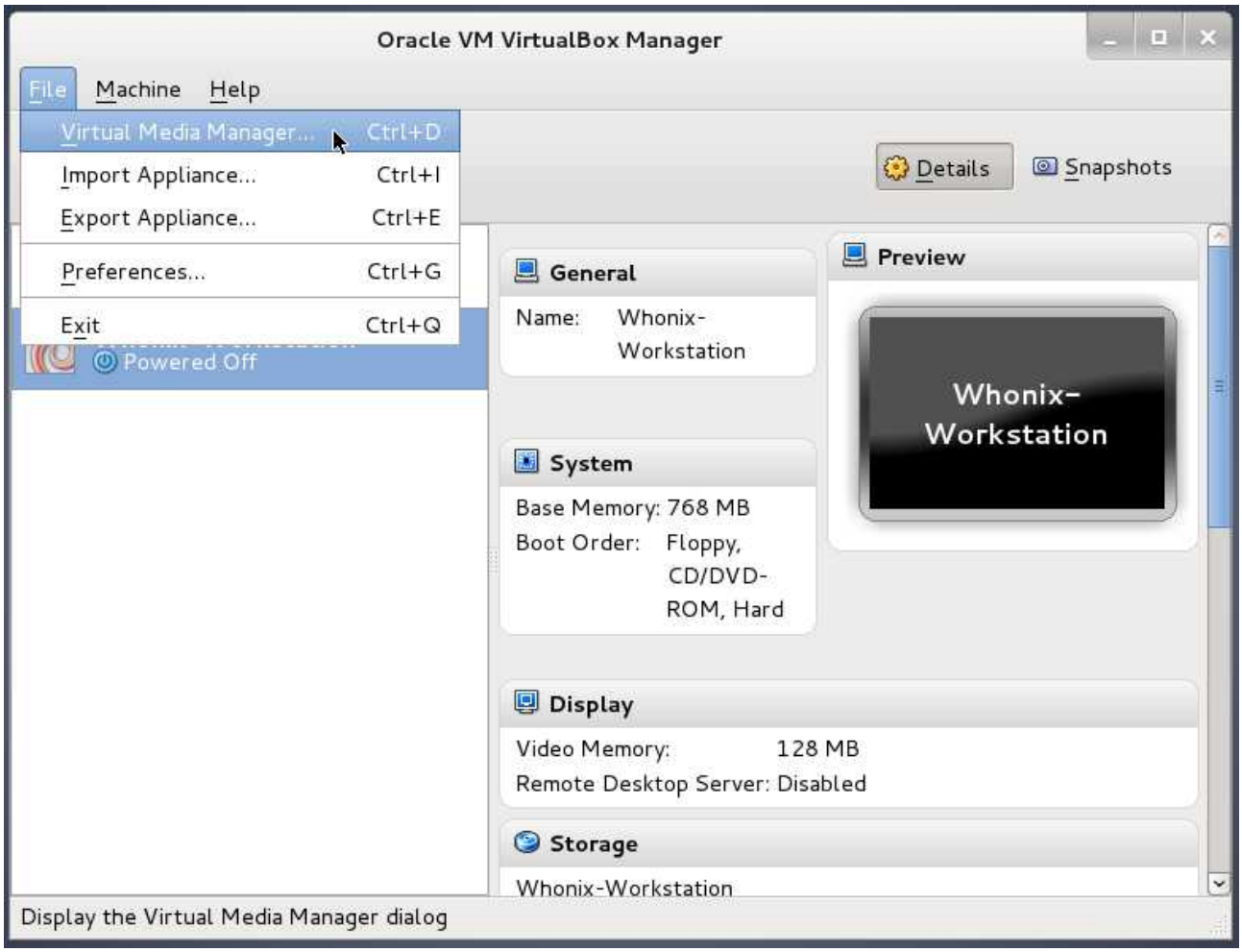
13. On the next window that appears, click on the “Create” button.



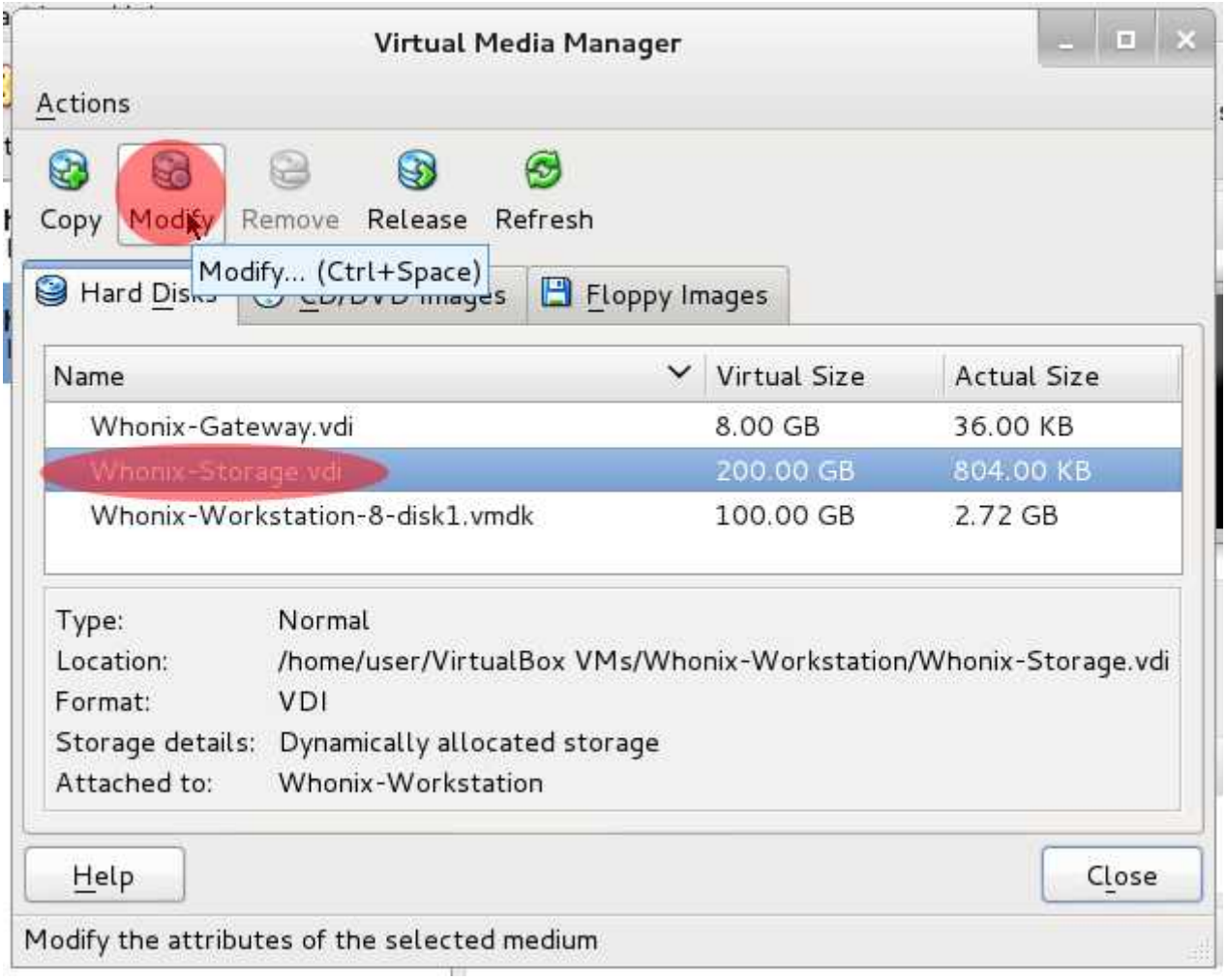
14. When you are returned the “Whonix Workstation Settings” screen of the VirtualBox Manager, click on the “OK” button.



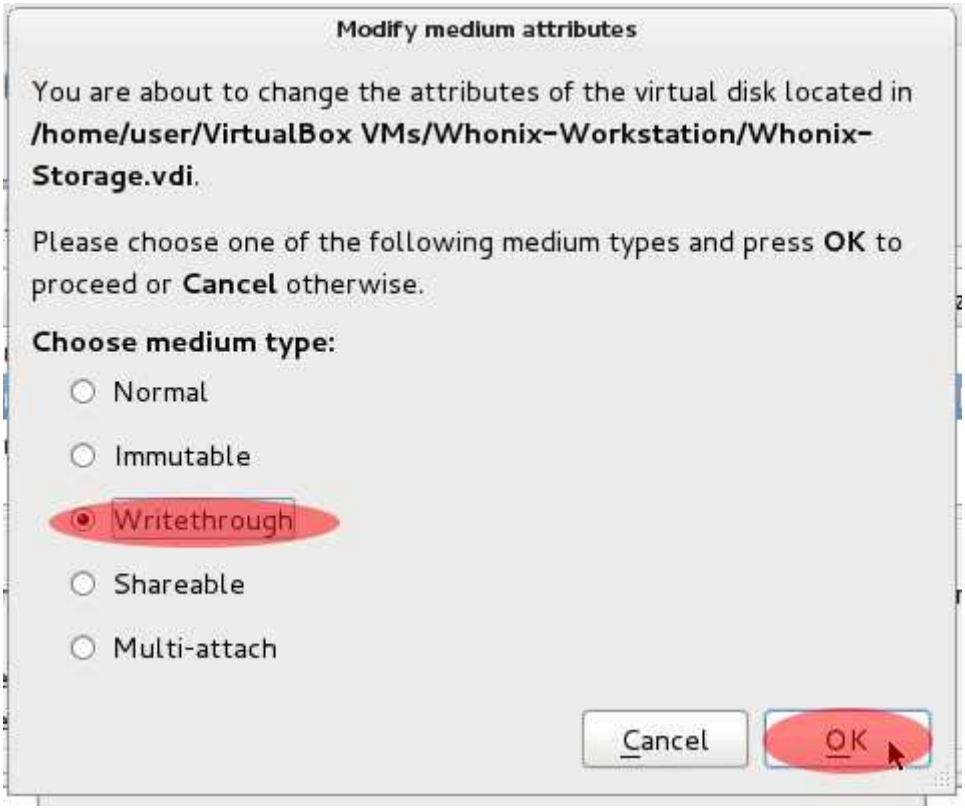
15. Next, you need to set the new hard drive you created to not be affected when you restore your Whonix Workstation from a snapshot. To do this, open the Virtual Media Manager in the VirtualBox Manager. Click on “File → Virtual Media Manager.”



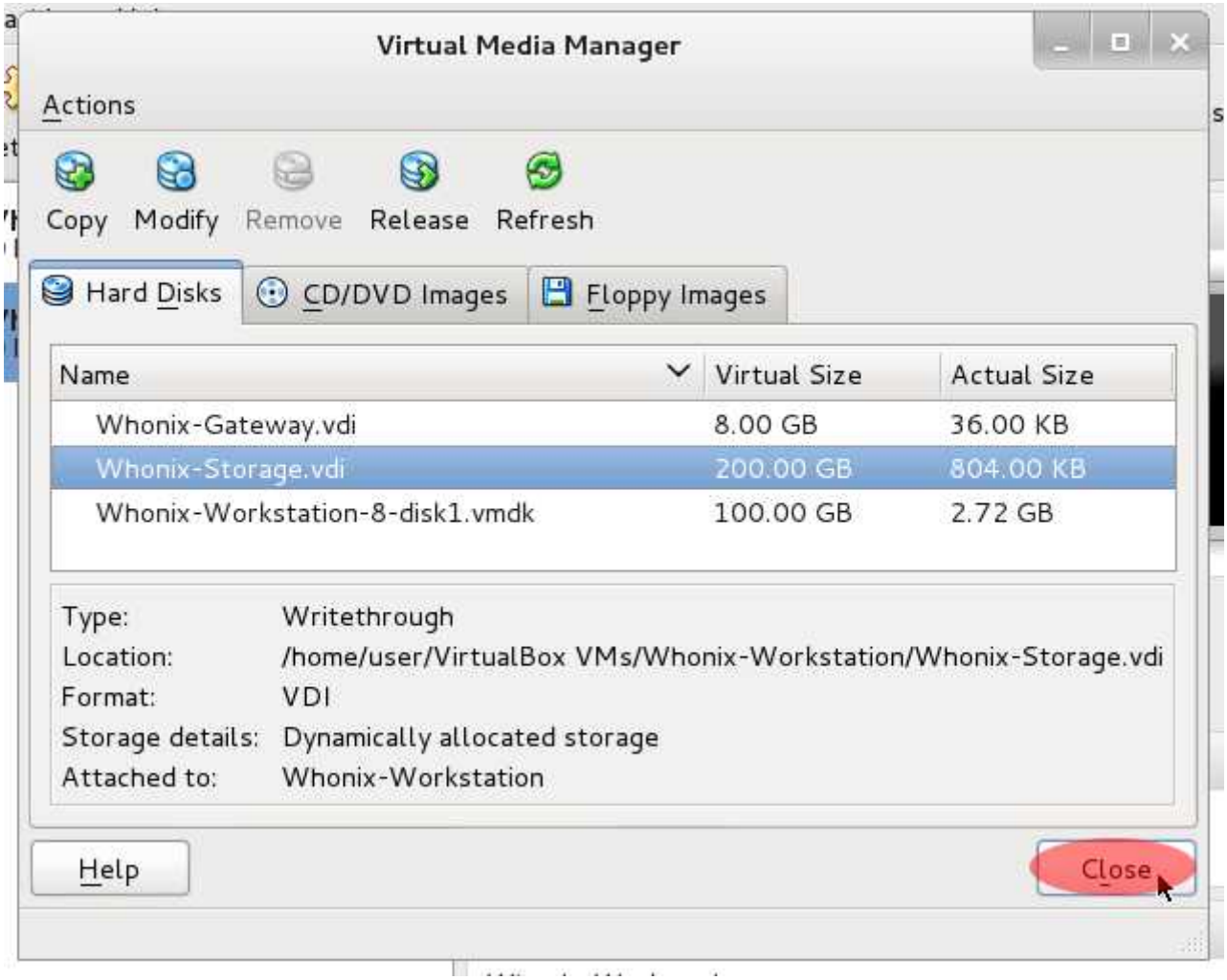
16. In the next window that appears, click on the name of the new virtual hard drive you created in the steps above and then click the “Modify” button.



17. On the next screen, select “Writethrough” as your medium type and click the “OK” button.

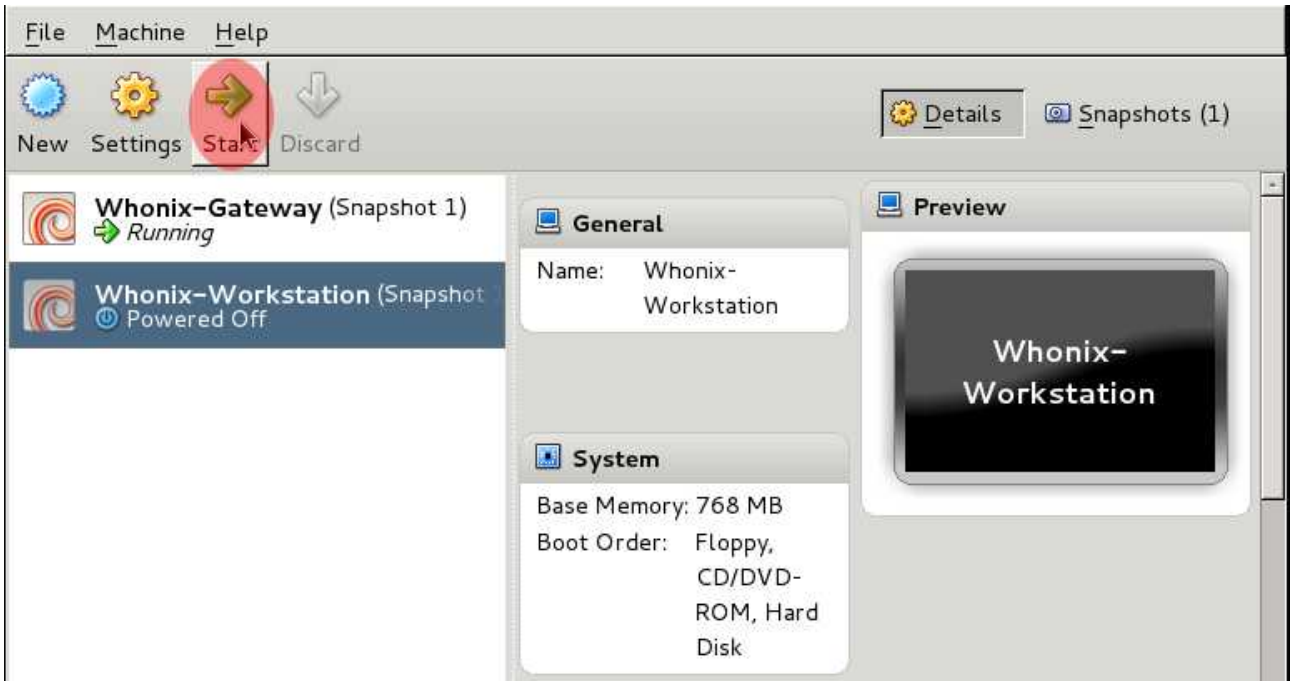


18. When returned to the Virtual Media Manager, click the “Close” button.



19. Now, start your Whonix Gateway. Click on “Whonix Gateway” in your VirtualBox Manager and then click the “Start” button.

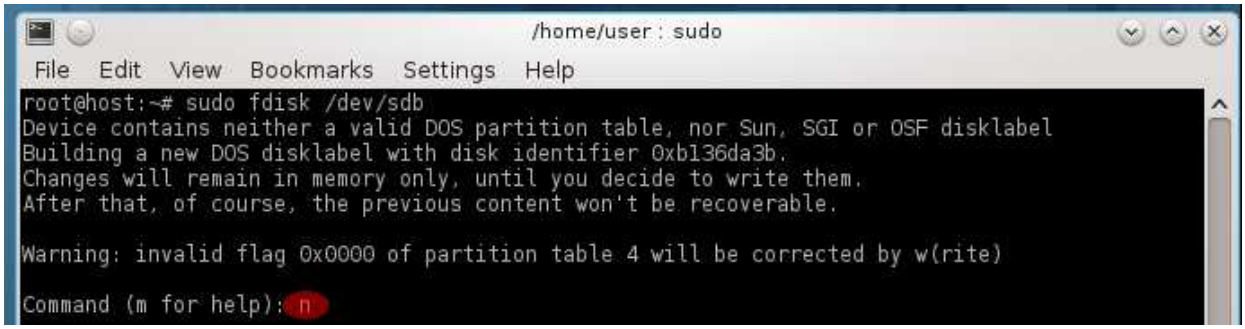
20. Next, start your Whonix Workstation. Click on “Whonix Workstation” and then click on the “Start” button.



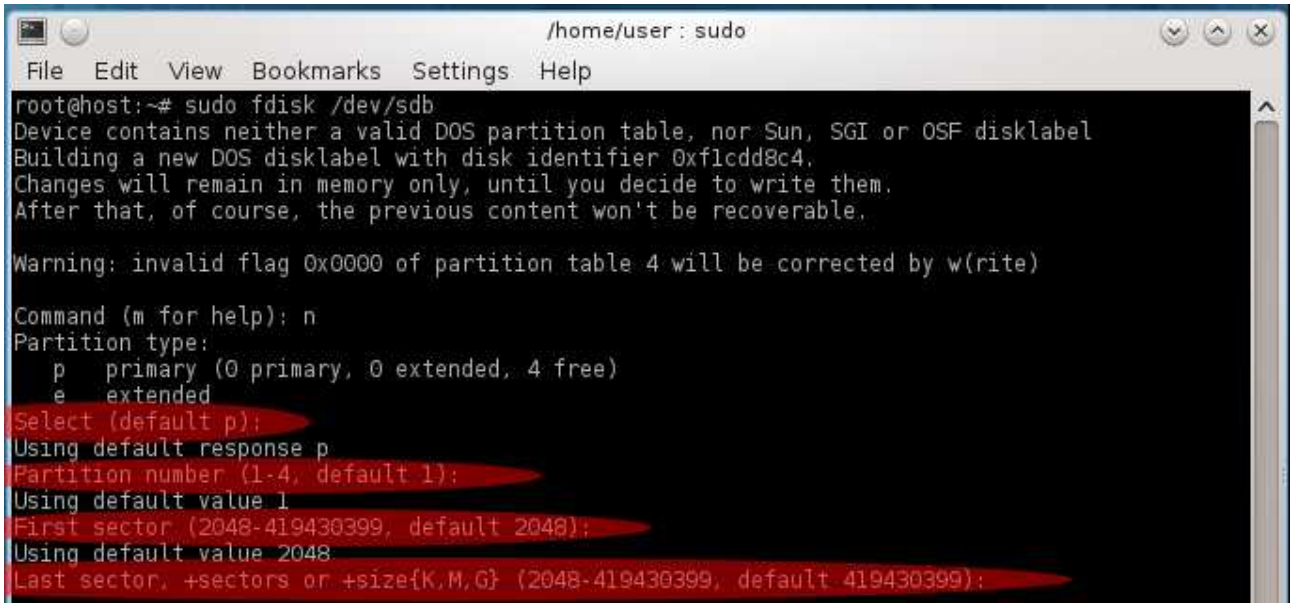
21. When the system boots and you reach the Whonix Workstation Desktop, click on the “Konsole” icon on your Desktop to open a terminal session.

22. Now, you need to format the new virtual hard disk you created. In the terminal, type "**sudo fdisk /dev/sdb**". When prompted for your password, type it and press "enter."

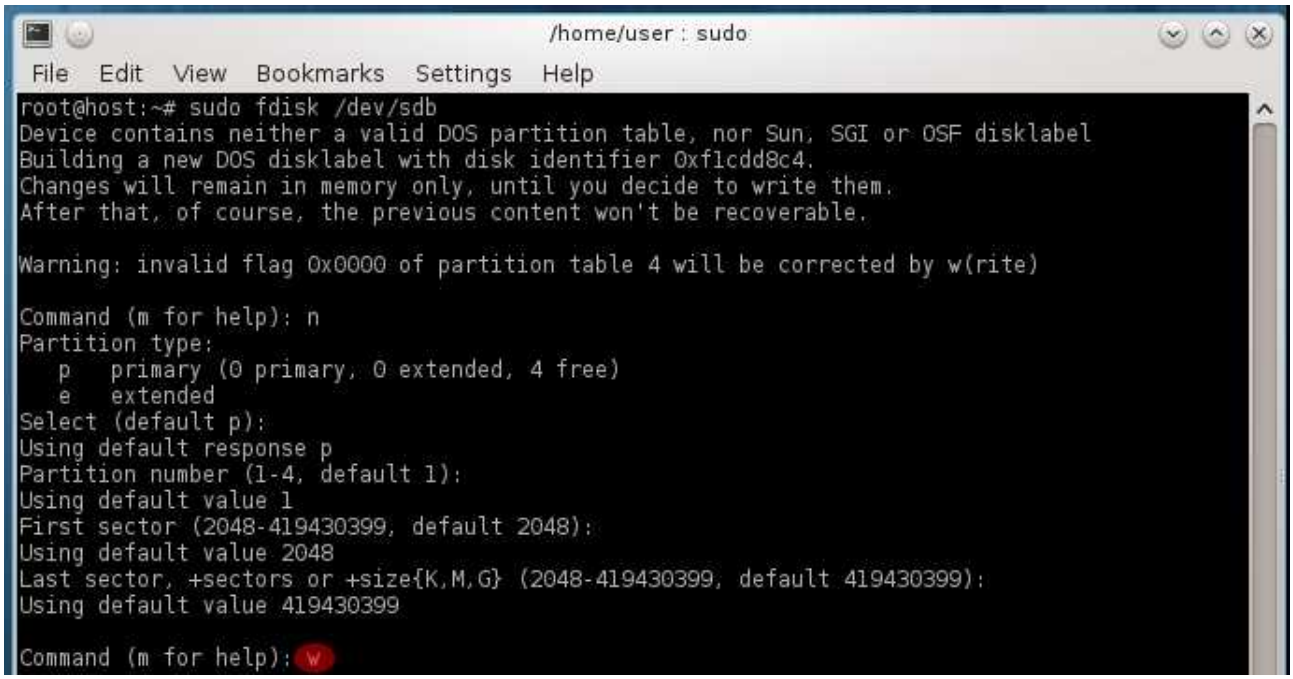
23. When you reach the command prompt in fdisk, type "**n**" to create a new partition.



24. For the remaining prompts that appear while creating the new partition, accept the defaults. Simply press "enter" after every prompt that appears that is highlighted in red below.



25. When returned to the main prompt in fdisk, type "**w**" to write the changes to disk.

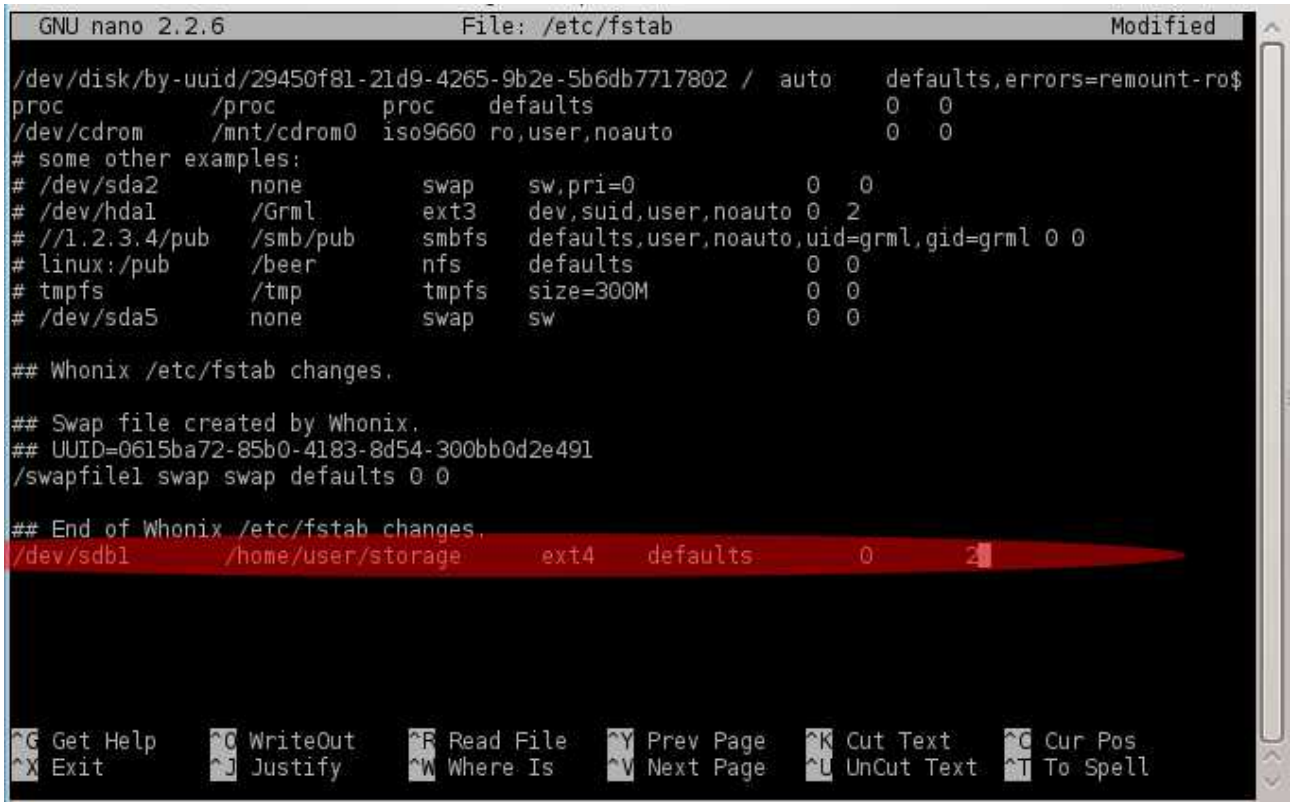


26. You will now be returned to your terminal command prompt. You need to format the newly created partition in order to be able to use it. Type "**sudo mkfs.ext4 /dev/sdb1**" and press "enter."

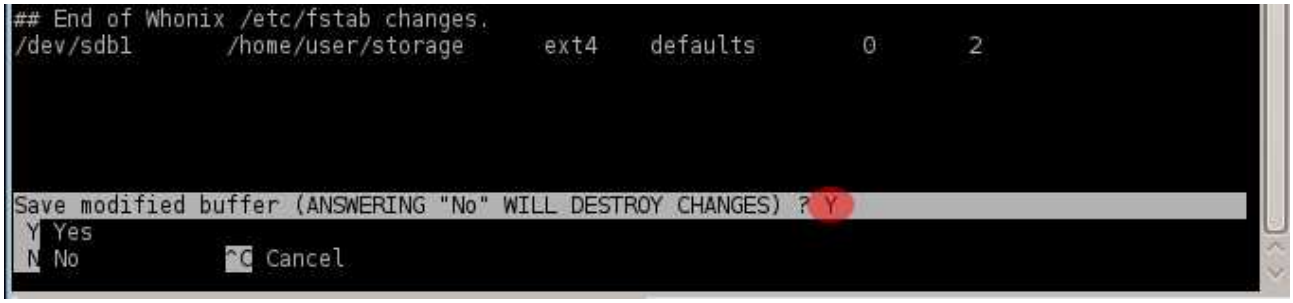
27. When the disk finishes formatting and you re returned to the command prompt, create a directory that will be used by the new virtual hard disk in the future.
Type "**mkdir storage**" and press "enter."

28. Next, you need to configure your Whonix Workstation to mount the new virtual hard disk on every boot. Type "**sudo nano /etc/fstab**" and press "enter."

29. The next screen is the nano editor. Use your down-arrow key to navigate to the bottom of the file and type "**/dev/sdb1 /home/user/storage ext4 defaults 0 2**" as the last line.

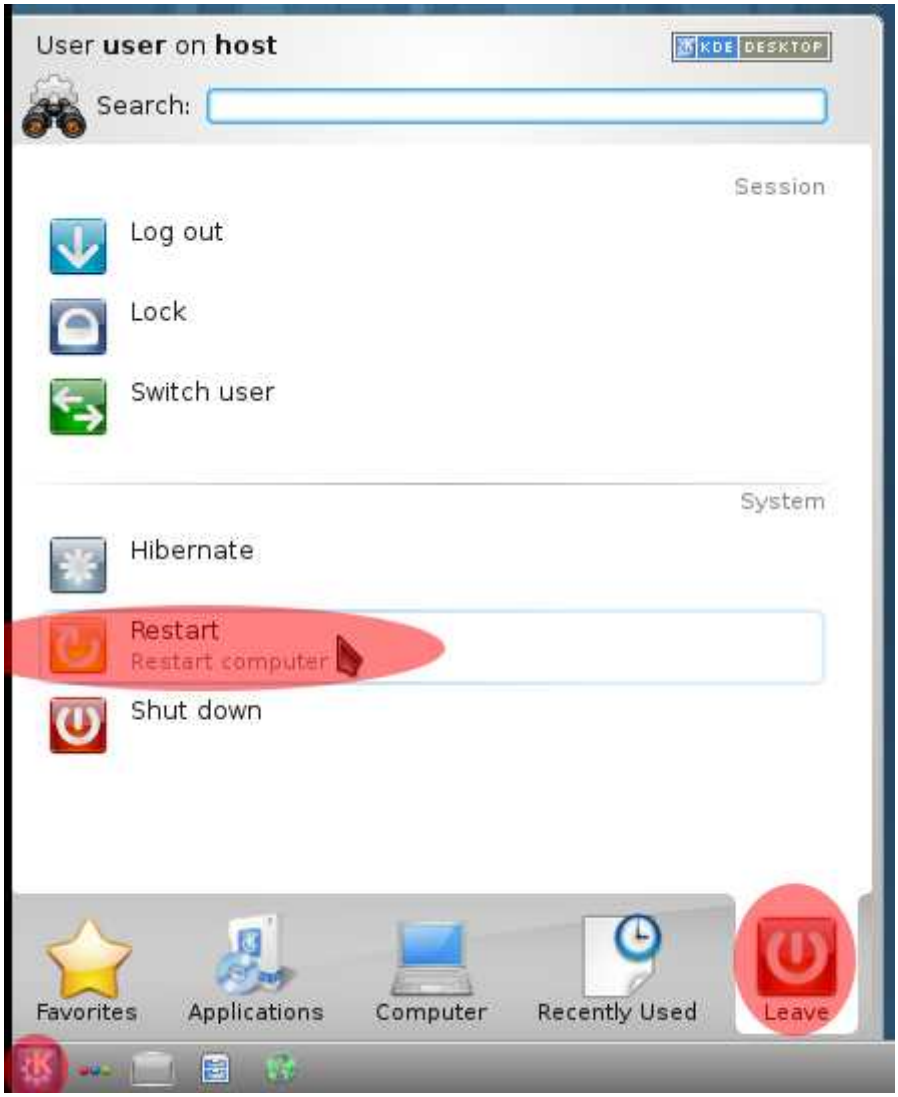


30. Next, type you need to use a left-control-keystroke to exit nano and save the file. Press "**LEFT CTRL-X**". When prompted to save your changes, type "**Y**".



31. The next prompt will ask you to select a file name to which you will save the file which should default to “/etc/fstab”. Press “enter” to continue.

32. Next, restart the Whonix Workstation for your changes to take effect. Click on the “K” start button in the lower left corner of your screen, hover the mouse over the “Leave” icon that appears in the right side of the Start Menu and then click on “Restart.”



33. In the next screen that appears, click on the “Restart Computer” button.

34. A window will eventually appear asking if you wish to “abort active sessions.” Click on the “OK” button.

35. Let the Whonix Workstation go through its reboot process. When you are returned to the Desktop, click on the “Konsole” icon on your Desktop.

36. Next, you need to change which account owns the “storage” directory in order to make use of it. Type “**sudo chown user:user storage**” and press “enter.”

```
user@host:~$ sudo chown user:user storage
```

37. Now, you need to move various files and directories to the persistent “storage” directory. **This step of the tutorial is assuming you saved your KeePassX password database as “mypass.kdb” in your home directory. If you saved it as something else, replace “mypass.kdb” with the path and file name you chose in the following command.**

    Type “**mv -t storage .gnupg .icedove .purple .xchat2 mypass.kdb**” and press “enter.”

```
user@host:~$ mv -t storage .gnupg .icedove .purple .xchat2 mypass.kdb
```

38. Next, you need to create symbolic links in your home directory to the files and directories you just moved to the storage directory. If you are familiar with Microsoft Windows, think of these as being similar to “shortcuts.” This will take a few steps.
    Create a symbolic link for your GPG encryption data. Type “**ln -s storage/.gnupg .gnupg**” and press “enter.”

```
user@host:~$ ln -s storage/.gnupg .gnupg
```

39. Next, create a symbolic link for your Icedove e-mail data.
    Type “**ln -s storage/.icedove .icedove**” and press “enter.”

```
user@host:~$ ln -s storage/.icedove .icedove
```

40. Next, create a symbolic link for your Pidgin instant messenger data.
    Type “**ln -s storage/.purple .purple**” and press “enter.”

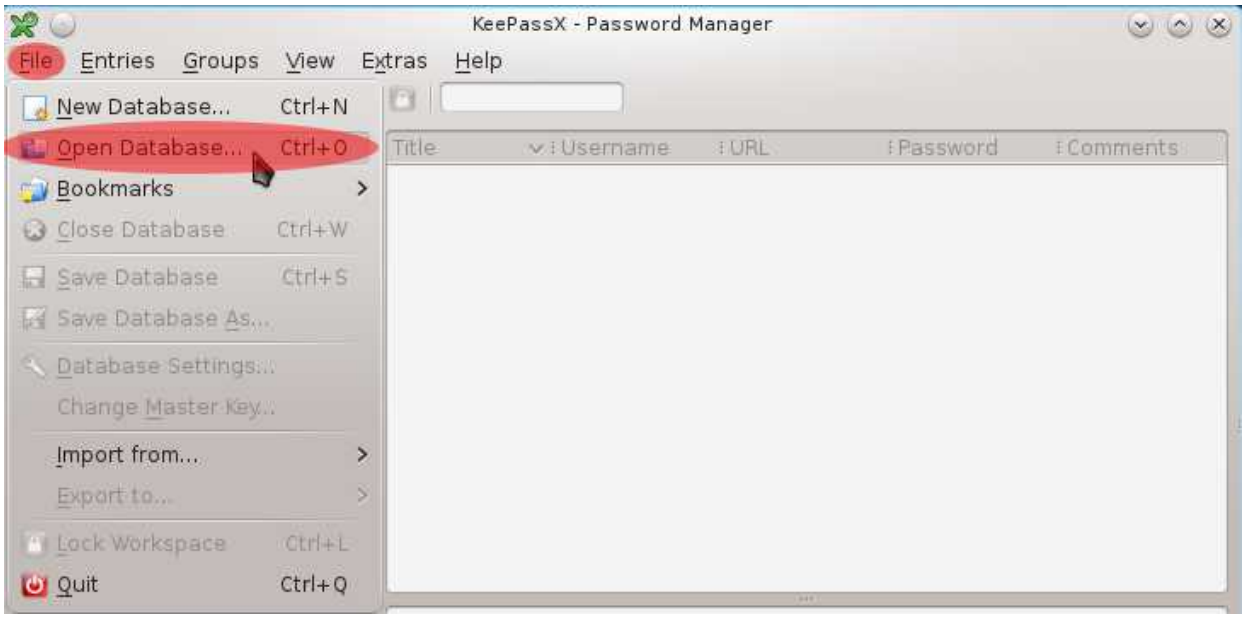
```
user@host:~$ ln -s storage/.purple .purple
```

41. Next, create a symbolic link for your XChat IRC data.
    Type “**ln -s storage/.xchat2 .xchat2**” and press “enter.”

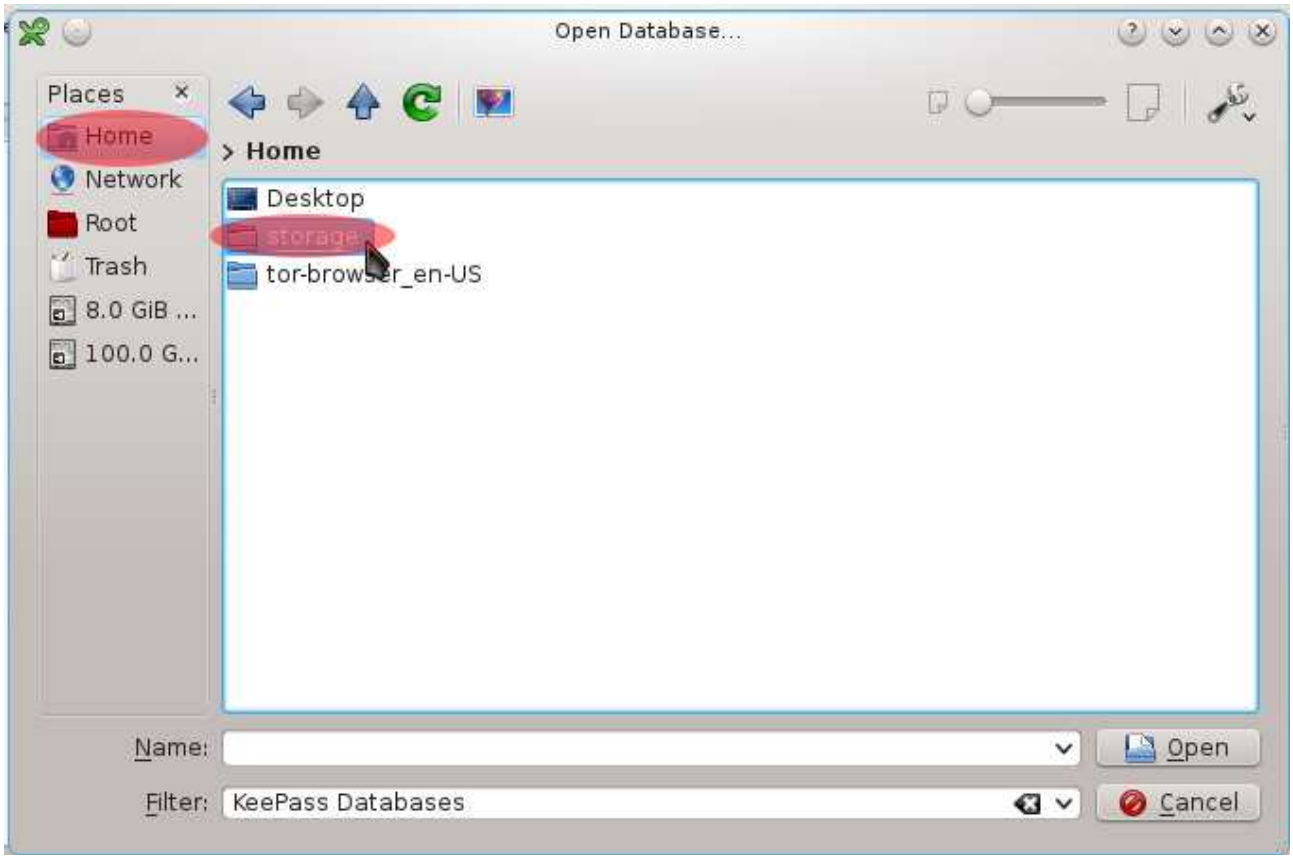
```
user@host:~$ ln -s storage/.xchat2 .xchat2
```

42. Next, you need to point KeePassX to where you've moved your password database. Either open KeePassX through the K Start Button or double-click on the KeePassX icon on your Desktop.

43. KeePassX will now open to an empty screen. Click on “File → Open Database.”

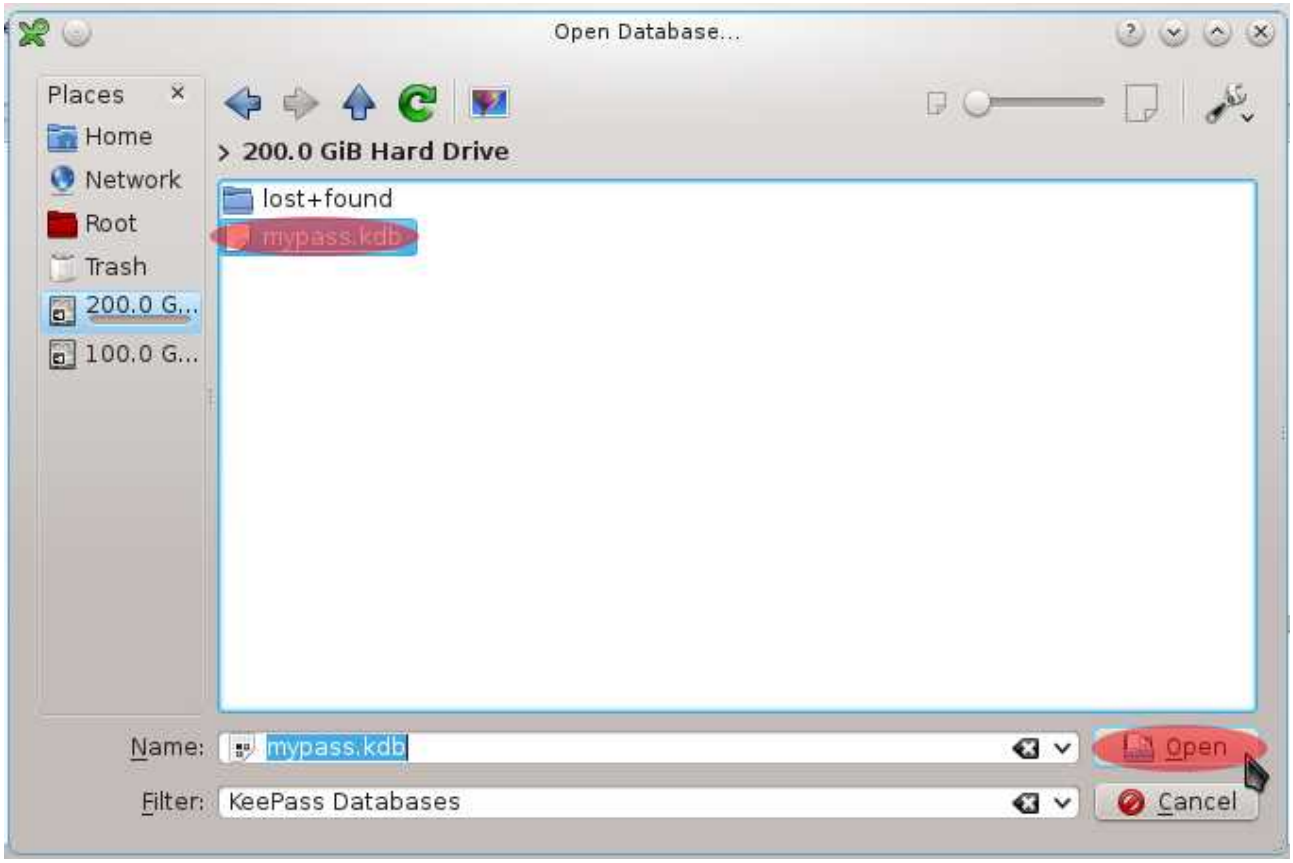


44. In the next window that appears, click on “Home” in the column to the left side. Then, double-click on “Storage.”



45. In the next screen, click on “mypass.kdb” and then click the “Open” button.

    NOTE: This step assumes you named your KeePassX database file “mypass.kdb.” If you named it something else, click on the file name you chose.

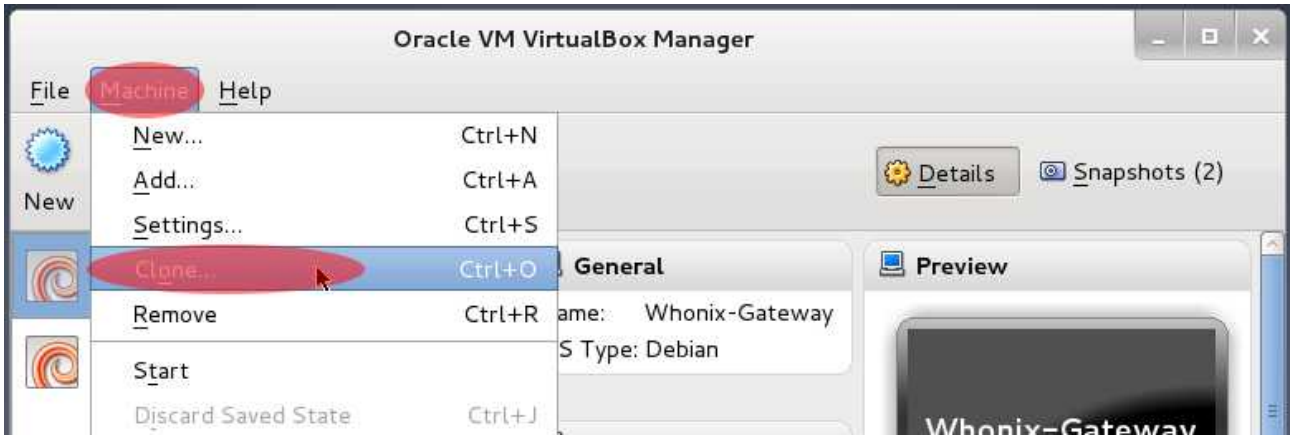


46. When prompted to enter your password, type the main password you set for your KeePassX password database in Step 6 of Chapter 4c in the field next to “password” and click the “OK” button.

47. Close KeePassX by clicking the “X” symbol in the upper right corner.

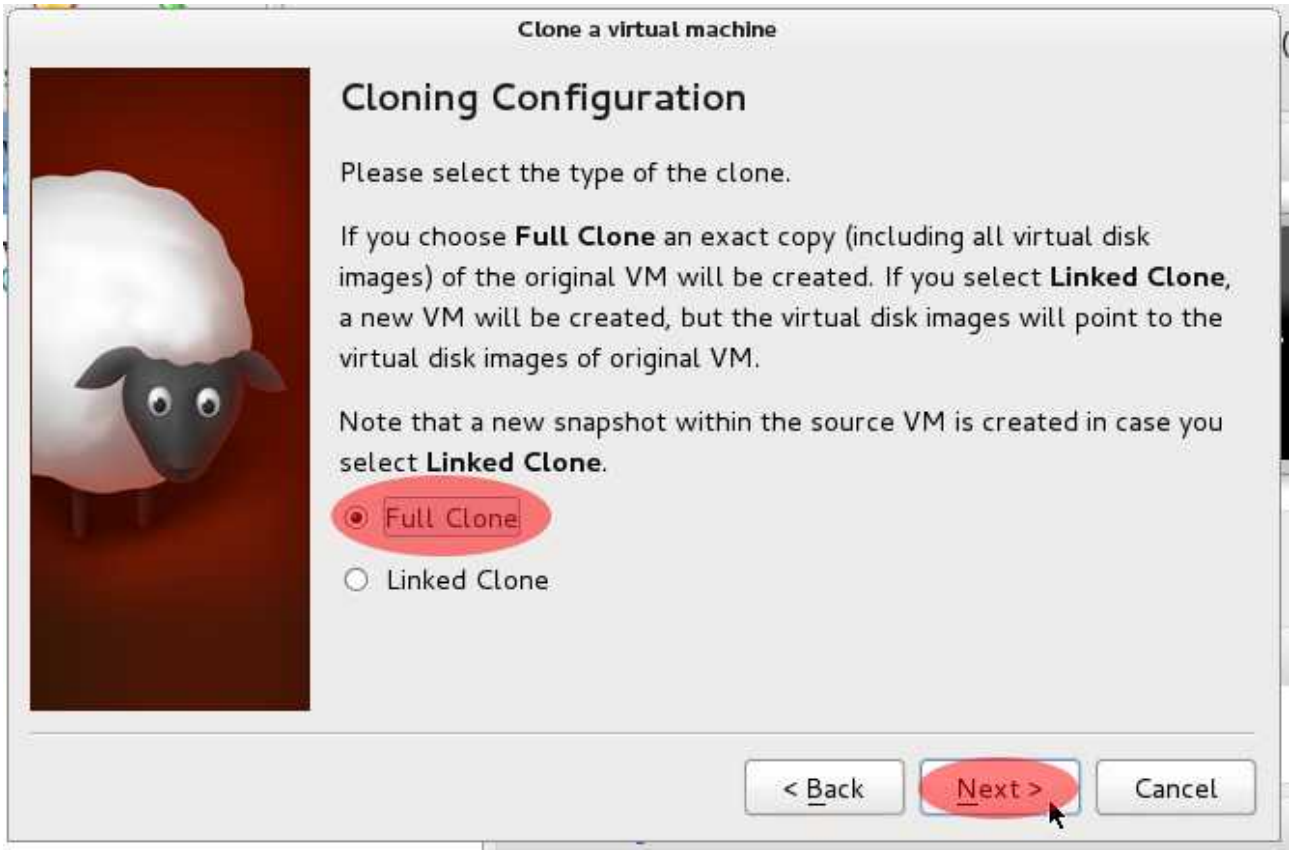
48. Next, **shut down both the Whonix Workstation and the Whonix Gateway as described in steps 4-7 of Chapter 4a.**

49. When both the Whonix Workstation and Whonix Gateway have shut down, you can now clone them. Click on "Whonix Gateway" to select it in the VirtualBox Manager. Then click on "Machine → Clone."

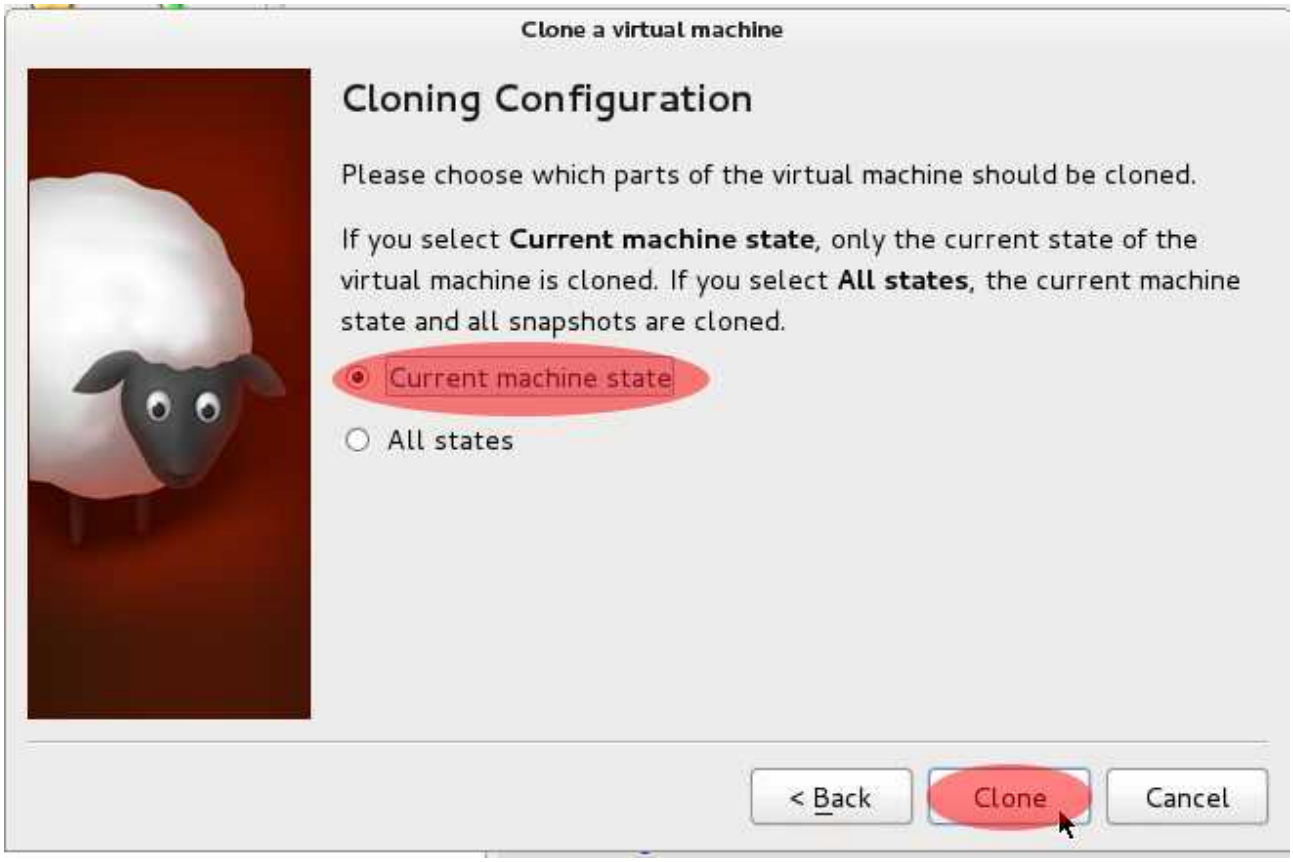


50. In the next window that appears, type "Whonix-Gateway [Mitigated]" for the name of the new virtual machine. Then, click on the "Next" button.

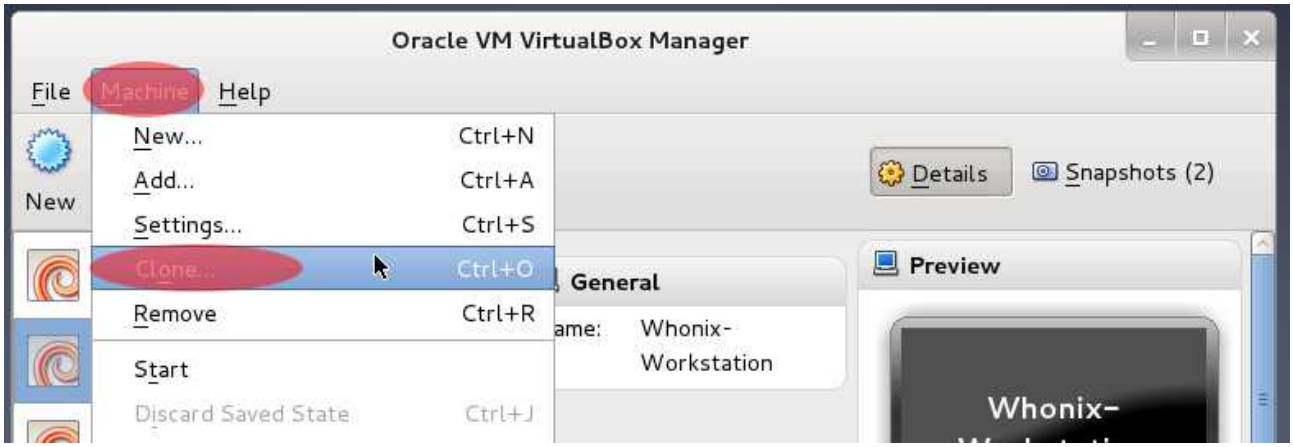
51. In the next screen, select “Full Clone” and click the “Next” button.



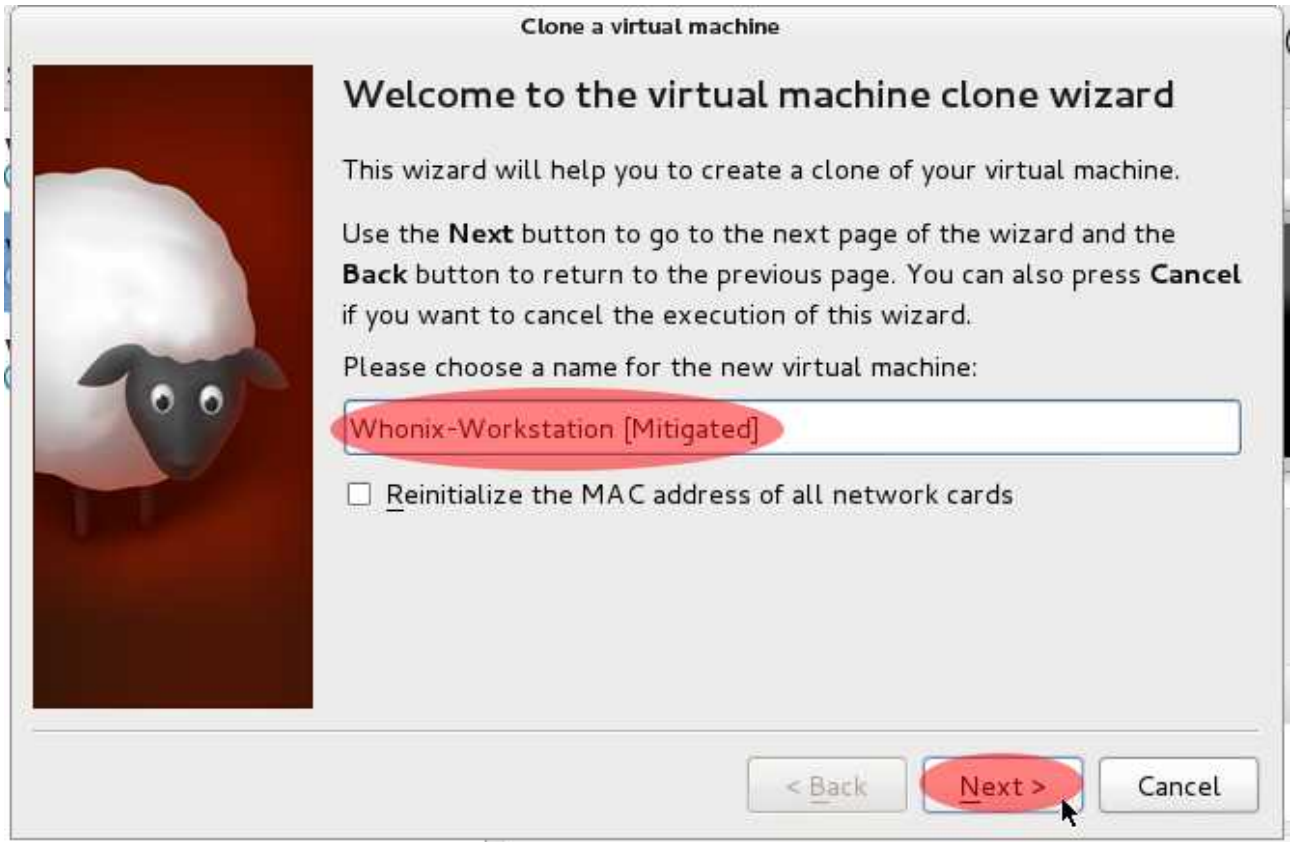
52. When the next window appears, select “Current machine state” and then click the “Clone” button.



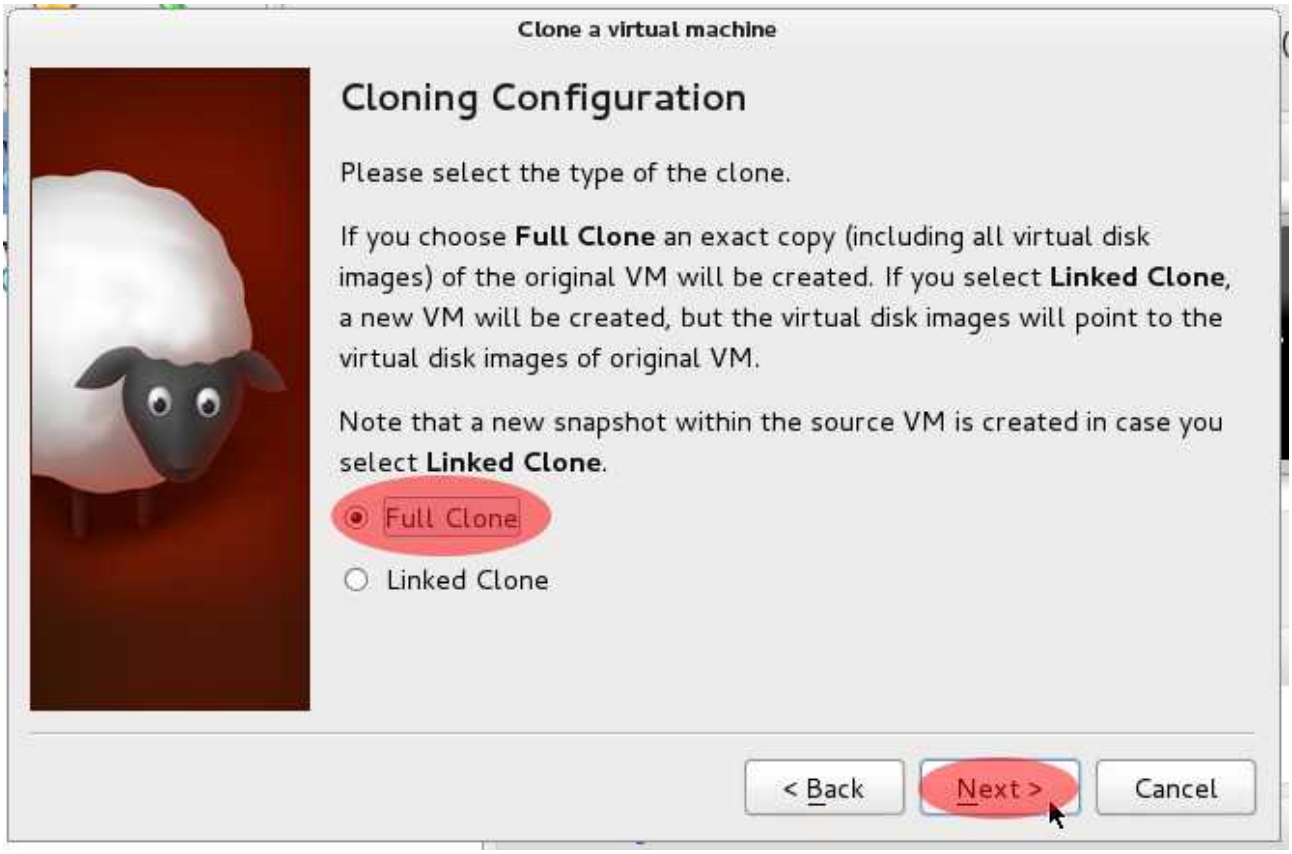
53. When you are returned to the VirtualBox Manager, click on “Whonix Workstation” to select it. Then, click “Machine → Clone.”



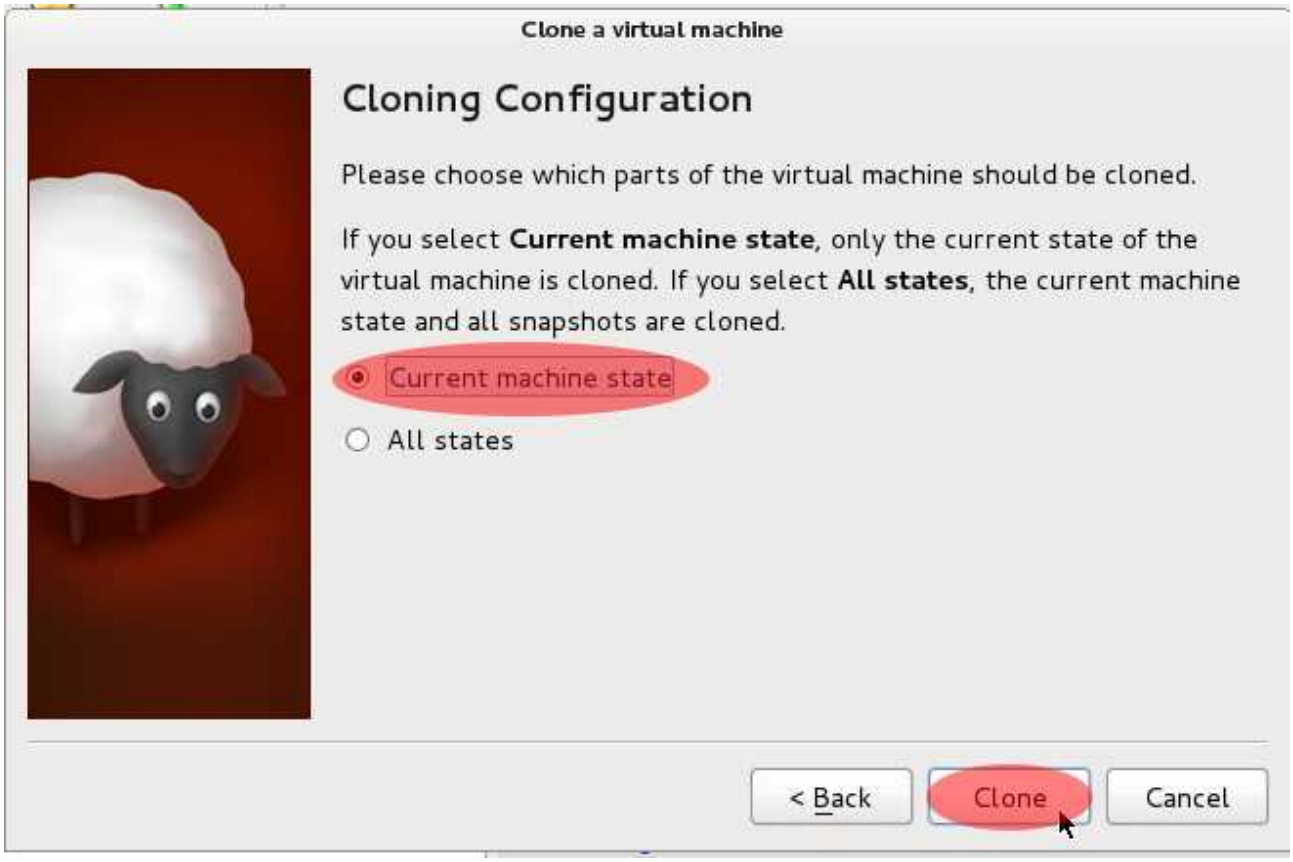
54. In the window that appears, type “Whonix-Workstation [Mitigated]” for the name of the new virtual machine. Then, click on the “Next” button.



55. In the next screen, select “Full Clone” and click the “Next” button.

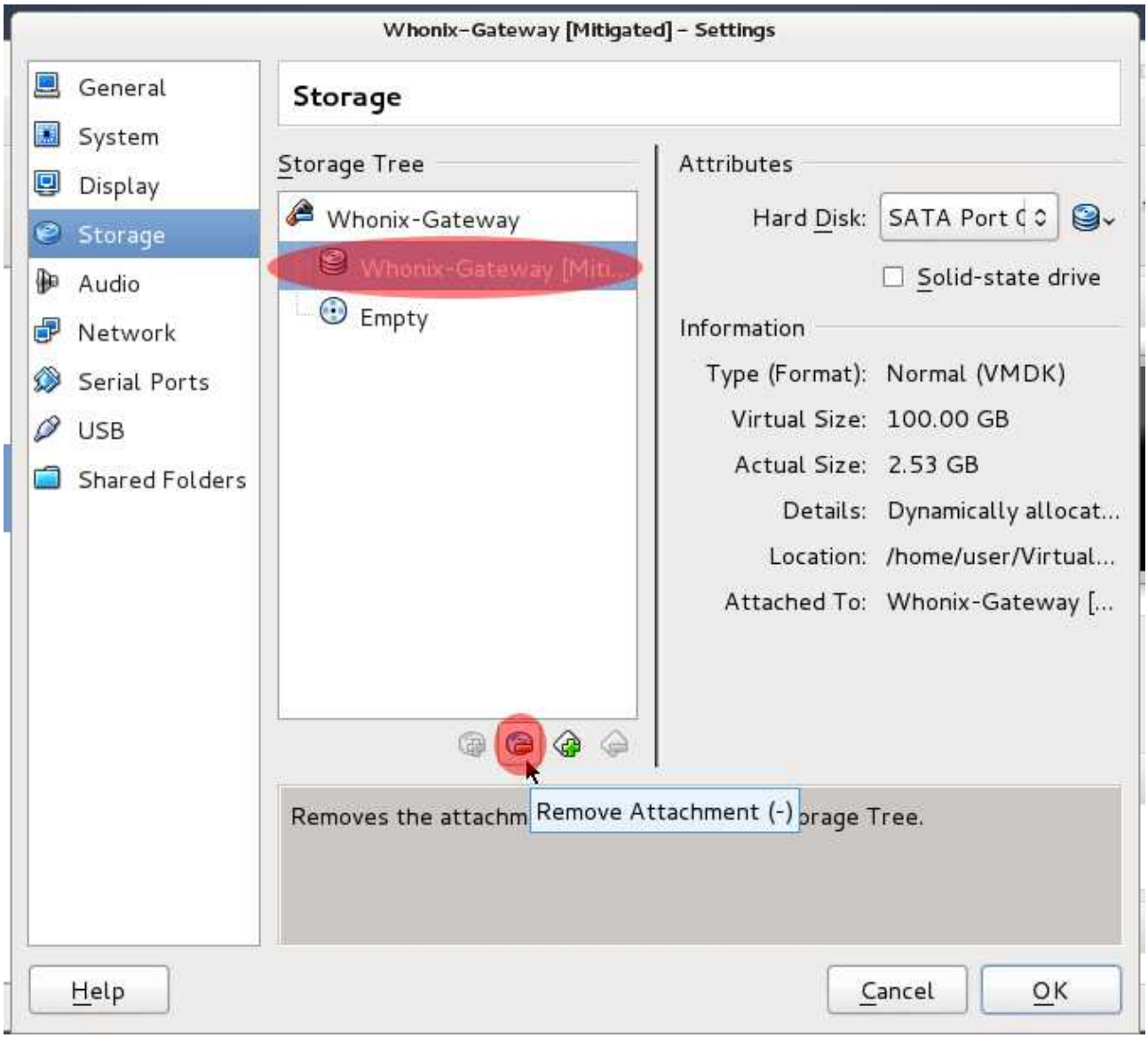


56. When the next window appears, select “Current machine state” and then click the “Clone” button.

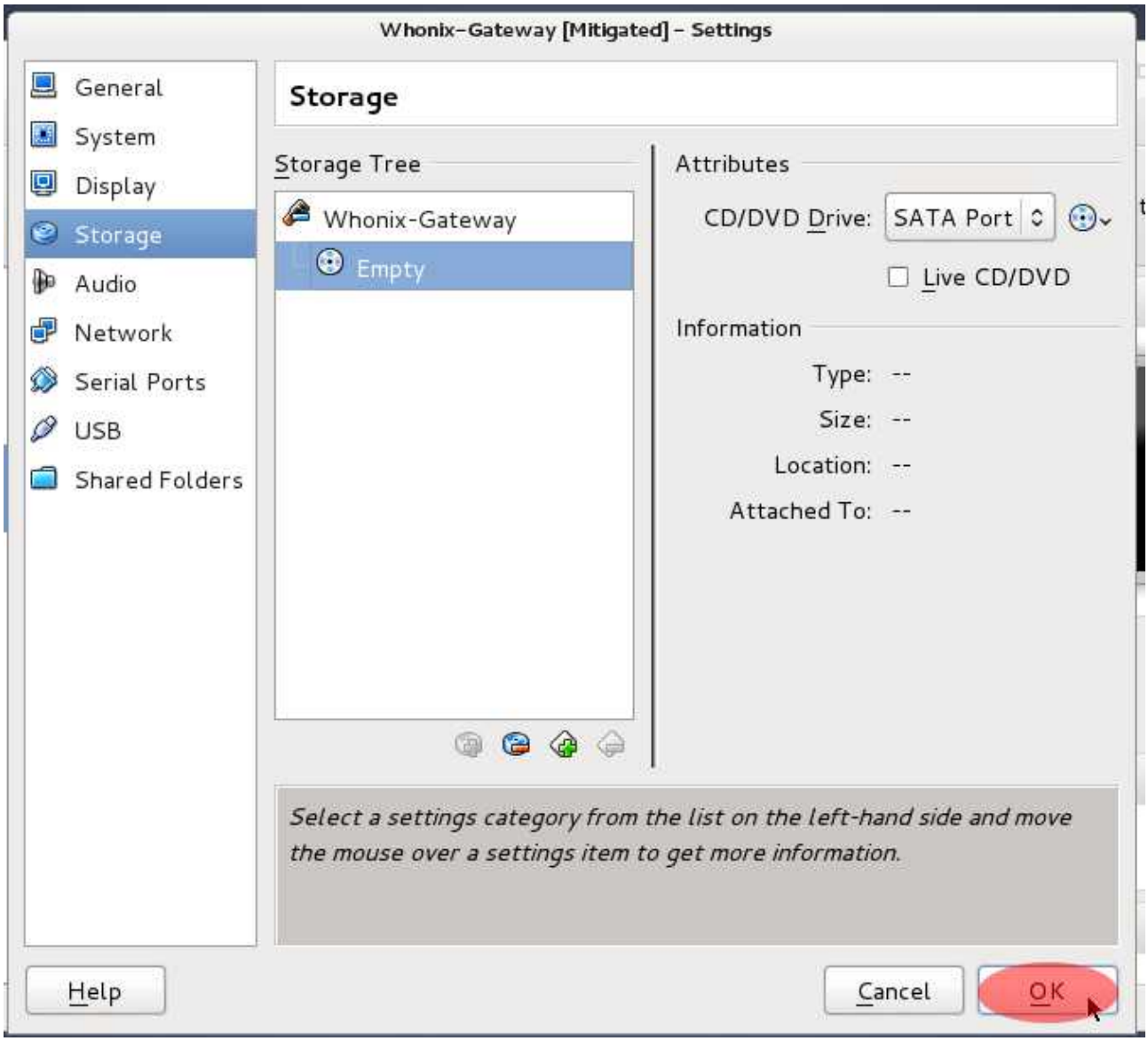


57. Next, you have to temporarily remove some drives from your Whonix virtual machines in order to change the state of those drives. When returned to the VirtualBox Manager, click on “Whonix Gateway [Mitigated]” and then click on “Settings.”

58. Next, click on “Storage.” Then, click on the disk entitled “Whonix-Gateway [Mitigated]-disk1” and click on the icon of the disks with the “-” symbol on it towards the bottom of your screen to remove the disk.

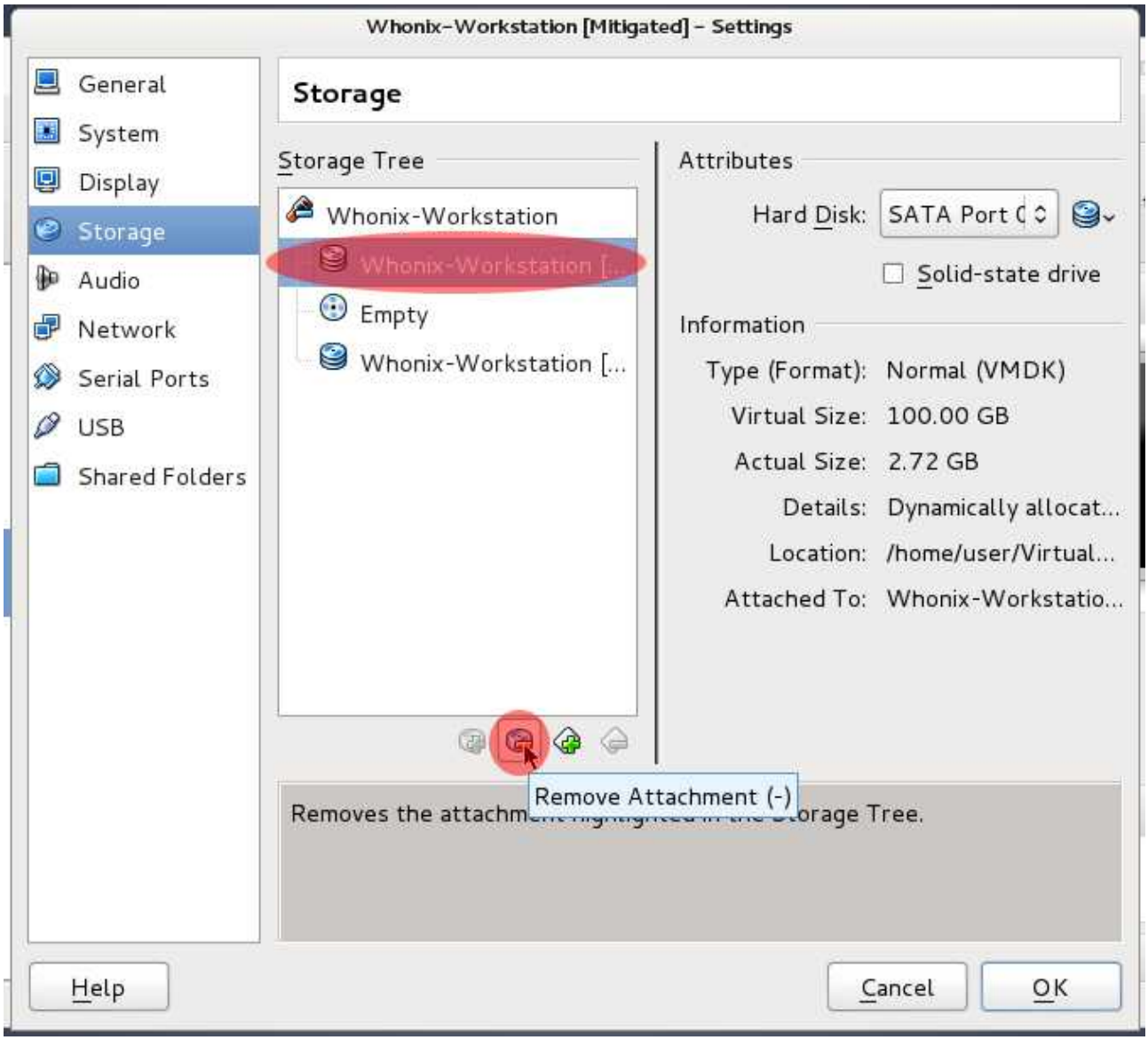


59. Once you have removed the disk, click the “OK” button.

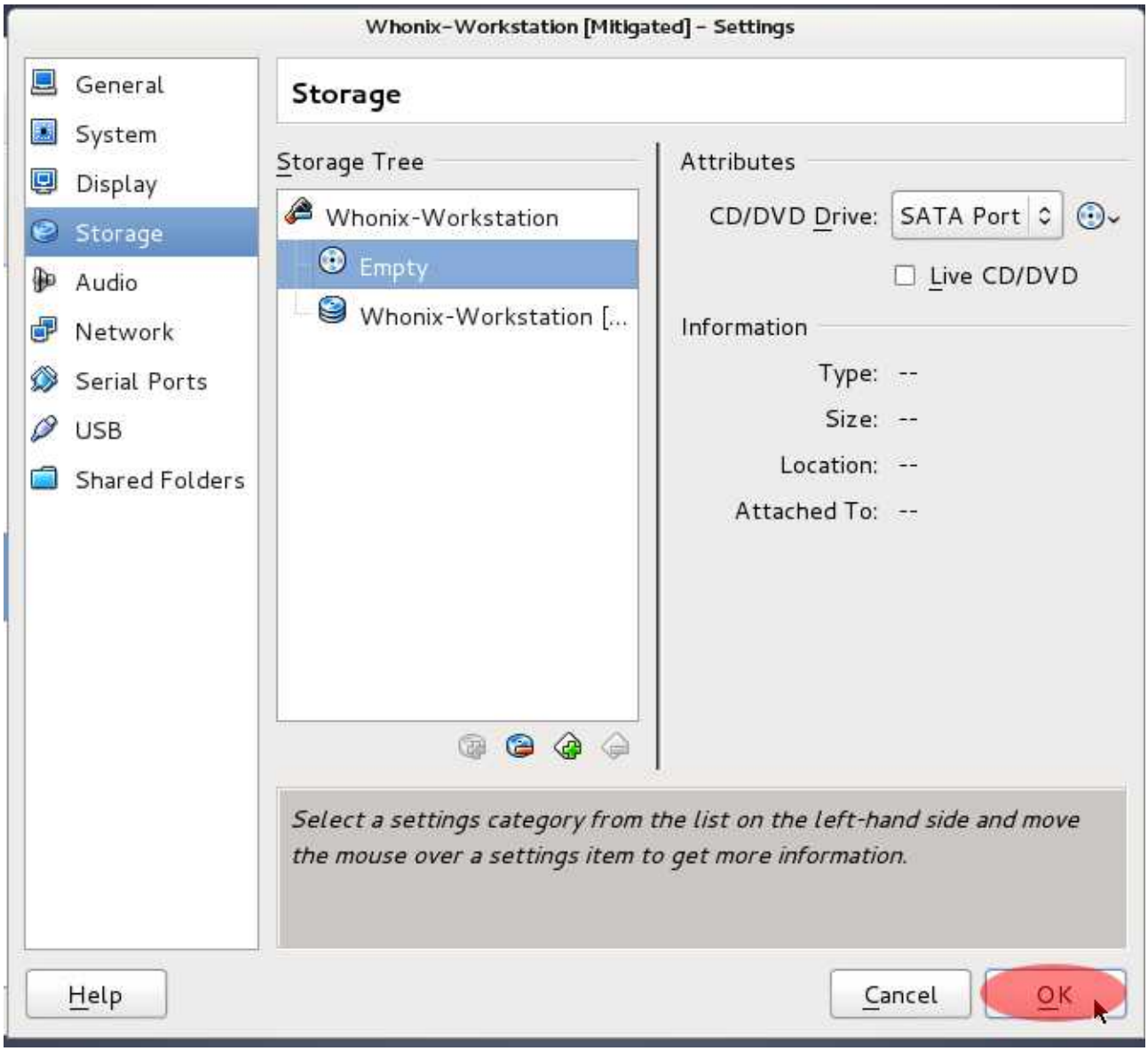


60. When you are returned to the VirtualBox Manager, click on “Whonix-Workstation [Mitigated]” to select it and then click “Settings.”

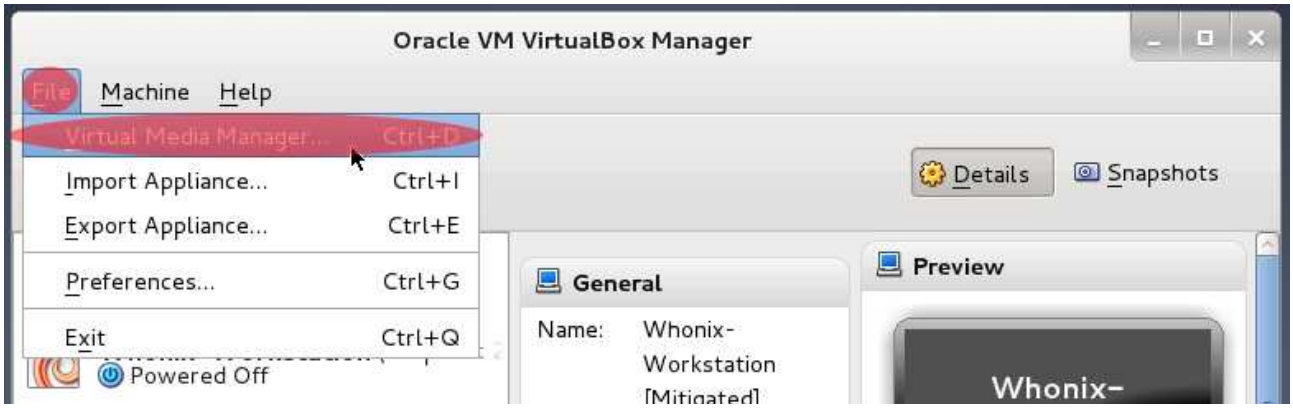
61. Next, click on “Storage.” Then, click on the disk entitled “Whonix-Workstation [Mitigated]-disk1,” which will be the disk closer to the top in the series of disks, and click on the icon of the disks with the “-” symbol on it towards the bottom of your screen to remove the disk.



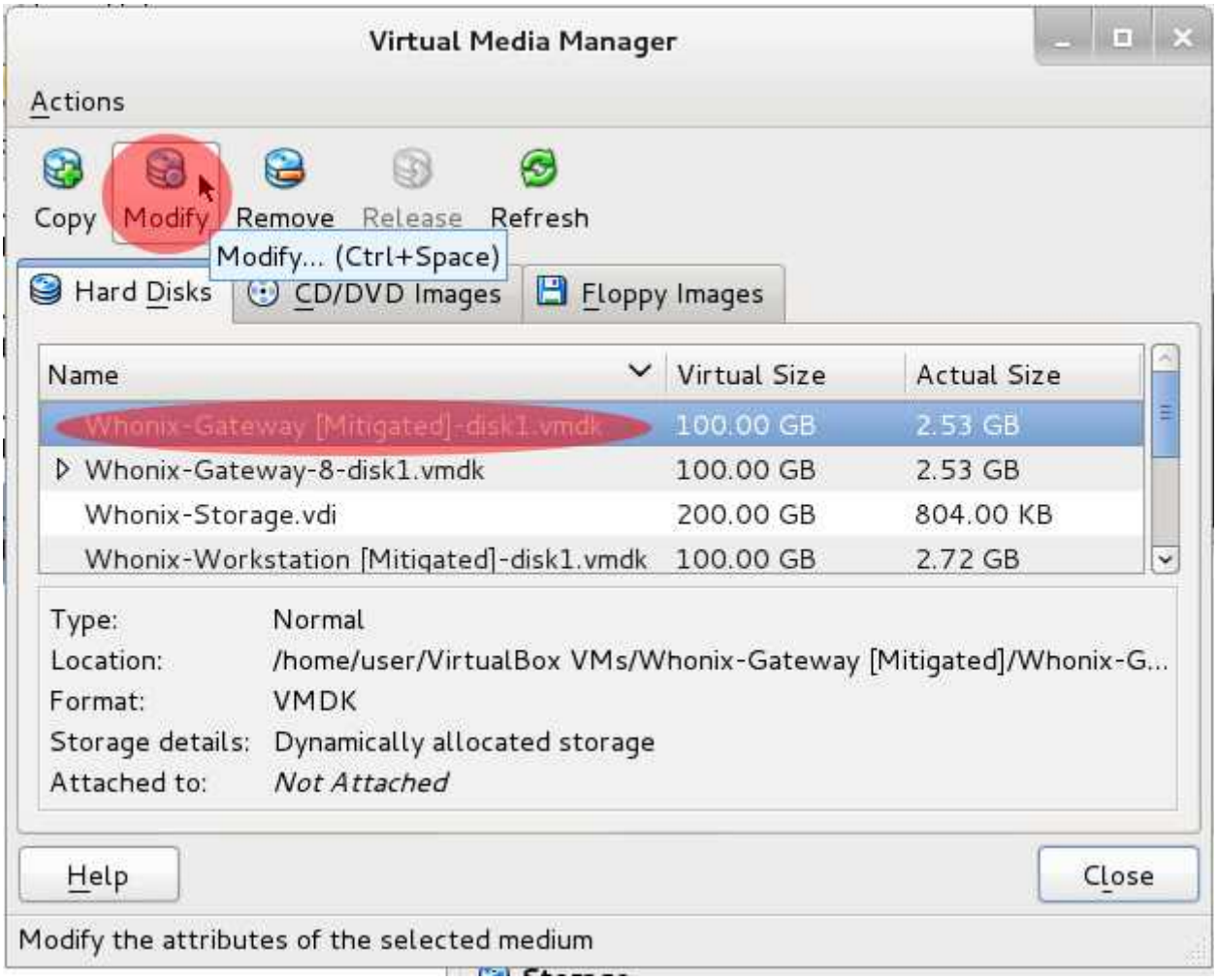
62. When you have removed the disk, click on the “OK” button.



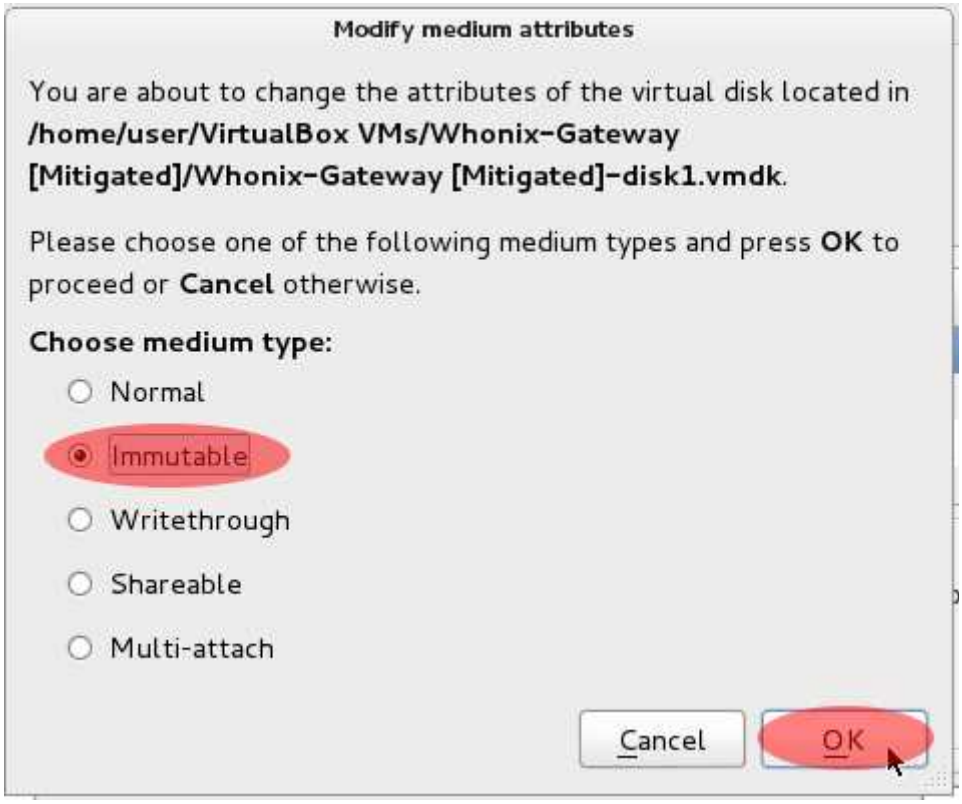
63. When you are returned to the VirtualBox Manager, click on “File → Virtual Media Manager.”



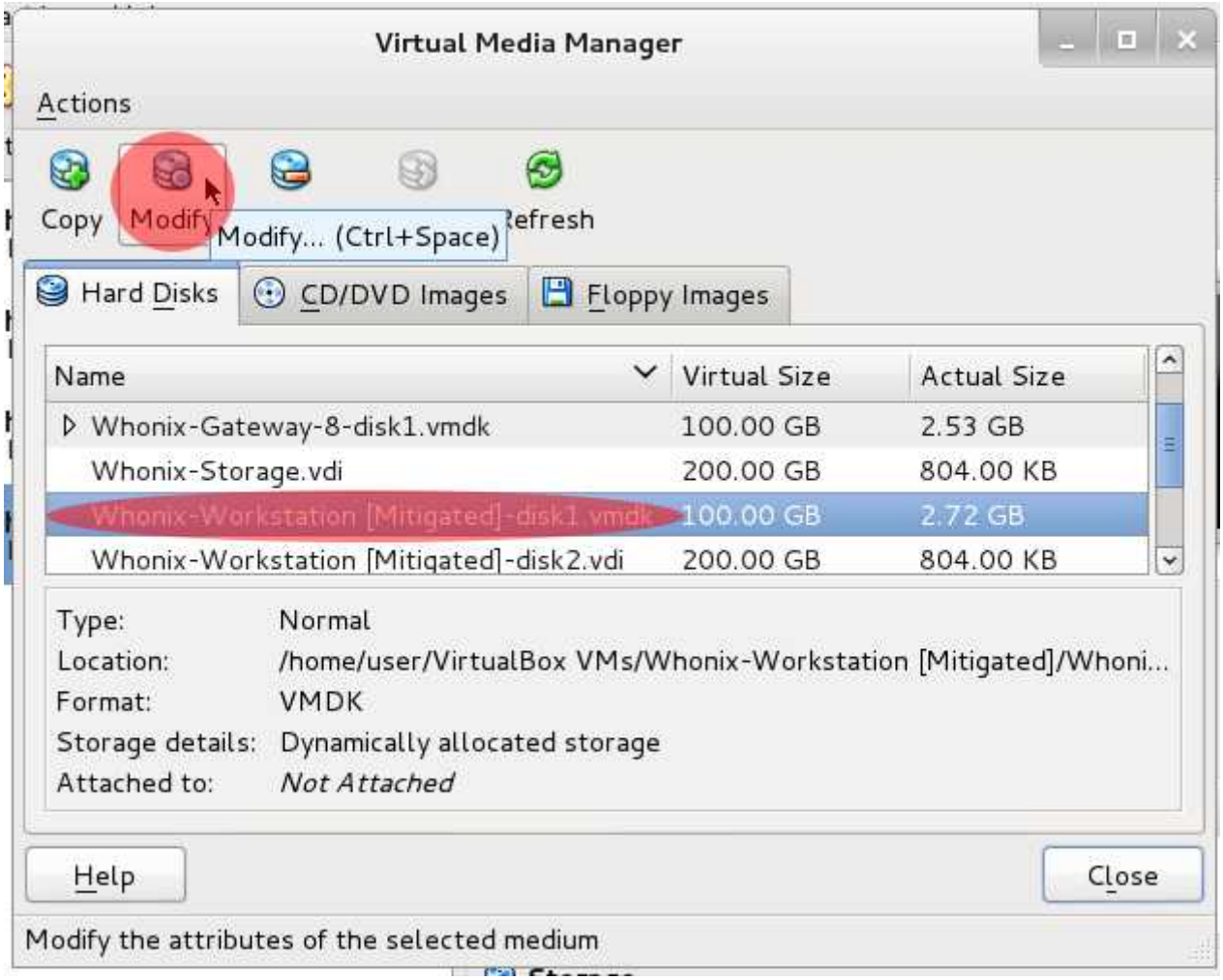
64. In the next window that appears, click on “Whonix-Gateway [Mitigated]-disk1.vmdk” and click the “Modify” button.



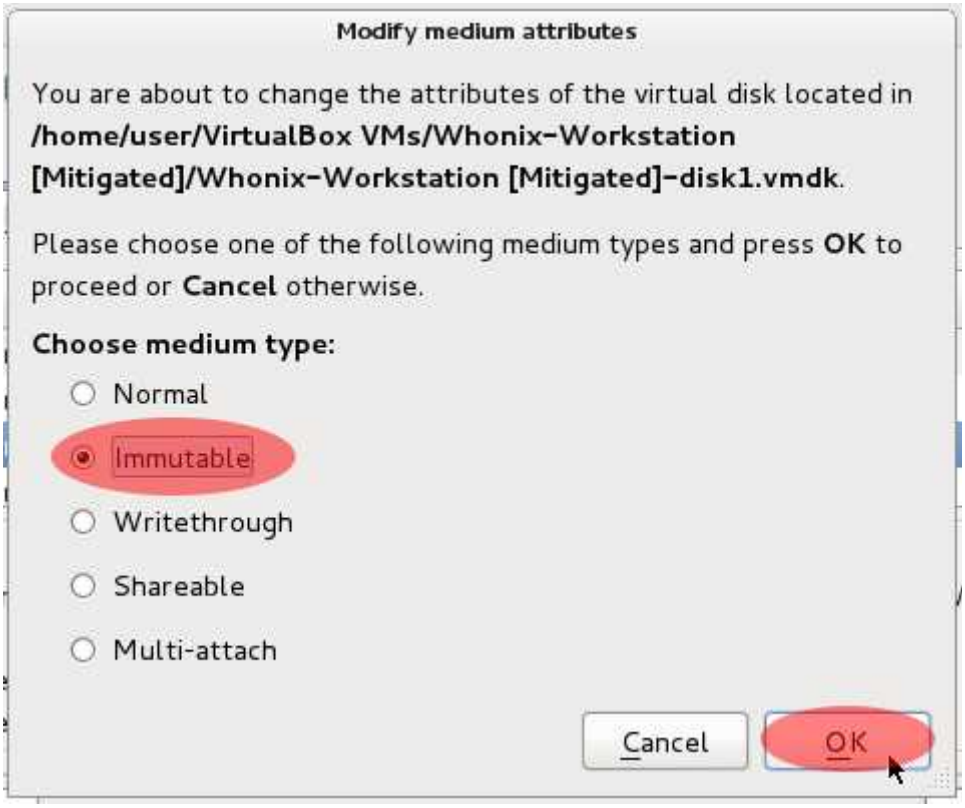
65. On the next screen, select “Immutable” and click the “OK” button.



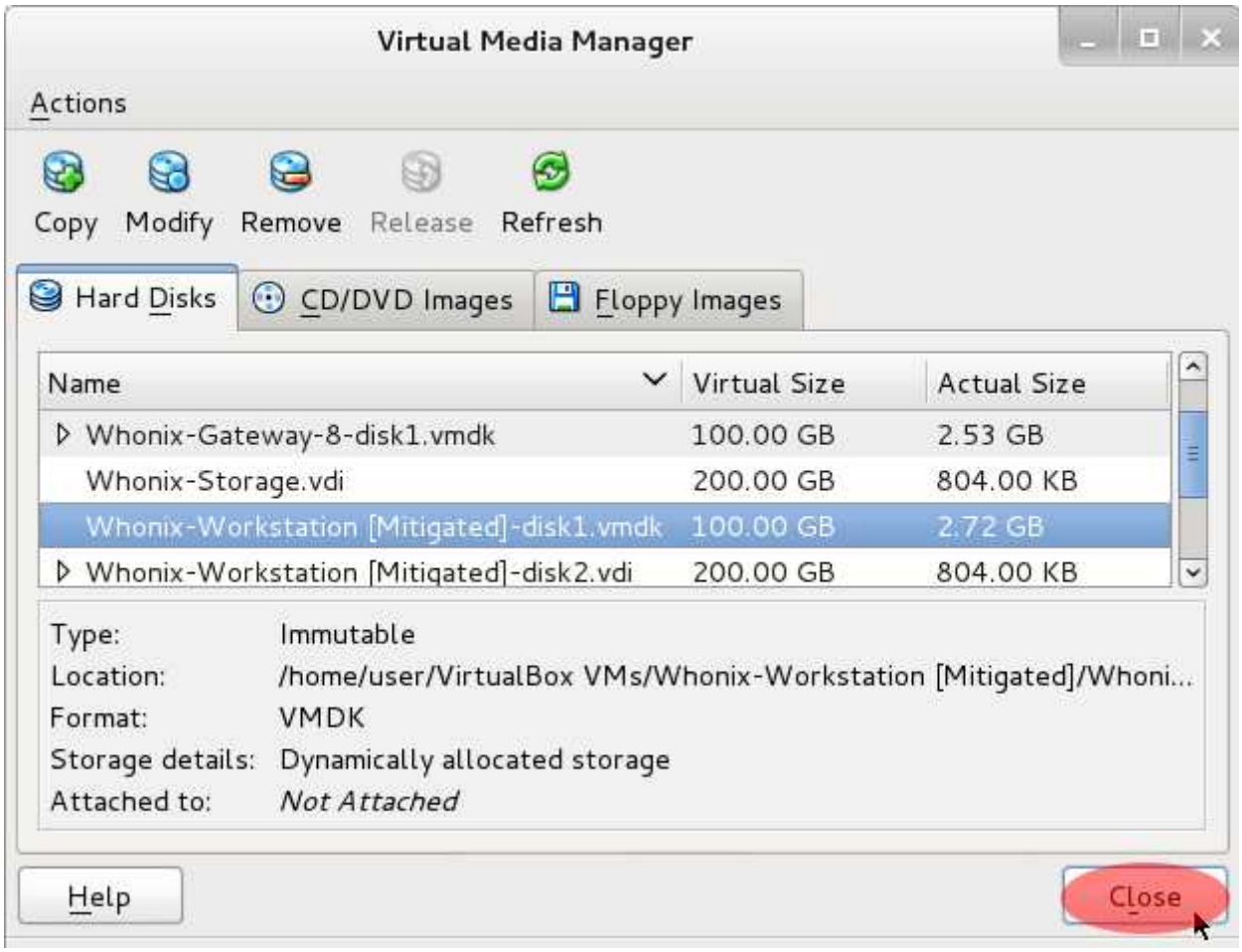
66. When you are returned to the Virtual Media Manager, click on "Whonix-Workstation [Mitigated]-disk1.vmdk" and then click the "Modify" button.



67. In the next window that appears, select “Immutable” and click the “OK” button.

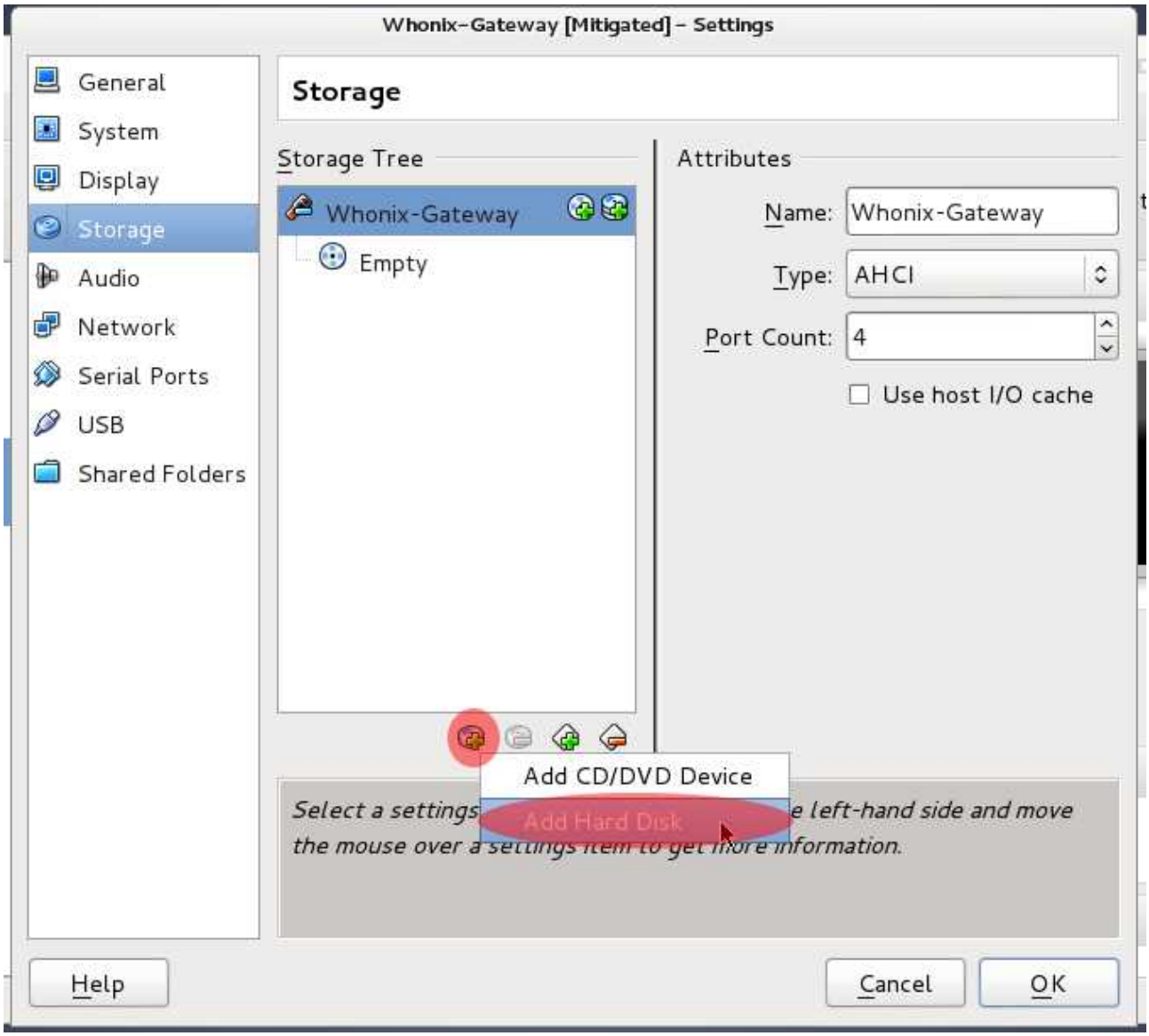


68. When you are returned to the Virtual Media Manager, click the “Close” button.

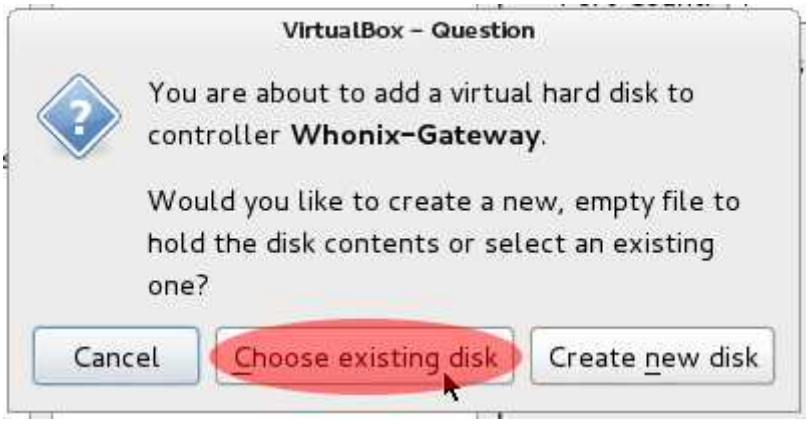


69. Now you need to reattach the disks to the Whonix virtual machines. When you are returned to the VirtualBox Manager, click on “Whonix Gateway [Mitigated]” and then click on “Settings.”

70. In the window that appears, click on “Storage” on the left side of the window. Then, click the small icon that looks like a circular disk with a “+” sign on it towards the bottom of the window and select “Add Hard Disk.”

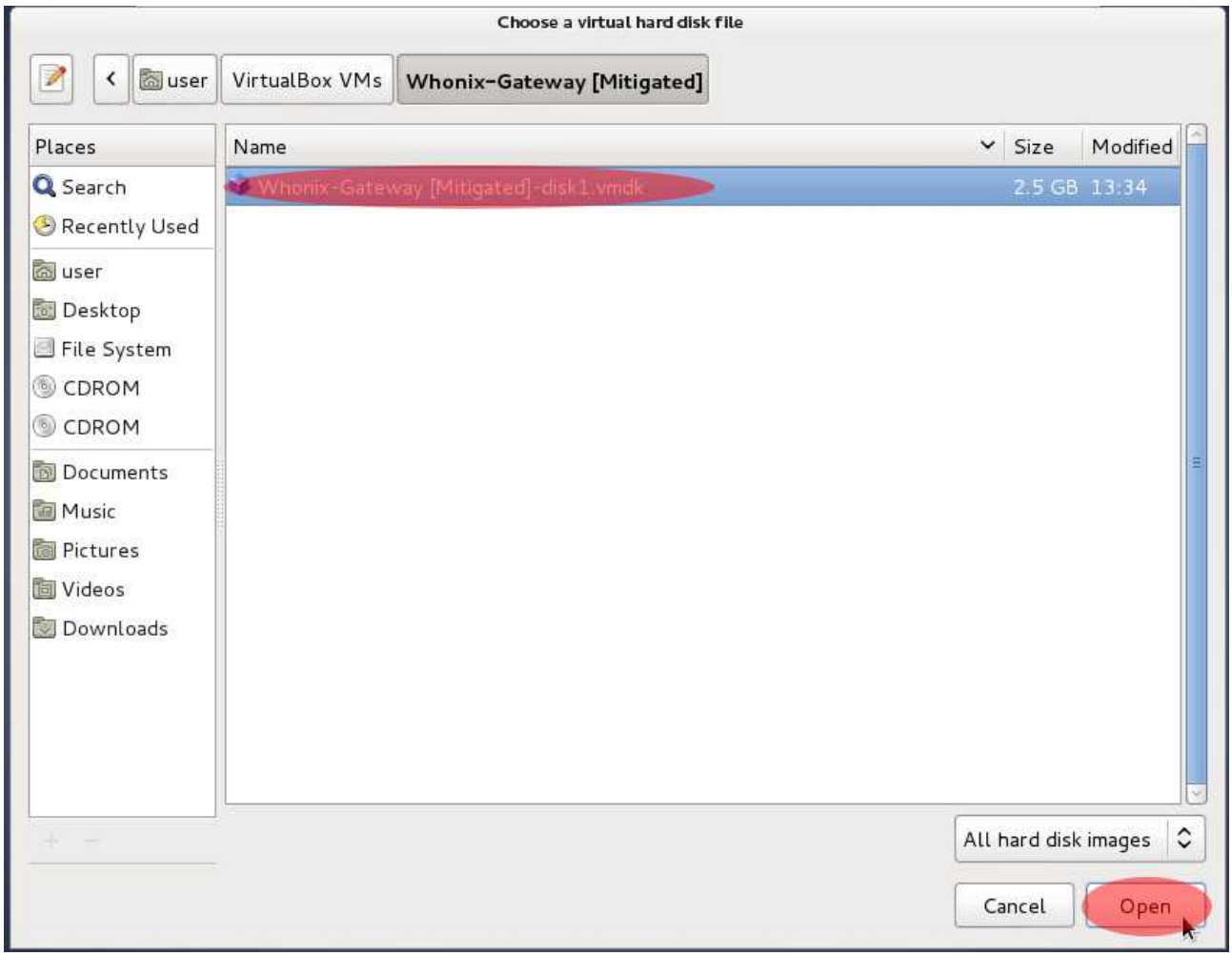


71. On the next screen, click on the “Choose existing disk” button.

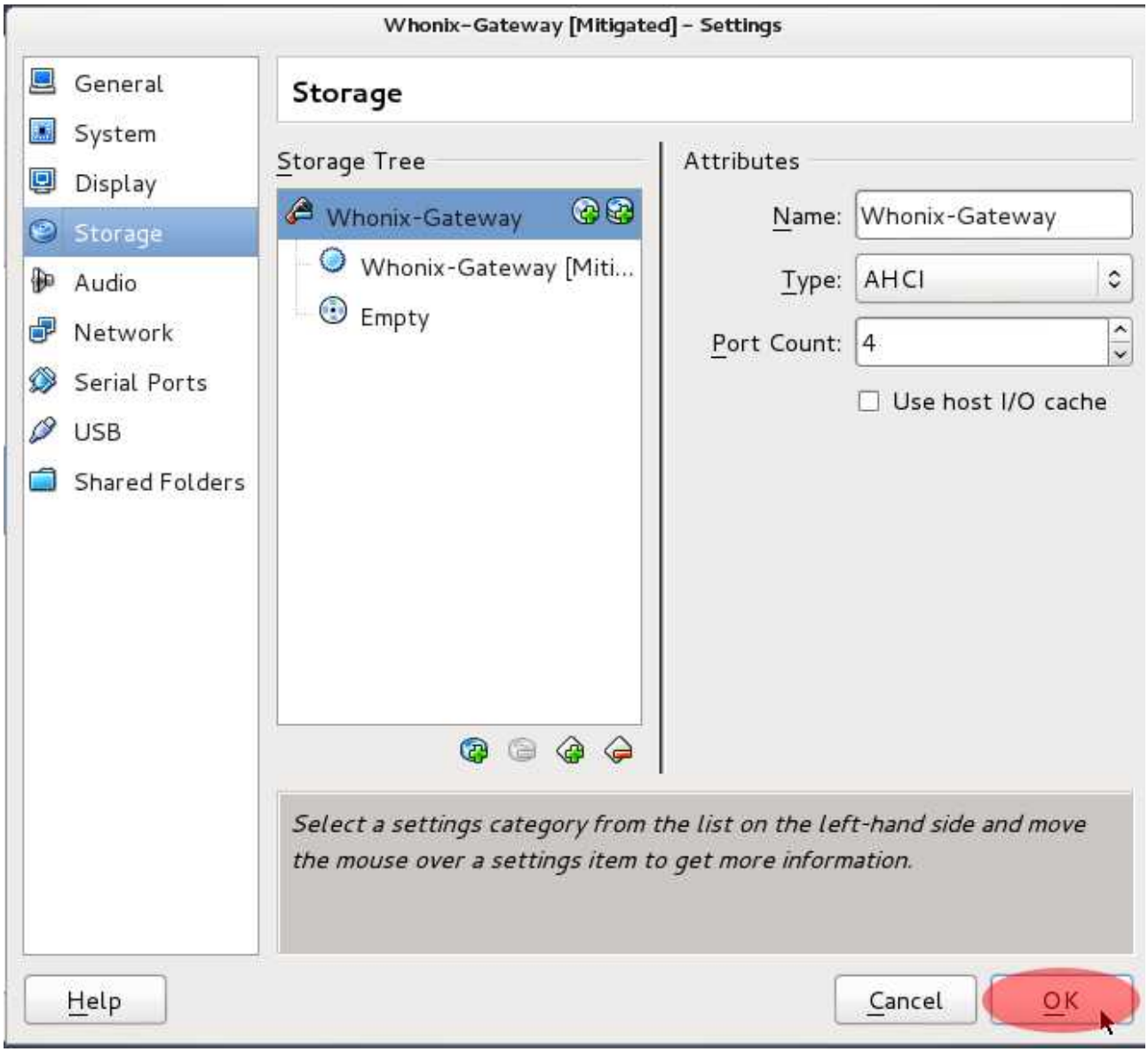


72. Next, select “Whonix-Gateway [Mitigated]-disk1.vmdk” and click on the “Open” button.

    Note: This file is located in “/home/user/Virtual Box VMs/Whonix-Gateway [Mitigated].” It should come up by default in this step. But if it does not, click on “user” in the left hand column of the window. Then, click on the “Virtual Box VMs” folder. Then, click on the “Whonix-Gateway [Mitigated]” folder. You will find the file you need to open in that location.

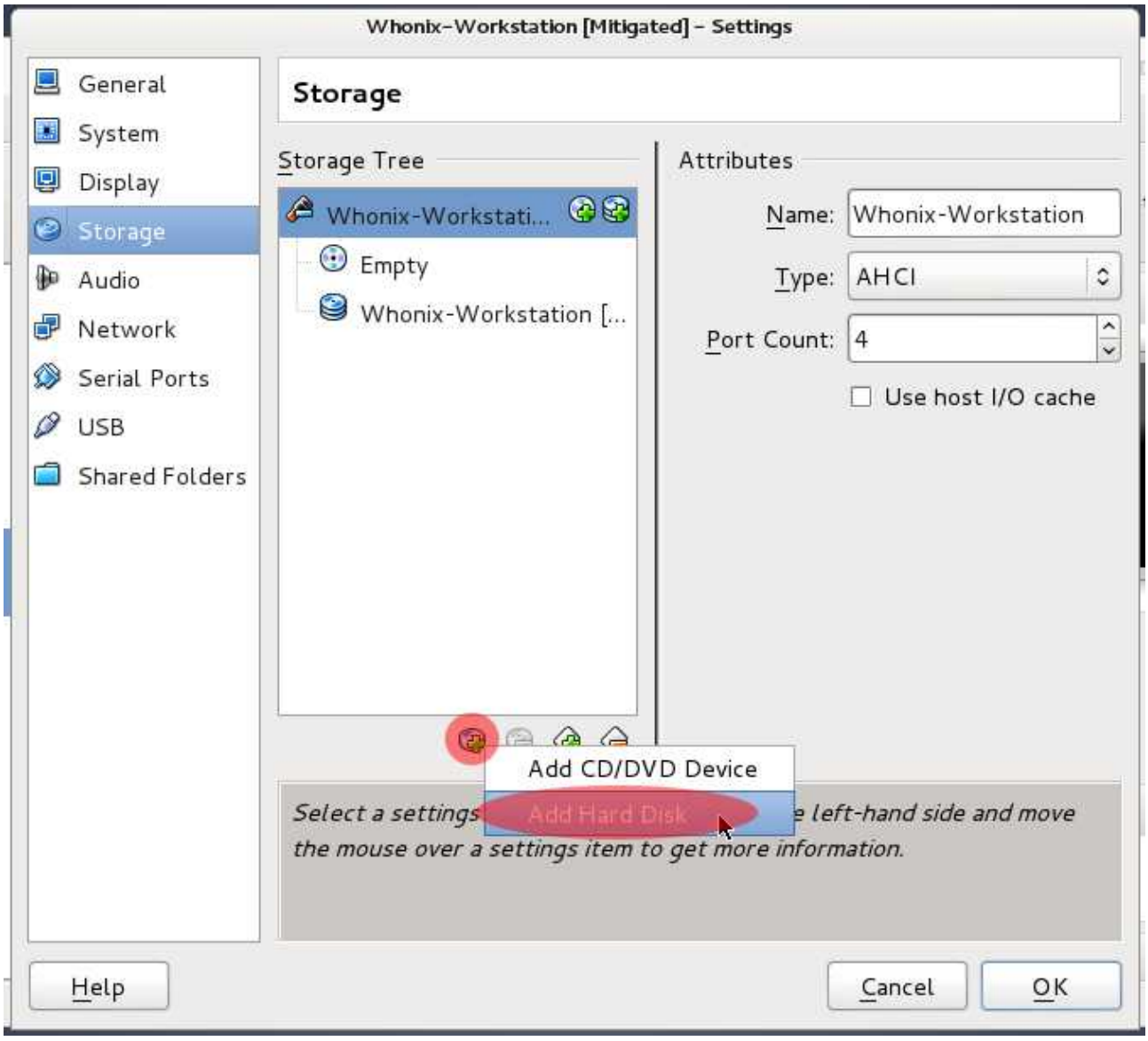


73. When returned to the “Settings” screen, click the “OK” button.

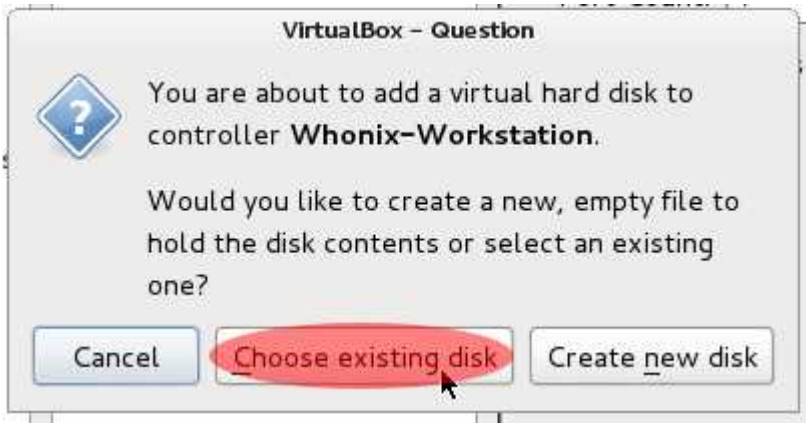


74. When you are returned to the VirtualBox Manager, click on “Whonix-Workstation [Mitigated]” to select it and click on the “Settings” button.

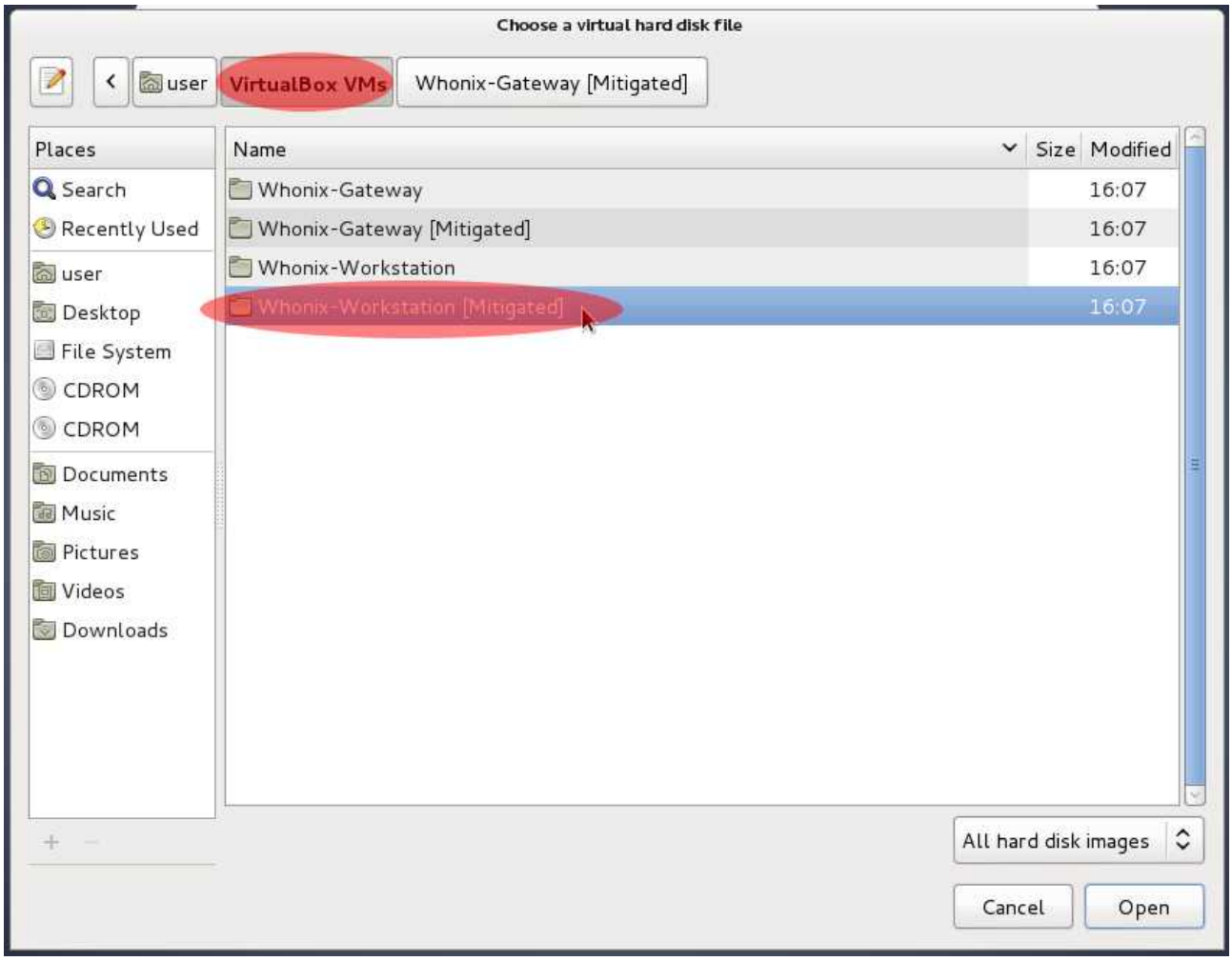
75. In the window that appears, click on “Storage” on the left side of the window. Then, click the small icon that looks like a circular disk with a “+” sign on it towards the bottom of the window and select “Add Hard Disk.”



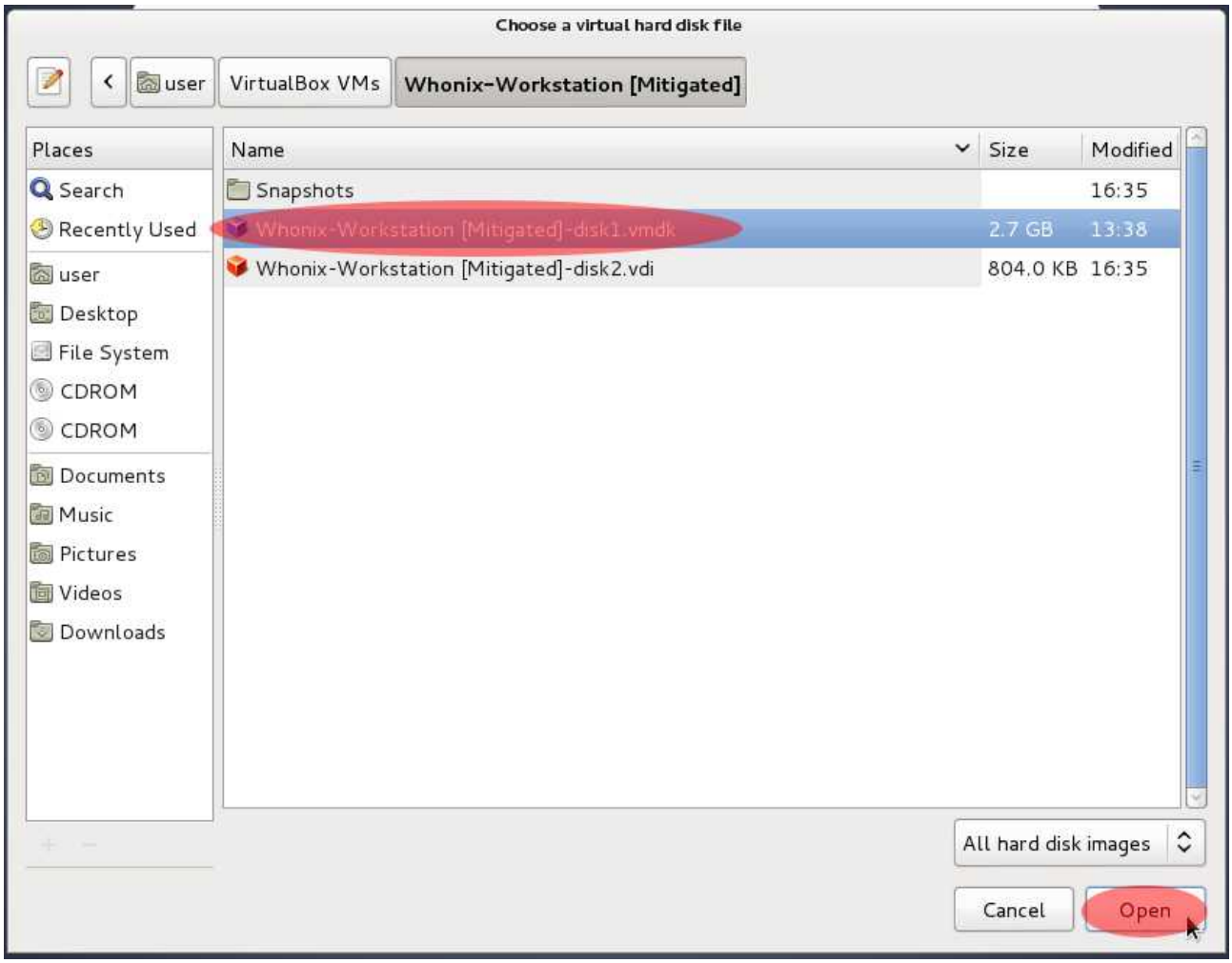
76. On the next screen, click on the “Choose existing disk” button.



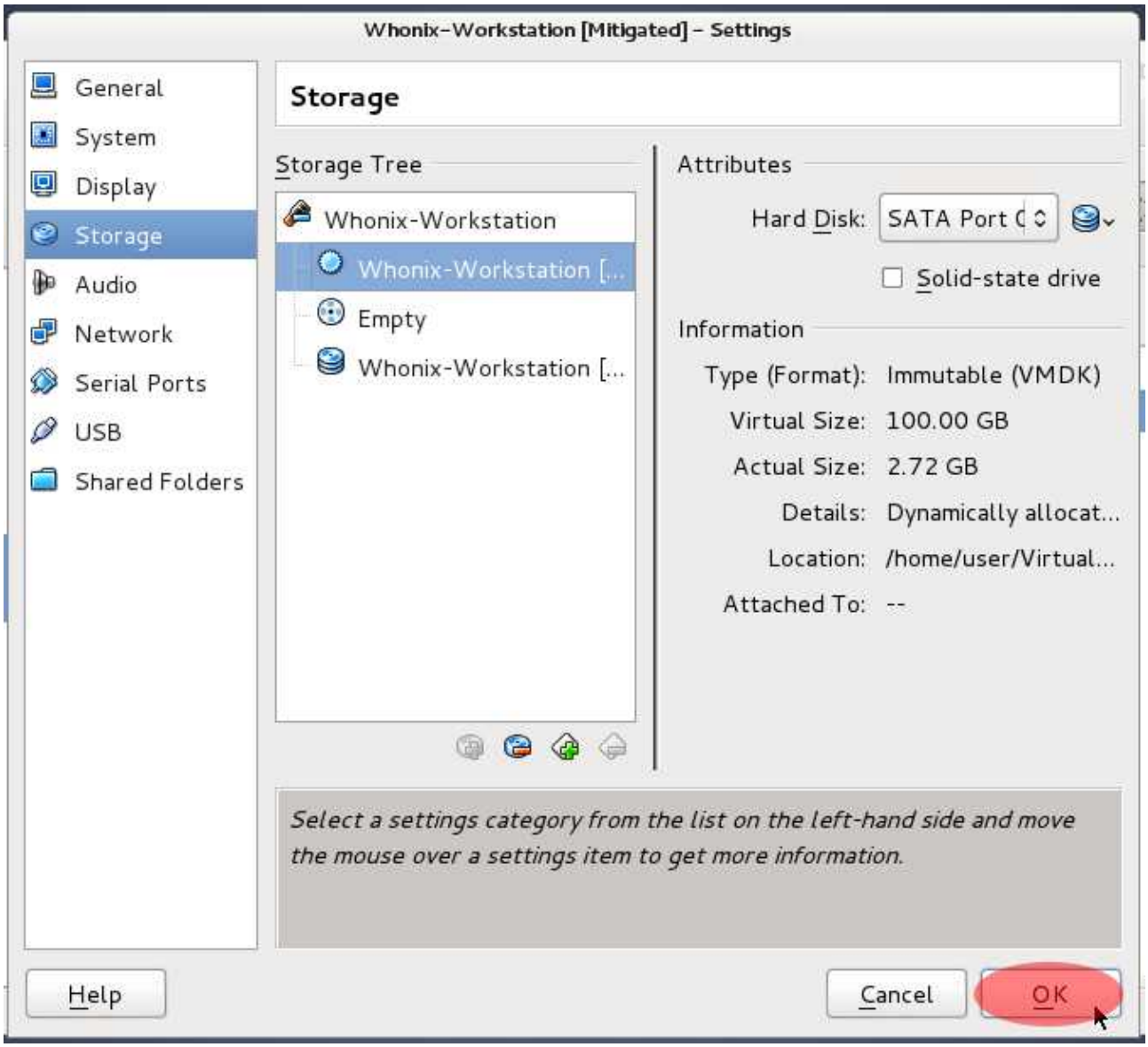
77. In the next window that appears, you will need to navigate to a new location. Click on the “Virtual Box VMs” folder button towards the top of the window. Then, double click on the “Whonix-Workstation [Mitigated]” folder to open the folder.



78. Next, select “Whonix-Workstation [Mitigated]-disk1.vmdk” and click the “Open” button.



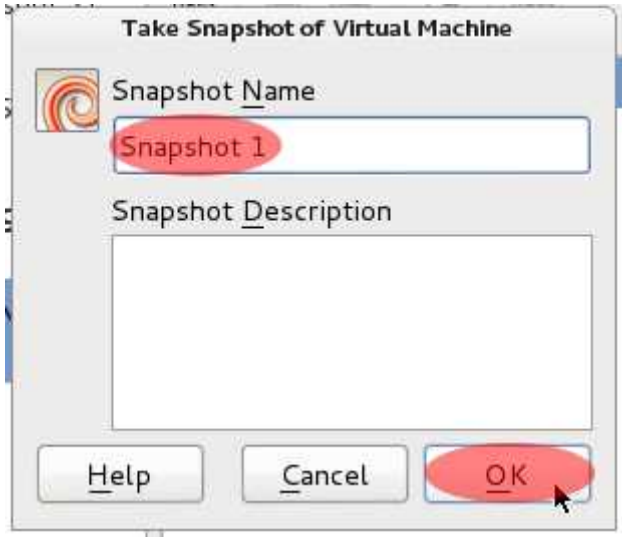
79. When you are returned to the “settings” window, click the “OK” button.



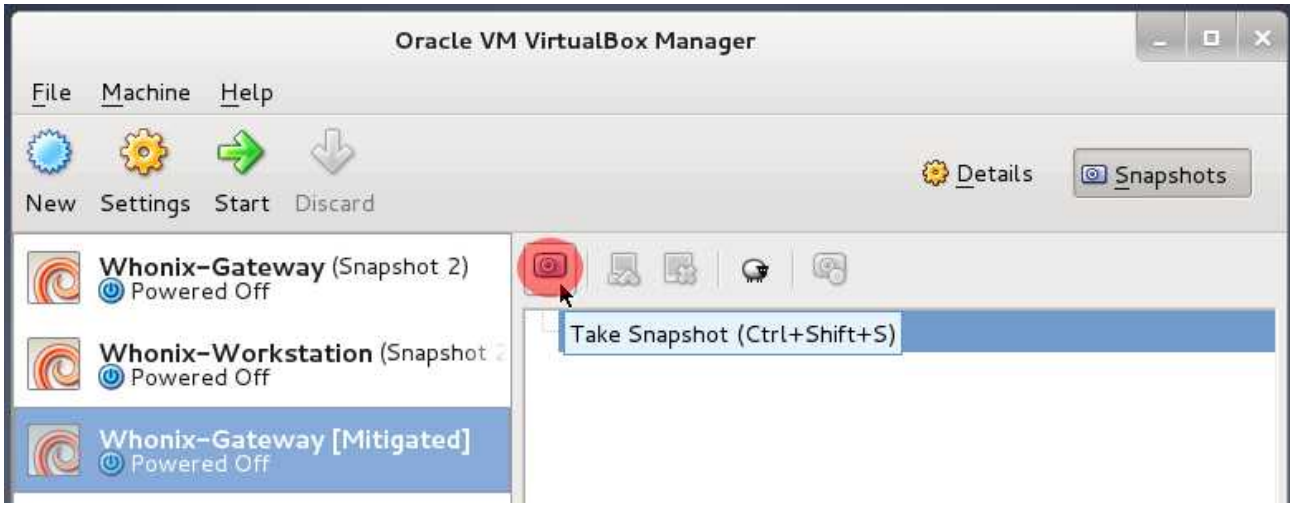
80. When you are returned to the VirtualBox Manager, select “Whonix-Workstation [Mitigated]” and click “Snapshots.”

81. Click on the camera icon towards the upper center of the screen to take a snapshot of the “Whonix-Workstation [Mitigated]” virtual machine.

82. On the next screen, choose the name you want for your snapshot and then click the “OK” button.



83. Next, click on “Whonix-Gateway [Mitigated]” in the VirtualBox Manager and click on the camera icon towards the upper center of the screen to take a snapshot of the “Whonix-Gateway [Mitigated]” virtual machine.



84. On the next screen, choose the name you want for your snapshot and then click the “OK” button.

Congratulations! You have reached the end of the steps necessary to configure the “Malware Mitigation” system. The next page will provide explanation on how it works and how you should use it in the future.

IMPORTANT! DO NOT SKIP THIS PAGE!

Now that you have the malware mitigation system installed, here is an explanation of how it works. When you changed the two Whonix virtual disks to "immutable," this makes it so they will be erased and restored from the most recent snapshot connected to the virtual machine on every boot. Thus, every time you start "Whonix-Gateway [Mitigated]" and "Whonix-Workstation [Mitigated]," anything that was written to the immutable disks will be erased unless you specifically chose to take snapshots. The benefit of this is that, if you obtained malware during any regular use of the virtual machines, unless it was advanced enough to break out of the virtual machines and infect your Host OS, it will be gone the next time you use the Whonix "Mitigated" virtual machines.

With that in mind, **there is something that is incredibly important for you to understand. Any documents you create, or files you download to the system will be erased on the next boot unless you save them in your "/home/user/storage" directory.** The "storage" directory that you created earlier is connected to a disk that you configured as a "writethrough" device. This means that it is not affected by snapshots and, thus, will not be erased on reboots. All of the programs that you configured in the earlier subchapters of Chapter 4 have been moved to this directory. Therefore, when you add new servers to XChat, download new e-mail, add other people's public encryption keys, add new accounts and passwords to KeePassX, etc., they will not be erased on next boot. Therefore, for anything else that you work on which you do not want to be erased on the next boot, **you must save them in your "storage" directory.**

There is one more **very important** strategy to using this system. It deals with installing periodic OS updates to your Whonix virtual machines in order to keep them the most current with application updates, security patches, etc. When you do an upgrade to your system by the steps described in steps 61 and 76 of Chapter 3, which is something you should do regularly, **make sure you have not used the virtual machines for anything else during that session.** Start both the "Whonix-Gateway [Mitigated]" and "Whonix-Workstation [Mitigated]" virtual machines. Then, open a terminal in each and run the "**sudo apt-get update && sudo apt-get dist-upgrade**" command. When the upgrade has finished, shut down your machine as usual. Then, **create a new snapshot for both the "Whonix-Gateway [Mitigated]" and "Whonix-Workstation [Mitigated]" virtual machines as you did in steps 76-79 above.** Once you take the snapshots following the shutdown of the virtual machines you updated, the OS updates will stay persistent through the next uses of the virtual machines.

That's all there is to it. As usual keep the following practices in mind to avoid malware infection:

1. Do not EVER use the Host OS for anything but hosting the Whonix virtual machines. This betters your odds of keeping it free of malware. If your Host OS is compromised, none of the protections otherwise afforded to you by Whonix are secure.
2. Do not use javascript in your web browser unless absolutely necessary. If you must use it for some sites, try to minimize the sites that you allow to send you javascript in the session through selective use of the NoScript plugin.
3. Beware of suspicious links sent to you through the IRC, your instant messenger, e-mail lists or anywhere else.
4. Be wary of attachments sent to you in e-mail, especially if you did not ask for them.

Chapter 5. Supporting the Projects that Made this Tutorial Possible.

Those of us who wrote this guide are merely users who took the time to document a means of effectively using a number of tools. If it were not for the teams that actually developed these tools, then this system would not be possible. If you have any funds or bitcoins that you can spare for any of the projects listed below, please donate what you can. It greatly helps the continued development of advanced tools to help protect our anonymity and privacy. Obviously, if you wish to maintain your anonymity, be cautious in how you go about giving donations.

The Debian Project: The Debian Project is composed of many volunteers throughout the world who have been active in creating and developing the Debian Operating System. Debian is the Operating System used as both the base host Operating System in this guide, in addition to being the Operating System which drives Whonix. The Debian Project established a non-profit corporation in order to accept donations. For more information on donating to the Debian Project, go to **https://www.debian.org/donations**.

The Tor Project: The Tor Project is the team that picked up and continued the development of Tor. Tor is the software used throughout this tutorial to protect your anonymity by encrypting your networking connections and layering them over multiple proxies. The Tor Project is a non-profit corporation that relies heavily on grants and donations for funding. For more information on donating to the Tor Project, go to **https://www.torproject.org/donate**.

The Whonix Team: The Whonix Team is a small group of volunteers that have put all the work into the development and distribution of Whonix. Whonix is the Operating System relied upon in this tutorial to ensure that all of your networking activity is initially sent through the Tor Network. The only full time developer for Whonix is Patrick Schleizer. If you would like to donate to the Whonix Project, please go to **https://www.whonix.org/wiki/Donate**.

Cyberguerrilla.org: Cyberguerrilla.org is a number of servers and services run by Anonymous for everyone. Cyberguerrilla.org hosts the IRC server used in this tutorial, hosts a Wiki for this guide at no cost, while also offering a number of other online services to the community at large for free. If you are interested in donating to Cyberguerrilla.org to keep the services running, go to **https://cyberguerrilla.info/donation** or **http://lu4qfnnkbnduxurt.onion/donation**.

Off-the-Record Messaging (OTR): OTR is the primary tool used in this tutorial to ensure that, even if your networking connections are subjected to surveillance somewhere within an instant messaging network, the content of your instant messaging discussions still remain private. For more information on donating to OTR, go to **https://otr.cypherpunks.ca/donate.php**.

G10 Code (GPG): GPG is the main tool used to encrypt and decrypt emails as described in this tutorial. The current source of funding is a German corporation known as G10 Code. To learn more about donating the the continued development of GPG, go to **http://g10code.com/gnupg-donation.html**.

CalyxInstitute.org: The Calyx Institute is the service providing the instant messenger services detailed in this guide. Their approach is unique in that they offer access on a Tor Hidden Service and require OTR encryption for messages to go across their network. For more information on donating to the Calyx Institute, go to **https://www.calyxinstitute.org/support-us/donate-by-mail**.

Conclusion

First and foremost, congratulations if you made it to this page. That likely means you read this whole tutorial unless you are the kind of person that reads the last page of a book first. The topics covered by this tutorial are fairly advanced for many users. Getting through this entire tutorial shows that you are curious about what exists and have the patience to learn about it.

On that note, here is our final advice. With this system, your worst enemy will be yourself. Do not ever expose any real information about yourself. Based on how you use this system, despite all the efforts you make, you will still create fingerprints that may correlate to your true identity. Never voluntarily divulge any information that may identify you. Or, if you feel that is necessary, pad it with a lot of false information. How well you use this system is up to you. But, this system cannot protect you from giving up social information that may identify you. Play it smart. Play it safe. Don't "own yourself."

Additionally, **to emphasize this point again, read the documentation provided by the Whonix Team to learn how to use this system to its maximum potential at the following links:**

- https://www.whonix.org/wiki/Documentation [Whonix Documentation]
- https://www.whonix.org/wiki/Security_Guide [Whonix Security Guide]
- https://www.whonix.org/wiki/Warning [Warnings Guide & Behavior to Avoid]
- https://www.whonix.org/forum [Community for Whonix Troubleshooting/Talk]

Finally, if you wish to share this guide, please use the official distribution links. This will guarantee that people will get the most current version of the guide. Currently, the official distribution links for this guide are https://anonguide.cyberguerrilla.org or http://yuxv6qujajqvmypv.onion**.**

Thank you for taking the time to read this tutorial. We hope it was useful to you. Please send any comments, suggestions or corrections you may have to **anonguide@bitmessage.ch,** GPG Key = 0xBD8083C5237F796B, Fingerprint = 6422 2A88 D257 3091 0C47 A904 BD80 83C5 237F 796B.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.