TOR AND THE DARKNET

Remain Anonymous and Evade NSA Spying

JAMES SMITH

Tor and The Dark Net

Remain Anonymous and Evade NSA Spying

James Smith

Contents

Introduction

I want to thank you and congratulate you for downloading the book, “Tor and The Dark Net – Remain Anonymous and Evade NSA Spying”.

Internet privacy is a thing of the past. In todays day and age if you are using a computer or device that is connected to the internet you do not have any privacy. It is an unfortunate, but definite fact. For some this may not matter at all as they don’t care who has access to their files, data, browsing habits, or wherabouts. However, for others this can pose a significant problem. The NSA, the FBI, and even simple sophisticated hackers have the ability to track anything and everything you are doing. The good news is there are methods and tactics you can use to prevent this from happening. Inside this book you will find step by step instructions and techniques that can and will make you completely anonymous on the internet. If used correctly not even the NSA will be able to track you down. Everyones situation and needed security levels can be different so this book breaks down all the different options that are available to you and defines exactly what each one does and how secure it can be so that you can choose what will work for you.

It is my hope that this book is able to inform you of all your options to remain anonymous. Thanks again for downloading your copy!

INTRODUCTION TO TOR, HTTPS, AND SSL

First and foremost, to protect yourself while browsing the internet you should be using Tor which stands for The Onion Router. Tor will provide you with a degree of anonymity by using an 128-bit AES (Advanced Encryption Standard). There has been some debate as to whether or not the NSA can crack this code, and the answer is likely yes. This is why, you should never send anything over Tor that you aren't comfortable sharing with the entire world unless you are using some sort of PGP encryption which we will talk about later.

Communication from your computer, to the internet relies on an entry node which basically "enters your computer" into the Tor network. This entry node communicates with your computer; this entry node knows your IP address. The entry node then passes your encrypted request onto the relay node. The relay node communicates with the entry node and the exit node but does not know your computer's IP address. The exit node, is where your request is decrypted and sent to the internet. The exit node does not know your computer's IP, only the IP of the relay node. Using this model of 3 nodes it makes it harder, but not impossible to correlate your request to your original IP address.

The problem comes obviously when you are entering plain text into TOR because anybody can set up an exit node. The FBI can set up an exit node, the NSA, or any other foreign government, or any malicious person who may want to steal your information. You should not be entering any sensitive data into any websites, especially when accessing them over TOR. If any of the nodes in the chain are compromised, and some likely are, and the people in charge of those compromised nodes have the computing power to decrypt your request, then you better hope it wasn't anything sensitive.

So what can we do to fix this? Well, luckily we are now having more and more servers that are offering something called Hidden services. You can easily recognize these services by the address **.onion** . These services offer what's called end-to-end encryption. What this does is take the power out of the compromised exit nodes and put them back in your hands. The web server of the hidden service now becomes your exit node, which means the website you are visiting is the one decrypting your message, not some random exit node ran by a potential attacker. Remember, the exit node has the key to decrypt your request. The exit node can see what you are sending in clear text once they decrypt it. So if you are entering your name and address into a field, the exit node has your information. If you are putting a credit card, a bank account, your real name, even your login information, then you are compromising your identity.

Another step you can take, is to only visit websites that use something called HTTP Secure. You can tell if the website you are visiting is using HTTP Secure by the prefix at the beginning of the address. If you see **https://** then your website is using HTTP Secure. What this does is encrypts your requests so that only the server can decrypt them, and not somebody eavesdropping on your communication such as a compromised Tor exit node. This is another form of end-to-end encryption. If somebody were to intercept your request

over HTTP Secure, they would see encrypted data and would have to work to decrypt it.

Another reason you want to use HTTPS whenever possible, is that malicious Tor nodes can damage or alter the contents passing through them in an insecure fashion and inject malware into the connection. This is particularly easier when you are sending requests in plain text, but HTTPS reduces this possibility. You must be made aware however, that HTTPS can also be currently cracked depending on the level of the key used to encrypt it. When you visit a website using HTTPS, you are encrypting your request using their public key and they are decrypting it using their private key. This is how cryptography works. A public key is provided to those who want to send an encrypted message and the only one who can decrypt is the one with the private key.

Unfortunately, many websites today are still using private keys that are only 1,024 bits long which in today's world are no longer enough. So you need to make sure you find out which level of encryption the website you are visiting uses, to make sure they are using at a minimum 2,048, if not 4,096 bits. Even doing all of this unfortunately is not enough, because we have another problem. What happens if the web server itself has become compromised? Maybe your TOR nodes are clean, maybe you have used HTTPS for all your requests, but the web server itself of the website you are visiting has been compromised. Well then all your requests are again, as good as plain text.

PGP, TAILS, VIRTUAL BOX

So keep in mind that if you are a user of the Deep Web, or any other form of activism, you never want to enter any identifying details about yourself online. Make it so that even if the NSA intercepted and decrypted, or compromised the website you are accessing that the only information they have against you is your username and password. How safe is that username and password? Does your password contain any identifying information? Is it the same password that you use for your personal email? Does it contain a name of somebody you know personally? Always keep all of these factors in mind.

Another step you must take, especially when communicating with other users on sites in the Deep Web is using PGP encryption. This is not always possible, such as in cases when you are logging into a website, filling out a form, logging into an email, etc.. Consider any type of information you enter into a website using plain text possibly compromised. Never put anything sensitive in any type of plain text format online. PGP comes into play because it uses a very strong method of encryption called cryptography. PGP stands for **Pretty Good Privacy**, and it is used for encrypting, decrypting and signing texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

For the more technical users, it uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography. For the less technical users, the process of encrypting messages using PGP is as follows. You create a private key and a public key. The public key is the key you give out to people you want to send you encrypted messages. Your private key, is kept privately by you. This private key is the only key that can unlock messages that were previously locked with your public key.

If you are still confused, think about it like this. Think about a public key that can go around locking boxes that are intended for you. Anyone can lock a box that is intended for you, but you are the only one with the key to unlock the box. Either if the person who sent you a message locked a box (message) with your public key, they themselves cannot unlock it. Only the person possessing the private key can unlock it. If you wish to respond to this person, you must use their public key to encrypt the message you intend to send to them. And they themselves, use their own private key to decrypt the message you sent them.

If you are still with me, I am glad I haven’t lost you yet. This is called cryptography and was designed so that anybody intercepting your message could not decrypt the message without your private key. Even if you yourself, lose your private key, there is no method of key recovery. You can consider that message locked forever. So how do you use PGP?

Well before we get to that, I want to introduce you to a **Live Operating System**, which makes using PGP encryption and decryption very easy. A live operating system is an operating system that you can run on top of your current operating system. So for example, if you are a Windows user, you have 2 choices. You can download the live operating system, burn it to a CD or DVD and then boot your computer from that DVD or CD. This will make your computer run as if you have this operating system installed on

your computer. However, if you remove the CD or DVD and reboot, then your computer will boot as normal. You can also use a USB drive to perform this same feature.

Secondly, you can run this live operating system in what's called a Virtual Box. The benefits of this are that you can run Windows simultaneously as you run this other operating system and you can easily switch back and forth between them without rebooting the computer. Both methods have their pros and cons. The pros of running a live CD boot, is that it reduces the risk of having your computer compromised by viruses, malware and keyloggers that rely on Windows vulnerabilities to run.

If you are going to run this OS from a Virtual Box, I suggest downloading Virtual Box

from Oracle. Note the **https://**

https://www.virtualbox.org/

Next, the live operating system I would encourage you to use is **Tails**. Tails can be found at the following website.

https://tails.boum.org/

The reason I choose Tails, is because it has many of the security features that you require to stay anonymous already installed. Some users are not happy with Tails, but it really is a great operating system loaded with security features. Many I will talk about in this series on security including PGP encryption and decryption. Make sure you download the Tails ISO file from the official Tails website and you can either load it into Virtual Box or burn it to a DVD or load it onto a USB and booting your computer from that drive.

There are plenty of tutorials on how to load Tails into Virtual Box, so I won't go into much detail other than, make sure you run Virtual Box and Tails from a USB drive or SD card. I would suggest a USB drive however for reasons I will explain later. But basically when when Virtual Box runs directly on your hard drive, it creates a virtual hard drive that is uses as a temporary hard drive while Tails is running. Once Tails is closed, this virtual drive is deleted, but it's not permanently deleted. As we know from the power of recovery tools, deleted files are easily recoverable with the right tools. I will talk about how to protect your files from data recovery tools in future chapters but for now, just keep Virtual Box and Tails OFF of your hard drive, and load it either on a USB drive or SD card.

The same goes when booting your computer directly into Tails from a DVD or USB stick. Your hard drive will be used to store files used by Tails, so make sure any files that are saved or accessed using Tails are done from a USB stick or SD card, otherwise they will be recoverable. This is why I prefer using a Virtual Box and running both the Virtual Box and Tails inside of it, off of a USB stick. Keep as much as possible off of your actual hard drive. It is possible to shred files beyond recovery, but it's much easier to do this on a 16gb flash drive, then it is a 1 TB hard drive.

Next we will start learning how to use PGP. The reason I had to take a detour to using Tails is because we will be using Tails for many of the features from here on out, including PGP.

PGP Continued..

Ok, so by now I am assuming you have Tails running. Let’s learn how to use PGP within Tails. First thing you are going to want to do is create your own personal key, which consists of your public key that you can give out to people or post in your profiles online. As mentioned before, this is the key people use to encrypt messages to send to you. Your personal key also consists of your private key which you can use to decrypt messages that are encrypted using your PGP public key.

If you look up to the top right area, you will see a list of icons, and one of them looks like a clipboard. You need to click on that clipboard and click **Manage Keys**

Next click **File** -> New
Select PGP Key and click Continue
Fill out your full name (I suggest you use your online name, not your real name)
Optionally fill out an email and a comment as well.
Next, click Advanced Key Options.
Make sure Encryption type is set to RSA and set key strength to 4096.
Once you have done this, click Create and it will generate your key.

Once you have done this, you can view your personal key by clicking the tab **My Personal Keys** . You have now created your personal key! To find your PGP public key, you right click on your personal key and click Copy and it will copy your PGP public key to your clipboard, in which you can paste anywhere you wish. A PGP public key will look something like this.

—BEGIN PGP PUBLIC KEY BLOCK—

mQINBFLLWDcBEADEzn3mnLsezUDDAS5Q0lm1f6JdkI534WPuRlAN8pnuQsCSwUQUhPEAgNCUNhxN
IalvgDopXTISa9Sh7J3HHYYQazOZt9mfAjjuuRdaOqmAAtEe9dl43nrx+nSd/fqH
13XvMKhqJhIoJ02CBFfRBm86vtx5yiXqHZX438M9kbASqU0A2jAfRd+IZG5Z9gCI
W6FTror+F4i+bEdAuGTG1XFsQSgjKTIG0vgYiTJ93C2MZxrLvNnJp0g2zD0URyk8
Y2IdyCDfIL10W9gNMqLmjD0z/f/os66wTJkflSGaU9ZsrKHUKFN5OSfOZtNqktWn
fCpY4bigkJ8U/5C8mtr9ZE3Tv+RV4rPY0hAOtZucnhlRmYKVFNjvbS0MjqA1188c
wzBNG0XcpCNtmM5UsSvXwnDoUaEMXe50Hikxdk3d+CJzqYnor72g/WmIDROCiXl6
2D9rJ2JuLpl9bQLM+KCbXJf3kUSvzszZGXL/AwmynvqlruaXqr5975sCdfqXVexx
1sxsLofOzE01xSDEJRWwHQPlxTKPZFnXD709Xumjdinjv1w4onLk04Z96wARAQAB
tC5Kb2xseSBSb2dlciAoVGhleSB3b3VsZCBsaXZlIGFuZCBkaWUgdW5kZXIgaXQp
iQI3BBMBCgAhBQJSy1g3AhsDBQsJCAcDBRUKCQgLBRYCAwEAAh4BAheAAAoJEPuh6tSg81nyzNsP/
G6+sYg41mfMuZEimgavNb0Uc2r6mI7UyWy5lp1Gd/D+all81X7bm5EBpvl1isPgJ
EqjehEdh9FQjrTiRIJafM1m254hIAaZ1RvAphI0tM2lpudk+tNKq+ivV8PpsN9TP
0mg5ZAu1lIKtG9k5vS9HAQ0grJ01TFMEjlifrf7eRyJ1+dmRJ+Xtoy2js8UwS+wM
RrIi3G39P2BfEZFQka3EmQ2JgN4pDWFoI0hODGhTba8Z0XSnVtabOTi1TOWIFmFu
yqA9bNtuOt3KhIC/O+mEATRsc/VPbTY+80kf45LwlDBfKO3PcOXSOG7ygibzEqXn
Ms/Rfe1kNEBeR9Wx2NMJSdxypqGij17CLJwNLC3KypTIQrhzy3YAndeDG4TadW2P
v/FJxhz+MX+s+9VeX2fGC0Fsfp8JbeWMAznp8Rf6O/tzEYW+pbLoLRPdi/DvFBZV
yWGPspzt3Qspm+BHbeW9iFjvCyvP2/DrKmQM7ABuRh/TMZR7uQ5na11L8rf3nzrS
Al/lSul42xLzxG+h9mDixXd1Vh6rVGMbCjL7wO25TUneFo13U5J+klo1blQWV/DL
FZUwhh2utWNCMCtcdRW0HYa14Wdyy7H68WmsJqBWUsbyD9PZ2gSawBy7uQINBFLLWDcBEACg3IOr
gCj6NxRxbfdyLjL1gxSlJyFtclkFGS0lC0GIz7lINvemkewjde/bHXChz2IIaIli
L2A6Z6w3fP4jlQCw8NoGGJ360WMkZVTDDakYYkb50BrZSx4TVLjrHfFuLMXTE255
gQrId02jYO6240EDIhHITuiSwUQvHtXlOrHSohN83TD1I4H7iH/FLae9gYh4C/Ix
VLkzLUqvpf72Q/xogCZAJl4WEMmWD6dXufvyvhCXQnbjiLuAdQas0ef/t652LPw/

vJFDSDmguw9PXWpv3vFOe13UNU//+nw3kIGxaVWGvazXk8IFiDv9USgEGjcNn4zo
8HQlQrYz9/gyI3XojGV6L8iecWpHSweqR3NxKJmWKWEG1wwnWPL8M+z6OwEvRdxVspy+eG0Zs+6igb
73ZNX16krXqufl0HAJRd1PwhITPCtSviW3L2qKF2Pdak3j97A656EcInCcAyOUC/
mUNUDtXJik6uwFgFFn9/pnFr+acY7ppsWPG5rr7jRj+Lgjnjkckpkjo8jN1hZE17
CfJyrYrSqdglCcIgTHteIEZdPfPUmnbbSoyeufkyEW1AoIKatQARAQABiQIfBBgB
CgAJBQJSy1g3AhsMAAoJEPuh6tSg81ny4nIP/2lVf0DTp1n5xPEBZEUlgzcMNeh5
FTIS3J44g5a+OlkRVgHFtu7K/MUsftlUzkvMMa0sXllhKc6syxcytoD7LAt9tbQh
62yEzijTliU2QFgWJSS6IfbtC2IyRouAns3KD6XouKTFUs/i0n/QpwhnM+Ya/SAg
c/oroM7SE/T4g+v6EeRCq7In/TMgc74j+25zUF1rVSCenbZKkYezxqZ33cXLwl7l
IUBcK2uNHDBUB5G853NR0OkBm5i+KC8vM3K1/MZ+P/lK0xOcTGXZH/A7GrEsI4FJ
nw5i6zJZb8gmDt44Tp/1Ujxnm5xhVWgnOQeSVSyiRsHQ/gTCL1PqsZhW7yulwL05
yxZgN+oYVx4pNtLJMigRjoCY9IKEmZhY75cWXXA19j14Wnxu8IrwwSk1WyzMQcjj
7onP4OEhbPuotqWqVAc0M/+MV5oMGIG0Qepy6XpZOCCpZw/p1rDrZSYP5eQMd/4x
LB7xch6GjbWsnKhA1wGdjdclBodixorVfCRn4s5jTgXx7wWz/opM4ix/CPAkify7
4Sf0BdJ5YtFILZc5StED4WC5pljJbdEWVsb9rn6egvFn7W/ZlDJAerS6Mt5LJGAh
Aude0Kz2HJwDtOBF4nXeTzRCK5BrBnCYPHAtO2aqfowirzjMTd9A/ADoPmIbIJAm
04mA6krRiH909Bnx=Az2N
—–END PGP PUBLIC KEY BLOCK—–

Next, you are going to want to save the private key on a secondary USB drive or SD card. If you are running Tails from a USB drive, then you must use a separate drive to store your key on. If you are running Virtual Box, you want to **right click** on the icon in the bottom right corner that looks like a USB drive, and select your separate drive that you will be using to store your keys on. Again, never store your private keys on your hard drive, keep them OFF your computer.

To save your private key, you are going to right click on your personal key and click Properties. I know you probably saw where it says Export, but this is not what you want to do. Clicking export will ONLY export your public key and will not save your private key. If you lose your private key, you can never recover it even if you create another personal key using the exact same password. Each private key is unique to the time it was created and if lost, is lost forever. So once you have clicked **Properties** , go over to the tab **Details** and click **Export Complete Key** .

Once you have done this, you have saved your personal key for future use once you restart Tails. Remembering that Tails is not installed on your hard drive, so every time you restart Tails you lose all your keys. By saving your keys onto a USB drive or SD card, you can import your keys for use every time you restart it.

Next you are going to want to learn how to encrypt and decrypt messages using your key. Well, luckily for me, Tails has already made a tutorial on how to do this, so I will refer you to their webpage. But before I do that, I need to mention that you need to find somebody else's PGP public key, or you can practice by using your own. Needless to say, the way you import other people's keys into what's called your **key ring** is by loading them into a text file. You do this with the program called **geditText Editor** .

Click Applications -> Accessories -> gedit Text Editor and enter in someone's public key and hit save. Next you can return to your key program from the clipboard icon and click File -> Import and select that file. It will import that person's public key into your key ring. To add future public keys to your key ring, I suggest reopening the same file and just adding the next key below the previous key and each time you open that file it will load all keys within that file. This way you can keep all the PGP public keys together in one file

and save it on your SD card or USB drive for future use.

Finally, you can use the following 2 pages to learn how to encrypt and decrypt messages using PGP.

https://tails.boum.org/doc/encryption_and_privacy/gpgapplet/public-key_cryptography/index.en.html

https://tails.boum.org/doc/encryption_and_privacy/gpgapplet/decrypt_verify/index.en.html

Have fun with your new found ability to communicate in PGP!

WHOLE DISK ENCRYPTION AND FILE SHREDDING

Now that we have PGP figured out, hopefully, I want to remind you that using PGP whenever possible, is very very very important.

One of the reasons why I would suggest for you to store your PGP keys and other sensitive data on a SD card, is that if that day comes when you are compromised and you get a knock at your door, you have time to dispose of that SD card or USB drive quickly. Even better, if you have a micro SD card that plugs into an SD adapter, then you can snap it with your fingers or at the very least hide it. USBs would need to be smashed into pieces and it might not be easy to do this in the heat of the moment, so do what you feel best about. But always prepare for the day they might come for you.

But our next topic brings us to something called Whole Disk Encryption or Full Disk Encryption. From here on out I will refer to it as FDE (Full Disk Encryption). Tails has a FDE feature built into it, which is another reason why I encourage the use of Tails. It has many of these features to protect you. Essentially FDE will protect your drive, whether SD or USB from the people who may come for you one day. The method in which it does this is it formats your drive and rewrites the file system in an encrypted fashion so that it can be only be accessed by someone who has the pass phrase.

If you lose your passphrase, just like in PGP, there is no recovery. Your only choice is to format the drive and start over again. So make sure you remember it! And please for the love of God, Allah, Buddah, etc… don't store the passphrase on your hard drive somewhere. The tutorial on how to do this is located at the following webpage.

https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.en.html

Again, always prepare for the day they come knocking, encrypt everything. Use PGP when communicating with others and always shred your files when finished with them. Which brings me to my next topic. **File shredding** .

File shredding is extremely important and here is why. If you delete a file from your computer, you are only deleting where it is located on the drive. It is still on the actual drive, just its location data has been removed. If you take a file recovery tool you can recover virtually any file that you have recently removed. File shredding combats this by overwriting files instead. The idea is that instead of removing the file's location, you need to overwrite the file with random data so that is becomes unrecoverable.

There are a lot of debate happening on whether you can just overwrite a file once, or if you need to do it multiple times. Supposedly the NSA recommends 3 times, supposedly the Department of Defense recommends 7 times, and an old paper by a man named Peter Gutmann written in the 90's recommended 35 times. Needless to say, I personally think between 3-7 times is sufficient, and several people out there believe 1 time will get the job done.

The reasoning behind this is that some people believe the drive may miss some files the first time it over writes them and to be more complete, you should do multiple passes. Do what you feel most comfortable with, but I even think 3 passes would be sufficient, although it wouldn't hurt every now and then to run 7 passes and just leave it overnight.

The programs that can do file shredding are ones you will want to run from Windows or whatever operating system your computer is running. These programs can delete your files from your Recycling Bin, delete your temporary internet files and even Wipe your free disk space to make sure everything gets cleaned up. You always need to think; did I have any sensitive material on my hard drive? If so, maybe I need to shred my free disk space. When empting your Recycle Bin, you should always use a shredder. When only deleting under 1gb at a time, you can easily do 7 passes pretty quickly.

To put this in perspective, the leader of a group called LulzSec name Topiary has been banned as part of his sentence from using any type of file shredding applications so that if the FBI wants to check up on him, they can. File shredding keeps your deleted files actually deleted.

Here are some file shredding applications you can use.

http://www.dban.org/
http://www.fileshredder.org/
https://www.piriform.com/ccleaner

Next we're going to talk about removing harmful metadata from files, and some other topics as well.

JAVASCRIPT VULNERABILITIES AND REMOVING PERSONAL METADATA FROM FILES

Before I get into removing harmful meta data from your files, I want to talk about another vulnerability to our browsing capabilities called JavaScript.

In mid-2013, a person in Ireland was providing hosting to people that hosted hidden services including a secure email platform called Tor Mail. Unfortunately, they busted him on an unrelated charge relating to child pornography and seized all his servers. Whether or not he was related to child porn or not, is unknown to me, or it could be a silly charge the feds slapped him with but either way, the feds ended up injecting malicious JavaScript into his servers so that when users would visit certain sites, this malicious code would execute on their computers and reveal information about their computers to the feds. I suggest you read the following article to learn more about this.

https://openwatch.net/i/200/

With that being said, you may want to disable JavaScript in your browsers, especially when visiting certain websites like that may become compromised one day.

In Tails, the browser is called Iceweasel and when Tor in ran in Windows, it uses Firefox. Both browsers can disable JavaScript using the exact same method. Open up a Window and type the following command in the address bar, “about:config” and click the button that says “I’ll be careful, I promise.”

This will bring up a bunch of settings including a search bar at the top. Enter JavaScript in the search bar and look for the following two entries, “javascript.enabled” and “browser.urlbar.filter.javascript”. Right click on these and click “Toggle” and you will see the Value changed to false. If you want to enable JavaScript again, just click Toggle again and you will see the value change back to true.

Again, remember that every time you restart Tails you will have to do this again, so get into a habit of doing this every time. You never know when your favorite website could become compromised.

Moving onto meta data. There is a bit of a famous story about an online hacker named w0rmer that would take pictures of his girlfriend and post them online after he would deface a webpage. What he either forgot, or didn’t know was that photos taken with the iPhone and other smart phones save the GPS coordinates of where the picture was taken and store it in the meta data of the picture. Check out this article below.

https://encyclopediadramatica.es/W0rmer

You need to remove this meta data! Otherwise you could end up in federal prison with w0rmer. Luckily Tails has a solution for this! See why I love Tails?

Applications -> Accessories -> Metadata Anonymization Toolkit

Please get a clearer idea of how this works by reading the following page.

https://mat.boum.org/

Please note the currently supported formats. In terms of pictures, jpg, jpeg and png. But unfortunately MAT is not perfect and I wouldn’t solely rely on it, so a better idea would be to never upload pictures of yourself or your significant other online, especially bragging about a hack you committed. Please read the site provided above for more information.

GENERAL SECURITY PRECAUTIONS WHEN POSTING ONLINE, METADATA

Next I want to talk about good practices when using TOR, Tails and other hidden services.

First of all, it is highly recommended that you use multiple identities online for different things. Perhaps if you are a buyer and a seller on an infamous bazaar, you may want to have separate logins for this. And then possibly a third login for the forums. Then maybe you want to be part of another marketplace, then you might want a fourth login.

Well, Tails has another good program offered by Tails is called KeePassX. When you have multiple logins, it is hard to keep track of them all, so it might be a better idea to keep them all in 1 document that is encrypted with a strong password. KeePassX can help you with this.

https://tails.boum.org/doc/encryption_and_privacy/manage_passwords/index.en.html

You never want to use nicknames or locations, or anything else that is related to yourself online when you post or create usernames. And another thing you need to adopt are new ways of conducting yourself. If you are generally a messy typer, who makes the same grammar mistakes, or the same spelling mistakes all the time, this can be used to identify you. Always proof read anything you post publicly, or privately because the feds will always find ways to correlate things to you.

Think about the time you use your computer. Is it easy to correlate your time zone based on the time you go online? Or is it more random? Do you have patterns that are predictable? Always think about these things when you post online. Always think about what type of personality you are putting out there about your online name.

Expect that every single word you type online is being read by the Feds. To them, this is much easier than tracking drug lords on the streets. They sit in an office and read forum posts and try and make connections. Don’t underestimate the feds. Always treat everything as compromised, always treat everybody as compromised and don’t ever think anybody will ever go to jail for you. If somebody can avoid 10-20 years by ratting you out, they will do it in a heartbeat.

The perfect example is Sabu from LulzSec. After he was busted and facing 112 years in jail, they made him a deal to help them rat out his friends and he ended up getting many of his “friends” arrested. Even people who are your friends will turn their backs on you when it comes down to their freedom.

EXIF DATA

I forgot to mention above when talking about metadata, that when it comes to photos, there is another risk involved called EXIF data, this is another form of meta data specifically related to images and may not be properly removed by Metadata Anonymization Toolkit mentioned before.

EXIF data stands for **Exchangeable image file format** and affects JPG, JPEF, TIF and WAV files. A photo taken with a GPS-enabled camera can reveal the exact location and time it was taken, and the unique ID number of the device – this is all done by default – often without the user's knowledge.

In December 2012, anti-virus programmer John McAfee was arrested in Guatemala while fleeing from alleged persecution in Belize, which shares a border. Vice magazine had published an exclusive interview with McAfee "on the run" that included a photo of McAfee with a Vice reporter taken with a phone that had geotagged the image. The photo's metadata included GPS coordinates locating McAfee in Guatemala, and he was captured two days later.

To avoid this, only take photos that use PNG because it does not store EXIF data. To check if your photo has any revealing EXIF data attached to it, check out this site.

http://www.viewexifdata.com/

or you can download a tool by doing a quick search online to see what EXIF data may be contained in your photos before you upload them. Be very careful with any files that you upload online, because you never know what type of harmful data could be attached in them. It helps to use Tails, but always consider everything you put online as a potential piece of evidence to be used against you and always prepare for the day the feds come to your door.

RETAINING A LAWYER, HOW TO HANDLE GETTING CAUGHT OR INTERROGATED

Next in the series on security is how to handle getting caught.

Let us face it. We are all human and we make mistakes. Unfortunately, you only need to make one mistake, and the Law Enforcement, commonly referred to as LE can bust you. Maybe they will wait for you to do something more serious before they nab you, but if you slip up and they feel you are worth going after, you can expect them to get you no matter where you live, with rare exception.

The main question is, should I keep an emergency lawyer fund on hand? And how much should it be. The response I think was most appropriate for this question was the following.

> *"Give your lawyer 50k and put him on a retainer.*
>
> *Don't have an emergency fund 'stash' lying around if that is what you mean…. you should already have your lawyer paid + plus extra in case he needs to post bond for you and they seize the majority of your drug funds."*

Once you get arrested by **LE** , they can seize your money based on the assumption that it is drug related. So you need to have a lawyer paid for ahead of time. That way, in the unfortunate case that you get a visit from the feds, you have a lawyer ready to go. The agreed upon amount was around $50,000.

Next I want to talk to you about what to do in case you get interrogated by **LE** .

Keep your mouth shut. The feds are going to try all types of tactics on you to get you to admit to guilt of the crimes you are being accused of. They will likely use the good cop, bad cop on you. First they will tell you that they want to help you, and that they are after the big guys. They just need your help to put away the big guys. Do not listen to this, I have never cooperated with a good cop LE and have it end up working in my favor. Once you admit to being guilty, you can kiss your freedom good bye.

Secondly, if you refuse to cooperate, their attitude will change to bad cop. They will say, "OK fine, you do not want to cooperate? I tried to help but now you are going to be in a lot of trouble. Do you have any idea what kind of charges you are facing? You are going away for a long time unless you start talking."

They are going to try and scare you into admitting guilt. Again, keep your mouth shut and continue to ask for a lawyer, hopefully the one you put on a $50,000 retainer prior to this happening. Never speak without a lawyer present and never do anything you do not have to do legally. If you have the right to remain silent, then exercise that right. I know there are some circumstances in which you do not have that right, but unless that is the case, you are better off staying quiet.

Third, drop the attitude. Do not argue with the cops about having **nothing on you** , or something for that matter. Act scared, anxious and confused. Act like you have no idea what is going on and that you are scared for your life. Tell the cops they are scaring you and you want to see your lawyer because you do not know what this is about. They need evidence, and solid evidence at that, to charge you with a crime.

They are going to try and correlate posts you made on forums, phone numbers you called, perhaps a package shipped to your home, all forms of communication, bank transfers, and so forth, until they can find a way to link you to the crime you are being accused of. But the biggest piece of evidence will always be your willingness to admit your guilt for a lesser sentence.

When Sabu found that he was facing 112 years in federal prison, he quickly spilled everything and started working for the feds. Again, talk to your lawyer, find out the evidence against you and only answer questions your lawyer advises you to answer, and answer them in a way your lawyer advises you to answer them.

Try and be as honest as possible with your lawyer. Your lawyer can not and will not share any admittance of guilt you have with the prosecutors or **LE** , this is called Attorney-client privilege. Please note there are a few instances where this does not apply.

https://en.wikipedia.org/wiki/Attorney%E2%80%93client_privilege#When_the_privilege_

COMBINING TOR WITH A VPN

Here is a greatly debated topic.

Should I use a VPN with TOR?
Should I use TOR to connect to a VPN, or use a VPN to connect to TOR?

Let me say first of all, that when you are browsing the internet without TOR, you should probably be using a VPN regardless of whether or not you are using TOR. And make sure that the VPN uses some form of encryption as well. For those of you who are very beginner, think about when you connect to a public Wi-Fi network at a coffee shop, or an airport and you get all these warnings that your requests sent over this network are vulnerable.

All networks, but especially public Wi-Fi networks are vulnerable to traffic analysis. Put this together with the fact that some internet service providers monitor your activity to some level, and you can see why it might be a good idea to always use an encrypted method of using the internet. At the very least to protect your personal information when you are entering credit cards, usernames and passwords, as well as other personal data online. Again, especially if you are using a public Wi-Fi network.

Choosing a VPN that uses at least 128-bit encryption like TOR is good practice, and will stop the majority of eavesdroppers. But if you can get 256-bit encryption, you are even safer. Before we get into whether or not we should be using a VPN together with TOR, I want to give you a few warnings regarding how you should be using a VPN.

If you are going to be using a VPN for any type of freedom fighting, make damn sure that your VPN does not keep logs. This is actually a lot harder than you might think. Many VPN providers will claim to not keep logs of your activity in order to gain you as a customer, because they have to compete with the other providers out there. Customers are going to trend towards providers who offer no identifying data retention. Unfortunately, this claim of theirs is not always the real case and I will give you an example.

There is a well-known VPN provider named HideMyAss that previously claimed not to keep logs of its users. Unfortunately, when met with a court order from their government in the UK, they handed over evidence of a suspected hacker from an internet group LulzSec which helped lead to his arrest. The story can be found below.

http://www.theregister.co.uk/2011/09/26/hidemyass_lulzsec_controversy/

One of the take home quotes from this article is the following.

> *"We are not intimidated by the US government as some are claiming, we are simply complying with our countries legal system* ***to avoid being potentially shut down and prosecuted ourselves."***

A very smart man that goes by the online handle The Grugq, said when doing your freedom fighting online that nobody is going to go to jail for you, and he is 100% correct. When it comes down to it, no VPN provider is going to risk jail to protect a $20 a month

subscriber. No matter how tough they sound, no matter how much they claim to care about protecting their customers, when faced with a choice to give you up or go to jail, they will always choose freedom.

Another thing to consider however, is using a VPN does hide your internet activity from your internet service provider. It can also hide the fact that you are using TOR, which may flag some suspicion when the feds start asking ISPs to provide data about their users. This may or may not be relevant, since many people use TOR and you can argue there are many legitimate reasons to use TOR and nothing suspicious about TOR. But it is just another factor to arouse suspicion that may or may not come into play and should be considered.

If you choose to use TOR over a VPN, the benefits are that you would be again, hiding from your ISP the fact that you are using TOR. Also, your VPN would only be able to see that you are connecting to TOR nodes and that you are sending encrypted data. The VPN would not be able to see what data you are sending over TOR unless they decrypted it, because remember, all information relayed over TOR is encrypted.

The downsides of course, as mentioned are that VPN providers may or may not log everything that you do in the form of meta data or even content if they have the storage capacity, and keep those logs on hand for a long time. In this case, it is no better than connecting to TOR through an ISP. Another thing to mention to those who will use VPNs when not using TOR, but also use VPNs when using TOR is remember when you are, and are not connected to your VPN. Sometimes VPNs can unexpectedly drop connections and you may not even be aware of it. If the reason you are using a VPN is to hide TOR activity from your ISP, then if your VPN drops, your ISP will start seeing your TOR traffic instead.

Or, maybe you forget that you are connected to your VPN and end up punching in your address on Google Maps to find directions somewhere. Well guess what Google does with all data entered into their system? They keep it. And they likely keep it indefinitely. So if one day the NSA identifies you on the TOR network by occupying a large number of nodes and using traffic analysis to identify you based on statistical analysis, it will link them to your VPN IP address.

At this point, they will likely ask the VPN to turn over data on their users, but if the VPN refuses to comply because they are not subject to US law, or the laws of other countries, they may check some of the big surveillance websites out there to see if you slipped up and used that IP address for anything else online. They will check logs from Google, Yahoo, Facebook, Twitter, Netflix and other big data collection companies to see who has been using that IP address to connect to their servers.

If you accidentally punched in your address on Google when connected to that VPN, you are now a suspect. So always keep things like this in mind. Just because you are covered behind a VPN does not mean you are not traceable by human error. The benefits of TOR, are that you get a new identity every time you connect. This may or may not be the case with your VPN, so please check and make sure.

Next we will talk about the advantages and disadvantages of using TOR to connect to a VPN.

THE ADVANTAGES AND DISADVANTAGES OF USING TOR OVER A VPN

Ok, now let us talk about why you may want to connect to a VPN over TOR.

The data flow would look like this. You -> Tor -> VPN -> Internet

The benefits of doing that are as follows. You are more anonymous to your VPN in case they happen to keep logs, or if you do something using the VPN that you are not supposed to and a website or server grabs your VPN IP address. In the case of this happening, even if the VPN manages to keep logs of everything you do, they can only identify you as an anonymous TOR user as long as you did not purchase the service like an idiot with your credit card or Paypal account. If you use Bitcoin, and made sure the Bitcoin trail is not easily traceable you should be okay. Some websites block TOR users from connecting to their websites or servers, by using your VPN to appear as the exit node, you are hiding your TOR activity from the website you are visiting and hopefully bypassing their filters.

Another advantage, is that if your VPN connection does drop, your fall back will be your TOR IP address instead of your real IP address. And finally, if you are passing through a compromised TOR exit node, your information will remain encrypted through the VPN's encryption protocol until it reaches the exit node of the VPN. This is a good thing if you are passing through a compromised exit node, but do not forget that the VPN could be logging everything you are doing anyways. **Do not trust anybody who has access to your unencrypted data!**

A few of the downsides of doing things this way, as mentioned in the previous chapters are that your ISP knows you are using TOR, when and for how long. This may or may not matter to you, but it is just something to consider. Second, you will be unable to visit hidden services websites. Remember those **.onion** sites we talked about in the beginning? You need to be connected to the TOR network to visit those hidden service websites.

But I am connected to TOR aren't I? Yes, you are, but your final method of communicating with the internet does not come from the TOR network, it comes from your VPN. And your VPN is likely not configured for TOR. In order for you to be able to connect to a hidden service, you must either be connected directly to TOR, or use a VPN to connect to TOR. TOR must be your final node of connectivity in order to visit onion websites.

The choice is ultimately up to you, and every person in every state, province and country will have different reasons for wanting to do VPN to TOR or TOR to VPN, or just TOR, or just VPN. Whatever choice you make, please keep all the things mentioned in this chapter and the previous one in mind. None of these methods will save you if you enter anything identifying about yourself online. Do not log into your Facebook account using your VPN. Do not check your email or search a nearby address on Google using your

VPN. In fact, stay away from Google altogether unless absolutely necessary.

There are two other search engines out now that do not store information about their users.

#1 – DuckDuckGo. They have both a clearnet URL and a hidden services URL for both types of users.
https://www.duckduckgo.com
http://3g2upl4pq6kufc4m.onion/ – Please note the hidden services mirror is not HTTPS

#2 – StartPage. This server also does not store any information about its users.
https://www.startpage.com

Before we move on, I want to go back to how to choose a good VPN. When looking for a VPN provider, you will most likely come across two protocols to choose from. Find out which one your VPN provider is using before you sign up with them. PPTP and OpenVPN. At this time, I am going to highly recommend that you avoid PPTP and stick with OpenVPN providers. Check out this site for a quick comparison.

http://www.goldenfrog.com/vyprvpn/openvpn-vs-pptp

As you can see, PPTP uses a weaker encryption, 128-bit versus 160-bit to 256-bit for OpenVPN. It offers basic security versus a high level of security using something called digital certificates. This is basically a way to make sure they data coming in is sent from your VPN provider and not injected by some malicious third party because the incoming and outgoing data are signed using specially obtained certificates, similar to showing your ID to get into a restricted area.

The only downside is that setting up OpenVPN can be a little challenging for the less technical users, but there are plenty of great tutorials online to set up OpenVPN providers and your VPN provider itself will likely help you get set up as well. PPTP has been abandoned by those who demand the highest level of security, so I would recommend to avoid it. A third option for VPN providers is L2TP/IPsec, but many users now believe it has also been compromised by the NSA due to its weaker levels of encryption and should be avoided as well. **Stick with OpenVPN.**

Lastly, if you want to know how to connect to TOR over a VPN. If you are using OpenVPN like I recommended, thenit is really quite simple. Make sure you are connected to your VPN, check your IP address to on any website such as **WhatIsMyIpAddress.com** to make sure it has changed. Then, open TOR or open TAILS and start using TOR and you are now connected to TOR over a VPN.

Connecting to a VPN over TOR is a trickier but is currently only able to be used by Windows users.

CONNECTING TOR -> VPN FOR WINDOWS USERS

After a long search, I have found a way you can connect TOR -> VPN. It is not perfect, and some might not agree with doing things this way, but it works and I am giving it to you as an option, but it only works for Windows users at this time.

If you look back at my previous chapters regarding combining VPN and TOR then you will find the reasons why you would want to do so, and some of the reasons why you might not want to do it. But I was unable to provide you with a way to connect to a VPN using TOR so that the VPN does not know who you are. When it comes to TOR -> VPN, if you cannot trust your VPN, which you rarely should, then keeping your identity anonymous from your VPN is a good idea. Also, with more and more people using TOR, but with only around 4000 TOR exit nodes, many of the exit node IP addresses are being flagged as spammers on popular websites and limiting the usage of well-meaning TOR users to post on message boards like Stack Exchange and so forth.

The way that I found you can do TOR -> VPN is by using a virtual machine, preferably Virtual Box and running another instance of Windows, preferably one that uses less memory than your current version. You also want to run TOR Expert and Tortilla on your host OS. I talk about how to do this in previous chapters. Next set your Virtual Box to route all its network traffic through Tortilla (bridge adapter), which routes it all through TOR. Currently Tortilla is only supported by Windows, which is why this option is only available to Windows users at this time. Doing this also makes it easier to do things like watch videos on YouTube.

Now that you have your Windows Virtual Machine running on TOR, you can install a VPN of your choice, preferably one using OpenVPN on your Windows Guest OS and connect to it. Check your IP address before connecting and after and you should see a different IP address. If all went well, you now have a virtual machine running TOR -> VPN. Then if you want to add another layer, you can download TOR browser bundle onto your virtual machine and run that as well giving you TOR -> VPN -> TOR for another layer of security. Also you have the option using this method to use a VPN on your host OS, then Tor Expert with Tortilla, then another VPN on your guest OS, then TOR browser, giving you VPN -> TOR -> VPN -> TOR.

I am not advocating any which method, you need to make that decision on your own, I am just giving you the knowledge necessary to make an informed decision and you can ultimately choose which method you feel most comfortable with. Sometimes doing TOR -> VPN is necessary because of the spam filter reasons I mentioned above and other times having TOR as your last node to the internet is necessary like when accessing the onion network. It is completely up to you and I know that we are trying to shy away from Windows usage because of all the exploits and other reasons spoken about in the previous chapters, but if you have no other way of staying anonymous from your VPN than this, then I think it is a good compromise until we have something like Tortilla that is

compatible with Linux distributions.

TRACKING COOKIES

Next time I want to talk about is something that most people completely forget about. **Tracking Cookies** .

A recent article explains how the NSA uses things like Google Ads and other tracking cookies to identify users over TOR when doing so by other means is not possible.

http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/

For those of you who do not know what I am talking about, let me ask you this. Have you ever noticed that certain ads seem to follow you around from website to website? Perhaps something you searched for on Google or Yahoo is now showing up in ads on other pages? This was originally designed to market things to you based on your preferences by installing tracking cookies into your browser.

Luckily TOR clears its cookies every time you restart the browser, and yes Tails does too, but that does not mean you are not vulnerable within the same TOR session. What I mean by this is, let us say you went and did some freedom fighting on a forum somewhere and then after, using the same Tor session, visited another website with Google Ads on it. Then you went to another site with more Google Ads on it. You would be surprised how many sites now have Google Ads on them, by the way.

Google can use these tracking cookies to learn about your browsing behavior. Your search terms, your preferred sites, and so forth. Some people are even stupid enough to use the same TOR IP address and go check their Facebook news feed or their email. Guess who is in bed with the feds? Google, Yahoo, Facebook, MSN, and all of their email providers as well. Remember, when you start leaving patterns behind, they will start looking for similarities that start with just a suspicion.

Perhaps they correlated the freedom fighting forum posts with you because you logged into your email, and now they start noticing that you always misspell the same words, make the same grammar mistakes, the same slang terms. Perhaps you visited a website belonging to somebody local to you with Google Ads on it. It is not entirely sure how they are able to use these tracking cookies to identify you, but the point is, they keep everything. And if you happen to do something stupid like Google a local restaurant or what movies are playing in your local area on the same IP address that you did something you should not have earlier on, then Google can put 2 and 2 together.

Once they are on your trail, you are screwed. So do not give them anything to correlate to you, ever! So then you might ask, cannot I just disable cookies all together? Yes, you could, but, cookies are required for things like login sessions. Without cookies, you are unable to maintain a state of being logged in on certain websites, because they use that cookie ID to identify the session on the server. Again, you can certainly disable cookies, but you will not be able to maintain a login anywhere.

HOW FAR WILL LAW ENFORCEMENT GO?

Now we are going to talk about the lengths that law enforcement (LE) will go to try and catch you slipping.

The first question is, can LE ship drugs to buyers to try and set them up for drug charges? Let us just say, that they have done it to someone before who went by the name of Flush aka Chronicpain aka Curtis Green

http://www.usatoday.com/story/news/nation/2013/11/07/vendor-administrator-plead-guilty-in-silk-road-case/3469751/

> *"In April 2012, a DEA undercover agent in Maryland posing as a drug smuggler began communicating with "Dread Pirate Roberts" on Silk Road about selling a large amount of illegal drugs. "Dread Pirate Roberts" instructed [Curtis] Green to help the smuggler find a drug dealer who could buy a large amount of drugs, court papers say. Green found a buyer and agreed to act as the middleman for a $27,000 sale of a kilogram of cocaine. Green gave the DEA agent his address.*
>
> *An undercover U.S. Postal Service inspector delivered the cocaine to Green's house in Utah on Jan. 17."*

So as you can see, whether you view it as entrapment or not, once they have evidence against you, they will eventually figure out a way to get something on you and bust you for it like they did to Curtis Green.

The Secret Service posed as a vendor for fake IDs online for 5 years and actually shipped fake IDs that they made to buyers on an online Russian forum.

http://www.tested.com/tech/456882-how-secret-service-sold-fake-ids-catch-identity-crooks/

> *"The US Government's "Operation Open Market" resulted in indictments against 55 defendants. According to Wired, Special Agent Mike Adams shipped out more than 125 fake IDs over about five years of activity while going by the username Celtic. Amazingly, the entire scheme started when the government arrested the real Celtic, a Nevada man who got caught shopping at a Whole Foods where he'd previously used a fake credit card.*
>
> *Law enforcement discovered counterfeiting equipment among his possessions and learned about his online activities. Adams assumed his online identity and even improved Celtic's cred, shipping near-flawless IDs and becoming a trusted seller on Carder.ru."*

As you can see in this article, the Secret Service again sold illegal items to people online in order to bust them. Several of the buyers used their real addresses and sent real photos of themselves to this officer to have their IDs made, resulting in being arrested by the feds.

And in this particular case, the feds charged all the defendants under something called the RICO act.

> *"The main indictment is noteworthy because, in addition to the usual mix of credit card fraud and false identification charges, the 39 defendants have been charged under the mob-busting RICO act – a first for a cybercrime prosecution.*
>
> *Enacted in 1970 to help the FBI crack down on the mafia, the Racketeer Influenced and Corrupt Organizations Act* ***lets the feds hold every member of a criminal organization individually responsible for the actions of the group as a whole****. The losses collectively inflicted by the Carder.su members are easily enough to give every RICO defendant 20 years in prison."*

When you commit crimes online, especially in an online community, the feds may be able to hold you accountable for the actions of other users on that same community. So make sure when you do your freedom fighting, or whatever you choose to do, that you take this into considering. Always weigh out the worst case scenario, should you get busted, because the LE will try and set you up.

One last example of how LE will try and set you up, but not relating to online communities is when they put together a fake sweepstakes in Los Angeles.

http://www.nbclosangeles.com/news/local/La-Mirada-Inspired-by-the-Simpsons-to-Catch-Criminals-78093912.html

> "Sheriff's deputies in La Mirada attempted a rope-a-dope on some alleged criminals by offering them a fake sweepstakes prize. Out of the 960 letters sent to these "people of interest" only eight showed up at the La Mirada Holiday Inn to collect their prize, according to the Whittier Daily News.
>
> Posing as the "Pelican Marketing Group," deputies sent letters last week to people throughout the county wanted in connection with crimes ranging from misdemeanor warrants to murder.
>
> According to the report, the suspects were advised to bring their letter and identification to the Holiday Inn, and told that they were guaranteed a prize worth at least $100, and would be one of 200 people with a chance to win a 2010 BMW 238i sedan.
>
> They were all smiles when they showed up to collect their prizes, Deputy Janet Ramirez told the newspaper. "Once they tell them they're under arrest, the smile fades quickly," she said."

So the reason I made this chapter, was for those of you who think that LE will not go to certain lengths to try and set you up for charges. They will do it if they want you bad enough, and if you fall for it, they might get you on some tough charges. Curtis Green is facing up to 40 years for the sting operation by the DEA on him and the users who purchased fake IDs on the Russian forum could face up to 20 years each since they can be charged under the RICO act. Always keep these things in mind when conducting activities online and always take the worst case scenario into account.

It only takes one mistake to get caught and the government has unlimited resources and super computers to try and catch you slipping. You may only have a few laptops, desktops, servers, but nothing compared to the what they have. Be careful.

LEARNING FROM OTHERS' MISTAKES. HOW THEY BUSTED SABU

This next chapter I want to focus on more mistakes that other hacktivists and freedom fighters have made which ultimately led to their arrests. This is more proof that you only need to screw up once.

You have probably heard me talk about somebody named **Sabu** multiple times and maybe you are new to the online communities and you have no idea who I am talking about. Sabu was the leader of a self-proclaimed hacktivist group called LulzSec. They were responsible for taking advantage of security exploits in online servers and posting the information online on a website called PasteBin. They had done this many times.

https://www.informationweek.com/attacks/lulzsec-leader-sabu-unmasked-aids-fbi-hacker-sweep/d/d-id/1103214?

> *"The men have been charged with hacking Fox Broadcasting Company, Sony Pictures Entertainment, and the Public Broadcasting Service (aka PBS)."*

During the time all this was happening, the members of this group maintained an online Internet Relay Chat (IRC) channel in which they regularly discussed and took credit for their attacks and exploits. The agreed upon ring leader for these attacks, and this group went by the online handle Sabu. Sabu had also been linked to selling stolen credit cards on Facebook through his online handle, not his real one, which carries a charge of aggravated identity theft.

The group had leaked identities of law enforcement, Sony users, and all wreaked all types of havoc online including DDos attacks on the CIA. The FBI wanted Sabu, they wanted the ring leader, who would eventually be facing charges that could lead to 112 years in prison. But as I mentioned in previous chapters, it only takes one mistake to get caught. That is all they need.

http://www.foxnews.com/tech/2012/03/06/exclusive-unmasking-worlds-most-wanted-hacker/

> *"Sabu had always been cautious, hiding his Internet protocol address through proxy servers. But then just once he slipped. He logged into an Internet relay chatroom from his own IP address without masking it.* ***All it took was once.*** *The feds had a fix on him."*

However, this was not his first actual slip up, but it was his first slip up where the feds actually discovered his mistake. His identity was actually discovered, or "doxed" previously by another online hacking group called **Backtrace** who posted his identity and general location online weeks prior to this in an attempt to dox members of LulzSec.

http://arstechnica.com/tech-policy/2012/03/doxed-how-sabu-was-outed-by-former-anons-long-before-his-arrest/

> *"Sabu occasionally mentioned ownership of a domain called prvt.org in his chats, including those in Backtrace's "consequences" document. Every domain registration is associated with corresponding information in the WHOIS database. This information is supposed to include the name and address of the domain's owner.*
>
> *Often this information is incorrect (most domain registrars do nothing to validate it) or anonymized (many firms offer "proxy" domain registration, so the WHOIS database contains the details of the proxy registrar, rather than the person using the domain). Monsegur appeared to use one of these anonymizing services, Go Daddy subsidiary Domains By Proxy, for registering the prvt.org domain.*
>
> *The registration for the domain was due to expire on June 25, 2011, requiring Monsegur to renew it. But for some reason—error on Monsegur's part perhaps, or screw-up by the registrar—the renewal was processed not by Domains By Proxy but by its parent, Go Daddy. Unlike Domains By Proxy, Go Daddy uses real information when it updates the WHOIS database, so on 24th June (the day before it was due to expire),* ***Monsegur's name, address, and telephone number were all publicly attached to his domain name.***
>
> *Monsegur quickly remedied the mistake, changing the WHOIS registration to use various other identities—first to that of Adrian Lamo (who reported Bradley Manning to authorities) and then to "Rafael Lima" and subsequently to "Christian Biermann". This attempt to mislead those relying on the WHOIS information successfully misled some would-be doxers. But not all: by August there were extensive dossiers on Sabu's true identity."*

Two mistakes that we know of, is all that it took to bring down at one time, the World's Most Wanted Hacker. If you are familiar with the story of LulzSec, there was a time they were receiving mainstream news coverage and Sabu had gained a reputation of being this mystical untouchable hacker. Unfortunately for him, he made two small yet very costly mistakes which ended up putting him away. But we are not done yet on this story about Sabu.

Sabu had a weakness, that the feds used as leverage against him when he got busted.

> *"An unemployed computer programmer, welfare recipient and* ***legal guardian of two young children.***
>
> *"It was because of his kids," one of the two agents recalled. "He'd do anything for his kids. He didn't want to go away to prison and leave them. That's how we got him."*
>
> *Monsegur was quietly arrested on aggravated identity theft charges and released on bail. On Aug. 15 he pleaded guilty to a dozen counts of hacking-related charges and* ***agreed to cooperate with the FBI."***

So when you are doing your freedom fighting online, you need to ask yourself. What do I have to lose? Do I have a wife? Children? What would happen if I were to lose everything and be thrown away for 10 to 20 years, could I handle that? If you decide that you are willing to risk all that, then you again need to learn from the mistakes of those who have fallen before you. Ask yourself, if put in a hard place, where you had to choose between life in prison, and cooperation, in order to see your own family, you may think you will not talk now, but you may start talking when the feds are threatening to take them away from you forever.

Once the FBI had the leader of the group LulzSec working for them, they wasted little time getting the former hacker to turn on his friends and aid in their arrests.

LEARNING FROM OTHERS' MISTAKES. SABU BECAME FBI INFORMANT AND BETRAYED JEREMY HAMMOND

We are continuing the subject of how others were taken down after Sabu was compromised and started cooperating with the FBI. According to this article.

http://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/

> *"The day after Christmas, sup_g had another online chat about the Stratfor hack and about some 30,000 credit card numbers that had been taken from the company. His interlocutor,**CW-1**, engaged in a bit of gallows humor about what might happen should they all get caught.*
>
> *But the raid had, in fact, already happened. **CW-1 was "Sabu,"** a top Anon/LulzSec hacker who was in real life an unemployed 28-year old living in New York City public housing. His sixth-floor apartment had been visited by the FBI in June 2011, and Sabu had been arrested and "turned." For months, he had been an FBI informant, watched 24 hours a day by an agent and using a government issued laptop that logged everything he did."*

So we see here Sabu is chatting with a user **sup_g** to try and engage him about the hacks that took place.

> *"Sabu suddenly addresses sup_g by a new name, "anarchaos." It would turn out that sup_g went by many names, including "anarchaos," "**burn**," "yohoho," "POW," "tylerknowsthis," and "crediblethreat."*
>
> *CW-1: if I get raided **anarchaos** your job is to cause havok in my honor*
> *CW-1: <3*
> *CW-1: sup_g:*
> *@sup_g: it shall be so*
>
> *Normally, the attempt to link his various names would have raised the hacker's guard; as he confided to Sabu, someone else had once tried to link the names "yohoho" and "**burn**," but the hacker "never answered… I think he picked up some language similarities I've worked with [REDACTED] on other ops in the past." But this was Sabu, a sort of hacker demigod in the world of Anonymous. If you couldn't trust him, who could you trust? Sabu had even provided a server to store the stolen Statfor data, so he couldn't be a fed (in reality, **he had done so at the FBI's direction**)."*

And more details on how they looked through copious amounts of logs to correlate this

user **sup_g** to his real identity.

> *"To identify sup_g, the Bureau first turned to the voluminous chat logs stored on Sabu's computer. They went through every comment that could be plausibly linked to sup_g or one of his aliases. The goal was to see if the hacker had slipped up at any point and revealed some personal information.*
>
> *He had. On August 29, 2011 at 8:37 AM, "**burn**" said in an IRC channel that "some comrades of mine were arrested in St. Louis a few weeks ago… for midwestrising tar sands work." If accurate, this might place "**burn**" in the Midwest. FBI Chicago agents were able to confirm that an event called Midwest Rising was attended by Chicago resident Jeremy Hammond's twin brother. (Hammond had a history with anarchism and violent protest.)*
>
> *"Anarchaos" once let slip that he had been arrested in 2004 for protesting at the Republican National Convention in New York City. Much later, "yohoho" noted that he hadn't been to New York "since the RNC," nicely tying both online handles to the same person. The FBI went to New York City police and obtained a list of every individual detained at the 2004 convention; they learned that Jeremy Hammond had in fact been detained, though he had not been arrested. The pieces were starting to fit.*
>
> *"**Sup_g**" and "**burn**" both indicated later that they had spent time in prison, with "**burn**" indicating that he had been at a federal penitentiary. A search of Hammond's criminal records revealed that he had been arrested in March 2005 by the Chicago FBI and had pled guilty to hacking into a "politically conservative website and stealing its computer database, including credit card information," according to an FBI affidavit. Hammond was sentenced to two years in prison for the action.*
>
> *In yet another chat, "**Anarchaos**" told Sabu that he had once spent a few weeks in a county jail for possession of marijuana. He also asked Sabu not to tell anybody, "**cause it could compromise my identity**," and he noted that he was on probation. Both matched Hammond, who was placed on probation in November 2010 after a violent protest against the Olympics coming to Chicago. When the FBI ran a criminal history check on Hammond, it also revealed two arrests for marijuana possession.*
>
> *The FBI was so thorough that it even followed up on a "POW" comment saying "dumpster diving is all good i'm a freegan goddess." ("Freegans" scavenge unspoiled, wasted food from the trash of grocery stores and restaurants.) The FBI went to Chicago authorities, who had put Hammond under surveillance when they were investigating him back in 2005. As part of that earlier surveillance, "agents have seen Hammond going into dumpsters to get food."*
>
> *Now that they had a suspect, it was time to put him under surveillance."*

This is why you need to be extra paranoid with every single thing you say about yourselves online. I have seen people talking about what country they live in, some even

talking about which state they live in. If you think that the FBI will never put the pieces together, you may be sadly mistaken as Jeremy Hammond found out.

> *"Watching the WiFi network revealed the Media Access Control (MAC) addresses of each device connected to the network. Most of the time there was only one, an Apple Computer—and sup_g had told Sabu that he used a Macbook.*
>
> *On March 1, the agents obtained a court order allowing them to use a "pen register/trap and trace" device that could reveal only "addressing information" and not content. In other words, if it worked, agents could see what IP addresses Hammond was visiting, but they would see nothing else.*
>
> *His Macbook's MAC address was soon seen connecting to IP addresses known to be part of the Tor anonymizing network.*
>
> *And while this definitely sounded like their man, the Bureau went to even greater lengths to double-check their target. The main technique was to observe when Hammond left his home, then to call Sabu in New York and ask if any of Hammond's suspected aliases had just left IRC or the Jabber instant messaging system."*

If this does not open your eyes to some of the mistakes you may have been making online, then you need to reevaluate how you handle yourself online. Read the entire article to get a better picture, but remember, I do not care if it is your best friend from elementary school, do not, under any circumstances ever admit anything online to anybody. Never under any circumstances take credit for any freedom fighting or hacktivism you have participated in online. And for Christ's sake, NEVER log into a server, especially one that keeps logs with your real IP address!

WHERE YOU MIGHT CONSIDER RUNNING TO, IF YOU HAD NO OTHER CHOICE

In the case that you may have to run, here are some things to consider.

I am not an expert on evading extradition, or how to evade the federal government, NSA or other super powers, but I do have some recommendations that you might want to consider if you decide that you have no other choice but to run. The following countries do not currently have an extradition treaty to the United States.

> *"Afghanistan, Algeria, Andorra, Angola, Armenia, Bahrain, Bangladesh, Belarus, Bosnia and*
>
> *Herzegovina, Brunei, Burkina Faso, Burma, Burundi, Cambodia, Cameroon, Cape Verde, the Central*
>
> *African Republic, Chad, China, Comoros, Congo (Kinshasa), Congo (Brazzaville), Djibouti, Equatorial*
>
> *Guinea, Eritrea, Ethiopia, Gabon, Guinea, Guinea-Bissau, Indonesia, Ivory Coast, Kazakhstan,*
>
> *Kosovo, Kuwait, Laos, Lebanon, Libya, Macedonia, Madagascar, Maldives, Mali, Marshall Islands,*
>
> *Mauritania, Micronesia, Moldova, Mongolia, Montenegro, Morocco, Mozambique, Namibia, Nepal,*
>
> *Niger, Oman, Qatar, Russia, Rwanda, Samoa, São Tomé & Príncipe, Saudi Arabia, Senegal, Serbia,*
>
> *Somalia, Sudan, Syria, Togo, Tunisia, Uganda, Ukraine, United Arab Emirates, Uzbekistan, Vanuatu,*
>
> *Vatican, Vietnam and Yemen."*

This does not mean that these countries will not extradite you, but if you are going to pick a country to flee to, it would be favorable to your chance to choose from this list. One notable country on this list, which is famous for extraditing one of the owners of the **Pirate Bay,** Gottfrid Svartholm to Sweden, is Cambodia. Although no treaty exists between the two countries, he was extradited by the government.

We all know that Edward Snowden fled to Russia from Hong Kong after leaving the US from Hawaii and has remained there since without being extradited by the government and was granted a 1-year temporary asylum. It is unclear if Snowden will be able to stay longer than his 1-year temporary asylum grants, but as of right now he is badly wanted by the US government, and Russia is refusing to hand him over.

Another person involved in the Pirate Bay named Fredrik Neij fled to Laos in Asia following being convicted of “assisting in making copyright content available” and was sentenced to one year in prison and ordered to pay damages of 30 million SEK (approximately €2,740,900 or US$3,620,000). This is of course between Laos and Sweden, but Laos has not extradited Fredrik, so Laos may be a valid option.

I often hear people from the US claim that if “shit ever pops off” they would just flee to Canada. Do not even try it, you would not even make it through the border. Canada is like the baby brother of the United States. When the United States says jump, Canada says “how high?”. Stay away from Canada if you are running from the United States. Even a pot activist named Mark Emery who was a Canadian citizen, lived in Canada, but sold marijuana seeds over the internet to people in the US was extradited to the US to serve a 5-year sentence. According to the other seed vendors in the area, those who only sold within Canada had never been arrested, but because Emery sold to the US, he was arrested and extradited.

Although not on the list above, a woman, wanted in the US for parental kidnapping, named Chere Lyn Tomayko was granted asylum in Costa Rica.

http://www.usatoday.com/news/topstories/2008-07-25-3841863361_x.htm

> *“Tomayko’s claims that her actions were justified by domestic violence she suffered were taken into account by the Costa Rican authorities.”*

Assata Shakur was charged with murder, attempted murder, armed robbery, bank robbery, and kidnapping by the US and fled to Cuba. Cuba actually has an extradition treaty with the US, but the relations between the two countries have not been good since the cold war between the US and the Soviet Union and thus the requests were not honored, even for someone with such serious charges. Cuba may be an option for you, but again this is only something to consider as I am no expert in any way.

And finally according to a previous chapter of mine explaining how the Secret Service sold fake IDs online to people on a forum, several of the members of that forum were able to evade capture due to being in Eastern European countries, although not specified by the feds for obvious reasons, and remain at large to this day.

http://www.tested.com/tech/456882-how-secret-service-sold-fake-ids-catch-identity-crooks/

> *“The government made its move in 2012, arresting dozens of fraudsters in the US and in countries where extradition is easy. But many more, including the founder of Cards.ru, remain at large. Those in Eastern European countries, especially, are largely out of the government’s reach.”*

SECURING YOUR ACCOUNTS FROM FBI MONITORING

Something else you may want to consider.

I noticed that certain some people on forums were never shown as **Online** , even when they clearly were, and others were shown as online at times. I then realized to myself there must be a way to never show your status as **Online** .

The way you do this is to open up **Account Settings** and unselect the box that says **Show others my online status** .

So why would you want to do this anyways? For reasons we spoke about earlier, you do not want to give any law enforcement the ability to see when you log on and log off. It is bad practice, it can leave a trail, leave a pattern, and if you are a person of interest and they are able to connect the time you sign off on the forum with the time you leave your house, or go to sleep, it gives them more reason to be suspicious and more evidence to be used against you in court.

Consider disabling this option.

INVINCIBILITY MINDSET, FEDERAL GOVERNMENT BULLYING TACTICS

Some people have an invincibility mindset that nothing will ever be able to be tied to them or derived from their online communications.

Well guess what? They do not have to use your online communications to find out who you are. All that needs to happen, is for you to do something stupid and become a person of interest and they will be monitoring your activities online to the best of their abilities. Remember you only need to screw up once.

For example, maybe you become a person of interest and the FBI gains a subpoena to your Facebook account where you stupidly bragged to a friend of yours about participating in certain online activities. This happened to one of the members of **LulzSec** who transferred a data dump that he obtained through SQL injection exploits to a friend of his using his own Facebook in his own name. So do not ever talk about The Deep Web or any of your online activities on any social media platform.

Even if a company does not currently keep logs, a court order may perhaps be used to force a company to start keeping logs. **Hush Mail** was forced to hand over 12 CDs worth of e-mails from three Hushmail accounts, following a court order obtained through a mutual assistance treaty between the U.S. and Canada. According to the following article.

http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/

When it comes to being threatened by a court order from the federal government, 99.99% of all companies will comply to avoid either prosecution themselves, or shutting down their business as we saw previously with **Hide My Ass**.

But one company decided to stand up to this type of bullying that you may have heard of called **LavaBit** as seen in the following article.

http://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden

> *"The email service used by whistleblower **Edward Snowden** refused FBI requests to "defeat its own system," according to newly unsealed court documents.*
>
> *The founder of Lavabit, **Ladar Levison**, repeatedly pushed back against demands by the authorities to hand over the encryption keys to his system, frustrating federal investigators who were trying to track Snowden's communications, the documents show.*
>
> ***Levison** is now subject to a government gag order and has appealed against the search warrants and subpoenas demanding access to his service. He closed Lavabit in August saying he did not want to be "complicit in crimes against the American people".*

In July, the authorities obtained a search warrant demanding Lavabit hand over any

encryption keys and SSL keys that protected the site. Levison was threatened with criminal contempt – which could have potentially put him in jail – if he did not comply. Such a move would have given the government access to all of Lavabit users' information.

The court ordered Levison to be fined $5,000 a day beginning 6 August until he handed over electronic copies of the keys. Two days later Levison handed over the keys hours after he shuttered Lavabit."

You see what I am talking about? The federal government ordered this man to hand over all his encryption keys and SSL keys which compromised the privacy of 400,000 users just so they could gain more data on one man, Edward Snowden. And they used bullying tactics and attempted to bankrupt the owner of Lavabit by fining him $5,000 per day until he handed over the keys. Unfortunately, Levison had no choice but to hand over the keys or lose everything.

An interview on Reddit with Levison revealed what he claimed that other secure email providers who threatened to shut down were forced to stay up.

http://www.theregister.co.uk/2013/11/19/lavabit_analysis/

> *"Lavabit's founder has claimed other secure webmail providers who threatened to shut themselves down in the wake of the NSA spying revelations had received court orders forcing them to stay up."*

There you have it. Anyone who tries to stand up to the government, especially in the United States will be met with swift justice, court orders and outrageous fines unless they comply and on top of it, slapped with gag orders so they cannot tell anybody about what the government is doing.

HOW TO CONNECT TO TOR OVER TOP OF TOR

Here is another fun tip that may or may not interest you, but I figured I would throw it in for you anyways.

I figured this out while trying to figure out an effective way to do a TOR -> VPN connection. You can do TOR -> TOR connection with Tails by using a program called **Tortilla** , thus adding another layer for your adversaries to crack. Whether or not this is worth it, is completely up to you, but I am sharing in case it is something you want to do. This however currently only works for those using Windows because it was designed to be used by Windows users. Please note as well that this will noticeably slow down your connection since you are going through TOR twice. Here is the official homepage of Tortilla.

https://github.com/CrowdStrike/Tortilla

And the official download page for the prebuilt standalone exe below. There is a link to it on the home page if you do not trust me.

http://www.crowdstrike.com/community-tools/

The way you do this is very simple actually. You need to first download **TOR Expert Bundle** from the TOR Project download page and install it on your computer or better yet your USB drive.

https://www.torproject.org/download/download.html.en

Next open the **tor.exe** and just let it run until it says **Bootstrapped 100% Done** . Next you want to run the tortilla.exe file and make sure you run it with Administrator privileges. Also, if you are running Windows Vista or later, you will likely get an error that this program does not have a valid certificate, because it is actually signed with something called a test-signed certificate. In this case you need to allow test-signed drivers to run on your computer.

To do this, simply go to your Start Menu and type in the search box “command”. When command comes up, you right click it, and click run as Administrator and it will open up a command prompt. Next type in the following command. **Bcdedit.exe -set TESTSIGNING ON** and this will allow Windows to install test-signed drivers. Restart your computer and you will see in the bottom right hand corner after you restart **Test Mode Windows** . Now you can run Tortilla. And let it connect to TOR. Remember to have **tor.exe** from TOR Expert Bundle open first.

Finally, you open up Virtual Box or whatever Virtual Machine software you are using and click **Settings** on the Tails virtual machine. Click on the **Network** tab and change the drop down menu where it says **Attached to** : to **Bridged Adapter** and in the drop down menu below it called Name: Select Tortilla Adapter. Now your Virtual Machine, in this case Tails, will always connect to the internet **through Tortilla** , which connects through

TOR. And since Tails establishes its own connection to TOR, you will be running TOR over top of TOR. Again, you may or may not want to do this, but I am giving you the option should you want to.

If you are interested in learning more about the creator of Tortilla, he did a PowerPoint presentation at the 2013 Black Hat USA conference. Feel free to watch his talk at the YouTube link below. Please note however that YouTube is owned by Google and there are not many views on the video, so the government will likely correlate users who watch that video with users from forums and the deep web. Make sure you do not watch the video on YouTube with your real IP address. At the very least use a VPN or find another site that has it hosted. Always be extra paranoid.

https://youtu.be/G_jDPQU-8YQ

HOW TO VERIFY YOUR DOWNLOADED FILES ARE AUTHENTIC

As a general rule of thumb, you should **always** download files from the home pages of their respective developers.

TOR: https://www.torproject.org
Tails: https://www.tails.boum.org
Virtual Box: https://www.virtualbox.org/

The reason this is so important, is that there are people who host maliciously modified versions of these programs and will host legitimate looking sites to try and get you to download their version, which can install things like backdoors into your computers, keyloggers, and all types of nasty surprises. Sometimes developers will offer mirrors for their projects, which are simply just alternative links to download from in case the main server is too slow, or down. Sometimes these mirrors can become compromised without the knowledge of the developers.

Maybe you do not have TOR or Tails on your laptop and you are traveling out of the country and the hotel that you are staying at has TOR's homepage blocked. There are times when you may need to find an alternative mirror to download certain things. Then of course there is the infamous **man-in-the-middle** attack where an attacker can inject malicious code into your network traffic and alter the file you are downloading. The TOR developers have even reported that attackers have the capability of tricking your browser into thinking you are visiting the TOR home page when in fact you are not.

So what do you do about it? You can verify that the file you downloaded is in fact legitimate. The best tool for this is **GnuPG**. The TOR developers recommend you get it from the following page (Windows Users).

http://www.gpg4win.org/download.html

You can install this program on your USB drive or on your actual computer, you will hear your actual computer's operation system referred to as your Host OS. So download it, run it, install it and we will start showing you how to use GnuPG.

If you remain on the GnuPG download page you will see something under the big green box that is called **OpenPGP signature**. Download that into the same folder as the GnuPG file, this is the file that the download was signed with. Basically someone's signature saying, I made this file. And you also need a PGP public key to verify the signature. So to sum it up so far, the signature is created from the PGP private key, and can be verified by the PGP public key. The signature file is used to verify the program itself. So let us grab the PGP public key for GnuPG as well.

If you look on the same download page, under the heading Installation, you will see a link

where it says **verify** the integrity of the file. It will lead to you the following page.

http://gpg4win.org/package-integrity.html

Note where it says the following statement. **The signatures have been created with the following OpenPGP certificate Intevation File Distribution Key (Key ID: EC70B1B8)**. This is the link to the page that hosts the PGP public key file that you need to download, go there. On the page we just navigated to, go to the bottom right where it says **Intevation-Distribution-Key (public OpenPGP key for signing files)** and download that file. This is the PGP public key file, save it to the same place as your signature file for ease of use.

Okay, now that we have both the signature file and the PGP public key, let us now verify our download. First thing you need to do is navigate to the PGP public key file, called **Intervation-Distribution-Key.asc**, right click it and go to **More GpgEX Options** and down to **Import Keys**. This will import the PGP public key into your key ring, and now you can verify the file with the signature.

Right click your actual file you want to verify, in this case **gpg4win-2.2.1.exe** and go to **More GpgEX Options** and down to **Verify** and it should automatically detect the signature file where it says Input File, but if it does not, navigate to the signature file and make sure the box below it where it says **Input file is a detached signature** is checked. Look at the bottom and click Decrypt/Verify and you will likely get the following message.

Not enough information to check signature validity. Check details.

Believe it or not, this is completely fine. Click on show details, you are looking for a specific result.

Signed on 2013-10-07 08:31 by distribution-key@intervation.de (Key ID: 0xEC70B1B8). The validity of the signature cannot be verified.

If you navigate back to the page from Gpg4Win that says **Check Integrity** where you found the link to the page that contained the PGP public key, you will see on that page.

Intevation File Distribution Key (Key ID: EC70B1B8)

Note the key ID from your decrypt result and the key ID from the Check Integrity page and note the email address ending in the same URL that we downloaded the PGP public key from. We have a match! I will explain the reason for this warning message later.

Now that we verified that our verification program is legit. Let us try and verify our Tails ISO file, since if we have a compromised Tails OS, then nothing we do will be anonymous. Let us get right to the Tails download page.

https://tails.boum.org/download/index.en.html

Scroll down to where it says Tails 0.22 signature and download that to your Tails folder where you have the ISO file that we already downloaded. Next scroll down to where it says Tails signing key, this is our PGP public key. Exact same procedure, import the key,

then click Verify and specify the signature file if it has not already been specified for you, exact same settings and you will get the same warning message. As explained by Tails

> *"If you see the following warning:*
>
> *Not enough information to check the signature validity.*
> *Signed on … by tails@boum.org (Key ID: 0xBE2CD9C1*
> *The validity of the signature cannot be verified.*
>
> *Then the ISO image is still correct, and valid according to the Tails signing key that you downloaded. This warning is related to the trust that you put in the Tails signing key. See, Trusting Tails signing key. To remove this warning you would have to personally sign the Tails signing key with your own key."*

In other words, you need to basically promise that the PGP public key you downloaded is safe by signing the PGP public key with your own private key, but we do not really need to do that and I will not be including a tutorial on how to do that. Tails explains that if you are worried about a compromised PGP public key, just download the key from multiple sources and compare them, if they all match, it is a good chance you are using a legit PGP key. Now let us finally move on to TOR because this one will be a little less straight forward, but once you do this one, you should be able to figure out how to verify anything. Navigate to their download page and find the package that you want.

https://www.torproject.org/download/download.html.en

To keep things simple let us choose Tor Browser Bundle 3.5, and under the orange box you will see a link **(sig)**. This is the link for the signature file, I hope by now you know what to do with it. Next we need the PGP public key right? Well it turns out that with so many developers working on TOR, there are multiple PGP public keys, and certain bundles were signed with different keys than other bundles. So we need to find the PGP public key that belongs to our Tor Browser Bundle. Check out this page.

https://www.torproject.org/docs/signing-keys.html.en

It has a list of all the signing keys that they use and you can certainly use these key IDs to get what we want by simply right clicking on the signature file and click verify. You will get a warning.

Not enough information to check signature validity. Show Details

And in details it will say the following warning.

Signed on 2013-12-19 08:34 with unknown certificate 0x416F061063FEE659

Keep this entire number in mind for later, it is called a fingerprint. But for now if you just compare the last 8 digits to Erinn Clark's key ID (**0x63FEE659**) provided on the above page, and since she is the person who signs the Tor Browser Bundles you will see they match. But we want to be a bit more thorough, never settle for mediocrity.

Go to your task bar in Windows, and find the program called **Kleopatra**, it looks like a red circle with a small white square in it. Right click it and go to **Open Certificate**

Manager. We are going to import the full keys using this manager. Also note, if you go to the tab that says **Other Certificates** you will find the Tails and Intevation (GnuPG) keys we used earlier stored for the future when you need to download a new version of those programs and verify them again.

We are going to be following the instructions from the **verifying signatures** page on the TOR Project website. Feel free to follow along from that page so you know what I am talking about and where I am getting my URL and numbers from.

https://www.torproject.org/docs/verifying-signatures.html.en

In order to import keys, we need to first add an online directory where they are stored. So let us first add the online directory where the PGP public keys are stored according to the TOR website. Click **Settings** then **Configure Kleopatra**. Next, click New and we are going to enter the following URL which I took right from the page above. **pool.sks-keyservers.net**, and leave everything else as default and click OK.

Finally, click the button that says **Lookup Certificates On Server** and we will be searching for Errin Clark's PGP public key by searching for her **fingerprint** provided on the TOR website page called **Verifying Signatures** above, remember, she is the developer who signs the Tor Browser Bundle. The fingerprint we are entering is **0x416F061063FEE659**, does this number look familiar? It should, it is the number we got back the first time we tried verifying but without the actual PGP public key. if you get any warnings that pop up when searching just click OK and it should bring up Errin Clark's key, select it and click **Import**. You should now have her key listed under **Imported Certificates**.

Now let us go back and verify that signature one more time and see what happens. You should get something like the following.

Not enough information to check signature validity.

Signed on 201-12-17 12:41 by errin@torproject.org (Key ID: 0x63FEE659).
The validity of the signature cannot be verified.

TOR also explains this warning message in their words in case you are still not happy with the warning message.

> *"Notice that there is a warning because you haven't assigned a trust index to this person. This means that GnuPG verified that the key made that signature, but it's up to you to decide if that key really belongs to the developer. The best method is to meet the developer in person and exchange key fingerprints."*

I do not know about you, but I am happy with the result here, and I am certainly not going to track down Erinn Clark to get her key fingerprint, and it looks like our TOR Browser Bundle is legitimate as well! Now you know what to do when the PGP public key file is not directly hosted on the site itself, you have no more excuses to not verify your downloads.

TOR CHAT

By now you should know that any type of messaging system is likely compromised or storing your data for an unknown period of time, and if you ever become a person of interest can be looked back upon for 5+ years.

This means things like Gmail, Hotmail, Yahoo Mail, Skype Messaging, Facebook Instant/Private Message, Text Messages, and other forms of communication are all likely being monitored to some degree, at the very least logging the meta data. But you should always treat everything as if those who are monitoring it can read the content of the email as well.

We have talked about communicating with PGP, we have talked about using TOR and hidden services, and we have talked about good practices of OpSec. But some of us want to be able to instant message somebody else. The good news is; you can do this with something called **TorChat**.

TorChat is a decentralized anonymous instant messenger that uses Tor hidden services as its underlying Network, in other words it communicates over the Tor network through the .onion URL protocol. This provides **end to end encryption** that we talked about in previous posts. It provides cryptographically secure text messaging and file transfers for business dealings, and confidential communication between two people. The best news, is that you can use TorChat on your Windows, Linux and your smart phones. A French developer released a version for MAC users, but it still in beta and should be used at your own risk. You can get TorChat for the iPhone in the Apple store, you can get TorChat in the Android Market as well, so you can even use it as a means of text messaging somebody else who also has TorChat.

In TorChat, every user has a unique alphanumeric ID consisting of 16 characters. This ID will be randomly created by Tor when the client is started the first time, it is basically the .onion address of a hidden service. TorChat clients communicate with each other by using Tor to contact the other's hidden service. For example, the first time you open TorChat your computer might generate **d0dj309jfj94jfgf.onion** and from here on out, **d0dj309jfj94jfgf** will be your TorChat ID that you give out to people that you want to be able to message you. Here is the home page of TorChat.

https://github.com/prof7bit/TorChat
http://www.sourcemac.com/?page=torchat – MAC users

Unfortunately, at this time, TorChat does not run properly in Tails, so you will either need to run it on your Windows, Linux or MAC system. It is pretty straight forward, download it, unpack it and run it and everything else should happen automatically for you. Once the avatar beside your TorChat ID turns green, you are online and same with your contacts. You can add contains by right clicking and choosing Add Contact and just enter their TorChat ID.

At this time there is some people debate as to whether or not TorChat is completely safe, and I would say that TorChat is about as safe as Tor is, just make sure you practice the

same good practices you are used to. Do not give out personal information, if you are sending sensitive information use PGP encryption and so forth.

Here is another article on how TorChat works going into a little bit more detail. You can access it over the onion network.

http://kpvz7ki2v5agwt35.onion/wiki/index.php/Hacking_TorChat

OBTAINING, SENDING AND RECEIVING BITCOINS ANONYMOUSLY

We have talked about a large amount of ways to maintain your security, but we have not really talked about how to actually exchange currency. First thing I want to say as a disclaimer, is that I am not advocating that you do anything illegal. This is for educational purposes only and my recommendations are made assuming you are exchanging currencies anonymously as a means to protect your own privacy.

So you have found something online that you want to buy, and they are asking for Bitcoins as payment. How do you get the Bitcoins, and how do you get the Bitcoins to them? We are going to explore these options to a degree and hopefully by then you can make an educated decision on which method is best for your situation.

The options of buying Bitcoins are as follows.

1. **Sign up at an exchange online. Some popular exchanges are BTC-E, BitStamp and Coinbase**

   The downside of purchasing Bitcoins at these exchanges, are that you need to verify your identity with them by means of submitting documents such as a driver's license or passport and a utility bill. If you are able to get past this first obstacle, then you need to find a way to get money into the account. Exchanges generally only accept wire transfers as a way to fund your account, but some of them offer a way of transferring money directly from your bank account. You can obviously see that by doing this you are exposing your true identity to the exchanges in one way or another, if not at the very least your location.

2. **LocalBitcoins.com**

   LocalBitcoins offers a way for you to find a person in your local area, or if you want to go to another state or province to meet up with someone further away from you, you can choose where to look for people in that area selling Bitcoins either online (bank transfer or cash deposit) or meet them for cash in person. Traders have reputation lists, similar to a feedback score on eBay and you can find a trader who has a good reputation to buy off of. You send in a trade request and once the seller has received the money, he can release the Bitcoins from LocalBitcoins and they are sent to your wallet. Some people have expressed concern that law enforcement may act as buyers and sellers on LocalBitcoins, but it does not matter if this is the case in my opinion as long as you are not looking to buy large amounts. You can also, if you want, communicate with the buyer over email, arrive from public

transportation, wear a hat, and all sorts of secret agent type tricks to try and conceal your identity. Wear a wig if you are super paranoid.

3. **Use a Bitcoin ATM**

   Currently there is only one ATM in the world that I am aware of, and it is located in Canada. If you do not live in Canada, then this does not help you. Luckily according to an article, the company who is rolling out these ATMs called Robocoin is launching ATMs in other countries as well coming soon.

   http://techcrunch.com/2014/01/02/robocoin-the-bitcoin-atm-is-heading-to-hong-kong-and-taiwan/

   "The first shipping bitcoin ATM, Robocoin, is landing in Hong Kong and Taiwan as the company expands its reach this January. They are planning further releases in ***Europe, Canada, and the US*** *but, given Asia's clout in the BTC markets, this is definitely an interesting development."*

   There will likely be some way to try and cut down on money laundering by getting you to verify your identification, but from what I understand, they currently only do this if you are selling Bitcoins for cash using the ATM, and not buying them for cash. The way that it works, is you choose the amount of BTC you want to buy, and you feed your cash into the ATM machine. You can at that point either print out a generated paper wallet, or choose a wallet of your own to send the Bitcoins to. This method may be another good way because it takes dealing with another human out of the transaction. Something you may need to be aware of is surveillance cameras, so maybe wear a hood, hat, wig, sunglasses, and so forth to disguise yourself if you are worried about your identity.

4. **Craigslist**

   Believe it or not, there are a decent amount of people on Craigslist that you can meet up with in person and buy Bitcoins off of with cash. Your local area may not have a large number of listings, but you can always search in other nearby metropolitan areas and make a day trip out of it if you want. The same considerations about protecting your identity apply here as above.

5. **Mine your own Bitcoins**

   I am not going to get into how to mine Bitcoins, or whether or not you should, but if you want to get Bitcoins without dealing with other people, this is one of the ways you can do it. Run your miners over Tor, stay anonymous and you will have yourself some untainted Bitcoins.

Okay, so now you have yourself some Bitcoins, how can you get them to somebody else

that you want to buy something off of or trade with? As you probably know by now, every single transaction is tracked on **BlockChain.info**.

So you have Bitcoins sitting in your wallet, and if you send them to somebody else, it will show up on BlockChain exactly where you sent them. A couple of things to keep in mind.

1. You purchased your Bitcoins from somebody or something. They may have kept a record of the wallet those coins were sent to.
2. If you dealt with a law enforcement or somebody trying to track you, then they can track where the coins are sent after you forward them to somebody else.

Right now the best method of trying to lose this trail is using something called a mixer or a tumbler. You can think of this like throwing your Bitcoins into a giant pile of coins with other users and then withdrawing them at a later time from the mixer. If you threw in 1 Bitcoin and pulled out 1 Bitcoin, think of all the other people who did the exact same thing. Possibly thousands of others withdrawing 1 Bitcoin from the exact same pile of coins. It has now become much harder for you to be linked to those coins. Then on top of that, maybe you do not withdraw 1 Bitcoin, maybe you only withdraw 0.5 Bitcoin right now and leave the other 0.5 Bitcoin in the pile. It becomes even harder to link those Bitcoins to you.

One website that does this is called BitcoinFog and can be found on a clearnet URL and a hidden services URL.

http://www.bitcoinfog.com/
http://fogcore5n3ov3tui.onion/

BitcoinFog has been around for a while now and most people seem happy with the service they provide, so I would come to think that they are a trustworthy service. The way they work is as I mentioned above, and on top of that the service takes 1%-3% (randomized for obscurity) fee on each deposit. So you may put in 1.0 Bitcoins and take out 0.97 Bitcoin after fees and it mixes things up. You can also decide when you might want to withdraw it, whether it is in a month, week, days, and so forth. This is a good service to use and definitely mixes things up for you. The only thing you need to keep in mind, is that there is a trail of you sending your coins into BitcoinFog, which some people may or may not find suspicious. But what you do with your coins after BitcoinFog is going to be extremely difficult to track, if not impossible due to the vast number of transactions that are occurring in and out of BitcoinFog.

When you withdraw your coins from BitcoinFog, please make sure you send them to a **new** wallet, and not the same wallet that you used to deposit them into BitcoinFog. Another option you can have when withdrawing the coins from BitcoinFog, is to get BitcoinFog to withdraw the coins directly to the person you want to buy something from. This takes the step of creating a new wallet and then having to forward it on and will keep things again extremely hard to track. Just keep their transaction fees in mind to make sure your desired seller is going to receive the correct amount of Bitcoins needed for the purchase or exchange.

Two other options you can use are provided by Blockchain.info and can be accessed by

creating a wallet and logging in to it. **Send Shared** and **Shared Coin**. Send Shared is another way of mixing up coins, the way that it works is, you send your money into the giant pot and it gets matched up with somebody else who is sending the same amount. An example of this is let us say we have 4 people. A, B and X, Y. Person A is sending 1 Bitcoin to person B and person X is sending 1 Bitcoin to person Y. Send Shared will match these amounts together, and it will mix them so that person A sends their 1 Bitcoin to person Y and person X sends their Bitcoin to person B. This way you are breaking the chain that links person A to person B because there is no record of person A ever sending anything to person B. This is a very good option to use, and one that many people prefer. Of course, there are many people using Send Shared, so the likelihood of there just being 4 people mixing up transaction is going to be more like 10,000 or more, making it pretty much impossible to track.

Shared coin uses a different method called coinjoin. Shared coin hosts a coinjoin server which acts as a meeting point for multiple people to join together in a single transaction. Having multiple people in a transaction improves privacy by making transactions more difficult to analyses. The important distinction between traditional mixing services is the server cannot confiscate or steal your coins. A sharedcoin transaction will look something like the following.

https://blockchain.info/tx/e4abb15310348edc606e597effc81697bfce4b6de7598

As you can see multiple inputs and outputs make the determining the actual sender and receiver more difficult. Basically it sends the coins in and out of many different wallets that are participating in Shared coin at the time and it does this to throw hundreds or thousands of transactions in all the wallets participating making it extremely difficult to track. The downside though is that coinjoin can never completely sever the link between the input and destination address, there will always be a connection between them, it is just more difficult to analyze. The benefit to Shared Coin is that while this processing is happening, you can hit cancel and get your coins back. When you send your coins into a traditional mixing service, an untrustworthy mixing service could potentially steal your coins.

Now that you have the knowledge to make an educated decision on how to mix up your coins to your intended destination, I feel that you can now put your mind at ease when looking to buy something with Bitcoins.

THEY ARE WATCHING YOU – VIRUSES, MALWARE, VULNERABILITIES

Your computer will always be vulnerable to some sort of attack from those who want to harm you in some way. Whether it is harm your privacy, steal your information or throw you in jail.

It should come to no surprise to us that the US government is actually the largest purchaser of malware.

> *"According to a new report, the United States government is now in fact the single largest buyer of malware in the world thanks to the shift to "offensive" cybersecurity and is leaving us all vulnerable in the process.*
>
> *In order for the government to exploit vulnerabilities discovered in major software, they cannot disclose those vulnerabilities to the manufacturers or the public, lest the exploit be fixed.*
>
> *"My job was to have 25 zero-days on a USB stick, ready to go," one former executive at a defense contractor told Reuters. The defense contractor would purchase vulnerabilities from independent hackers and then turn them into exploits for the government to use as an offensive cyberweapon."*

http://endthelie.com/2013/05/10/report-us-government-now-buys-more-malware-than-anyone-else-in-the-world/#axzz2qIjeZ32e"

After reviewing the sources in the article and other articles, some of these defense contractors expressed concern that the government was essentially funding criminal activity. They are paying independent hackers, in some cases blackhats to find zero day exploits (ones that have not been publicly announced yet) and buy these exploits off of them for huge sums up money, upwards of $100,000.

If you are using a laptop with a built-in microphone and camera, you are extremely vulnerable to an attack as John McAffee, the man who started McAffee Anti-Virus explains.

> *""We don't have much [security] anymore, and certainly not in the online world," he said at Saturday's talk. "If you can give me just any small amount of information about yourself, I promise you, within three days, I can turn on the camera on your computer at home and watch whatever you're doing.""*

http://abcnews.go.com/Technology/john-mcafees-product-aims-make-internet-users-virtually/story?id=20424182

So the first thing you should do right now is go grab some opaque tape and put it over your camera. If you are on a desktop and you have a webcam plugged in, unplug it unless

you are using it. There is no reason to give an attacker an open window into your home. Next is your microphone, again desktops usually do not have built in microphones, but most laptops do. A microphone can be activated to listen to you talking and you need to find a way to physically disable it. The best way of course is to physically remove it, but I am not writing a tutorial on how to do that.

The FBI developed a keystroke logging software called Magic Lantern. Magic Lantern can reportedly be installed remotely, via an e-mail attachment or by exploiting common operating system vulnerabilities, unlike previous keystroke logger programs used by the FBI. It has been variously described as a virus and a Trojan horse. It is not known how the program might store or communicate the recorded keystrokes.

> *"The FBI intends to deploy Magic Lantern in the form of an e-mail attachment. When the attachment is opened, it installs a trojan horse on the suspect's computer.* ***The trojan horse is activated when the suspect uses PGP encryption, often used to increase the security of sent e-mail messages. When activated, the trojan horse will log the PGP password, which allows the FBI to decrypt user communications.***
>
> *Spokesmen for the FBI soon confirmed the existence of a program called Magic Lantern. They denied that it had been deployed, and they declined to comment further"*

https://en.wikipedia.org/wiki/Magic_Lantern_%28software%29

Then of course we have cell phones which can be activated remotely as well.

> *"Mobile phone (cell phone) microphones can be activated remotely, without any need for physical access. This "roving bug" feature has been used by law enforcement agencies and intelligence services to listen in on nearby conversations"*

https://en.wikipedia.org/wiki/Covert_listening_device#Remotely_activated_mc

According to a few of the sources in the Wikipedia article, the cell phone can be activated to listen to you even when it is off. Pulling the battery will likely do the job, but there is no guarantee. So make sure the phone is not in the same room as you if you are talking about anything sensitive. As always, be super paranoid. Turn on the shower and put the phone in the bathroom if you have to, or better yet if you are going somewhere and you do not need your cell phone, leave it at home. Since most people never leave home without their cell phones, if somebody is snooping on you, they might think you are still at home. The first group of people that went to visit Snowden in Russia were told not to bring any laptops or cell phones with them for those reasons.

So we know the government is actively trying to gain remote access to your computer, they can listen to your phones, what should you do about it?

You need to do the best you can to make sure the computers that you use are not exposed to the elements of risk. Always disable JavaScript when visiting any websites unless the website is 100% trusted. Start phasing out the use of Microsoft Windows and MAC OSX

because these closed source proprietary operating systems are not open to scrutiny and auditing the way open source Linux distributions are. There are more Windows users and thus more exploits available for Windows.

Running your operating system in a Virtual Machine, even if your host OS is Linux (remember Virtual Box can run on Linux) will help cut down on the retention of any malware you might pick up when on the internet. Do not go to any potentially harmful sites on your freedom fighting computers. Do not open any emails from anyone that you do not trust 100%. Regularly format your hard drives to keep them clean of any hidden viruses.

If you are unsure if something is safe, test it on a computer only meant for testing and one that is not connected to the internet. If you can reset your boot sector on your hard drive from time to time that would be a good idea as well, because you can get master boot sector viruses that would boot up a virus before your computer even boots into the OS.

Flash your BIOS, the BIOS is the first thing that runs when you turn on your computer, if you have a virus in your BIOS, there is no antivirus that can remove it, you would need to flash your BIOS and install a new firmware. Make sure the firmware is 100% trustworthy as infected firmware is the most common way to get a BIOS virus.

MONITORING YOU WITH AN ANTENNA

First thing I want you to do is find a secure way of watching this video. Remember they log everyone who watches these videos.

http://www.dailymotion.com/embed/video/x74iq0

This video shows how using a strong antenna, sitting in a van outside your home, the FBI could be picking up on your keystrokes on a **wired** keyboard. In fact, many people speculate that the new smart meters installed in many homes already have this technology to determine everything you are doing in your home electronically. Wired and wireless keyboards emit electromagnetic waves, because they contain electronic components. This electromagnetic radiation could reveal sensitive information such as keystrokes as shown in the video. Every electromagnetic wave is unique to the device using it, which gives a person spying on you the ability to tell the difference between you using your computer versus the dishwasher.

According to the people who did this experiment, they were able to extend the range up to 20 meters using relatively cheap technology. This was for wired keyboards by the way, and they go on to explain that wireless keyboards and mice are even easier. Which brings us to another area of interest, wireless transmissions. Things like wireless keyboards and wireless mice are vulnerable to eavesdropping as well. If they are not using a strong enough encryption to send data to the receiver, anyone can be listening in on your keystrokes and mouse activity. Probably something most people never thought about either, this is on top of the electromagnetic waves that can also be picked up.

> *"Microsoft has upgraded the weak encryption found on today's mass-market wireless keyboards with a new design that uses 128-bit AES to secure communication to and from the PC.*
>
> *Hitherto, keyboard encryption has been weak, with keys chosen from a small palette of possibilities,* ***with one hacking group claiming in 2009 that it had developed a tool specifically to sniff keystrokes from Microsoft keyboards at a range up to a 10 metres****."*

http://news.techworld.com/security/3284218/new-microsoft-wireless-keyboard-gets-128-bit-encryption/

Are you using wireless technology? How old is it? Might be time to upgrade your equipment. 10 meters is about 33 feet, but remember the technology available to the government could potentially reach beyond that. Then there are other things people forget such as wireless monitors which broadcast your screen to a receiver that can be picked up. Just think about the old antennas people used to have on top of their homes, and how far away those could pick up signals from TV stations, if you had one of those pointed at you in a van across the street, there is no doubt they could be eavesdropping on your activities

inside.

One researcher was able to use a wireless signal sent by a smart meter from up to 300 meters away (900 feet) to find out which house it was coming from and what the current power consumption was in plain text. She was then able to use this information to determine when people were and were not home based on average spikes in consumption since the meters pulse every 30 seconds.

> *"The data sent was in plain text and carried the identification number of the meter and its reading. The name of the home owner or the address aren't included, but anyone motivated enough could quickly figure out the source.*
>
> *"The meter ID was printed on the front of the meter we looked at, so theoretically you could read the ID [off a target meter] and try to sniff packets," Xu said.*
>
> *In her tests, Xu found she was able to pull packets out of the air from target meters between once every 2 to 10 minutes. That's fast enough to be able to work out the average power consumption of a house and notice start to deduce when someone is at home."*

https://www.networkworld.com/news/2012/110512-smart-meters-not-so-clever-263977.html

Things like automatic timers that flip switches might be worth investing in to always make it look like someone is home until security researchers start looking into ways to avoid the wide open door we are giving to anyone who wants to find data about us.

What can you do about these types of eavesdropping? Not a whole lot unless you want to start turning into a tin-foil hat type of person. There are some fun things you can do if you want to go crazy with it though as recommended by the following site.

http://www.lessemf.com/smart.html

> *"**Y-SHIELD***
>
> *YShield High Frequency Shielding Paint*
>
> *Easy to apply water-based paint for walls, ceilings, doors and other interior OR exterior surfaces. Very effective for blocking cell phone signals, CB, TV, AM, FM signals, radiofrequency radiation and microwaves. Tested highly effective up to 18 GHz!"*

http://www.lessemf.com/paint.html#290

There are lots of other things on there as well like drapes, curtains, garments, fabrics and so forth which disrupt the transmission of these signals. It is completely up to you what you want to do, I am just giving you the options and the education so you can make an educated decision of how far you want to go to protect your privacy.

COOKIES & JAVASCRIPT REVISITED, PLUS FLASH COOKIES AND OTHER BROWSER TRACKING

Your browser can reveal an alarming amount of information about you.

Surprisingly enough, or not too surprising, when you visit a website there is a surprisingly large amount of identifying data being sent to the website you are communicating with.

Cookies

Cookies are pieces of information that a web site can send to your browser. If your browser "accepts" them, they will be sent back to the site every time the browser accepts a page, image or script from the site. A cookie set by the page/site you're visiting is a "second party" cookie. A cookie set by another site that's just providing an image or script (an advertiser, for instance), is called a "third party" cookie.

Cookies are the most common mechanisms used to record the fact that a particular visitor has logged in to an account on a site, and to track the state of a multi-step transaction such as a reservation or shopping cart purchase. As a result, it is not possible to block all cookies without losing the ability to log into many sites and perform transactions with others.

Unfortunately, cookies are also used for other purposes that are less clearly in users' interests, such as recording their usage of a site over a long period of time, or even tracking and correlating their visits to many separate sites (via cookies associated with advertisements, for instance).

With recent browsers, the cookie setting that offers users the most pragmatic tradeoff between cookie-dependent functionality and privacy is to only allow cookies to persist until the user quits the browser (also known as only allowing "session cookies"). Tails does this automatically by the way with Iceweasel.

Recent Cookie-Like "Features" in Web Browsers

In addition to the regular cookies that web browsers send and receive, and which users have begun to be aware of and manage for privacy, companies have continued to implement new "features" which behave like cookies but which are not managed in the same way. Adobe has created "Local Stored Objects" (also known as "Flash Cookies") as a part of its Flash plug-ins; Mozilla has incorporated a feature called "DOM storage" in recent versions of Firefox. Web sites could use either or both of these in addition to cookies to track visitors. It is recommended that users take steps to prevent this.

Managing Mozilla/Firefox DOM Storage Privacy. If you use a Mozilla browser, you can disable DOM Storage pseudo-cookies by typing about:config into the URL bar. That will bring up an extensive list of internal browser configuration options. Type "storage" into the filter box, and press return. You should see an option called dom.storage.enabled.

Change it to “false” by right-clicking and choosing Toggle.

Managing Adobe Flash Privacy.

Adobe lists advice on how to disable Flash cookies on their website. **http://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-flash.html**. There are some problems with the options Adobe offers (for instance, there is no “session only” option), so it is probably best to globally set Local Stored Object space to 0 and only change that for sites which you are willing to have tracking you. On the Linux version of Adobe’s Flash plugin there does not seem to be a way set the limit to 0 for all sites and therefore its use should be limited or avoided. Luckily Tails does not have flash installed, but in case you are not using Tails be aware of this.

If you absolutely need to watch a video online, find a way to download the video to your computer and watch it that way. This takes the browser out of the loop of processing a video for you and eliminates those Flash cookies which help identify you.

JavaScript

JavaScript is probably the grand daddy of all vulnerabilities in internet browsing. The majority of exploits, malware, viruses and other computer take overs happen because of JavaScript code executing in your browser. JavaScript has many uses. Sometimes it is simply used to make webpages look flashier by having them respond as the mouse moves around or change themselves continually. In other cases, JavaScript adds significantly to a page’s functionality, allowing it to respond to user interactions without the need to click on a “submit” button and wait for the web server to send back a new page in response.

Unfortunately, JavaScript also contributes to many security and privacy problems with the web. If a malicious party can find a way to have their JavaScript included in a page, they can use it for all kinds of evil: making links change as the user clicks them; sending usernames and passwords to the wrong places; reporting lots of information about the users’ browser back to a site. JavaScript is frequently a part of schemes to track people across the web, or worse, to install malware on people’s computers. It is best to disable JavaScript (**about:config in URL bar search for JavaScript and Toggle it to disabled**) unless you absolutely trust the site or use the browser add-on NoScripts that comes with Tails and is available in Firefox to at least selectively block malicious scripts. Disabling JavaScript outright is the best option though.

Supposedly NoScript doesn’t block all Javascript even when it is enabled and no sites are on the whitelist. Not sure about that claim but I’ve seen people make it. **There’s a Firefox add-on (which also works in Tor Browser) called toggle_js which lets you toggle the about:config javascript.enable parameter through a toolbar icon so you don’t have to go into about:config**. I find it quite useful.

JavaScript can also reveal an alarming amount of information about you even if you are using TOR or a VPN, including your browser plug-ins, **your time zone**, what fonts you have installed (flash does this as well) and of course most browsers will send your user agent, meaning they tell the website what browser you are using and in some cases your operating system! Some of these details may not seem very important, but collected as a

whole, it can make it easier to identify who you are online by almost generating a finger print of you with your specific settings related to your browser. Then as you hop around from site to site with your finger print, correlations and patterns can be drawn from this and eventually linked to you if you are not extremely careful.

Luckily, Tails and Whonix overrides the majority of this identifying information, so as long as you use Tails with JavaScript disabled, or at the very least with NoScripts (Flash is disabled automatically) then you can cut down on the amount of information you share. Needless to say, it is not always possible to browse with Tails, so these are things you need to be aware of when you are browsing with regular browsers on your native OS with your browser of choice.

See what your browser is revealing about you at this page below. You may wish to search online for other sites that check what information your browser is revealing about you. If you are confident in your OpSec abilities, use the one below.

http://browserspy.dk/

A FEW RECOMMENDATIONS

Here are a few recommendations that may slip by the average user.

1. **Never leave your computer that you use for your freedom fighting unattended.** This may seem like a no-brainer, but if you have kids, or a spouse or a sibling that does not understand what you do on the computer and they decide to hop on your account and sign into their email, Facebook or doing things that could compromise your location while on that computer because they simply did not know, this could potentially cause you problems.

Maybe you are connecting through multiple layers like this TOR -> VPN(1) -> TOR -> VPN(2), so that is 4 layers and VPN(2) is the IP address that everyone sees. Then your child or spouse goes on to their email with that IP address, then signs off without your knowledge. That VPN is now linked to you. And we remember how when under pressure, companies will likely give out information about their customers to avoid fines, shut downs and prosecution.

2. **Do not tell your family members what you are doing, just instruct them not to touch your computer. Keep it passworded.** – You should never tell anyone what you are doing on your computer because if law enforcement ever did show up, they would question your family and friends about you. If they honestly do not know, then they cannot be held in contempt of court, so it is better to keep them in the dark. Or maybe the police might scare them into giving up all your secrets because they tell your family that if they do not confess that yourself and them will be going to jail, possibly for a long time. Just password your computer and never leave it unattended with the screen unlocked.

3. **If you use multiple layers to connect, make sure you regularly check to make sure all your layers are intact.** VPNs can drop sometimes without warning and while you should never set yourself up so that if one layer drops you lose everything, just keep in mind when one drops that you may need to adjust the way you handle yourself online until you get that next layer up. This is one of the reasons I like Tortilla so much, if my TOR layer does not work, it does not bypass it and go to my next layer, instead it just stops working altogether. When VPNs drop, your computer bypasses the dropped VPN and moves onto the next layer, which in some cases could be your real IP address. Just something to keep in mind.

4. **Do not use the same password for multiple forums, marketplaces, emails and so forth.** – Expect that one or more of the websites you are registered with is storing your password in plain text. This means that if somebody finds an exploit in the software and is able to dump the entire database, they can find your password. And if you used the same password for other sites, and god forbid with the same username as well, your entire list of accounts is compromised. Always use different passwords and keep them strong. Do not let anything about your password identify how you choose passwords, or identify anything personal about you.

COLD BOOT ATTACKS, UNENCRYPTED RAM EXTRACTION

Did you know that even if your system is whole disk encrypted, your data can still be extracted using something called a cold boot attack? Read on.

The first thing we need to talk about is RAM. RAM stands for random access memory. All you need to know about RAM is that RAM is the place in a computer where the operating system, application programs, and data in current use are kept so that they can be quickly reached by the computer's processor. RAM is much faster to read from and write to than the other kinds of storage in a computer, the hard disk, floppy disk, and CD-ROM. However, the data in RAM stays there only as long as your computer is running. When you turn the computer off, RAM loses its data.

When you turn your computer on again, your operating system and other files are once again loaded into RAM, usually from your hard disk. RAM can be compared to a person's short-term memory and the hard disk to the long-term memory. The short-term memory focuses on work at hand, but can only keep so many facts in view at one time. If short-term memory fills up, your brain sometimes is able to refresh it from facts stored in long-term memory. A computer also works this way. If RAM fills up, the processor needs to continually go to the hard disk to overlay old data in RAM with new, slowing down the computer's operation. Unlike the hard disk which can become completely full of data, RAM never runs out of memory.

Data can be extracted from the RAM using various tools. When you have a text document open and you are working on it, you are working from the RAM. Meaning that if you are working on a sensitive document, that document is temporarily stored in the RAM and is vulnerable to being extracted while the computer is on. When RAM is being stored, it is being stored **without** any form of encryption, making it very easy to steal and a huge security risk.

Shutting down a computer through its normal shutdown cycle usually goes through a process of clearing the RAM. However, if the computer loses power abruptly like in a power outage, the computer does not go through its normal shut down cycle and some information remains on the RAM chips for a few seconds up to a few minutes. This is one of the ways cold boot attacks can work.

I also want to quickly introduce a type of RAM to you which will help you understand the rest of this article better. Below is a research paper and they used a type of ram called DRAM. DRAM stands for **dynamic random access memory**. DRAM is the most common kind of random access memory (RAM) for personal computers and workstations. DRAM is dynamic in that, unlike static RAM (SRAM), it needs to have its storage cells refreshed or given a new electronic charge every few milliseconds. DRAM is designed to lose its memory quickly after losing power. Then there are subsections of DRAM called DDR. This is a way of making the memory more quickly available, but it is not really important to fully understand. Wikipedia can give you all you need to know about DDR.

In this article we are focusing on just the concept of DDR, DDR2 and DDR3.

These are newer versions of DRAM that keep getting better, and I believe we are currently up to DDR4. But most computers circulating around today have DDR2 and DDR3 in them unless they are older computers, this includes laptops. DRAM is known as a type of volatile memory; it is computer memory that requires power to maintain the stored information. It retains its contents while powered, but when power is interrupted, stored data is quickly lost. But how quickly is it lost?

In 2008, a group of researchers wanted to see the practicality of extracting unencrypted data from the RAM in your computer. They argued that DRAMs used in most modern computers retain their contents for seconds to minutes after power is lost, even at operating temperatures and even if removed from a motherboard. And by using an analysis tool they were able to search for key files (such as PGP keys) held in the RAM that could be used to decrypt encrypted volumes (drives) on your computer. They successfully were able to decrypt volumes using BitLocker, FileVault, dm-crypt, and TrueCrypt. Below is the abstract of their research.

> *"Lest We Remember: Cold Boot Attacks on Encryption Keys*
>
> *Abstract Contrary to popular assumption, DRAMs used in most modern computers retain their contents for seconds to minutes after power is lost, even at operating temperatures and even if removed from a motherboard. Although DRAMs become less reliable when they are not refreshed, they are not immediately erased, and their contents persist sufficiently for malicious (or forensic) acquisition of usable full-system memory images. We show that this phenomenon limits the ability of an operating system to protect cryptographic key material from an attacker with physical access. We use cold reboots to mount attacks on popular disk encryption systems — BitLocker, FileVault, dm-crypt, and TrueCrypt — using no special devices or materials. We experimentally characterize the extent and predictability of memory remanence and report that remanence times can be increased dramatically with simple techniques. We offer new algorithms for finding cryptographic keys in memory images and for correcting errors caused by bit decay. Though we discuss several strategies for partially mitigating these risks, we know of no simple remedy that would eliminate them."*

https://citp.princeton.edu/research/memory/ [Abstract] http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf [Full Text]

This was very troubling to most people, and had many people freaking out when the research paper was released back in 2008 because even tough encryption tools like TrueCrypt could be rendered useless with an attack like this. Upon further analysis of the paper, I wanted to note that they used SDRAM, DDR and DDR2, and not DDR3 because it was not available at that time. This prompted TrueCrypt to release the following statement on their website.

> *"Unencrypted Data in RAM*
>
> *It is important to note that TrueCrypt is disk encryption software, which encrypts*

only disks, not RAM (memory).

Keep in mind that most programs do not clear the memory area (buffers) in which they store unencrypted (portions of) files they load from a TrueCrypt volume. This means that after you exit such a program, unencrypted data it worked with may remain in memory (RAM) until the computer is turned off (and, according to some researchers, even for some time after the power is turned off). Also note that if you open a file stored on a TrueCrypt volume, for example, in a text editor and then force dismount on the TrueCrypt volume, then the file will remain unencrypted in the area of memory (RAM) used by (allocated to) the text editor. This applies to forced auto-dismount too.*

*Inherently, unencrypted master keys have to be stored in RAM too. When a non-system TrueCrypt volume is dismounted, TrueCrypt erases its master keys (stored in RAM). When the computer is cleanly restarted (or cleanly shut down), all non-system TrueCrypt volumes are automatically dismounted and, thus, all master keys stored in RAM are erased by the TrueCrypt driver (except master keys for system partitions/drives — see below). However, when power supply is abruptly interrupted, when the computer is reset (not cleanly restarted), or when the system crashes, TrueCrypt naturally stops running and therefore cannot erase any keys or any other sensitive data. Furthermore, as Microsoft does not provide any appropriate API for handling hibernation and shutdown, master keys used for system encryption cannot be reliably (and are not) erased from RAM when the computer hibernates, is shut down or restarted.**"*

To summarize, TrueCrypt cannot and does not ensure that RAM contains no sensitive data (e.g. passwords, master keys, or decrypted data). Therefore, after each session in which you work with a TrueCrypt volume or in which an encrypted operating system is running, you must shut down (or, if the hibernation file is encrypted, hibernate) the computer and then leave it powered off for at least several minutes (the longer, the better) before turning it on again. This is required to clear the RAM.

** Allegedly, for 1.5-35 seconds under normal operating temperatures (26-44 °C) and up to several hours when the memory modules are cooled (when the computer is running) to very low temperatures (e.g. -50 °C). New types of memory modules allegedly exhibit a much shorter decay time (e.g. 1.5-2.5 seconds) than older types (as of 2008).*
*** Before a key can be erased from RAM, the corresponding TrueCrypt volume must be dismounted. For non-system volumes, this does not cause any problems. However, as Microsoft currently does not provide any appropriate API for handling the final phase of the system shutdown process, paging files located on encrypted system volumes that are dismounted during the system shutdown process may still contain valid swapped-out memory pages (including portions of Windows system files). This could cause 'blue screen' errors. Therefore, to prevent 'blue screen' errors, TrueCrypt does not dismount encrypted system volumes and consequently*

> *cannot clear the master keys of the system volumes when the system is shut down or restarted.”*

http://www.truecrypt.org/docs/unencrypted-data-in-ram

A few key points to extract from here are that properly shutting down your computer reduces, if not completely eliminates this risk except in the case of encrypted system disks. What is meant by this is, for example, if your main operating system is Windows and you have encrypted that drive, this is your system drive and the master key for that drive is not cleared upon shutdown or restart. The solution is simply to never store anything sensitive on your system volume. Whether you use a partitioned drive or a USB stick that is encrypted, just make sure that your main drive that is booted into does not contain sensitive data. And if you have no other choice, then you need to separately encrypt the data inside the system volume with a different passphrase and private key so that even if they get into your system volume, they cannot access the other encrypted data you want to protect.

They can use these same techniques to sniff around for your PGP private key files in the RAM, so this is a very real threat in the case that if your computer is still powered on if they come to get you, they can use these techniques to retrieve data from your computer. However, there is a debate about whether or not this type of attack can persist even now into 2014 with newer types of RAM. I point to a random blog online and I make no judgement as to whether or not this is a legitimate claim, but it is interesting nonetheless.

> *“Now to test the actual cold-boot attack. Fill memory with around 1000 taint markers, just to be sure there are enough.*
>
> *Now shut down. Ostensibly, the markers could be recognizable in RAM after whole minutes, but I’m impatient, so I just waited 10 seconds for the first test. Boot up, into the minimal linux installation. Load the kernel module: insmod ./rmem.ko. Run hunter.*
>
> *Nothing.*
>
> *That’s ok, though. There should be at least some data corruption. The default marker size is 128 bytes, so let’s set the hamming distance to 128, meaning that one bit out of every byte is allowed to be flipped. (Statistically, that’s equivalent to a 25% corruption rate, since a corrupted bit has a 50% chance of remaining the same).*
>
> *Nothing.*
>
> *Looks like in 10 seconds, memory was completely corrupted. Let’s try a shorter interval: 2 seconds. Same results. Nothing is left of our “encryption key”.”*

http://bytbox.net/blog/2013/01/cold-boot-attacks-overrated.html

The user claimed to be using a newer type of RAM called **DDR3**. which is known to hold memory for a much shorter time than DDR2. And a newer research paper released in September 2013 tried to reproduce the findings of the 2008 research but using computers

with DDR1, DDR2 and DDR3 and their findings were interesting.

> *"Even though a target machine uses full disk encryption, cold boot attacks can retrieve unencrypted data from RAM. Cold boot attacks are based on the remanence effect of RAM which says that memory contents do not disappear immediately after power is cut, but that they fade gradually over time. This effect can be exploited by rebooting a running machine, or by transplanting its RAM chips into an analysis machine that reads out what is left in memory. In theory, this kind of attack is known since the 1990s. However, only in 2008, Halderman et al. have shown that cold boot attacks can be well deployed in practical scenarios. In the work in hand, we investigate the practicability of cold boot attacks.* ***We verify the claims by Halderman et al. independently in a systematic fashion. For DDR1 and DDR2****, we provide results from our experimental measurements that in large part agree with the original results.* ***However, we also point out that we could not reproduce cold boot attacks against modern DDR3 chips. Our test set comprises 17 systems and system configurations, from which 5 are based on DDR3."***

https://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6657268&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%

So what does should you do? Number one, always shut down your computer when you are not around it or put it into hibernation mode, otherwise your sensitive documents could be lingering around in your RAM. Simply locking the screen will do you no good. Make sure your computer is using a DDR3 type of RAM, if possible. Some of you this means you need to upgrade. If you are unsure what kind of RAM your computer has, search online to find a tool that will detect it for you. Never store anything sensitive on an encrypted **system** volume, because this attack can be used to break into the volume and anything unencrypted can be retrieved. If you are using a laptop, pull the battery out so that if you need to quickly pull the power, it will turn it off immediately. If you have time, shut down the computer, otherwise turn it off immediately so that it is not running. The more time you can waste are precious seconds where they cannot retrieve any data. So immediately shut things off if you do not have enough time to do a proper shutdown.

Consider putting a lock on your computer case, and if you want to go take it a step further, bolt it to the floor. That way the amount of time it would take them to get inside your computer would waste valuable minutes and more than likely render any recoverable memory useless. Some people have even suggested that you solder the RAM into the motherboard so they cannot take it out. This may help slow things down, but remember that cooling the memory down can preserve things for quite a while if you are using DDR1 or DDR2. With DDR3, you should be good to go and I believe with this realization, manufacturers will likely start looking at ways to encrypt RAM, but until that time you do need to be aware of this as a possible means for stealing your sensitive data and something you should keep in the back of your mind and prepare yourself for just in case.

THE STRENGH OF CRYPTOGRAPHY AND ANONYMITY WHEN USED PROPERLY

This chapter is meant to serve as an example of how, when cryptography and anonymity is used properly, you can evade just about anybody including the police.

By now, everyone has likely heard of someone getting locked out of their computer and being forced to pay by the attacker to have it unlocked, this is CryptoLocker. Dell SecureWorks estimates that CryptoLocker has infected 250,000 victims. The average payout is $300 each, and millions in laundered Bitcoin have been tracked and traced to the ransomware's money runners.

CryptoLocker is a ransomware trojan which targets computers running Microsoft Windows and first surfaced in September 2013. A CryptoLocker attack may come from various sources; one such is disguised as a legitimate email attachment. A ZIP file attached to an email message contains an executable file with the filename and the icon disguised as a PDF file, taking advantage of Windows' default behavior of hiding the extension from file names to disguise the real .EXE extension. When activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography to generate a 2048-bit RSA key pair, with the private key stored only on the malware's control servers.

The malware then displays a message which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid voucher) is made by a stated deadline, and threatens to delete the private key if the deadline passes. If the deadline is not met, the malware offers to decrypt data via an online service provided by the malware's operators, for a significantly higher price in Bitcoin.

Dell SecureWorks estimates that CryptoLocker has infected 250,000 victims. The average payout is $300 each, and millions in laundered Bitcoin have been tracked and traced to the ransomware's money runners. In November 2013, the operators of CryptoLocker launched an online service which claims to allow users to decrypt their files without the CryptoLocker program, and to purchase the decryption key after the deadline expires; the process involves uploading an encrypted file to the site as a sample, and waiting for the service to find a match, which the site claims would occur within 24 hours. Once a match is found, the user can pay for the key online; if the 72-hour deadline has passed, the cost increases to 10 Bitcoin.

To date, no one has successfully defeated CryptoLocker. The Swansea, Massachusetts police department was hit in November. The officers paid CryptoLocker's ransom. Police Lt. Gregory Ryan told press that his department shelled out around $750 for two Bitcoin on November 10. One of the reasons I am writing this, is that CryptoLocker uses 2,048 RSA encryption, and if you remember in the PGP section earlier in this book I recommended to use 4096. Even with 2,048-bit encryption, no one has successfully

defeated CryptoLocker, and this is the power of properly implemented cryptography.

And, using the proper methods of anonymity, this person or group has managed to acquire, according to research done by ZDNet, around 41,928 BTC.

http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/

> *"In research for this article ZDnet traced four bitcoin addresses posted (and re-posted) in forums by multiple CryptoLocker victims, showing movement of 41,928 BTC between October 15 and December 18.*
>
> *Based on the current Bitcoin value of $661, the malware ninjas have moved $27,780,000 through those four addresses alone – if CryptoLocker cashes out today.*
>
> *If CryptoLocker's supervillans cash out when Bitcoin soars back up to $1000, like it did on November 27… Well, $41.9 million isn't bad for three months of work."*

As you can see, properly executed cryptography and anonymity allowed this group of people to acquire the Bitcoin equivalent of almost $42 million in just now 4 months at the time of this writing. I am not recommending or advocating that you do this, but just giving you a perfect example of how powerful the combination of these two very important factors are in protecting anybody online when used properly.

HIDING TOR FROM YOUR ISP – PART 1 – BRIDGES AND PLUGGABLE TRANSPORTS

People are more worried about hiding their tor usage from their ISP, than hiding it from a VPN. There seems to be a back and forth debate about whether using a VPN will or will not protect you. Whether or not the VPN can be convinced to log your connection, and so forth. Those who rely on VPNs to protect them are historically known to end up in jail.

In my previous chapter about VPN -> TOR and TOR -> VPN, I tried to remain neutral in that you should be able to make your own decisions about how you wish to protect yourself. But just remember, at the end of the day, nobody is going to go to jail for you. If you simply want to hide the fact that you are using tor from your ISP, then we have other options than a VPN. We have bridges, and several different pluggable transports. What are these, and how can we use them in Tails?

> "**What bridges are and when to use them**
>
> When using Tor with Tails in its default configuration, anyone who can observe the traffic of your Internet connection (for example your Internet Service Provider and perhaps your government and law enforcement agencies) can know that you are using Tor.
>
> This may be an issue if you are in a country where the following applies:
>
> 1. Using Tor is blocked by censorship: since all connections to the Internet are forced to go through Tor, this would render Tails useless for everything except for working offline on documents, etc.
>
> 2. Using Tor is dangerous or considered suspicious: in this case starting Tails in its default configuration might get you into serious trouble.
>
> Tor bridges, also called Tor bridge relays, are alternative entry points to the Tor network that are not all listed publicly. Using a bridge makes it harder, but not impossible, for your Internet Service Provider to know that you are using Tor."

https://tails.boum.org/doc/first_steps/startup_options/bridge_mode/index.en.htr

The first thing we are going to do is get some bridges. Let us do this before we configure Tails to use bridges, because once Tails is in bridge mode, we will not be able to connect to tor without working bridges. So the first thing we want to do is visit the following webpage.

https://bridges.torproject.org/bridges

Enter the impossibly difficult captcha, and click "I am human", and you should get a list of bridges that look like this. These are actual bridges pulled from the tor bridges page.

“5.20.130.121:9001 63dd98cd106a95f707efe538e98e7a6f92d28f94
106.186.19.58:443 649027f9ea9a8e115787425430460386e14e0ffa
69.125.172.116:443 43c3a8e5594d8e62799e96dc137d695ae4bd24b2”

These bridges are publicly available on the Tor Project website, so they may or not may be the best choice to use, but they are a good start. Another option is to send an email to **bridges@bridges.torproject.org** with a message in the body saying “get bridges” without the quotes. This will only work if sent from a Gmail account or Yahoo, unfortunately. If you want to use this, set up the email account using tor and you will receive a list of around 3 bridges shortly thereafter. Save them somewhere you can use them the next time you boot up Tails, or write them down.

Ok, so now we have our bridges. How do we use bridges in Tails? This is an option we need to activate when we boot up Tails. To activate the bridge mode, we will be adding the **bridge** boot option to the boot menu. The boot menu is the first screen to appear when Tails starts. It is the black screen that says Boot Tails and gives you two options. 1. Live, 2. Live (Fail Safe). When you are on this screen, press Tab and a list of boot options will appear in the form of text at the bottom of the screen. To add a new boot option, add a Space then type “bridge” without the quotes and press enter. You have now activated bridge mode.

Once Tails boots up completely, you will get a warning that you have entered bridge mode and not to delete the default IP address in there, which is 127.0.0.1:*. This is advice we will follow, so just click OK and the settings window for tor will pop up. At this point you need to add your bridges. So you are going to take the three bridges you got, and enter the IP address and the port. If we were going to use the example above this is what we would enter.

“5.20.130.121:9001
106.186.19.58:443
69.125.172.116:443”

For each bridge you add, type it in the available text box where it says “Add A Bridge” and then click the green + button to add that bridge. You will need to add one bridge at a time. Once you are finished adding your bridges, you can click OK. At this point, your yellow tor onion icon in the top right should turn green shortly after and you will be connected to the tor network using a bridge. Again, since these bridges are less likely to be known by your ISP, they are less likely to know that you are using tor when you use bridges.

You may wish to look up your bridge before you use it however. Maybe you want to find out where your bridge is located, maybe you want to see who is hosting the bridge, and you can do this by looking for a IP look up service online, by doing a search and typing in the IP address. The three listed above are located in the following locations.

“5.20.130.121 – Country: Lithuania
106.186.19.58:443 – Country: Japan
69.125.172.116:443 – Country: New Jersey, United States”

And with that, you can decide which bridge would be a better choice for you to use. I suggest however, that you go and get new bridges and do not use the ones I listed above for obvious reasons. I should note that the way bridges hide the fact that you are using tor from your ISP, is that you are connected to an IP address that is likely not known to your ISP to be affiliated with tor entry nodes.

While bridges are a good idea, unfortunately they may not be enough. According to Jacob Applebaum, (a tor developer) bridge traffic is still vulnerable to something called DPI (deep packet inspection) to identify internet traffic flows by protocol, in other words they can tell you are using tor by analyzing the traffic. While tor uses bridge relays to get around a censor that blocks by IP address, the censor can use DPI to recognize and filter tor traffic flows even when they connect to unexpected IP addresses. This is less likely to be done by your ISP, and more likely to be done by the NSA, or other oppressive governments like in China and Iran, so you can choose if this is an issue for you.

> *"Lately, censors have found ways to block Tor even when clients are using bridges. They usually do this by installing boxes in ISPs that peek at network traffic and detect Tor; when Tor is detected they block the traffic flow.*
>
> *To circumvent such sophisticated censorship Tor introduced obfuscated bridges.* ***These bridges use special plugins called pluggable transports which obfuscate the traffic flow of Tor, making its detection harder."***

https://www.torproject.org/docs/bridges#PluggableTransports

Pluggable transports are a newer, but less talked about technology being implemented by tor to disguise the fact that you are using tor to your ISP and other censors. As mentioned above, it attempts to transform your tor traffic into innocent looking traffic that would hopefully be indistinguishable from normal web browsing traffic. Currently the most popular pluggable transports are obfuscated bridges. Obfuscation by definition, is the hiding of the intended meaning in communication, making communication confusing, willfully ambiguous, and harder to interpret. Obfuscated bridges actually transform the traffic to look like random packets of data. Obfuscated bridges currently have 2 protocols.

1. obfs2
2. obfs3

Obfs2 (The Twobfuscator) is talked about at length at the following official page.

https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/blob/HEAD:/doc/obfs2/obfs2-protocol-spec.txt

But for the layman out there, basically obfs2 uses a protocol that disguises your traffic to look like random data, whereas tor has a more distinct structure to it. However, it should be noted in the case of obfs2, that if an attacker sniffs the initial handshake between your computer and the obfuscated bridge, they could get the encryption key used to disguise your traffic and use it to decrypt the disguised traffic which would reveal it as tor traffic. They would not be able to decrypt your tor traffic, but they would be able to see you are using tor. This is not likely something your ISP would do, but it may be something law

enforcement or the NSA would do. So if you are only worried about your ISP, then obfs2 would likely suffice.

Obfs3 (The Threebfuscator) is talked about at length at the following official page.

https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/blob/HEAD:/doc/obfs3/obfs3-protocol-spec.txt

Obfs3 uses a very similar protocol to disguise your traffic as obfs2, however it uses a more advanced method of an initial handshake called the Diffie Hellman key exchange. They however found some vulnerabilities in the protocol and had to go a step further and customize the Diffie Hellman key exchange to make it an even more robust method of establishing that initial handshake. Using obfs3 would be a better bet to disguise your traffic if your adversary is the NSA or other law enforcement.

So how do you get these obfuscated bridges? They are not as easy to get, but they can be obtained from tor through email. However, you need to request those bridges specifically to get them. You need to use a Gmail or Yahoo account and send an email to bridges@bridges.torproject.org and enter in the body of the email “transport obfs2” without the quotes, and for obfs3, simply enter “transport obfs3”. Please note that you can only send one request to tor per email, every 3 hours. Which one you should use, is entirely your choice, I am just giving you the information necessary to make an informed choice. Enter them in this format so that Tails knows which protocol to use.

obfs3 83.212.101.2:42782
obfs2 70.182.182.109:54542

tor also provides a few obfuscated bridges on their home page which you can use as well, and I will list them below. If you send a request to tor and get a response containing bridges without obfs2 or obsf3 at the beginning of the lines, then these are normal bridges, not obfuscated, and they are likely to be out of obfuscated bridges at the moment. You will have to try again another day. So if you get a response with bridges that are without obfs2 or 3 at the beginning of each line, please again, be aware these are normal bridges, unlike the ones below.

obfs3 83.212.101.2:42782
obfs3 83.212.101.2:443
obfs3 169.229.59.74:31493
obfs3 169.229.59.75:46328
obfs3 209.141.36.236:45496
obfs3 208.79.90.242:35658
obfs3 109.105.109.163:38980
obfs3 109.105.109.163:47779
obfs2 83.212.100.216:47870
obfs2 83.212.96.182:46602
obfs2 70.182.182.109:54542
obfs2 128.31.0.34:1051
obfs2 83.212.101.2:45235

I have a feeling that some of you reading this will be inclined to go out and get yourself some obfs3 bridges right away, because you think they are the best choice out there for staying anonymous. And right now they have the potential of being what you hope for in that regard, except for one huge flaw. The number of obfs3 bridges is small. Last report I read put it at around 40 bridges running obfs3, and obfs2 was around 200. So while obfs3 is the most secure option out there, its limited number of available bridges would pool you into a smaller group of people making connections to the 40 available bridges and may not provide any more anonymity for you. tor is in desperate need of more obfs2 and obfs3 bridges at this time and these factors should be taken into account when using obfuscated bridges.

One of the solutions to this shortage problem, is to run your own obfuscated bridge. I am not going to go into it, but if you are interested in doing this, you should visit the following page to set up an obfuscated proxy, or better yet, purchase a few VPS and set them up as obfs2 or obfs3 proxies. One of the best things about doing it this way, is that you can configure it (with the instructions provided) to be a private obfuscated bridge, and therefore tor will not give it out to the public. You can then connect to your own private obfs3 bridge. You can also use a friend's computer, or use a server that you know is secure. But again, make sure that you trust the computer you are using, otherwise it is no more secure than a VPN.

Another possible solution to the lack of obfuscated bridges may be another pluggable transport option, something called a **flash proxy**. This is brand new and not perfectly implemented yet, and please be aware that this is basically still in beta. When thinking about a flash proxy, think about the characteristics of a flash, quick and short lived. This protocol was developed by a tor developer who attended Stanford University, and the idea is that the IP addresses used are changed faster than a censoring agency can detect, track, and block them. This method is similar to using normal bridges, in that, it hides the fact you are connecting to IP addresses known to be related to tor, including when the bridge's IP addresses listed by tor are discovered by your ISP or law enforcement. **This does not however, hide the fact you are using tor if somebody is analyzing your traffic using DPI (deep packet inspection).**

The main benefit to this option is that the proxies are run by many people all over the world. They are run when random internet users visit a webpage with a specific plugin that turns their browser into a proxy as long as they are on that page. You are basically using somebody else's connection through their browser to connect to a tor relay. You are only using 1 active connection at any time, but you have around 5 established connections to different proxies in case your active connection drops off, then you can start using another proxy in its place. Below is another explanation of how this process works.

> *"In addition to the Tor client and relay, we provide three new pieces. The Tor client contacts the facilitator to advertise that it needs a connection (proxy). The facilitator is responsible for keeping track of clients and proxies, and assigning one to another. The flash proxy polls the facilitator for client registrations, then begins a connection to the client when it gets one. The transport plugins on the client and*

relay broker the connection between WebSockets and plain TCP. (Diagram below)"

https://crypto.stanford.edu/flashproxy/arch.png

A sample session may go like this:

1. The client starts Tor and the client transport plugin program (flashproxy-client), and sends a registration to the facilitator using a secure rendezvous. The client transport plugin begins listening for a remote connection.
2. A flash proxy comes online and polls the facilitator.
3. The facilitator returns a client registration, informing the flash proxy where to connect.
4. The proxy makes an outgoing connection to the client, which is received by the client's transport plugin.
5. The proxy makes an outgoing connection to the transport plugin on the Tor relay. The proxy begins sending and receiving data between the client and relay.

In other words, you end up going from your computer, to the proxy, then the proxy to the tor relay.

The whole reason this is necessary is because the client cannot communicate directly with the relay. (Perhaps the censor has enumerated all the relays and blocked them by IP address.) In the above diagram, there are two arrows that cross the censor boundary; here is why we think they are justified. The initial connection from the client to the facilitator (the client registration) is a very low-bandwidth, write-only communication that ideally may happen only once during a session. A careful, slow, specialized rendezvous protocol can provide this initial communication. The connection from the flash proxy to the client is from an IP address the censor has never seen before. If it is blocked within a few minutes, that's fine; it wasn't expected to run forever anyway, and there are other proxies lined up and waiting to provide service.

I know this might be a bit complicated, but you really do not need to understand how it works to benefit from it. You also might be asking about somebody just blocking your ability to connect with the facilitator (the supplier of the proxies). But, the way you actually connect to the facilitator is in a very special way that tor has designed, and this is built into the flash proxy pluggable transport. This explanation is just for your comfort, not to help you make it work.

> *"The way the client registers with the facilitator, is a special rendezvous step that does not communicate directly with the facilitator, designed to be covert and very hard to block. The way this works in practice is that the flash proxy client transport plugin makes a TLS (HTTPS) connection to Gmail, and sends an encrypted email from an anonymous address (nobody@localhost) to a special facilitator registration address. The facilitator checks this mailbox periodically, decrypts the messages, and inserts the registrations they contain. The result is that anyone who can send email to a Gmail address can do rendezvous, even if the facilitator is blocked."*

https://trac.torproject.org/projects/tor/wiki/FlashProxyFAQ

Two questions you should be asking. 1) Can I trust the proxies, and/or facilitator? 2) How do I use this?

Well, the facilitator is chosen and currently only run by tor, so you can take that at face value. As far as the proxies go, the proxies themselves may or may not be trustworthy, and this is the risk you run every time you use tor. Your bridges that you use may be compromised, your entry nodes, your exit nodes, every single possible hop along your way to the internet can be compromised at any given time. Luckily, even if the proxy is compromised and logging your traffic, they are only going to be able to see encrypted tor traffic. And as I mentioned above, anybody who visits a webpage with a specific plugin on it, becomes a flash proxy as long as they are on that site. This means, some people will be a flash proxy without their knowledge, and others will be flash proxies because they want to be one. The idea behind this is to have multiple users, tens of thousands, if not hundreds of thousands of flash proxies available at all times to increase the number of possible IP addresses you rotate between to keep your ISP and possibly the NSA guessing.

So do you use this? **It actually currently is not supported in Tails.** But it can be used with Tor Pluggable Transports Tor Browser Bundle outside of Tails. You can get it at the following page and it will run on your normal operating system, whether it is Windows, MAC, or Linux. Get the package at the following page.

https://www.torproject.org/docs/pluggable-transports.html.en#download

Next follow the following tutorial, which is pretty straight forward and has pictures of exactly what you need to do, and will probably do a better job than I would at explaining how to set it up.

https://trac.torproject.org/projects/tor/wiki/FlashProxyHowto

Essentially it comes down to, enable port forwarding for port 9000, add “bridge flashproxy 0.0.1.0:1” without the quotes, to your torrc, and leave everything else alone unless you need to use a different port, which is unlikely. You may need to make an exception in your firewall for the flashproxy plugin if it asks you. As long as you are using the Tor Pluggable Transports Tor Browser Bundle, it should be pretty easy to get this feature working. But until Tails adds support for it, this is the only option you have if you want to use flash proxy bridges.

Ok, so you have a lot of information right now and maybe are left a bit confused, but read over this one a few times and try to extract as much out of it as possible at once. Try setting up normal bridges, then try doing the obfuscated bridges, and once you get those working, then maybe consider doing the flash proxies if you are okay without using Tails. Tails will likely implement support for this later. Ask yourself some questions, do I just want to hide the fact that I am using tor from my ISP? Or am I hiding from somebody much bigger than that?

Consider whether it is plausible for you to run a private obfuscated proxy, or even a private bridge. Hopefully now you have enough information to make an informed decision.

Currently there are other pluggable transports currently under developed, but not yet deployed. Here is a list of upcoming projects.

> *"**ScrambleSuit** is a pluggable transport that protects against follow-up probing attacks and is also capable of changing its network fingerprint (packet length distribution, inter-arrival times, etc.). It's part of the Obfsproxy framework. See its official page. Maintained by Philipp Winter.*
> *http://www.cs.kau.se/philwint/scramblesuit/*
> *Status: Undeployed*
>
> ***StegoTorus** is an Obfsproxy fork that extends it to a) split Tor streams across multiple connections to avoid packet size signatures, and b) embed the traffic flows in traces that look like html, javascript, or pdf. See its git repository. Maintained by Zack Weinberg.*
> *https://gitweb.torproject.org/stegotorus.git*
> *Status: Undeployed*
>
> ***SkypeMorph** transforms Tor traffic flows so they look like Skype Video. See its source code and design paper. Maintained by Ian Goldberg.*
> *http://crysp.uwaterloo.ca/software/SkypeMorph-0.5.1.tar.gz*
> *http://cacr.uwaterloo.ca/techreports/2012/cacr2012-08.pdf*
> *Status: Undeployed*
>
> ***Dust** aims to provide a packet-based (rather than connection-based) DPI-resistant protocol. See its git repository. Maintained by Brandon Wiley.*
> *https://github.com/blanu/Dust*
> *Status: Undeployed*
>
> ***Format-Transforming Encryption (FTE)**transforms Tor traffic to arbitrary formats using their language descriptions. See the research paper and web page.*
> *https://eprint.iacr.org/2012/494*
> https://kpdyer.com/fte/
> Status: Undeployed
>
> *Also see the unofficial pluggable transports wiki page for more pluggable transport information.*
> *https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports"*

Source: https://www.torproject.org/docs/pluggable-transports.html.en

CAPABILITIES OF THE NSA

I wanted to share a 1-hour video by one of the tor developers Jacob Applebaum.

He talks about legitimate, confirmed capabilities of the NSA from FOIA leaked documents showing just how technically capable the NSA is. Anywhere from simple backdoors, flying a drone over top of your house to sniff packets, mold injecting backdoor chips into your computer case, to beaming energy into your house. None of this is conspiracy theory, it is all confirmed with documents shown in his presentation.

The video can be watched on YouTube using HTML5 embedded instead of flash at the following page.

https://youtu.be/vILAlhwUgIU

BITCOIN CLIENTS IN TAILS – BLOCKCHAIN AND ELECTRUM

In this chapter I want to talk about 2 options for trading your Bitcoins.
#1 – Blockchain
#2 – Electrum

By now, hopefully you know how to use BlockChain. If not, you simply go to http://blockchain.info and press the button “Wallet” and you can open up your existing wallet or create a new account. Very straight forward and can be done all from your web browser.

But what about Electrum? Electrum is an easy to use Bitcoin client. It protects you from losing coins in a backup mistake or computer failure, because your wallet can be recovered from a secret phrase that you can write on paper or learn by heart. There is no waiting time when you start the client, because it does not download the Bitcoin blockchain. If you use the normal Bitcoin client from https://bitcoin.org then you would need to download the entire blockchain, which is several GB of data. In Tails, we are trying not to download too much to our computers. Downloading the entire BlockChain can take over 24 hours.

So how do we set up Electrum in Tails? First thing we need to do is download it.

https://download.electrum.org/Electrum-1.9.7.tar.gz

Now extract it (right click -> Extract here) and rename the folder to electrum to make things easier. (Right click -> Rename). You might also want to move the folder to the **tmp** directory so it is easier to find. (Places -> Computer -> File System -> tmp)

Next open up a terminal and type the following command

cd /tmp/electrum

You can replace /tmp/electrum with whatever directory electrum is currently in, but this is why we put it in tmp, to make things easier for us. Next type the following command.

./electrum -s 56ckl5obj37gypcu.onion:50001:t -p socks5:localhost:9050

This will allow your electrum to connect through Tor, to make sure it does not connect over clearnet. You will get a warning when you do this that electrum is attempting to connect in an unsafe manner, but this is expected, and do not worry, it is safe to do this. This step was recommended on the Tails web page at the following URL.

https://tails.boum.org/forum/Report:_the_electrum_bitcoin_client_in_tails/

Since you are likely going to want to reuse your wallet that is generated in Electrum, you can specify where your wallet is kept by replacing the above command with the following command.

./electrum -s 56ckl5obj37gypcu.onion:50001:t -p socks5:localhost:9050 -w

/tmp/electrum.dat

You would replace /tmp/electrum.dat with whatever the path to your wallet is, and you can rename **electrum.dat** to whatever you want to call your wallet, like **srwallet.dat** or whatever you want. Or leave it the way that it is. Then each time you want to start up electrum, reuse the same command, and make sure you copy electrum.dat into **/tmp** or whatever directory you wish to use. Then when you are finished, make sure to back up electrum.dat onto your USB drive or SD card, especially if you do not have Tails persistence. This way you can reuse the same wallet and you will not lose your balance.

Electrum is likely going to be the Bitcoin client of choice for Tails users. And you can read more about how to use Electrum by visiting the home page at the following link.

https://electrum.org

Conclusion

I hope this book was able to teach you exactly how to remain anonymous on the internet through the use of Tor. There are many different reasons for which you may wish to have your identity remain anonymous. Sometimes it might seem a little challenging to cover all the bases and make sure you don’t make any mistakes, but remember to always stay up to date on the latest bug releases and never stop looking for more knowledge as the tech world is always changing. Better paranoid and safe than lazy and sorry.

I want to thank you again for downloading this book and I wish you the best of luck in your endeavors.

James Smith