Security and Anonymity in the Digital Age.

1. Introduction
2. Getting Started
3. The Tor Network
4. VPNs and Proxies
5. Media Access Control (MAC) Addresses
    5.1 Changing MAC Address On Windows
    5.2 Change MAC Address On Linux
    5.3 Change MAC Address On Mac OS
6. Domain Name System (DNS) Leaks, What Are They?
7. Some Key Points Regarding Tor
8. Better than Tor: Tails
9. Do Not Use Google
10. Delete Tracking Data Regularly
11. Download CCleaner
12. Use Linux
13. Take Precautions With Your Email
14. Creating Fake Accounts
15. Protonmail
16. Use Bitcoin
17. Use Secure Passwords
18. Do Not Use Compromised Websites
19. Get a Hard Drive Encryptor
20. Social Media
21. Using A Virtual Box

APPENDIX 1: Anti Forensics
    A1.1 Disabling Time Stamps

APPENDIX 2: Encrypting Your Computer
    A2.1 Making Encryption Secure
    A2.2 Disabling Windows Hibernation
    A2.3 Disable and Remove USB Logs
    A2.4 Windows Security Misc
    A2.5 Do Not Get Found In The First Place

APPENDIX 3: Useful Resources
    A3.1 End Note and TL;DR

Important Note
This document is an edited version of a file produced in 2015.
No content has been changed, other than grammatical corrections.
PLEASE, for your own safety, confirm that the software and security measures listed in this document are still secure in Current Year+X.

1. Introduction (see final page for TL;DR)

Good OPSEC is vital for any activist regarded as a 'subversive element of society', but especially for those involved with the digital information war, who pose a real threat to the global System.

The System is often portrayed by the media as being all-powerful, able to imprison you for life by magically logging where you last shoved a USB stick. In reality, hackers are always ten steps ahead of the security agencies that are working for the police and government organizations. However, the System does actively spy on *all* of its citizens, and takes a special interest in surveilling nationalists and other troublesome political dissidents.

This simple guide is written for a beginner and should be accessible even to the most technophobic among us. This is NOT a guide on hacking, but a guide to securing the privacy of your computer systems on all levels. It is possible to be (almost) totally anonymous on the internet, and it is possible to secure your data from any prying eyes, anyone who says otherwise is misleading you.

It is absolutely imperative that you regard cybersecurity with the utmost seriousness, not just for your own sake but for the sake of your friends, allies and fellow dissidents.

Loose lips sink ships.

2. Getting Started

The best place to begin is the *basic entry units* aka what you're using to access the internet. This is hardware such as your computer or laptop, and software such as the operating system (OS), Windows, Mac or Linux. Your first line of defense is a firewall, we assume that your computer already has one installed (check if this is the case). Familiarize yourself with the basics of your hardware and OS.

According to research conducted via hacker forums, approximately 90% of individuals are caught because:

1) They use Windows.

2) They don't anonymize and encrypt their traffic (they don't use an IP masking proxy, or better yet a VPN).

By ‘traffic’, we mean the flow of information from the internet to their computer and vice versa. The best way to easily encrypt this traffic is with a software tool called Tor.

3. The Tor Network

www.torproject.org

Tor is a free and an open network that helps you defend against *traffic analysis*, a form of network surveillance.

Tor protects you by bouncing your communications around a network of relays run by volunteers all around the world. This prevents anyone who’s spying on your internet connection from learning which sites you visit, as well as preventing the sites you visit from learning your physical location. Tor operates in the same manner as a VPN, by changing or masking your IP.

Tor alone will not 100% protect you from surveillance; getting the *HTTPS Everywhere* browser extension, or the *Tor Browser Bundle* (which includes HTTPS everywhere), will ensure encryption throughout. HTTPS prevents hackers from stealing your information at ‘exit nodes’ by *encrypting* (locking/jumbling) the data. You don't really need to know what an exit node is or how it works.

Tor TL;DR: your location and site usage are masked.

HTTPS TL;DR: data is locked/jumbled for extra protection.

4. VPNs and Proxies

VPNs and Proxies are very different concepts, though people sometimes get the two mixed up.

Proxy

Proxies are similar to VPNs but do not encrypt traffic. They are less secure but work great for basic browsing. Proxies are often free or cheap, opposed to VPNs, which usually cost money.

Foxy Proxy is a common, usually reliable proxy. Keep in mind that both VPNs and proxies will slow down your traffic, since the data has to travel much further than normal (remember how Tor worked?). Free/cheap proxies are generally a bad idea if you wish to completely secure your browsing: https://blog.haschek.at/post/fd9bc

VPN

http://en.wikipedia.org/wiki/Virtual_private_network

A VPN (Virtual Private Network) is an end-to-end encrypted tunnel. *Private Internet Access* and *TorGuard* are good VPNs which do not keep user records (helping to protect you from government requests). A good VPN will often allow you to send your data through almost any country in the world, which is useful for accessing any government-banned websites. Anyone can set-up a VPN for free. For Linux a *PPTP protocol* is a simple, good choice.

5. Media Access Control (MAC) Addresses

MAC addresses are often overlooked when it comes to computer security. Every network interface on your computer, and any networked devices, will have a unique MAC address. For example, a typical laptop will have both Wi-Fi and a wired ethernet port, and each of these will have a unique MAC address, even though they both connect your machine to the internet.

These MAC addresses are assigned in-factory, but you can change, or “spoof,” MAC addresses via software. MAC addresses are also commonly referred to as *physical addresses* or *hardware addresses*, because they correspond to a hardware adapter.

Mac addresses are used for:

Device Identification

Many airport Wi-Fi networks and other public Wi-Fi networks use a device's MAC address to identify it. For example, an airport Wi-Fi network might offer a free 30 minutes and then ban your MAC address from receiving more Wi-Fi. Change your MAC address and you could get more Wi-Fi (Free, limited Wi-Fi may also be tracked using browser cookies or an account system).

Device Tracking

Because they're unique, MAC addresses can be used to track you. When you walk around, your smartphone scans for nearby Wi-Fi networks and broadcasts its MAC address. A company named Renew London used trash bins in the city of London to track peoples' movements around the city based on their MAC addresses. Apple's iOS 8 uses a random MAC address each time it scans for nearby Wi-Fi networks to prevent this sort of tracking.

Static IP Assignment

Routers allow you to assign static IP addresses to your computers. When a device connects, it always receives a specific IP address if it has a matching MAC address.

5.1 Changing MAC Address On Windows

Most network cards will allow you to set a custom MAC address from their configuration panes in the Device Manager, although some network drivers may not support this feature.

First, open the Device Manager: on Windows 8.1, press Windows Key + X and click Device Manager; on Windows 7, press the Windows key, type "Device Manager" to search for it, and click Device Manager.

Locate the network interface you want to modify under Network Adapters, right-click it, and select Properties

Click the Advanced tab and select Network Address in the list.

If this option isn't visible, then your network driver does not support the feature.

Enable the Value option and enter your desired MAC address without any separating characters — don't use dashes or colons.

Click OK.

5.2 Change MAC Address On Linux

Modern Linux distributions like Ubuntu typically use Network Manager, which provides a graphical way to spoof a MAC address.

For example, on Ubuntu, click the network icon on the top panel, click Edit Connections, select the network connection you want to modify, and click Edit. On the Ethernet tab, enter a new MAC address under "Cloned MAC address", then save your changes.

5.3 Change MAC Address On Mac OS

Mac OS X's System Preferences pane displays each network interface's MAC address, but doesn't allow you to change it. You can do so with a single command.

Open a Terminal window (press Command + Space, type Terminal, and press Enter.) Run the following command, replacing en0 with the network interface's name and filling in your own MAC address.

The network interface will generally be either en0 or en1, depending on whether you want to configure a Mac's Wi-Fi or Ethernet interface. Run the ifconfig command to see a list of interfaces if you're not sure of the appropriate network interface's name.

As on Linux, this change is temporary and will be reset when you next reboot. You'll need to use a script that automatically runs this command on boot if you'd like to permanently change your Mac address.

You can verify your change took effect by running a command that shows your network connection details and checking what MAC address your network interface reports afterwards. On Windows, run the ipconfig /all command in a Command Prompt window. On Linux or Mac OS X, run the ifconfig command.

If you need to change the MAC address on your router, you'll find this option in your router's web interface.

The standard format for printing MAC addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order (e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab).

6. Domain Name System (DNS) Leaks, What Are They?

When using an anonymity service, it is important that all the traffic originating from your computer is routed through the anonymity network. If any traffic leaks outside the secure connection, anyone monitoring your traffic will be able to log your activity.

DNS is used to translate domain names such as www.egg.com into numerical IP addresses (e.g. 123.123.123.0), which are required to route packets of data on the internet (send your data from A to B).

Whenever your computer needs to contact a server on the net, when you enter a URL into your browser for example, your computer contacts a DNS server and requests the IP address. Most internet service providers assign their customers a DNS server which they control and use for logging and recording your internet activities.

Under certain conditions, even when connected to the anonymity network, the operating system will continue to use its default DNS servers instead of the anonymous DNS servers assigned to your computer by the anonymity network.

DNS leaks are a major privacy threat since the anonymity network may be providing a false sense of security while private data is leaking.

To check for DNS leaks when using Tor or other VPNs go to **dnsleaktest.com** and run either the standard or extended test. The results displayed will detail how secure your connection is. It is also

useful if you think someone is monitoring your traffic (through spyware etc).

Running a leak test on Tor etc will take quite some time, given how much your traffic is routed around. However, **the URL below*** lays out it simply. It is safe to say Tor Browser and TorGuard VPN are often secure against such DNS leaks.

*** http://torguard.net/vpn-dns-leak-test.php**

Tor VPN can be purchased here:
http://torguard.net/anonymoustorrentvpn.php

7. Some Key Points Regarding Tor

Do Not Torrent Over Tor

Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor. Even if your torrent application connects only through Tor, you will often send out your real IP address in the tracker GET request, because that's how torrents work. Not only do you deanonymize your torrent traffic and your other simultaneous Tor web traffic this way, you also slow down the entire Tor network for everyone else (noteworthy during times when multiple dissidents will be using it).

Do Not Enable Or Install Browser Plugins

The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy. The lack of plugins means that Youtube videos are blocked by default, but YouTube does provide an experimental opt-in feature that works for some videos.

Use HTTPS Versions Of Websites

Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser Bundle includes HTTPS Everywhere to force the

use of HTTPS encryption with major websites that support it. The “s” after HTTP means that the website traffic is encrypted with the SSL protocol, making the traffic more secure. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, **include https:// in the URL**, and display the proper expected name for the website. Additionally, see EFF's interactive page explaining how Tor and HTTPS relate.

Do Not Open Documents Downloaded Via Tor While Online

The Tor Browser will warn you before automatically opening documents that are handled by external applications. DO NOT IGNORE THIS WARNING. You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.

Use Bridges And/Or Find Company

Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them.

There’s also a Tor app for Android mobile, known as Orbot.

8. Better than Tor: Tails

Tails is a ‘Live’ operating system which is built from the Linux Operating System (as opposed to Mac or Windows). You can start it

on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

1) Use the Internet anonymously and circumvent censorship; all connections to the Internet are forced to go through the Tor network.
2) Leave no trace on the computer you are using unless you ask it explicitly.
3) Use state-of-the-art *cryptographic tools* to encrypt your files, emails and instant messaging.

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc. Tails is the equivalent of buying a computer and then throwing it away every time you use the internet. It's pretty secure.

9. Do Not Use Google

Google are sneaky little merchants who keep records of everything to make more money and appeal to their overlords.

When you search something in Google, it usually sends search terms to that site and your browser data and computer info. These sites thus build up a profile of you, and will bombard you with ads. **Your online profile can also be sold.**

Google, being a tool of the paranoid and power obsessed System, also saves all search histories of users. These search histories can be legally requested:

"Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to hand over user data. In this report, we disclose the number of requests we receive from each government in six-month periods with certain limitations. Usage of our services have increased every year, and so have the user data request numbers.

We continue to look for new ways to organize information and provide more detail. For example, starting with the July-December

2010 reporting period, we began to disclose the percentages of user data requests we comply with in whole or in part. And starting with the January–June 2011 reporting period, we began to disclose the number of users or accounts about which data was requested.

Our FAQ about legal process provides information about how we aim to put users first when we receive user data requests. To learn more about the laws governing our disclosure of user data and reforms to those laws that we think are important, visit http://digitaldueprocess.org/. We hope this report will shine some light on the appropriate scope and authority of government requests to obtain user data around the globe."

- Google

10. Delete Tracking Data Regularly

Your browser keeps track of where you go, what you type, and any other data it can capture about you. A basic security measure is to regularly delete this data (history, cookies and cache).

11. Download CCleaner

This scrubs your hard drive, internet search history, cache and cookies squeaky clean, as well as containing other features. Highly recommended and 100% free: https://www.piriform.com/ccleaner/download (you can buy the Premium version for around $30, and it's pretty based).

12. Use Linux

Micro$oft is one of the greediest, cuckold corporations out there, and should be avoided and boycotted at all cost avoid purchasing anything from them, and avoid using any technology that uses their software or operating system. Windows is also notoriously unsafe, given most viruses are designed to infect Windows operating systems, since they make up the majority of personal computers.

Microsoft provide an entry key for the police which bypasses all Windows password encryption.

Linux is generally considered to be one of the most secure operating systems, it has a slight learning curve but soon becomes second nature. Linux is probably the best thing you can use when it comes to securing online privacy and computer protection. Ubuntu is the best place to begin.

13. Take Precautions With Your Email

Use secure email services when you can. Use a dummy email address when emailing people you do not trust and make sure that that dummy email is not attached to any of your real information (use a fake name, age, etc). You can also set up emails to reroute, so that you can receive them at your normal address - just make sure that you reply from the dummy account.

This is not particularly secure against government agencies but it is fairly secure against hackers. There are also free, disposable, temporary email services, such as Guerilla Mail, that allow users to create randomly generated accounts that get automatically deleted once the user ends their browser session, or after a time limit.

14. Creating Fake Accounts

http://www.fakenamegenerator.com

When it comes to making dummy accounts, Fake Name Generator is a great site to use. The site creates a wealth of fake information, from name and address, to email and eye color. It even generates social security numbers and other realistic criteria.

15. Protonmail

https://protonmail.ch/

Proton Mail is an up and coming anonymous email provider which was developed by researchers at CERN. It uses state of the art cryptography and a cast iron promise that employees are unable to

access your data. Given Swiss laws, it is also notoriously difficult for agencies to request information from companies, nigh on impossible. It is recommended that Protonmail is used by any and all serious Nationalists.

16. Use Bitcoin

Bitcoin is a largely untraceable form of currency which has gained a lot of attention in the last year or two. Not every website accepts it, but for the websites that do, this can be a great way to help protect your identity when making purchases.

17. Use Secure Passwords

www.identitysafe.norton.com/password-generator

Use secure passwords which use at least 8 characters, uppercase letters, lowercase letters, numbers, and characters. Never use dictionary words in your password, either. Do use different passwords for every site you have an account with, if possible. Change your passwords frequently (monthly is good practice). And don’t write all your passwords down in a jotter, for someone to find. Some security sites have password safes, which come in handy.

18. Do Not Use Compromised Websites

Don't use any untrustworthy sites, or click on emails from unknown addresses. Be wary of porn and file sharing websites, as they’re notoriously infected. (You shouldn’t be browsing porn websites anyway, Mr. Goldstein & friends are sapping your Vital Essence).

19. Get a Hard Drive Encryptor

These are pretty useful gadgets when they're not being made by Window$. *Truecrypt* used to do the trick, but it was

abandoned by the author and is untrusted in many circles. However, the project has been taken up by developers and is now back up and running. An audit of version 7.1a indicated that it was safe. This is thanks to open source, which allows transparent reading of source code and further development. Practically every Jewish owned information company has been explicitly anti-open source, which is interesting. A search for hard drive encryptors should yield a good set of alternatives.

20. Social Media

Facebook, being the ZOG tool that it is, is growing less and less fond of user privacy. However, if you absolutely must use it, there are safety precautions you can take;- it all depends on how much info you put on there about yourself.

21. Using A Virtual Box

While Linux might prove a challenge for some, it's security credentials cannot be underestimated. Given that most viruses and spyware are built for Windows systems, having a Linux computer makes intrusion much more difficult. Linux is also free from the myriad of backdoors Windows creates for the authorities. The pros of using Linux are almost endless.

One excellent way of getting the security boost of Linux and easing the learning curve is by running a Windows Virtual Box, also referred to as a Virtual Machine within a Linux system (you can do the opposite too - run a Linux VB in your Windows computer to get used to using it without installing Linux straight away).

Virtual Machines have been used in this way by hackers and cyber security activists with great success.

Step 1: Download Virtual Box
https://www.virtualbox.org/wiki/Downloads

Step 2: Learn How To Run It
https://www.virtualbox.org/manual/UserManual.html

APPENDIX 1:
Anti Forensics

Anti-computer forensics (sometimes *counter forensics*) is a general term for a set of techniques used as countermeasures to forensic analysis.

Anti-Forensics is the art of leaving no trace on your computer. It is combating common forensic tools in preventing any penetration for forensic tests on your computer. It can pretty much be summed up with one famous quote: **“Make it hard for them to find you, and impossible for them to prove they've found you.”**

Because Linux installations are pretty much already secured, this guide will only focus on Windows. Windows is a security nightmare, and we strongly advise getting to grips with, and downloading, a Linux OS. VPNs, proxies, and Tor only get you so far, but what do you do when they've traced it to your computer?

This guide is designed to help you prevent them from proving you've done anything wrong even if they have your computer.

A1.1 Disabling Time Stamps

Using Time Stamps, forensic experts can build a 'digital time-line', this can be very compelling evidence when cross-referenced with other known evidence. In order to strengthen security, we must disable these logs.

Step 1: User Assist File

There is a registry setting that keeps logs and dates of all launch programs, forensic experts can use this to build a digital timeline, we must disable this for computer security. Navigate to:

HKEY_Current_User\Software\Microsoft\Windows\Currentversion \Explorer\User assist

(Do this by hitting the Windows button on your keyboard and R at thesame time and typing regedit in For Windows 8, this guide is invalid. Answer? Don’t use Windows 8 - or do some research yourself).

You should see two subkeys called Count, delete both these keys. Now right-click the UserAssist key and create a new key named 'Settings'. In this key (right clicking on it) create DWORD value named NoLog, set the value to 1. Windows will no longer store hidden logs of the exact times you have been accessing files, therefore forensics experts can no longer use these hidden logs to create a digital timeline.

Step 2: Last Access Logs

Next, we will disable the last access in Windows. What last access is a setting on Windows that allows you to see when you opened, modified, and/or created files on your computer and is similar to the UserAssist registry key. By disabling this, forensic experts won't as easily be able to tell when you've been accessing programs or files on your computer.

To disable last access open command prompt on your computer, if on Vista or Windows 7 make sure to run as administrator. In command prompt type the following:

```
fsutil behavior set disablelastaccess 1
```

Last access has now been disabled, in order for it to take effect you must restart your computer. (You have to have admin rights to do this).

APPENDIX 2:
Encrypting Your Computer

It is very important to make sure that your computer is encrypted. Any unwanted visitors attempting to breach your computer will not be able to gain access if it is correctly encrypted.

Step 1: Open-Source Disk Encryption

To encrypt your computer, you can use hard drive encryptors. This is also very secure, but you may be forced to give up your password due to court-order (In this situation, if you are a VERY good liar, you could simply say 'I forgot', but you would have to make it believable- according to time frames, this can work. If say, you are arrested and bailed and the police do not come to you for a month or more, then turn up demanding the password, you can simply say your forgot- and inwardly relish in their frustration).

TrueCrypt 7.1a

A good tool to use for encryption is TrueCrypt. Whilst the developers abandoned the project, TrueCrypt is opensource, meaning future generations can develop and implement it further. TrueCrypt devs now recommend BitLocker as an alternative, but Bitlocker is a Microsoft creation, and will no doubt have backdoors for police investigators. The latest iteration of TrueCrypt, which stands up to security tests is 7.1a.

Step 2: Encrypt Your Keystrokes

You need to protect yourself from keyloggers. As strange as it may sound even the government has keyloggers, a few years ago the law speculation about CIPAV, a government spyware known to send the users IP address, MAC address, open ports, operating system, installed applications, default web browser, visited URLs, logged in user, etc.

In order to protect yourself from keyloggers, you should encrypt your keystrokes. You can do this using a software called 'Keyscrambler'. Please note, you should NOT use the free version of Keyscrambler, you should only use the Premium version, which costs a decent sum of money. Or get it off a torrent site i.e kat.ph, thepiratebay.se etc.

Keyscrambler Premium supports 170 programs, including windows logon, most web browsers, and popular IM programs (i.e. Skype). Keyscrambler Personal works as a browser extension for Firefox and IE.

A2.1 Making Encryption Secure

Encryption is pointless if it can be easily bypassed or overcome. You need to make sure that the encryption is secure too.

Step 1: Make Sure Your Password Is Strong

Even with your computer encrypted, it is still vulnerable. Make sure your password is good (for optimal security, your password should be twenty or more characters, with symbols, numbers, and random capitals, and a special symbol, like ALT+1456, to really increase security). Norton password generator is great for this.

Step 2: Make Sure Your Password Is Strong

This may seem obvious, but all this is pointless if you get infected with a keylogger that takes screen shots. Having a good anti-virus is one of the most important things you can do. You should consider McAfee, BitDefender, ESET, Nod32 and Kaspersky. Advance System Care Ultimate is good too. In theory, you rarely even need anti-virus software when using Linux, as most viruses are built to infect Windows systems, given these make up the majority of computers, but it's best to be safe. Especially if using a Linux tailored to end users, such as Ubuntu or Mint.

All anti-virus programs are expensive, but for the other anti-virus you can torrent them from i.e Kat.ph, ThePirateBay.se, or one of your choice. Just make sure you find one with a lot of seeders and read the comments. Also Malwarebytes Pro is a must.

A2.2 Disabling Windows Hibernation

You may as well hand your computer over to the feds if they raid your house and your computer is in hibernation. Also, putting your computer into hibernation is pretty much just taking a screen shot of

your RAM that gets saved to your hard drive.

To Disable Hibernation In Windows Vista/7:
Open your Control Panel. Click System and Security, then click 'Power Options'. Click 'Change plan settings' for your current power plan. Now click 'Change advanced power settings'. Expand 'Sleep', then expand 'Hibernate After'. Enter “0" for 'Setting:' to set hibernate to 'Never'. Hibernation is now disabled.

A2.3 Disable and Remove USB Logs

Next on the list of Anti-Forensics in to disable logs of USB activity, flash drives, etc. This can be valuable if you have a flash drive with sensitive data and you don't want any logs of it ever being plugged it to your computer.

Step 1: Delete the USBSTOR Registry Setting
The USBSTOR setting contains history of plugged in USB devices. To delete it, hit the WINDOWS Home Button + R at the same time. This will open up 'Run'; type: "Regedit" (without quotes). Browse to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

Now, right click 'USBSTOR' and hit 'Delete', then confirm that you want to delete the key. Now, the key has been deleted.

Step 2: Delete The Setupapi.log File
The Setuppapi.log is a plain-text file that stores the list of installed USB devices and their drivers. We will delete it with a program called CCleaner. CCleaner is actually one of the best anti-forensic tools out there and it’s free.

Download for free from this site;
https://www.piriform.com/ccleaner/download

A2.4 Windows Security Misc

For things related to windows anti-forensic security, but not big enough to warrant their own section. That does NOT mean this section isn't important, **the stuff in here may actually be the most important in the whole guide**.

Step 1: Disable System Restore Points

System Restore points can be used to bring your computer back to a date when it wasn't secure and can also be used to restore overwritten files. To disable System Restore points, right click 'Computer' and click 'Properties'. Now click 'Advanced System Settings'. Under 'System Protection' click 'Configure'. Now, select 'Turn Of System Protection' and apply it.

Step 2: Disable 'Send Error Report to Microsoft

This is self-explanatory, we obviously don't want Microsoft having logs of all our crashed programs. To do this, go to your start menu and search 'problem reporting settings' and then click on 'Choose How To Report Problems'. Click 'Change Report Settings For All Users' and then set it to 'Never check for solutions'.

Step 3: Wipe With CCleaner

This is the heart of Anti-Forensics right here. CCleaner is actually one of the most powerful Anti-Forensic tools, -IF- used correctly.

As it turns out, when deleting files, you DO NOT need to do multiple overwrites. With modern hard-drives, one overwrite really is enough to delete a file beyond repair, even though it is a popular belief that you need several overwrites to be secure.

With CCleaner, we recommend three overwrites, just in-case it misses something the first time around (remember, it is a free software).

Once you have CCleaner installed, run it (AS ADMIN), go to 'Settings' and make sure you have it set to overwrite deleted data with three passes. Go back to 'Cleaner' and check EVERYTHING. Hit 'Run Cleaner'. You might want to leave this on overnight.

Do this every time you are done with a major hacking job. When using normally (what should be every time you are done with your computer), uncheck 'Wipe Free Space', this will cut down the time from hours to a few minutes.

Step 4: Disable Debugging Upon Failure

This keeps logs of your computers failures and blue screen info. To disable it, right click 'Computer' and go to 'Advanced System Settings', now go to 'Start Up and Recovery'. Now, set 'Debugging Information' to 'None'.

Step 5: Disable Windows Event Logging

Windows keeps logs of all events on the computer. First, before we disable, we must clear all the logs. To disable it, go to Control Panel then System and Security. Now, click Administrative Tools, and then Event Viewer. In either pane of the Event Viewer window, right-click System and then select Clear All Events, you will get a window that says: "Do you want to save 'System' before clearing it?", click 'No'. Now we must disable Windows Event Logging. Go to 'Run' and type in 'msconfig', then go to 'Services' and make sure 'Hide all Microsoft Services' is UNCHECKED. Now scroll down until you find 'Windows Event Logging', and UNCHECK it. Now restart your computer right away.

A2.5 Do Not Get Found In The First Place

You should never be tracked in the first place. Follow these guidelines to stay anonymous:

1) Use Tor or Tails for web browsing you wouldn't want the Police, or your ISP looking at.
2) Never release personal information online and use different aliases. Never connect ANY real information to your hacking alias. Build fake information if you are paranoid. fakenamegenerator.com might help with this.
3) Don't get lazy, be patient.

APPENDIX 3:
Useful Resources

A few useful links and resources.

https://www.eff.org/
Electronic Frontier Foundation site

https://www.us-cert.gov/ncas/tips
United States Computer Emergency Readiness Team

http://iag.me/tech/10-tips-to-make-your-computer-more-secure/
10 Handy Tips

http://en.wikipedia.org/wiki/Computer_security
Good Wiki article

https://www.sans.org/tip_of_the_day.php
Security Awareness Tips

https://ssd.eff.org/en/playlist/activist-or-protester
A guide for activists and protesters created by the Electronic Frontier Foundation.

https://ssd.eff.org/en/playlist/online-security-veteran#introduction-public-keycryptography-and-pgp
An EFF guide to PGP

https://techtoolsforactivism.org/
Site containing a wealth of resources. Very useful. The list of software and media is especially helpful.

http://www.gimp.org/downloads/
Gimp Image software. Just as good as Photoshop, but free.

https://fakeinbox.com
No prizes for guessing what this is.

https://privnote.com
Self-destructing temporary notes.

https://disconnect.me
Browser add-on for filtering and preventing online tracking.

https://identitysafe.norton.com/password-generator
Random password generator (gives tips on creating strong passwords)

http://www.fakenamegenerator.com/
Generate an entire fake id. Excellent for fake forms etc.

http://www.datafakegenerator.com/
Generate not only name, address etc. but credit card details too.

http://www.whatsmyip.org/
Self-explanatory. Tor usually covers this problem, but always safe to double check and see what your ip is. The site also contains great tools you'll learn about in time, including DNS leaks and stuff.

https://www.torproject.org/projects/torbrowser.html.en
Excellent VPN, contains built in: browser, proxy routed, https everywhere, tons of privacy features. Saves a lot of time.

After you install Tor, you can enter 'the deepweb' aka the darknet.
Here is a list of deepweb addresses:
http://deepweblinks.org/

A3.1 End Note and TL;DR

Send this PDF to anyone who may find it useful. Educate your friends and allies on the necessity of good cybersecurity, and ensure you’re always up to date on how to keep yourself safe and secure.

Don’t get vanned.

TL;DR
- Use Tor
- Get AntiVirus
- Try using Linux
- Use Truecrypt
- Use Keyscrambler
- Use Protonmail
- Use CCleaner
- Get a Tails stick
- Do your homework