The 2023 Cyberpunk Dystopia Almanac

By: runick

Contact: runick@fastmail.com

Public Key:

https://keys.openpgp.org/vks/v1/by-fingerprint/019483E1FD3302997FEF03A6ACA86A050621698D

Date: June 2022

Table of Contents

Introduction.....**6**
Financial and Doxxing Protection.....**8**
Credit Freeze.....8
Credit Cards.....9
Cypto Currencies.....10
Major Crypto Currencies.....10
Crypto Exchanges.....12
Alternative Means of Buying Crypto.....13
Crypto Wallets.....14
Personal Data Removal.....19
File Metadata Removal.....20
Images.....20
Office Documents.....25
PDFs.....26
Passwords and Account Management.....**28**
Creating Passwords.....29
Password Managers.....31
2FA.....32
Software Options.....33
Hardware Tokens.....34
Recap.....34
E-mail and RSS.....**36**
E-mail Client Configuration.....36
Initial Setup.....37
Organization and Spam.....37
Remote Content.....38
Disable JavaScript.....39
DKIM and Authentication.....39
Encryption.....44
RSS.....46
Finding RSS feeds.....47
Web Browsing.....**50**
Browser Configuration.....50
uBlock Origin.....52
Alternative Front Ends.....58
Search Engines.....63
Coping with Slow Internet.....64
Backups.....**68**
Versioning.....69
Image Backups.....73
Windows.....74
Linux.....76
Multiple Hard Drives.....77
RAID.....77
Android.....**80**
Ad Blocking.....81

Keyboard....82
Encryption....82
Backups....83
Encryption....84
Asymmetric Versus Symmetric....84
Key Versus Password....84
File Encryption....85
Disk Encryption....86
Verifying Signatures....87
VeraCrypt....91
Sanitizing Disks and Data....96
Properly Deleting files....97
Wiping Entire Disks....99
Windows Configuration....101
O&O ShutUp!....101
Windows De-Bloat Script....103
Proxies, VPNs, Encrypted DNS and Tor....105
Proxies....105
VPNs....107
Encrypted DNS....108
Tor....109
Information Search, Archiving and Sharing....111
Advanced Search....111
Bypassing Paywalls....114
Academic Papers....114
Newspapers, Magazines, etc....114
Archiving....117
Saving Single Webpages....117
Downloading YouTube Videos....119
Downloading Websites....123
Cache Recovery....124
Windows....124
Linux....127
File Sharing....131
Anonymous File Sharing Services....131
Torrents....132
Non-Computer Stuff....135
Economics....135
Transportation....137
Advice for New Mechanics....142
Sewing....151
Security....152
Securing the Home....152
Non-Firearm Weapons....154
Firearms....158
Spouses and Other Family Members....167
Misc Resources....170
APPENDIX....172
Command Line Interface....173

Path Variable....174
Privacy Drama....**180**
Law Enforcement....180
Advertising....181
Honeypots....182
Linux....**185**
Distros and Desktop Environments....188
Paralysis by Analysis....192
Keyboard Shortcuts....**194**
General....194
Text Editing....195
Web Browsing....196

Introduction

This originally started as a beginner guide to online privacy and security, but quickly grew in scope into more intermediate territory; as well as I couldn't resist the urge to throw in some miscellaneous computing tips here and there for things that weren't relevant for either privacy or security. Ultimately I decided to give functional computer and Internet skills the same priority as privacy and security. So you can think of this document as a crash course in the computer skills you should've been taught in school or as a guide to becoming the equivalent of a shade tree mechanic when it comes to computers.

Additionally on the purpose of this document. It's not intended to be a technical walk through on how exactly to implement what is discussed; largely because of the immense number of combinations of operating systems and software out there. However, I generally have this ordered in terms of more basic and important things with more "walk through" type guides, at the beginning and move on to more advanced material that's more educational rather than a guide as well as less relevant to the typical person later in the document. However there are some exceptions when something is topical, for example using crypto currency is in the first section since it's related to finances, however I don't think crypto currency is something that the average person should feel compelled to get into if they don't see a personal use for it; although if you're curious about it, and have $50 to spare, I would recommend trying it out to just become familiar with it.

A disclaimer I'd like to add before getting into the meat of it. The privacy and security portions of this document are intended to protect you against common threats. Such as websites with your login or other personal data getting breached, malicious e-mails, device theft or lose. It is in no way intended to provide protection against law enforcement or other sophisticated attackers. Although some of these practices could hinder an investigation, you should assume that following this guide to the fullest probably wouldn't result in more than mildly frustrating them. If federal law enforcement or intelligence agencies are a serious concern for you, the only advice I can give you is settle for nothing less than Tor and encrypt everything with a hardware key you can destroy in seconds at any time and never use a cell phone again.

Lastly, throughout this document I will use specific service providers, programs and manufactures when discussing topics. For example when talking about e-mail clients, I'll use Thunderbird since it's quite popular and what I use personally. However that's not to be taken as a claim that Thunderbird is better than alternative e-mail clients and although configuration steps will certainly be different between Thunderbird and its alternatives, it ought to be close enough to get the ball rolling for you. At times I will make recommendations on particular products or services, but I will make it explicit I'm doing so. Recommendations I do make are based off of the best of my knowledge and experience, so don't treat them as gospel. Lastly, I'm not getting paid, or receiving any sort of favors, by any person or service to mention them.

Financial and Doxxing Protection

Credit Freeze

What a credit freeze does is block the ability for your credit score to be checked which is a requirement for taking out lines of credit such as mortgages, auto loans, credit cards etc. Naturally it's not something you want to do if you plan on taking out a new line of credit in the near future, but if you aren't it does provide *an additional layer* of security in the event someone acquires enough of your personal information to try to take out a line of credit with your identity. Emphasis on *additional layer* of security, because it's certainly no guarantee to prevent that from happening; but it is an easy and free step you can take to protect your finances.

The three main credit bureaus you'll want to freeze your credit with are Equifax, Experian and Transunion. It's also important that when you enable these freezes you follow good security practices with any passwords, PINs and/or e-mail accounts you may associate with the credit bureaus that would be utilized to either unfreeze your credit or reset your password. See sections on passwords and e-mail for more information.

It's also worth mentioning that there's more than just the big three credit bureaus. Here's a short list of smaller ones with a brief description of what they do.

https://web.archive.org/web/20220424230308/https://www.thebalance.com/6-small-credit-reporting-agencies-consumers-should-know-about-4210980

They typically specialize in aggregating information regarding a particular type of credit and as far as I can tell, they mostly provide supplemental information to financial institutions; meaning that just freezing your credit with the big three should be adequate. However I'm not a financial expert, so do your due diligence regarding them.

Credit Cards

Credit and debit cards are not only financial tools that deserve protection in their own right, but also are usually associated with your real name and address. Making them a high priority whether trying to protect your money or identity on the Internet. Fortunately the methods to protect them is actually very simple and likely free. The best and easiest solution is to utilize virtual credit cards from privacy.com. The way it works is that you'll link your checking account or debit card with your privacy.com account and with the free account you'll be able to have up to 12 virtual cards that they'll generate for you. Each individual card can only be used with one vendor and will be declined if anyone besides the first vendor to charge it tries to. Additionally spending limits can be set on each card (monthly and yearly) to limit them with the one vendor they're authorized to be used with. Lastly, all cards can be canceled at anytime which is nice if you're worried the vendor won't stop charging you and you can even make cards that can't be charged at all to use for free trials that require card information.

The best part of these virtual cards is that essentially when the card is charged, if the vendor checks with privacy.com to verify the name and address is correct, privacy.com will respond that they're valid regardless of what you entered when you provided the card to the vendor. Meaning you can use completely made up names and addresses with them. Although it's worth keeping in mind that some vendors will independently verify the address is real, so don't get too creative with the addresses.

Note that at least in the United States, this is 100% legal. The only real draw back I suppose is that they can't/won't issue physical cards like these. If you'd like a little more information on the subject of credit card authentication here's an article on it.

https://archive.ph/wip/eZ3dJ

Lastly, I just want to reiterate the earlier disclaimer. I only discuss privacy.com since it's the only such service I'm aware of and I use it myself without issue. I can certainly recommend it however, I'm not saying that there aren't other or even better alternatives.

Cypto Currencies

Naturally it'd be strange to discuss purchasing items over the Internet pseudo-anonymously without addressing crypto currencies. First of all, in regards to crypto as an investment, I can assure you I have absolutely no advice to give in that regard. However for crypto being used as an actual currency, I think it's quite obvious by now that it has found a little niche in the economy and is here to stay given the current conditions of Western governments freezing banking accounts and the like (the Canadian trucker protest off the top of my head) as well as private financial institutions denying service to individuals and organizations due to "reputation risk"

https://archive.ph/2uBaP

Again, I know nothing about crypto as an investment nor do I own any crypto *as an investment*, however I think it's important to become familiar with actually using it. So rather than spend a chunk of savings on it, if you have $50-$100 to play around with. I'd highly recommend creating a wallet and buying some crypto and either buying something or donating some just to learn how to use it as it will likely become more relevant and common in the coming years.

Major Crypto Currencies

Disclamer: I'm not a huge crytpo nerd, so take this section with a grain of salt. This is just to give you a very basic idea of popularly used coins.

This will by no means be an all inclusive list of all crypto currencies, or even relevant ones. But if you're looking to get into crypto for using it, here's the big three. Bitcoin (BTC), Ethereum (ETH) *not to be confused with Ethereum Classic (ETC)*, Monero (XMR) and an honorable mention to Bitcoin Cash (BTH). All of which are quite widely supported by exchanges, wallets and vendors who accept crytpo. However before getting into crytpo you should definitely check what potential vendors you would be patronizing accept and pick your exchange, wallet, etc accordingly. I will say Bitcoin Cash and Monero are the least common of the ones listed, but still quite popular coins for actually using as currency.

As for pros and cons of them. In terms of buying them on exchanges, storing them in wallets, etc they're all quite similar. One of the big differences to look at is the stability of the coin. If you've heard anything about crypto, it's probably the drastic swings in the value of bitcoin up or down. I think it's safe to say it's the most volatile of the ones listed, however if you're only looking to play around and get familiar with crypto, I don't think it' s huge issue. Bitcoin is by far the most commonly accepted crypto and even if it does crash and goes to nothing, for throwing in $50 - $100 to play with, I don't think it's that big of a risk and could also work in favor of you with a huge upswing. The biggest concern with Bitcoin would be that it's the easiest crypto currency to trace and law enforcement can certainly do it if they're willing to.

https://web.archive.org/web/20220418164509/https://www.cnet.com/personal-finance/crypto/is-bitcoin-really-anonymous/

However, again law enforcement is out of scope of this document and tracing bitcoin is still quite time consuming and expensive in terms of manpower. My point is, using the Canadian trucker protest as an example. If they used bitcoin, instead of gofundme or whatever, if you sent them $20 in Bitcoin, I think it's highly unlikely they'd go through the trouble of tracing back every nickel and dime given to them. However this issue isn't something to be totally dismissed and I think all else being equal, you should try to use more anonymous coins even if you're not worried about law enforcement.

On the subject of difficult to trace coins. The current king in that regard would be Monero. I won't get bogged down in the details, but *at the moment* it's deemed truly anonymous and law enforcement has bounties out for people who can find a way to trace it.

https://archive.ph/wip/7PTWv

As for Ethereum. Honestly I don't know much about it, although it's certainly a very popular coin and it has a lot of features for things being built off it. I'm not too sure about the anonymity of it, but I think it would be safe to assume it's not significantly better than Bitcoin.

Two more things to wrap up, concerning Bitcoin there's something called the "Lightning Network" that was built on top of regular Bitcoin itself. I'm not knowledgeable on it, but it's supposed to offer a number of improvements to Bitcoin transaction speeds. Lastly, I haven't said anything about Bitcoin Cash yet. As you could infer from the name, it's based off of the original Bitcoin (however it's a separate coin, you can't send Bitcoin Cash to a Bitcoin wallet, etc) that was made to compensate for some deficiencies with Bitcoin concerning how transactions are conducted. It is also more stable in price than Bitcoin.

Crypto Exchanges

The first and easiest option for getting into crypto is through crypto exchanges. Most of them are under KYC (Know Your Customers) laws and the registration process will usually include submitting a photo/scan of a government id, such as a driver's license, as well as submitting a timestamped photo of yourself to verify it and of course you'll also need to link some sort of traditional checking account. Once your account is verified you'll be able to login and be able to purchase any of the crypto currencies offered at that exchange.

Once you've purchased your coins you can then transfer them to a wallet, which you could think of as where the coins are stored. This process will very slightly per exchange, but there's the guide for sending coins from the Kraken exchange to an address.

https://archive.ph/wip/CnOkY

Note: that despite the term "withdraw" being used. You can send the coins to any address, not just your own.

Password and account security will have their own section, however for now just know that for your exchange account, use a good password and enable 2FA (two factor authentication) preferably with some sort of authenticator phone app or hardware token.

Alternative Means of Buying Crypto

Briefly I'll cover a few other aspects of acquiring crypto currencies. One option is crypto currency ATMs. They typically offer all 4 coins discussed so far, although not always. Typically these machines are located in similar places as regular ATMs and look quite similar. Here's a map of one manufacturer of them, but they're far from the only ones. So if they don't show any near you, check other companies as well.

https://www.coin.cloud/dcms#map

Generally the way these work is before hand you'll get the wallet address you intend to send to as a QR code. Then go to one of these machines and select whether you're withdrawing or depositing, what coin and amount. The amount you're withdrawing/depositing will determine how much information they want from you. I don't recall the exact rules, but if it's something along the lines of $250 or less and they will want a phone number and/or e-mail and over a certain amount, $700 or so, they'll want a to see a government ID. After going through the verification process, it'll ask for the QR code of the address to send the coins to and afterwards you'll give it the cash (I could be mixing up the order of these last two steps). With this method you very well could use the wallet address of the person you ultimately intend to send the coins to, however I wouldn't recommend that. Since like regular ATMs, these machines typically work in set increments such as $20, $50, $100… etc. So unless the person you're trying to give the coins to wants exactly $20 and is willing to eat the fees himself, the better bet would be just doing $100 or so to your own wallet and sending them from your wallet to theirs.

Another option, and most appealing if you would like to buy crypto without doing any verification, is to buy crypto directly from another person who has crypto. Obviously the best choice would be someone you already know and trust, but P2P (Peer2Peer) exchanges exist which facilitate meeting people in person to buy crypto with cash and also act as an escrow to prevent scams.

https://blog.localcoinswap.com/how-to-buy-bitcoin-with-cash-in-person-on-localcoinswap/

Above is one P2P exchange that facilitates in person transactions. Another option is exchanges like

https://localbitcoins.com/

That are P2P and still act as an escrow, but don't facilitate meeting in person, so you'll need something like Paypal, Zelle, etc to buy the coins with.

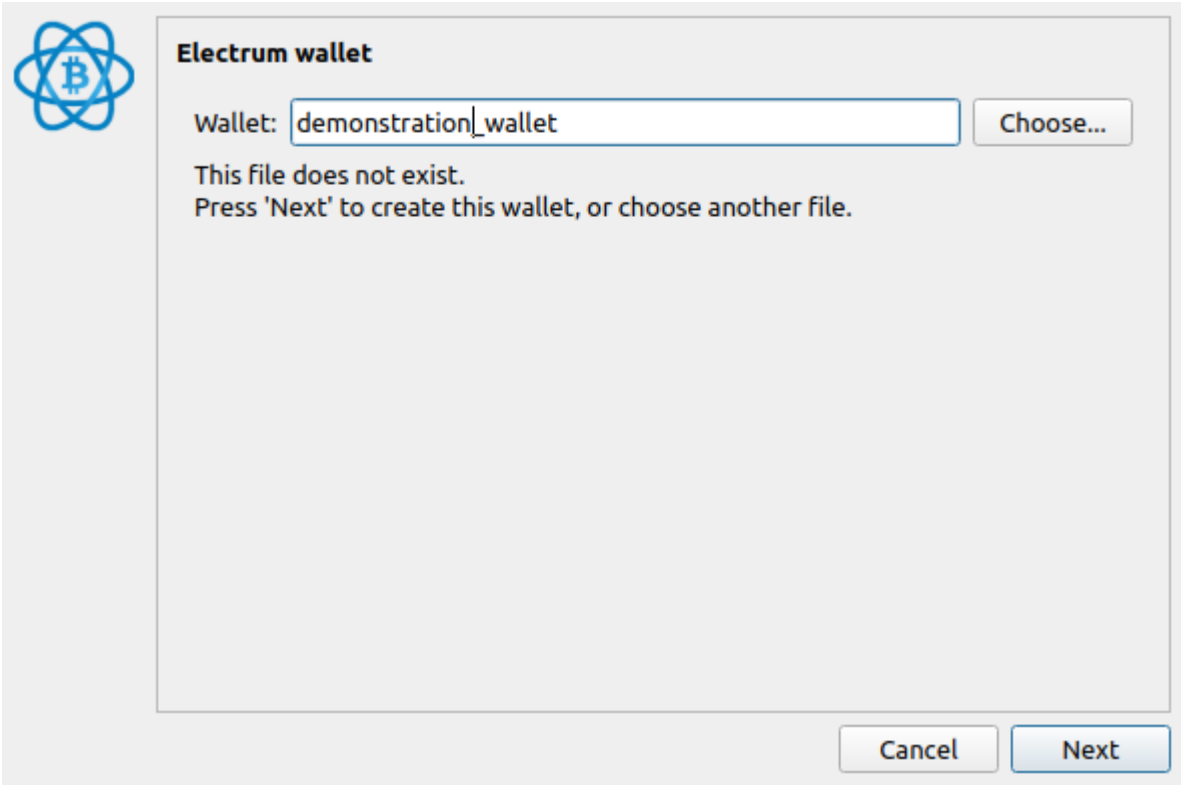
And of course if you're feeling adventurous you could just put an ad on Craigslist and hope for the best :^)

Crypto Wallets

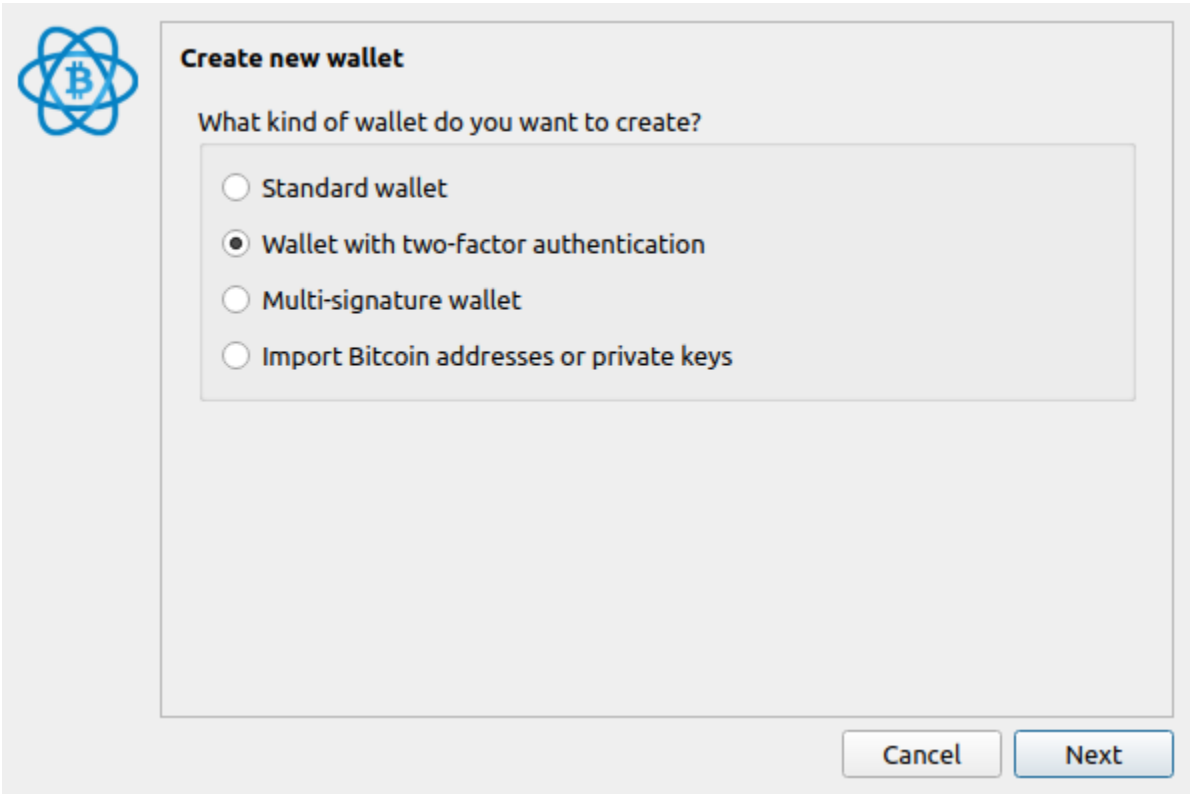
Again, this will be a general guide, as the procedures for different wallets and coins will be more or less that same. Also I won't be covering hardware or "cold" wallets, which are crypto wallets that are stored on something like an external HDD, I'll just be covering the type of ones you install on a computer or cell phone, although I won't be covering cell phone ones either, since I have no experience with them and obviously security is a concern.

Once you've chosen and installed a wallet on your computer (If provided, you should verify the signature of the installer, although that will be covered later in the encryption section), one of the first things that'll happen when you create a new wallet is that you'll be given a seed, which will be a dozen random words or so that can be used to recover the wallet should you lose access to the exact one installed on your system. Remember with crypto the transactions are publicly logged, so it's not like the coins are physically stored in the wallet, but rather the wallet holds your keys which can claim ownership of certain transactions on the public ledger. I'll cover backups and encryption in another section, but generally the best way to store your seed would be to write them down or print them out and store them somewhere safe like a safety deposit box at a bank or in a safe, although again if you're just using playing around money it's not quite so necessary. Ideally you should have multiple backups with at least one being somewhere besides your home and any digital backups should be encrypted.

Here's a quick demonstration of setting up a Bitcoin Electrum wallet. Again, should be similar enough for other wallets and coins.

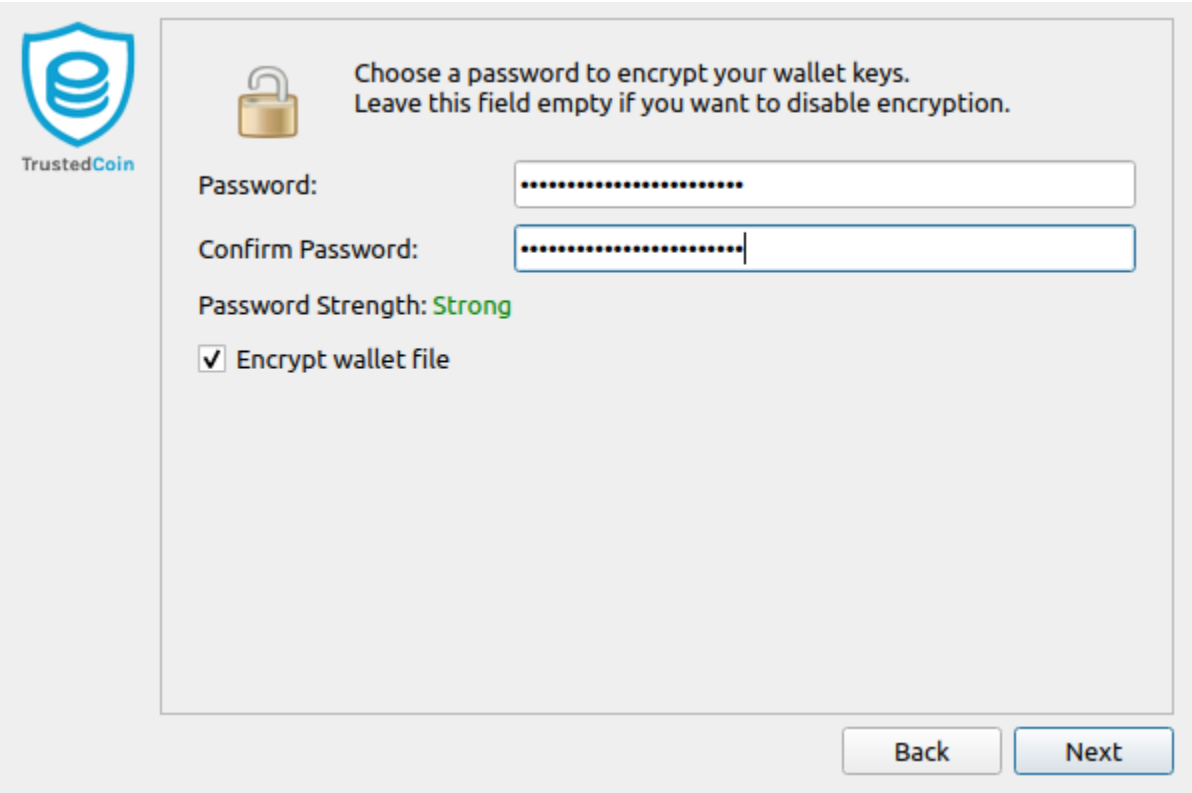

Electrum wallet
Wallet:
demonstration_wallet
Choose...
This file does not exist.
Press 'Next' to create this wallet, or choose another file.
Cancel
Next

Naming the new wallet. For your own organizational purposes. The only thing you'll give to people is addresses which are very different. Also you can have multiple wallets on the wallet program.

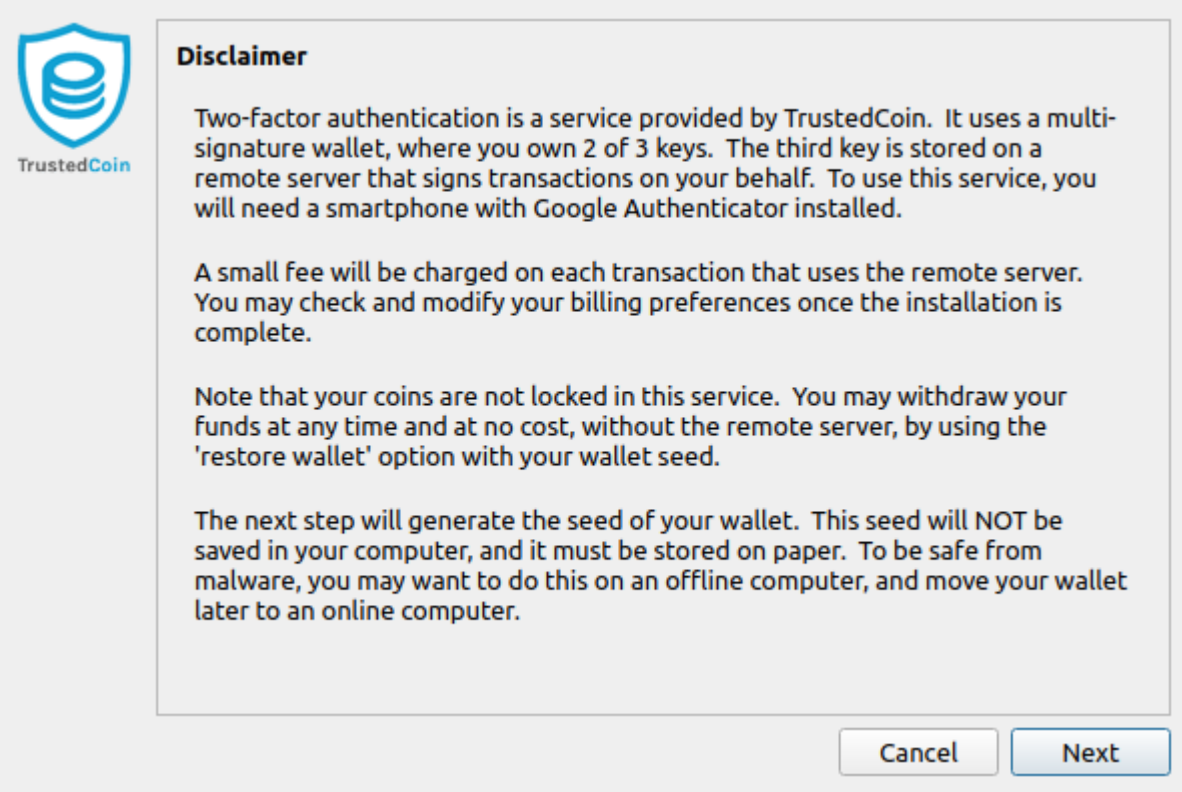


There's your options for the new wallet. Standard means it'll generate a private and public key for the wallet, with the private key being encrypted with the password you provide later, so that even with a standard account, someone would need either the recovery seed, or the private key and the password to use it.

No reason to not encrypt your wallet. A password is literally the least you could do to secure it.

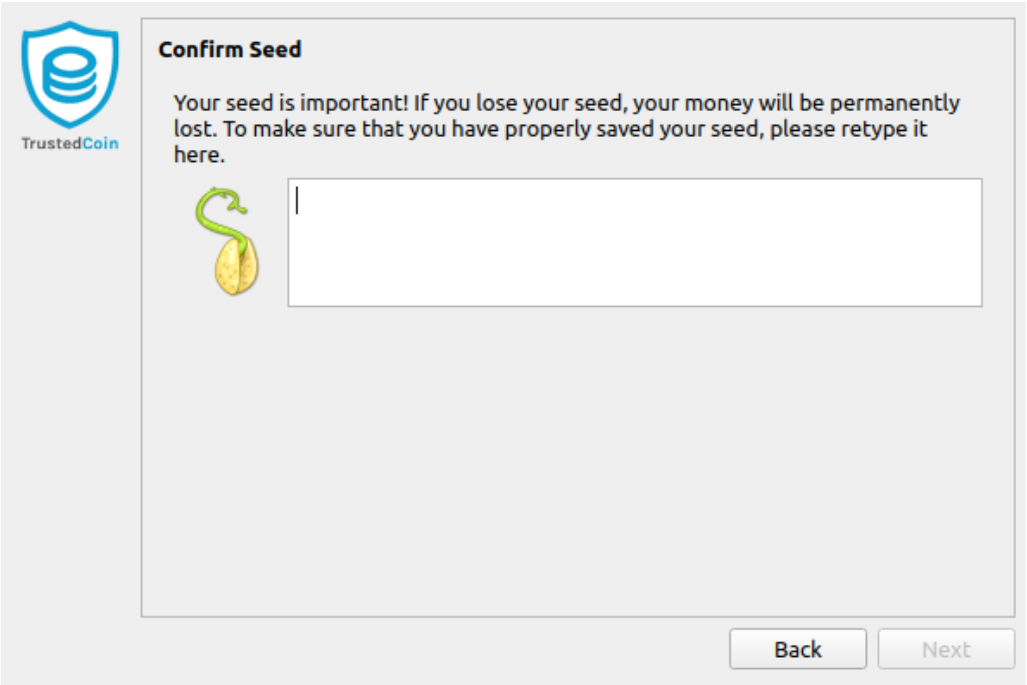


For Electrum, the 2FA is done over e-mail and it requires a small fee each time it's used. I'm not sure what the multi-signature wallet is, but I'm guessing it's for wallets shared by two or more people.



Recovering from the 2FA account to a standard does work, I did it since I didn't want to bother with 2FA for demonstration purposes. However since you'll still be missing the 3rd key that's stored with party that does the 2FA, you won't be able to sign or encrypt messages with your wallet keys (not covered in this document)

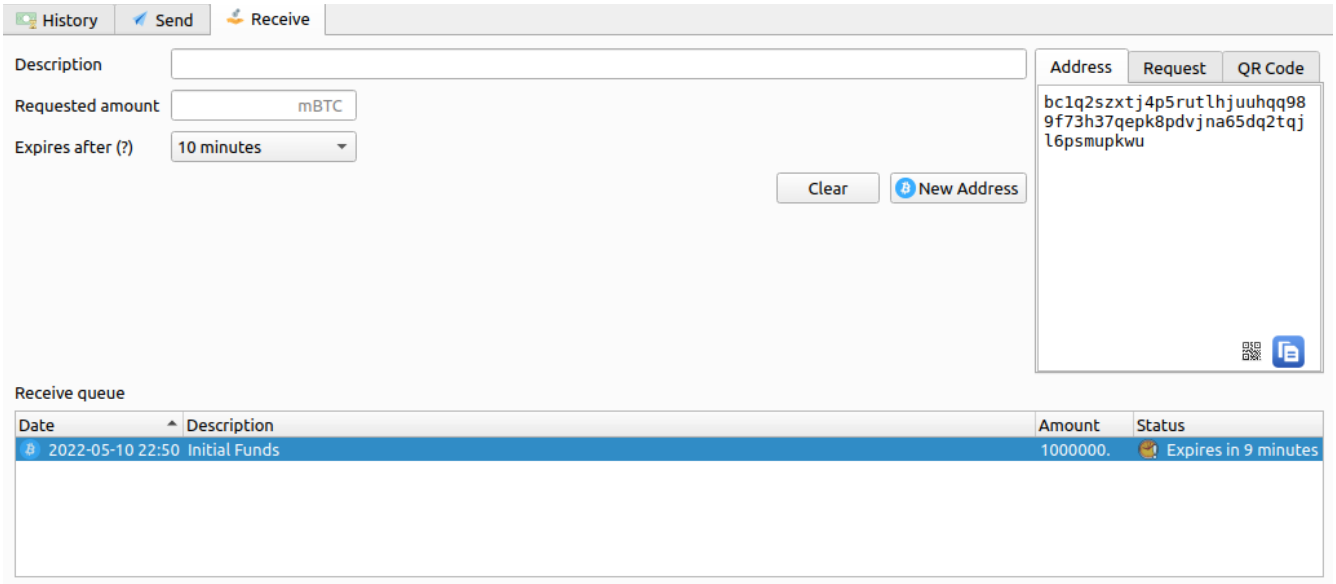
Afterwards it generates your seed and prompts you to save it. The next screen afterwards asks you for the seed to make sure you did save it somewhere.



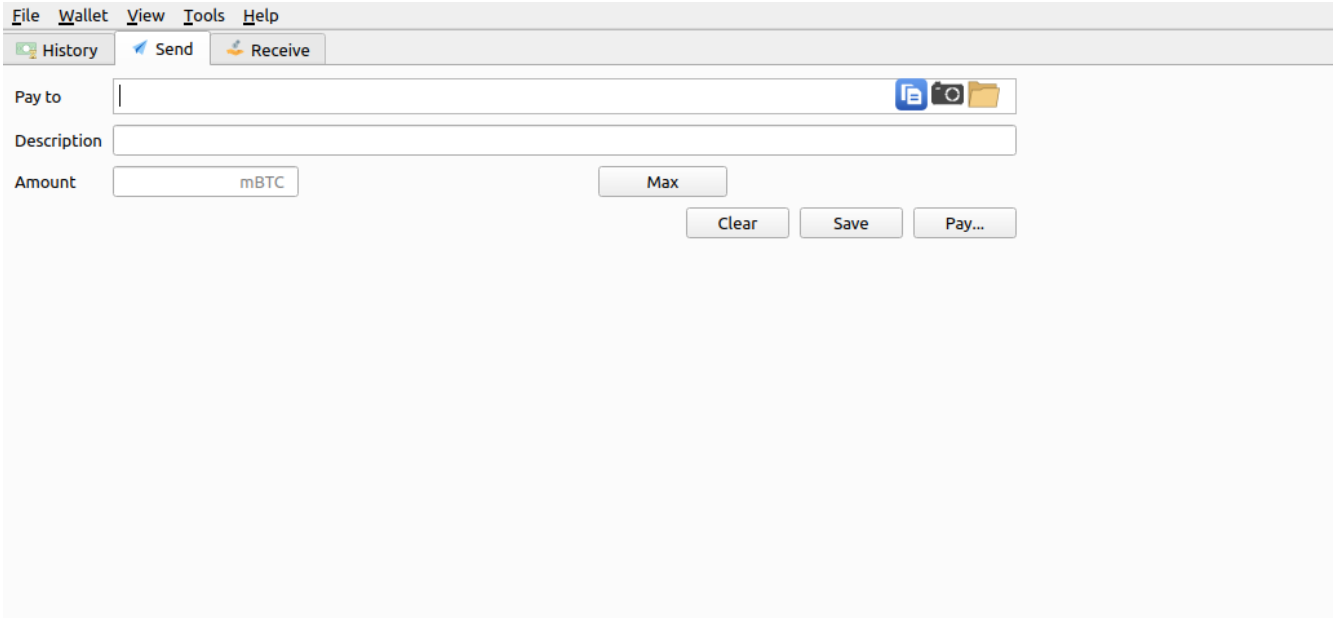
Then it will show you where the wallet file is located. Later after you're done setting it up, you can backup your wallet file from the file tab.

Here's how you can generate an address for the wallet to receive Bitcoin. The description field is local to your wallet, no one else see it, it's purely for your own reference. Similarly with the requested amount, it really means nothing.

Similarly the "Expires after" field means nothing for regular Bitcoin, I believe that's for the lightning network or something. Once you hit the "New Address" button with the blue Bitcoin logo, the boxes to the right and below will show up. As you can see in the one on the right, it's current displaying the address and also has a tab for a QR code. If you were going to use a crypto ATM, the QR code is what you would want to take.



Sending crypto isn't rocket surgery either. Just paste the address or you can scan a QR code (camera icon) or open from file (folder icon). Enter the amount and description and hit pay.



Important: that wallet was for demonstration purposes only. I and no one else have access to it anymore, so don't send any bitcoin to it. Also if anyone accuses me of being a shill, remember I turned down an opportunity to put a working wallet address here :)

Personal Data Removal

All the information in this section is from Michael Bazzell's work and he deserves full credit for it. His website is

https://inteltechniques.com/podcast.html

where he has a podcast and recently started a free magazine as well. He's hands down one of the best resources for privacy and security and I'd highly recommend checking his content out if you're interested.

With that out of the way. The quick run down is there's "people search" sites that for a relatively small fee will give out names, addresses and plenty of other personal information on nearly anyone. Michael Bazzell's put together a worksheet of common people search sites along with a short note on how to go about requesting they remove your data from them. The

reason it's not more in depth is that they frequently change the procedure on requesting data removal especially when people put out guides on how to do it. The work sheet is linked here

https://inteltechniques.com/workbook.html

Although of course this isn't a bulletproof method to prevent doxxing, it takes care of a lot of the low hanging fruit of what can be used to dox or otherwise harass you.

File Metadata Removal

First I'd just like to clarify that this section will be about metadata that's *inside* a file's data. To explain there's generally two types of metadata about a file. The first is file system metadata which is stored separately from the file itself. This generally contains the information you see in your file explorer such as name, size, MAC (modified, access and creation timestamps), permissions etc. Generally most of this metadata is rewritten when files are copied or moved across partitions and file systems, but the important thing is that it's not much of a privacy risk. This section is about the metadata stored in the file itself that's preserved whenever it's copied, regardless of partitions or file systems. The two main ones we're concerned with is EXIF data in JPG files and account information stored inside Microsoft office documents.

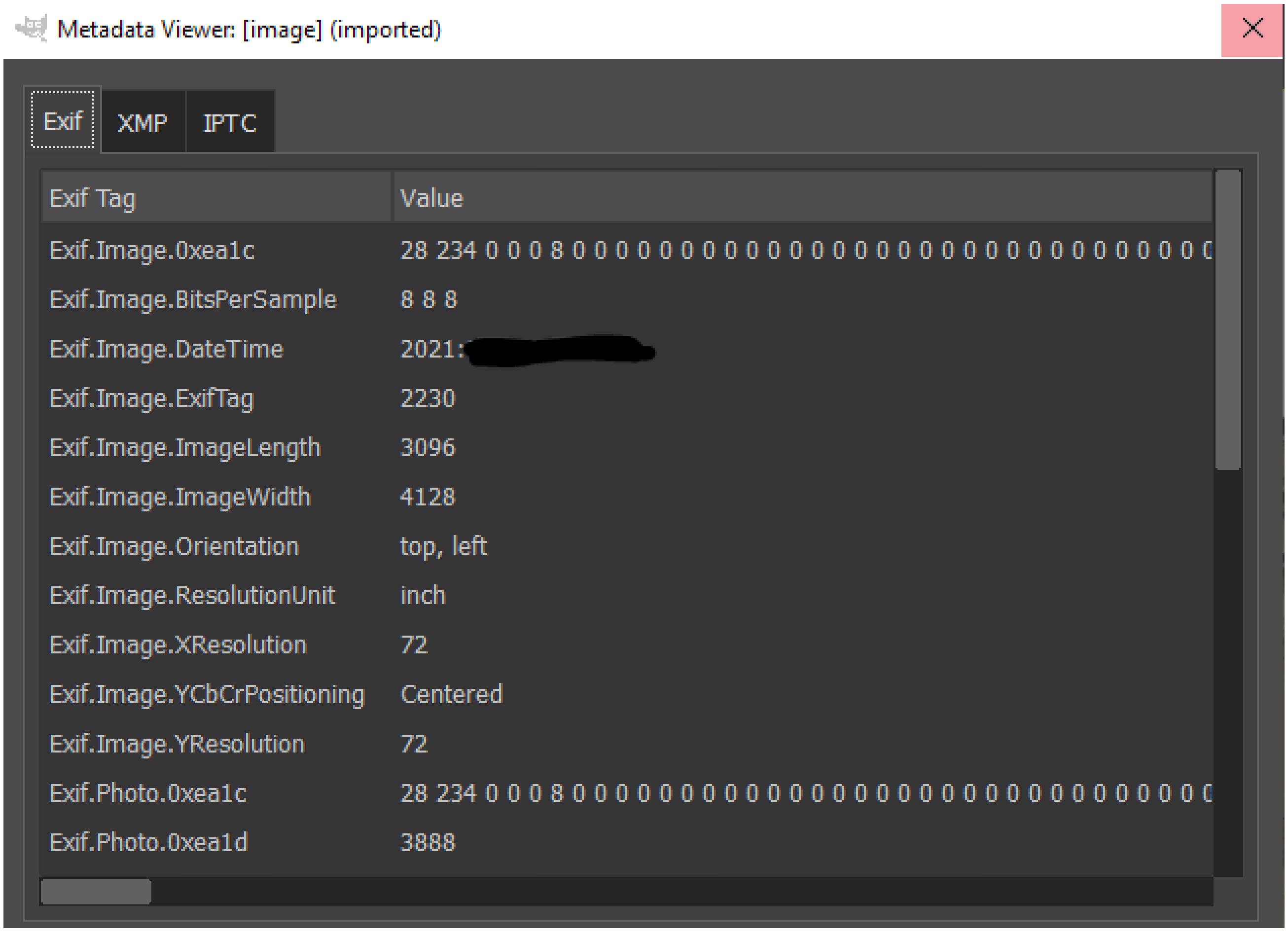
Images

We'll start with EXIF metadata inside JPG files since it's by far the most important concerning privacy. By default, many cell phones and cameras will store information such as the GPS coordinates, timestamp as well as make and model of the device that took the pictures (as well as other technical information about the pictures, such as exposure, if flash was used, aperture size, etc; not very relevant for privacy). Typically devices will have a setting to not include the location data in pictures, which is better to set than not, however we don't want to just rely on that setting as well as there's other potentially revealing information in EXIF such as timestamp and make and model.

Now windows has the ability to remove *some* EXIF data, however it's quite lacking. Here's the original EXIF data of the picture as viewed with GIMP.

Exif Tag	Value
Exif.Image.BitsPerSample	8 8 8
Exif.Image.DateTime	2021:[redacted]
Exif.Image.ExifTag	226
Exif.Image.ImageLength	3096
Exif.Image.ImageWidth	4128
Exif.Image.Make	samsung
Exif.Image.Model	[redacted]
Exif.Image.Orientation	top, left
Exif.Image.ResolutionUnit	inch
Exif.Image.Software	[redacted]
Exif.Image.XResolution	72
Exif.Image.YCbCrPositioning	Centered
Exif.Image.YResolution	72
Exif.Photo.ApertureValue	F1.9
Exif.Photo.BrightnessValue	5.41
Exif.Photo.ColorSpace	sRGB
Exif.Photo.DateTimeDigitized	2021:[redacted]
Exif.Photo.DateTimeOriginal	2021:[redacted]
Exif.Photo.ExifVersion	30 32 32 30
Exif.Photo.ExposureBiasValue	0 EV
Exif.Photo.ExposureMode	Auto
Exif.Photo.ExposureProgram	Auto
Exif.Photo.ExposureTime	1/191 s
Exif.Photo.FNumber	F1.9
Exif.Photo.Flash	No flash
Exif.Photo.FlashpixVersion	30 31 30 30

After running the Windows tool (in file explorer: right click file → properties → details → remove properties and personal details) there's still unnecessary EXIF data like the timestamp of when the photo was taken.



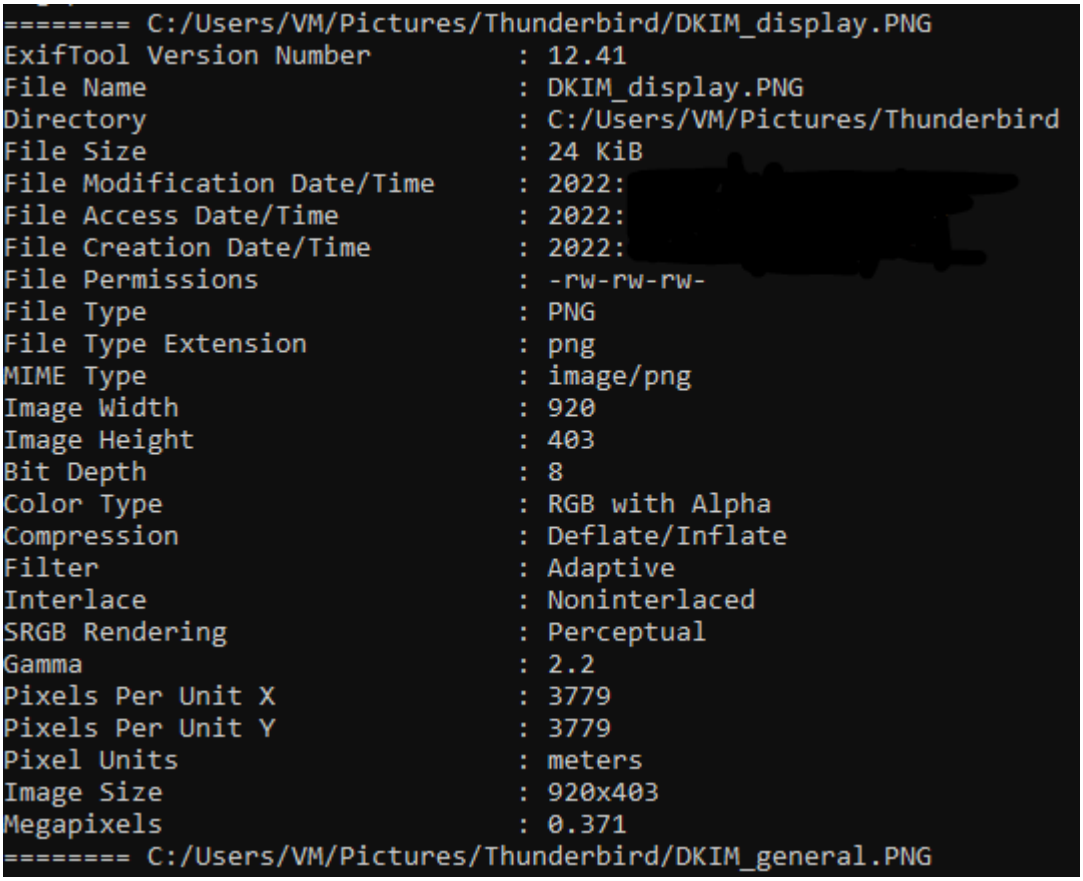
The file I was testing didn't have location data, but since it didn't remove the time stamp I wouldn't trust it to remove location data either. The better solution, that does remove all non necessary EXIF data, is *exiftool.*

https://exiftool.org/

(On Linux it's likely in your repository)

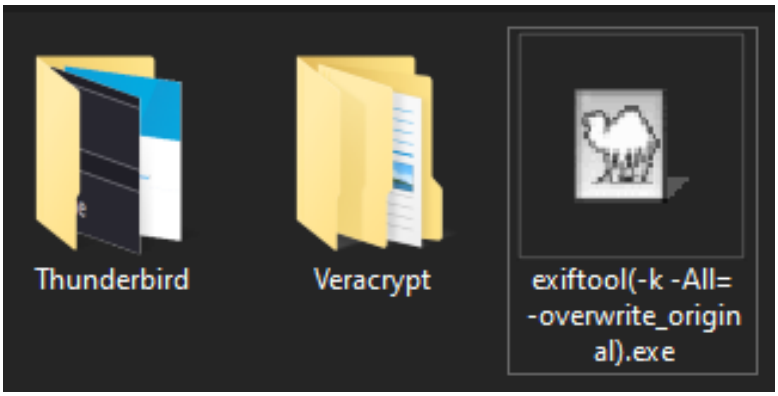
There's a separate section on CLI Navigation you can use the link to jump to. Although this particular program has a neat feature you can add the options in the file name and just drag and drop files or folder onto it to run the program on them.

By default it has the option -k which is in the filename by default and all it does is prevent exiftool from closing immediately after running so you can read the output (if used via drag and drop method). Using the exiftool with just this option (or none from the command line) will show the metadata of the file, both file system and EXIF.



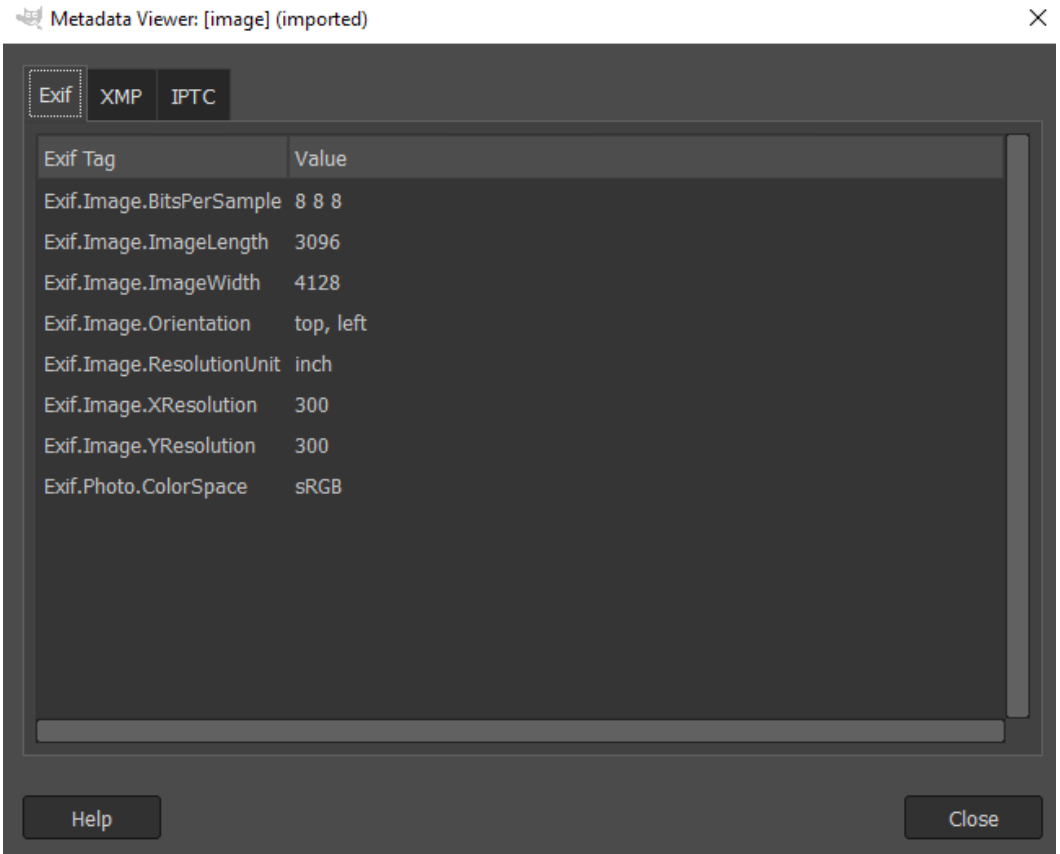
Note: this is a PNG file of one of the screenshots I took, pretty much all the meta data is from the file system (timestamps) or is necessary like resolution, etc. It's worth noting that exiftool works on nearly every image format PNG, GIF, and even MP4. It's also able to *read* the metadata on many file types, but for the most part it can only remove them from images (except for WEBP)

To set the options exiftool will use with drag and drop, you put the arguments separated by spaces, inside the parenthesis in the file name.



The picture above demonstrates the configuration to remove all unnecessary metadata and overwrite the original file. Without the *-overwrite_original* option it'll rename the original file to *<name.JPG>_original* and the new file with the metadata removed will have the previous name without the extension.

Here's the metadata that's left after running it with the remove all option. (This is the first JPG we viewed from GIMP, not the PNG file we viewed with exiftool)



Office Documents

Another file type to be concerned about is your typical office documents from Word, Excel, Powerpoint, etc and to some extent even alternatives like Libre or Open office. Most of the embedded metadata is innocuous stuff, like editing time, number of revisions, etc. However particularly with the Microsoft suite, it'll include the name of the Microsoft account that created the document and those that have edited it.

To see for yourself, you can take a .docx, or other office document, and change the extension to .zip. Then extract the zip file and you'll get a folder with a series of .xml and other files in it. I believe it's the one called core.xml that will have the Microsoft account name in it. From what I've seen it doesn't look like Libre or Open Office includes a user name or anything like that embedded in the file.

To remove the embedded meta data, the basic procedure is to first click *File* in the top left corner and from there click *Info* and the *Inspect* option should be on the left side. Regardless here's an article from Microsoft about what data is stored and the removal procedure.

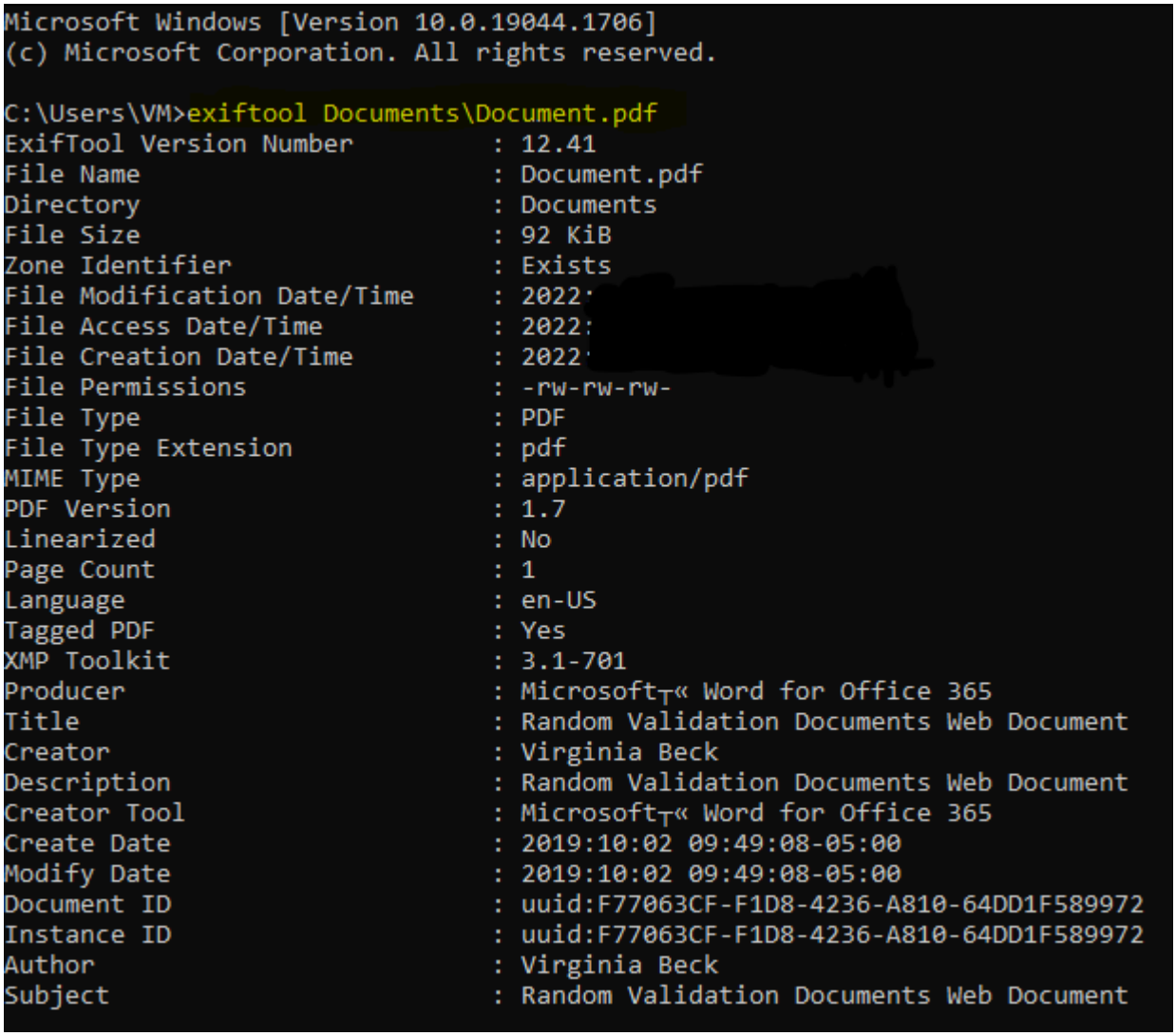
https://archive.ph/wXcs4

The procedure for Libre Office is similar, click *File* and then select *Properties* from the drop down and a window will pop up showing, at least some of, the metadata which can be cleared with the *Reset Properties* button presented to you. Although again, as far as I know, it doesn't seem like Libre or Open Office put any revealing info in documents.

Lastly, if you're concerned about Word, or other Office Suite program, not actually removing the metadata, similar to using file explorer on images. I've tested it on my work computer and it does at least remove the Microsoft account name of the person who created it, although I don't have screenshots of it, and again you can test is yourself by converting the file to a zip, extracting it and open the core.xml file in notepad and search for your Microsoft account name.

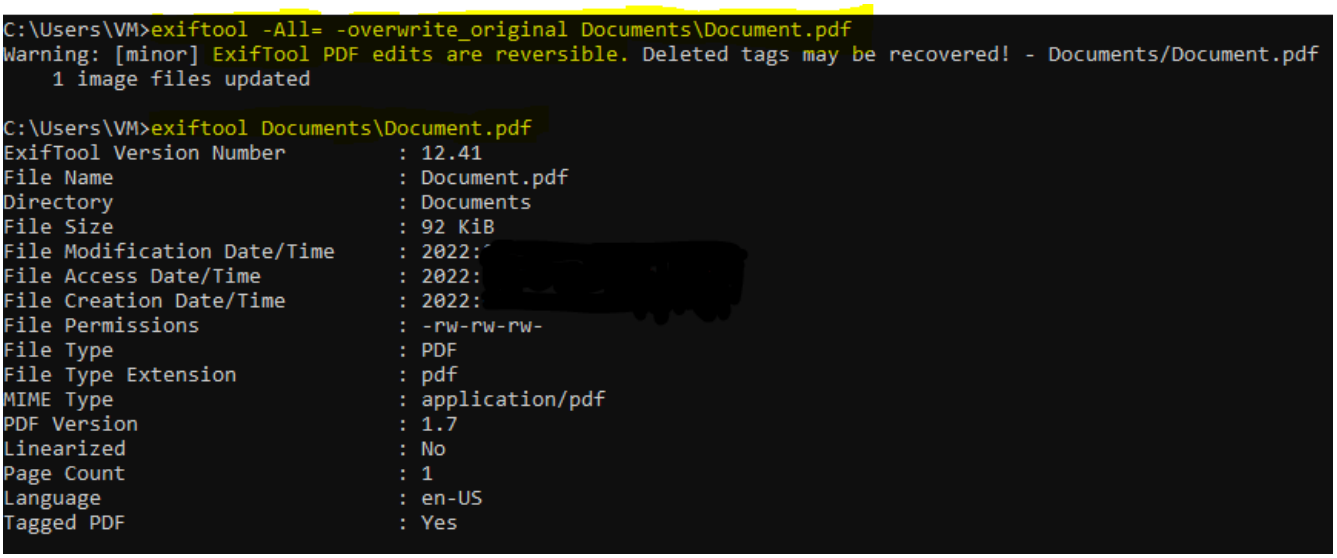
PDFs

I'm not to sure exactly what metadata PDFs will typically have, as it's very dependent on what was used to create or export the PDF. However it's certainly a concern if you're creating PDFs with Microsoft Word as demonstrated in the below image. (Also an example of using exiftool from the command line, the commands are highlighted)



Again, that command just shows the metadata the file has, to remove it we can use either the option *-All=* or -*= the -All option should be used in the file name to do the drag and drop method, since * isn't a valid character for a filename on Windows and probably Linux and Mac as well.

Removing and then viewing the remaining metadata. (Highlighted the message that tag removal is reversible, I didn't type that, just wanted to bring it to your attention)



Again, the time stamps are from the file system, as we saw with the original tags, the document was created in 2019, but these are all 2022 when I downloaded it on my computer. I redacted the exact date, because I'd find it weird if you knew the exact time I was working on this.

Passwords and Account Management

Likely passwords are already an annoyance for you as many as the typical person has these days. This section won't just be about having good passwords, but also making it much easier to manage those passwords.

First, I'd like to clarify what exactly we're concerned about in regards to password security and a few misconceptions people have about the subject. The main concern is websites getting hacked and their database of user login info being leaked. A fairly common misconception people have is that if a website gets hacked, it doesn't matter how good you password is, the hackers will have it. Generally this isn't true, sites will store a hash of your password not the password itself (I won't go into detail on hashes, I'll just drop a link)

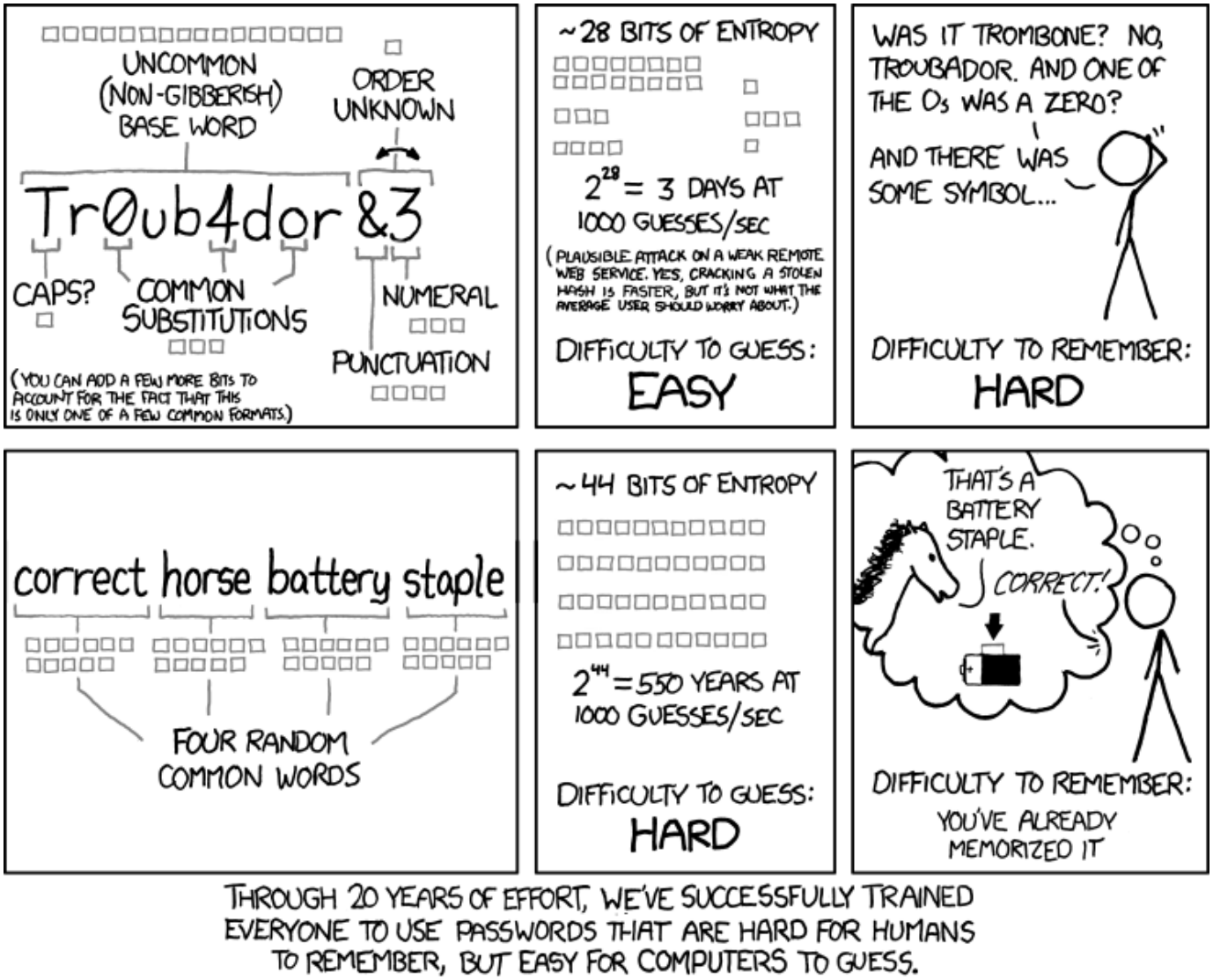
https://web.archive.org/web/20220323043000/https://www.okta.com/blog/2019/03/what-are-salted-passwords-and-password-hashing/

The important thing is that even if hackers get access to the hashes of the passwords, having a good password still reduces the chances of the hackers figuring out the actual password that generated the hash associated with your account.

The other big concern is password reuse. Since most websites just use your e-mail as your username, if one password is discovered, then it's trivial to try that e-mail and password on other popular sites to see if it works, if all of our login passwords are unique the damage is limited to that one account. At the very least we don't want to reuse passwords for important account such as e-mails, financial, etc.

Creating Passwords

Something many people still aren't aware of is that the mainstream guidance on creating passwords isn't that good. The comic below explains it more concisely than I can.



The general idea is that you want to focus on making passwords you want to remember, you want long rather than random. If you wanted to go above and beyond what's demonstrated in the comic you could use something like a quote or phrase as your password and if you wanted to add a bit of randomness to it, you could still do easy substitutions like using the %

instead of spaces between words, or a simple capitalization scheme, such as every 3rd character in a word is capitalized.

Example

```
the quick brown fox jumped over the lazy dog

the%quick%brown%fox%jumped%over%the%lazy%dog

thE%quIck%brOwn%foX%juMped%ovEr%thE%laZy%doG
```

This is all well and good, however there's still two problems that haven't been addressed. Which is the sheer number of passwords people need to memorize and the fact many websites require having special characters and numbers in the password and many even require the password be *less* than 12 characters. This is where password managers come in. I believe the optimal password strategy is to have a handful of good, but memorable passwords, for things such as encryption keys, device login, password manager and accounts you would want to have access without access to your password manager; additionally due to the inherit insecurity of phones (likelihood to get lost or stolen) I wouldn't recommend setting up your phone to utilize your password manager or save passwords to account you care about at all, for anything you'd want to access from your phone, use a good memorable password or a separate password manager that has limited passwords.

Password managers offer a lot of benefits, not only do they prevent the need for us to remember all our passwords, but typically they also are able to generate random passwords and passphrases. Not only are truly random passwords the most secure, but they can also be set to include special characters and numbers to meet website requirements as well so even if we're limited to 12 characters, a truly random 12 character password is still very secure. Also, depending on the password manager, they can also be used for storing things such as 2FA backup codes or, in the case of local password mangers, be a 2FA device themselves.

Another quick note, browsers such as Firefox can be used as ghetto password managers, I know at least Firefox offers the option of setting a master password that's used to encrypt the logins it saves. Additionally it will offer to create random passwords for you, however last I used it, they only used alphabet characters meaning they couldn't be used for most sites for lack of special characters. However there's numerous ways to generate good random passwords such as sites like.

https://passwordsgenerator.net/

and programs such as *pwgen*

It should also be noted that you should keep backups if you're using a browser or a local password manager. Local password managers will typically store everything in an encrypted database file on your computer that can be backed up without much trouble and every browser offers the option to export your logins as CSV files, however they'll be unencrypted so you'll need to encrypt them yourself or store it on an encrypted drive. For more information see the sections on encryption and backups.

Password Managers

On password managers. Most are online services that will store your passwords on one of their servers encrypted with your master password. I'm sure most of the reputable services are fine, however I don't have any experience with online ones, so I'll just use KeePassXC as an example. They can explain their product better than I can so here's their explanation of it and this will likely be similar for other password managers, although for online one's you'd likely have to pay for some of the more advanced features.

https://keepassxc.org/docs/KeePassXC_GettingStarted.html

One thing I'll mention with KeePassXC is the user interface can be a bit awkward. For example if you go into the settings menu, you can't leave by clicking on a different menu option, you have to click the settings menu again to go back to the spot you previously were.

Overall it's an excellent password manager, not only does it work with your browser with their official browser extension, but it stores everything in a single encrypted database file which

makes backups incredibly easy and since it's encrypted you can have a backup on google drive, dropbox, etc without much concern (and I'd recommend doing so on the off chance your house burns down or something). Additionally you can also attach files to entries which is convenient for storing things like 2FA backup codes or exported phone contacts file.

Lastly concerning phones. Due to their inherit insecurity, most likely to be lost or stolen, and typing in good passwords/phrases being tedious. I think the primary goal with phones is simply to minimize the accounts we use on it. For the one's we do use on it, either have few enough you can remember good passwords for them or use a free password manager service that only has passwords for accounts you'll use on your phone to minimize the potential damage if someone gets access to the password manager on your phone.

2FA

Likely you already have some experience with 2FA as nearly all online banking accounts will require it, usually through text message or e-mail. I won't cover text message and e-mail 2FA since although they're better than no 2FA, we can do much better without much trouble. The main problems with e-mail and text message 2FA is that in the case of e-mail, it's probably the most commonly attacked service and due to it's importance, we really want to have 2FA on our e-mail account and having to do 2FA on our e-mail so we can get our 2FA code for another service is quite tedious. Text messages are better, however they're tied to that SIM card, so if we lose the phone we're shit out of luck until we can get a new one activated with the old phone number. (It is possible to steal text messages and thus the 2FA codes, however that's a targeted and quite sophisticated attack and not in the scope of this document)

Generally the way the various 2FA protocols works is that some sort of shared secret is generated by the service and imported into the device that will be performing the 2FA. On mobile authentication apps this is typically done through a QR code or as a string of random characters. Then when you go to login to a site a new code is generated from the shared secret and the time. There's many options for this sort of 2FA from mobile apps such as

Google authenticate or FreeOTP to password managers themselves and other desktop applications that handle 2FA.

Software Options

As for the different options, there's two main things you'll want to consider. First is privacy, as options like Google, Microsoft and Authy will require a phone number and/or e-mail to use, it's up to you if you're comfortable providing them with that information. However if you don't want to do that there's other options available such as FreeOTP. The second concern is redundancy and backups. If we just install a 2FA app on our phone and take no recovery measures, we're not much better off than using text messaging 2FA. One solution to this is redundancy, which is to have 2FA setup on our desktop/laptop as well so that in the event of losing our phone (or vice versa) we still have the other one to get codes from. The other thing is backups, some 2FA services will generate about 10 one time use codes that don't change that are to be used as backups should we lose our 2FA device so we won't be locked out of all our accounts, however you can also just save the original shared secret. Obviously these should be stored some where safe and password encrypted.

The best option for backup and redundancy, provided you don't want to use a local password manager and you're okay with giving up your e-mail and/or phone number, is authy. It's cross platform so can also be installed on your laptop/desktop as well as they will store backups encrypted with a password on their servers so you don't have to manage your own backups, you'd just reinstall the app and log back in. (Note: if you plan on using 2FA on your e-mail this might not be a good option since they'll likely use your e-mail to verify you when you log in on the new install). Although you can do your own backups and have redundancy with other services, authy is more convenient in this regard.

If you don't want to provide an e-mail or phone number to a service you're not out of luck. Although there's not any that I'm aware of that are cross-platform, you can still use two different 2FA applications for the same accounts, such as FreeOTP on mobile and WinAuth, Oathtool or KeePassXC on your desktop. Although with these options you'll need to manage your own backup codes. You can register two different devices with the same shared secret,

so if you were going with the KeePassXC + FreeOTP route (which is what I'd recommend). When you configure 2FA with an account, you'd scan the QR code with FreeOTP on your phone then click the "I can't scan the QR code" and you'll be presented with the string that you can copy and paste into KeePassXC. Plus since the shared secret is now stored in KeePassXC, it'll be included in your password backups and so you'll only have one backup to worry about for both your passwords and 2FA, plus you still have the redundancy of having both your phone and desktop be 2FA devices. Additionally KeePassXC and FreeOTP are both free and open source and run locally, so you don't have to pay anything or worry about some company getting hacked or selling your info.

Hardware Tokens

Lastly I'll give a quick mention to hardware tokens. Obviously they require purchasing something since hardware is involved, but they more or less operate under the same principle as the software we've talked about previously. Modern ones like YubiKey, and their equivalents, work by inserting the hardware token into a USB slot on the device (or NFC for phones) and touching them to generate and send the code via mimicking a keyboard. This option is more secure as it separates the code generator from your device, such as your phone or laptop, so if someone were to steal your phone and get full access to it, unless they also grabbed the hardware token they still wouldn't be able to login to any of your accounts protected by it. One difference to note with this option is that each key has a unique shared secret, as far as I know nobody offers duplicate keys with the same secret, so if you have two keys you'll need to register both with every site you intend to have 2FA with. So after initially adding the keys to all your accounts, if you want to add a new one later, you'll also need to get the backup key out and associate it with that account.

Recap

To briefly wrap up what a decent password and account strategy is. We want the majority of our passwords to be randomly generated and managed by our password manager. However we'll still need a couple of strong and memorable ones for things like the password manager itself, device login and any accounts you would wish to still have access to if you don't have a access to your password manager. Additionally for very important accounts,

primarily financial and e-mail, we'd also want to setup 2FA to further protect them. (e-mail's very important since it's typically what password resets are done through)

E-mail and RSS

Despite how antiquated e-mail as a communication protocol is, it's still very relevant today and although most people associate e-mail with endless spam making it nearly useless, managing even a 10 year old free e-mail account isn't nearly as bad as you think. We'll also cover RSS which is probably the most underappreciated and underutilized technology for average people.

E-mail Client Configuration

One of the most important parts of making an e-mail usable is using a proper e-mail client instead of accessing e-mail through a web client, not to mention there's a lot of privacy and security benefits that can be obtained from using a e-mail client. I'll use Thunderbird as an example, since it's probably the most popular e-mail client for personal use, it's available on Windows, Mac and Linux as well as is free and open source. However there's plenty of alternatives out there. A brief word about something to keep in mind with e-mail service providers, with many secure/private e-mail providers (protonmail, tutanota, etc) is that they generate your encryption keys and keep them on their servers, encrypted with your password, and most won't let you export your private key. Meaning you're limited to using their website or their official desktop e-mail client if they provide one. However you can still send and receive encrypted e-mail with any provider if you're using a desktop client. Also something to keep in mind with tutanota is that they use their own encryption system that's superior to OpenPGP however isn't compatible with any other e-mail service or open protocol like OpenPGP. Whereas at least with protonmail you can import other people's public keys and vice versa, so you can send encrypted e-mail between providers if you import the public keys yourself.

Initial Setup

After you've installed the e-mail client of your choice and login to your e-mail account with it, likely the first two options you'll be presented with are the authentication protocol to use and the e-mail protocol. For the authentication protocol, it'll be dependent on what your e-mail provider uses (gmail, yahoo, etc) but will likely be OAuth2. If that doesn't work, try a quick google to see what your provider uses, another option you might be presented with is the protocol to connect to the server, just chose SSL/TLS. The other important option you'll have is the e-mail protocol to use. I won't get into the weeds of it, but IMAP will be the "normal" option. Essentially the e-mails stay on the server and the client "views" them there. Meaning those e-mails will stay on the server to be viewed from other devices such as your phone or other computers. The other option is POP3, the way this works is periodically your e-mail client will pull the e-mails from the server and download them onto your computer and *delete them from the server* meaning they'll be gone and you won't be able to view them from any other device except the one that downloaded the e-mails. There is privacy benefits from using this method, since if the e-mail service was hacked, most of your e-mails won't even be there on the server, however if you do chose to use POP3, make sure to have a good backup system for your computer if you care about having access to your old e-mail.

Lastly, if there's an option to change the port, just leave it at it's default value. Changing it will almost certainly be unnecessary and changing it will likely to prevent it from working.

Organization and Spam

The main functional benefit of using an e-mail client is that you'll have access to things like rules and tagging to organize your inbox, if you've ever had a work e-mail you're probably familiar with doing this in Outlook. Again I won't get into the details, but to manage your rules in Thunderbird, first press the Alt key to show the menu bar in the top left, then select "Tools" and then pick "Message filters". The quick rundown is that between creating folders for different things and rules to sort incoming mail and setting aside the time to go through and unsubscribe from companies who have you on a mailing or promotional list, usually a small link at the bottom of the e-mail, however if you still get e-mails from them after unsubscribing

you can just add that e-mail address to the rule that sends e-mails directly to the trash and mark it as junk. A quick guide on e-mail rules and the junk filter.

https://support.mozilla.org/en-US/kb/organize-your-messages-using-filters

https://support.mozilla.org/en-US/kb/thunderbird-and-junk-spam-messages

Note: There's also additional junk mail settings if you go to

Preferences → Account Settings → Junk Settings

Remote Content

Another nice option that Thunderbird sets by default, and I'm sure can be set in other e-mail clients, is blocking remote content in e-mails. Essentially e-mails are just web pages which can run JavaScript and load things like images and fonts from other places. Not only does this save bandwidth, but it also helps your privacy quite a bit. By blocking remote content and only rendering what's in the e-mail itself, nobody but the e-mail server will know when or where you've accessed the e-mail from. If when viewing the e-mail the client goes out and fetches things like images or scripts for it, whoever is hosting that content could log the time and IP address that accessed it, which is a tactic that could be used in attempting to dox someone, as the attacker could send an e-mail to you with an embedded link (not one you'd click on, but for example a link to an image that the client would load and display as part of the email) that's only given to that e-mail so that when the e-mail fetches that image from their server, they get the time and IP address of what accessed it. Although IP addresses won't reveal your actual identity to anyone but the government or ISP, it still narrows your location down to roughly a zip code size area. Additionally it's not just a technique that would be doxxers use, but it's been used by advertisers and corporations for a long time.

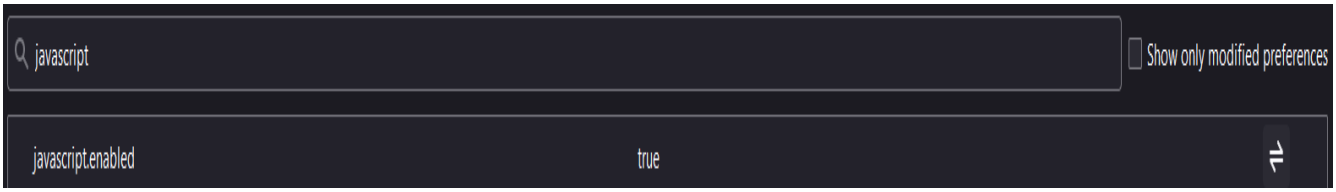
https://archive.ph/QL4ID

Also it's worth mentioning, blocking remote content rarely impacts e-mail functionality. Apart from images and fonts not always loading in promotional e-mails, I don't think I've ever had to turn on remote content for an e-mail in the years I've been using it.

Disable JavaScript

Another step I'd recommend taking with any e-mail client is completely disabling JavaScript. Unlike websites that often break with JavaScript disabled e-mails and articles you get via RSS almost never need JavaScript to function or appear correctly so you can avoid the overwhelming majority of tracking bullshit and not have any inconvenience from it to boot. Although bear in mind JavaScript normally needs to be enabled when your e-mail client first logs into your e-mail account, however it will be able to log in subsequently without JavaScript enabled, but if you ever change your password for that e-mail provider, you'll likely need to re-enable JavaScript to reconnect your e-mail client and provider.

To disable JavaScript in Thunderbird, press the Alt key and select "Edit" from the tool bar and then click "Preferences" near the bottom of the list. Make sure you're on the "General" tab from the left then scroll all the way to the bottom of the page until you see a button called "config editor" at the very bottom right. Afterwards type in "javascript" and you should see an option titled "javascript.enabled" set to "True" click the icon with the two arrows on the right and it should change to "False".



DKIM and Authentication

The last thing I'll talk about is a bit extra, so feel free to skip it or just read it for an insight into the fascinating world of e-mail authentication! There's an add-on for Thunderbird called *DKIM Verifier* that helps you tell if e-mails are coming from a legitimate source. Here's a brief overview of the various authentication protocols for e-mail.

SPF – Checks with the domain the e-mail came from to see if that particular address is authorized to send e-mail from it. Obviously it won't help if the domain the e-mail claims to be

from doesn't utilize SPF or an attacker spoofs an e-mail that is authorized to send e-mails from that domain.

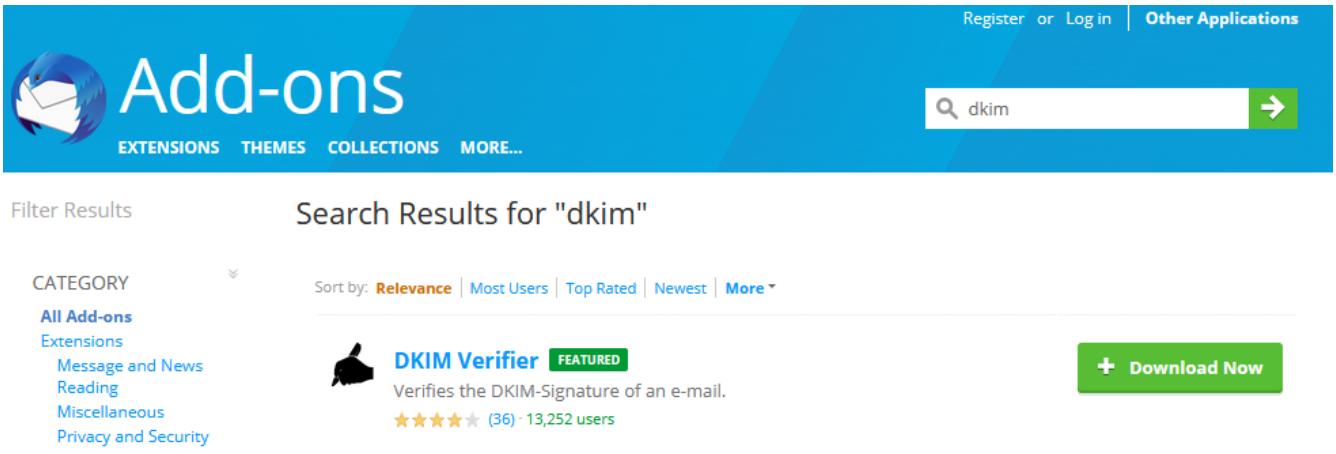
DKIM – Signs the e-mail with a certificate from the domain that sent it which also allows verifying that the content of the e-mail hasn't been changed after being sent.

DMARC – Is a policy set by a domain that if an e-mail received from it fails SPF and/or DKIM what to do with it, either quarantine it, reject it or do nothing to it.

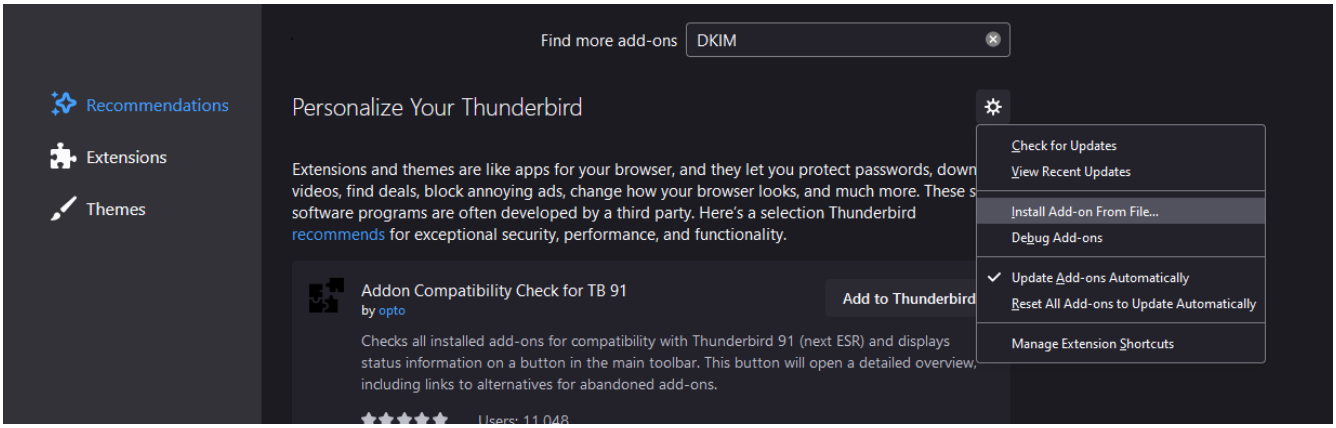
ARC – Is essentially a helper protocol that keeps DKIM from breaking when e-mails are forwarded or sent to groups.

If you'd like to learn more about e-mail analysis, it's actually simpler than you think. Almost any e-mail client, desktop or web, will allow you to save e-mails as plaintext (usually with .eml extension) which allows you to see all the authentication information and various stuff the mail servers write on it as well as the raw code of the e-mail itself. By default what the DKIM Verifier does is when you open an e-mail it'll check to make sure that the DKIM signature is valid and display it to you without having to check the raw code of the e-mail.

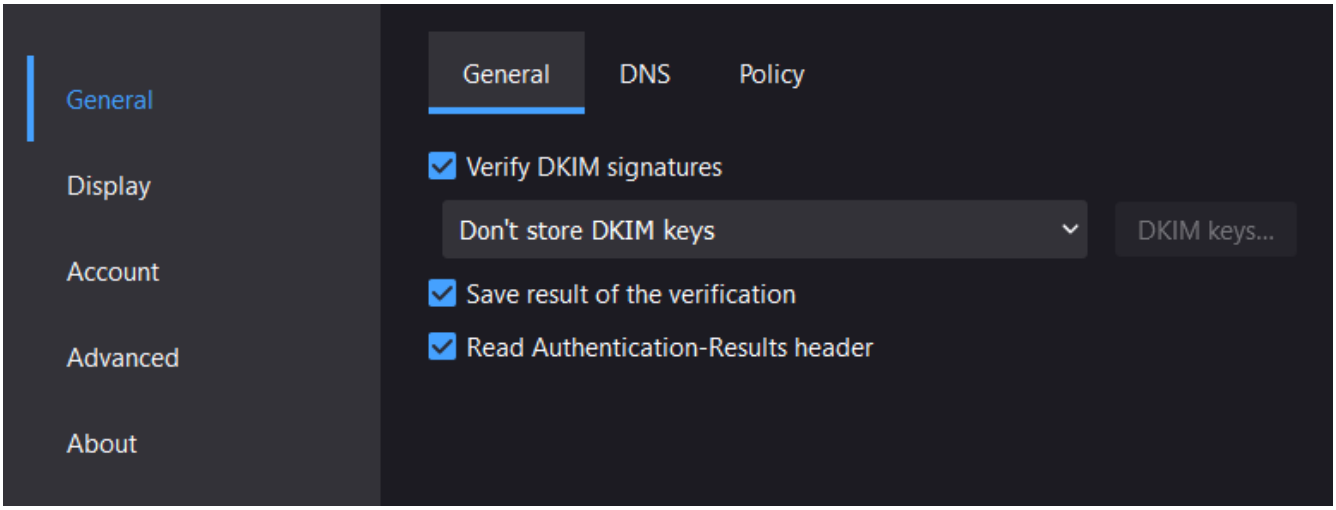
To add the extension to Thunderbird, again press the Alt key then select "Tools" and then "Add-ons and Themes". That will take you to a page with a search bar at the top, enter and search "DKIM" which should take to you to a page like this with the extension and a download button next to it.

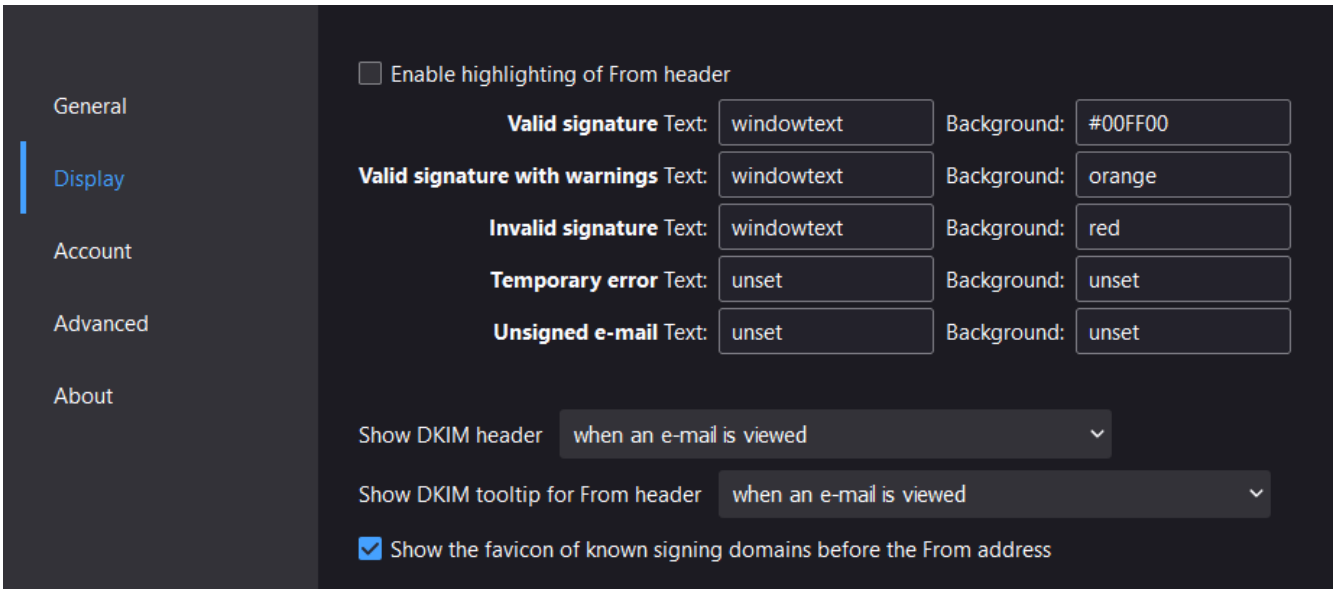


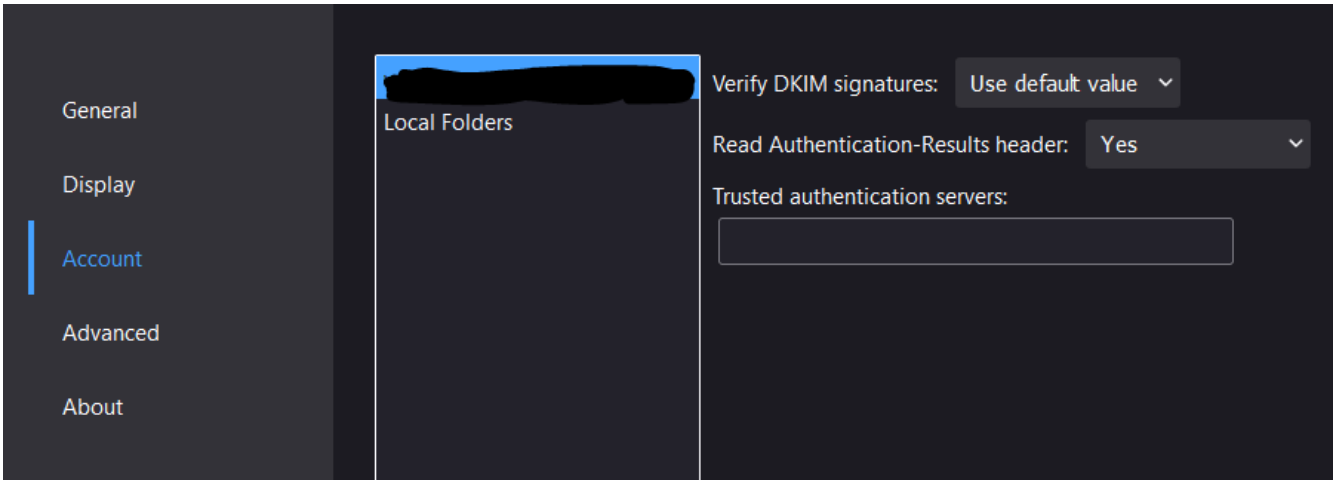
Click the download button and it'll download a file with an .xpi extension. Then go back to the previous page (will likely be the tab to the left like a web browser) and click the gear icon on the right and select "Install Add-on From File"



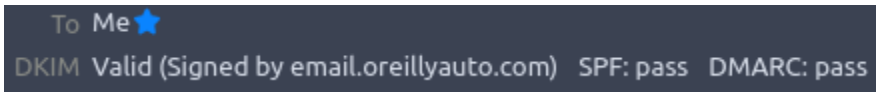
From there select the .xpi file you downloaded a moment ago. Now that it's installed, there's a few configurations I'd recommend making so that it shows you the SPF and DMARC results as well as just reads them from the e-mail rather than running a check itself. To change the setting for the add-on, click the button with the wrench next to it and apply the following configurations.




General
Display
Account
Advanced
About
Enable highlighting of From header
Valid signature Text: windowtext Background: #00FF00
Valid signature with warnings Text: windowtext Background: orange
Invalid signature Text: windowtext Background: red
Temporary error Text: unset Background: unset
Unsigned e-mail Text: unset Background: unset
Show DKIM header when an e-mail is viewed
Show DKIM tooltip for From header when an e-mail is viewed
Show the favicon of known signing domains before the From address



Now instead of running the verification when you open the e-mail when you view it, it should have all the available checks displayed immediately after viewing an e-mail.



Once last thing worth mentioning, don't automatically get spooked if an e-mail is signed by a different domain. It's common for businesses to contract out automated e-mails for stuff like receipts and invoices, so in that case just google the domain that provided the DKIM signature and likely it'll just be one of those services. Essentially the From address will be the business, but the actual e-mail will be generated and sent by the contractor which will likely cause DMARC to fail, but it's not a concern if it's one of the legitimate services that does this, mailgun.com is one I can think of off the top of my head.

Encryption

Encryption will have it's own section however I'll briefly cover the aspects that are specific to e-mail. Another benefit of using an e-mail client is that it gives you the ability to have E2E (End To End Encrypted) with any e-mail provider using the open encryption standard OpenPGP. Most e-mail clients will allow you to generate an OpenPGP pair (one private that you keep secret to decrypt messages and a paired public key that others use to encrypt in a way only your private key can decrypt). The key pair will be associated with one of your e-mail accounts and you'll want to publish the public key some where such as.

https://keys.openpgp.org/

Or on a site/blog associated with you or your online persona, not only so people can send you encrypted e-mails without having previously established contact, but you can also use the private key to sign e-mails or any file to verify it's authenticity, meaning it came from you and hasn't been modified since you signed it.

For sending encrypted e-mail to other people, you'll need to get their public key and import it into your e-mail client. To find other people's public key, your e-mail client will likely be able to search for public keys using WKD or a public key server you give it. If that doesn't work check any blog or websites they have to see if they've posted one there. If neither of those work you could try searching keys.openpgp.org, it's often searched with WKD so unlikely it'll be there if your e-mail client couldn't find it.

https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq#w_how-do-i-get-the-public-keys-of-my-correspondents

If they use an encrypted e-mail service provider, depending on the the provider, you can often find them just searching from your e-mail client. But if that doesn't work you can use the below link to get the public key of a protonmail account.

```
https://api.protonmail.ch/pks/lookup?op=get&search=example.username@protonmail.com
```

by replacing "example.username" with the username of the protonmail account and your browser should download the key.

Also other providers, like mailbox.org, have their own key servers where you can get pubic keys for their accounts.

https://kb.mailbox.org/en/private/e-mail-article/the-mailbox-org-hkps-key-server

RSS

This section isn't primarily about privacy or security, although there certainly are benefits in those regards if you're reading articles in an e-mail client with JavaScript disabled as opposed to a mailing list or web browser. For those of you who are too young to have heard about it or too old to remember it. RSS is an old protocol that was popular in the 00's that would automatically go fetch updates from websites you told it to, the idea being instead of having to spend time browsing the Internet, you could just let the updates come to you and check and see if there's anything new on your favorite sites with just a glance. Also on some sites like YouTube you can avoid relying on their notifications, being logged into an account and generally avoid being at the mercy of *The Algorithm*™ when it comes to what you're presented with.

https://archive.ph/0FBZY

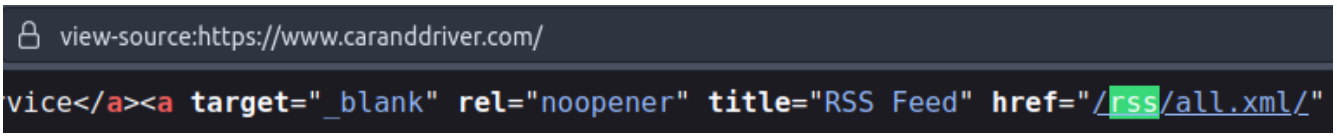
The reason it's included in the same section as e-mail is that nearly all e-mail clients will support having RSS feeds as well as being capable of displaying the articles. The key benefit from this is that not only are RSS feeds generally more convenient and time efficient. If we have JavaScript disabled in our e-mail client we can still view the article without issue, since the page with the article likely won't need JavaScript to format text. As opposed to navigating the website with a browser and likely having to run at least some JavaScript for the homepage to be functional enough for us to get to the new article. Again, this lets us completely avoid most of what's used by advertisers to track and data mine you.

RSS feeds are very simple to add in Thunderbird, the tricky part is finding them for things that aren't podcasts. To add a feed once you've found it, simply right click on "Blogs & News Feeds" on the left hand side and then select either subscribe and enter the RSS feed and set how often you want it to update, or select "New Folder" and name it then do the new process on the new folder. Note that you can have multiple feeds in one folder, each feed doesn't need it's own. Also when viewing articles in Thunderbird, at first they'll be in a window about the size of a quarter of the screen, you can view them in a full sized window by either pressing "Ctrl + O" or clicking the "More" button and selecting "View in New Window" from the options to see it full screen in a new tab.

Finding RSS feeds

Even though RSS has fallen out of favor for everything besides podcasts, it's actually still quite common for websites to have an RSS feed. Thanks to services like WordPress, websites that are built on it will automatically have an RSS feed generated for them. These are usually very easy to find, even if they're not displayed anywhere on the site, by just adding "/rss" to the end of the URL for the home page. This also works on most other sites that support RSS, however sometimes it might not be the home page but on a blog or news page of the site. For example on Michael Bazzell's website the RSS feed for his blog is located at /blog/rss on his site, however some sites are a bit trickier.

Using ESPN as an example. If you simply go to espn.com/rss you'll just get a page not found error. The next trick works quite well, which is to right click somewhere on the page and select "View Page Source". This will open a new tab with the raw code of the website displayed. From here press "Ctrl + F" and type "rss" into the search box and hit enter and if there's any hits, cycle through them and likely one will be next to the URL of the RSS feed. However on ESPN, this doesn't work, at least on the home page. An example of where this does work is caranddriver.com the /rss doesn't work either, but after viewing source and searching for rss you find this.



Usually it'll be a full link such as https://www.caranddriver.com/rss/all.xml however in this case we just take this relative link and add it to the end of the homepage URL to get the RSS feed.

The last trick we can use is to open up a search engine (Google, DuckDuckgo, etc) and use the advanced search operator "site:" followed by the domain we're searching. (In this case the domain would simply be espn.com without "https://" and with "rss" in quotes to emphasize and/or require that in our search results (depends on the search engine), so our search would look like the following.

`site:espn.com “rss”`

Using startpage, my first result was

https://www.espn.com/espn/news/story?page=rssinfo

Which is a page that has links to the many RSS feeds they have for different categories.

One that might surprise you is that YouTube supports RSS as well, although the feed URLs are even more obfuscated. To get an RSS for a particular YouTube channel, take this URL

`https://www.youtube.com/feeds/videos.xml?channel_id=`

and append the channel id to the end and then you can give the new URL to your RSS client. To get the channel id, go to YouTube and one of the videos for the channel you want an RSS feed for and click on the name of the channel which should bring you to the homepage of the channel. The channel id *should* just be a string of random number and digits, if that’s what’s at the end of the URL (after /c or /channel) you can use that. However if instead the channel name is at the end of the URL, you’ll need to right click and choose “View Page Source” again and search for “channel_id” or “rssurl” to get either the channel id or the full RSS URL.

description":"Professor of Internet Happenings.","rssUrl":"https://www.youtube.com/feeds/videos.xml?channel_id=UCR1D15p_vdP3HkrH8wgjQRw"

Just copy that random looking string after “channel_id=” and append it to the URL so we end up with something like this, or just copy the full RSS URL.

```
https://www.youtube.com/feeds/videos.xml?channel_id=UCR1D15p_vdP3HkrH8wgjQRw
```

Which can be given to an RSS client. However be aware YouTube RSS feeds do go down somewhat frequently, so if you do this and get an error, just wait and try again in 30 minutes. The other is that if you’ve disabled JavaScript in your e-mail client, YouTube won’t work at all, however the feed will still give you links to the videos so you can watch them on YouTube in your browser or one of the YouTube alternatives we’ll talk about in another section.

A few more things to note about RSS feeds. Using them in an e-mail client like Thunderbird you can configure rules for RSS messages just like e-mails. So if there’s certain authors or topics you don’t care about on a site you can setup rules to filter them out or vice versa. Lastly when you click or otherwise visit the URLs to a RSS feed in your browser, usually your browser will automatically download the XML file that is the feed. You don’t need to download the file, you just need to give the link to that file to the RSS client and it’ll reach out and download it every so often.

Web Browsing

First I want to mention that it's generally a good idea to have a couple different browsers on your system, not necessarily for "browser isolation" that some people practice, but because generally there's a trade off in terms of privacy and websites working properly. Tools like browser canvas and WebRTC provide various useful functions, on some sites, however are also used for tracking and identifying users. An example is WebRTC is used for live video calls in the browser, which is a commonly used for interviews these days as it doesn't require the interviewee to have any software pre-installed they just follow the link provided by the interviewer and can video call in the browser. The strategy I recommend is having a normie browser, such as vanilla Chromium, reserved for occasions like this with little to no privacy settings, so if you need to access a site that isn't working on your more privacy configured main browser, you can just use your normie one without having to figure out exactly what setting is causing the issue. However I'd recommend having a middle ground browser that you do the majority of your browsing on. For this purpose I'd recommend Brave, Firefox or Librewolf as the overwhelming majority of sites will work on them, however some features you'll need on occasion may not work and you'll need to use your normie browser for it. If you want a browser that's more secure than the ones listed above for occasional, or other wise limited use, I'd recommend the Tor Browser if you'd also like to hide your traffic from your ISP or similar; or Ice Cat if you're more worried about JavaScript or other technologies running in the browser rather than network surveillance.

Browser Configuration

A quick word about Firefox OOTB (Out of the Box) is not a very good browser for privacy, however it's highly configurable and can be made into one. Librewolf is very much just Firefox with a good configuration for privacy OOTB. Although it does lean a little more towards privacy than functionality by having stuff like WebGL off by default, so for example some sites with lots of animations or that play games might not work without turning it back on. The point is with Firefox you'll want to make quite a bit of changes to it for it to be private. Librewolf will be very good out of the box, however *may* require some configuration for use as a main browser depending on what your use case is and how willing you are to have a different

browser reserved for those things. Another option is to use the “Arkenfox” user.js, basically a premade configuration for Firefox, however I know little about it and have never used it, but will drop a link to their github.

https://github.com/arkenfox/user.js/wiki

The section is mostly browser agnostic, however I’ll leave a small guide on configuring Firefox as it does need some changes OOTB. Also this will only scratch the surface of browser configuration as it’s a very deep topic that could easily be the entire length of this document by itself. However this section will provide you with a very good and achievable position to be in.

Below is a privacy configuration guide for Firefox. Overall it’s pretty good, there’s a few things I’d like to add to it from the one below it that I’ll list individually, I don’t recommend all of the ones from the second guide, however feel free to read through it.

https://restoreprivacy.com/firefox-privacy/

https://gist.github.com/0XDE57/fbd302cef7693e62c769

```
network.http.referer.defaultPolicy          0
network.http.sendSecureXSiteReferrer        false
plugins.enumerable_names                    0
geo.enabled                                 false
geo.wifi.uri                                blank
browser.search.geoip.url                    blank
```

uBlock Origin

Probably the most important part of browsing the modern Internet is using the add-on uBlock Origin. It's an incredibly powerful ad blocker which is capable of much more than just blocking ads. The first thing I'd recommend after installing it is going to the settings and the "Filter Lists" tab and enabling all the available default lists provided.

Note: There's a few settings at the top, out of the screenshot you don't need to modify unless you want.

Not only will this enable additional privacy lists that will block various tracking scripts, but the "Annoyances" lists will block stuff like the "Subscribe to our newsletter" and "Accept our cookies" pop ups as well as remove social media stuff like facebook like buttons on none facebook pages, etc making web browsing much less unpleasant.

+ 94,420 network filters + 164,837 cosmetic filters from:

- [x] My filters 12 used out of 13

+ Built-in (6/6)

- [x] uBlock filters 32,000 used out of 32,045
- [x] uBlock filters – Badware risks 4,129 used out of 4,132
- [x] uBlock filters – Privacy 220 used out of 220
- [x] uBlock filters – Quick fixes 210 used out of 210
- [x] uBlock filters – Resource abuse 75 used out of 75
- [x] uBlock filters – Unbreak 1,791 used out of 1,791

+ Ads (1/3)

- [x] EasyList 66,563 used out of 67,181

+ Privacy (1/4)

- [x] EasyPrivacy 26,464 used out of 27,050

+ Malware domains (1/3)

- [x] Online Malicious URL Blocklist 8,493 used out of 8,493

– Annoyances (7/7)

- [x] AdGuard Annoyances 48,779 used out of 53,155
- [x] AdGuard Social Media 16,024 used out of 17,113
- [x] Anti-Facebook 69 used out of 69
- [x] EasyList Cookie 31,996 used out of 32,097
- [x] Fanboy's Annoyance 15,455 used out of 71,104
- [x] Fanboy's Social 23,349 used out of 23,377
- [x] uBlock filters – Annoyances 4,428 used out of 4,432

+ Multipurpose (1/2)

- [x] Peter Lowe's Ad and tracking server list 3,670 used out of 3,673

+ Regions, languages (0/34)

Another convenient tool uBlock has is cosmetic filtering. When you open the uBlock menu, the two buttons on the bottom left are used to block any element on page, such as an image, side bar menu, etc. The one on the end to the left only temporarily block that content until you leave the page, the one to the right of it will create a rule so that the element will be blocked every time you come back to the site.

If you want to go a bit further, from the setting page you can go down to the bottom and check the box “I am an advanced user” nothing will happen at first, but now if you click on the uBlock Origin logo in your browser, the menu will now look something like this.

This is the dynamic filtering list, which allows you to block certain domains on certain sites. I'll leave the official guide for it, but I just want to mention I'd only recommend doing this on your main browser. On your normie browser I'd still recommend having uBlock, but just enable all the default lists and don't enable dynamic filtering, since if you block stuff like 3rd party scripts

by default, it will break lots of sites. Although on your main browser I would recommend following the example used in the guide, blocking 3rd party scripts and iframes globally, but making a global noop rule for YouTube so that YouTube iframes will still work on any site.

https://github.com/gorhill/uBlock/wiki/Dynamic-filtering:-quick-guide

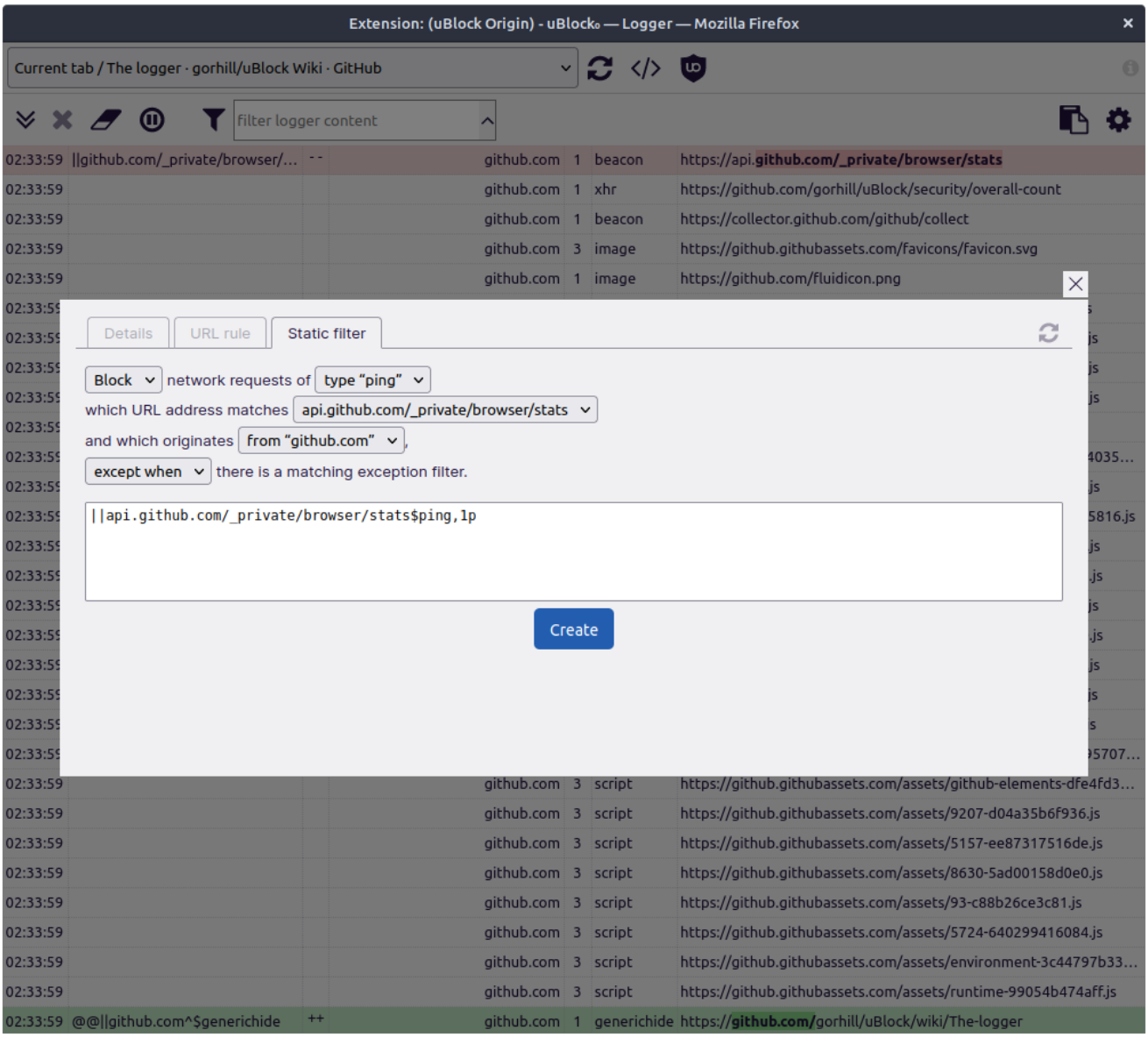
If you do the above config, if you come across a site that's not working correctly, the fastest and easiest fix would just be to give 3rd party scripts a local noop rule on that site and refresh the page. That'll fix the overwhelming majority of broken sites you come across. Another solutions for broken pages that just have articles is to use a reader mode that only needs the site's HTML to work. Firefox has one by default and add-ons are available on Chromium based browsers.

However, if you want to fix a site in a more precise way, allowing the minimal amount of connections, we can utilize the uBlock logger to create more specific rules.

To get to the logger, it's the second icon from the bottom right of the menu that pops up when you click the uBlock Origin icon. To the right of the two cosmetic blocker icons. Once the logger is open, you'll need to refresh the page, as the logger only logs anything when it's open so it'll be blank when you first open it. After refreshing you'll have a list of each connection that was made and why it was or wasn't blocked. Here's the official guide on it.

https://github.com/gorhill/uBlock/wiki/The-logger

It's towards the bottom of the guide, but you can easily create specific static rules not just for a domain, but blocking certain content types from different levels of a domain. For example, if you click on the 2nd column of a connection it'll pop up this window which will allow you to set a very specific rule to block or allow certain connections.



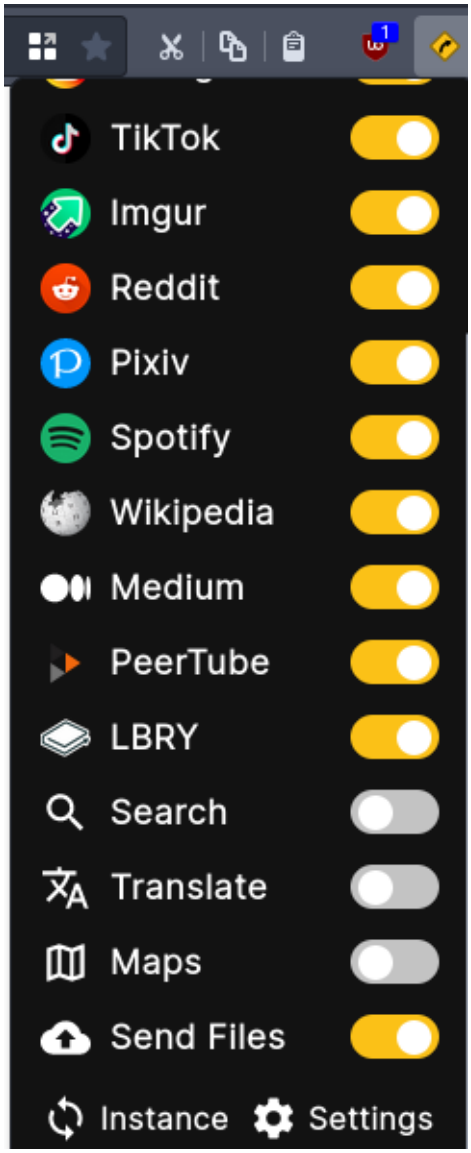
In this example the one blocked connection at the very top was selected. In the static filter, it starts of with a static rule filled out to specifically block that connection. However if I thought I needed to allow this for the website to work (unlikely for a beacon, usually blocked Javascript or CSS is what will break sites) I could change the “Block” to “Allow” and then this specific connection would have a static rule permitting it. Additionally I can adjust the other aspects such as the URL to match “api.github.com/_private/browser” or “api.github.com/_private” to have the rule affect different levels of the domain. Additionally the box with “from github” determines whether this new rule will apply globally or only to github.com. The other option for that box is “from anywhere” which would make this new rule global.

Alternative Front Ends

As you're probably aware, large social media sites are the worst offenders in terms of tracking. Beyond the content you post associated with your account, they also make the most out of utilizing JavaScript to datamine and track individuals across the Internet. Although things like uBlock Origin are great for blocking unnecessary JavaScript, we can also do better when it comes to social media, which is avoiding their sites altogether by using an alternative front end which is essentially a proxy site for that site.

One thing to note about these alternative front ends; something that might be an issue for you is that they can't login to your account with the site. So although they can display the content of the site for you, you won't be able to post on these sites through the alternative front ends nor have curated content as you won't be logged in on the real site.

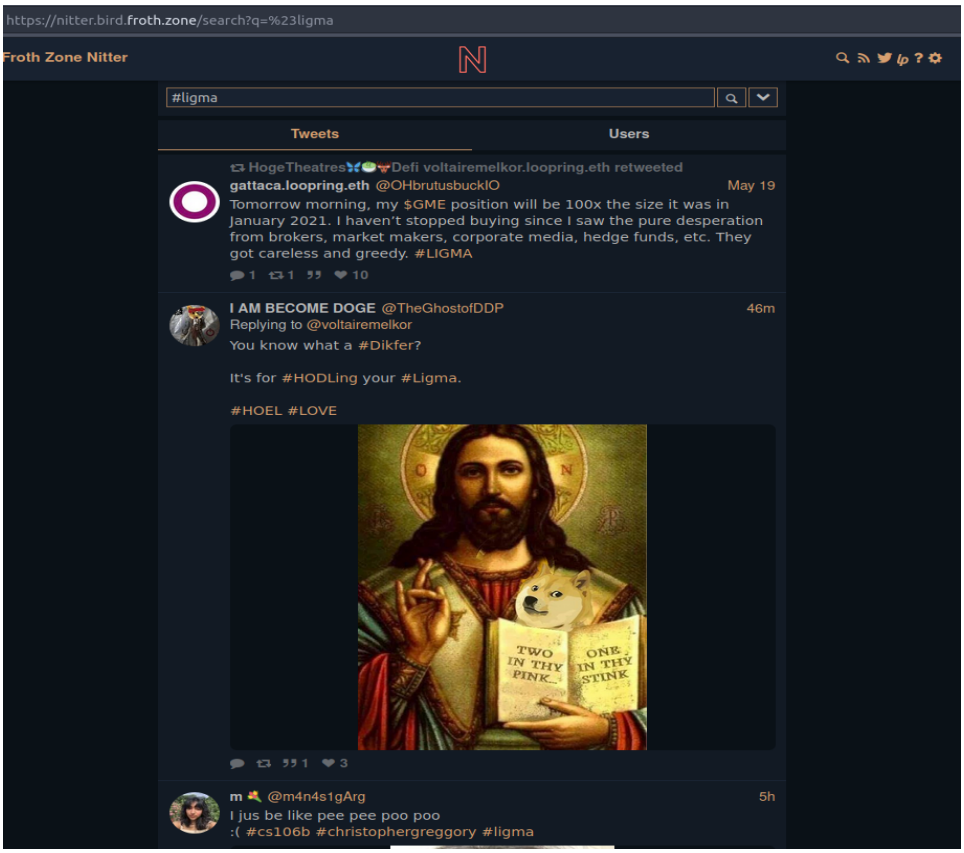
These alternative front ends aren't run on a single large website the way the social media sites are. Essentially they're open source websites that various people run their own instances of, meaning each instance isn't always up and running. This might seem like a big problem, however it's easily solved with an add-on called *libredirect.* It's available on both Chromium and Firefox based browsers and it'll redirect and URLs to large sites like YouTube, Twitter, Reddit and even Wikipedia to an instance of an alternative front end for them (more on them later). It's quite configurable and you can set which sites you would like to be redirected from to an alternative front end. Personally I would recommend turning it off for google maps, search (more on that in the search section) and translate, since unlike the other alternatives, they aren't close to replicating the functionality of the actual sites.



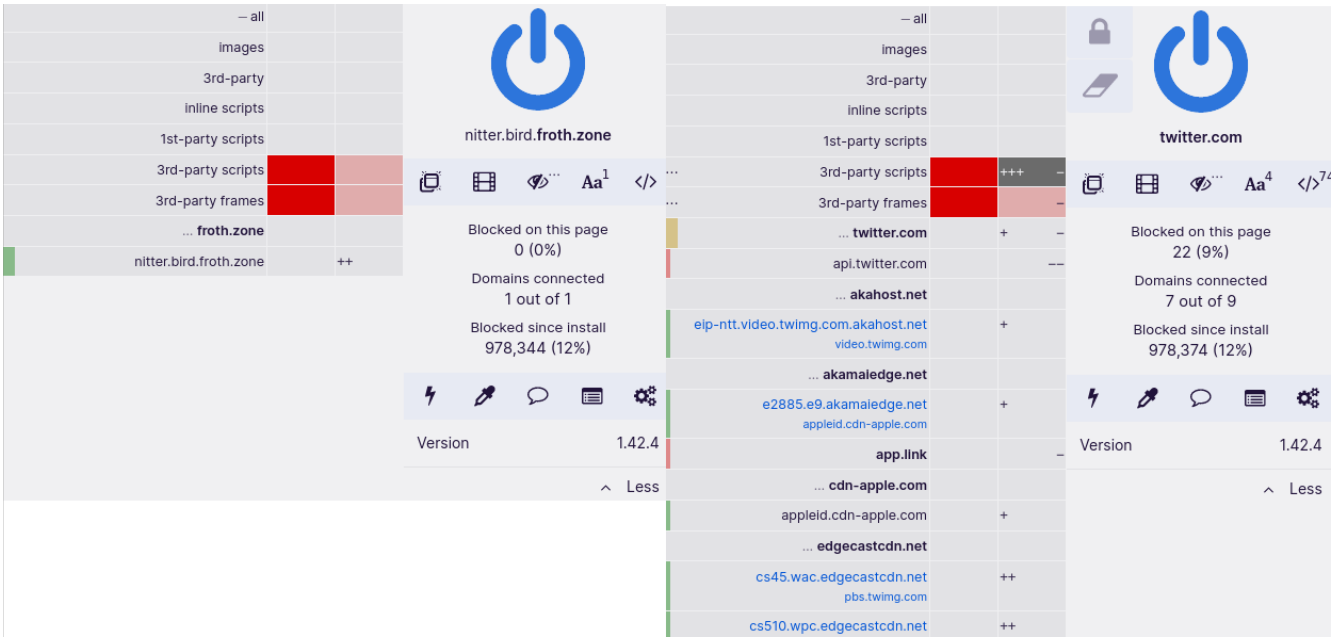
You can update the list of instances (which ones are up and running) via the button at the bottom, or do that from right clicking on the add-on's icon, similarly you can get to the settings that way as well.

In the settings you can set more specific options, such as having preferred instances to use or default options to set when going to a new instance of a specific front end, such default settings for invidious, the primary alternative front end for YouTube. Also for invidious, if you're getting a lot of buffering on a video. It's likely age restricted, it'll play age restricted videos, but the buffering makes it almost unwatchable.

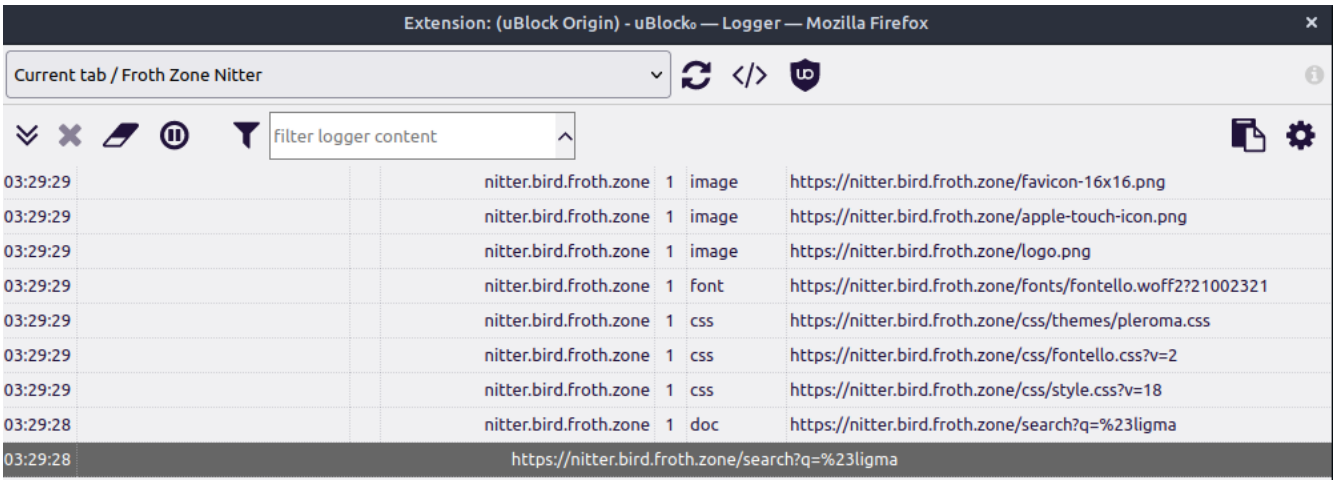
Now to give you an idea of what these alternative front ends do; they pull the page you want from the actual site, however they display it to you through the open source front end they're running. So when you click a link or enter some where like twitter in your URL bar, you'll be redirected to that same page, but view it through nitter instead of twitter. In the example the urt "twitter.com/hashtag/ligma" takes you to this page. From here you can still navigate to other parts of twitter, show comments, search, etc just as if you were on twitter and see the same content. It's also worth mentioning these alternative front ends usually have a lot of different themes and other options to chose from.



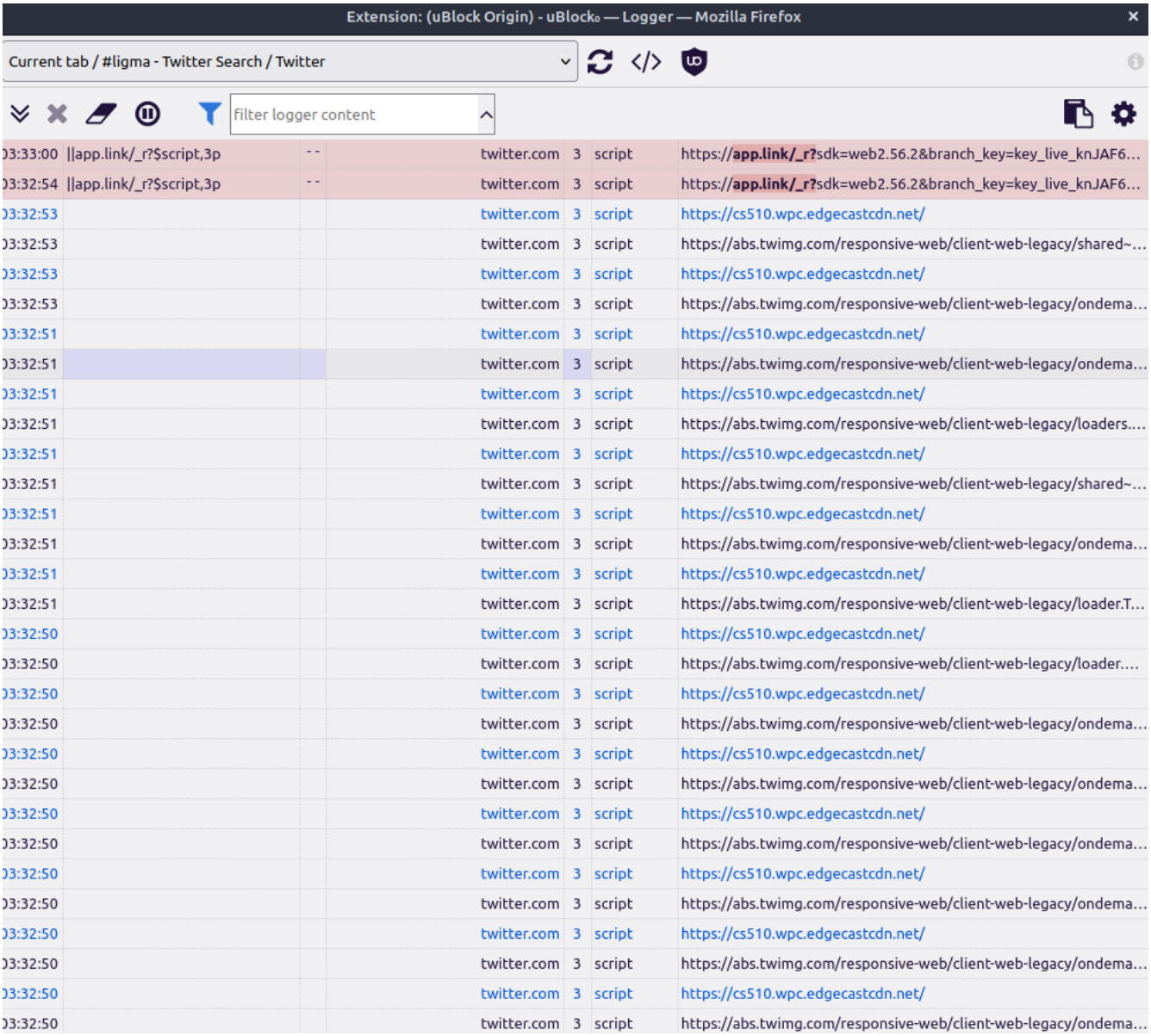
Now as for the main reason we want to use the alternatives in the first place, here's a comparison of what uBlock Origin is blocking on the main site versus the alternative front end.



As you can see, nitter doesn't make any connections out side of it's own domain. Additionally here's the logger for the nitter page. Notice it only requests a document (the HTML page) CSS (styling) and image files, no JavaScript, although there's likely inline JavaScript in the HTML to make things like showing comments button work.



Again for comparison, here's the logger for the twitter page, I filtered it to just JavaScript and there's about 3 windows worth of scripts alone.



```
3:33:00  ||app.link/_r?$script,3p  --  twitter.com  3  script  https://app.link/_r?sdk=web2.56.2&branch_key=key_live_knJAF6…
3:32:54  ||app.link/_r?$script,3p  --  twitter.com  3  script  https://app.link/_r?sdk=web2.56.2&branch_key=key_live_knJAF6…
3:32:53                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:53                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/shared~…
3:32:53                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:53                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:51                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:51                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:51                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:51                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/loaders.…
3:32:51                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:51                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/shared~…
3:32:51                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:51                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:51                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:51                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/loader.T…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/loader.…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
3:32:50                                twitter.com  3  script  https://cs510.wpc.edgecastcdn.net/
3:32:50                                twitter.com  3  script  https://abs.twimg.com/responsive-web/client-web-legacy/ondema…
```

Lastly, if you're a user of one of these sites like Twitter (you post there and don't just lurk) and again these alternatives can't let you post on the sites. I'd recommend just using your normie browser to visit and post on those sites to keep it separate from your main one; although I'd still recommend having uBlock Origin installed, just not with dynamic filtering enabled (advanced user mode). Also, don't forget about the cosmetic filtering! It can be quite useful on some sites.

Search Engines

This section will be quite brief as there isn't too much to discuss here. In regards to private search engines there's two main options, duckduckgo and startpage (there's various other ones such as qwant, swisscows and ecosia). For now I'll just cover duckduckgo and startpage, although most of what I say about them is likely true for the others, with the exception of SearX/SearXNG which I'll get to later.

To be clear both of these do display sponsored links (by default, although it can be turned off) and is implied will involuntarily cooperate with government surveillance programs per their privacy policy.

https://www.startpage.com/en/privacy-policy

https://duckduckgo.com/privacy

I bring this up just because some people on the Internet like to think they stumbled upon some secret plot when they find out that startpage is owned by an advertising company and the founder of duckduckgo was in the business of collecting personal data to profit off of before.

https://en.wikipedia.org/wiki/Names_Database#History (Founded by the same guy as duckduckgo)

https://archive.ph/31zE5

Yes they have sponsored links/ads and likely sell anonymous user search data, other wise they wouldn't be able to run their servers for free of charge. What you're getting with them is that, if their privacy policies are true, the data they do keep is anonymous and not tied to you. Additionally both of them hide your search terms from the sites you visit through their service.

As far as I know, the only differences worth mentioning between the two is that duckduckgo proxies Bing whereas startpage proxies Google. Additionally startpage has a feature called *anonymous view* where they'll render the page on their server and just send you the already

rendered page, so that all the connections to the webpage come from their server and you only connect to the startpage server and not the actual site.

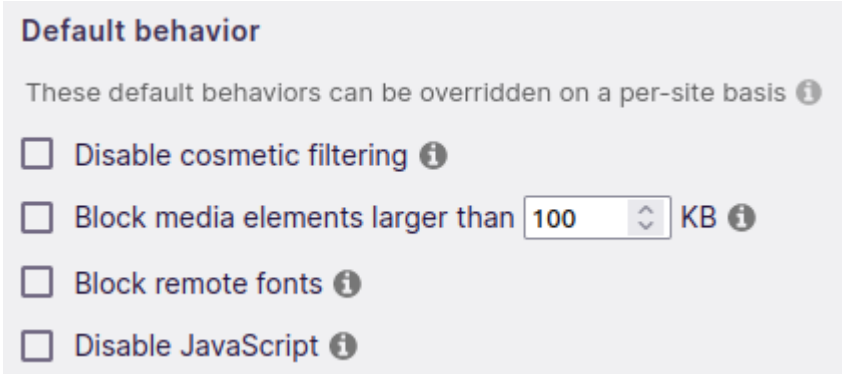
https://www.startpage.com/en/anonymous-view/

Lastly I'll cover SearX/SearXNG (which I'll just refer to as SearX from now on), which is similar to the alternative front ends for social media sites mentioned earlier. Rather than a single site you go to, it's an open source website than many different people run and you just visit a particular instance of someone running SearX. However unlike duckduckgo or startpage, it doesn't just proxy a single search engine like Bing or duckduckgo, but it's a meta-search engine that's highly configurable to use many different search engines and for different types of searches. I highly recommend checking out a SearX instance, however there are a couple downsides to it. In my experience, it doesn't seem to handle advanced search operators well, if at all. Additionally since a lot of people like to make their search engine their home page, the fact SearX is instance based and not a single site can be annoying as instances do go up and down or degrade in performance. Don't let this dissuade you from using it at all, it is fantastic in many regards. However I just wouldn't recommend setting it as your default search engine. I'd recommend just using duckduckgo or startpage as your primary search engines and have a SearX instance on hand for when it might be handy.

Coping with Slow Internet

Although there's not much you can do to improve your Internet speeds, there are ways that you can reduce what your browser downloads and thus improve the the overall experience.

By now you may have noticed that in uBlock Origin, there's an option to block media content over a certain size. By checking the box and having a value there, it'll block content over that size on all sites, however by setting a value and leaving the box unchecked, we can have the value set, but by default uBlock Origin won't block content over that size on pages.



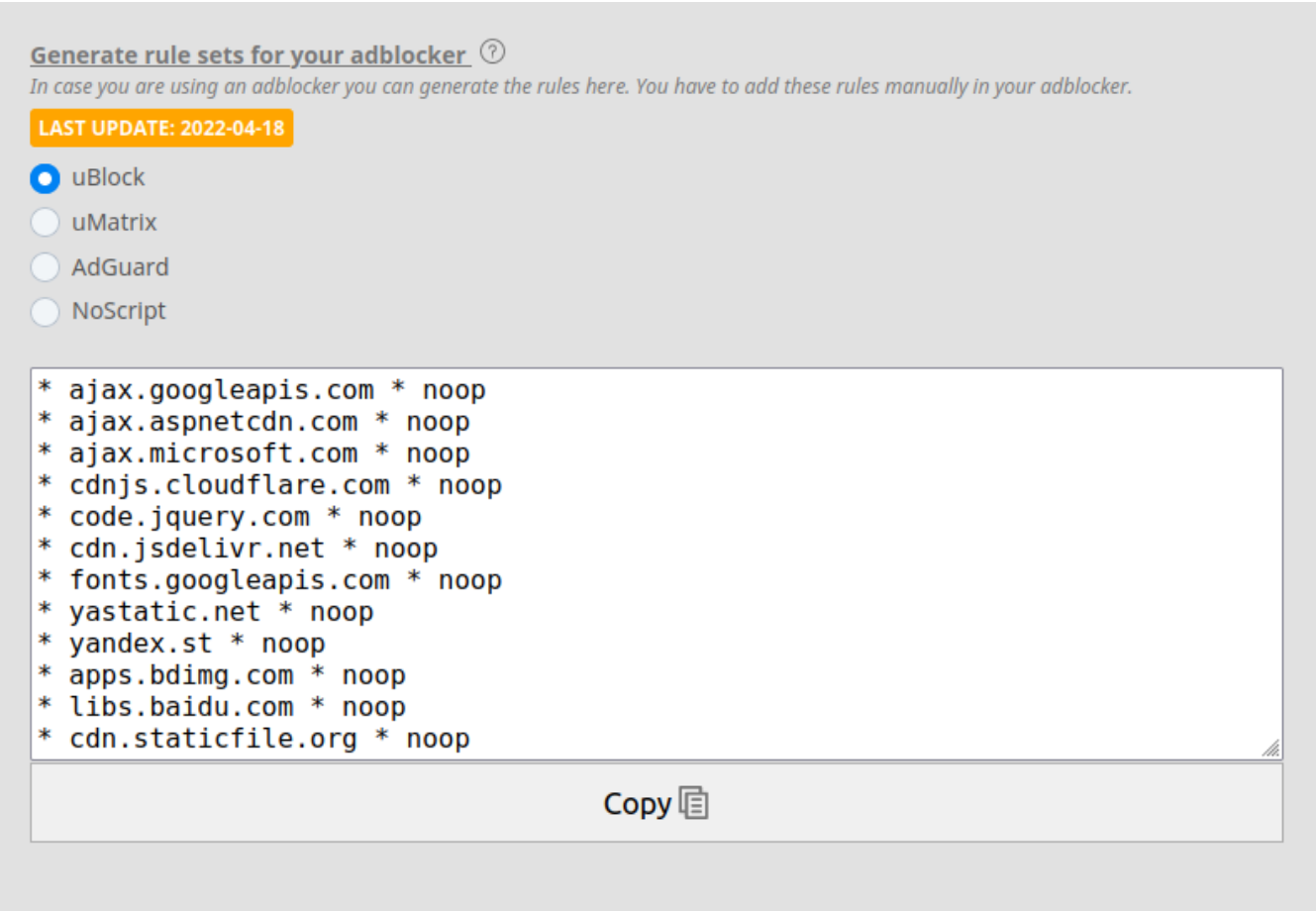
This is useful, because whether we set it to block or not by default, we can still manage it on a per site basis. When you go to a site and click on the uBlock Origin button, the pop up menu provides you the option to enable or disable large element blocking on just that site.

In order from left to right, the buttons decide whether popups, large media, cosmetic filtering, remote fonts and JavaScript are enabled by default; as well as the number of connections that have been blocked, in this case we can see uBlock Origin is blocking 5 large media elements on this page. You can toggle whether each category is allowed simply by clicking the corresponding button and then the lock in the top left of the button to save the changes. The JavaScript option is also worth remembering if you frequently visit a site that's functional without JavaScript.

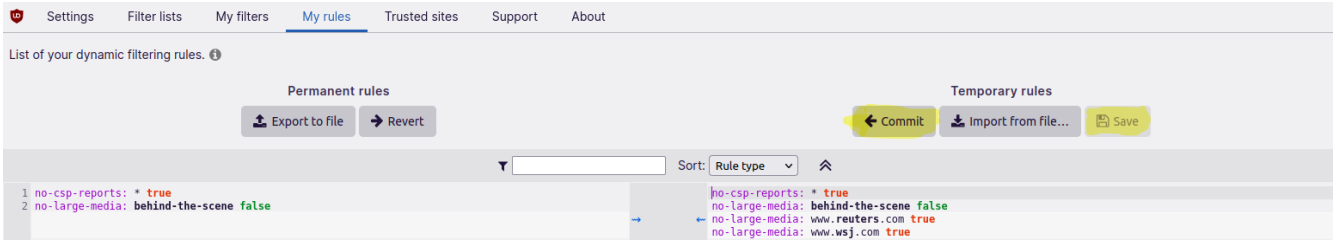
Blocking remote fonts is also a way to reduce what your browser needs to download for a webpage; however, if you choose to do so, I'd recommend just blocking them globally from the same menu we set the media size limit since blocking remote fonts minimally impacts the appearance and function of websites. Some sites this will prevent small icons from being loaded, but again we can reverse blocking on a per site basis just like large media.

Another option is we can install an add-on called *Local CDN.* Without getting too technical, it enables our browser to cache JavaScript and other programming libraries so that when we visit a new webpage that uses a common library, like jQuery, instead of downloading it again each time we visit a site that uses it. Once it's installed it does require one configuration change if we're blocking 3rd party JavaScript with uBlock Origin; to prevent uBlock Origin from blocking Local CDN from fetching libraries we haven't downloaded yet. (I'd recommend doing this step even if you aren't, in case you decide to do so later in the future)

Once installed, left click on the icon for it and press the button with the gear. From there go to the "Advanced" tab and scroll to the bottom section and select "uBlock Origin"



Click the “copy” button to copy them to your clipboard, then go to settings in uBlock Origin and go to the “my rules” tab. Once their, paste the new rules at the bottom of the section on the right, then click the save icon and then “commit” to make these new rules permanent.



Backups

Probably the most important computer maintenance chore people neglect is having backups. In this section we'll cover a few different types of backups and cover their purposes. One thing too keep in mind is there's fundamentally two different types of backups, image backup and file based backups. In computer terminology an "image" is essentially an exact copy of all the bytes of a hard drive or partition. Image's themselves will be a single file on the media we're backing up on however, unlike a zip file, we can't pull individual files we want out of the image file. The recovery procedure for an image file is essentially to take the data from the image file and write it on to the new hard drive. This results in having an exact copy of when the backup was taken be what's restored when we implement the recovery. One thing to remember is that the new hard drive we're recovering the image on must be the same size or larger as the original drive that was imaged. So if we imaged a 500 GB drive, the new drive we recover on must be a minimum of 500 GB. We can recover onto a larger one, such as a 1 TB drive, however when recovering with the image, it won't automatically take up the extra 500 GB and leave it alone. However after recovering we can expand the volume of the recovered system to claim the extra space on the drive.

The other type of back up is backing up files from our system. This is more or less akin to copying files from our computer to a flash drive and can include backing up everything in our home folder

`C:\Users\<user name>`

Windows

`/home/<user name>`

Linux and probably Mac

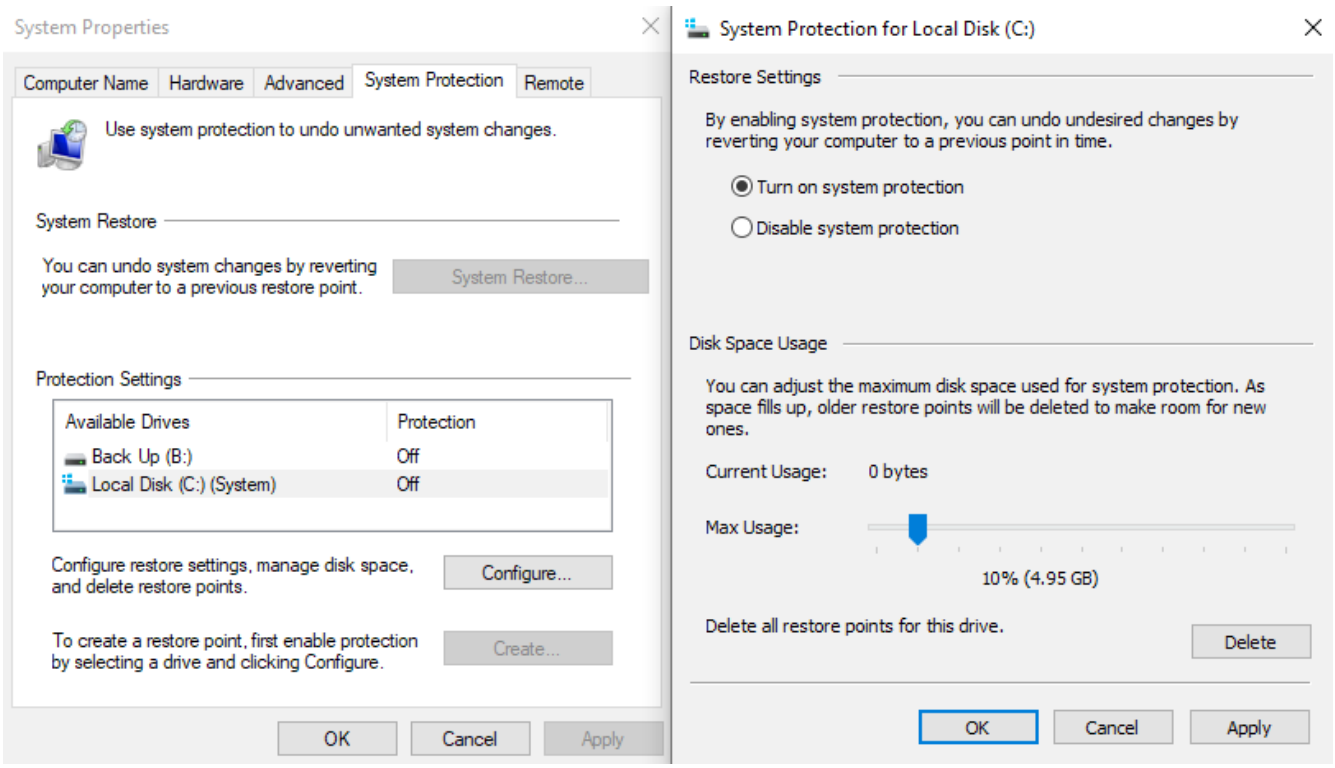
I'll be referring to files in these folders as "user data" and files in folders above these as "system data". The difference user data being the files you create and work with yourself as a

user, whereas system data is where the operating system keeps it's files and configuration data.

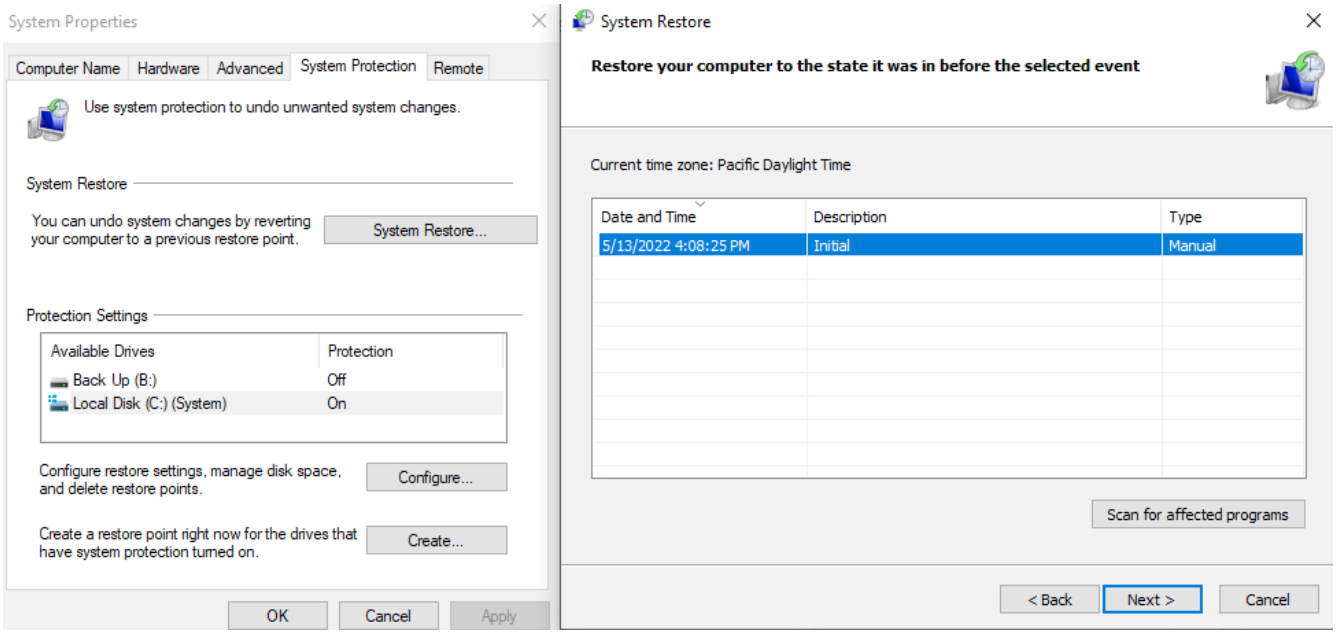
Versioning

The first type of "backup" (technically it's not a backup, but relevant for our purposes) is what I'll call "versioning" although this isn't really a technical name for it either. On Windows this is called the "Shadow Volume" and Mac uses a similar program called "Versions". Linux, as far as I know, doesn't really have an equivalent. On the surface Timeshift seems do this, however it works quite different and so is only feasible for backing up system data, not user data. The reason is that Timeshift makes copies of the files (it's essentially a front end for rsync) whereas on Windows, it takes an incremental image of the drive. Essentially it creates and image of the main C: drive when first installed, then periodically takes another image but only stores the blocks that are different from the previous image. This is a much more efficient method and so Windows Shadow Volumes are able to also work on user data as well as system data. However by default it keeps these backups on the same drive that it's imaging, so although it won't protect you against the drive dying or getting lost, it does provide a way of recovering older versions of modified or deleted files. Additionally since it makes these incremental backups on the same drive it is backing up, you may want to disable it so that it doesn't take up space on your drive. I believe by default it uses about 10% of the drive's space, so on a 250GB drive, that's be 25GB of space being used by it.

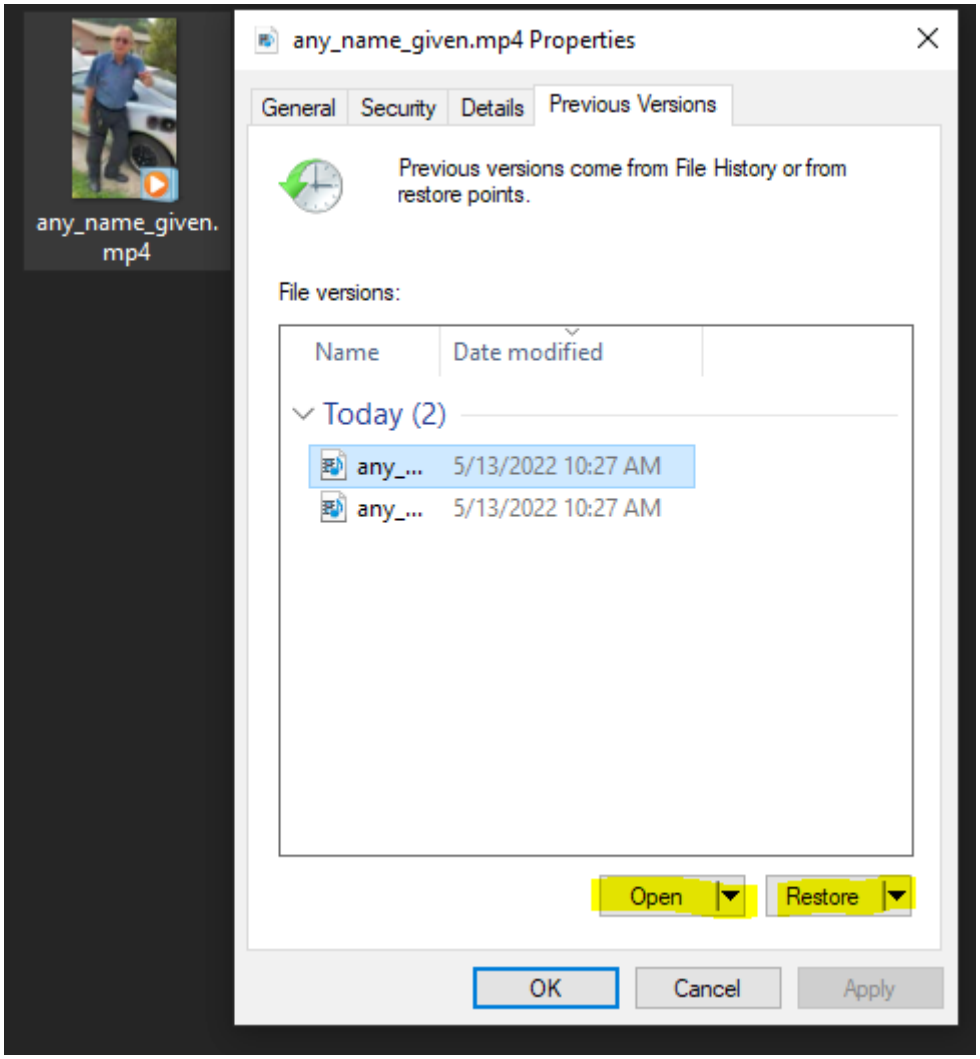
Whether you wish to use it or not, first you should check to see if it's currently being used. To do so, enter "System Protection" in the Windows search bar and something like "Create a restore point" should show up as an option. Once open, it should be on the "System Protection" tab, if not navigate there. From there click "Configure" and you should be presented with the window shown on the right.



As you can see, here you have the option to turn it on or off as well as delete old restore points if you'd like to turn it off. From here you can restore you're entire system from clicking "System Restore" and selecting from the available restore points.



However, if you just want to restore a single file, all you need to do is right click on the file in file explorer and select the “Restore Previous Versions” options. Additionally you can preview the older version to see if it’s the one you want.



For files that are deleted, and for some reason or another aren’t in the recycle bin, you can do the same procedure on the folder that contained the file and view the contents of the folder from the available snapshots.

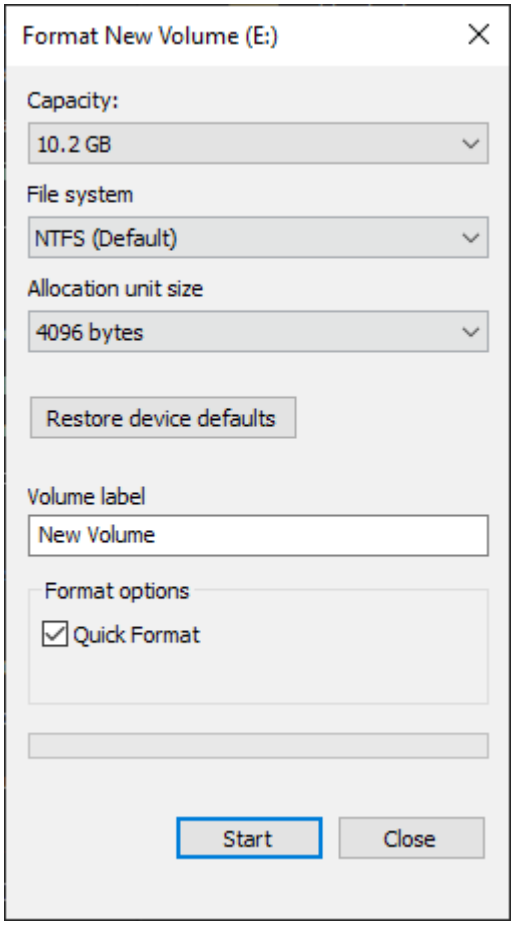
Image Backups

Probably the most important type of backup to do is an image backup, that way our entire system can be restored in the event of a hard drive failure, theft, etc. Ideally, we'd have two backups of our system. One we'd keep in our house and another offsite that could either be on the a cloud provider like Dropbox or Google Drive (although of course we'd want it encrypted) or on a physical device somewhere like a bank safety deposit box or storage unit. That way in the event of something extreme such as a house fire or burglary where our on site backup is stolen, we still have something we can recover from. However I know the vast majority of people won't actually do this, so a more realistic option is to have the onsite image backup and then have a small backup of important files, such as password manager database, scans of personal documents, crypto wallet/seeds, phone backups, etc onto a flash drive that we store offsite or upload to the a cloud provider, however in either case we'd again want these files encrypted.

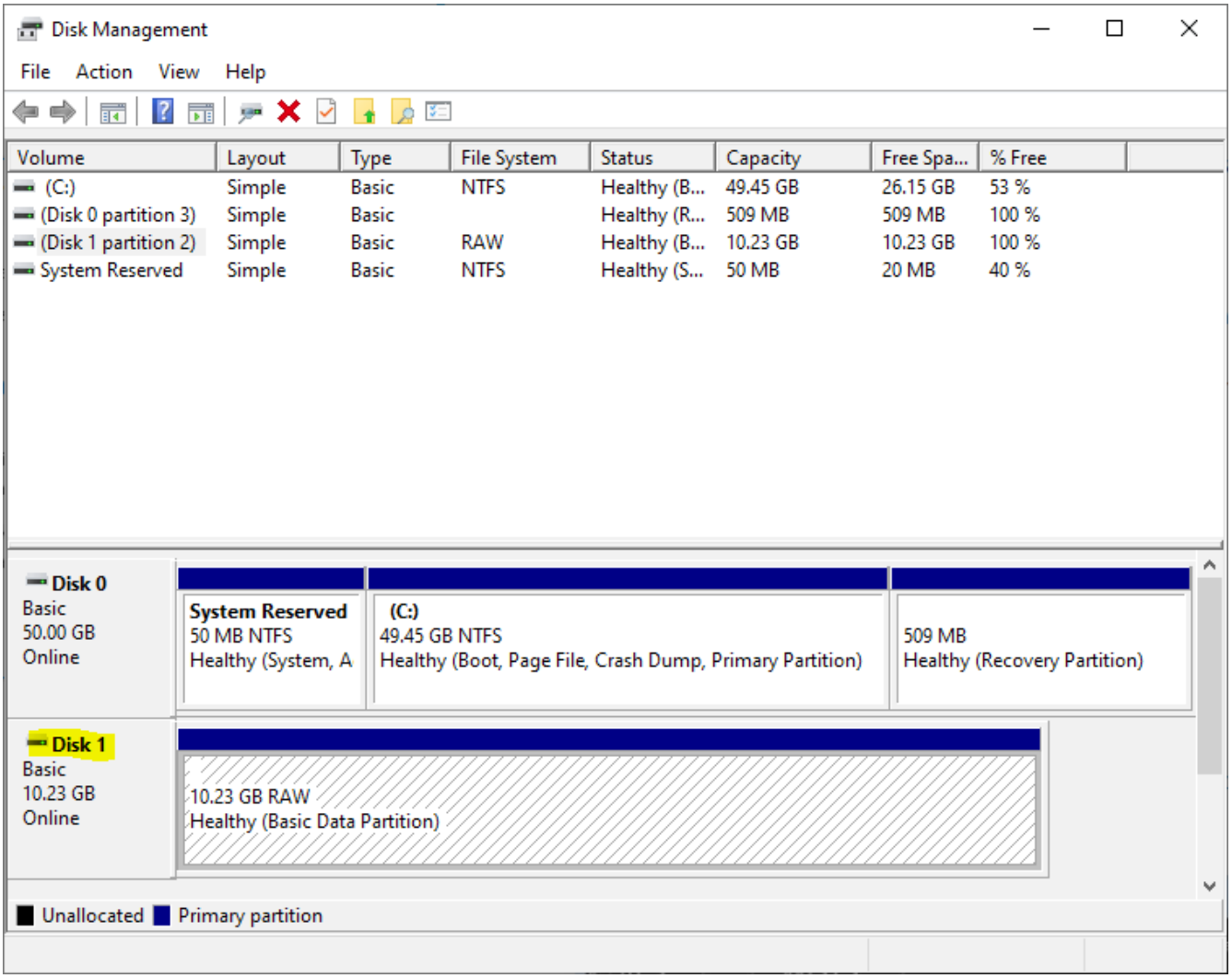
To do an image backup, we'll want an external hard drive that's the same size or larger as the drive that we're backing up. Typically external drives are at least 1TB which should be enough for most laptops, however if you have a desktop with more storage, you may have to shop around for a bigger one. They definitely exist, but are of course a bit more expensive. Many external hard drives you buy will come installed with some sort of backup software on them already, however I've never used them before so can't comment on whether they should be used or not. If you buy one of these drives and wish to do a backup the "proper" way, the first thing you'll need to do is format it to the file system your operating system uses. Not only will this get rid of the preinstalled backup software on them, but it's also a requirement on Mac and Windows for the backup drive to be the appropriate file system. On Mac that would be APFS (Apple File System) and NTFS (New Technology File System) on Windows.

Windows

I won't cover Mac, but I'm sure the process is similar. All you need to do is open File Explorer and right click on the connected drive you'd like to do the backup on and click "format'



This will likely be the default settings and this is what you want, change the volume label to whatever name you like, but the rest is fine. However if when you plug the drive into your computer, it doesn't show up in file explorer, you may need to format it manually. To do this just type "disks" into the Windows search bar and something like "Create and format hard disk partitions" should show up. Click on it and you'll see something like this.



Disk 0 will always be the operating system's disk, we can confirm that since the C: drive is on a partition of Disk 0. From here simply click on the area representing the Disk 1 partition and select "format" from the menu. From here we'll be presented with a similar menu seen earlier when formatting from file explorer, just make sure it's set to NTFS and name the volume what you like and format it.

From here you can now use the built in Windows backup tool to create image backups of your system. I won't go through it here and just leave a link to a guide on it.

https://archive.ph/wip/k6ZRn

Linux

Most distributions will come with a graphical backup tool installed that shouldn't be hard to figure out if you installed Linux, but for the lols I guess I'll cover the 733T haxxor way to do backups on Linux. Once you have your drive formatted and mounted, presumably the external drive will be /dev/sdb and your operating system drive will be /dev/sda and for the example we'll say it's mounted under /media/backup.

The first 733T haxxor thing you'll want to do is zero out the unused space on your drive. This way the unused space of the drive will be easily compressed since it'll just all be zeros. To do this we'll use the following command

```
dd if=/dev/zero of=zero ; rm zero
```

What this command does is pull from an unending stream of zeros and writes them to a file in the current directory called "zero". It'll do this until the drive runs out of space and the command fails, afterwards it'll run the next command that deletes the file freeing all that space.

Now we can create our image. First we'll want to make sure we have the program "pv" installed so we can monitor our progress, it should be in your distro's repository. Next we'll use the following command to create and compress our disk image onto our backup drive.

```
sudo pv < /dev/sda | gzip -c > /media/backup/computer.img.gz
```

To do the restoration, you'd boot Linux from a USB with the recovery drive connected and the new drive installed, and the process would be much the same.

```
pv < /media/backup/computer.img.gz | gunzip -c | dd of=/dev/sda
```

Multiple Hard Drives

I briefly want to cover configuring multiple hard drives, even though it's not really a backup, it can be relevant which I'll get to later. Most of this won't be relevant for laptops, but for desktops, but I will cover using an external hard drive as an extension of your main drive.

The first and simplest option, for desktops with multiple drives, is to put multiple drives on the same volume. This way you could use the combined size of two different drives to act as a single one.

https://archive.ph/wip/vTf6C

For something like a laptop with an external drive that's connected 90% of the time, but not all the time, It'd be better to keep it a separate volume and if you'd like to; you could either mount the drive to a folder, rather than as a drive letter, or create a link to the external drive from somewhere on your C: drive.

https://web.archive.org/web/20220310232323/https://www.windowscentral.com/how-mount-hard-drive-folder-windows-10

Creating a soft link, or shortcut, is very simple. Go to the folder on your main drive where you'll want the link to be (such as your home folder C:\Users\<user name>) and right click and select "New" and then "Shortcut" on the next menu, then you'll be prompted to ask where the shortcut will point to and you'll just select the external drive. Now that shortcut you created will essentially act like a regular folder that stores it's contents on the external drive.

RAID

RAID (Redundant Array of Inexpensive Disks) is a more advanced method of combining of combining multiple drives into one logical one, typically with redundancy as is in the name. Typically most consumer motherboards will only support RAID 1 and 0. However I'd can't really imagine a scenario where I'd recommend RAID 0 for personal use. The purpose of RAID 0 is to improve read and write speeds to the drive by striping data across 2 or more drives. The problem with this, unlike having an extended volume, is that if any disk in the array goes out; you lose *all* the data on the array. As opposed to an extended volume, you'd

only lose what was on the drive that died, you could recover the data that's on the good one(s). Additionally for a personal computer, the performance benefit of RAID 0 won't really make much of a difference; except maybe loading video games however you'd still probably be better off just using good quality SSDs without RAID.

RAID 1 on the other hand is much more relevant. Essentially RAID 1 configures two drives to be exact copies of each other. So if you put two 1TB drives into RAID 1, the operating system would see one 1TB drive. However you really have two drives with exactly the same data on them, so if one drives that data is still there and usable, you just replace the bad drive and rebuild the array. Now you may have heard the maxim *RAID is not a backup.* For enterprise purposes it's true, however I think it's fine for personal use. The reason being, the main concern of personal backups is hard drive failure. Since we're talking strictly about desktops, since laptops that can do RAID are very rare. Plus most people who do backups will use an external drive they'll leave connected to or close to their computer. Meaning in the event of a home burglary, fire, flood, etc. The backup drive is likely to be lost if the computer is. Again I encourage everyone to have some kind of offsite backup, whether it's a full backup or just your most important files. Additionally personal computers have the recycle bin (even most Linux distros have an equivalent now) and Shadow Volume to recover from accidental deletion, unlike most servers. Point being, for personal use, I believe RAID 1 qualifies as an on site backup.

I can't give too much info on configuring RAID 1, since it's done in the BIOS/UEFI of your computer. You'll need to look up your computer's motherboard model to see if it supports RAID and how to configure it. Generally to get to your BIOS you'll press a key like "Delete" or "F11" during the boot process to enter it, you typically have a brief window to do it, so usually you just spam that key after turning your computer on until it loads you into the BIOS. Also for Windows, you'll likely need to install drivers specific for your brand of CPU (AMD or Intel). These are typically available from your motherboard manufacture's website and if you're installing Windows onto a RAID array, you'll likely need the driver on a flash drive so that they can be installed before Windows is installed, otherwise the Windows installer won't be able to utilize the RAID array.

https://archive.ph/Jhgq3#Installation%20of%20RAID%20driver%20with%20Intel%20Controller

Note this guide is for Dell servers, however the process is basically the same for consumer AMD and Intel CPUs, just know that your motherboard’s manufacturer site should make it very easy to find the correct drivers.

Android

I won't be covering iPhones, due to my lack of experience and knowledge of them, however the section on ad blocking should be applicable to iPhones as well. I'd also like to briefly cover custom ROMs for Android. Custom ROMs are typically forks of Android that have all of the tie ins to google removed, although google services can be installed on them, it kind of defeats the purpose of having a custom ROM in regards to privacy. Additionally if you're considering a custom ROM, I'd highly recommend first trying an alternative to Google maps and see if you'd be fine using it. Because Google maps is probably the most likely thing to make or break using a de-Googled phone versus a regular Android one. Another consideration is that with a de-Googled phone, your contacts and such won't sync with Google and thus you'll need to perform your own backups with your phone, which I'll cover here. I won't go too much more into custom ROMs, I'll leave a link below to a resource that has more information about FOSS applications and such, however I'll just mention the big 3 are GrapheneOS, LineageOS and CalyxOS. LineageOS seems to be falling out of popularity to the other two and GrapheneOS is only support on Google Pixel devices. Additionally you should verify that a custom ROM supports your make and model of phone. Close enough isn't good enough, if you have some slight variant of a supported phone it likely won't work on that variant.

https://gofoss.net/intro-free-your-phone/

It's also still worth checking out this guide even if you don't plan on using a custom ROM as it has a list of a lot of FOSS apps to replace Google and other privacy violating ones with.

Something else I want to mention; if you plan on attending some type of event where the government may monitor cell phone activity in the area of it or subpoena information from cell carriers afterwards. Your best bet is to simply not bring your cell phone or if you do, have it in a faraday bag to block any emissions. Air plane mode isn't enough to block location tracking and I don't think it's worth taking the risk of just turning it off since we can't be sure some parts of the phone aren't still running on some kind of low powered mode.

https://archive.ph/2CGZO

Additionally it's worth considering taking this point even further in that really the endgame of privacy is to simply do things in real life as opposed to the Internet.

https://odysee.com/@Luke:7/if-you-really-care-about-privacy,-don't:0?&sunset=lbrytv

Ad Blocking

One issue with phones is that typically mobile browsers don't support add-ons and we're also likely using apps which have no reasonable method of modifying or configuring them to not see ads. The way around this is to block ads at the DNS level, not only will this work in the browser, but also other apps if they pull their adds from an advertisers domain (example, youtube ads likely won't be blocked since they're served from a youtube domain). Really quick, DNS is the protocol that's used to get the IP address for a domain such as google.com. What DNS ad blocking does is use a DNS server that's configured to not return an answer for domains used for serving ads so that your device gives up making a connection to it and thus the ad is never loaded.

This may be different on newer Android phones, but most won't let you change the DNS server your phone uses. The way to configure it on your phone is to install a secure DNS app that will create a split tunnel VPN (it'll send your DNS traffic over the VPN connection, but not any other traffic) which means it will consume the "VPN slot" on your phone. There's multiple options for this including *Rethink DNS* and *AdGuard for Android* the later shouldn't be confused with *AdGuard Content Blocker* which ties into a browser. Rethink is completely free, whereas AdGuard has some features restricted to paying customer, however the free features are more than adequate. Once installed I'd recommend playing around with the settings for it, I believe AdGuard blocks ads by default, but I think with ReThink DNS you have to enable the ad blocking lists in the app. Additionally they have other settings and features worth checking out. Another potential benefit of this is that sometimes it can get around website filtering since the DNS queries will go over the VPN and not seen by the local network or DNS server.

Lastly you can also implement this across your home network by setting the DNS server on your router to an ad blocking DNS server, such as AdGuard's. Obviously the steps to change the DNS server will be different on different routers. But the general idea is you'd go to AdGuard, or whoever's site, and get the IP addresses of their ad blocking servers. Here's AdGuard's

https://kb.adguard.com/en/general/dns-providers#adguard-dns

On your home router, you'd just want to use the normal "DNS IPv4" IP addresses. I'll cover secure DNS in another section, but it's something you'd setup on your computer or phone not on a consumer router with stock firmware.

Keyboard

Something else we'll want to do on a regular Android phone is replace the stock keyboard program with a FOSS one. Regardless of how secure the messaging apps you use, if you're using the stock keyboard Google will have access to whatever you type. One I know of and use is *OpenBoard* which will likely have more and better features than the stock one as well as prevent Google from having easy access to everything we type.

Encryption

One thing you'll certainly want to do on your phone is encrypt it. I believe iPhones do this by default and probably some Androids do, however double check if yours does. The reason it's so much more important on phones rather than computers is that our phones are much more likely to be lost or stolen than a desktop or laptop computer. A PIN or pattern to unlock the phone isn't enough by itself, because a tech savvy person could still read the data off of the phone as a regular drive, without having to boot into the phone and get through the login prompt. Encrypting even an older Android phone is very easy. Again it'll vary a bit depending on the exact phone. But generally you'll first need to set some kind of login challenge whether it's a PIN or connect the dots pattern thing. Afterwards go into the security settings and poke around until you find the option to encrypt it. It'll likely require you to have the phone plugged in while it encrypts the drive. Additionally there's very little to no

performance penalty for having an encrypted drive apart from maybe slightly longer boot times when turning the phone on.

Backups

This section will be very important if you use a custom ROM, as Google won't be automatically backing up your contact and/or other user data automatically. I'll only cover ADB (Android Debugging Bridge) on your computer, since it'll apply to any Android phone, custom ROM or not. However it's worth noting some companies like Samsung have their own programs for doing backups, however I believe there is only available for Windows. I'll leave a guide to making backups as well as removing preinstalled apps with ADB.

Setting up ADB

https://web.archive.org/web/20220521041833/https://www.xda-developers.com/install-adb-windows-macos-linux/#adbsetup

Full Backup with ADB

https://web.archive.org/web/20220511203352/https://9to5google.com/2017/11/04/how-to-backup-restore-android-device-data-android-basics/

Export contacts to file without ADB

https://web.archive.org/web/20220209000634/https://support.google.com/contacts/answer/7199294?hl=en&co=GENIE.Platform%3DAndroid

Additional info on ADB

https://wiki.gentoo.org/wiki/Android/adb

Encryption

Asymmetric Versus Symmetric

Symmetric encryption is what you typically think of when you think of encryption. With symmetric encryption the data is encrypted and decrypted with the same key. It's by far the most commonly used form of encryption, because it's much more efficient and straight forward; however in order for it to work you have to have some way of securely giving the shared key to the recipient which can be an issue. Asymmetric encryption can solve this issue as well as do some other interesting things. Asymmetric encryption works with key pairs, one public and one private, usually associated with an individual or organization. How it works is you encrypt the data with the public key and then the data can only be decrypted by the private key. This allows you to send encrypted communications/data to people without having first shared a key through some other channel. Additionally the private key allows us to digitally sign data that verifies it hasn't been modified from when it was signed, as well as it came from someone who has the corresponding private key to the public key that verified the signature. This is most often used for programs to ensure you're installing exactly what the developers published and not one modified by a 3rd party. However it can also be used for anonymously verifying online personas. If you have some type of presence on a particular site, you could publish a public key associated with your persona and later you could verify that you're the same person somewhere else by signing something with the private key that can be verified with the public key you shared previously.

Key Versus Password

Something else to keep in mind with encryption is key versus password based encryption. As you might guess with password encryption, the key is derived directly from the password given. With key based encryption the encryption key is randomly generated to a predefined length. The only thing you really need to know is that key based encryption is orders of magnitude more secure than even a good password. Often encryption keys will be encrypted with a password, to add an additional layer of security. However the concern with keys is that if you lose the key, even if you remember the password for it, you'll lose the data yourself at

well. Password based encryption is more forgiving since as long as you remember the password you'll be able to decrypt the data.

File Encryption

We'll start with just encrypting individual files. This is useful if you don't encrypt your hard drive, but have some files with important information you'd want to protect in the event your device is lost or stolen (although drive encryption takes care of that for all your files) or if you're sending a file to someone through means you don't completely trust, like e-mail or some sort of cloud provider. The easiest and most cross platform option is to use 7zip to create encrypted zip files of a single file or a folder. It only supports passwords, but that should be adequate for most circumstances, just send the password through some other channel such as text or other messaging app so that anyone who manages to stumble on the encrypted file on the Internet won't have access to it.

If you want to sign or encrypt a file with a key you'll need to have GPG installed. This is typically installed by default on Linux and can also be installed on Windows with gpg4win which also includes the graphical interface Kleopatra. Kleopatra integrates nicely into Windows, you simply need to right click on a file or folder to encrypt, sign or decrypt the files. Additionally you can easily generate keys in Kleopatra by opening it and going to "File" and then select "New Key" and choose to create a new OpenPGP pair and at the screen where you fill in the name and e-mail (doesn't have to be real, it's not verified) click "Advanced Options" and set it to RSA, either 3072 or 4096.

To encrypt a file with an RSA key pair, you'll first need to import the public key of the recipient into your key ring (In the e-mail section I go over finding someone's key). Once you've downloaded the key, again just go to "File" from within Kleopatra and select "Import" and then select the public key file you want to import. Afterwards when you encrypt a file with Kleopatra, it'll prompt you with which key you'd like to encrypt it with.

Disk Encryption

Although disk encryption may seem like overkill, I'd still recommend it particularly on laptops you take with you places. To reiterate, an unencrypted drive can be read more or less like a regular thumb drive without having to give the login credentials when booting the operating system. Now if for some reason or another, we don't want to encrypt our drive (I'll get to that later) we also have the option of encrypted containers which are more or less sections of a hard drive that are encrypted rather than the whole thing.

The best time and manner to encrypt a device is when the operating system is installed and using the operating system's built in tool. Both Mac and Windows have built in tools that can be enabled at any time without losing the data already on the drive. I could be mistaken, but I don't believe you can encrypt drives on Linux and preserve the data already on there. So it's much better to do it during installation (this is very easy, almost every distro it's just a checkbox you select during the install) although I suppose it's possible to backup you're data somewhere, reinstalled the operating system with encryption and then migrate your data back over. Although regardless of operating system you should do a backup before encrypting, even with the built in tool.

https://web.archive.org/web/20220313080435/https://www.windowscentral.com/how-enable-device-encryption-windows-10-home

Above is a link to a guide on enabling a disk encryption on Windows 10 Home, since BitLocker is only available on pro and above, however the Windows option requires that your mother board have TPM, which yours may not. Again I'd highly recommend going through the guide trying to enable TPM before resorting to the next option as first party tools are much less likely to have issues than third party ones, especially with something like encrypting the system drive. However this part is also relevant for non Windows users, because VeraCrypt is cross platform so is great for external drives as well as making encrypting containers on any operating system. However first I'll cover a related topic which is verifying file signatures, which is something we'll want to do when installing VeraCrypt.

Verifying Signatures

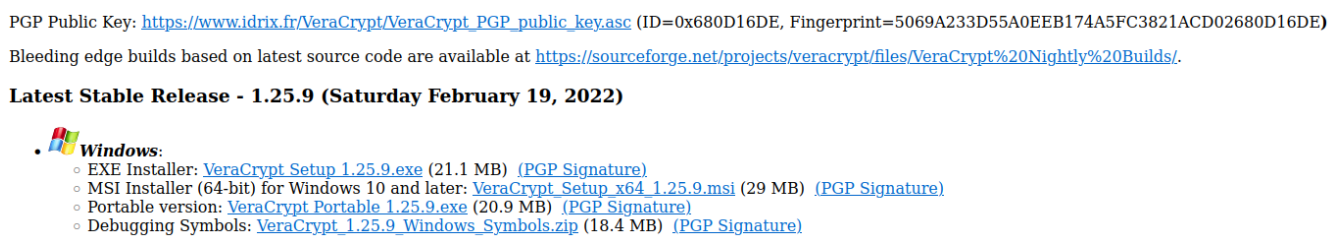
Previously we discussed how private keys can be used to sign files so that the authenticity and integrity of a file can be verified. Although most of the software you download of the Internet won't have this option, for important programs such as VeraCrypt, Tor Browser, Installation images, etc. It will usually be provided and we'll want to verify it ourselves. For example, a few years ago the Linux Mint installation image was replaced with a malicious one, verifying the signature would've shown that the malicious one wasn't signed by the Mint developers and you could have avoided installing it.

https://archive.ph/dctSs

For this example I'll be doing it on Windows using Kleopatra, which means you'll need to have gpg4win installed (Kleopatra will install along with it). For using GPG from the command line on Linux, there's plenty of guides out there on doing that.

To begin, we'll first go to the download page of VeraCrypt's site.

https://veracrypt.fr/en/Downloads.html



PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)

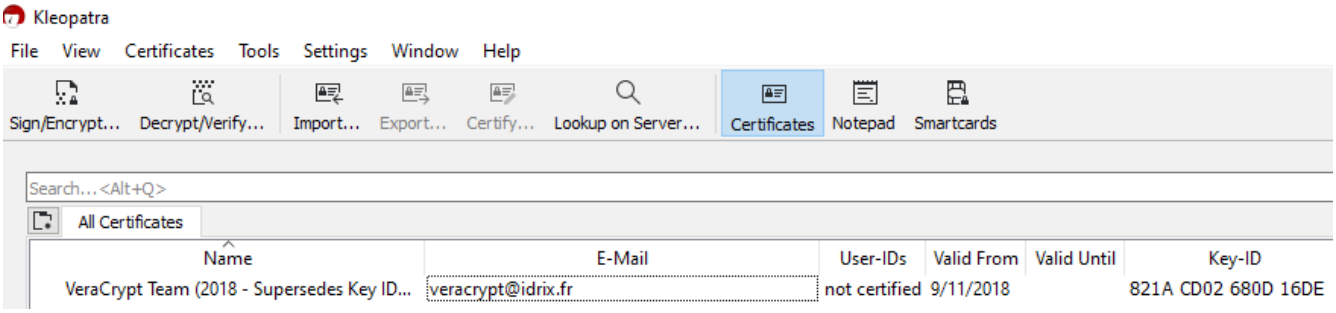
Bleeding edge builds based on latest source code are available at https://sourceforge.net/projects/veracrypt/files/VeraCrypt%20Nightly%20Builds/.

Latest Stable Release - 1.25.9 (Saturday February 19, 2022)

- **Windows**:
  - EXE Installer: VeraCrypt Setup 1.25.9.exe (21.1 MB) (PGP Signature)
  - MSI Installer (64-bit) for Windows 10 and later: VeraCrypt_Setup_x64_1.25.9.msi (29 MB) (PGP Signature)
  - Portable version: VeraCrypt Portable 1.25.9.exe (20.9 MB) (PGP Signature)
  - Debugging Symbols: VeraCrypt_1.25.9_Windows_Symbols.zip (18.4 MB) (PGP Signature)

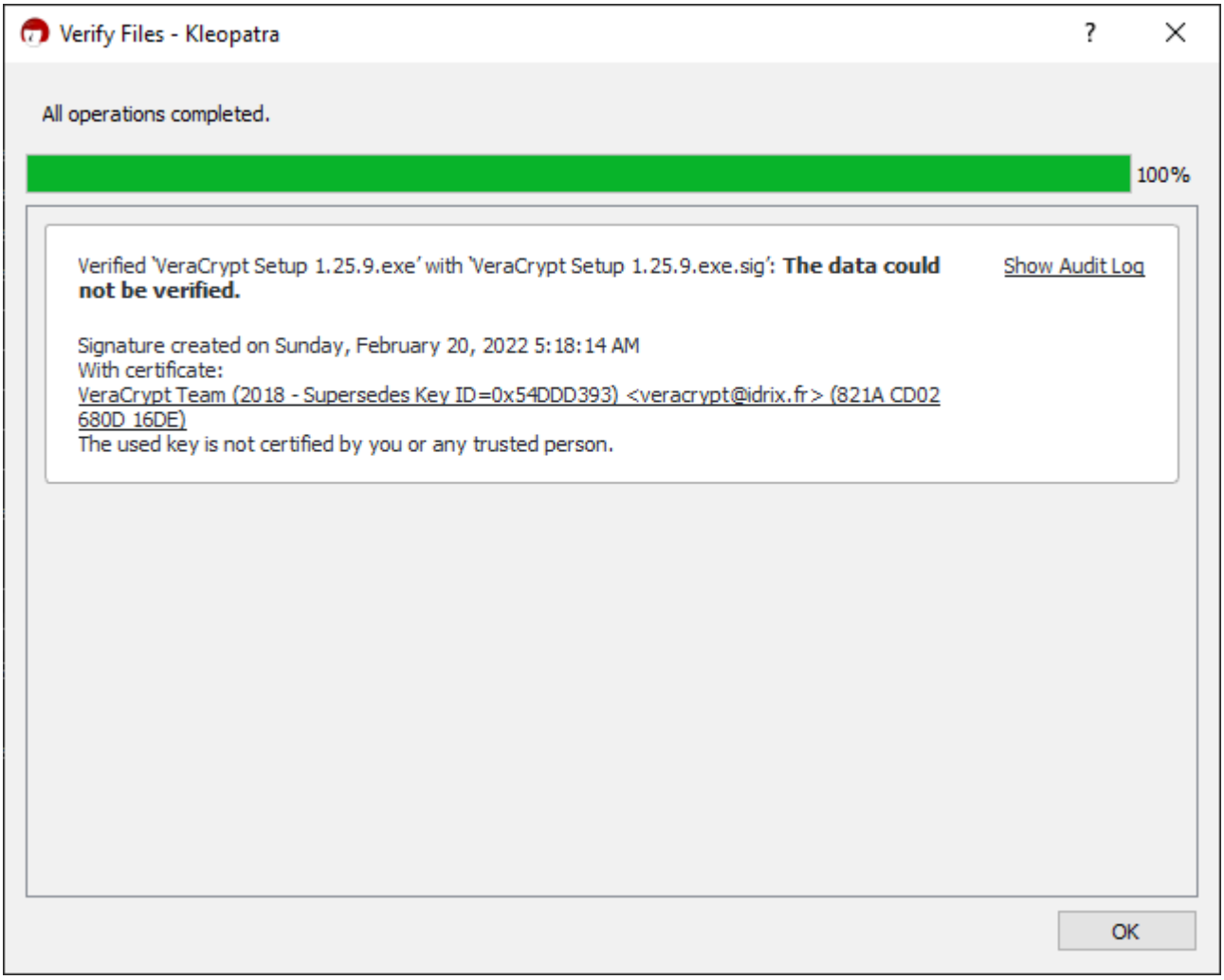
As you can see they provide a link to their PGP key as well as show the fingerprint of it. Additionally you can see the signatures our separate files next to their respective installers, we'll want to download both the installer and the corresponding signature and have them in the same directory (your Downloads folder is fine).

First you'll want to download the public key so it can be imported (To download it, right click on it and select "Save Link As" the default name and location is fine). Then open file explorer and right click on the file and you should see an option "More GpgEX options" if you have gpg4win and Kleopatra installed. From that sub menu select "Import Keys" and then a window should pop up telling you one key as been imported. If you then open up Kleopatra it should like like this.



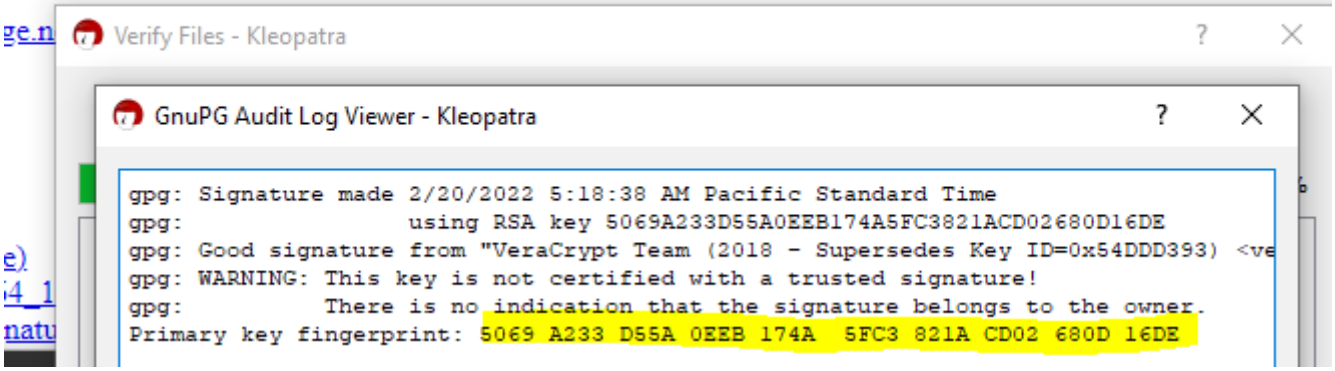
You'll note that it's labeled as "not certified". This just means that your computer doesn't know it can trust this key, however that's not necessary to verify the signature, but if you do want to certify it right click on the key and select "Certify" and you'll then be prompted to make your own key pair if you don't already have one. Again this is unnecessary and we can verify it without certifying it.

Next we'll want to download either the exe or msi installer from the website along with it's corresponding signature file, both need to be in the same folder and the default Downloads folder is fine. From here we'll simply open File Explorer and right click on the installer file (the one that *doesn't* end with .sig) go to "More GpgEX options" and select "Verify". Afterwards we'll be presented with something like this.

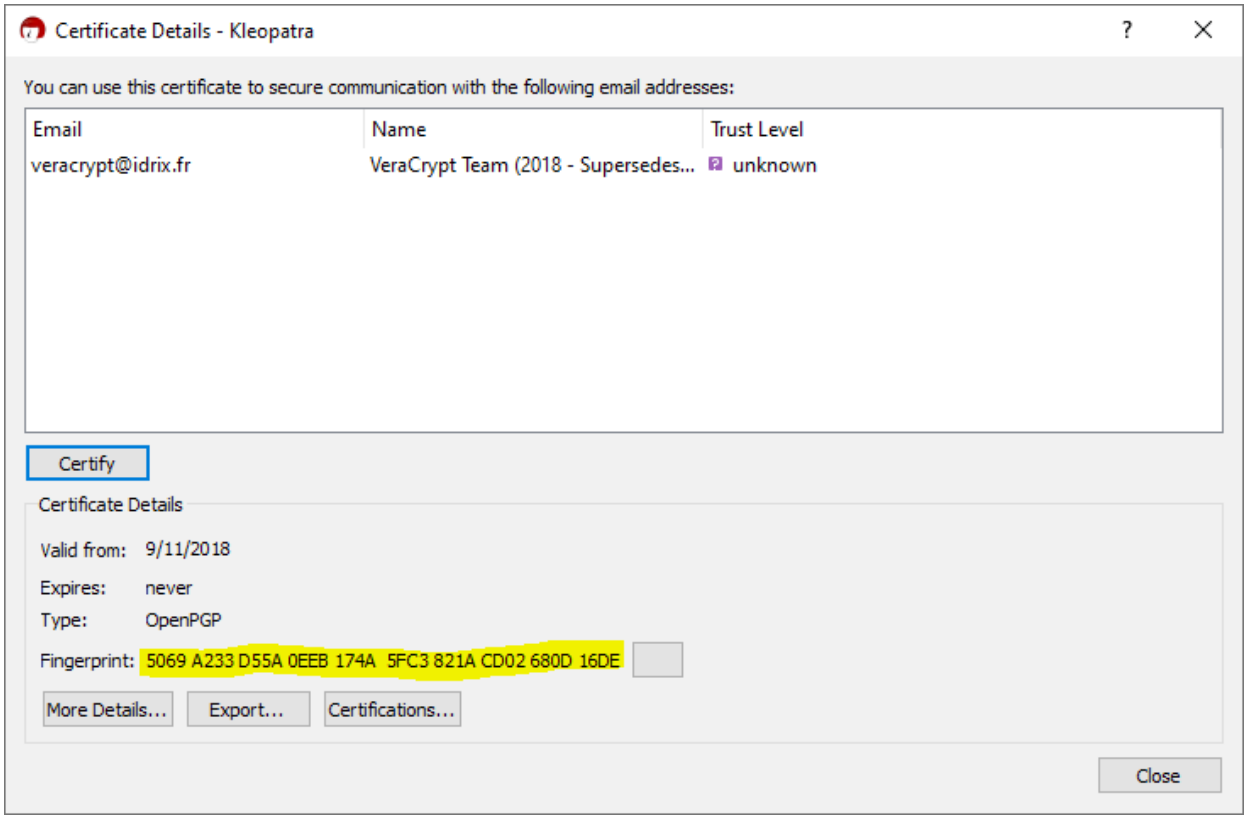


If you certified the key earlier the area with the text should be shaded green and telling you it's verified and trusted. However if you didn't we can still verify the file, simply click "Show Audit Log" below and to the right of the progress bar and a new Window will pop up showing the fingerprint of the key that verified the file. We simply compare this fingerprint to the one shown on the website and if they match.

(ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)



Alternatively (actually this would be the better option) we could compare the thumbprint to that of the key we downloaded rather than relying on what's on the website. To do so open Kleopatra and double click on the key we imported and at the bottom of the window, compare that to the fingerprint we got when we verified the file.



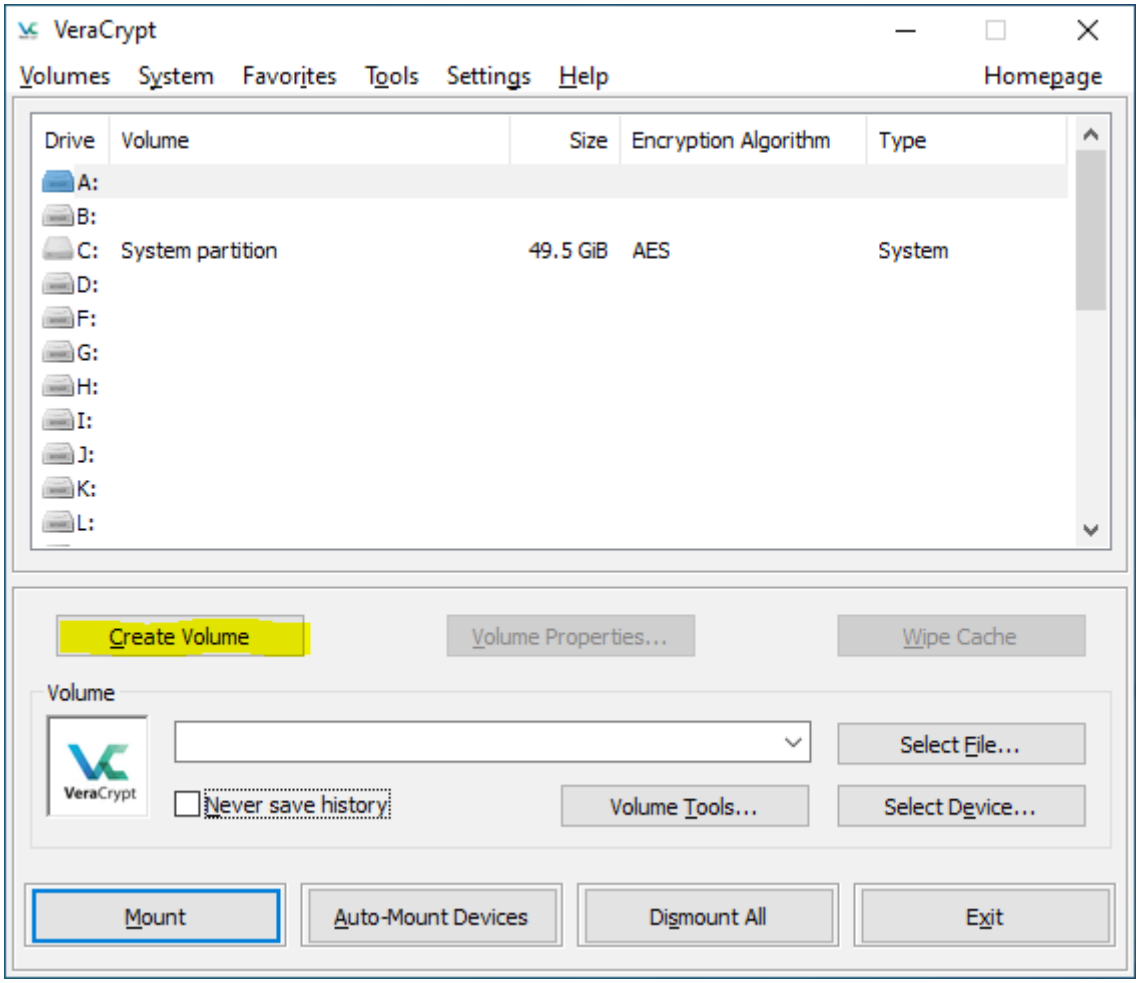
Now we can consider the file verified and exactly what the developers wanted us to have and run the exe or msi to install VeraCrypt.

VeraCrypt

There's 3 basic options when using VeraCrypt. You can encrypt the entire system drive, encrypt a non system drive (such as USB or external HDD) or encrypt a set amount of a drive. And remember that VeraCrypt is cross platform, so if you already have a Linux install and don't want to bother with backing up your data, reinstalling Linux with encryption and then migrating your data back; you could just do an encrypted container and put sensitive files in it.

For this demonstration we'll just be making an encrypted container since I recommend using your OS method of disk encryption for a system drive as well as it'll allow me to cover the additional step of mounting the encrypted drive/container. If you do encrypt the system drive with it, whenever you boot the computer you'll be presented with a black and white screen where you'll be prompted for the password and PIM (just blank if you don't use it, which I'd recommend, more on that later)

You'll want to open up VeraCrypt and select "Create Volume". Note: I already had the system drive encrypted with VeraCrypt, yours won't show any drives like mine.

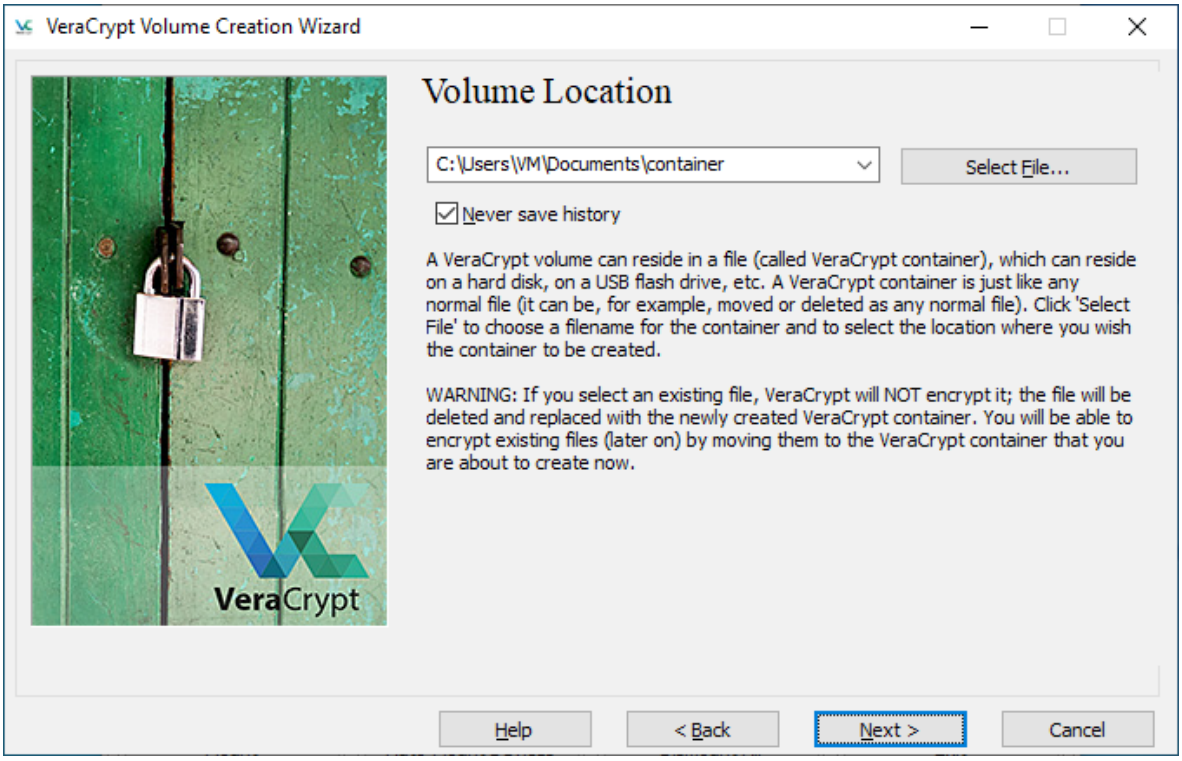


Next you'll select what you'll be encrypting, the options listed at the beginning of this section. The steps for all three are similar. For system drive you won't need to select a particular drive as VeraCrypt can figure it out (it's the C: drive on Windows or /dev/sda on Linux if it does ask you) and if you're encrypting an entire non-system drive, you'll just chose the USB/external HDD you're using, we'll get to what to for containers in a bit.

Next you'll be asked whether you want to create a normal or hidden container. If you're not worried about law enforcement or the mob, just do a normal container, if you are do your own research as I'm not knowledgeable on them.

For a container, now you'll be asked where you'll want to create the container. Click "Select File" and File Explorer will open up, select the folder you want the new container to be in and

then give it a name. Afterwards it should have the path to the new file you created. In this example I name it “container” and had it in my user’s Documents folder (“VM” is the user name)



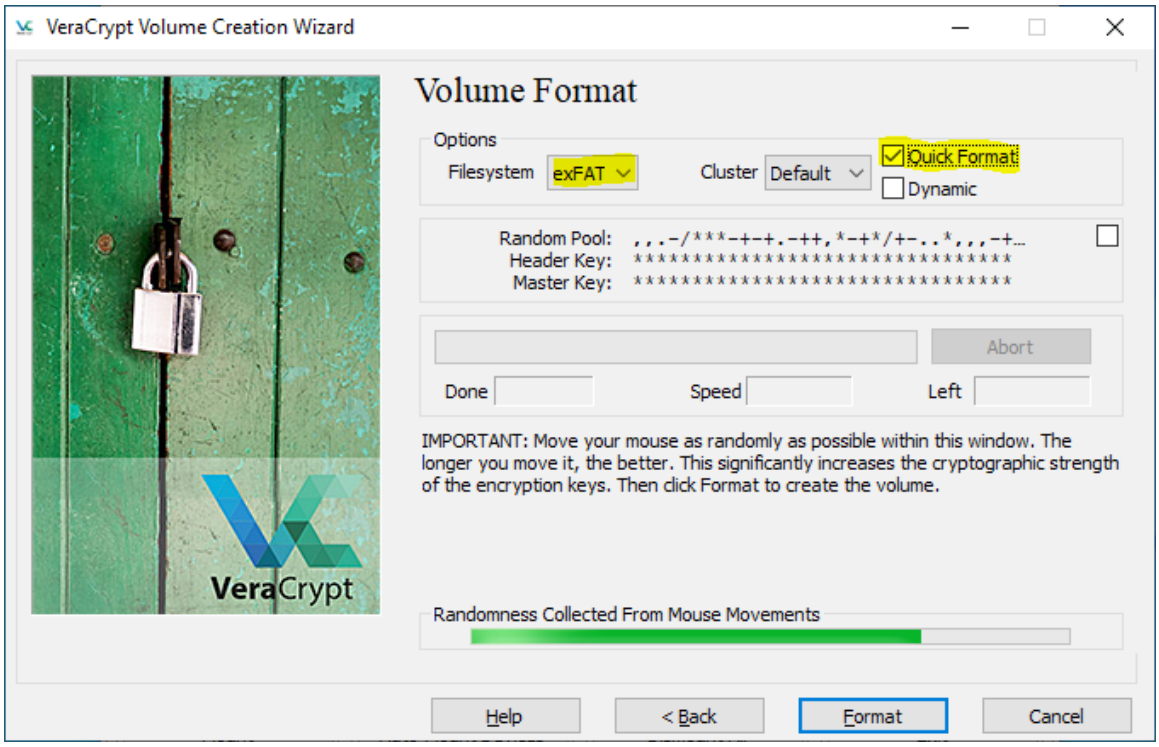
Next you’ll be asked about the encryption and hashing methods for it to use, the defaults are fine so feel free to use them.

The next part is only relevant for containers, not when encrypting entire drives. You’ll be asked to select the size of the container. If you don’t know how large to make it, just make it 1 GB to be safe (for anything besides video, that’s a lot of space) although note the default value is MB not GB, so be aware of that so you don’t accidentally set it to 1 MB.

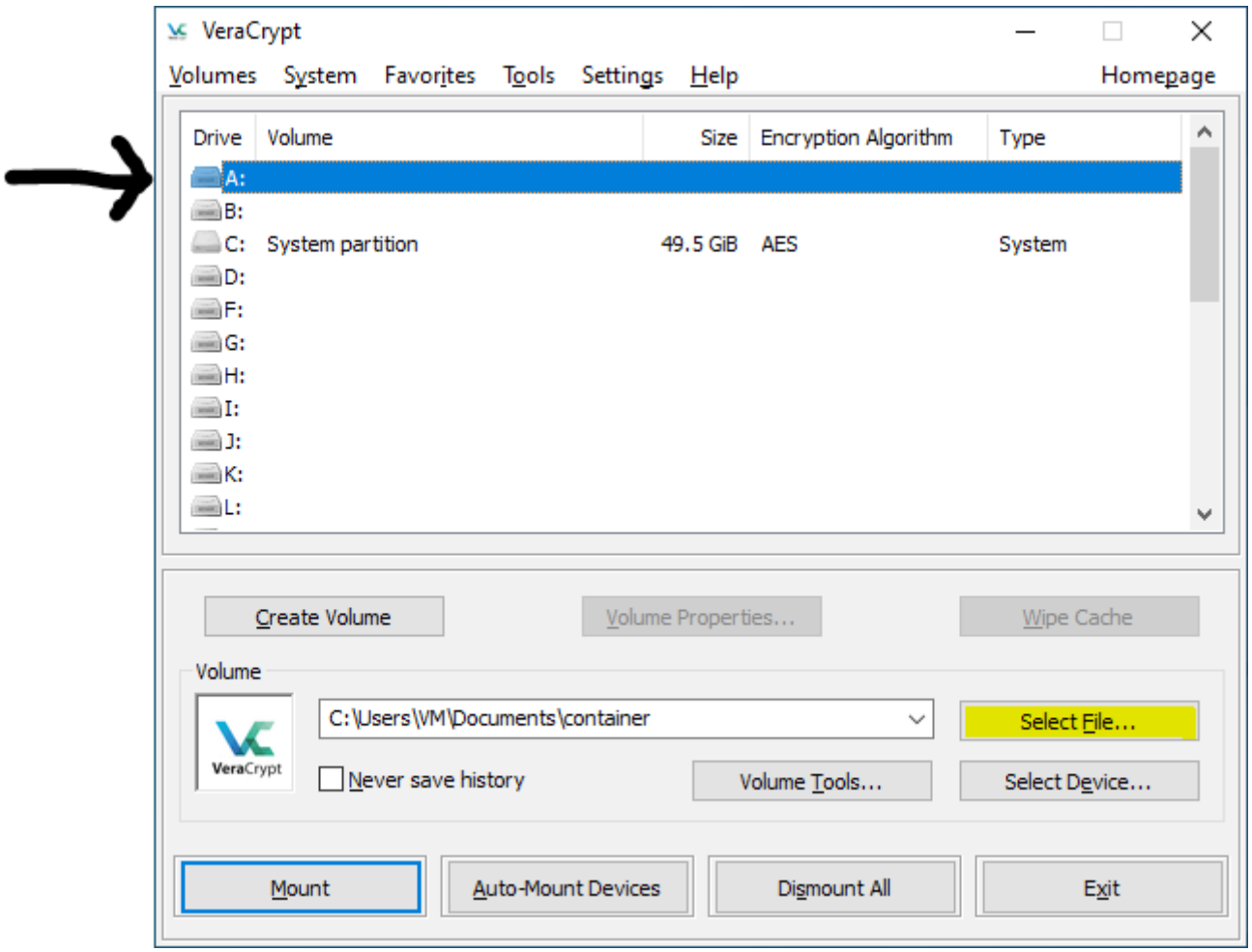
Afterwards you’ll be prompted for the password for the volume as well the keyfile and PIM settings. Since we’re mostly doing this to stop a some what tech savvy thief (or the person he

sells the device to) from easily reading our data, using either of these options isn't really necessary.

The next part is where you provide random data for the encryption key as well set a few options like file system to use. If you don't know what file system to use, just use exFAT. Although if it's a container that's smaller than 4GB you could also use FAT without issue (FAT can't handle files larger than 4GB, exFAT it's not an issue at all). Additionally for our purposes feel free to check the "Quick Format" option as well. Lastly, move your mouse around in the window until the bar turns green.

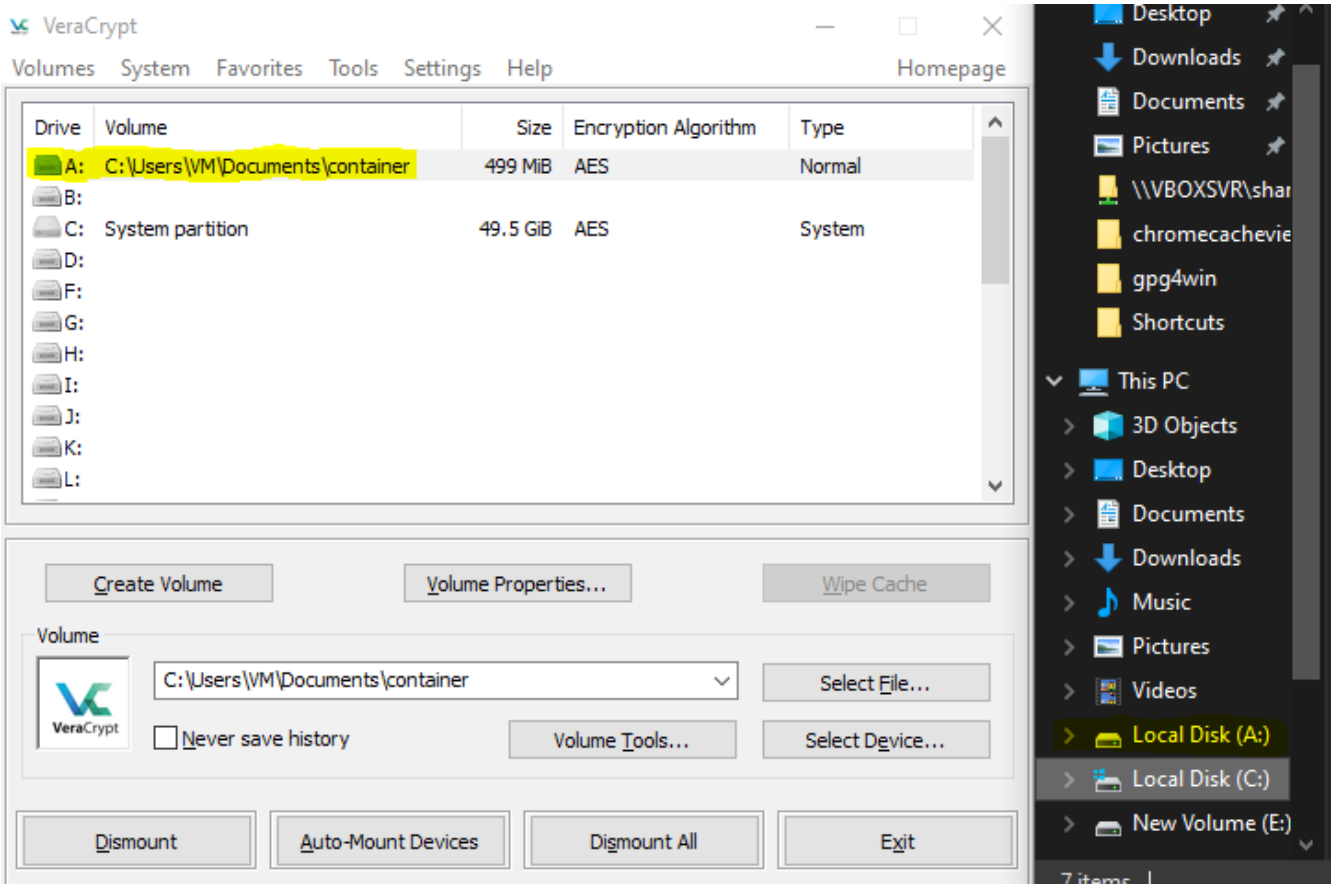


Now, if we made a container or encrypted a non-system drive, we'll need to mount it through VeraCrypt so that your operating system can use it. To do so open up VeraCrypt and select a drive letter for what you'll want the container/drive mounted as and then select "Select File" for a container or "Select Device" if you encrypted an entire non-system drive.



In this case, I'll be mounting the container I made as drive A: in the picture above the file's already been selected and it's path is shown in the box. If you allow VeraCrypt to save history, in the future you can just chose from previously mounted drives/containers with the drop down menu. From here just press "Mount" and provide the password when presented.

After it's done mounting VeraCrypt should show the container/drive as mounted and the drive letter should be available in File Explorer for you to place and retrieve files from.



Sanitizing Disks and Data

Although it doesn't necessarily involve encryption, it can and it is very relevant to protecting personal information. Whenever you get rid of a disk for whatever reason, you'll want to wipe it or otherwise make the data on it inaccessible, whether you're intentionally giving it to someone else or just throwing it away. Additionally we'll also cover sanitizing individuals files versus an entire disk. One thing that should be mentioned first is the differences between an SSD and HDD. I won't get into the technical details, but what's relevant is that with an HDD your computer more or less has full control over where data is written on the disk, making it very easy to over write old data. However with SSDs your computer doesn't have the same control, in order to extend the life of the disk the drive itself will determine where it writes new data to. This can cause issues because if your computer tells the drive to overwrite a particular file, the drive may decide to write the new random data

somewhere else on the drive that's been written to less in order to prevent that particular section to fail before the other because it's being written to more often.

Properly Deleting files

First let's clarify what happens when you normally delete a file. We touched on this a bit earlier in the metadata section, when a file's stored on your drive and file system there's the file data itself and what we'll call a pointer to the file data. This pointer contains the file's metadata (timestamps, size, name, etc) as well as the location on the disk of the actual file data, additionally this pointer is located inside the file data of a folder (which is why moving large files on the same drive is instant, because the file data isn't actually being "moved" just the pointer to the data). Normally when a file's deleted all that happens is the pointer is removed from the folder's file data and area on the disk where the file data is located is marked as "unused" however the data is still there and *not* overwritten. (Note: this is after a file's been removed from the recycle bin or similar, the recycle bin is essentially just a special folder that deleted files are initially moved to). Granted, it does take a fairly tech savvy person to recover deleted files, however plenty of free programs exist out there that will recover deleted files if they haven't yet been overwritten by anything.

In order to actually overwrite a file's data so that's it's not recoverable, we'll need a program that will tell the drive to overwrite a specific portion of it's self (where the file's located) with either random data or to just write zeros at that location. The two programs we'll discuss are sdelete for Windows and srm on Linux, the two are used nearly identical, but with slightly different options. I'll demonstrate with the Windows program, but on Linux just check the man page for srm. Additionally, see the section in the appendix on using the CLI for Windows.

You can get the sdelete program from Microsoft with the link below and on Linux srm is likely in your distro's repository.

https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

It can be used without any options, just typing in

```
sdelete <path/to/file>
```

This will overwrite the file's data once with random data (srm will do 3 by default) as well as remove the pointer from the folder that holds it and the file won't go into the recycle bin or equivalent (On Windows even files deleted normally from the CLI, using the "del" command, don't go to the recycle bin).

This process can be quite slow, especially on large files. Thankfully overwriting the data multiple times and with random data is overkill, we can use sdelete with the -z option to overwrite the file with just zeros which still makes the data unrecoverable, but doesn't take as long since the computer doesn't have to generate a bunch of random data to overwrite with.

Note 1: Recovering data that's been overwritten is technically recoverable, however it's a very, very advanced procedure and I'm not aware of any examples of it being done except for very small amounts of data as a proof of concept. However it's worth nothing that many government agencies and corporations require that disks that contained sensitive information be overwritten 7 times, meaning that for government intelligence agencies recovering data overwritten once is likely within the realm of possibility. However for our purposes, overwriting once is more than enough to prevent a random person from running a program that will recover normally delete files, however I just thought I'd bring up for education at least.

Note 2: As mentioned at the beginning of this section, this method isn't 100% reliable on SSDs as your computer can't control exactly what parts of the drive are written to unlike HDDs. It's still worth doing on SSDs as it likely will work, however to be absolutely be sure, you'll want to zero out all unused space on the disk after the file in question has been deleted. To do this with sdelete use this command run as administrator.

```
sdelete -z C:
```

If you want to do this on a none system drive, such as a USB or external HDD, just replace "C:" with the letter of the drive you want to zero out the free space on. Additionally free space on drives can be zeroed out on Linux with the following command.

```
sudo dd if=/dev/zero of=zero ; sync ; rm zero
```

The brief explanation is that it pulls zeros (/dev/zero is a virtual device that just pumps out zeros) and writes them to a file named “zero” on current drive for infinity, however at some point the drive will run out of space and then the last command will delete the file releasing that zeroed out space to be used by the system again. (Sync just helps ensure the cache is actually written to storage)

Wiping Entire Disks

Since the previous method was mostly relevant for HDDs and how common SSDs are these days, we’ll begin with SSDs. To solve the problem of sanitizing SSDs, most SSDs have a feature called “Secure Erase”, which is accessed through your computer’s BIOS, which wipes the SSD completely as well as the drive is usable as a completely blank drive afterwards.

For wiping HDDs, your best bet is to use Linux live booted from a USB stick. I won’t go into detail on it, but I’ll leave a link to a guide.

https://archive.ph/wip/UGACS

Once you’re booted into the Live Linux disk, open a terminal and type “lsblk” to list all disks attached to the computer. Since to be safe, the only drives that should be connected are the live USB and the disk you intend to wipe, there should only be two disks shown /dev/sda (and it’s partitions /dev/sda1 /dev/sda2 etc, which don’t matter for our purposes) and /dev/sdb. Since /dev/sda will always be the disk which the operating system loaded from, the disk you want to wipe will likely be /dev/sdb, however to make sure check the sizes of the disks. If the USB stick is 8 GB and the drive you want to wipe is 500GB, make sure /dev/sda is 8 GB and /dev/sdb is 500 GB.

Assuming the drive you want to wipe is indeed /dev/sdb. Use the following command to completely overwrite the disk with zeros.

```
dd if=/dev/zero of=/dev/sdb
```

Additionally if you want to use random data instead of just all zeros, you could replace /dev/zero with /dev/urandom. However again, for our purposes all zeros is sufficient.

Windows Configuration

Naturally it's impossible to discuss configuring Windows for privacy or even general usability without Linux being brought up. I do highly recommend normal people switch to Linux, not only for the privacy benefits, but also because in my humble opinion it's a more pain free desktop operating system than Windows 10/11 even for non technically inclined people. I'll elaborate more on why and things to consider when switching to Linux in the appendix, but for now I'll just stick to Windows as many people use it for one reason or another. Additionally this is by no means a definitive guide on the subject.

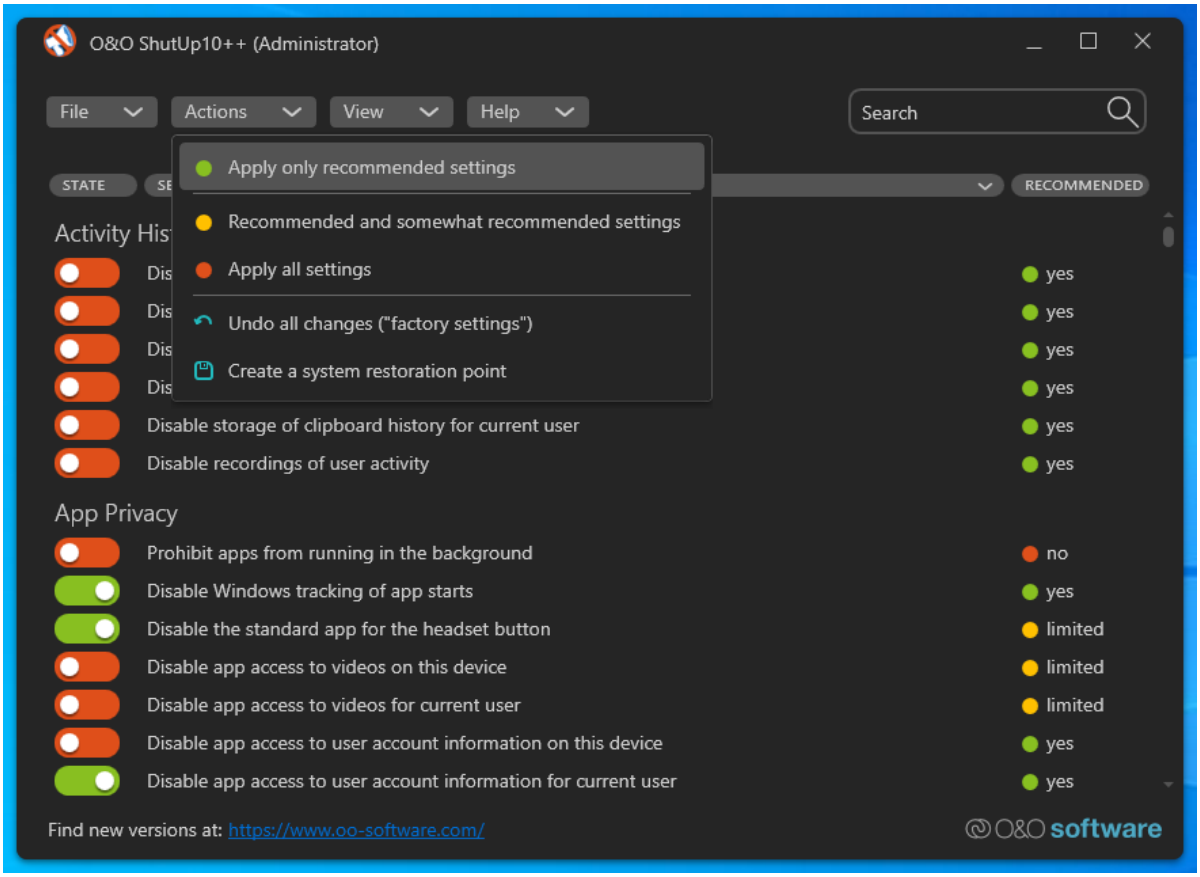
The first and easiest step is to simply go to "Settings" and then "Privacy" and turn everything off, however who knows if these options *actually* do anything as well as we can do much better anyways.

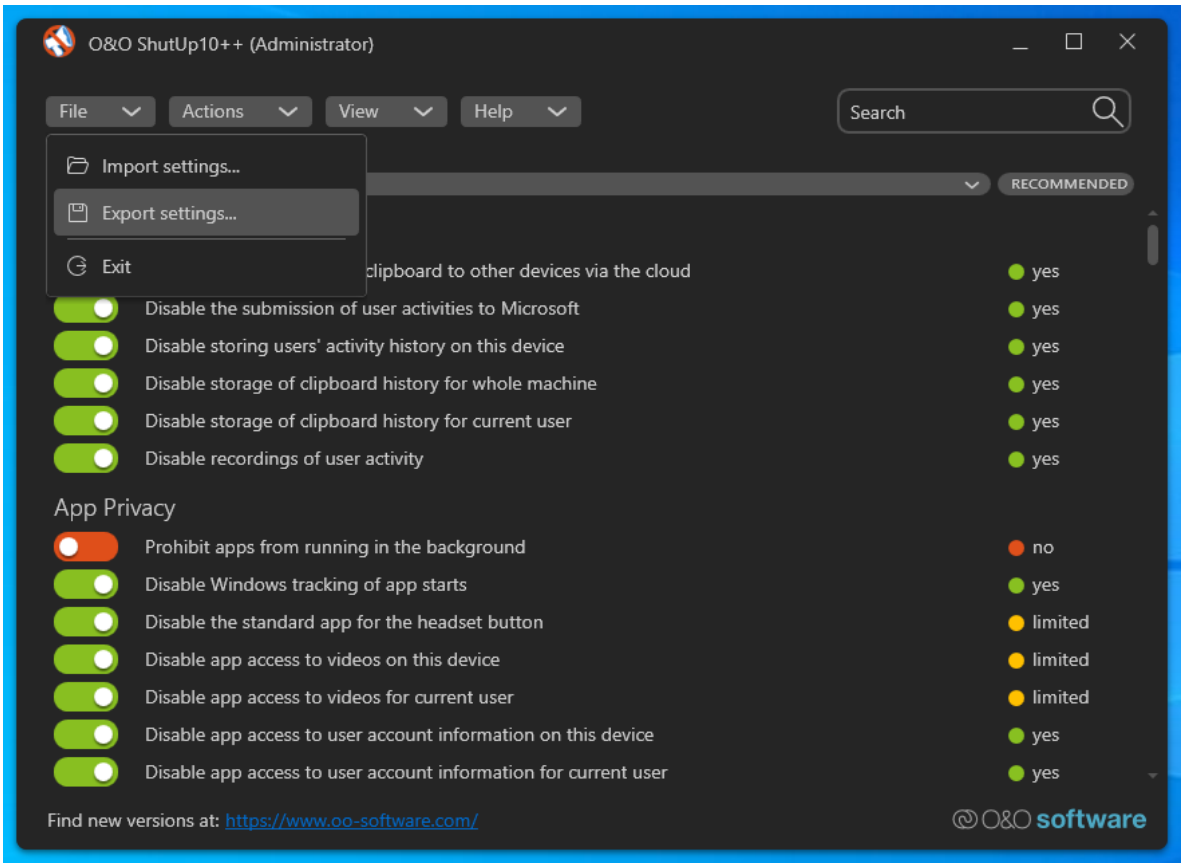
O&O ShutUp!

The next thing we can do is install a program called "O&O ShutUp!". It essentially blocks various spyware that Windows utilizes and comes with presets for you to choose since disabling some of these things will limit functionality. Another thing to note is that it needs to be run after any Windows update, as the "features" it turns off will be re-enabled. If you use more than just one of the presets you can export the configuration to a file and just run O&O and import the config file after the update.

The program is downloaded as just a single exe file, so it doesn't install. Just put the file somewhere you'll remember and run it. First just set one of the presets, either "Recommended" which will have minimal to no impact on functionality or "Recommended and Somewhat Recommended" which will impact functionality more. I'd recommend using one of those presets and then using your computer as normal for a week or two. If you do lose some functionality you want back, of course go back to O&O and try allowing "features" to get it back, or if you didn't lose any functionality, try the "Recommended and Somewhat

Recommended” and repeat the process. Lastly, if you do make any changes beyond the presets, you can export a configuration file from “File” tab and just import it after an update.



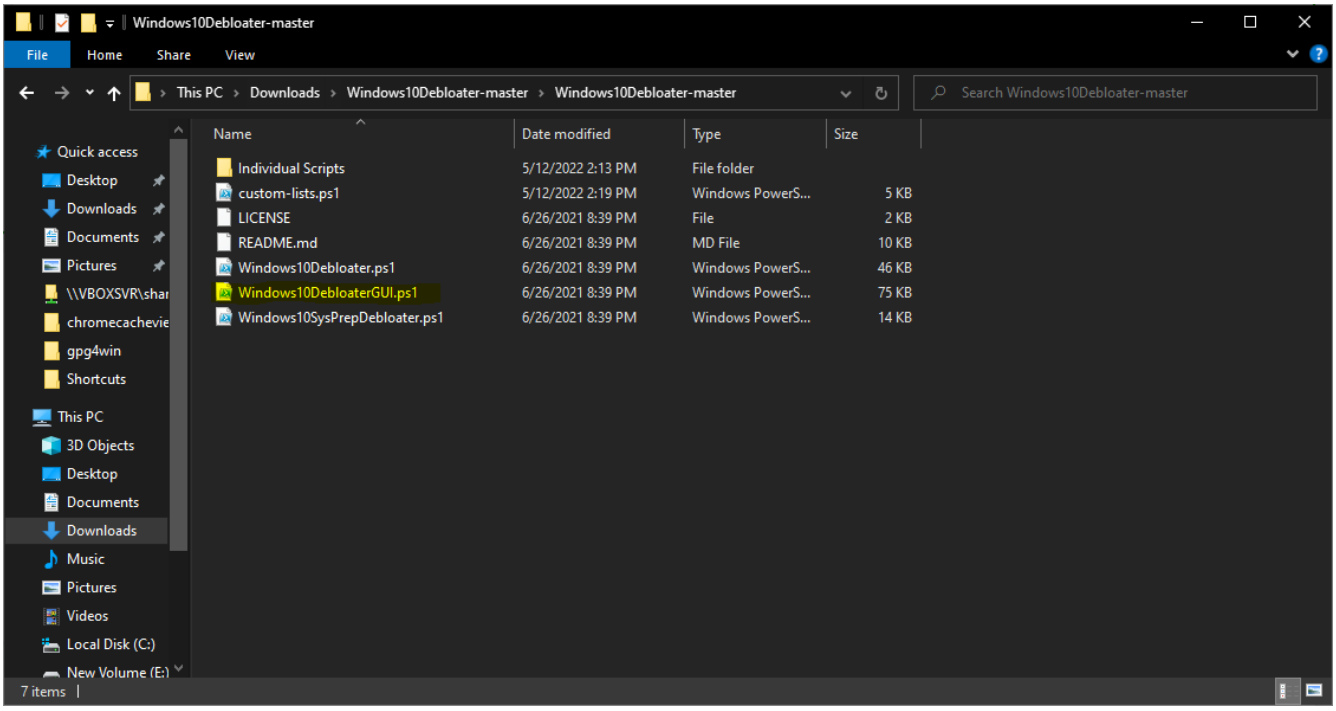


Windows De-Bloat Script

Another way we can remove bloatware and spyware on Windows is by using the Sycnex debloat script. Although it's a script it does have a GUI (Graphical User Interface) to make using it easier. Here's the link to the github where you can download it and I'd recommend utilizing the second option of running it.

https://github.com/Sycnex/Windows10Debloater

If you download the zip file to your Downloads folder, you can double click on the zip file in File Explorer to see the files in it. You'll want to find the GUI script which is shown below.



Right click on the GUI script and select "Run with Powershell". A blue terminal will pop up and likely ask you about the permissions for running powershell scripts. By default Windows won't run unsigned scripts (which this is) and it'll either prompt you to just run this single script or to change the settings so that any script can run. If you get the option to just run this script without changing the setting do that, but if your only option is to allow all scripts to run,

afterwards you can reset it to default by running powershell as Administrator and using the command

```
Set-ExecutionPolicy Default
```

to return the setting to it's default value. I'd highly recommend doing this afterwards if you don't know what powershell is before and/or have no intentions of using it yourself.

I'll drop a link to a guide on using the debloat tool, however I'd NOT just run "Remove All Bloatware" as that will remove things such as the calculator from Windows. Select "Customize Block List" and go through and see what you want to keep or get rid off (a checked box means that program will be removed/disabled when "Remove Bloatware With Custom Blocklist" is chosen). Additionally I'd also recommend removing/disabling Cortana, Telemetry and OneDrive if you do not use those features.

https://archive.ph/FESQw

Proxies, VPNs, Encrypted DNS and Tor

I'll try to keep this section brief, as there's a plethora of material out there at least on VPNs and Tor. I'll also address some of the drama regarding VPN providers in the appendix. One thing to mention that's relevant for both proxies and VPNs is that typically they're located in datacenters. The problem with this is that many services and websites will block or otherwise impede IP addresses coming from datacenters on the suspicion they're bots or hackers in the cases of online banking/financial services. Apart from being out right blocked you'll likely be forced to solve extra captchas on sites that you wouldn't have to if you were coming from a residential address.

Proxies

The way proxies work is essentially an intermediary between you and the server you're tying to connect to. To make an analogy with regular mail, if I was your proxy server, you'd write a letter to someone with their address in the letter and put it in an envelope addressed to me and when I receive it, I make out a new envelope with the address of the recipient in the letter and send it off. When I get the reply addressed to me, I do the same process in reverse. This way from the perspective of both the post office and the recipient/server, you never sent a letter to them.

Something to note about proxies, there's no encryption in this process, so if the post office were to look at the letter both between your house and mine; and my house and the recipient, they'd be able to verify both letters are the same, as well as read the intended address from the first letter to me. Additionally proxies are usually either enabled across the entire computer, or often individual applications can use a proxy while the rest of the computer doesn't, this is important later.

The other catch with proxies, is that most of them out there are free. Of course there's no such thing as a free lunch and the catch with the free proxies is that many make there money by injecting ads and other malicious stuff into the pages you visit.

https://web.archive.org/web/20220401064413/https://blog.haschek.at/post/fd9bc/

Of course HTTPS helps in this regard, but as the author points out is defeated if an HTTPS site loads libraries from an HTTP source.

However proxies do have a niche which is torrenting. When you get a cease and desist letter from your ISP, how that comes about is the owner of the movie joins a torrent swarm of that particular movie, and torrent being a peer to peer protocol, allows them to see the IP addresses of everyone in the swarm downloading or uploading the file. They collect everyone's IPs and send a letter to all the ISPs involved saying these IPs were involved in the swarm and the ISP sends the letter out to whoever had those IP addresses at the time.

Even free proxies work well for this since the owner of the movie only sees the proxy server connecting to the swarm and not you, nor your connection between you and the proxy. Additionally most torrenting applications have a setting for proxy servers, meaning you can set the proxy server in the torrenting application and only that application will use the proxy while the rest of your computer won't. For the security concern, I can't guarantee proxies are incapable of injecting malicious stuff into torrents, however injecting malicious stuff into a torrent file is much, much harder than doing so with HTML. Of course a paid VPN is preferred, however if you're unwilling or unable to pay for a VPN, a free proxy for torrenting can be a good option.

If you do want to use a free proxy for something besides torrenting, there is a tool to check to see if a proxy server is malicious before using it.

https://proxycheck.haschek.at/

VPNs

VPNs work very similar to proxies, however there's an additional layer of encryption between you and the VPN server. From the proxy/VPN server to the final recipient the packets will essentially be exactly the same, no additional security with either one, just between you and the VPN server has the extra encryption. The advantage of this is that someone looking at the same packet between you and the server; and the server and the recipient won't be able to tell they're the same packet. Meaning your data is more or less anonymized with everyone else using that VPN server.

As for whether you should get a VPN service, if you're American your ISP can sell your data and they'll give up user data to the government if they ask nicely, so getting one really can't hurt, no matter how bad the VPN service is. However there is extra annoyances with using a VPN on the internet as generally sites and services will be distrustful of you, particularly banking sites. The privacy advantage of VPNs is that your Internet activity is hidden from your ISP as well as advertisers/sites won't be able to locate or identify you by your IP addresses, additionally you'll be anonymized with the other users of the same VPN server.

If you're interested in the privacy benefits of using a VPN, proton offers a free tier of theirs. It does come with limitations being free, such as they block torrenting as well as have minimal server locations (in case you're trying to get around geo locked content). However it'll give you a taste of using a VPN to see if it interferes too much with your typical Internet usage.

Lastly, I do have a recommendation on VPN services, which is Mullvad. Mostly because they're one of the few VPN services that will let you buy the service without disclosing any personal information or even an e-mail. Essentially they'll generate a random number that will be associated with your account and you'll pay them via cash (you can literally mail them cash and they'll take it), crypto, credit card, etc with the random number for the account you'd like to fund and once they process it you'll have access to their service. The only real drawback with Mullvad is they don't have as good server location selection as someone like

NordVPN or Surfshark, so if you're primary purpose of a VPN is to get around geo locked content, you'd probably be better off with one of those two.

Encrypted DNS

We touched on this briefly in the Android section however I'll mention it here even though it's benefits are underwhelming, but the redeeming aspect of it is that it's completely free just like regular DNS (Domain Name System), so no downside of having malicious stuff injected into your connections like with free proxies. DNS is the protocol that computers use to turn human usable names like "google.com" into an IP address they can use and connect to. Normal DNS queries are done unencrypted so your ISP or a network administrator (really the firewall on a public network, not the actual person) can see the domain names you're looking up.

Two big downsides one, many websites share IP addresses with one another through services like Cloudflare and other hosting providers. Naturally this poses a problem if a domain is suppose to resolve to an IP address that connects to a particular website. To get around this DNS queries use something called an SNI (Server Name Indication) which the server hosting the websites sharing the IP can use to direct the user to the correct website. The problem arises in that both encrypted DNS protocols do *NOT* encrypt this SNI header, meaning that any ISP or network administrator who bothers to look could still see which websites you're looking up.

The other downside is that DNS does nothing to hide the IP address you're connected to, nor mask your IP address from the server you're connecting to. It only encrypts the DNS query, it has no effect on the actual connection to the site.

With that said, encrypted DNS *can* get you around blocked sites on public networks and the like, since many website blocking is just done at the DNS level and not at the IP level. However you shouldn't really count on it, especially if it's something sensitive were there

would likely be repercussions for you having tried accessing something. However encrypted DNS is totally free to use and can help in some instances, so it's one of those "why not do it?" type of things.

Here's a quick guide on configuring encrypted DNS on Windows and for Linux just install the package "stubby".

https://archive.ph/wip/7XNNa

(You'll want to create the registry key first before changing the DNS server, idk why it gets those steps backwards)

Lastly, there was a protocol that encrypted the SNI header called ESNI, however it was killed off shortly after being implemented by Cloudflare and Firefox who went on to begin working on ECH instead which is suppose to solve more problems than even ESNI. If you want to read more I'll leave a link.

https://web.archive.org/web/20220529043406/https://blog.cloudflare.com/encrypted-client-hello/

Tor

The quick run down on Tor is that it's by far the most anonymous and private way of doing anything on the Internet and it's also free. To use it simply download the Tor browser and then do whatever you like on it. (Don't forget to verify the download!)

https://www.torproject.org/

Apart from being the best for anonymity and privacy, because it's free it's also a great option if you're fine with using a normal Internet connection, but occasionally want to have the privacy and anonymity of a VPN without paying anything. You could just use the Tor browser for that and not pay for a VPN service, additionally the Brave browser also has a feature

where you can open tabs in Tor which is fine for this purpose, although if you truly need the protection of Tor, you should just use the Tor browser.

One last thing about Tor, it’s best practice to use it in the default window size that in launches in rather than maximizing it like you’d normally do. The reason is that websites can easily see the resolution of the window that the website is displayed and everyone using the default window size helps anonymize everyone using the Tor browser.

Information Search, Archiving and Sharing

Probably the biggest misconception about the Internet is that once something's uploaded to it, it's there forever. This may be the case when using services such as Facebook, however the average life span of a webpage is 100 days

https://web.archive.org/web/20220530224112/https://blogs.loc.gov/thesignal/2011/11/the-average-lifespan-of-a-webpage/

Part of the reason I often use archived pages in the guide is that some of the guides I found had their images missing, even though the site the guides were on were alive and well. Additionally even if content is archived by someone, there's still the matter of sharing it to other people. The purpose of this section is to give you the skills so that you'll have the ability to find, preserve and share content from the Internet you deem worthy of preserving.

Advanced Search

I'll start with advanced search, since even if you're not interested in archiving, you'll likely find some use for this. Many people when they use search engines, such as google, will phrase questions the same as if they were asking a human, such as "How to make fried chicken". Search engine maintainers go to great lengths to make searches like these work and for something simple like this example, it probably would. However imagine a spectrum where on one end you have how humans think and on the other side, how computers think. Using human phrasing in a search engine is at the far end of human thinking which is the most difficult for the computer to understand and give you accurate results for. Rephrasing the query as "Fried chicken recipe" is much friendlier to the computer and although wouldn't be super helpful in this simple scenario, will typically give you better results than human phrasing.

Advanced search operators take us much further into the computer side of the spectrum, however they're still quite easy for humans to understand and don't require any special knowledge like programming does.

Although search operators will vary slightly from one search engine to another, for the most part they are the same and even operators that aren't officially supported on one search engine will often work. Typically these operators follow a pattern of "operator:term" were term is just what you want the value for that operator to be. For example a common operators is "filetype" which as the name implies, specifies the filetype you're searching for and is very helpful when searching for PDFs or other ebook formats. If you wanted to search for a PDF of something, somewhere in your query you'd just add "filetype:pdf" and now all of your results will be PDF files.

Before we get to far into operators, quickly let's go over the one's you'll likely use the most. These are double quotes (" ") plus (+) and minus (-). Plus and quotations more or less do that same thing. A plus in front of a word will emphasis results that have that word in them, words or phrases inside of double quotes will be required to be in the results. Inversely when minus is in front of a word or phrase in double quotes, results containing that word or phrase are excluded. Additionally the minus operator can also be used on other operators. For example, the "site:" operator that takes the domain name of a site and limits results to ones originating from that site. Not only is this useful whenever a website doesn't have their own search bar or has one that's horrible (like bitchute), but the minus operator can be placed in front to exclude results from that site. An example being

```
-site:twitter.com
```

Will exclude anything from twitter in your results.

Two operators that are very helpful when trying to find content from a certain time period is "before:YYYY-MM-DD" and "after:YYYY-MM-DD" with dates formatted as shown. Note you don't have to give a full date, just a year or year and month is acceptable. Although recognize the date it's searching is when the content was uploaded at that particular location, not when the original content was created. So if you're looking for scans of news articles from the 1920's, this won't help you much unless you knew the date range they were uploaded to the

Internet. But say you're looking for stuff about Jeffery Epstein from before his second arrest in 2019. You could use the search term.

```
Jeffrey Epstein before:2019
```

Or if you wanted information posted between his first and second "incidents" you could use the after operator in combination such as.

```
Jeffrey Epstein after:2005-02-30 before:2019
```

as well as any other operators you'd like to use.

I'll go ahead and just leave a link to a list of operators, but I'll go ahead and talk about a few more that I find come in handy quite a bit.

https://web.archive.org/web/20220524122458/https://ahrefs.com/blog/google-advanced-search-operators/

Next the "link" operator. This one is deprecated, so it doesn't work very consistently and only with Google in my experience. However it can be quite useful at times. Link takes a URL as a value and filters your results based on if they contain a link to that URL or not. So if you want to find places or communities on the Internet that are discussing a particular video or article, you can use the "link:url_of_page" to perhaps find links to the URL in question.

Another is the "around" operator. This operator uses a slightly different format than the others as we'll see in a bit. It takes two words or phrases and searches for them being within X words to each other. So if you wanted to the words "foo" and "bar" to be within 5 words on each of your results, you could use the following search term.

```
foo around(5) bar
```

Note as is the case with many advanced search operators, if there's not many results that fit that exact term, but are similar (such as include foo and bar, but not within 5 words of each

other) they may be included as well. Although this isn't the case for some operators such as "site".

Also if you're looking for content that's already been removed, you can either search directly for it on archive.org, by using the site operator to search archive.org or you could try to use the "cache:" operator if you have the URL of the page in question and could potentially get it if Google still has the webpage cached.

Bypassing Paywalls

Academic Papers

One issue you may run into while searching for something is coming across a scientific, or otherwise academic, paper where only the abstract is free to the public and the actual paper is paywalled to some academic journal. A great resource for accessing this kind of content is

https://sci-hub.st

When you initially come across the article and it's abstract, copy either the URL or the DOI number if provided and enter it into sci-hub and the overwhelming majority of the time sci-hub will have access to that particular journal and you'll be able to view the full paper.

Newspapers, Magazines, etc

Besides academic journals, many newspapers and the like also have paywalls that may prevent you from reading an article. The key here is something called "referer headers". What they more or less are is the website you were on where you clicked the link to go to the current webpage. The reason they're important is that many sites will allow users who came to their article from a link posted on a social media site such as twitter or facebook to bypass their paywall, so as to not discourage people sharing their articles on social media.

The easiest way around this is to use a browser extension that will more or less automatically spoof the referer. I don't believe any that do this will be allowed in the Firefox or Chrome

extension store, however you can manually download and install extensions that do this from github, one such extension is

https://github.com/iamadamdev/bypass-paywalls-chrome

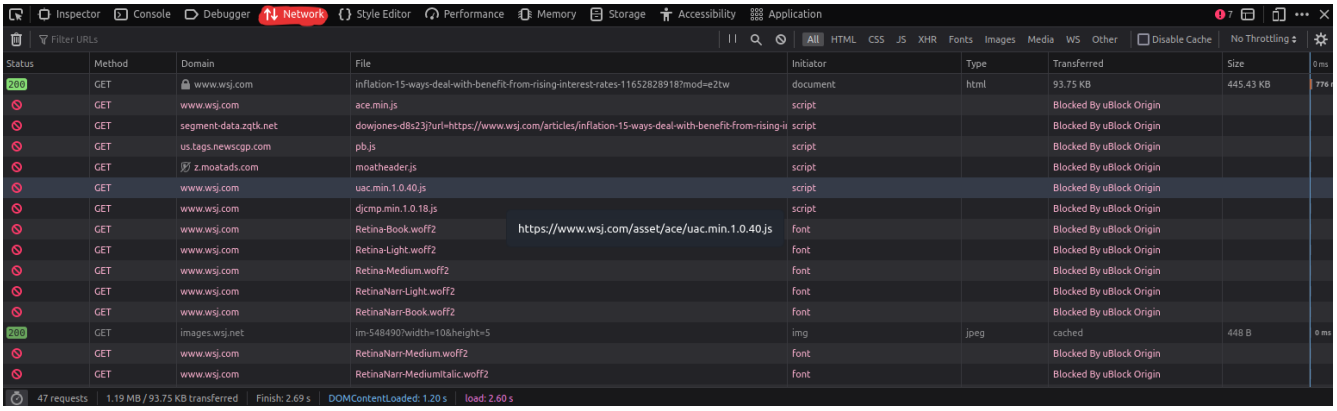
Another fairly easy way to do this for a particular article, is to use the advanced search operators listed above to simply find a link to the article from twitter and follow it to naturally have a twitter referer link without even having to spoof it. Simply use the term "site:twitter.com" with the title of the article and you'll likely get results from twitter with a link to the article which you can follow and bypass it.

Another fairly easy way is to copy the URL of the pay walled article and check archive.org and archive.is to see if it's already been archived there. Often on archive.is, someone will have archived a version without the paywall block you can read.

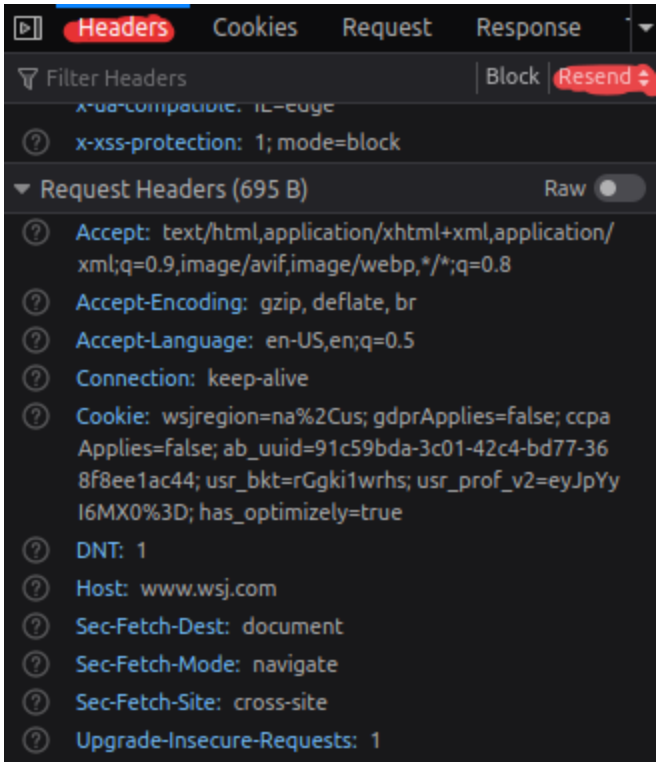
The last resort is simply manually spoofing the referer header. The easist one to spoof is facebook, simply past the following in front of the URL of the paywalled article and hit refresh

https://facebook.com/l.php?u=

This facebook one is a bit hit or miss, the next one is more involved, but works much more often. I'll only cover Firefox, I tried it on Chromium but it doesn't seem it'll allow you to do it. When you're on the page of the pay walled article, right click any where and select "Inspect" or "Inspect Element". From there select the "Network" tab and then refresh the page how you normally would or clicking the "reload" button from underneath the network tab. The network tab doesn't log anything until it's opened, hence why you'll need to refresh after opening it.



The one you'll want will be of type "Document" and will likely be the very first result. Left click on it and a new window should pop up showing more information about that request. From this new windows select the "Headers" tab and scroll to the "Request Headers" and click the "Resend" button, both highlighted in the picture.



After clicking on "Resend" you should be asked whether you want to "Edit and resend" or simply "resend", select "Edit and resend". You should then be presented with a text box with

the headers you saw previously inside it. Make a new line at the bottom and add the following.

Referer: https://t.co

and then click resend and the vast majority of the time this will get you past the paywall.

Archiving

In this section we'll cover downloading content from the Internet and either storing it locally or on an archive service like archive.org or archive.is; additionally we'll briefly cover downloading entire websites as well as YouTube and videos hosted on other platforms. Wget and yt-dlp will be covered, so reference the section on the CLI to install those programs on Windows if you'd like to use them (on Linux wget will already be installed and yt-dlp can be added easily through pip). Lastly recovering webpages from cache will also be briefly covered.

Saving Single Webpages

To start off, the simplest way of saving a single webpage would be to simply save it through your browser. Generally you'll have the option of saving it as a PDF or HTML. Saving it as a PDF will save it as a single PDF file, however although the majority of the content will be saved correctly. Often stuff like the background and other elements that are remote (linked to from the page) or that are displayed with JavaScript won't save. If it's an article the main body will likely save correctly, but it's not the best option if you'd like as an intact copy as possible, you'd want to save it as HTML. Saving it as HTML will usually create both a single HTML file and in the same folder a new folder with multiple files inside of it. It's important that both the new folder and the HTML file are in the same folder. The reason is that just as webpages simply link to content like scripts and images, the new HTML file has those links rewritten to point to inside that newly created folder. They're relative links so you can move the HTML file and folder together, but they must always be in the same folder. The best way to store them would just be to put both into their own folder, additionally if you'd like to share this local copy of the website, then you could zip the folder containing the two and just send the zip file to someone.

To save a webpage on archive.is (I don't believe you can manually save webpages on archive.org, they just do automatic scans). Simply go to archive.is (you may be redirected to archive.ph or similar, that's fine) and paste the URL of the page you'd like to save into the top bar. If that page has already be archived, it'll ask you to view the already archived version to see if it's close enough to the current version that you'll be fine with the older version. If so just use that, or if there's been a substantial change, go ahead and archive the current version. If you do create an archive of the current version, you'll see it start to download various elements from that page, at this stage the URL in your browser is the URL that will point to that particular archive and you can go ahead and grab that URL if you'd like. Just remember to save that link somewhere on your computer, as if you don't have the exact URL you can't really search archive.is without an exact URL. Lastly, if before you archive something on archive.is, it's a good idea to check on archive.org to see if they've already taken a snapshot of that page. Lastly on archive.org you can search for archived pages or content like a normal search engine without the exact URL, although you can of course check with an exact URL as well.

Lastly we'll briefly cover using wget for downloading a single webpage. It's not ideal for just one webpage as for the sake of brevity, it won't handle content rendered with JavaScript the way saving it from your browser will, however wget has many powerful features for when you're downloading more than a single page, but even using it to download a single page, it's still handy as wget can be used in scripts. There's a myriad of options with wget to do the same thing or slight variants, but the simplest is the following command

```
wget -kp <webpage-URL>
```

Wget will save *all* the files for the webpage inside one folder, so you won't have a folder and HTML file that need to be kept together. However the HTML file you'll want to open in your browser to view the downloaded webpage will be buried somewhere in that folder, possibly with the name index.html, however not always.

Downloading YouTube Videos

First you'll need to install Python3 as well as ffmpeg. Installing Python isn't different from installing any other program on Windows, just make sure to get Python3 *not* Python2.

https://www.python.org/downloads/windows/

For ffmpeg you'll need to download the executable file (it'll come with a few others such as ffprobe which you might as well keep) and add ffmpeg somewhere to your path, see the CLI guide for more info. On Linux you can just install it from your repository, if it's not already installed and you can get it for Windows here.

https://ffmpeg.org/download.html

Once you have both installed, open up a command prompt and use the following command to install yt-dlp

```
pip install yt-dlp
```

Once yt-dlp is installed, I'd recommend creating a configuration file with a few options, especially on Windows. The configuration file is essentially where you put yt-dlp options that are essentially default options used every time yt-dlp is run, however if you give an option on the command line that conflicts with an option in the config file, the one given on the command line will have preference.

To create the configuration in Windows, open file explorer and in the top bar with the current location, clear it and type "%APPDATA%" and hit enter. There should then be a couple folder one of which named "yt-dlp", if there isn't, create a folder named "yt-dlp" there. Open that folder and create a new plaintext file just named "config" (Right click → New → Text Document). Open the new document in notepad or some other text editor and add the two following lines.

```
--windows-filenames
```

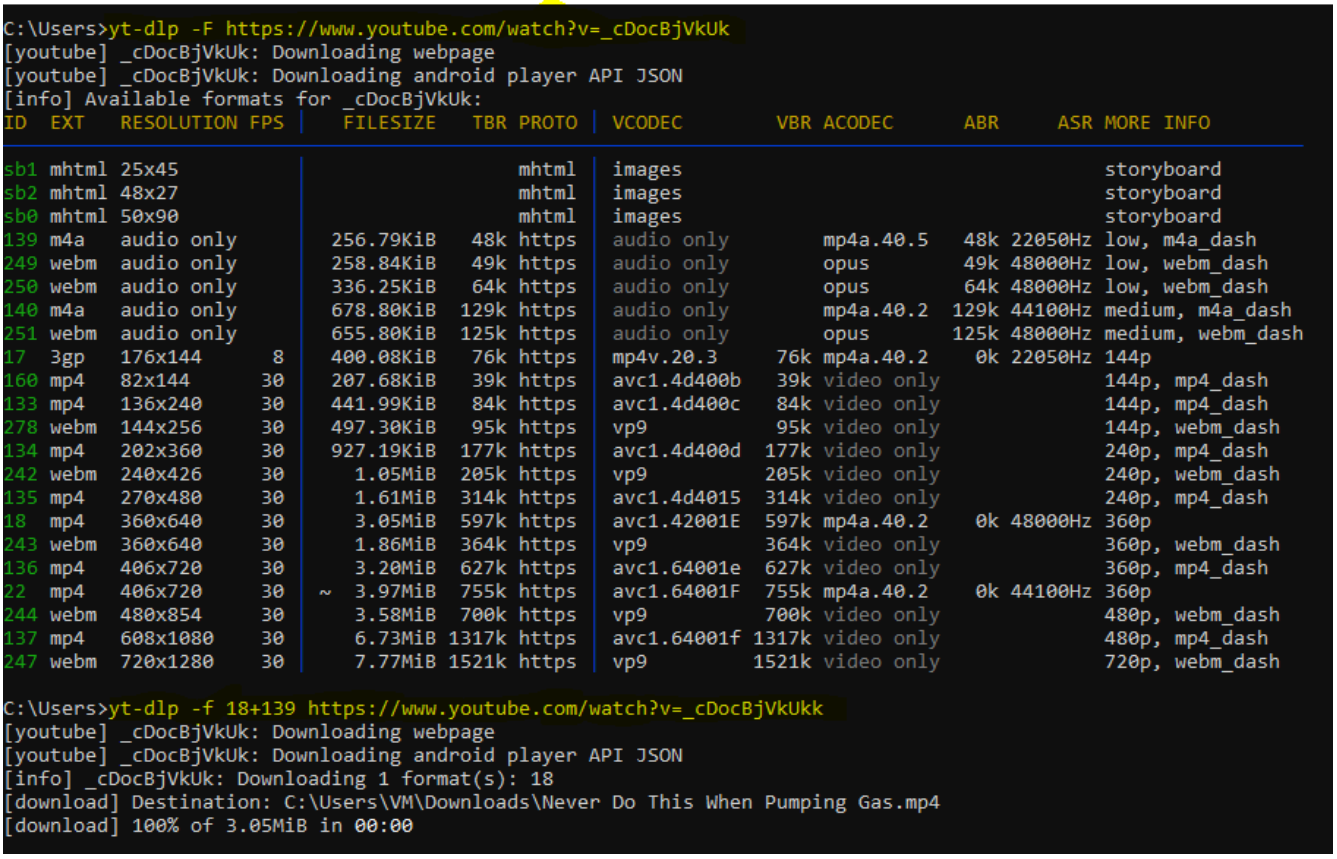
```
-o "C:\%HOMEPATH%\Downloads\%(title)s.%(ext)s"
```

and save the file as just “config” *without the .txt extension*. The first option just makes sure that yt-dlp won’t save videos with characters in the name that are illegal in Windows and the second option sets yt-dlp to save videos to your Downloads folder with the filename being the title of the video and the correct extension. Again, these default options can be overridden, so if you give your own -o option when using yt-dlp that will be used instead of the one in the config.

Using yt-dlp is quite simple and remember, even though it was primarily made for YouTube, it works on many other video sharing sites. One of the options you’ll likely use the most is -F and -f. The -F format lists all available formats for a video, both audio and video, and the -f options is used when actually downloading the video and is used to select which formats you’d like the downloaded video to be in. Although note, it’s not necessary to specify formats when downloading a video. Just “yt-dlp <video-URL>” will download the video and likely use the VP9 format in 1080p as a webm file. When specifying formats, most formats will be only video or only audio, so you’ll likely need to specify both a video and audio format. To use the -F option simply use the following

```
yt-dlp -F <video-URL>
```

and you’ll get an output that looks like this. Also in the picture is using the -f option to download the video with the specified formats.



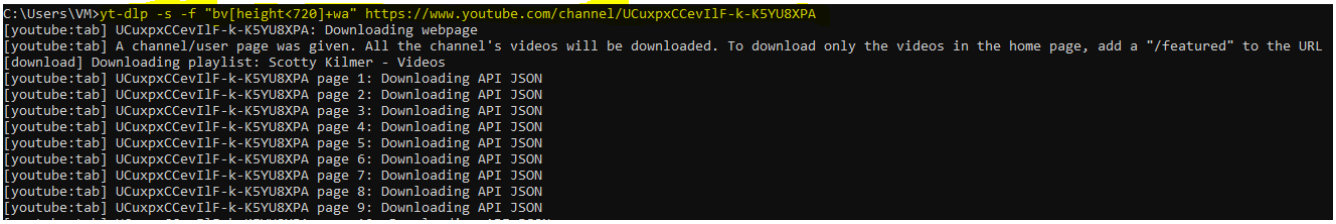
```
C:\Users>yt-dlp -F https://www.youtube.com/watch?v=_cDocBjVkUk
[youtube] _cDocBjVkUk: Downloading webpage
[youtube] _cDocBjVkUk: Downloading android player API JSON
[info] Available formats for _cDocBjVkUk:
ID  EXT   RESOLUTION FPS |   FILESIZE   TBR PROTO | VCODEC        VBR ACODEC      ABR     ASR MORE INFO
------------------------------------------------------------------------------------------------------------------------
sb1 mhtml 25x45          |                  mhtml | images                                    storyboard
sb2 mhtml 48x27          |                  mhtml | images                                    storyboard
sb0 mhtml 50x90          |                  mhtml | images                                    storyboard
139 m4a   audio only     |  256.79KiB   48k https | audio only        mp4a.40.5   48k 22050Hz low, m4a_dash
249 webm  audio only     |  258.84KiB   49k https | audio only        opus        49k 48000Hz low, webm_dash
250 webm  audio only     |  336.25KiB   64k https | audio only        opus        64k 48000Hz low, webm_dash
140 m4a   audio only     |  678.80KiB  129k https | audio only        mp4a.40.2  129k 44100Hz medium, m4a_dash
251 webm  audio only     |  655.80KiB  125k https | audio only        opus       125k 48000Hz medium, webm_dash
17  3gp   176x144      8 |  400.08KiB   76k https | mp4v.20.3     76k mp4a.40.2    0k 22050Hz 144p
160 mp4   82x144       30 |  207.68KiB   39k https | avc1.4d400b   39k video only              144p, mp4_dash
133 mp4   136x240      30 |  441.99KiB   84k https | avc1.4d400c   84k video only              144p, mp4_dash
278 webm  144x256      30 |  497.30KiB   95k https | vp9           95k video only              144p, webm_dash
134 mp4   202x360      30 |  927.19KiB  177k https | avc1.4d400d  177k video only              240p, mp4_dash
242 webm  240x426      30 |    1.05MiB  205k https | vp9          205k video only              240p, webm_dash
135 mp4   270x480      30 |    1.61MiB  314k https | avc1.4d4015  314k video only              240p, mp4_dash
18  mp4   360x640      30 |    3.05MiB  597k https | avc1.42001E  597k mp4a.40.2    0k 48000Hz 360p
243 webm  360x640      30 |    1.86MiB  364k https | vp9           364k video only              360p, webm_dash
136 mp4   406x720      30 |    3.20MiB  627k https | avc1.64001e  627k video only              360p, mp4_dash
22  mp4   406x720      30 | ~  3.97MiB  755k https | avc1.64001F  755k mp4a.40.2    0k 44100Hz 360p
244 webm  480x854      30 |    3.58MiB  700k https | vp9           700k video only              480p, webm_dash
137 mp4   608x1080     30 |    6.73MiB 1317k https | avc1.64001f 1317k video only              480p, mp4_dash
247 webm  720x1280     30 |    7.77MiB 1521k https | vp9          1521k video only              720p, webm_dash

C:\Users>yt-dlp -f 18+139 https://www.youtube.com/watch?v=_cDocBjVkUkk
[youtube] _cDocBjVkUk: Downloading webpage
[youtube] _cDocBjVkUk: Downloading android player API JSON
[info] _cDocBjVkUk: Downloading 1 format(s): 18
[download] Destination: C:\Users\VM\Downloads\Never Do This When Pumping Gas.mp4
[download] 100% of 3.05MiB in 00:00
```

Note that it saved to the location set in the config file, the Downloads folder with the specified filename. If no option is given in the config file or on the CLI, it'll save it in the current directory with a name that's part of the title with some random characters at the end.

Something else you may want to do with yt-dlp is download entire channels or playlists. Downloading an entire channel is simple, just use the channel URL instead of a video URL. You can get the channel URL by going to a channel's homepage and then the "Videos" tab. For playlists, either get the URL of the playlist itself, or just a video that's in the playlist and use the "--yes-playlist" option. However specifying formats can be a little tricky when downloading entire channels or playlists, as not every video is available in the same formats which can cause issues if you specify specific formats. The best solution is to use more general formats than using a format's id number. There's a few ways to use more general formats, but the easiest are "worstaudio", "bestaudio", "bestvideo" and "worstvideo". If you're not downloading music, I'd recommend just using the "worstaudio" option since it won't make a noticeable difference. Video is trickier, since "worstvideo" will usually download a very, very

low resolution video that will probably be unsatisfactory. You can simply specify a resolution using “[length<720]+worstaudio” which will use the best format that is less than 720p. Similarly you can also use “<=” for less than or equal or “>=” greater than or equal if you’d like a higher quality video. However in my opinion 720p is a good option for downloading multiple videos as it’s not as large as 1080p, but still good quality.



Note, the -s option just simulates what it’ll do without actually downloading anything, I only used it for demonstration purposes. Also note the “bv” in front of [length<720] is for “bestvideo” likewise “wa” is the abbreviation for “worstaudio”.

Much like wget, there’s a myriad of options you can use with yt-dlp, I’d recommend using “yt-dlp –help” on Windows or “man yt-dlp” on Linux, to see all the available options and what they do. Another useful option I’d like to mention before moving on is the -a option, which reads a plaintext file you created with a list of URLs to download, instead of specifying URLs on the command line.

Lastly, some videos on YouTube are age restricted and so won’t let you view or download them if you’re not logged into your account. There’s a few ways to log in to your account, you can use the -u option followed by your account name and yt-dlp will prompt you for your password when it tries to download. The other option is to log in to YouTube on your browser and then add the browser extension “cookies.txt” and use it to export your cookies for YouTube to a text file, then use yt-dlp with the option --cookies followed by the path to the file with the exported cookies.

Downloading Websites

For this we'll be using wget, so you'll need to have it installed and added to your path if you're using Windows. Downloading a website for local viewing is quite simple, all we *need* to accomplish that is the following command

```
wget -kpm <website-url>
```

however we also don't want to accidentally DDoS the web server we're downloading the site from, as well as some sites will try to prohibit you from doing this through various means. So in order to avoid attempts at stopping us and just generally being social Internet users even if they're not, we'll want to use a couple options that will reduce the resources we'll be demanding on the server. Probably the most two common for this is --wait=X and --random-wait. Wait simply allows you to specify how long in seconds to wait between each request, random wait adds some randomness to how long it waits which is useful if the website tries to prohibit wget and other non-browser downloads. Random wait can also be used without --wait and will default to a wait time of 2 seconds. Another option is -U which allows you to specify a user agent string which will help you look a little more like a web browser than wget. If you don't know what a user agent looks like, just google "what is my user agent" and use that. The last one you'll want to consider --limit-rate=Xk which will limit the bandwidth that wget uses while performing the download. So --limit-rate=20k would limit the download to using 20 kilobytes per second.

So all in all our final command for downloading a website will look something like this.

```
wget --wait=5 --random-wait --limit-rate=20k -U "Mozilla/5.0
(Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0" -mkp
<website-URL>
```

Again, this is only scratching the surface of what wget can do, I'd highly encourage you to read the man/help page and look into some tutorials and guides on it to become more familiar with it, as it's a very powerful program.

Cache Recovery

One very possible scenario with today's Internet, is that you may read some article or other post and a short time later that content is either edited or removed and you'd like to have a copy of the original that you viewed, however you didn't think to save it when you first viewed it.

Not to worry, with a little bit of trouble you can recover items from the cache of your browser as you saw them. This is easiest on Windows, however on Linux it's really only feasible on Firefox although the process is a bit tedious. As for what a cache is, the browser cache is simply content you've already viewed in your browser that's saved to your computer to reduce what needs to be downloaded on other pages of the website (different webpages on the same site will often use the same CSS, JavaScript, etc). Which is why if you have a slow internet connection, you probably have noticed that when you click the back arrows in your browser it's much faster than downloading a new page and that sometimes even with no internet connection your browser's homepage may show up normally since it's cached.

The first and easiest way to recover something from cache, this works on an OS or browser equally, is to simply disconnect your computer from the Internet and then navigate back to that page through your browsers history. This method doesn't always work, but it's an easy first effort. If it doesn't work simply close out any tabs that are open to the website you're trying to recover a page from and reconnect to the Internet if you'd like.

Windows

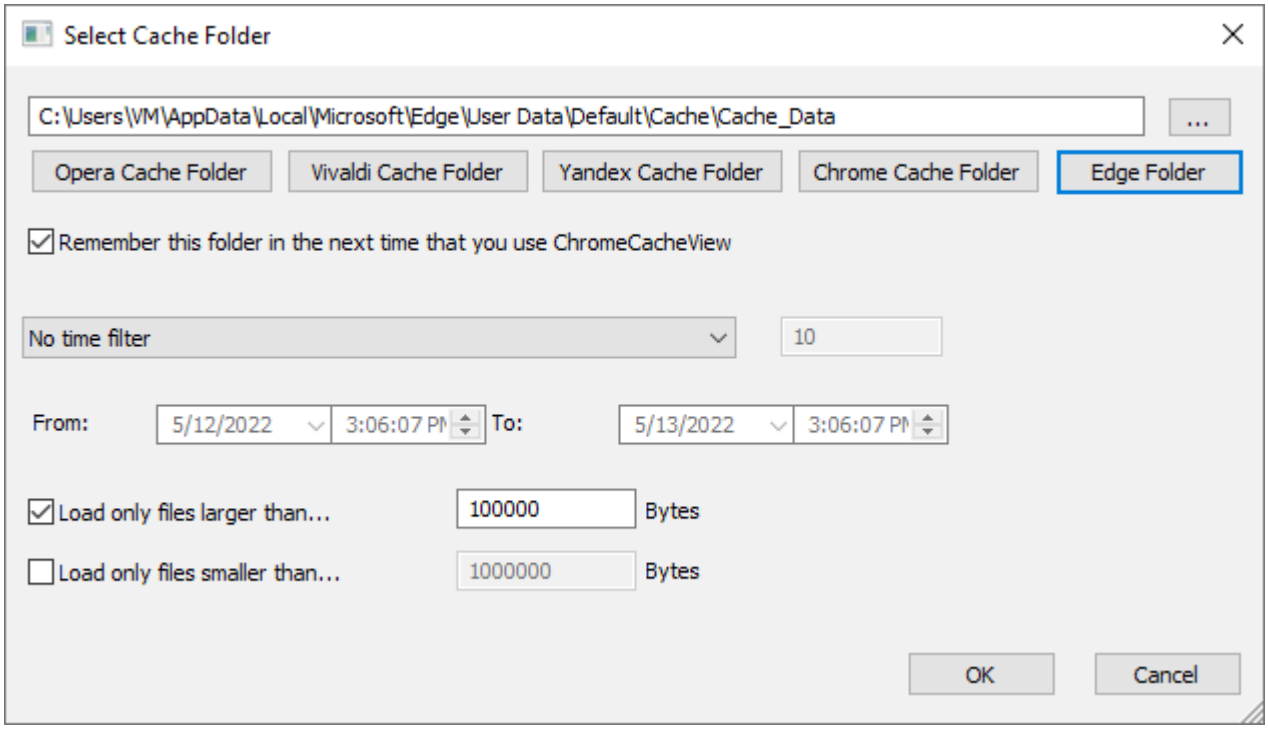
This next process will be for Windows and will work with any nearly any browser. Download the appropriate cache viewer program from nirsoft (Internet Explorer, Firefox or Chrome. Note Brave, Edge, Chromium will all work with the Chrome version with one small change).

https://www.nirsoft.net/utils/chrome_cache_view.html

The IE and Firefox ones are listed at the top, however the Chrome viewer is listed towards the bottom of the page just above the table of available languages.

The program doesn't need to be installed, it's just a single executable file that runs. However we will want to move it somewhere with it's own folder, since it'll create a configuration file that needs to be in the same folder for if we make any changes to the settings, which we'll need to do if we're using a Chrome based browser that's not Chrome itself. Once you've put it where ever you like, create a shortcut on the desktop to it for accessing it easily (Right click the exe file in File Explorer → Send To → Desktop (create shortcut)).

Afterwards run the program. If you're not using Google Chrome the first thing you'll want to do is set the correct cache folder location, as by default it'll be set for Google Chrome, but the derivative browsers will have slightly different locations. To do this click (File → Select Cache Folder) and you should see something like this.



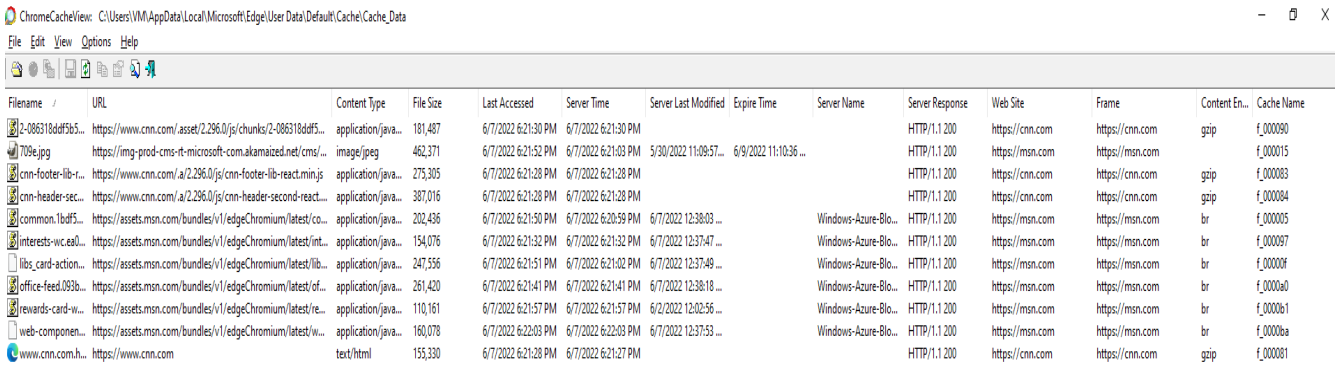
As you can see, there's a few buttons for common browsers such as Edge, Chrome (if you already changed it to something else), etc. Brave isn't listed, but you can simply paste the following line (replacing the username with your own)

```
C:\Users\<user-name>\AppData\Local\BraveSoftware\Brave-Browser\
User Data\Default\Cache
```

Or click on the button with the three dots and go to “C:\Users\<user-name>\AppData\Local\” and search for folders named after Brave or whatever organization used the Chrome derivative browser you’re using and find the cache folder that way.

Additionally we have a few other options, such as setting filters based on time and content sized. If we’re looking for a webpage, it’ll be helpful to set the minimum size to 100,000 bytes to weed out some of the smaller stuff and of course use the time filter if you can remember a time frame that you visited the page in question.

After you’ve applied these settings you should see something like this, but likely with a lot more options.



Probably the two most helpful options will be sorting by size, going largest to smallest, or sorting by content type and checking that way, whether it’s a webpage/document or image, etc.

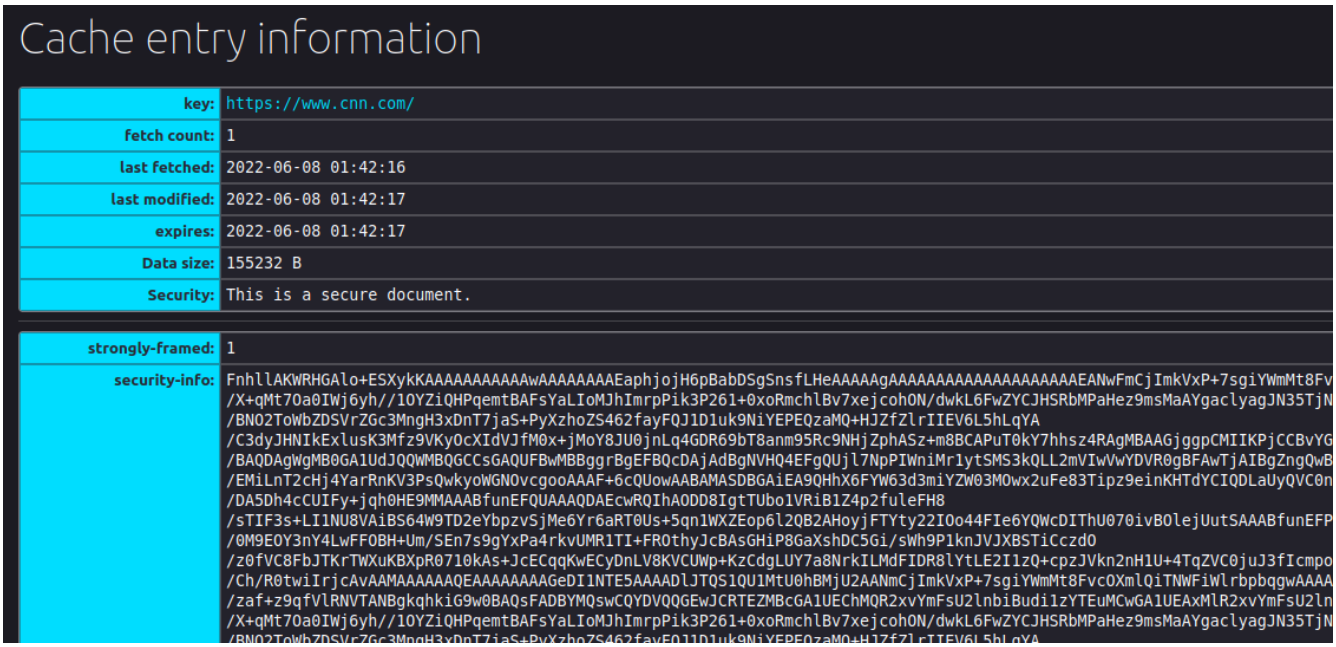
Once you think you’ve found what you’re looking for, right click on it and open it. If it’s what you want, go back and right click on it again and select “Copy Cache Files To” to save the file

outside of the browsers cache. Although note, that even if you find the right page, this method may not work depending on how JavaScript heavy the site is.

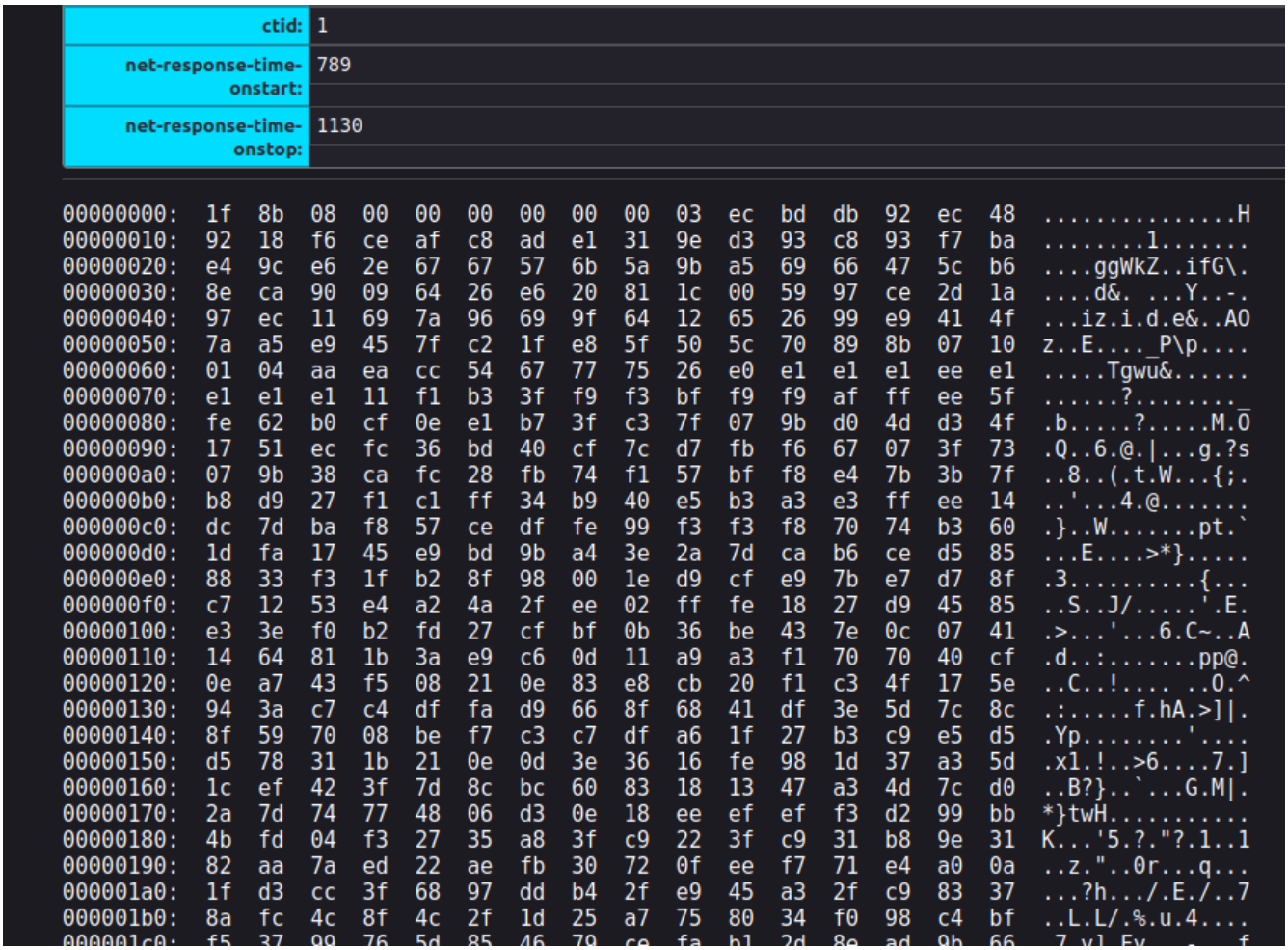
Linux

I'm only aware of how to do this on Firefox, no idea how or if it can be done on Chromium browsers on Linux. I'm not aware of any such cache viewer programs for Linux like there is on Windows, however I have read of people having success setting up Chrome cache viewer on WINE. This is more or less a manual process and will start with typing in "about:cache" into the URL bar of Firefox.

From there, you'll have the choice of viewing the memory cache or the disk cache. I can't really give any advice on what content will be in which one, so just take a guess. From here you can use "Cntrl + F" to search for what you want. Once you think you've found it, click on the link for it in the far most left column and you should see something like this.



From here, scroll down until you see something like this.



ctid:	1
net-response-time-onstart:	789
net-response-time-onstop:	1130

```
00000000:  1f  8b  08  00  00  00  00  00  00  03  ec  bd  db  92  ec  48  ................H
00000010:  92  18  f6  ce  af  c8  ad  e1  31  9e  d3  93  c8  93  f7  ba  ........1.......
00000020:  e4  9c  e6  2e  67  67  57  6b  5a  9b  a5  69  66  47  5c  b6  ....ggWkZ..ifG\.
00000030:  8e  ca  90  09  64  26  e6  20  81  1c  00  59  97  ce  2d  1a  ....d&. ...Y..-.
00000040:  97  ec  11  69  7a  96  69  9f  64  12  65  26  99  e9  41  4f  ...iz.i.d.e&..AO
00000050:  7a  a5  e9  45  7f  c2  1f  e8  5f  50  5c  70  89  8b  07  10  z..E...._P\p....
00000060:  01  04  aa  ea  cc  54  67  77  75  26  e0  e1  e1  e1  ee  e1  .....Tgwu&......
00000070:  e1  e1  e1  11  f1  b3  3f  f9  f3  bf  f9  f9  af  ff  ee  5f  ......?........_
00000080:  fe  62  b0  cf  0e  e1  b7  3f  c3  7f  07  9b  d0  4d  d3  4f  .b.....?.....M.O
00000090:  17  51  ec  fc  36  bd  40  cf  7c  d7  fb  f6  67  07  3f  73  .Q..6.@.|...g.?s
000000a0:  07  9b  38  ca  fc  28  fb  74  f1  57  bf  f8  e4  7b  3b  7f  ..8..(.t.W...{;.
000000b0:  b8  d9  27  f1  c1  ff  34  b9  40  e5  b3  a3  e3  ff  ee  14  ..'...4.@.......
000000c0:  dc  7d  ba  f8  57  ce  df  fe  99  f3  f3  f8  70  74  b3  60  .}..W.......pt.`
000000d0:  1d  fa  17  45  e9  bd  9b  a4  3e  2a  7d  ca  b6  ce  d5  85  ...E....>*}.....
000000e0:  88  33  f3  1f  b2  8f  98  00  1e  d9  cf  e9  7b  e7  d7  8f  .3..........{...
000000f0:  c7  12  53  e4  a2  4a  2f  ee  02  ff  fe  18  27  d9  45  85  ..S..J/.....'.E.
00000100:  e3  3e  f0  b2  fd  27  cf  bf  0b  36  be  43  7e  0c  07  41  .>...'...6.C~..A
00000110:  14  64  81  1b  3a  e9  c6  0d  11  a9  a3  f1  70  70  40  cf  .d..:........pp@.
00000120:  0e  a7  43  f5  08  21  0e  83  e8  cb  20  f1  c3  4f  17  5e  ..C..!.... ..O.^
00000130:  94  3a  c7  c4  df  fa  d9  66  8f  68  41  df  3e  5d  7c  8c  .:.....f.hA.>]|.
00000140:  8f  59  70  08  be  f7  c3  c7  df  a6  1f  27  b3  c9  e5  d5  .Yp........'....
00000150:  d5  78  31  1b  21  0e  0d  3e  36  16  fe  98  1d  37  a3  5d  .x1.!..>6....7.]
00000160:  1c  ef  42  3f  7d  8c  bc  60  83  18  13  47  a3  4d  7c  d0  ..B?}..`...G.M|.
00000170:  2a  7d  74  77  48  06  d3  0e  18  ee  ef  ef  f3  d2  99  bb  *}twH...........
00000180:  4b  fd  04  f3  27  35  a8  3f  c9  22  3f  c9  31  b8  9e  31  K...'5.?."?.1..1
00000190:  82  aa  7a  ed  22  ae  fb  30  72  0f  ee  f7  71  e4  a0  0a  ..z."..0r...q...
000001a0:  1f  d3  cc  3f  68  97  dd  b4  2f  e9  45  a3  2f  c9  83  37  ...?h.../.E./..7
000001b0:  8a  fc  4c  8f  4c  2f  1d  25  a7  75  80  34  f0  98  c4  bf  ..L.L/.%.u.4....
000001c0:  f5  37  99  76  5d  85  46  79  ce  fa  b1  2d  8e  ad  9b  66  .7.v].Fy...-...f
```

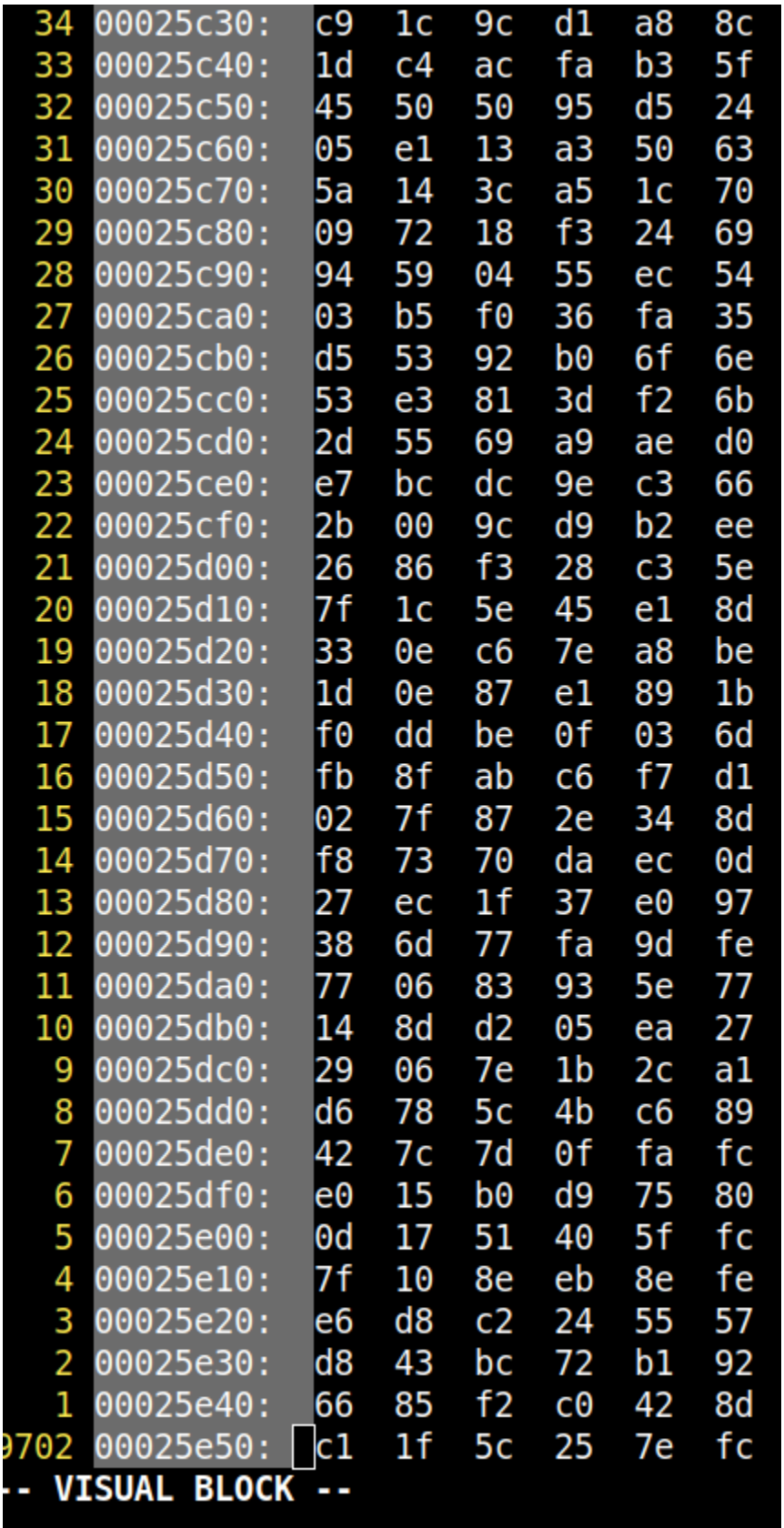
That part underneath the table with the blue on the left is what we want. Starting with left column counting by 10 starting from zero to the very end of the right column with the gibberish, we'll want to highlight all of it and copy it (holding down the "Page Down" key will be much faster than scrolling :)

Once we've copied all of it, we'll want to open up a terminal and give the command

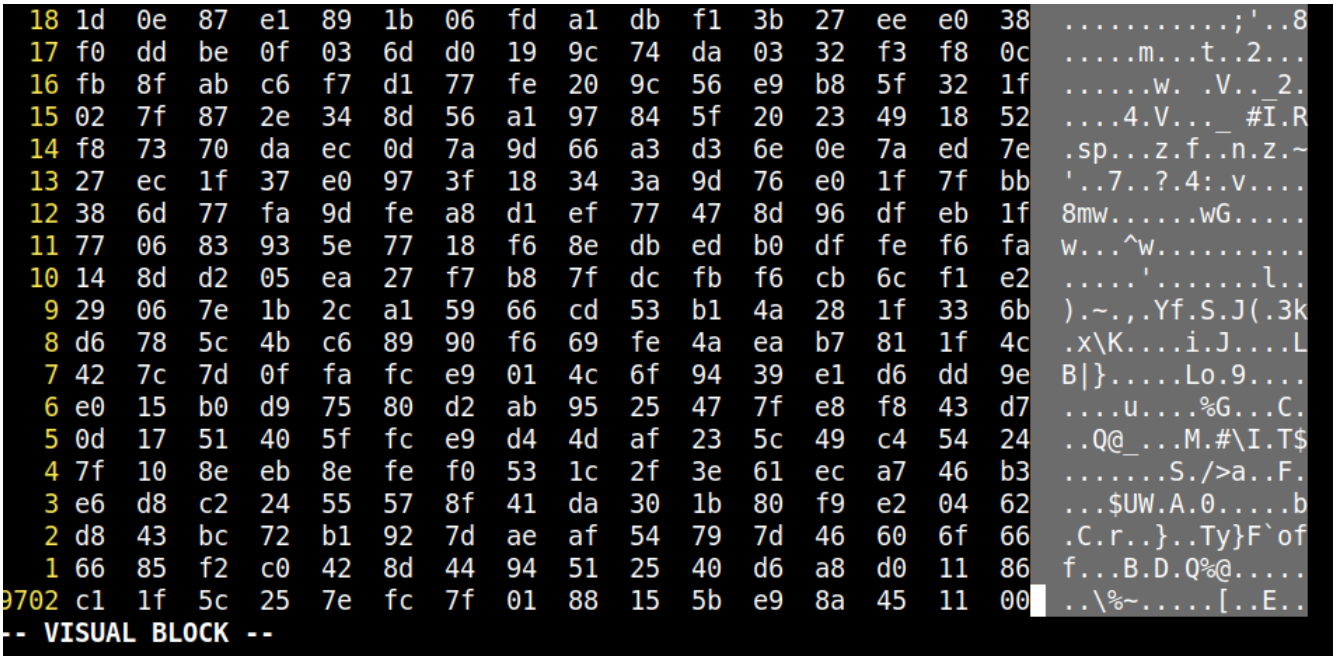
```
cat > test
```

afterwards press "Cntrl + Shift + V" in the terminal to paste the data and then press enter and then "Cntrl + D" to close the new file named "test".

Next we'll need to open the newly created file in vim. If you don't know how to save and exit in vim, google that now. Once opened in vim and the character is in the upmost left corner, press "Cntrl + V" to go into visual block mode. Press "Shift + G" to go to the bottom of the file, then press "L" until you've highlighted the first column and the spaces after the colon, like so.



From here simply press “d” to delete all the highlighted portions. Press “gg” to go back to the top and then “$” to go to the end of the first line. Repeat the process removing the entire right column including the preceding space, it should look something like this.



And again press “d” to delete the highlighted area. Finally press “:wq” and enter to save the changes and exit vim.

Now that we have our data cleaned up, simply run the command

`xxd -rp test > test1 (or whatever name you like)`

next run “file test1” and see what file type it is. The reason is that the recovered fill could be compressed with gzip as it was sent to the browser, in which case we’d need to run “gunzip” on it before we can have our totally extracted file. Note that if file returns the type “data” as far as I know you’re kind of shit out of luck. Sometimes you get this on very JavaScript heavy sites, but most websites, you should get an HTML file out of this process or an image if that’s what you were looking for. (Video is possible, however videos are too large to be stored in

one “slot” so you’d have to repeat this for each segment of the video appending the extracted data to a file. If you’d like to have a go at it, watch a YouTube video and then in cache look for stuff from the googlevideos.com domain, good luck! :)

File Sharing

One thing that’s surprisingly hard to do with the current Internet is sharing large files. E-mail typically has a pretty small file size limit that’s quite restrictive and services like Google Drive and Dropbox have a lot of privacy implications as well as require some sort of account and maybe even to pay. In this section we’ll cover how to retrieve and share files in a more “native” way without having to rely on a service, however a few anonymous file sharing services will be covered since they can be easy and convenient.

Also when it comes to restricting who’s able to access the content, file encryption is important since most of the methods we’ll cover don’t have ways of determining who is authorized to access the file, so we’ll likely want to encrypt the file and share the password through some other channel to the people we want to access it.

Anonymous File Sharing Services

First we’ll briefly cover a few anonymous file sharing services being catbox.moe (and it’s temporary service litterbox.catbox.moe) as well as pastebin.com. Catbox isn’t hard to use at all, simply upload the file you’d like and it’ll generate a link to it that you can share. However the main catbox service stores files permanently (although I’m sure it deletes them at some point), but is restricted to 200MB which isn’t much better than e-mail. The other service litterbox allows larger files up to 1GB at the moment (I believe in the past it was 2GB, will likely change in the future). However the longest you can host a file on it is 3 days, which is may or may not be suitable.

The other anonymous service is pastebin. It’s intended for sharing code snipets so it only supports plain text, however you can convert any file into base64 which will encode it into

plaintext so it can be shared this way. To convert a file or some text into base64 and back again, there's a myriad of services that do this, one of which is.

https://base64.guru/converter/encode/file

Note that encoding something in base64 is not encryption, anyone can decode it without any shared secret like a password, so if you want to encrypt it you'd want to do that before encoding it as base64. Also if you're using Linux, you can encode and decode base64 using the "base64" command from the command line.

Another nice feature of pastebin is that you can password protect what you upload as well as set a time for it to expire and presumably be deleted.

Torrents

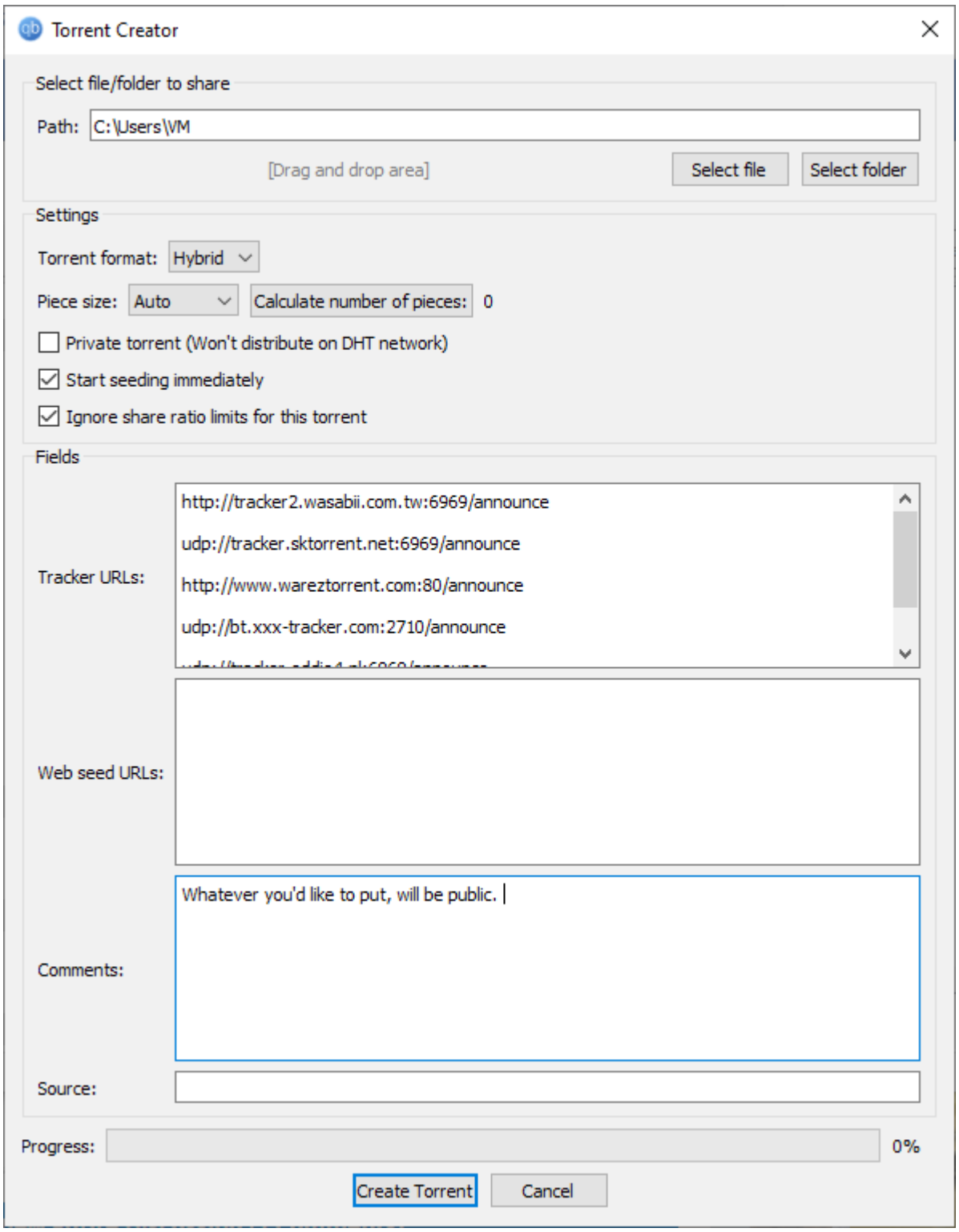
First I'd like to clarify that the bit torrent protocol is a perfectly legitimate protocol and as far as I know isn't illegal in any US or European jurisdiction. I bring this up because many people have the idea that torrenting is illegal since it's mostly used for sharing copy righted content (movies, TV shows, etc) which is illegal no matter what protocol you use to share it. Torrents can be created for any file you like and generally there's nothing illegal about it so long as you have the legal rights to distribute this content, for example I could create a torrent of this PDF and share it and it'd be perfectly legal. The main advantage of torrent is that it's anonymous in that it doesn't require any sort of account, although the IP address of the device will be revealed (this can be obscured using a VPN with port forwarding, or renting a server to seed from). The other big advantage is that there's no restriction on the file size, as long as the device downloading has enough space on it's hard drive.

First we'll cover downloading torrents to cover that base as well as explain a little more about how the protocol works.

First in order to upload or download a file via torrent, you'll need a torrent client installed on your computer. If you're using Linux you'll probably already have "Transmission" installed and on Windows there's many options like "qbittorrent" you can use.

There’s two methods of downloading a torrent, magnet links and torrent files. Magnet links are essentially just URLs to a particular torrent, whereas a torrent file is a separate file (with the extension .torrent) that tells the torrent client where it can find the actual file. Both are simple to use, to use a torrent file download the file and for a magnet link just copy the link, then go to your torrent client and click “File” and you’ll likely have the option of either using a torrent file or magnet link, just chose the appropriate option and paste the link or select the torrent file to use.

Sharing isn’t much more complicated. First if you’d like to keep the data private only to those few you want to share it with. It’d be best to encrypt the file before creating the torrent for it. Once you have your file or folder you’d like to share (you can turn an entire folder into a torrent as well). Simply go to your torrent client and under either “Tools” or “Files” you should have an option to create a new torrent. From there select the file or folder you’d like to share and for the most part leave the default options. Don’t check the box for private if you’re not using a private tracker (if you don’t know what that is, you aren’t) although you may want to check the box for ignoring the upload ratio. Lastly just google “popular public torrent trackers” and get a few to put in the trackers field and put a comment if you’d like, the source field is also something for private trackers you don’t need to worry about.



Afterwards it'll create the .torrent file that you'll want to share with whoever you want to download the file. The .torrent file will be very small so you can share it via e-mail, catbox/litterbox or any chat app likely. Some torrent clients may give you the option to create a magnet link instead of a torrent file which is obviously easier to share.

Non-Computer Stuff

To wrap this up, I'd like to end this covering some topics not related to computers. It would be an understatement to say that the events of 2020 and the years afterwards have a lot of people concerned about the future of their countries and the world overall. I'd like to try to shed some light on what to expect as well as things to consider moving forward with your life.

Economics

If there was one idea I wish I could get everyone in the world to consider. It's that the economic prosperity of post WWII America was a fluke that will likely never happen again in our lifetimes and things will only get worse from here.

There's many factors to this, but I'll just stick to the quick run down of one, which could be called the "Surplus Energy Economic Model" or could also be refereed to as "Peak Oil". A lot of people dismissed the thesis of Peak Oil due to the large amount of oil reserves that exist which would seem to contradict it. However the point of the Surplus Energy Economic Model and Peak Oil was that the easiest to extract oil and other forms of energy would be utilized first since they're the most cost effective. Essentially all economic activity in the modern age is dependent on having physical energy to expend on some process. So the early stages of extracting fossil fuels would be extremely prosperous as the easiest and cheapest sources would be utilized first. As these initial easy to access sources are depleted, more difficult to access sources must be used later that are more energy intensive/expensive to extract the energy from. An example of this is fracking and the Canadian Tar sands. These were touted as insuring the continuation of the current economy by the raw volume of energy that can be extracted from them, however it really just proves the peak oil theory that we're now getting to a stage where we're extracting more expensive energy which leaves less "left over" for other economic activity. Here's a link that explains the phenomenon better than I can.

https://web.archive.org/web/20220510045409/https://surplusenergyeconomics.wordpress.com/professional-area/

Whether you buy into the theory or not, I think it's very important to work on self sufficiency to prepare for the future. You can gain a great deal of self sufficiency without becoming a full blown homesteader who's 100% off the grid. Also in regards to emergency preparedness or "prepping" people often have this conception that it's about preparing for TEOTWAWKI (The End of The World As We Know It) or some other apocalyptic scenario, which seems to turn a lot of people off to it because they find these events unlikely. Always remember that *no prep is insignificant.* From personal experience there's been times that having 5 gallons of water saved helped massively in dealing with storms and the associated damage. Don't discount small preps as many of the scenarios you're likely to face will be short in duration. Even if you live in a small apartment you can have a few gallons of water and a week's worth of food stored away for a scenario such as a storm or temporary civil unrest that may bring down infrastructure like water or prohibit going to the grocery store (It's also worth noting even FEMA recommends having 3 days worth of supplies on hand, and that guidance was created well before 2020). Also consider having a method of cooking without city power or gas such as a camping stove and required gas. For sanitation and hygiene having some baby wipes and hand sanitizer on hand can help without having to dig into your water reserve. I won't go too much further on emergency preparedness as there's plenty of content on that already, although most of it is biased towards large catastrophic events, however I'll mention you should have a proper first aid kit and if you don't know how to use it, take a course on first aid.

Back to the topic of self reliance, to help illustrate what we're trying to achieve, we want to reduce how often we're paying for a service we could do ourselves. As the economy gets worse prices generally go up (whether you want to call it that or inflation), your personal income very well may go down as well as shortages are a very real thing at the time of this writing and have been the past few years. There's many ways we can do this without moving into the woods and living like Ted Kaczynski. Although I absolutely do recommend procuring food from "outside the system" such as a garden, buying eggs from a neighbor or hunting. Should there be some food crisis in the near future, a deer in a deep freezer or personal garden can go a long way in holding you over until the crisis is resolved. Additionally doing your own repairs on things like cars, house and computers can save a lot of money. Even just learning how to change brakes and fluids on a car will be the majority of the maintenance

your car will need, as well is a good stepping stone to other jobs like thermostat, accessory belt, suspension, etc. Remember with prices going up when you take your car to a shop or something, that price is getting baked in for each thing the shop spends money on, whereas with doing it yourself you're only eating the increase in price once.

Transportation

Besides food and water, another critical and underappreciated aspect that many preppers seem to overlook is transportation. Gasoline can be stored and rotated insuring you always have a fair amount of usable gasoline available. However even the most fuel efficient cars only get about 40 mpg which even if you have 50 gallons save is 2,000 miles before you run out and are forced to buy gas again. This would probably be enough to get you through a temporary crisis, however I think we should also consider the possibility that gas will increase significantly and permanently and to try to protect ourselves from that. Ultimately I think everyone should have an alternative means of transportation that either doesn't use gas/diesel or uses it more efficiently than cars by an order of magnitude (ie motorcycles or mopeds).

I'd like to give a brief mention to motorized bicycles, as they greatly reduce the physical exertion required for traveling on a normal bicycle and don't carry the insurance and registration requirements of motorcycles. You've likely heard of electric assisted bicycles at this point, but also consider gas assisted ones as well, although they come with a lot of draw backs such as noise and much more mechanical complexity. There's many 2 and 4 stroke kits available on the Internet that can be installed on a normal bicycle to provide mechanical assistance. I'm not very familiar with the differences in weight and range of gas versus electric although I'm sure range varies greatly with how much you use the assistance. I mention them because particularly if you live in a rural area and can't afford a motorcycle or it's out of your comfort zone, some sort of assisted bicycle could be a much more feasible option without you having to become a cycling athlete.

Consider preparing for this now rather than later as whenever gas goes up more fuel efficient vehicles go up in price as people want them to pay less in gas. Besides avoiding things like

the price surge, options like motorcycles take quite some time to get good enough on to be able to safely ride in traffic to do your day to day activities. If you wait too long you could wind up having to wait months for an MSF course, buying gear and a motorcycle (and likely paying more for it) and practicing, all the while suffering from high gas prices or potentially a shortage. Versus already having the skills and equipment to transition to the motorcycle or moped before that situation occurs. I'd also like to point out that for general purpose transportation mopeds are likely the better option as they typically have a lot of storage for their size and are much cheaper and easier to operate than a motorcycle (usually have automatic transmissions as opposed to manual and the brakes are more similar to a bicycle) and larger ones are capable of highway speeds; so if you live in a rural area and need to get up to 55-60mph, they should have you covered there. Regardless of whether you need to achieve these speeds, I'd highly recommend getting a moped capable of them. One for better acceleration and also so you're not riding the engine at max RPM when you're going 35mph. Some jurisdictions don't require a motorcycle license for mopeds below a certain engine size, besides not recommending you go that small for the reasons listed previously, getting your motorcycle license is well worth it. Beyond the training itself and getting to ask experienced riders questions, completing the MSF course will get you a discount on your insurance on a motorcycle or moped.

A bicycle is much less skill and gear intensive than a motorcycle, but I'd still recommend getting a setup before you need it as well and even going about using it in place of a car to try to figure out any issues you have or things you may need. Try to get some cargo system for it and go grocery shopping with it and see how it works and try to find some good routes you could use to go about some of your tasks.

Another thing that I'd recommend for nearly any alternative mode of transportation is getting a back pack with waist and chest straps. Whether you get a motorcycle, bicycle or simply walk. A backpack with waist and chest straps will help immensely as the waist straps help distribute the weight off your shoulders making it less fatiguing and chest straps help secure the shoulder straps from sliding around which is nice when riding a bicycle or motorcycle. Although these straps are often on rucksacks, many smaller bags often called "day hike bags"

or “assault packs” will have these as well. The former will usually be styled similarly to a ruck sack and the later will normally be “tactical” looking although solid black ones are available.

A quick note about motorcycles. Make sure to get quotes for insurance before buying a motorcycle. Insurance rates vary drastically for different models as well as engine sizes, much more so than cars. Something else, many people on the Internet will advise you to get a 650cc as a first bike because “You’ll get bored of the 250cc in less than a year and get rid of it”. I disagree for a few reasons. First for new riders with no experience, engine size makes a big difference in insurance rates, some companies quoted me over double for the midsized version of a bike as opposed to the smaller displacement one. Additionally I think there’s a bit of bias in the people who say this as there’s plenty of experienced riders out there who are perfectly happy with small displacement bikes. I think the more “adrenaline junkie” (I don’t mean that as a pejorative) riders are over represented in people who talk about motorcycles online as well as I suspect they’ve somewhat lost touch with what it’s like as a beginner rider, especially for someone who’s not getting into them just for thrills.

Lastly we’ll cover vehicle selection and ownership in regards to cars. In addition to gas prices something else to be concerned with is vehicle longevity as it’d be an understatement to say the car market post 2020 has been crazy and it’s entirely possible this change could be more or less permanent. Also, seriously consider getting a FFV (Flex Fuel Vehicle) if buying a car; also check the gas cap of your current one to see if it can take E85, as many FFVs don’t have badging indicating they’re a FFV. In the future E85 could potentially be much cheaper than normal gas and be a great savings opportunity. If your car isn’t an FFV conversion kits are available if you’re interested in that.

First things first in regards to car buying. Before buying a car on the premise of saving fuel, make sure to do the math on how long it’ll take to pay for itself. Additionally take the EPA mileage rating with a grain of salt and check websites such as fuelly.com or fueleconomy.gov which show self reported fuel economy from owners of the vehicle which are often much

closer to reality than the EPA ratings. And definitely don't fall for the heuristic that newer and better fuel economy equals money saved, if you drive a 10 year old Ford Expedition and are looking to downsize to a compact sedan or hatchback, buying a brand new Prius probably won't save you any money for a long time. Try to look for something that's about the same value as your current car and gets better gas mileage. New cars boast better MPGs than their predecessors, but even the advertised mileage isn't all that much better in the grand scheme of things as things like turbo chargers and 9 speed transmissions become more common as well as cars weighing more due to safety and other regulations. In my experience it seems like cars really haven't made any significant gains in fuel economy since the 90's with the introduction of multi point fuel injection. I've personally owned mid 90's and late 00's compact cars that got exactly the same fuel economy in real world driving and the 90's car cost a fraction of the price of the newer one although of course repairs were more frequent.

It's important that you *never finance if at all possible!* I'll cover a few exceptions in a bit, but paying compounding interest on a depreciating asset is as stupid as Dave Ramsey says it is. Some people seem to misinterpret this advice and think it means that if you're planning on buying a $30k car with $10k down on it that it means you should just pay the $30k upfront in cash. This is *NOT* what it means, it means in that scenario you should buy a $10k car in cash and take what would be the payment on it and put it towards your mortgage or some other asset or savings. A lot of people have trouble with this because cars are a big status symbol, but at some point you have to deal with the current reality which isn't looking nearly as good as we were told it was going to be growing up. The main exception to this rule was implied by *if at all possible* which is a scenario where you can't afford a reliable car in cash. Say in your area the cheapest cars that can be trusted for daily driving duties are $5k and you only have $3k in the bank. In this situation you really don't have a choice but to finance, but I won't leave you high and dry. The first thing is *DO NOT FINANCE FROM THE DEALER* small loans like these is how shady used car dealers make all their money, don't do it full stop. Instead go to a credit union in the area and see about a loan with them. Typically credit unions are much more willing to make small loans like these and will often have reasonable terms, one thing to look for and confirm is that there's no penalties for making payments beyond the minimum. The reason is that my recommendation is to make the smallest down payment possible

(because even credit unions will often have minimum loan amount of around $5k which might be an issue with a large down payment) and just pay the loan off as quick as you can to minimize the interest you pay as well as your odds of ending up underwater on it.

Also, another reason why I advocate finding alternative means of transportation now rather than later is that in the event your car breaks down and you need to be at work the next morning, already having other means of transportation helps you better cope with this situation. Public transit or a bike (motorized or not) may not be viable for everyday use at the moment, but think of it as an insurance policy should something happen to your car or there is a gas shortage in your area (I've experienced brief gas shortages in the United States even before 2020, it's a much more real scenario than many Americans think it is)

As for vehicle selection, for brevity's sake I'll skip talking about specific brands and models and just discuss a few high level concepts. One newer cars are absolutely getting more difficult and expensive to work on and repair, pretty much everything your grandpa complains about modern cars is true. Electronics are getting incorporated into more and more trivial parts making them more expensive to replace as well as difficult to troubleshot and replace. Compared to even just ten years ago many new cars today have various sensors in the side mirrors for blind spot detection, electronically controlled shocks to change ride firmness and even electronic parking brakes that some cars require a special tool from the dealer to retract so that you can replace the rear brake pads (again I 100% encourage doing as much maintenance and repairs yourself.)

Additionally since one of the original topics of this document was privacy, it's also worth mentioning that there's serious privacy concerns regarding newer cars to say the least.

https://web.archive.org/web/20220505220145/https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect

As for longevity, without delving into makes and models, I think the simplest advice is to simply stay away from turbocharged vehicles and before buying any make or model, do research into issues with it burning oil. A surprising number of newer cars are having issues with burning oil while being practically brand new and the manufacturer claims that it's "normal". No, new cars burning enough oil that the owners have to add oil between changes is never normal, except perhaps some high performance exotic. And it's not just the usual suspects that this happens to either so make sure to do your research.

Also if you do decide to purchase a newer vehicle, be very weary of new sophisticated technology in regards to important things such as the powertrain. If some new sophisticated engine or transmission is introduced try to avoid it as if there's a serious issue with it, manufactures will jump through hoops to avoid an expensive recall and if the catastrophic failure doesn't normally happen till the vehicle is out of warranty, even less likely they'll do anything to fix the issue on cars already on the road. A perfect example of this is the automatic transmission of early Ford Fiestas that would nearly always go out before 100k miles. Also note that these cars are fairly old now so even when shopping for used cars, look out for these issues.

Advice for New Mechanics

The first and most important thing anyone getting into vehicle repair should know is *NEVER* get under a vehicle that's not properly supported. Your vehicle likely comes with a scissor jack which is there for changing a tire on the roadside. Under no circumstances (unless not getting the car repaired could lead to death or serious harm) get under a vehicle only supported by this. These jacks are fine for changing a tire because that can be done without ever getting under the vehicle. When removing or placing the new tire on, grab the tire by the sides so that if the jack fails your hands won't be crushed, also be aware of how your legs are positioned so that they won't be crushed either if the vehicle falls.

Additionally this same principle applies to hydraulic floor jacks. Although they appear much more sturdy and stable than a scissor jack all that stability and contingent on a rubber seal

holding. If that rubber seal fails gravity will do it's thing and return the vehicle to the ground. Floor jacks should only be used for raising the car up for jackstands to be placed underneath it which can be trusted to hold the car up on flat even ground. Additionally if you're raising the front of the car up, it's best practice to have the parking brake engaged (not just putting the transmission in park) to prevent the vehicle from rolling backwards. If you're jacking up the rear of the car, make sure something is placed in front of at least one of the front wheels to prevent the car from rolling forward (if you're only raising one of the rear wheels, you'd specifically want to chock the front wheel on the opposite side of the one being raised)

With raising a car up, you also need to be aware of what locations it's safe to place the jack and jackstands. If you know how to change a tire you're likely aware of the pinch welds next to each wheel well, towards the center of the car. These are safe lift points and for jackstands, however if we use the floor jack on them we won't be able to place a jackstand in that location since the jack itself will be using that spot. What you want to do is lift the vehicle from the front or rear subframe member, not to be confused with the bumper, and place the jackstands underneath the pinch welds while the jack holds up that end of the car from the center of the subframe which will often have a designated lift point.

Also it's worth mentioning in areas where roads are salted in the winter, it may be a better option to use part of the frame along the side of the car rather than the pinchwelds as the area around the pinchwelds is subject to lots of salt being kicked up by the tires and is often one of the first places of the car to rust.

If you're not confident in your abilities to identify the safe lift and jack points of your vehicle, this is one reason I'd highly recommend picking up a Haynes or Chilton repair manual for your vehicle. These manuals will often list all or most of the safe lift and jack points including subframe members as well as they offer good guides on most common repairs and simply reading them will help your mechanical knowledge greatly. I initially got most of my mechanical knowledge as a teenager from just reading the Haynes repair manual for the family truck. Although I'll add that you should still find guides and information on doing specific repairs on the Internet and not just solely rely on these manuals as Internet guides will often

include tips about how to do the job more efficiently or to deal with annoyances that the repair manual might not mention. Additionally as you get into more advanced mechanical and electrical repairs, something to consider is buying the factory repair manual for your vehicle. These manuals are often a couple hundred dollars and assume a fairly high level of mechanical knowledge of the reader than the simpler Haynes and Chilton manuals. However they give an incredible amount of information about the vehicle which is very useful for more advanced repairs especially electrical, as the electrical diagrams in the more basic manuals leave a lot to be desired.

For Internet resources I'd highly recommend the YouTuber "Eric The Car Guy" older repair videos. Although they're mostly on 90's and 00's Hondas, these repairs are quite similar on different vehicles and he does a very good job explaining how the part works and how to trouble shoot it which will also usually be universal across different cars, although you absolutely should seek out information specific to your vehicle before trying a repair as their can be quirky issues with common repairs on some vehicles.

Another piece of advice is to check with your insurance company to see if they offer coverage for towing your vehicle in the event of a break down or some other failure. Many insurance companies offer this incredibly cheap, I believe mine only adds $10 to the six month premium. Considering that even short tows can easily be a few hundred dollars, you only need to use it once or twice for it to pay for itself and at least with my company using it doesn't affect my insurance rate at all. Also remember you likely won't be required to tow it to a mechanic. I've used it multiple times to tow a vehicle to my house where I fix it myself or to a motel on road trips and fix it there in the parking lot, so you're not limited to having it towed to a professional mechanic.

Another important topic worth covering is acquiring parts. Generally your big box part stores like AutoZone, O'Reillys, NAPA, etc. Should be avoided if possible. The parts at these places

are usually quite expensive and low quality compared to what's available online. I'm not sure about outside the US, but within the US

https://rockauto.com

is far and away the best place for buying car parts. They're usually much, much cheaper than the big chains and if you don't get the lowest "economy" tier, the parts are *much* higher quality than what you get at the big chain stores.

Another potentially good idea is sourcing parts from junkyards. In my opinion the best advantage is that this gives you the opportunity to practice as a new mechanic since you'll get a chance to remove the part on the junk car without fear of damaging something on your own. Also junkyard parts are often even cheaper than parts bought online through rock auto. However obviously these are used parts that have been sitting in a junkyard for some time without use. So it's best to avoid getting parts from junkyards that are consumable (ie brake pads) or have rubber as an important component (brake calipers, master cylinders, belts, etc). However junkyards can be a good option for mostly mechanical things such as alternators, powersteering pumps, exhaust (although catalytic converters will already be stripped from the cars in the yard) and radiators (all of which tend to be quite expensive new or re-manufactured). Junkyards are also a good source for interior components which are often incredibly expensive brand new as very few are made for replacements. Things like cruise control switches, turn signal stalks and various interior switches can be gotten from junkyards or bought used on places like eBay very cheaply. Additionally junkyards and eBay can be good sources for safety equipment like seat belts and airbags as new ones are often very expensive.

Next I'd like to cover a few potentially dangerous ideas that might be enticing to new mechanics, the first being the engine flush. The idea of the engine flush is that you add something to your engine oil a couple hundred miles before an oil change which will dislodge sludge in the engine so that it'll come out during the oil change. This is typically a bad idea on modern cars as modern vehicles have very small oil passages for sophisticated technologies

like variable valve timing and the like. The issue is that these smaller oil passages can be clogged by the dislodged sludge and lead to total engine failure as part of the engine stops receiving oil. 00's Honda's are the most notorious for this happening, but it's a very serious concern on many modern vehicles. In my opinion it's not worth risking on any vehicle with VVT (variable valve timing) and it's better to simply change the oil more frequently if your engine has lots of sludge, since most off the shelf oils have additives for removing sludge and this will happen at a much slower rate, but it is extremely unlikely to cause any issues. (To see if your engine does have a sludge issue, simply remove the valve cover(s) and inspect the valve train.) Although in my experience, it's quite unlikely any given car will have a sludge issue as even the most non mechanically inclined and irresponsible people seem to understand the importance of somewhat regular oil changes.

Something else to be aware of is automatic transmission fluid changes (this does not apply to CVT, manual or DCT transmissions). Which is that if the transmission fluid is too far overdue, replacing the transmission fluid can actually be very bad for the car and the best option is to just simply leave the old fluid in. The reason for this is that automatic transmissions rely on friction material on various clutches, very similar to the singular clutch on a manual transmission, which as the clutches wear the friction material comes off and becomes suspended in the fluid. What can happen when transmission fluid is too far over due is that there's not enough friction material on the clutches for proper operation, but because the friction material is suspended in the fluid, the transmission continues to work correctly. However if you were to replace it with fresh fluid without the old friction material suspended in it, this could cause the transmission to fail and require replacement.

As a general rule if the transmission fluid appears dark like used motor oil without any red color to it, it should just be left in until the transmission fails. However if it appears as dark red, depending on the service history and mileage/use of the transmission, it's more likely that it'd be good to replace the fluid; although when in doubt it'd likely be safer to just leave it in.

Another pitfall many new mechanics and car people fall for is cheap/easy performance enhancers or modifications that are designed to increase fuel economy. Although many are quite silly and few people fall for them, one of the most common ones people fall for is “cold air intakes” and after market exhaust systems.

On a car with no other modifications, “cold air intakes” and exhaust are essentially completely useless. The sparknotes version is that, although it may be hard to believe, the engineers who designed the car generally knew what they were doing and as power and fuel economy have been important metrics for selling cars for a long time, considered them when they were designing the intake and exhaust system. The reason I’m saying “cold air intakes” in quotes is that often these are actually the opposite of what they claim to be. Taking in colder air from outside the engine bay for the engine to use does improve power and efficiency, however if you’re car was made in the 90’s or later, it probably came with a true cold air intake from the factory. If you open the hood and locate your air filter and follow the hose leading away from the engine, you’ll likely see that it actually intakes air from either above the radiator where cool outside air is blowing in, or on some cars it’ll intake air from somewhere near the front wheel well or headlamp. The ironic part is that most of the “cold air intakes” get rid of the very thing they claim to be and simply suck in air from where the factory air filter is located which just sucks in hot air from the engine bay, the extra plumbing they get rid of to improve the air flow is the plumbing that actually makes it a true cold air intake.

As for the claims of power, I’ll try to keep it brief, but it’s a very complex topic. Technically it is true that improved air flow in the exhaust or intake system will improve horsepower (not so much for the intake if you’re going from a true cold air intake to one that’s drawing in hot air from the engine bay), but there’s a large caveat. Engines are often advertised of having horsepower of a single number, which is their *max* horsepower rating. Engines don’t make their max horsepower all the time. Maximum horsepower is usually only made at full throttle and at a particular RPM (revolutions per minute) and on gas engines, that RPM is usually quite high and above what you’ll typically be driving at in day to day use. So for example, a car may have a max RPM of 6,000 and make peak horsepower at 5,200 RPM at full throttle,

however most of the time driving it you'll rarely go over 3,000 RPM. The point being that max horsepower isn't very representative of what your engine will actually be making during day to day driving.

There's also the matter of tuning, which is that at higher RPMs typically larger intakes and exhaust are more efficient since they can allow a greater volume gas to pass through them. However much like with water, if you cover the tip of a garden hose with your thumb, decreasing the diameter of the pipe, the water that does come out is going much faster due to the increase in pressure. This is a bit of an oversimplification, but the same effect is true for engines. At lower RPMs (where you're typically driving) smaller diameter intakes and exhausts *can* be more efficient than a larger one at certain RPMs. And again remember the engineers who designed the system understand this stuff much better than you or I and also took into account that most of the time the car will be driven below 3,000 RPM and not at full throttle.

I'm certainly not qualified to say what the best intake and exhaust system is for any particular car, but the important part is that engines are tuned to be most efficient at a particular RPM range and modifying the intake or exhaust systems without considering all the other tuning of the engine (ECU programming, camshaft profile, etc) is likely to reduce performance during everyday driving although it may marginally improve performance at high RPM and full throttle, hence how they're able to claim that their products give you 5 extra horsepower.

On the topic of modifications for fuel savings another one to be very cautious of is low rolling resistance tires. The idea is that by reducing friction between the road and the tire, the car needs less energy to accelerate and maintain speed. This is fundamentally correct and does work as advertised however the caveat is that friction between the road and tire can also be called something else, which is *grip.* Essentially the friction between the tire and the road is more or less the only force that's allowing your car to stay under control. If another force were

to overwhelm this friction, that tire or tires would begin to skid and you'd lose at least partial control of your vehicle.

I'm not saying you should never get low rolling resistance tires, however I would say to seriously consider if it's worth giving up a considerable amount of grip with the road in exchange for some marginal fuel economy gains. I've had a set of low rolling resistance tires before and personally will never use them again. Even though I drive conservatively, the low rolling resistance tires made the wheels lock up during hard braking much more often than normal tires and even thought the car had ABS, the hard braking of the car was significantly worse due to either ABS kicking in earlier and harder to prevent the wheels from locking or from me not braking as hard to prevent ABS from kicking in in the first place. I wouldn't call low rolling resistance tires exactly dangerous, however I don't believe they're worth the trade off for marginally better economy.

Lastly I'll address tools and more specifically Harbor Freight. If you don't know, Harbor Freight is pretty much the Wal-Mart of the tool world. Specifically in regards to buying more specialty tools that won't be used very often as opposed to more common and basic stuff like socket and ratchet sets which you should absolutely get better quality than Harbor Freight. Most of Harbor Freight's stuff is significantly cheaper than any competitor's, however it's absolutely lower quality. The dilemma is that as a home mechanic you don't really need the robustness and durability of professional grade tools, however you can get burned if you buy something from harbor freight and it winds up not being adequate and you're forced to waste time and maybe money buying a better quality one later.

The two philosophies surrounding Harbor Freight are "Buy once, cry once" which means never get anything from there and get something of better quality initially. The other is any time you need a non common tool, buy it from Harbor Freight first and if that breaks or is inadequate, return it if possible and then buy a better quality one. The idea is that over the long run you'll wind up saving more money on the tools from Harbor Freight that do work and

last a fair bit of time compared to the money and time you waste buying ones that don't work or failed soon after the warranty.

I used to very much be in the latter category, however I've recently more or less shifted to the former of almost never buying things from Harbor Freight. At the very least I'd say never buy any safety equipment from Harbor Freight. For a while I would use floor jacks and jackstands from harbor freight, thinking that jackstands were too simple for them to fuck up and a floor jack failing not being that big of a deal since I never get under cars only supported by a floor jack. However in the past couple of years there quality has seemed to be going down even further. It started with them having to recall a few models of jackstands (one of which I owned)

https://web.archive.org/web/20220323195822/https://images.harborfreight.com/hftweb/recalls/Jack-Stand-Recall-56371_61196_61197.pdf

Although this failure would only cause them to fall to the lowest settings, which would be unlikely to crush you, needless to say it left quite a bad taste in my mouth. The other incredibly poor experience I had with them was purchasing a new floor jack from them when my old one failed. When I took it out of the box brand new, it wouldn't work because some adjustment screw needed to be set first according to the instructions. So I take out an appropriately sized screw driver and try to adjust it per the instructions and the screw head just disintegrated as if it was made of cheese. Thankfully I was able to get a refund on it, but that was the final straw for me. I personally wouldn't go to Harbor Freight or recommend other people to unless it's a tool that's not totally necessary for a job and wouldn't pose a safety risk if the tool failed.

Also on the subject of specialty tools. One option is that franchise parts stores will often have tool loaner programs where you pay a deposit to borrow a tool from them and get the full deposit back when you return it. If the tool you need is available through one of these programs I'd highly encourage taking advantage of it. Additionally if you need an OBD scan and are unable to get the car to the store, they'll often let you borrow an OBD scanner to take with you to the car and scan and come back with to return and get the reading (these are

special scanners that only show the reading when plugged into one of their computers so people can't use it if they just steal it).

Lastly I'd again just like to reiterate on the importance of having an alternative means of transportation besides a car (or at least a second car) so that if you're in a situation you need to go to a junkyard for a part or store for a special tool, you can get there while your car is inoperable.

Sewing

Another skill that I think is severely underrated in current society is sewing, specifically repairing and modifying clothing. It's actually quite easy to do simple repairs and modifications such as sewing closed holes, replacing or adding fasteners as well enlarging or adding pockets in some cases. Basic stuff like this doesn't require very much equipment and can usually be done by hand with a simple and cheap sewing kit. It does take more time than using a sewing machine, but depending on how frequently you do such work may or may not be worth it. There's plenty of material about sewing available online however like many things books are a very good resource as they're easy to use as a reference as well as you can read through them to improve your general knowledge about the topic. I'd recommend just checking out a used bookstore and seeing if they have anything on the topic in the DIY section (good books on gardening, cooking and home repair can also often be found at used bookstores).

Security

Naturally between the current political decisions being made in the US and if the economy continues to deteriorate property and violent crime will likely continue to increase in the near future. Even if you currently feel safe at your current house and city, that feeling may not continue in the feature and I'd highly recommend preparing now rather than waiting for that to change.

Securing the Home

Probably the easiest and most effective thing you can do to secure your house is upgrading the strike plate on your doors which makes it significantly harder to kick in, as normal doors are actually trivially easy for an adult male to kick in. Here's a brief video on how to install these kits.

https://youtu.be/rPrWDsgGtg8

Also in regards to locks, although lock picking criminals are rare, key bumping is an easy and commonly used method of opening typical residential door locks. The easiest way to defeat this is single sided deadbolts that have no key hole on the exterior side which is common for doors to have. The issue with this is that if no one is home, at least one of your doors won't have the single sided deadbolt engaged since presumably you left through a door. One way to fix this would be to install a higher quality lock that's more resistant to unsophisticated attacks (bumping, drilling, etc) on at least the door that you typically leave through so you could engage the deadbolt from the outside, although if you only do this on one door you'll need two different keys for your house.

Also on locks, in America there's essentially no regulation or standards for consumer grade locks, meaning advertisers can essentially say whatever they want about their locks regardless of it's actual capabilities. Europe does have official standards and ratings in this regard but these "euro locks" are shaped and sized differently from common American locks so installation is much more complicated on American doors. However in America commercial grade locks can be a good option and often come with official standards; also a company

called “Schlage” makes locks that are considerably higher quality than most consumer grade residential locks.

Obviously besides the doors, windows are also very vulnerable to being used in break ins, especially those large sliding glass doors some houses have in the back. As for normal windows, obviously bars would be the most secure but you may not want to go that route for obvious reasons. Of course window locks exist, but don’t offer much protection as once the glass is broken, it’s not too much trouble to undo the lock, however they protect against prying the window which is much quieter than breaking glass so installing or upgrading windows locks is still a good idea (this applies to sliding doors as well).

There’s a few “good” options short of bars, for both windows and sliding doors. One is security film that can be applied to glass that more or less limits how much of the glass falls away when it’s shattered. Generally limiting the glass that falls away to the area that was impacted. Obviously this won’t stop a burglar in their tracks, but if someone’s home at the time of the break in, it would certainly buy them a bit of time.

https://youtu.be/hXfxRCvuYog

The other option that can be used in conjunction is glass break alarms. As the name implies these are alarms that go off if they detect glass breaking. There’s two basic types, acoustic that listen for the sound frequency of glass breaking as well as shock sensors that attach to the glass itself and physically detect if the glass is shattered. Obviously the acoustic ones will be more prone to false positives, since most houses have glass besides windows that can break, however the shock sensors can be unsightly and one is required for each piece of glass. Additionally many are intended to integrate into some sort of home security system, although stand alone ones that just sound an alarm or send some sort of notification to your phone do exist. Lastly, if you have a sliding glass rear door, typically these are near the kitchen which is probably the most common place for glass to break. So in that case I’d recommend getting a wireless shock glass break sensor for the sliding door to limit false positives from dropping a plate or bowl in the kitchen.

https://web.archive.org/web/20220222010333/https://www.security.org/home-security-systems/glass-break-sensor/

The last topic I'll mention is a bit dubious as for it's effectiveness, but I figured I may as well mention it as it could be something worth looking into, which is defensive vegetation. The idea is to plant some kind of thorny shrub underneath and around windows to make it more unpleasant to access them or thorny vines on fences to make climbing them more difficult. As well as taller vegetation can be utilized to obscure things from view for privacy.

Non-Firearm Weapons

I'll exclude firearms for now, as I'll have a section dedicated to them, so for now let's just discuss options for those unwilling or unable to procure firearms for self defense; in this case home defense as most of what we'll cover won't be suitable for carrying in public.

The first and likely obvious choice would be some sort of melee weapon. This could range from a breaker bar or tire iron to the classic baseball bat or golf club. Obviously this isn't the ideal format for teaching physical techniques, however I will attempt to address some common misconceptions people have about using melee weapons and give a few pointers.

The first of which is "power". This misconception also applies to punching which mechanically is actually very similar to properly using melee weapons. Many amateurs when they throw a punch will "wind up" to get more power into it. The problem with this is that it telegraphs to the recipient what you're intending to do as well as most people who do this don't properly power the strike with their body and rely mostly on their arm for power which makes the strike very weak to what it could otherwise be. Here's a pretty good video that covers the basics of what I'm talking about, skip to 2:35 for the important part.

https://youtu.be/lL4AcmEIo20

Also here's a perfect example of a "wind up" telegraphing what the attacker was trying to do and backfiring on him massively.

https://www.youtube.com/watch?v=s_7kVn4ejq0

The main thing to remember is that most of the mechanics of punching carry over to striking with a melee weapon. Obviously there is some difference in how your arm and shoulder move. I'd highly recommend learning how to punch properly first, many boxing gyms will allow you to take a few classes without needing to provide your own equipment and maybe even free which should give you a decent foundation on how to throw a punch. And even though YouTube videos and practicing by yourself is far from ideal, you can at least learn how to throw a decent punch that way. Once you've learned that, practice with your melee weapon of choice and try to carry over the fundamentals.

A few other things to be aware of is making sure not to round your shoulders while you swing. The tops of your shoulders should stay flat and at the same height throughout the strike. To try to figure out what I'm talking about, put one hand on the opposite shoulder blade and then with the other arm straight down your side, turn your palm so that it's facing behind you. Now raise your arm 180° so that it's straight up. When your arm is close to straight up, you will feel your shoulder blade "dive" away. This motion is what we want to avoid as well as shoulder shrugging. To get an idea how your shoulder should move during a swing, repeat the same procedure but with the palm of your hand facing in front of you. Do the same thing and you'll notice your range of motion is reduced a bit towards the top, but your shoulder blade stays in place. You can do the same thing while feeling the top of your shoulder to get a feel for how that should be stabilized as well.

The other big mistake new people often make is, particularly when stepping with a strike, is springing up with the strike almost like jumping. Any vertical motion (apart from your shoulder rotating, although that's not really vertical) is a waste of energy and is slowing down your strike considerably. Focus on keeping both your hips and shoulders at the same height as when you started throughout the strike.

Unfortunately this is about as helpful as I can be in text. Additionally note that melee weapons offer you some unique advantages compared to punching which is that you can attack from multiple directions more or less equally. Typically the only punches you can through with your dominant hand is a straight/cross, uppercut, hook and your big overhand/haymaker. However your range with the uppercut and hook are reduced as opposed to the straight/cross. With melee weapons you have a lot more options that don't affect your range as much as it does with punches, such as striking from below or from either side with minimal delay or reduction to range. Also try out switching the direction of your strike halfway to striking from a different direction. Additionally melee weapons can also be used to block attacks more effectively than bare hands and can even be used for grappling and restraining people although of course that is a much more advanced skill.

Something else I'd like to address is when it comes to melee weapons, people often think that the most important characteristic in how effective a melee weapon is it's weight. Although more weight will certainly cause more damage, all else being equal, it's far from the most important aspect of a melee weapon. Essentially the length of the weapon and speed at which it's swung are equally important in determining how much force it has. Speed should be quite obvious, but somewhat less obvious, is that the weapon also acts like a lever. Meaning that the force you apply is multiplied by the length of the weapon. To demonstrate this go to an open door and place your hand somewhere near the hinges and press the door closed. In this example the length between your hand and the hinges is representative of the length of your weapon. After closing the door with your hand close to the hinges, now open it up again and place your hand near the edge of the door away from the hinges and press it closed. Notice how much less effort that took? This is what using a longer weapon does except of course imagine you used just as much force as when your hand was close to the hinges, the door would've closed much faster and with more force. Additionally the longer weapon also gives you the advantage of more range.

Also weapons that are heavier towards the tip will be more unwieldy, but deliver more force with the weight out near the tip, however it slows down your strike as it takes more force to

change the direction of the weight out near the tip so keep this in consideration when selecting a weapon. Conversely weapons weighted towards the handle will feel much lighter than they really are as the weight near the handle takes less force to change directions. Not only should you be aware of how deceptive their weight can be, but the additional speed increases the force they strike with. All else being equal, ideally you want the weight, or center of balance, towards the handle as opposed to the tip.

If you're serious about using some sort of melee weapon for self defense, I'd highly recommend Massad Ayoob's book "Fundamentals of Modern Police Impact Weapons" (ISBN: 0398037485)

https://ipfs.io/ipfs/bafykbzacedtibfwtw5wmqwzdqiwet5um7vjsfuvlqnbjv4ba76fjpacrp7fva?filename=Massad%20F.%20Ayoob%20-%20Fundamentals%20of%20Modern%20Police%20Impact%20Weapons-Police%20Bookshelf%20%281996%29.pdf

Although it's quite an old book and I'm sure the latest and greatest techniques have changed, neither human anatomy or the laws of physics have since it was published.

Lastly, although the word "weapon" may not be the best term to use here, I'd be remiss to not mention pepper spray and pepper ball guns. The way pepper spray works and what it does is pretty straight forward, but it's often overlooked for home defense and seen as something primarily for use outside the home. Something else to consider for home use is larger cans of pepper or bear spray which have more volume as well as could be easier to use since they're larger (as for bear spray versus pepper spray, pepper spray isn't nearly as regulated as bear spray is, so there's pepper sprays on the market that are substantially "more powerful" than bear spray and weaker pepper sprays that are the same or "weaker" than bear spray, do your due diligence on the topic). Something else to consider is that bear spray usually also has a much longer effective range since it's intended for use outdoors.

It's also worth mentioning civilian pepper ball guns such as byrna's

https://byrna.com/collections/non-lethal-self-defense-byrna-sd

(Not endorsing them in particular, just the first one off the top of my head)

These are legal to use in many jurisdictions that prohibit firearm ownership or use for self defense (although of course check your local laws) as well as offer a significant range advantage over typical pepper spray.

Firearms

First and very important for people who are already into concealed carrying. Many states have passed constitutional carry in recent years which means you can conceal carry without a permit or license. However in some states you don't have a lot of the liberties with constitutional carry that you do with a permit or license. For example in Texas signs saying that weapons aren't allowed on the premise aren't legally binding to people who carry with a license, unless it sites the appropriate Texas law (30.06 or 51%) however these signs *are* applicable for people carrying without a permit. Do research on your state's laws to see if it's similar in your state.

Something else before those familiar with firearms skip this section. If you have any intention at all of using firearms for self defense, the book "Deadly Force: Understanding Your Right to Self Defense" (ISBN: 978-1-4402-4061-4) is an absolute must read. It doesn't cover all the legalities of self defense in the United States, however it discusses many important legal concepts that are more or less consistent across the United States. I can't stress enough how important this book is as there's a lot of misunderstandings about what justifies use of lethal force for self defense.

https://ipfs.io/ipfs/bafykbzacebljyle5zbvunh5lnzlysga4uyy7igozp6gwfdlno4cfjo54ih6e4?filename=Massad%20Ayoob%2C%20Jeff%20Weiner%20-%20Deadly%20Force_%20Understanding%20Your%20Right%20to%20Self%20Defense-Gun%20Digest%20Books%20%282014%29.pdf

With those PSAs out of the way, much like alternative transportation, I'd highly recommend getting a concealed carry permit and associated equipment now; even if you don't currently feel a pressing need to. Even in very pro gun states getting your concealed carry license and associated equipment can potentially take a month or two since you'll need to schedule a class as well as purchase a handgun and holster(s). Additionally this will likely take longer if you have no experience with firearms since you'll want to take a beginner course and find a handgun and become proficient with it before getting your concealed carry permit. If you don't have any large gun ranges nearby that offer beginner courses, call the range and ask if there's any shooting coaches or range staff who would be willing to give you one on one instruction if you paid them. I'm sure they'd be more than happy to introduce someone on how to use a firearm correctly and safely.

I'd also like to take a moment to point out why I'm recommending getting a weapon for concealed carry first. The reason should be fairly obvious, concealed carry lets you carry outside the home and the gun doesn't turn into a pumpkin whenever you return home. Weapons for concealed carry are very compromised in order to be small enough to be concealed, but they're still a whole lot better than a stick for home defense.

Additionally on the subject of technical specifications. Don't get too wrapped up in caliber and capacity wars. The internet is full of gun enthusiasts austistically arguing all the minute pros and cons of different firearms. At the end of the day all handguns are going to perform very similarly to each other when compared to a stick. The important thing is that you find a weapon that fits your budget, your body and one you're comfortable shooting. Many gun ranges will allow you to rent handguns so you can actually fire them on the range before deciding which one to purchase. One piece of advice I'll give is that if you're a new shooter, don't judge guns you're renting too much based on accuracy. Look mostly for size and ergonomics (how comfortable it is to shoot). Handguns are much more difficult to shoot accurately than a rifle and so as a beginner you're probably going to suck pretty bad with everything. The point being, if you rent two handguns and handgun A was more comfortable to shoot and a good size for concealability, but you were more accurate with handgun B, but

didn't like it as much. Get handgun A; since your accuracy will increase a lot as you become more competent shooting handguns in general.

Also, if you want to hear from somebody besides me about how gun enthusiasts often make mountains of of molehills concerning handgun capability, here's some stuff for ya and I'd highly recommend watching/reading the below content regardless.

https://www.youtube.com/watch?v=Cv6PxB2TqLM

https://odysee.com/@paul_Harrell:a/gun-fight-statistics.:b

https://www.youtube.com/watch?v=MiT8MxPJVmo

https://web.archive.org/web/20220509100332/https://www.buckeyefirearms.org/alternate-look-handgun-stopping-power

At the end of the day, just remember the maxim *"The .380 in your pocket is better than the .45 you left at home"*

Another important topic that I want to bring up is training. As already mentioned handguns are much more difficult to use effectively than rifles due to having only one point of contact with the weapon as opposed to three with a rifle or shotgun. There's no replacement for going to the range and shooting live ammo however range training can be prohibitive due to time, money for ammo as well as safety restrictions. Most ranges won't allow you to practice drawing from your holster and firing, firing from cover, etc. This is where supplemental dry fire practice comes in.

Dry firing is "firing" an unloaded weapon or one loaded with dummy ammunition. The vast majority of modern firearms are safe to dry fire (except for rimfire such as .22lr), however to be safe you can use dummy ammunition "snap caps" to ensure that the firing pin or other parts won't be damaged from repeated dry firing.

It should go without saying, be 100% sure that the firearm is not loaded with live ammunition before dry fire practice.

The reason dry fire practice is so important is that it allows us to work on many aspects of handgun usage without spending time or money going to the range. Dry firing may seem silly and of little value, but on the contrary it can actually be incredibly valuable. Probably the biggest factor concerning accuracy with handguns is ability to hold the handgun stable as well as to have a smooth trigger pull so that the gun doesn't move too much while we're pulling the trigger. Both of these skills can be improved through dry fire practice. Simply aim the unloaded firearm at a target and pull the trigger as if you were firing for real and keep the sights on target during and after the trigger squeeze. It's not a perfect method of practice, since another large issue with accuracy is "anticipating the recoil" which will throw off your shot and can't really be practiced with dry fire as there's no recoil. Again, there's no substitute for live firing, but dry firing can get us a lot of *additional* repetition we can't get on the range.

As mentioned earlier, dry fire also lets us practice skills that most ranges won't allow you to practice which is drawing and firing from the holster and maybe even while moving. Another good skill to practice would be drawing from the holster towards a target that is not directly in front of you. Often when people practice their draw they do so standing still with a target directly in front of them. This is fine for working on the fundamentals as well as it is quite likely a threat will be directly in front of you, however still consider practicing scenarios where a target is off to the side or you're moving for one reason or another (a good argument can be made for side stepping when you draw to help avoid an attacker. Good luck finding a range that will let you practice that with live ammo.)

Another consideration for defensive use of firearms is hearing protection. In a concealed carry scenario you almost certainly won't have time to put on hearing protection, so don't bother. However for home defense, I'd highly recommend having hearing protection close by to your weapon and putting it on if time permits (although if it doesn't just skip it). Handguns, even

indoors, aren't too bad compared to long guns; however if you do plan on using a shotgun or rifle for home defense, especially an AR-15, I'd recommend having hearing protection near or on your rifle. Additional emphasis on AR-15s because they are exceptionally unpleasant to fire without hearing protection and I've only had the unfortunate experience of doing that outside. I'd rather not find out what it's like to fire one indoors without hearing protection.

As for hearing protection, in my experience the Christmas tree type ear plugs offer an excellent balance between not interfering with your hearing ability while still offering a great deal of hearing protection, although I'm sure they offer less protection than basic over ear sets. That said the plugs take longer to put on than over ear protection so if I was to use an AR-15 for home defense, I'd keep a set of over ear protection next to the rifle and have a case with Christmas tree plugs attached to the front sling mount or something. I'd use the over ear protection in a home evasion type scenario as they offer better protection and are faster to put on and use the plugs in a situation were I'm preparing for a threat that's not imminent and having hearing in between now and then is more important. Additionally by having the plugs attached to the rifle, if I forget to put them in right away they're with me without having to go back and fetch them.

It might seem a bit silly to put so much effort into hearing protection for defensive use, why worry about it and just except the fairly minor (all things considered) hearing loss? It's not so much about the permanent hearing loss as it is the temporary hearing loss. Having temporary hearing lose could lead you to not hear a sign of another attacker you weren't aware of, someone calling for assistance or a law enforcement officer issuing you verbal commands who may not consider you're suffering temporary hearing loss and you're holding a gun and being non compliant.

I won't dwell too much on technical aspects of firearms as there's already a plethora of material out there; however there is one topic I'd like to mention as I feel the current gun community doesn't give this argument the merit it deserves. I'm not saying you should absolutely do this or it's objectively better than the alternatives, just that it's a better argument than is typically given credit for. That argument is that you should carry a double action or double action/single action pistol for concealed carry.

To quickly go over what double and single action means. A double action means that pulling the trigger does two things, first it cocks the hammer to prepare for firing (and in a revolver rotates the cylinder) and at the end of the pull releases the hammer causing the weapon to fire. In a single action (and most striker action pistols, which for the purpose of this discussion we'll include with single action) the hammer is cocked by racking the slide which will cock the hammer. This is done when initially loading the weapon which means the hammer will be cocked and ready when the gun is loaded and when the gun is fired this whole process repeats so that when the new round is loaded, the hammer is again cocked.

The disadvantage of double action is that because the trigger is both cocking the hammer and releasing it, double action triggers have a much longer and heavier pull as they're having to work against the hammer's spring. As mentioned earlier the biggest factor in handgun accuracy is holding the gun stable and squeezing the trigger smoothly, a double action trigger makes this significantly more difficult to do and thus they are considerably harder to be

accurate with, particularly for beginners who aren't experienced with handguns. Whereas single action triggers only release the hammer, making the trigger pull much lighter and shorter and thus easier to shoot accurately.

This might make it seem that single action is the clear choice given that it's much easier to shoot accurately, however consider the following. When it comes to carrying a handgun, the general consensus is that because a proper holster will prevent the weapon from firing while it's holstered and that if the situation arises that you need to draw and fire the weapon, it's best to have that weapon as close to being ready to fire as possible to prevent the weapon from not firing when desired because either a safety was not disengaged in the heat of the moment or a round needing to be loaded into the chamber. Because of this the most common recommendation you'll find on the Internet is to carry a single action pistol, with a round in the chamber, without a safety (many weapons intended for concealed carry don't even come with a safety unless required in a jurisdiction).

However the crowd in favor of double action argues that this is a bit too dangerous as when drawing from concealment or holstering, the smallest force on the trigger could fire the weapon when you don't intend for it to be fired. The argument is that the additional length and force required for a double action trigger gives you a larger margin of error both when drawing and holstering and doesn't reduce the speed or complicate the process of firing the weapon after drawing like a safety does.

Criticism of this theory typically follows the logic that safely drawing or holstering a pistol is purely a matter of training and that if you're concerned about or have a negligent discharge while drawing or holstering a single action pistol, it's 100% your fault for not being trained well enough. As well as the point about double actions being more difficult to shoot accurately is also part of the argument.

My personal thoughts on the matter is that I find it quite ironic that drawing and holstering the weapon is seen as something that can be perfected through practice whereas the double action trigger pull itself isn't. I should clarify that myself and most people who advocate for using double action pistols don't argue that the double action is a replacement for proper training and technique in regards to drawing and holstering, however it gives an extra safety margin should something go wrong in the process. My opinion is that drawing and holstering a concealed weapon has many more variables to it that can affect the outcome as opposed to the accuracy of shooting double action pistols. You can practice and improve the double action trigger pull through dry firing and practice at the range. The only main difference between pulling the trigger then and in a defensive situation is your physiological state from the stress of being in a defensive situation, however this is a bit of a moot point as it applies equally when drawing or holstering the weapon in a defensive situation as well. Compare to drawing or holstering a concealed weapon which has many more variables to it. For example, each time your gun will be located in a slightly different spot, from the way you put your holster on in the morning, to what activities you've done throughout the day and according to different clothes you'll wear throughout the day. Plus depending on your manner of dress, you may not even be carrying in the same location or even the same gun all of the time. As well as the fact different clothes will have slightly different procedures for drawing, such as wearing a jacket as opposed to just a t-shirt as opposed to a button up shirt and a t-shirt, etc. All of these variables change things up a little bit and make it that much more likely for things to go wrong when drawing or holstering, which again, as compared to a trigger pull where there will be comparatively little difference when doing so in training versus in a defensive scenario.

My final opinion is that it's better to carry a double action pistol and frequently practice the trigger pull, both with dry fire and live range practice, however it's still necessary to practice and execute safe drawing and holstering technique. However this is just my opinion, do your due diligence in regards to the topic as ultimately you'll need to decide for yourself.

A bit of housekeeping in regards to topics I glossed over. For simplification I included striker actions as single actions. Striker actions work is that the action of the slide only partially cocks

the “hammer” (striker actions technically don’t have a hammer, the firing pin works similarly to a pen you write with) and the trigger pull cocks the “hammer” the rest of the way and then releases it. This may sound more similar to a double than single action, however most striker actions cock the “hammer” most of the way with the slide action, meaning very little force is required to cock it the rest of the way before firing. In reality striker actions behave very much like single actions in that they normally have a very light and short trigger, hence their popularity because they’re easier to shoot accurately than a double action. It’s worth noting that some manufactures such as Kahr Arms advertise their striker actions pistols as “double action” because they’re designed for the slide action to not cock the “hammer” as much as most striker actions do, making the trigger pull longer than most other striker action pistols. I’ve never handled one so I can’t say much more about them.

Also, earlier I mentioned double action/single action pistols. These pistols are the “best of both worlds” in a way. There’s a few variations in how they work, but typically they operate like a single action pistol, but come with a de-cocker (often part of the safety if equipped). When the weapon is loaded the hammer is fully cocked by racking the slide, then the de-cocker is used to safely drop the hammer without firing the round in the chamber. This essentially turns the pistol into a double action, since the hammer is de-cocked it much be cocked again by the trigger before firing. When it is fired, the action of the slide cocks the hammer fully and any subsequent trigger pulls will be single action; so long as the de-cocker isn’t used. It’s also worth mentioning that much of the time when people say “double action” they’re actually referring to double action/single action as they’re much more common than DAO (Double Action Only) which are fairly uncommon. Additionally most revolvers are similar in except they’re double action but the hammer can be manually cocked making the trigger single action. However firing the weapon doesn’t do anything to cock the hammer or rotate the cylinder so the next shot will always be double action again without manually cocking the hammer.

Lastly, I’d just like to mention that it’s always a good idea to carry pepper spray with you regardless of whether you carry a firearm or not. Statistically you’re 3 times more likely to be

the victim of simple assault as opposed to aggravated assault and in many such cases, you won't be authorized to use a firearm in self defense. Additionally pepper spray is a much more "covert" way of resolving a situation as it's much less likely the police, and more importantly media, will get involved in a negative way than if some sort of weapon or physical violence is used.

Spouses and Other Family Members

This section will be quite brief due to the nature of it, it's highly personal and so I can't give too much advice on it without knowing you and who lives in your house. Additionally I will not be covering securing weapons from those in the household who should not have access to them as I don't have much to say on it besides get a quick safe and/or conceal carry at home.

The question to ask yourself is, what is/should be available to other members of my household should they need to defend themselves and I'm not there? Most likely there's periods of time where you're not at home, but loved ones are. The issue is that if your choice of home defense weapon is a .357 magnum or 12 GA pump action shotgun, your spouse or other adult members of the household may not be adequately trained or trained at all on using such weapons effectively or even safely. It's quite common for one spouse to not share the enthusiasm for firearms and defense as another and especially considering the difficulty of operating a pistol as opposed to a long gun, even if a spouse is familiar with rifles and can safely and effectively use them, they may not be as qualified with handguns. Additionally they may not practice, either dry fire or actual range practice, as often as you or may not even want to learn to how to use firearms.

If you find yourself in a situation were for whatever reason a firearm isn't an option at all. In this scenario consider various other weapons or tools that could be left around the house that could be utilized if the occasion arose. Think a sturdy pot or pan left out on the stove or a baseball bat or crowbar tucked away somewhere. And of course pepper or bear spray is something to consider as well.

On the subject of weapons for people besides yourself, if you're concerned about a more serious issue than typical crime, you might want to consider having extras for people in your party. Next time PSA has a sale on ARs or something else, consider picking up a *few* :)

Misc Resources

S2 Underground

(even if you're not preparing to wage an insurgency, very interesting stuff is covered)

https://odysee.com/@S2Underground:7

The Privacy, Security and OSINT Show

Michael Bazzell (Best resource for computer and general privacy)

https://inteltechniques.com/podcast.html

Massad Ayoob

I consider his book "Deadly Force" mandatory reading for anyone who owns firearms.

https://ipfs.io/ipfs/bafykbzacebljyle5zbvunh5lnzlysga4uyy7igozp6gwfdlno4cfjo54ih6e4?filename=Massad%20Ayoob%2C%20Jeff%20Weiner%20-%20Deadly%20Force_%20Understanding%20Your%20Right%20to%20Self%20Defense-Gun%20Digest%20Books%20%282014%29.pdf

---

Dr. Jason Fung

Wrote an excellent book on diet, would recommend whether you're overweight or not.

https://ipfs.io/ipfs/bafykbzacedxzgpdc7naqzpillno7uokfzki3isplvlcs7ykdfypm5ic3rt6js?filename=Fung%2C%20Jason%20-%20The%20obesity%20code_%20unlocking%20the%20secrets%20of%20weight%20loss-Greystone%20Books%20%282016%29.pdf

---

Anonymous

"A World Turned Upside Down" Document about a Strelo/k/s observations and thoughts on the current state of the world.

https://odysee.com/@runick:1/A_World_Turned_Upside_Down:3?&sunset=lbrytv

APPENDIX

Command Line Interface

This section will cover installing and using command line programs in Windows. The basic commands you'll need to know are

cd – Change directory, followed by the path of the folder you'd like to move to

dir – List the contents of the current directory, or you can give it a path to another directory to list the contents of

Another important thing to know about the command line is relative and absolute paths. A path to a file is essentially the series of folders that a file or folder is in. So for example, the path to your home folder on Windows is

`C:\Users\<user-name>`

The letter followed by the colon is the drive letter, C will always be the system drive. If in File Explorer you click on the C drive to go to the root of it (root is the highest folder on the drive) you'll see many folders, one of which will be named "Users" and within that folder, should be one with your username. From there is where your Downloads, Music, Video, etc folders are located as well as any files saved there.

The path listed above for your home folder is an absolute path. An absolute path is one that goes all the way from the drive root (or letter) to the folder or file itself. A relative path is one that is added to the end of your current location to create the full path to the file or folder. So for example, when you open a command prompt you'll be in your home directory (listed above) from there you can reference another folder or file with a relative path. Since the Downloads folder is in the home folder, the relative path to the Downloads folder would simply be "Downloads" or ".\Downloads" (A "." specifies the current directory and is unnecessary to use) and any folder or files within Downloads can be referenced similarly such as "Downloads\video.mp4" "Downloads\ffmpeg\bin\ffmpeg.exe" etc. Similarly to how "." references the current directory ".." references the directory above and can be used with the cd command to go up/back a directory as well as can be used as apart of paths, even multiple times. So if you're in the directory

```
C:\Users\<user-name>\Downloads\foo
```

You can change directory to your home folder's Videos directory with the following relative path.

```
cd ..\..\Videos
```

The first ".." means to go back to the Downloads directory and the second means to go back up again to the home directory and then Videos specifies to go into the Videos directory from there. Additionally we could use the following absolute path to get to the Videos directory no matter where we are on the command line including on another drive

```
cd C:\Users\<user-name>\Videos
```

From this point we're ready to call programs from the command line, in fact we've already covered it as the commands "cd" and "dir" fundamentally work like any other command line program. You type them out and then give them a folder or file path as an argument (an argument is essentially a value given to a command line program, for our purposes we'll only be discussing ones that take one or more file paths as arguments.) As well as any options which are specified with either a "/" followed by a letter or string or one or two hyphens followed by a letter or string. Options basically modify the behavior of the program to do different things. Windows programs such as "dir" "del" (deletes files) and "rmdir" (Remove directory: deletes folders) have options that use a "/" followed by a letter and to list the options available for a Windows program, type the program name followed by "/?" which will show the help information for that program. Note that for programs made primarily for Linux/Unix you would use "-h" or "--help" instead of "/?" even if they're running on Windows. Many of the programs we'll be installing such as wget, yt-dlp and exiftool will use this method.

Path Variable

The programs listed above cd, dir, del, rmdir, etc are preinstalled and already in the system's PATH variable. The PATH variable isn't to be confused with a file or folder path. The commands listed above are essentially just .exe files somewhere on our computer and when we type "dir Videos" on the command line, the computer finds the location of the file "dir.exe"

and then runs it with the argument ".\Videos" to list the contents of the Videos directory. It's able to find dir.exe when you type dir on the command line is through the PATH variable. The path variable is essentially a list of the paths of different folders that contain executable files you would like to be able to call from the command line regardless of which folder you're currently in. If it wasn't for the PATH variable, every time we wanted to use a program from the command line we'd have to specify the path to the executable file itself, such as

```
C:\Program Files\foo\dir.exe
```

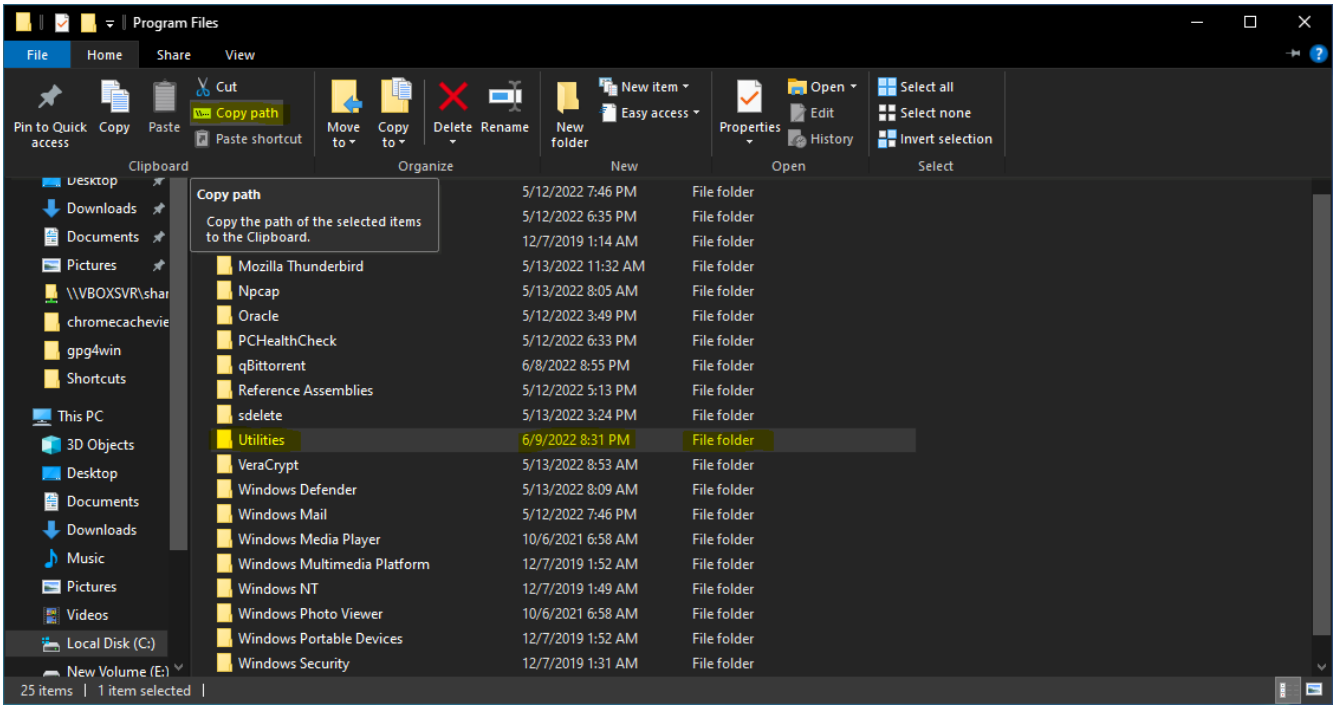
to use the program dir (I don't know where it's actually located I just made that up). The point of this is that when we download a new program we'll need to put it somewhere that's in the system's PATH variable of folders it will check whenever we type the name of it on the command line.

The easiest way of handling this is to create a new folder called "Utilities" within the "C:\Program Files\" folder and adding the folder

```
C:\Program Files\Utilities"
```

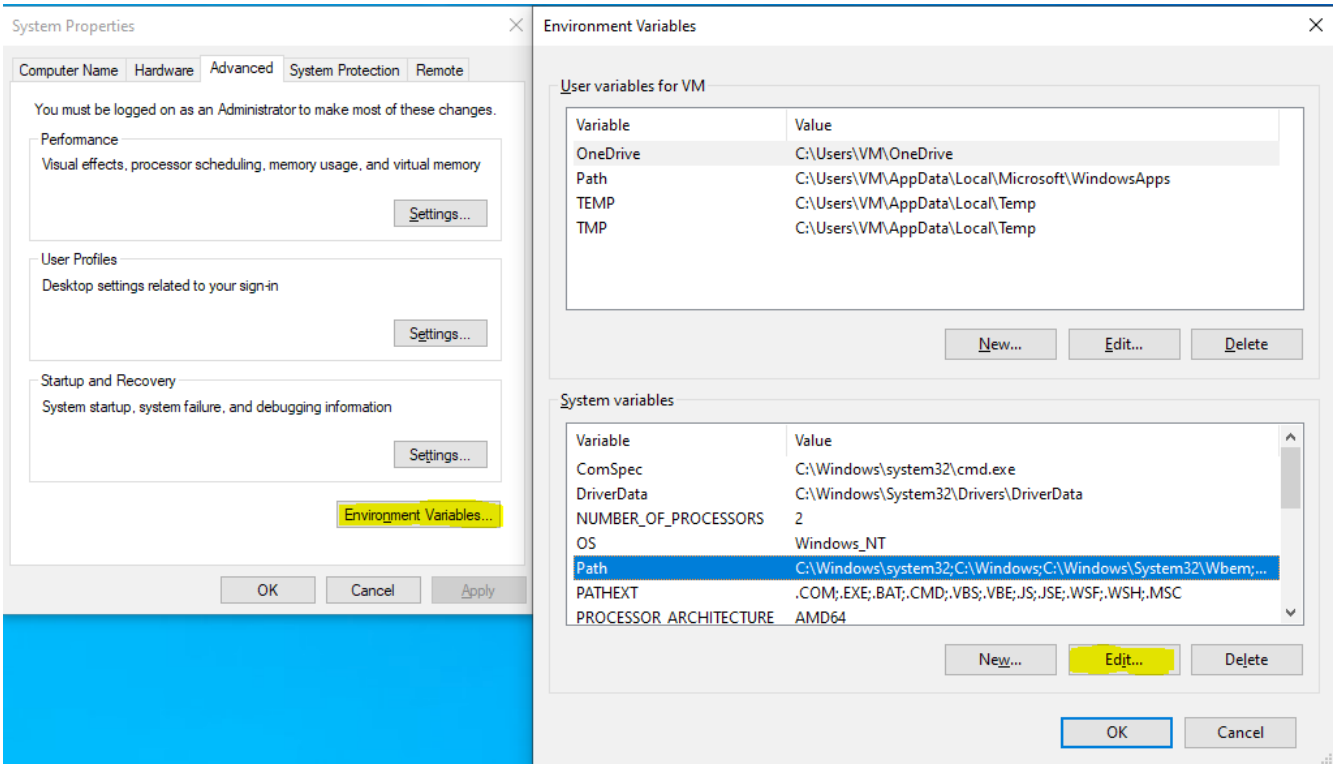
to the PATH variable and then any exe files we download later, we just dump in this Utilities folder and then they'll be part of the PATH variable.

After we've created the Utilities folder inside of "C:\Program Files" in file explorer, click on the "Home" tab in the top left and from the subsequent menu chose "copy path" highlighted in the screenshot below.

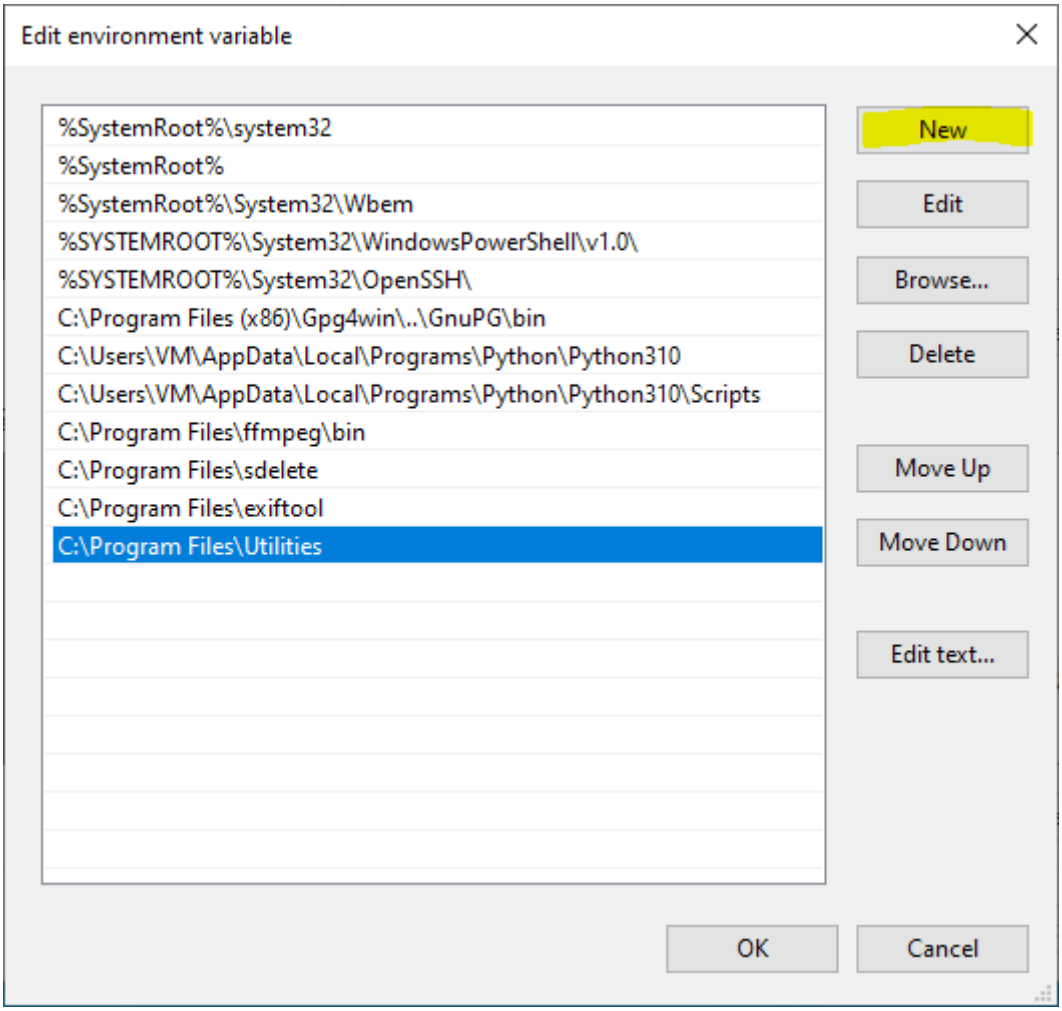


This will copy the path “C:\Program Files\Utilities” to our clipboard which just reduces the chance of making a typo when we add it to our PATH variable.

Afterwards, in the Windows search bar type, “System Variables” and an option along the lines of “Edit System Environment Variables” should appear, choose that and the box on the left should appear, click on “Environment Variables” to make the box on the right appear. From here click on “Path” in the lower window and then the “Edit” button beneath it.

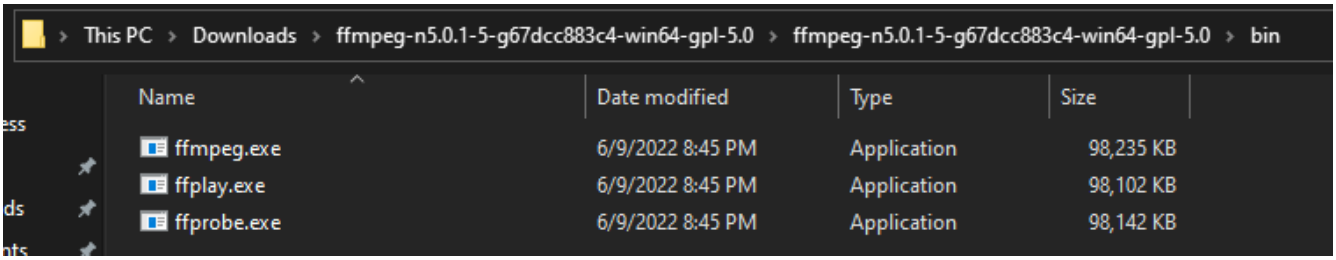


After clicking “Edit” you should see something like this pop up



In this case I took the screenshot after having added the “Utilities” folder, so it won’t already be there when you do it, but simply click the “New” button and just paste in the path to the “Utilities” folder and hit enter. From there just click “OK” or “Apply” until you’re back out of it.

Now that the “Utilities” folder is in the PATH, any .exe files you download in the future just need to be added to it and they can be called from any place on the command line. Just note that when you download some programs, such as ffmpeg, they’ll be within a subfolder when you download them. As you can see below, when I extract the zip file for ffmpeg in my Downloads folder, it’s within a couple of folders from where I extracted it.



In this case if I were to just move the folder “ffmpeg-nXXXX” into the “Utilities” folder, it wouldn’t work. As only the “Utilities” folder is in the PATH, none of it’s subfolders will be searched, so I’ll need to move the actual ffmpeg.exe file directly into “Utilities”. (You’ll also want to go ahead and do the same with ffplay and ffprobe even if you don’t think you’ll need them)

Privacy Drama

Given that I mentioned privacy services such as private e-mail and VPNs, I think it's somewhat unavoidable that I address some of the drama around these various services. If you've spent any time around the "privacy community" you've probably seen this yourself. Almost any privacy oriented service is going to receive quite a bit of criticism, some valid and certainly some that's not. In this section I'll try to explain the limits of what we can expect from privacy services.

Law Enforcement

In the introduction of this document I said that this guide is in no way intended to provide any serious protection against law enforcement or intelligence agencies. This mindset should also be extended to *any* privacy oriented service in that they will either be unwilling or unable to protect you from government actors, whether they pursue actions through legal means or through illegal methods as was documented by the Snowden leaks. A handful of examples are Tutanota being required to log IP and e-mails of specific users requested by the German police, Protonmail complying with French authorities to log a user's IP address (the exact legal order they complied with came from a Swiss court, more on that later), Hong Kong based PureVPN has cooperated with the FBI and RiseUp also complied with US law enforcement.

(Tutanota) https://web.archive.org/web/20220604222158/https://techcrunch.com/2020/12/08/german-secure-email-provider-tutanota-forced-to-monitor-an-account-after-regional-court-ruling/

(Protonmail: best article of the 4) https://web.archive.org/web/20220604221859/https://restoreprivacy.com/protonmail-logs-users/

(PureVPN) https://web.archive.org/web/20220503182125/https://torrentfreak.com/purevpn-logs-helped-fbi-net-alleged-cyberstalker-171009/

(RiseUp) https://web.archive.org/web/20220224190153/https://riseup.net/en/about-us/press/canary-statement

The point is that businesses are legal entities and will ultimately be forced to either comply with their governments requests or shut down the way lavabit did for Snowden.

https://web.archive.org/web/20220407054333/https://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden

It may seem like using a service that's not based in your country or one that's closely aligned with your country may be a really good idea, and although it probably does make it marginally more difficult for law enforcement to get to, it's by no means a guarantee as can be seen by Swiss courts issuing court orders on behalf of the French and Hong Kong VPNs cooperating with US law enforcement.

Now to be fair to VPN providers, many have complied with court orders simply by showing that they had no data at all to hand over. Typically these are the gold standard of a VPN service since it shows they truly aren't keeping any data about their users, however it's still not a guarantee that things will continue to be that way into the future. Again if you are doing illegal activity online, Tor is your best bet.

Advertising

One thing to be weary of when regards to VPNs is that they've become a hot business the past few years and many have formed corporate relationships with media companies or been bought out by foreign companies (such as ExpressVPN and PIA being bought by an Israeli company with a sketchy history)

https://web.archive.org/web/20220605033637/https://restoreprivacy.com/kape-technologies-owns-expressvpn-cyberghost-pia-zenmate-vpn-review-sites/

Additionally the relationships between media and VPN providers is something to be concerned about. Windscribe VPN put together a nice little graphic that illustrates at least some of the know business relationships that VPN companies have with other corporations including media. Certainly something to take into consideration at least when reading "reviews"

https://embed.kumu.io/9ced55e897e74fd807be51990b26b415#vpn-company-relationships

Additionally I'd also recommend giving the article it was posted in a read.

https://web.archive.org/web/20220511062152/https://blog.windscribe.com/the-vpn-relationship-map/

If all this is a bit overwhelming for you and you just need to pick one that's not horrible, again my recommendation would be Mullvad although I make no claim I've thoroughly evaluated all of their competitors, just that all things considered, they're pretty good in many aspects.

Honeypots

One accusation that you may hear levied is that such and such a service is that it's a honeypot. A honeypot is essentially a fake organization, plot or service that's run by law enforcement or intelligence agents to entice someone to become involved in criminal activity. Think undercover cops trying to buy drugs or those people who would pose as young girls online to try to catch pedophiles. A real life example of a technical honeypot would be the Anom phone project that was targeted at organized crime.

https://web.archive.org/web/20220605161650/https://en.wikipedia.org/wiki/ANOM

One service that fairly often gets accused of being a honeypot is protonmail. Personally I find most of these technical arguments unconvincing, although if you have doubts about the companies and organizations proton is connected to, that's more of a political concern than a technical issue. I won't go through all the various accusations, since someone's already done that more concisely than me.

https://web.archive.org/web/20210727224547/https://serpentsec.1337.cx/i-was-asked-to-review-an-article-from

The main point I'd like to make about honeypots is that at least US law enforcement agencies have a long history of utilizing undercover agents and informants to infiltrate and disrupt various movements they want to curtail. The point being is that if there was a group or type of people that law enforcement wanted to spy on, particularly one that communicates over the Internet, it'd be much easier for them to simply get an informant or agent to participate in the group nullifying any technical defenses of the service rather than building an attractive service with a backdoor they can use to read messages. Additionally something I find ironic with a lot of the sillier accusations of services being honeypots (such as protonmail using eml format for e-mails, which is one of only a handful of formats anyone can use) is that bad jacketing is an often used tactic by feds to disrupt organizations. Bad jacketing is agents or informants accusing legitimate member of organizations of being informants or agents to destroy trust in them. I'm not accusing any of the people who criticize protonmail of doing this, but I think a lot of honeypot accusations are closer to being bad jacketing than valid criticism.

Ultimately I think a lot of this type of criticism originates from elitism. E-celebs need to look like they're more informed than the average person in regards to privacy and one way of doing that is talking about how some popular service is actually a honeypot. Something else that needs to be taken into account, not just in regards to privacy, but any type of e-celeb. I think it's a common problem for e-celebs to run out of material they're knowledgeable on and interesting stuff to talk about and they wind up reaching and reaching further for material to talk about contributing to the problem mentioned earlier of having to come up with novelty takes to stay interesting. I think a very good example of this is a YouTuber "The Hated One's" video claiming that phones are more secure than desktops.

https://www.youtube.com/watch?v=Wd4Pa03LvLk

I won't bother going through the video and why it's ridiculous, just remember that ultimately phones are the least secure due to the ease of which they can be lost and stolen and the attacker having physical access to the device is pretty much game over for security, if he's

able to login pretty much no security feature can stop him at that point. Additionally just due to the nature of touchscreens versus keyboards, most people aren't going to have nearly as a secure password/PIN on their phone as they will a computer. Lastly most of the points he makes in regards to security features are total non sequesters, at least compared to Linux. Linux repositories are signed and essentially offer all security benefits of an app store with none of the privacy concerns of using Google's app store. Additionally permissions can be set on apps using AppArmor although it's not really even necessary since the vast majority of software for Linux is open source as opposed to mobile apps.

A video that summarizes what I'm trying to get at, likely more coherently and concisely, is this one

https://odysee.com/@techlore:3/everything-you%27ve-heard-about-privacy-is:e?r=Aa2n89YPtkFsvWCo3uCtM3cee9LAQj1Z

One point raised is that clickbait is absolutely an issue in the privacy and security community. Particularly for security, I can't tell you how often there's articles written about some devastating attack and then when you read into the actual attack it requires having physical access to the device and messing with the BIOS/UEFI, a much more sophisticated attack than the typical person needs to worry about. This is the case most of the time when you hear about some vulnerability for an Intel or AMD CPU.

Linux

I'm a huge advocate for switching over to Linux from Windows or Mac for your personal computer not only for privacy, but also it simply works better and has fewer issues than Windows at this point. The main privacy advantages of Linux is that at the very least you can completely opt out of telemetry as well as there's many distros where telemetry is disabled by default, as well as the telemetry that Linux uses is much less invasive than Windows or Mac. Additionally the vast majority of Linux distros are FOSS (Free and Open Source) meaning anyone's allowed to view the code and propose changes as well as fork it, meaning copy it and make their own modifications and release and distribute their version. This greatly improves code quality as well as disincentives putting spyware or other unwanted stuff in projects as it's easy for someone to simply fork the project and remove the questionable code. Granted software being FOSS isn't a *guarantee* that software is 100% private or secure, but it is generally much better in those regards than proprietary software. Besides the distros themselves, much of the software developed for Linux is also FOSS as well.

As for security, realistically the main benefit is that with Linux you typically install software via a repository. These repositories are maintained and signed by the team that maintains the Linux distro. The benefit of a repository over installing programs the way it's done in Windows, is that you get most of the security benefits of using an appstore without the privacy concerns since you're not logged into some account.

The other security benefit of this model is that it's much easier to update all the software on your system instead of each piece of software needing to have updates done individually. When ever you update your Linux computer, your package manager will check for newer versions of all the software that's installed through your package manager and update them as well if updates are available, although you can choose to "hold" certain packages meaning they won't be updated. Additionally Linux updates rarely require a restart and you can continue to use your computer normally while the update runs, some updates to things like the kernel will require a restart to go into effect, however you can continue using your

computer normally with the older version without issue, some distros will prompt you to restart but you can dismiss it if you like.

As for functionality, this is anecdotal, but at least in my experience I've run into way fewer issues using mainstream Linux distros than I do when using Windows. Also there's a misconception that Linux *requires* using the terminal to do basic things. On most mainstream distros you can very well do everything you need to without ever needing to open a command prompt if you don't want to, however many Linux users do use the command line at least occasionally because it does have advantages over doing things graphically sometimes. Particularly when giving advice as it's easier to give people exact commands to run than it is to guide them through exactly what to click through graphical menus (although you should always research commands found online to troubleshoot or fix issues, you don't need to be an expert to figure out using the man pages if a particular command is a troll trying to get you to do something bad and it's also a great learning opportunity).

The main drawback to Linux is it's support for a lot of proprietary software. There's often FOSS alternatives on Linux, however sometimes these alternatives lack compatibility or the capabilities of the proprietary programs they're trying to replace. Adobe Photoshop and other creative products are ones that are often sited. There are FOSS alternatives such as GIMP and Krita however many people report they lack features necessary for professional use, however in my experience they're perfectly adequate for the casual home user who occasionally makes memes or does amateur photography. Another common FOSS alternative is the Libre and Open Office Suites. These are alternatives to the common Microsoft Office suite (Word, Excel, Powerpoint, etc). They vary in capability for each one, personally I find Libre Calc (the Excel equivalent) to be as good or better than Excel itself, however at the very least it's more than adequate for making budgets and typical home use, additionally there's also gnumeric to try out if you don't like Libre Calc. As for Word I will admit Libre Office Writer is a bit lacking compared to Word, however it's still a very capable text processor and find it more than adequate for home use. For example this very document was created in Libre Office Writer so make of that what you will.

Additionally because software for Linux is usually FOSS, it means it's likely available for Windows as well, so if you're concerned about a program being adequate for your use, you can try it out on Windows before switching to learn it and see if it's suitable for you. Additionally if there's some software that you can't find a suitable replacement for on Linux dual booting is a great option for that. Often dual booting is the preferred solution, the best way to go about it is to simply have two hard drives installed on the computer and whenever you boot the computer, grub will ask you which operating system you'd like to boot into. This is great because if Linux if fine for personal use, but you need a Windows machine for work or playing video games, you can continue to use Windows for those purposes while having your personal use on Linux, totally separated from Windows.

Of course this is more difficult on a laptop as you'll likely only have one hard drive available to use. You can dual boot from a single hard drive however you can run into issues with Windows seeing the Linux partition (and thinking it's just unused space) and messing with it and ultimately breaking your Linux install. My understanding you can configure a single hard drive to dual boot in a way that eliminates this issue, however it's something to be aware of should you go this route.

The other option for laptops (and you could do this on desktops as well) is to install Linux and run a Windows virtual machine to do the tasks you need Windows for. For such a configuration you'd likely want to configure a shared folder between the virtual machine and the real machine, which isn't difficult and I won't go into it here. As well as install VMware tools or VirtualBox guest additions respectively, which are software you install on the virtual machine and help do things like size the window appropriately, as by default the virtual machine will only run in quite a small window, these tools help it communicate better with the display drivers so that the virtual machine can run at the full resolution without being stretched.

Virtual machines can also be utilized for evaluating Linux to see if you'd want to switch to it. I won't go over the details of setting up a virtual machine as that's covered plenty of places on the Internet already. As mentioned above I'd recommend configuring a shared folder between the guest and host operating systems as well installing VMware tools or VirtualBox guest additions to that you can use the virtual machine at full resolution.

Distros and Desktop Environments

Another key difference between Linux versus Windows and Mac is the option of desktop environments (the graphical environment you're loaded into when your computer boots). On Linux you can quite easily switch out the desktop environment any time after you've installed Linux and often have many choices of which desktop environment to initially install any Linux distro with. Although many distros will only have a couple of officially supported desktop environments, often versions made by the community will be made that come with a different desktop environment, essentially the official version with the change in desktop environment done properly, it is possible for some things to not work correctly when changing desktop environments and generally it's better to install Linux with the desktop environment you want initially. You can of course use a virtual machine to test out different desktop environments before installing Linux for real on hardware. Another neat feature this allows is on Linux you can have multiple desktop environments installed at the same time and when you log in, you just chose the desktop environment you'd like to use. This is nice not just if you want to play around with another desktop environment, but also can be functional on laptops. You could wind up preferring one desktop environment when using a laptop connected to a monitor, mouse and keyboard and another when using the laptop by itself.

As for distros of Linux, there's a plethora, but the main ones you'll hear about and likely be recommended the most (including their derivatives) is Debian/Ubuntu, Fedora and Arch. My personal opinion is that as a beginner just ignore Arch (and especially it's derivative Manjaro). The deal with Arch is that it's a very bleeding edge distro meaning it gets the latest updates before anything else. The problem is pretty minor but this can cause issues on the system

because one package may update and another doesn't and isn't expecting the other package it depends on to update and have it's behavior change. In the grand scheme of things it's not a big issue for people familiar with Linux, but considering the average user will have little need to have bleeding edge packages, I just don't see a reason to use it unless you're a developer who likes to play with the latest and greatest software. (security updates are pushed out quite quickly on all distros, it's not really a security issue). Although if this does appeal to you, use Arch or Artix as opposed to Manjaro.

https://manjarno.snorlax.sh/

Of the least popular of the two remaining distros (families) would be Fedora. I won't get into the weeds of it, but it's a perfectly usable distro and it's available in many different desktop environments. Really the only two issues worth addressing are that package availability is ever so slightly worse than Debian/Ubuntu, mostly due to the enormous popularity of Debian/Ubuntu however this is an extremely minor issue. Also if you do chose Fedora I'd highly recommend adding the "RPMFusion" repository. It's a semi-official repository that will greatly increase the software you can install via the package manager. The other "issue" isn't really so much of a problem, but is worth considering which is that Fedora has quite short life cycles and so you'll need to upgrade to new versions quite frequently compared to other distros. Here's a quick look at Fedora's life cycle

https://endoflife.date/fedora

Upgrading versions isn't a big deal and it's very unlikely for something to go wrong and break something like on Windows, however it is best to do a full backup before upgrading versions.

The last and by far the most popular distro (family) is Debian/Ubuntu. To clarify, Debian is the "root" distro so to speak, Ubuntu is a derivative of Debian and many, many distros out there are derivatives of Ubuntu. One reason for Ubuntu's popularity over Debian is that although Debian is an extremely stable distro with a very long lifecycle and basically no updates (besides security updates) between versions, it's a completely FOSS distro which means it doesn't have as good of hardware support as others distros which will include proprietary

drivers that are necessary for some hardware to work. There is a “non free” version you can install with that includes these drivers, however it’s an extra step that most distros don’t have. Also the slow updates are also an issue for some people, although it does get frequent security updates, many people do like to get feature updates more often than Debian does, which is where Ubuntu comes in. Ubuntu is maintained by the corporation Canoncial (similar to how Redhat/IBM manage Fedora). Essentially Ubuntu is a derivative of Debian that installs with non free drivers by default, has a similarly long life cycle (the LTS release, they have a mainline release with a shorter life cycle) and also gets feature updates much more often than Debian.

You may wonder what would be the point in using a derivative of Ubuntu if it’s so good sort of a “goldilocks” distro in terms of lifecycle and updates. There are some past and present concerns with Ubuntu. One big one from the past was when they added Amazon recommendations to the search bar, which you can read about here.

https://web.archive.org/web/20220224223925/https://www.pcworld.com/article/436097/ubuntus-unity-8-desktop-removes-the-amazon-search-spyware.html

Although they haven’t done anything so egregious since then, Canonical is still in ill repute with many in the Linux community due to how snaps are implemented in Ubuntu and to some extent snaps themselves. I’ll just leave a link that goes into more detail on the issue, but some software on Ubuntu when you try to install it using the normal package manager (apt) will instead install the program as a snap package instead of using apt to install the native .deb package as you told it to.

https://web.archive.org/web/20220524150803/https://www.zdnet.com/article/linux-mint-dumps-ubuntu-snap/

The article does a pretty good job of explaining the issue, and also mentions Linux Mint which is one of the most popular derivatives of Ubuntu.

Mint retains a lot of the benefits of Ubuntu with a few minor changes. Pretty much the point of it’s existence is to be Ubuntu that won’t implement these controversial things that Canonical

does with Ubuntu from time to time, like the Amazon recommendations and snap controversy. By default snaps are completely disabled in Mint so any time you use the package manager (APT) or the software center to install software, it's installing a native .deb package from the repository and never a snap. If you want you can enable snaps on Mint, however I wouldn't recommend that and if you do want some software that isn't available in a .deb package and don't want to build/compile yourself, I'd recommend using Flatpak or AppImage instead. Flatpak is more or less the same as snap, but without the concerns about usurping the package manger without you requesting it to and is also less locked down, in that you can install Flatpaks from a variety of sources and aren't limited to one proprietary store front like with snaps. AppImages are a bit different and pretty much behave like .exe files in Windows in that they're standalone files that run a particular program.

Another difference between Mint and Ubuntu is the available desktop environments (again you can install any desktop, but I'm talking about options "out of the box" so to speak). GNOME is the only official desktop of Ubuntu, however there's community spins for most desktop environments for normal Ubuntu. Mint doesn't officially support GNOME, but officially supports 3 different desktops Cinnamon, MATE and XFCE; with Cinnamon more or less being the flagship. (Note: by default all three are ugly as sin, however changing appearances and themes is incredibly simple in nearly all distros including Mint, so don't be turned off by the default appearance). The main advantage of this is that Cinnamon is a desktop environment that is quite similar to Windows user interface in terms of layout and such, so it can be more comfortable for long time Windows users to switch to, however I do believe there's a better desktop environment for migrating Windows users which I'll get to in a bit. Additionally if you do want to use the GNOME desktop with an Ubuntu derivative distro, but without dealing with the snap issue, Pop! OS is another fork of Ubuntu that comes with a slightly modified and themed version of GNOME and has the snap issue resolved (installing packages via APT or the graphical software center will install .deb packages, not snap). There are some other minor differences with Pop! OS, I believe one is that it installs the proprietary Nvidia drivers by default which have better performance than the open source ones.

Another nice benefit of using Mint over Ubuntu is that Mint doesn't have any telemetry whereas with normal Ubuntu, telemetry is on by default and you must turn it off manually. I believe in Pop! OS the telemetry is off by default and is opt-in, however I could be mistaken.

Paralysis by Analysis

If this whole topic is a bit overwhelming and you don't know where to begin to try to decide what to use and just want someone to recommend you a single distro/desktop that doesn't suck. My recommendation would be the KDE spin of Fedora.

https://spins.fedoraproject.org/kde/

The primary reason is that I believe KDE is the best desktop environment for people migrating from Windows, with Cinnamon coming in second. Is that although Cinnamon is a perfectly fine desktop, KDE is the Cadillac of Linux graphical programs and most Windows users will be much more comfortable with graphical programs than using the command line to do more advanced things. I could go on and on about all the neat features KDE and it's related programs have, but to keep it brief. Here's a list of most or all of the applications made by KDE and typically come default with any KDE installation.

https://apps.kde.org/

In particular Kdenlive (video editor) and Krita (Paint/Vector Art) are generally regarded as the best and most feature rich options on Linux for their respective types of program; arguably Dolphin (File Manager) and Okular (PDF reader) are as well.

One concern is that the default GNOME version of Fedora has a similar issue with Flatpaks that Ubuntu has with snaps, in that it'll prefer to install Flatpaks instead of .rpm packages (Fedora's equivalent to .deb packages). It's easy to fix just using the graphical software manger/center program set it to prefer .rpm packages from the repository over installing from Flatpak. The last time I installed the KDE spin, it was *not* configured to do this and preferred .rpm packages to using Flatpak by default, however double check anyways to be sure.

Lastly I'd also recommend adding the RPM fusion semi-official repository as it includes a lot of software that isn't in the official repository.

https://docs.fedoraproject.org/en-US/quick-docs/setup_rpmfusion/#proc_enabling-the-rpmfusion-repositories-using-command-line-utilities_enabling-the-rpmfusion-repositories

Note: this is the command line method since all of the graphical guides are about how to do it in GNOME, the default desktop environment, although I'm sure it can be done easily using the graphical program in KDE. Also I'd recommend using the non free repository as well since it'll include more software, but of course not all of it will be completely FOSS.

Keyboard Shortcuts

This will be a guide of some common keyboard shortcuts that are fairly universal across programs and operating systems, although Mac is obviously an exception, so hopefully they'll open the door for to the magical world of keyboard shortcuts which can be quite handy at times.

Also note that the pipe character "|" means "or". It may be used for two different keyboard shortcuts that do the same thing, or a key board shortcut with two options like "← | →" for left or right arrow. Also the plus key itself will have single quotes around it '+'.

Also "Mod" means the "Windows Key" which is usually to the left of the left Alt key.

General

Alt + F4 | Cntrl + Q	Close Window/Application
Cntrl + W	Close Tab
Cntrl + S	Save File
Cntrl + F	Find text
Alt + F7	Move Current Window
Alt + F8	Resize Current Window
Alt + F9	Minimize Current Window
Alt + F10	Maximize Current Window
Alt + F11	Full screen Current Window
Mod + D	Minimize all Windows to show Desktop
Mod + L	Lock Screen
Print Scr	Take Screenshot

Text Editing

Double Click	Highlight Word
Triple Click	Highlight Line or Paragraph
Cntrl + X	Cut
Cntrl + C	Copy
Cntrl + V	Paste
Cntrl + Z	Undo
Cntrl + Y	Redo
Del	Delete character to right of cursor
Insert	Insert mode (overwrites characters when typing)
Home	Go to beginning of line
End	Go to end of line
Page Up	Scroll Window length up
Page Down	Scroll Window length down
Cntrl + ← | →	Move cursor one word forward or back
Cntrl + Del | Backspace	Delete one word forward or back
Cntrl + ↑ | Down	Move cursor to beginning or end of paragraph
Shift + ← | →	Highlight character left or right
Cntrl + Shift + ← | →	Highlight word left or right
Cntrl + Shift + Home | End	Highlight to beginning or end of line
Cntrl + Shift + ↑ | ↓	Highlight to beginning or end of paragraph
Cntrl + A	Select All

Web Browsing

Alt + ← | →	Page Forward or Back
F5 | Cntrl + R	Reload Page
Cntrl + Shift + R	Reload Page, Ignore Cache
Page Down | Space	Scroll Down one Window Length
Page Up | Shift + Space	Scroll Up on Window Length
Cntrl + '+'	Increase Zoom
Cntrl + -	Decrease Zoom
Cntrl + 0	Return Zoom to Normal
Home	Go to Top of Page
End	Go to Bottom of Page
Cntrl + Tab	Go One Tab to Right
Cntrl + Shift + Tab	Go One Tab to Left
Alt + 1-8	Go to Corresponding Tab
Alt + 9	Go to Last Tab
Cntrl + T	Open New Tab
Cntrl + Shift + T	Open Last Closed Tab
Cntrl + Shift + I | F12	Open Developer Tools