Welcome to BASEC – The Basic Security Guide for NETSEC Students

SSH[ghost]

ABOUT BOOK

This is a prototype guide. It has a long way to go before being released outside UAT. BASEC is based off of Incognito Toolkit, parts of How to Disappear, CyberPunk's System Hardening Guide, Gibson Research Corporation's ShieldsUP!, and my own personal experiences, research, ideas, and scripts. There are myriad more sources that were scheduled to be added to BASEC but have not been included yet and will not for some time. I would not call this guide my most fluid and concise work since the larger BASEC gets the harder it is to manage it. It would take months to expand and polish it.

BASEC is an interactive guidebook, or small collection of scripts, created for those new to cyber security and / or Linux. The scripts are coded for Ubuntu / Debian, but many of the commands can be altered for other *nix systems. The purpose of BASEC is to teach basic defensive security measures users can take whether pertaining to NETSEC, SYSSEC, or PERSEC and to help ensure those measures are applied. Not everyone has an easy time with a foreign distro or OS architecture they've never interacted with, thus BASEC is more than a guidebook in a PDF. The secondary scripts are meant to help establish a secure, hardened system with relative ease. Excluding PERSEC, the NETSEC and SYSSEC chapters utilize the secondary scripts.

BASEC will display photos relevant to each page. The three chapters will converge on some topics. PERSEC is a light chapter in comparison since PERSEC is discussed throughout the guide. It’s the most important element of securing yourself. For greater privacy and security options, visit https://www.privacytools.io

This PDF is organized by how BASEC.sh would be ran. Tools and scripts have been added to where they should be run relevant to the sections they follow.

RED = Main Section

PINK = Chapter

CYAN = Header

ORANGE = Link

WHITE = General Text

YELLOW = Project

GREEN = Download & Install TOOL

PURPLE = Pokemon Script

ABOUT AUTHOR

SSH[ghost]

I'm a coder with a passion for all things cyber security. I currently attend a private university for a Bachelor of Science degree in Network Security. I spend most of my time coding and testing well-known or newer security applications through stress testing and

breaking. I also spend a good deal of time researching security applications, vulnerabilities, exploits, methods, concepts, past failures / successes of well-known "hackers," etc. I really like finding and breaking code and applications, if anything, to learn how it works and how it can be improved beyond the initial coders' intent. My main focuses in cyber security and security in general are personal security, digital reconnaissance, social engineering, skip tracing, penetration testing, forensic analysis, honeypot / net installation and management, data obfuscation, security management automation, and personal projects that lead toward fields I've yet to study. My previous education in psychology has becomevery useful and applicable to several of these fields. Every system’s biggest vulnerability is always PEBCAK. To clarify, my professional interests are making myself a ghost and finding those that failed to make themselves ghosts. Think contemporary Hans Landa meets the antics of Shawn Spencer.

My main coding interests are shell / bash, *nix commands, Ruby, and Python. I hope to add PHP next. My coding name is SSH[ghost] and it's pronounced as ghost in the secure shell.

If I had to describe myself, I would say I am very analytical, an autodidactic philomath, and a high performer. Others have described me as creative, meticulous, extremely inquisitive, Devil's Advocate of all trades, and, as a friend puts it, "How do we kill that which has no life?" After all, I'm a ghost.

TABLES OF CONTENTS

PERSEC

PERSEC is personal security. This chapter of the guide has everything to do with you as a user. It’s the most important and often overlooked aspect of cyber security. You can secure your network and system to the point that it’s nearly impossible to break, but you still exist and you’re the one using the network and system. An attacker just has to target you to successfully penetrate your network and system. You’re a constant vulnerability. You can harden yourself, but you’ll always be a vulnerability.

This chapter is meant to get you thinking about how you manage your information and digital activities. It will try to help you better manage yourself, remain cognizant of your actions and surroundings, mitigate what information you release, and harden yourself. OPSEC has been dropped from the guide since its only relevance to security is keeping activities a secret between two or more parties and this guide is specifically made for the individual.

PII = personally identifiable information.

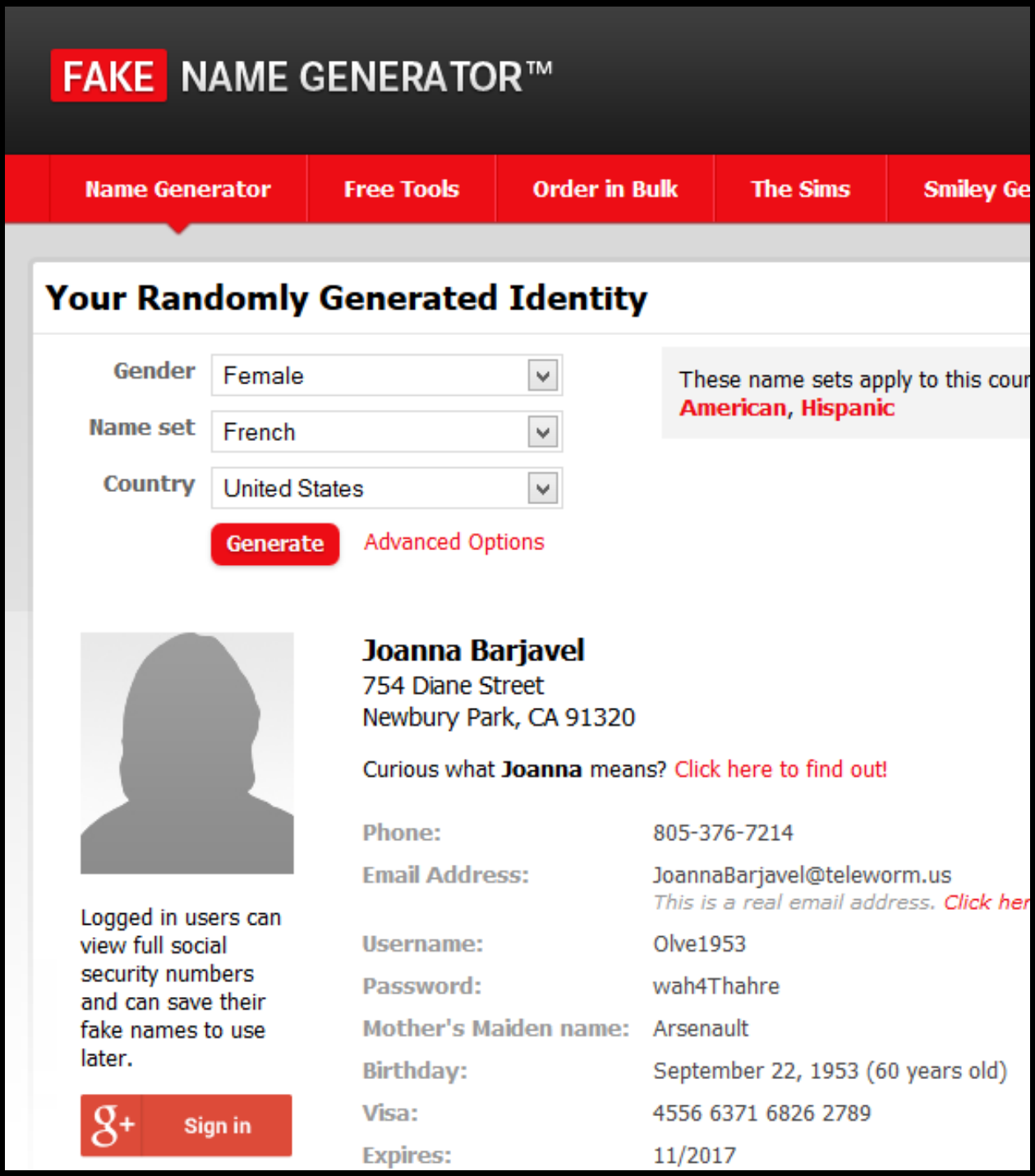
ONLINE IDENTITY

Let’s start by talking about how using your real, full name online is bad idea. Are you a professional contractor? Are you an artist trying to get your name out there to sell your work? Balance of probability states you’re a social media user that has absolutely no reason putting your real, full name online. Ross Ulbricht learned this lesson the hard way when he promoted Silk Road in the beginning with invitations that could only be received by emailing him and the email address used his full name. Many platforms do allow you to create random usernames vs using a person’s name. Social media is already advised against for both security and privacy purposes. However, if you have to have an account, I normally suggest tweaking the first or last name to a nickname. A friend named Zach loved Jack Daniels so we called him Zach Daniels. The surname is an actual last name that social media sites will accept. Otherwise, it’s suggested you either create a fake online persona or use a service to do so like Fake Name Generator.

FAKE NAME GENERATOR

Fake Name Generator creates fake identities in full at random. It creates information from name to the make and model of the car you drive and from your geolocation coordinates to your blood type. The bare essentials include: name, gender, DOB, SSN, address, city, state, zip, phone number, username, password, and email address. The email

address is a disposable email address created using Inbound+. It’s a useful tool for obfuscating your actual PII and there’s plenty of reasons, unfortunately, that you need to lie about your identity from non-government-sanctioned entities. One such reason is privacy from stalkers. Another reason is from telemetry services: smart, digital stalker services. Telemetry is actually the means of collecting user data, compiling data, and creating a user profile based on the collected and compiled data. It’s how companies like Google, Amazon, Microsoft, Facebook, etc. can target what services you may like better. When you create single-use, disposable accounts that require some form of PII and you don’t want to create the identity yourself., Fake Name Generator should be your go-to tool.



FAKENA.ME

A less feature-rich alternative is fakena.me. It doesn't include the additional information that would most likely be needed such as blood type, car make and model, favorite color, current employment with

position, credit card information, etc. What it creates are the bare essentials already covered by Fake Name Generator: name, gender, DOB, SSN, address, city, state, zip, phone number, username, password, and email address. The email address is a disposable email address created using Guerrilla Mail, but without the Guerrilla Mail domains that large, popular sites may have flagged as illegitimate.

DELETE ME ----------

We were previously acting under the pretense that you wanted to create an identity to engage online. What if you wanted your actual identity to not be found through digital reconnaissance? You can either 1) scour each directory site and opt out to have your identity listed or 2) use a service like DeleteMe. The latter collects and removes your data from these directories and other online sites from comments to photos, blocks data collectors, and generates reports. DeleteMe is not

free and you have to trust that it doesn’t retain your PII as it scours the Internet to delete your PII for you. A lot of reviews have stated this service to be effective, yet unnecessary. It costs $130 annually, which means its usage is limited to that timeframe. It’s great if you’re in a hurry, don’t want to deal with the research and opting out, and you just have money to burn. Otherwise, research the people-finding directories yourself, try to find yourself on each, and get them to take it down where applicable. This option is costly in time whereas DeleteMe is costly in money.

There is a third option. It’s easier to do, completely legal even though it wouldn’t seem like it, and still keeps you secure. Obfuscate your PII with spelling mistakes. Kent Adams is Kent Addams, Ken Adams, Ken Addams, Kent Adam, Kent Addam, Ken Adam, Kent Addams, etc. and

those are just playing on the t, d, and s in the name. It makes it harder for people to find you. Another option with obfuscation is beyond the basics of BASEC with creating shell corporations and placing your finances and assets under the company or creating an actual company and doing the same. You can’t find Kent Adams if all of his bills and PII are actually under Acting Enterprises, Ltd. How would you know to make that connection unless you actually knew the person well enough to know that’s their company? These are just a few ways of keeping your PII private.

ACCOUNT MAINTENANCE / PII REQUIREMENTS

This page is a continuation from the previous. Incognito Toolkit suggests you save the Fake Name Generator information in LastPass. I recommend local with an office type doc. My recommendation will ALWAYS be local alternatives that don’t require Internet access. You have to put a lot of faith in the software developers that they’re software is both secure and benevolent. Unless you know reverse engineering, good luck. Simply trusting a 3rd party’s analysis is the same issue. Just remain aware and do your research.

You want to save the Fake Name Generator information so you have a solid lie. This book is made with the worst in mind that someone is attempting skip tracing and / or digital recon against you like a stalker. If they find several accounts linked together with separate PII, then it’s obvious that the real account owner is obfuscating their data. You should obfuscate that you’re obfuscating your data. That means lie about the lies you’re telling. Plus, in case you event want to access an account you created with the generated PII, it helps to know the fake data when you can’t login.

BUGMENOT

For all accounts that require PII, I recommend using BugMeNot. It's a site that shares login credentials of generated accounts so you don't have to enter PII to join a service. The only downside is that major sites have banned BugMeNot access, which defeats the purpose for the most part. The vast majority of sites that don't require authentic PII or PII verification don't care if you lie. However, it's a nice tool that allows you to access a site service without even having to use Fake Name Generator. You don't even need to invest in burner phones or create temporary email accounts.

ACCOUNT KILLER

We were previously acting under the pretense that you wanted to create an account to use a service. What about when you no longer want to use

the service and you want to delete your account? There's usually a setting is account settings to do this, but that's not always there and sometimes you have too many accounts you want to delete at once. It's a repository of instructions and links to delete accounts for numerous, well-known services with ratings of difficulty for each service.

JUSTDELETE.ME

JustDelete.Me is an alternative to Account Killer with less support, same difficulty indicators, and includes a fake identity generator. This is a notable service is that it attempts to integrate and compete with Fake Name Generator and Account Killer. If you want one service that offers both, this is a somewhat decent choice. It's also open-source with a GitHub project so anyone can make it their own. It has the potential to succeed both predecessors.


justdelete.me

EMAIL

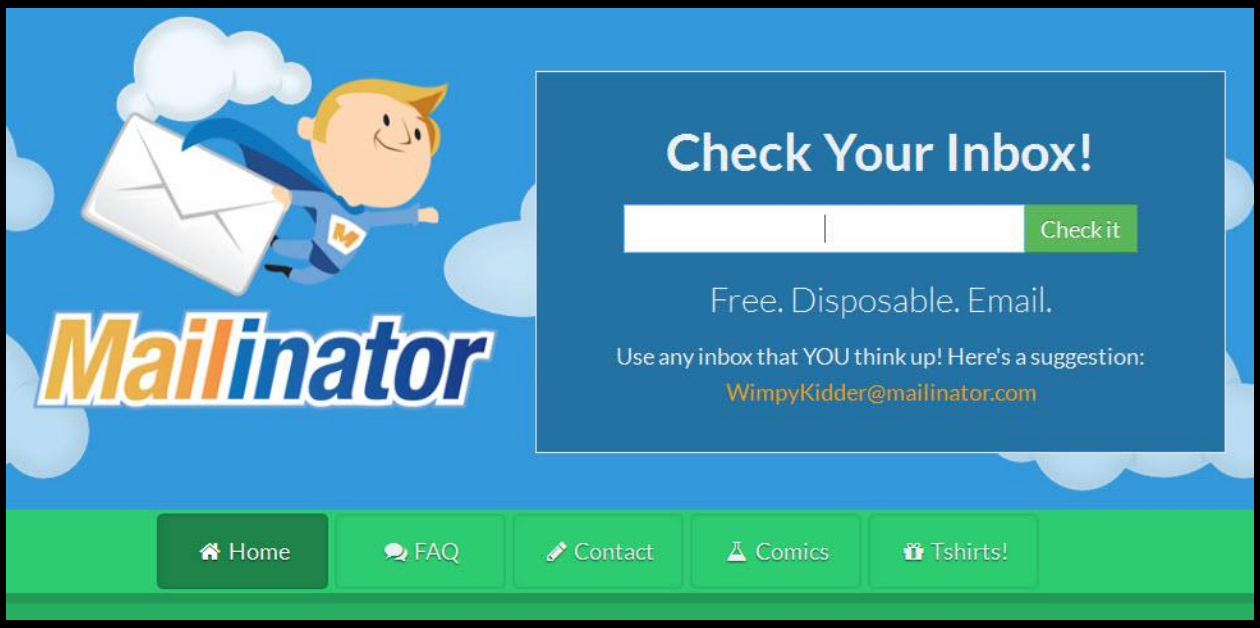
Sometimes, you need disposable email addresses. I use these before I use Fake Name Generator since even creating an identity isn't as necessary and more time consuming that obtaining a temporary email address. Some sites flag them as illegitimate accounts and block them. However, they're a great way of avoiding spam, not giving up your PII, and not giving up one of your email addresses when a site is requiring you to join them to use their service. I've added my own options further down the list due to the issue of some of these services being flagged as illegitimate and blocked. There's a lot more disposable email services that you could imagine, but I'll only cover the key few. I've ignored 10 Minute Mail, My Trash Mail, and Temp Inbox because they're lackluster in comparison to the few chosen.

DISPOSABLE EMAIL

- Guerrilla Mail: Sends and receives mail with attachments, has browser and Android support., saves mail for 1 hour, is not secure, generates new address each visit or allows user to input address, allows domain selection, and scrambles address. The differences between free and premium accounts are that the premium accounts allow custom domain selection, includes privacy features, bypasses blockades, and remains easy to use with just

entering the Name Server and allowing Guerrilla Main to do the rest.

- Mailinator: Only receives mail for disposable option, has browser, Google, and Slack support, deletes after a “few” hours, is not secure, requires user to generate address allows domain selection, and scrambles address. The differences between free and premium accounts are that free accounts aren’t secure, it saves nothing for more than a day, and allows many alternate domains. Premium accounts vary on the amount they offer, but they include storage, several thousand emails a day, private domain use, API access, and it saves messages.



- Inbound+: Only receives mail, has browser support, saves mail for 24 hours, can only hold 10 emails, is not secure, generates new address each visit so long as cache and cookies are cleared or allows user to input address, does not allow domain selection, and does no scramble address. The difference between Inbound+ and the previously mentioned options is that it doesn't have a premium account option. Inbound+ was only chosen because it's used by Fake Name Generator vs. Guerrilla Mail like Fakena.me.

ENCRYPTED EMAIL ----------

I'm only covering one aspect of encrypted email in conjunction with disposable email services. Encrypted email is fully discussed in NETSEC under Email. I've been annoyed at times when I'm in a hurry and a temporary email service doesn't work because it's been blocked whether the service I signed up for explicitly states such or just

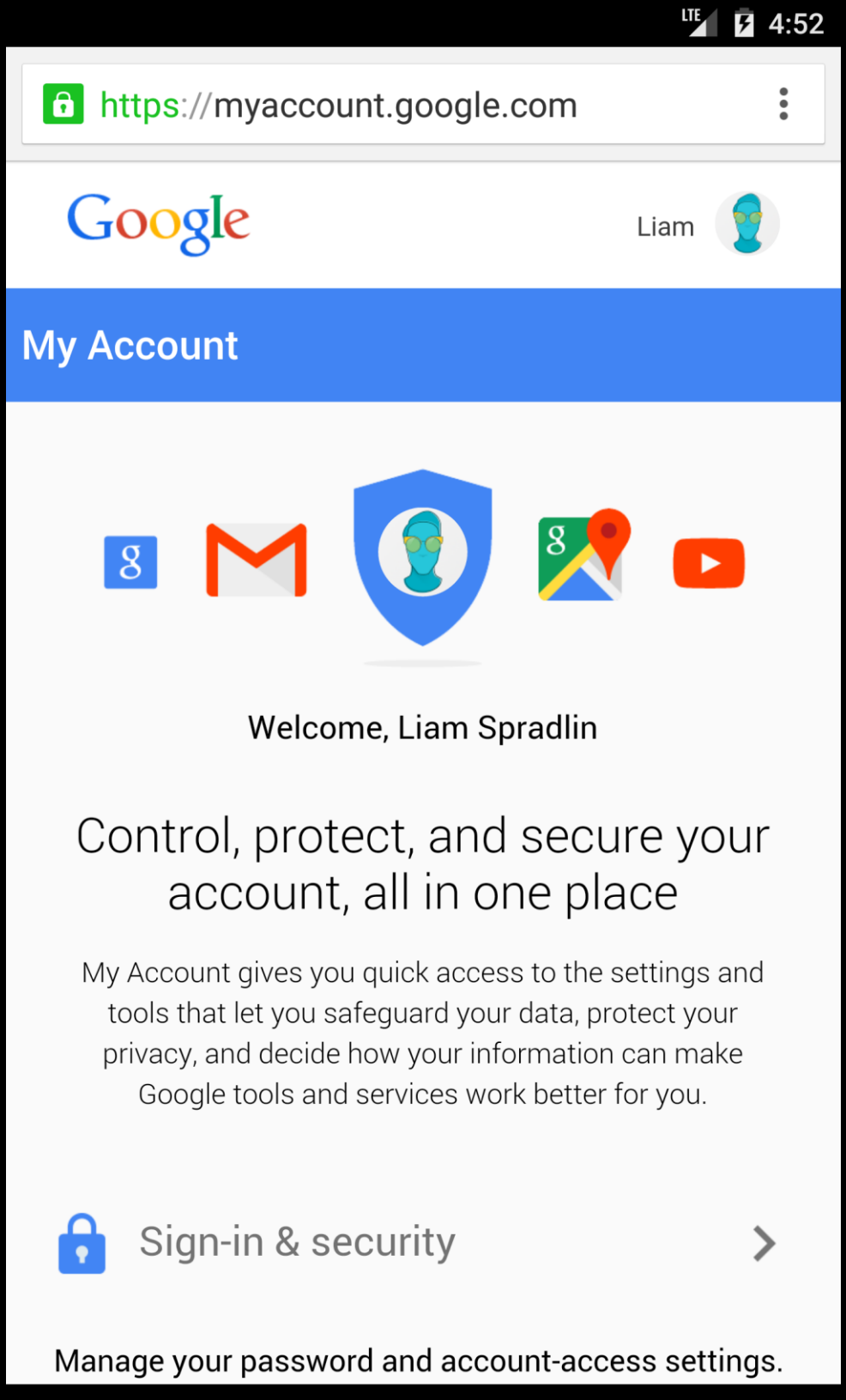
never sends the confirmation email to the temp address. One sure-fire I've come to combat this issue is to use Tutanota or ProtonMail; two highly trusted, encrypted email service providers. They're easy to set up, require no PII verification since privacy is one of their primary principles, is secure, and can be easily deleted once finished, especially Tutanota. It's not my first choice since I have to spend time creating the account and I'm wasting an email address another user may want. However, both are accepted since they aren't primarily used for fake data or creating temporary accounts for single-purpose usage like disposable email services. It's a thought to consider if you want to use a temporary email address on a site that's blocked disposable emails, yet you don't want to sign up for an email address that makes you prove your identity.

PRIVACY MAINTENANCE

Now that you know how to obfuscate and delete your actual PII and create PII, let’s talk about maintaining privacy. Screwing up at this level makes everything else you’ve done with the last chapters useless, assuming you’ve been making changes or notes throughout your reading. I can keep and maintain my privacy, but I can’t do it for the people around me. A friend or relative sharing your information, intentionally or not, can undo everything. You can start by asking them not to do so, but you can finish by making sure they have no information to share. I use an email address on a disposable virtual machine to keep in contact with my family, especially since the last encounter using a primary account led to multiple forms of spam and social engineering attempts. They were using the share feature on some relatively unknown site vs copying and pasting the URL into an email, which is also not a good idea but nowhere near as bad. Another issue might actually be yourself. Don’t ever post hard PII and avoid posting soft PII. Hard PII is the PII we’ve discussed previously like your address, full name, phone number, SSN, etc. Soft PII is stuff like favorite colors, movies, hobbies, etc. All of these identify you as a person. If you want to share this information, then you have to accept the consequences of losing your privacy.

GOOGLE

I highly recommend avoid using Google for as much as possible. They might have better services than Yahoo!, Microsoft, Facebook, Amazon, Apple, and more and they may allow you control over your data, but you have to trust Google to not be evil. They’re very good at data aggregation and analysis. You don’t need a YouTube account to watch most YouTube videos and you don’t need to subscribe to videos via an account when RSS exists. Google Drive isn’t an encrypted cloud storage service, Google Docs has poor quality in comparison to MicroSoft Office, Gmail isn’t encrypted and Google reads your emails, you don’t need an account to use Chrome Web Store, etc. Using Android without a Google account is difficult though. While Google doesn’t encrypt emails, it does have PGP support. The only issue is that PGP has a learning curve, but this will be discussed in later in the chapter under Encryption. Google does have some uses even though alternatives exist. In fact, the only real pro Google offers is cross-service integration. One of the few uses is setting up Google Alerts to notify you when a change has been made to your online PII like if a directory site adds your information. Another is for Google Calendar with reminders if you can’t use local alternatives. Reminders such as password frequency rotation deadline, but this will be discussed later in this chapter in Password Manager.


4:52
https://myaccount.google.com
Google
Liam
My Account
Welcome, Liam Spradlin
Control, protect, and secure your account, all in one place
My Account gives you quick access to the settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google tools and services work better for you.
Sign-in & security
Manage your password and account-access settings.

If you’re going to use Google, I have some suggestions, all of which are under your account settings:

- Use a recovery email specifically for security uses like recovery.
- Don’t add your phone to recovery list.
- Make security answer irrelevant to security question.
- Check your connected devices regularly.
- Regularly check your account permissions. Remove what you haven’t used in 30 days and / or will not use in the foreseeable future.
- Check your app passwords. If you’re using 2FA and email through any email app that’s not Gmail, you need to generate an app password so you can still access your Gmail through that app.
- Don’t use Gmail, especially with secure, private, encrypted emails out there.
- Keep your 2FA up-to-date. Keep list of back-up codes in a txt file encrypted with whatever service that uses AES256 like AES Crypt. This will be discussed further later in the chapter under Encryption.
- Review what public information you’re giving.
- Disable or pause all Google activity such as YouTube watch history.
- Disable ads based on your interests.
- Delete Google services not in use and their data.

- Set up Inactive Account Manager.

PHOTOS

Don’t post personal photos of yourself online. If you do so, then make sure to obscure the data first. We’re talking about adding layers onto layers, pixelating, creating glitch art, and / or blurring images while always removing EXIF data. Using Photoshop to make your face into a swirl is reversible and has been used by the FBI against a suspected pedophile. Good for them for catching a criminal, but we already know thanks to the Snowden Revelations that triple-letter agencies don’t make the distinction between criminal and law-abiding citizens when data harvesting. Especially don’t use camera phones. Digital cameras are bad enough with metadata, but smartphones include geolocation data too. Both give the date and time of the photo taken, the make and model of the device used to take the photo, the dimensions of the photo, and more. Some mobile apps like Obscuracam exist to wipe metadata, but it replaces the metadata with new metadata stating the original metadata was removed by Obscuracam and this will be further discussed in SYSSEC under Mobile. If you take photos on your phone, privately and securely transfer them to your computer. Use EXIFTool to wipe the EXIF data or metadata. It doesn’t replace the original metadata with new metadata but scrubs it completely short of size dimensions. I prefer to blur my face, add an image over my face,

take pics with my face already covered, pixelate my pics, or blur them so all of them can’t be used to identify me.

ACCOUNTS

Don’t use social media. They’re not really secure and the people close to you should know your email and / or phone number. Especially don’t use social media services that don’t give you robust security options. I don’t recommend blogging or vlogging either, but therein lies the distinction. Do you use social media for social interaction with friends and / or family or are you using it for professional purposes? You have to accept the consequences of the latter, but the former is

an avoidable vulnerability you’re needlessly adding to your digital life.

Try to maintain as few accounts as possible. The more accounts you have, the harder it is to manage them. I suggest compartmentalizing your accounts and separating by use on different email account and VMs, which will be discussed later in the chapter under Virtualization. Delete what you don’t use regularly. Before deleting the account, delete all of the data on the accounts and obfuscate what can’t be deleted.

DOWNLOAD & INSTALL EXIFTOOL

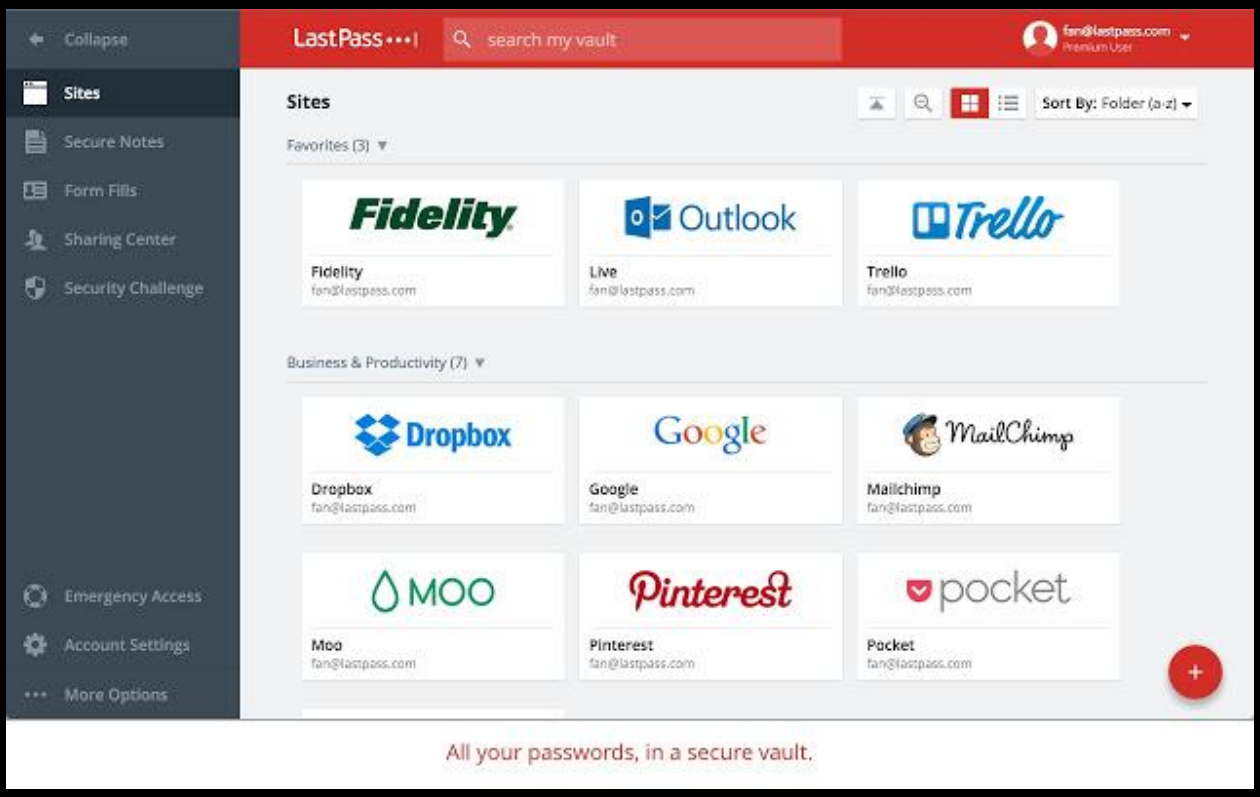
PASSWORDS

Passwords are important. Use strong passwords. To clarify, use long passwords without repeating clusters of characters. Complexity matters, but length matters more. Also, use unique usernames per account cluster (PROJECT DEVICE PERSEC) and use unique passwords for all accounts across the board. Try to auto-generate passwords as long as possible with password managers. Some places have limits of 64 characters and other 16. You have to test it yourself. However, the shorter the password, the more frequently you should change them out. There is no formula for this and I doubt there ever will be since increasing computational power would directly affect frequency rate. The longer your password, the less often you need to change them. However, if you're using a service that doesn't salt the password hashes, you're screwed either way. Every 30 to 90 days is a great policy for how often you should change your password. Bruce Schneier has a good article on the matter of password rotation frequency: https://www.schneier.com/blog/archives/2010/11/changing_passwo.html It's hardly inconvenient if you're using your password manager to generate these passwords, except pwd.sh (it may be great, effective, local, and transparent, but being forced to enter the master password with each change or access can be annoying). If you're not using a

password manager to maintain and generate your passwords, you need to adopt some type of password manager policy. Whatever the frequency, you can always automate the process in cron with zenity, but it’s your responsibility to research and test your notification capabilities. Cron will be discussed in SYSSEC under Automation.

LASTPASS

LastPass is the most talked about password manager online and I’ve held an account with them twice. However, I personally can’t stand a network option if I can use a local option that never touches the Internet. However, there’s no denying the greatness of LastPass as being the most versatile password manager yet. It’s password generator not only allows you to select the password length but the use of characters, how often a number appears, and whether or not every character type is required. It stores identity information for autofill services, conducts all AES 256 encryption and decryption on your computer, the encrypted information is salted before it leaves the computer (which was proven when an attacker successfully social engineered a few people and could not retrieve the logins), and they never receive the decryption key, unlike Microsoft with BitLocker (will be discussed later in chapter under Encryption). LastPass can be set to logoff when idle or after Chrome has been closed for so long, supports myriad account types, allows for autofill for password when on recognized site of stored data, allows encrypted notes, uses many



forms of 2FA from Google Authenticator to Yubikeys and even includes its own 2FA system, generates security score on passwords and LastPass account, auto-changes passwords, allows offline connection, has cross-platform support on browsers, allows importing and exporting of passwords, and has more than one use for Yubikey. The premium accounts of an annual $12 includes unlimited device sync, shared family folder, priority tech support, even greater 2FA, and everything included on the free version. 2FA will be discussed shortly in next section of this chapter. LastPass also includes business accounts with even more features for companies to make use. The mobile app includes similar features for the phone to make password entry easier without having to type out all the characters on the phone's keyboard. I highly

recommend this service for the layperson and heavily advise against it for the paranoid. It might have proven to be secure, but it still involves a lot of trust. The password decryption aspect is hardly any different than a local password manager though. You’re screwed either way if your system has been infiltrated.

1PASSWORD

1Password is also a critically-acclaimed password manager. Unlike LastPass, it’s local, which makes it better even though it may not be as feature rich. It’s another trade-off of security and convenience. The difference between LastPass and 1Password is that it requires a monthly subscription of at least $5 or a one-time purchase of $65. Pricing depends on whether shared use up to 5 people for monthly subscription or single-user use for one-time purchase. While it may be a local password manager, it’s still requiring you to give PII online making it less than desirable.

1Password families (subscription) works on Mac, Windows 10, browser, iOS, and Android, has 1GB encrypted document storage, allows unlimited passwords and stored information, includes full features, has own built-in syncing, has offline access, sharing and access control, web access, account recovery, always-up-to-date at no charge for new versions, and has one-on-one support.

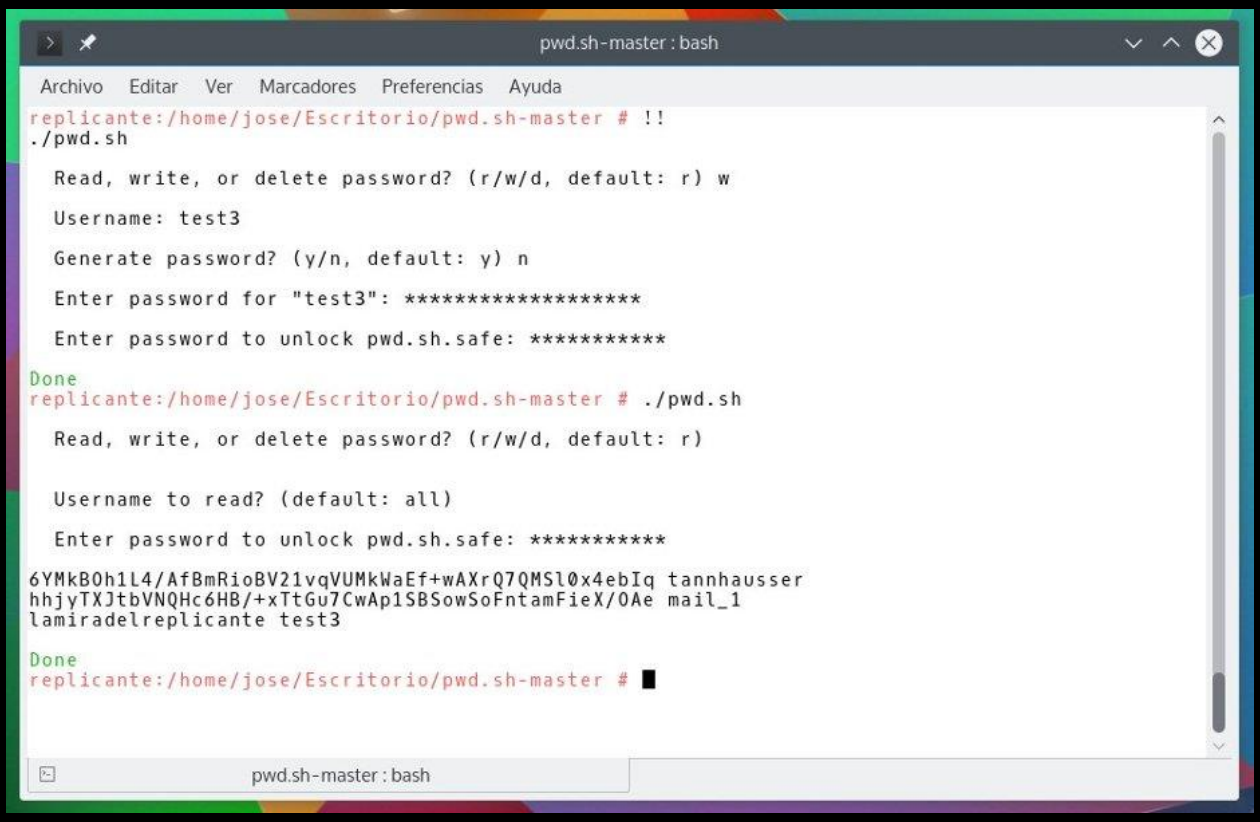
1Password (one-time purchase) works on Mac, Windows 7 and newer, browser, iOS, and Android, includes basic features with it-app purchase of full features, allows 3rd party cloud syncing, allows offline access, and has one-on-one support.

1Password also uses AES256 and Account Key 2FA for exponentially increased strength for the master password, encrypts data over servers, and is allegedly impossible to crack. It also uses WebCrypto and is transparent by documentation. Not a lot more can be said without signing up for a free trial or paying for the service. Like LastPass, it’s definitely worth researching and testing, especially for the whole family to use.

PWD.SH ----------

Pwd.sh is my personal favorite and only works on Linux currently. It’s CLI-based, uses GnuPG, is local, open-source, and completely

transparent (not just by documentation but by code too). It has less than 250 lines of code and you, the user, can view it all. Unlike the other password managers, you know exactly what's happening. It can be a pain not being a feature-rich with the previously mentioned password managers. I have to always enter the master password when creating, storing, reading, or deleting passwords whereas it's optional in the other two for a single session. One typo and you have to start all over executing the script, entering the letter option you want, entering a username, and master password or whether you're storing and creating a password, the password length, the username, and then the master password. You could modify your master password to use the



Yubikey, but that means anyone that knows you use Yubikey for your

master password, has access to it, and knows how to use Linux can own your information. Yubikey will be discussed in the next section of this chapter. It’s a script that’s best run with root, storing the script in the home directory, and never deleting or moving the pwd.sh.safe file out of the same directory as pwd.sh. It’s the file where all your passwords and usernames are stored. Pwd.sh allows you to create a password from 1 character to 100, can find the password with username entering any word used in the username, and is very simple to use. In regards to the username search, if you store a username that reads as, “John Doe Email Account,” you only have to enter any one word of that username for pwd.sh to retrieve it. This also means that if you use the same word with other usernames in pwd.sh, it will have retrieved them too. Let’s say you have, “Jane Doe Email Account,” too. Entering, “Doe,” Email,” and / or, “Account,” will retrieve both usernames and passwords. It makes for some interesting customization. The auto-generated passwords generally create enough special and numerical characters in proportion to the password length so you won’t see a lot of special characters. That makes it easier to crack. That said, it cannot retrieve certain usernames with certain special characters. I can’t access any, “SSH[ghost],” accounts because I used brackets so I have to search using, “SSH,” or the modifier for the specific account. I can’t use, “ghost,” because it’s between the brackets. Each username and password

has to be filled in one at a time, is not quick to store information, and does not change the order of things just because you entered in a new password. It stores all usernames and passwords from oldest to newest. Unless you know how to use GnuPG, you cannot simply crack pwd.sh.safe to change the information. If you need to back up your information, back up the safe file itself.

SELF-CREATED SAFE

I used to use this with steganography before switching to AES Crypt, which will be further explained in this chapter under Encryption. Since pwd.sh cannot be used on Android and I may need to access my passwords on the phone, I created an encrypted txt file that's stored my usernames and passwords. Just write everything neatly into txt file, use AES Crypt to create an encrypted copy, and delete the plaintext version. You just have to enter the password you entered for AES Crypt for it to create a cleartext copy that you can view or edit. If you make any changes, you have to create a new encrypted copy. Since Crypt4All is AES Crypt for Android, I can still access my passwords. This may not be as secure as pwd.sh so I've take the liberty of not only encrypting the file but the compressed folder in which it's stored too. However, it does provide me with a back-up in case I can't use pwd.sh for whatever reason and vice versa.

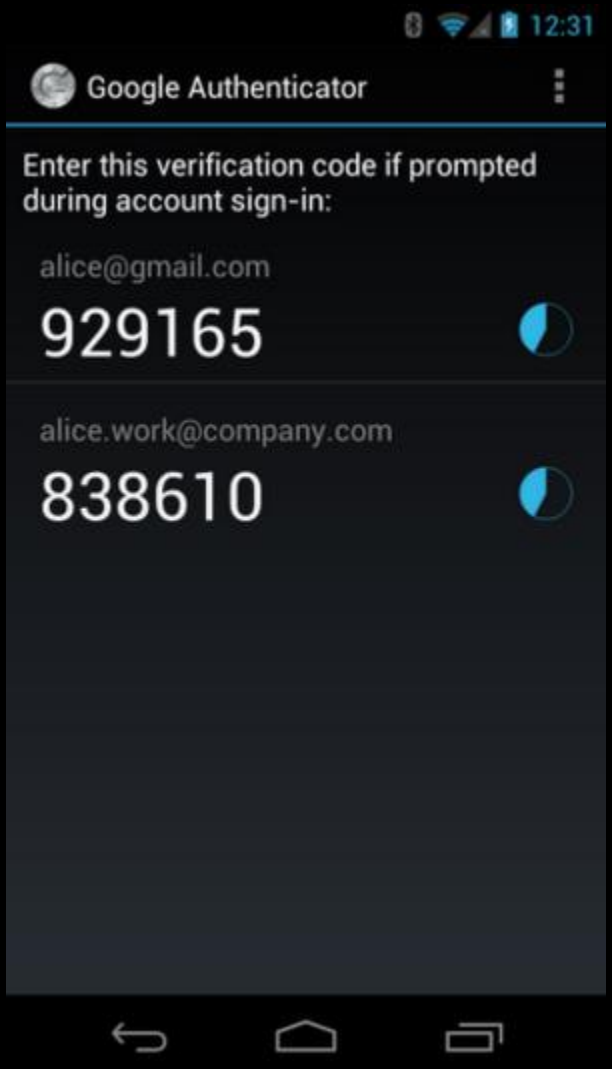
DOWNLOAD & INSTALL PWD.SH

TWO-FACTOR AUTHENTICATION

2FA is two factor-authentication. You use it since attackers may get your login credentials. 2FA is based on the model that passwords are something you know so 2FA must be something you have. Something you have may include mobile or desktops apps that generate passcodes, email access, USB keys, or a phone with SMS. Don’t ever use SMS two-factor authentication if you can. It’s the least secure. If you’re the average user, and odds are you are, email 2FA is just as bad. Unless you engage in PROJECT DEVICE PERSEC or already have a separate email account only used for 2FA, you likely engage in some unsafe habits that makes the email option a bad idea. For example, we already know that if a thief gets your phone that they have a great chance of owning your data. This is worse if you use 2FA on your phone with SMS, an email account that you have set up on the phone, or an app that uses TOTP like Google Authenticator. TOTP means time-based one-time password. Never put your more essential email accounts on your phone and try to use encrypted email and text services. These will be explained in SYSSEC under Mobile and NETSEC under Email. If you’re going to use any of the 2FA options available, be very careful about how to manage and maintain your options.

GOOGLE AUTHENTICATOR

Google Authenticator is a mobile-only app for Android, iOS, and Blackberry that uses TOTP and HOTP. You store your login credentials in the app so it can generate 6- or 8-digit passcodes every 10 seconds. It’s got a lot of support, but it’s main flaw is that it’s always running. If your phone is stolen and the thief bypasses the phone’s lock, then they can access the passcodes generated by the app.



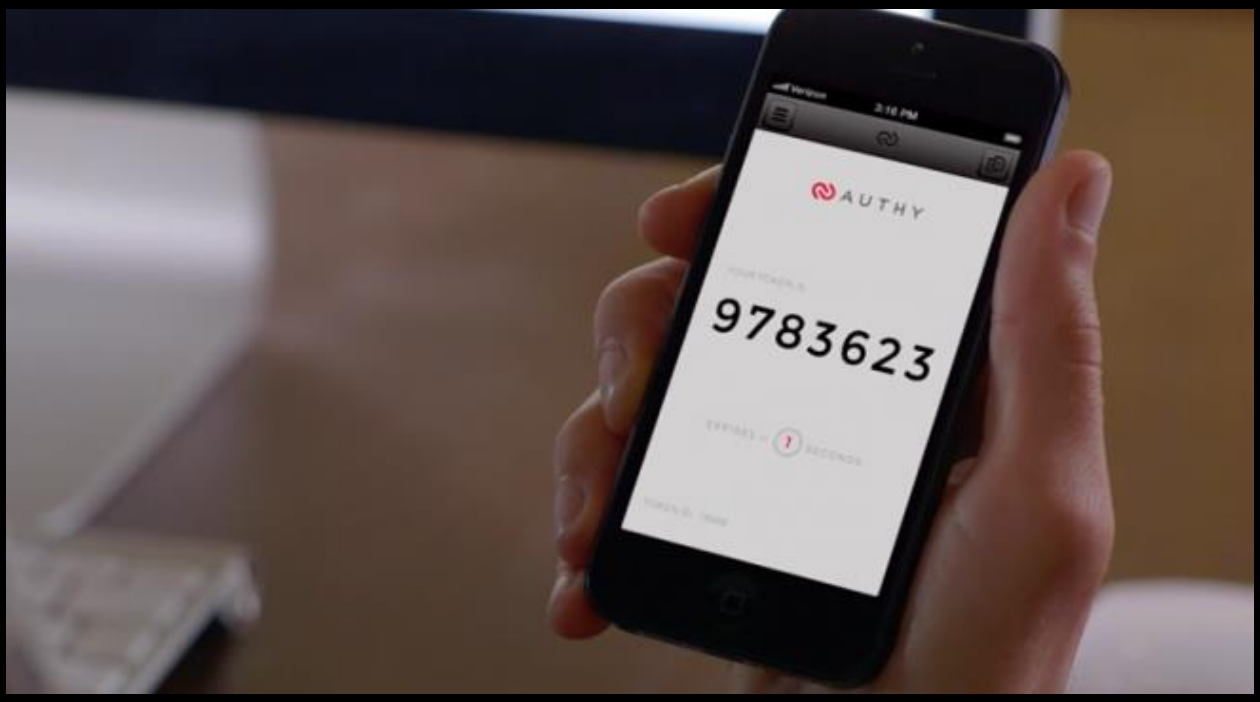
At this point, it’s a good idea to invest in some sort of phone-wiping service (it’s a good idea regardless). If you don’t want to engage with this gaping vulnerability, there are other services. Another drawback is that it’s device limited. If you lose your phone, you’re screwed. This may seem like a good idea since the information is only in one spot, but it’s the type of issue that can keep you locked out of your services. Case in point, when you soft brick your Android phone and you have to reinstall your custom ROM, you can’t just sign into Google

if you were using Google Authenticator for your 2FA. This is why 1) Google makes sure you have at least 2FA options selected if you have 2FA enabled and 2) why it’s a good idea to back up your apps and app data. This will be covered in SYSSEC under Mobile. Unless you’re going to maintain a separate mobile device for security-only use or use some form of virtualization on your laptop or desktop to run one of the mobile OSes, it’s unwise to use Google Authenticator, especially without back-ups.

AUTHY

Authy is more versatile than Google Authenticator for security services and is business-oriented as much as user-oriented. It’s a mobile and desktop app for Android, iOS, and Google Chrome on OS X, Windows, and Linux. It uses 7-digit TOTP to generate passcodes every 20 seconds. Its support is also very wide and in can integrate Google Authenticator tokens through QR code scanning. In order to use it, you have to sign up for an account, which can be free or premium. Unlike Google Authenticator, if you lose your phone or computer, you can still have access to the 2FA codes generated since Authy backs up your credentials with encryption. There are some drawbacks. First, you have to have an account. That’s an additional vulnerability you don’t need and an additional account you have to manage. Second, it backs up your data. You have to take it on faith that the data is properly encrypted, that Authy is a secure service, and that Authy isn’t

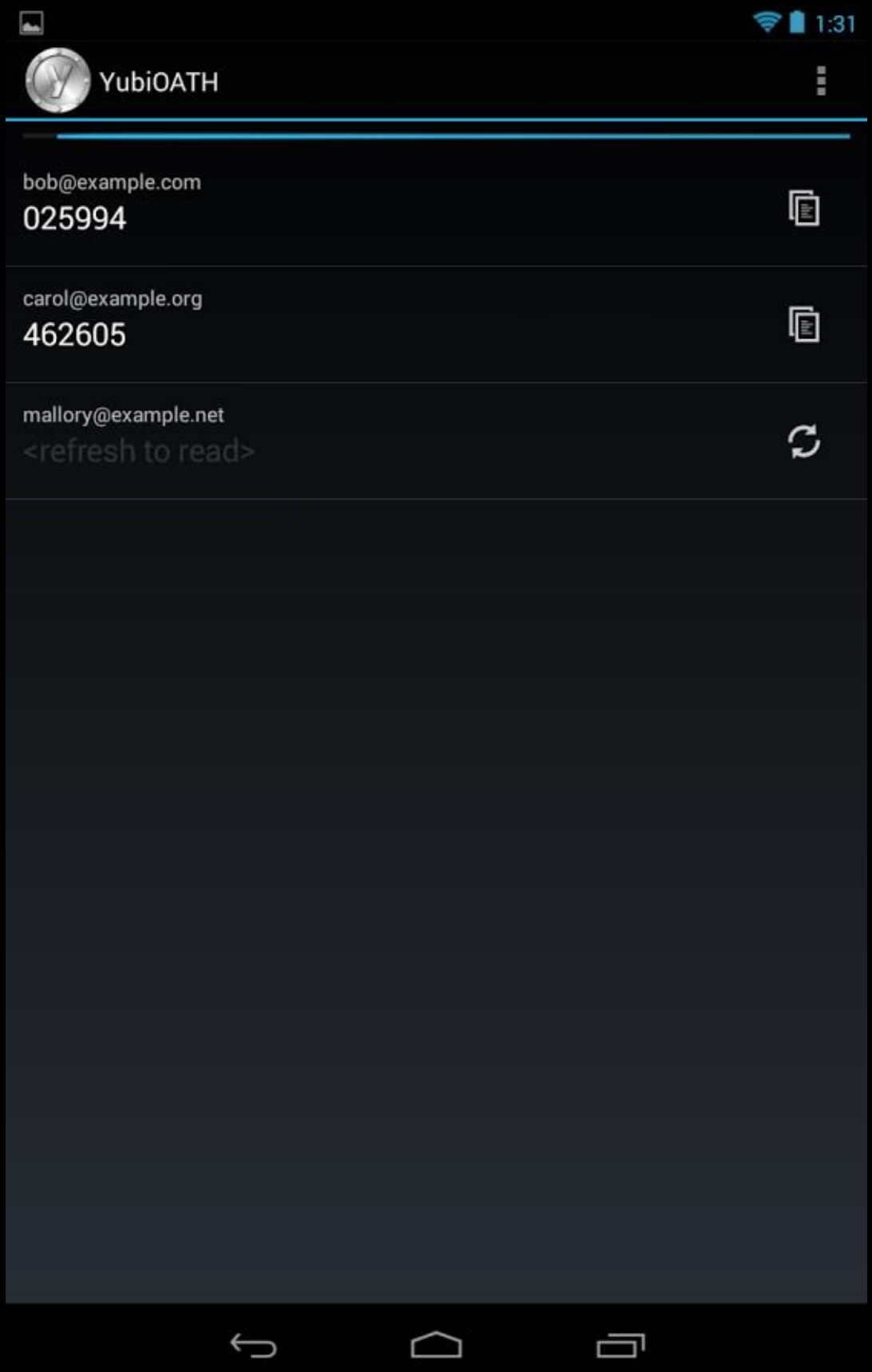
selling your data let alone viewing it. That’s a lot of trust needed.



Last, the free version conducts less than 100 authentications a month. Since Authy is based on AWS, the premium accounts are used to pay for the AWS usage and is the reason why Authy’s free version is so limited.

YUBICO AUTHENICATOR & OTHER YUBICO SERVICES ----------

This one is my personal favorite and requires a one-time purchase of a Yubikey Neo for $50 or any other Yubikey if you don’t plan on using the Android app or want NFC support. It’s dependent on you owning a Yubikey, which is a 2FA physical key that connects to USB ports. It’s support and versatility is as wide as LastPass, but not as easy to use. One use for it is storing a password into the Yubikey so that entering it into a USB port and clicking the key enters the passwords

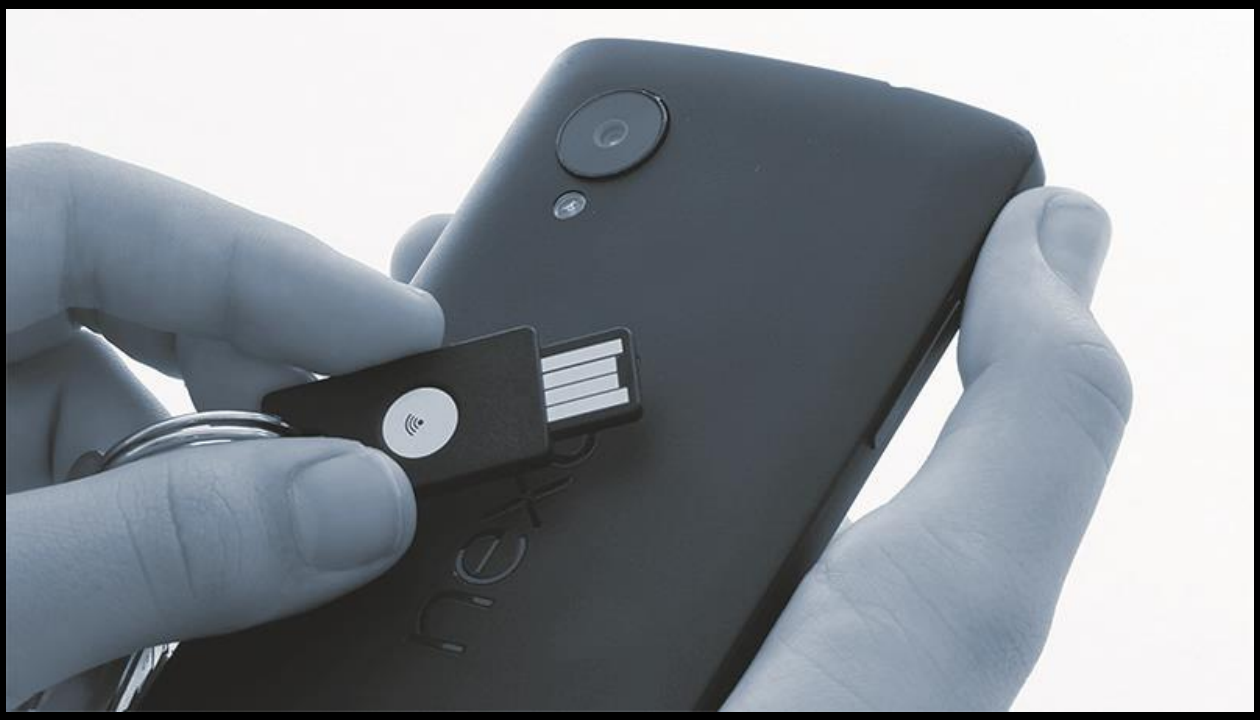


and executes the function of the ‘Enter’ key. The Yubico Authenticator

app for Android is built right on top of Google Authenticator without the crippling issues of storing your credentials within the app and without constantly running. Instead, it only runs when activated by a Yubikey and the credentials for 2FA are stored within the Yubikey itself. This in of itself is another drawback. In case you lose the key, you're screwed. Yubico explicitly states to treat Yubikeys like actual keys. Buy a spare and keep it hidden just in case of emergencies. However, another upside is the repetition of its versatility. I've programmed mine very easily to be a smart device for my Android phone so I can unlock my phone with a full password or the Yubikey. I've also set my phone with an additional pin for when a thief tries to break into my phone with the Yubikey, but this will be covered in SYSSEC under Mobile. One of the other great aspects is that it's a local security measure since it's physical hardware, is encrypted so it can't be easily cracked and tweaked or have the stored data stolen, and is recognized by computers as a keyboard making in even harder to tweak by attackers.

I use a Yubikey Neo for my 2FA and, like the previously mentioned services, does come with its own drawbacks. One of which is knowing what you're doing. Apart from the Android version, the iOS and desktop versions involve some work. Unlike Authy, the desktop options are actual desktop options and not a browser app. The Android version is as easy as installing it from the Google Play Store or F-Droid. The

iOS version of the app is the oddest with needing a browser, a specific Yubico URL, and an Apple Camera Connection Kit. The desktop versions require too much work to simply explain, but you will end up installing more than just the app. While the desktop and iOS version can use any Yubikey, the Android version needs Yubikey Neo since it’s the only version that supports NFC. Other USB 2FA options include Nitrokey and Swekey, but I haven’t tested either.



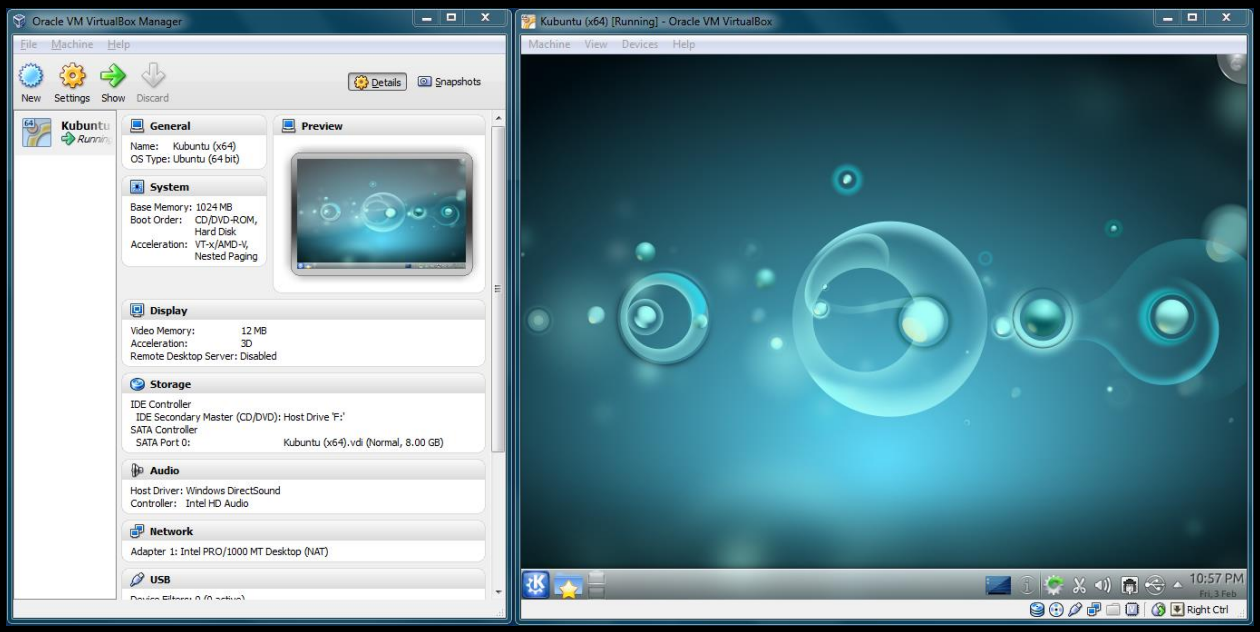
VIRTUALIZATION

VMs, or virtual machines, are great for a large number of reasons. You can use other operating systems simultaneously with your main system, you can test software or configurations on a guest OS (VM; main OS is host OS) that could break the guest OS without it breaking the host, you can set up a network of systems to communicate while on one computer, you can go online without as much concern for malware or cyber-attacks without the host OS usually being affected, and more. The one drawback worth noting is that using hypervisors can eat up a lot of your system resources so you need to test and configure your VMs properly and not run them on cheap machines that lack any real computational power. Since my host OS is a Linux distro and I need to use a current version of Microsoft Office, I have a VM set up with Windows 10 to run MS Office 2016. However, there’s still more reasons for virtualization. In the context of PERSEC, we need VMs so we can use separated systems on a single machine without the systems necessarily being connected to each other. Previously, under Accounts, I stated that account types need to be separated with different email addresses and systems. Create a Linux VM and encrypted email account for your finances and transfer your finance-related emails and accounts to the new email account that you only access via the VM. Do

not use mobile banking apps and be cognizant of what's connected to what. This will be covered later in this chapter under Finances.

VIRTUALBOX

VirtualBox is a free and open-source hypervisor commonly used in the *nix community for creating, maintaining, and using VMs. It doesn't have the prettiest design nor does it have all the robust features

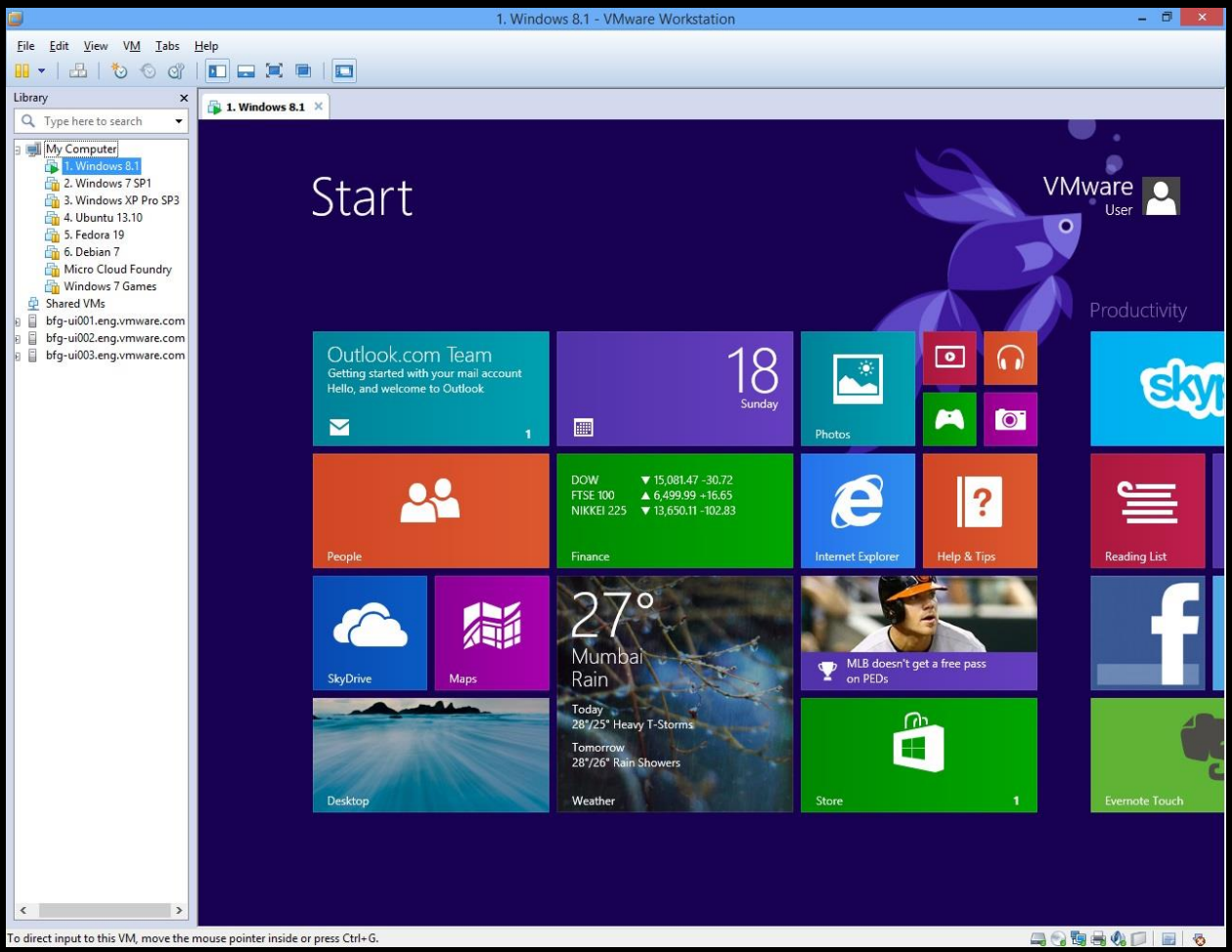


most VMware products have, but it's still extremely useful for many people. It can be used on Windows, OS X, Linux, and Solaris. It's much easier to install OS X on than VMware Workstation, is a lot lighter and easier to configure than VMware Workstation, and has an active development community. However, VirtualBox is also owned by Oracle and has closed-source USB drivers and cannot issue commercial licenses for said drivers. If your intent is to keep Windows as your host OS and

use Linux as your guest OS in your VMs, then this might be the better choice for you.

VMWARE WORKSTATION

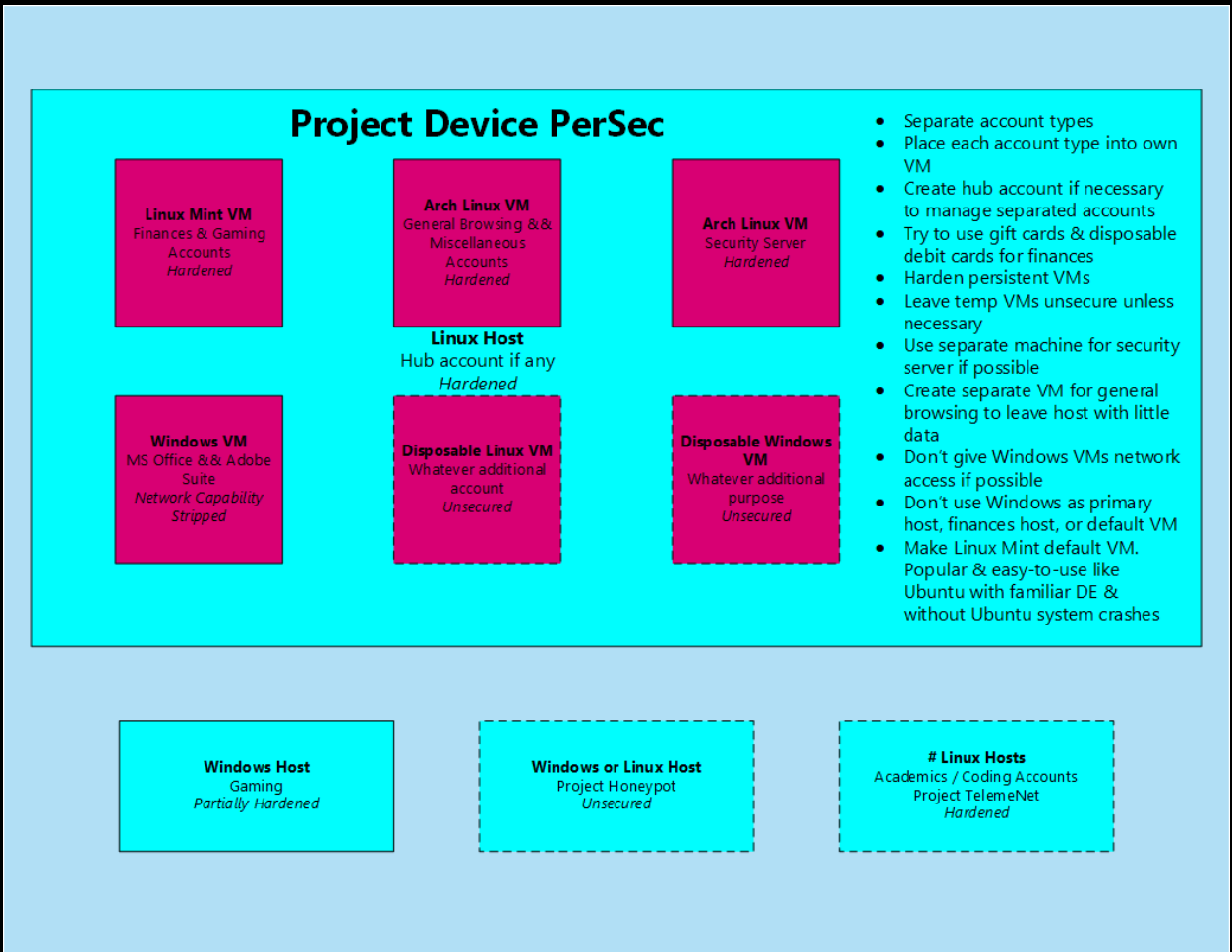
VMware Workstation is just one of many of VMware’s products. Unlike VirtualBox, VMware Workstation is neither free nor open-source, but it is a professional-grade hypervisor. It can be used on Windows and



Linux. VMware Player is free, but lacks the features VirtualBox has so the best option for trying to spend nothing is VirtualBox. Otherwise, choose VMware Workstation or any one of VMware’s greater products. VMware can sell commercial licenses and has well-established third-

party development and distribution programs. If your intent is to use Windows or Linux as your host OS, use Linux and Windows as your guest OS in your VMs with better networking capabilities and more features, and spend over $200 to do so, then this might be the better choice for you. I haven't used VirtualBox in several years and I don't plan on going back. The last time I did, the networking capabilities proved loo limited to make use of, but I use VMware for a lot more than PROJECT DEVICE PERSEC.

PROJECT DEVICE PERSEC



Qubes OS is the easiest alternative to this project, but if you're new to Linux, you may want to put off testing Qubes OS until you have a decent amount of experience. It will be covered further in SYSSEC under Other Linux.

01) Switch to a Linux host if it's not already your host.
02) Create a list of accounts and services you currently use.
03) Categorize list of accounts and services by type. For example, Chase and Amazon are financial-related services and should be separated from Facebook and Twitter accounts.
04) Download and set-up virtualization software.
05) Create and configure VMs for each account and services category.
06) Configure guest OS of VMs by diagram or own use.
07) Create new, encrypted email addresses for each category.
08) Separate previous accounts and services to new addresses. **Never log onto accounts on a VM that isn't the specific VM type.**
09) Delete accounts and services not separated and delete email account from which the other accounts were separated. For example, if a single Gmail account was used to house all account types and account types were separated to ProtonMail, then delete Gmail account once separation is completed.
10) Create additional, secure VM for general browsing to keep data off of host.
11) DO NOT LOG ONTO ACCOUNTS VIA HOST.

FINANCES

Finances are always going to be a huge issue with PERSEC regardless of whether or not we can get you to stop posting PII to social media. It requires constant awareness and management. It’s best to never use your banking information where applicable and never accumulate an unmanageable amount of debt. Use cash when you go to restaurants since waiters and waitresses use your card outside your proximity. Use gift cards wherever possible so you never build up a profile on you on the services you use and the products you buy. You can grocery shop with gift cards, buy mobile apps, games, eat at restaurants, buy clothes, etc. They’re great at being disposable cash in card form. Wherever you manage your finances, remember these three principles: avoid managing finances online or through your phone, do not use mobile banking apps whatsoever, and, if you going to manage your finances online, then get a separate computer or create a VM with an account separated from all of your other accounts to conduct your management. Contrary to the anti-online banking principle, you should engage in paperless billing. There’s no real form of secure billing without moving to an advanced level of PERSEC with shell corporations, moving your assets to your shell corporation, and using mail drops over P.O. boxes. However, paper bills are a larger vulnerability to your privacy and security

than paperless billing. For whatever paper billing you have, destroy what's no longer needed with a cross-shredding paper shredder, soaking in water, or burning. I suggest the first and last for best results, but try not to use shredding alone since it still leaves a trail.

BANKING APPS

We'll cover why you shouldn't use mobile computing over desktop computing in SYSSEC under Mobile, but it's essentially that mobile OSes are not as secure as desktop OSes. Some of the banking apps have ridiculous permissions to use them such as being permitted access to your camera or microphone. Some permissions make sense, but others are just intrusive. While there are means of changing app permissions, which will be covered in SYSSEC under Mobile, it's still an unnecessary vulnerability that's on the one device that we seem to destroy all PERSEC, SYSSEC, and NETSEC principles. If you must bank online, don't use SMS text alerts or banking apps. They may be convenient, but they're dangerous and can be intercepted. The last thing you need is some snooping party to collect your login credentials and wipe your accounts because you wanted to check your Chase balance really quick on the Starbuck's Wi-Fi.

GIFT / PREPAID CARDS & CASH ----------

These options are your best friends and you don’t even know how awesome all three can be when combined. Case in point, prepaid cards often require some other card to purchase it so it can be authorized. Did you know that if you wanted a $500 prepaid card that you could put $504.95 on a grocery store gift card, purchase the prepaid card placing $500 on it, and use the $4.95 to activate the prepaid card? It

requires two transactions and less than 5 minutes. I will advise that you should only use prepaid cards when you can’t use cash or gift cards. One such case is with your VPN provider. If you can’t use Bitcoins, use prepaid cards. However, make sure each prepaid card is

single-serving only. Don’t purchase a VPN subscription and then use the card to purchase Steam games. That links the VPN account to your gaming account. Your use for prepaid cards should be rare so your management of your cards should be great, otherwise you jeopardize the very anonymity you’re trying to achieve.

Cash is your best friend for all in-store transactions, except be wary of how much you carry on your person because law enforcement will seize it under civil asset forfeiture under the assumption that the money is for drugs regardless of guilt or your record. They need a new Magaritaville since the last one doesn’t come with a salsa dispenser.

Actually, you shouldn’t carry a lot of cash on you for a lot of reasons, but the previously mentioned is the most perverse reason yet. Instead, use gift cards. Most major retailers have a gift card of some sort and most large grocery stores carry an assortment. You can especially use grocery store gift cards to buy other gift cards that you may not want traced back to you if you couldn’t use cash to do the same. I suggest experimenting with what disposable plastic can buy what.

BITCOINS

Bitcoins are another form of anonymous payment, but aren’t as easy as using prepaid cards. Bitcoins are a well-known form of cryptocurrency using blockchains to store the public ledger of transactions. It’s a virtual, decentralized currency that can be mined in return for

processing power to verify and record these transactions. However, it’s not as beneficial to mine these days as it has been in the past. There are a few rules I’ve come across when dealing with Bitcoins since, like everything else in PERSEC, it only takes one wrong move to unravel your anonymity.

- Sell items online & accept Bitcoins to build a collection
- Purchase Bitcoins in face-to-face transactions
- Mine Bitcoins
- Use ZipZap to purchase Bitcoins with cash at participating local businesses & create a new, disposable email address with each purchase
- Use LocalBitcoins to buy or sell Bitcoins like it’s Craigslist
- Do NOT use traditional Bitcoin exchanges
- Use a disposable laptop, TAILS, Tor, and a public network for creating a Bitcoin wallet, then verify your IP is addressed without DNS leaks, download Bitaddress, and disconnect your Internet connection to create a Bitcoin wallet without safely
- Use services like Electrum for off-site Bitcoin wallets
- Use Bitcoin sharing & mixing services to destroy potential trace back to you since each transaction is stored in blockchain
- Use a VPN on whatever system on whatever network and not TOR to make purchases online using your Bitcoin wallet

There are other types of cryptocurrencies, there are lists of places that accept Bitcoin that you can research, and there are more, extensive rules to Bitcoin use beyond these basics. I will say that using Bitcoin to purchase VPN subscriptions is probably easier than using prepaid cards to do the same after you've become experienced with both methods.

FULL DISK ENCRYPTION

You've read me mention AES256 several times. Let me explain its importance in the shortest description I can imagine. Until quantum encryption exists, AES256 is impossible to crack. All the computers in the world attempting to crack AES256 using a strong password would take myriad lifetimes. Don't misunderstand me. This chapter exists for a reason. AES256 might be uncrackable, but you're the biggest vulnerability to any one system out there. Follow PERSEC and you might deserve your security and privacy yet. Another aspect discussed will be FDE, or full disk encryption. It's used for securing an entire drive unlike system partition encryption. System partition encryption only encrypts the system partition and not the other partitions created by the OS or user during installation. For Windows, this means the restore and recovery partitions are vulnerable to attack. For Linux, this means the swap partition is vulnerable to attack. FDE takes care of this issue for almost all partitions. The boot partition is not encrypted by either system partition encryption or FDE so they it's always vulnerable to attack. However, by moving the boot partition to a separate drive, you *can* have actual FDE and a fully secure OS. PROJECT LINUX INSTALLATION and PROJECT WINDOWS INSTALLATION will cover FDE setup for Linux users and Windows users.

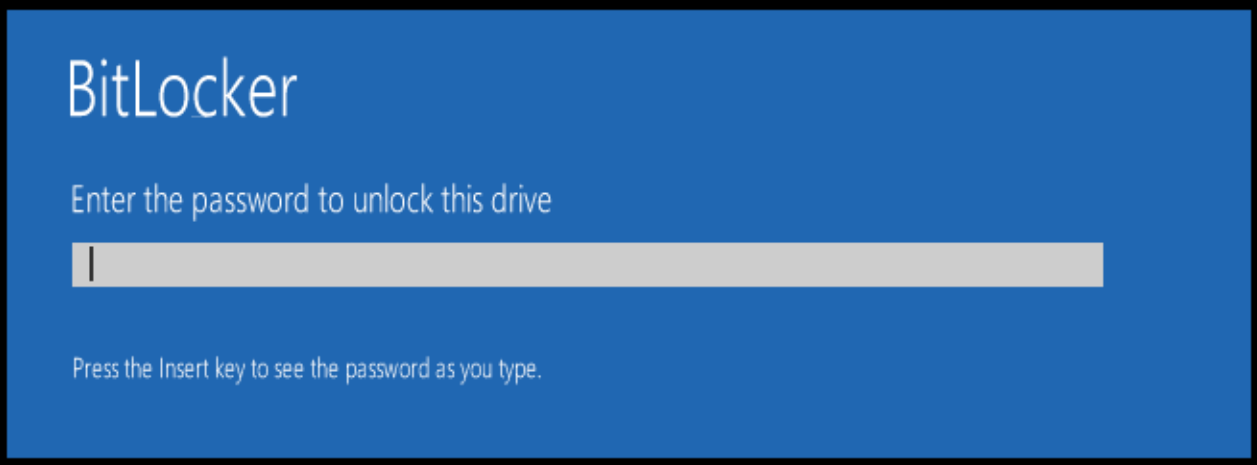
DM-CRYPT

DM-Crypt is not a downloadable tool or, I should say, is not a tool you should download. It comes pre-installed in the Linux kernel and DragonFly BSD. The BSDs are Unix-like systems like Linux, but we won’t be covering any *nix system outside of Linux. DM-Crypt is employs FDE, or full-disk encryption, partition encryption, RAID encryption, logical volume encryption, and file encryption using LUKS, or Linux Unified Key Setup, encryption. However, our focus is on FDE. The other aspects have a learning curve you won’t be able to obtain anytime soon (I sure still haven’t). The FDE option is extremely easy though since it only involves a few mouse clicks, but some operating systems are easier than others. Arch and Debian have less-that-easy installation processes, but Linux Mint and Ubuntu make it difficult for a new user to make mistakes. You will be asked during the installation after it detects what operating systems are on the drive selected if any if you want to install the OS normally or with encryption with LVM, or logical volume manager. If you choose to install with encryption, the installer will bring you to a partition editor where you can create, delete, and / or resize partitions. I suggest creating separate partitions for /tmp and /home. Don’t forget to add a swap partition if it’s not already listed. I also suggest moving the boot partition to a UFD, or USB flash drive, that you can hide so you can keep attackers out from all avenues.

BITLOCKER

BitLocker is an FDE and partition encryption tool for Windows systems like DM-Crypt is for Linux and it too comes preinstalled. The only issue is that it’s only fully available in Pro and Enterprise versions of Windows. It uses CBC, or cipher block chaining or XTS mode with 128- or 256-bit keys. BitLocker has three authentication mechanisms: transparent operation mode, user authentication mode, and USB key mode. Transparent operation uses a TPM, or Trusted Platform Module, chip to decrypt the system, but is vulnerable to cold boot attacks. User authentication mode uses pre-boot authentication with a PIN or password. USB key mode requires a UFD to be entered during pre-boot to unlock the OS. This isn’t the same as the USB idea previously mentioned in DM-Crypt or in PROJECT LINUX INSTALLATION, which moves the bootloader itself to a UFD. The USB Key Mode for BitLocker is a security key like Yubikey but on any UFD of your choice. Another issue with BitLocker is that, if you have a Microsoft account set up on your Windows system, Windows will store a copy of your encryption key on OneDrive. The reason for this is to help you decrypt the system in case you forget the password, but it’s safe to presume with all the heavy telemetry settings and strong partnership with NSA that this is not the only reason. It will be discussed further in the SYSSEC chapter under Windows, but you really shouldn’t set up your Windows system with your Microsoft account or have a Microsoft account for

that matter. If you choose to set up Windows with your account anyway, use BitLocker to encrypt your system, and you don’t want Microsoft to have the encryption key, you can delete the link to the recovery key in OneDrive and use CMD to generate a new recovery key.



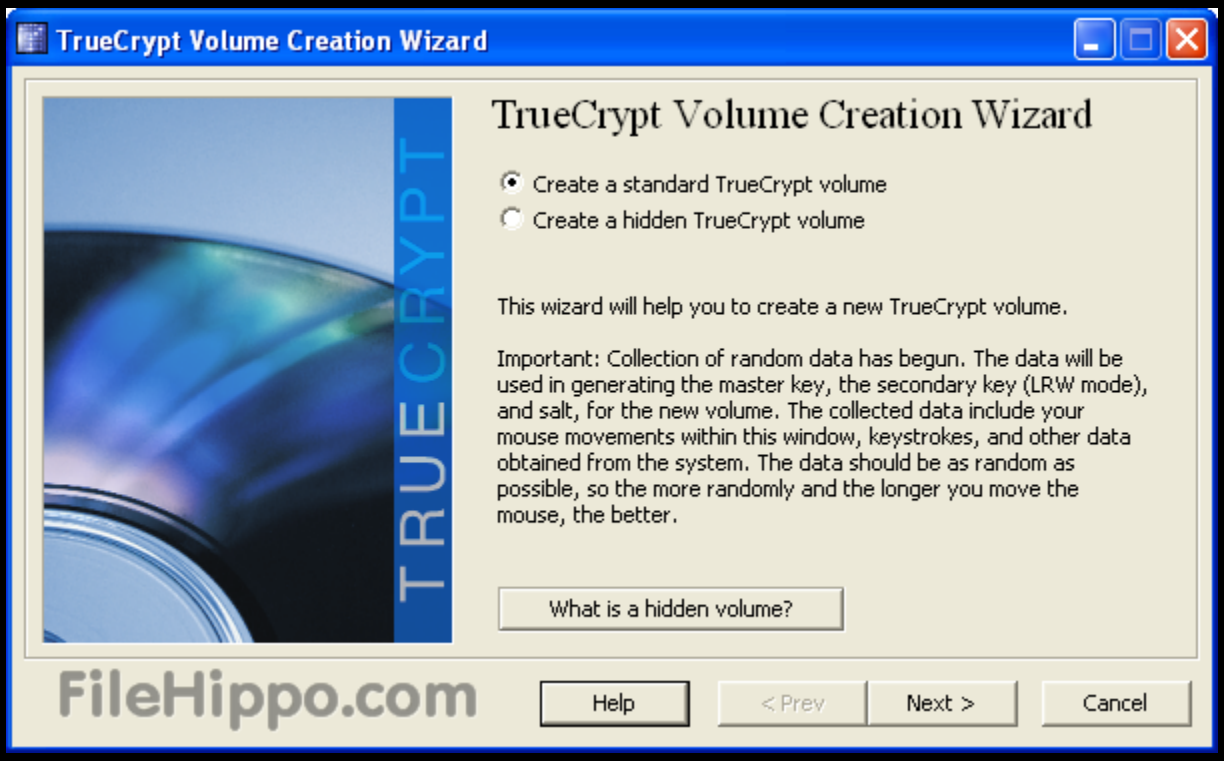
PARTITION ENCRYPTION

Partition encryption is the encryption of each portion of a storage drive. Systems usually only have their own system partitions and require the user to modify the system partitions to create a new partition, unless a system with more than one drive is being used. Such partitions are generally made to sort data by type onto any partition but the systems that 1) data isn’t lost when the system dies and 2) the data can be accessed by more than just one system.

TRUECRYPT

TrueCrypt has been a widely-used and recognized partition encryption software up until sometime after the Snowden Revelations. It used on-the-fly encryption with AES256, Serpent, Twofish, or any combination of the three in any order as well as SHA512, SHA256, and Whirlpool hash algorithms. It supports Windows, OS X, Linux, DragonFly BSD, and Android and uses CBC and XTS modes like BitLocker. One reason why TrueCrypt was popular was the creation of hidden partitions. You could create a normal, outer partition with weaker encryption and a weaker, unique security key a hidden, inner partition with stronger encryption and a stronger, unique security key. The hidden partition takes longer to decrypt since entering the password for the hidden partition has to decryption the outer volume first. The reason why you would want to do

this is so that, when made to decrypt by whomever, you could decrypt the outer partition without having to expose the files in the hidden partition. There's only one way of knowing if there's a hidden partition and it's up to you if you want to risk it being found or you



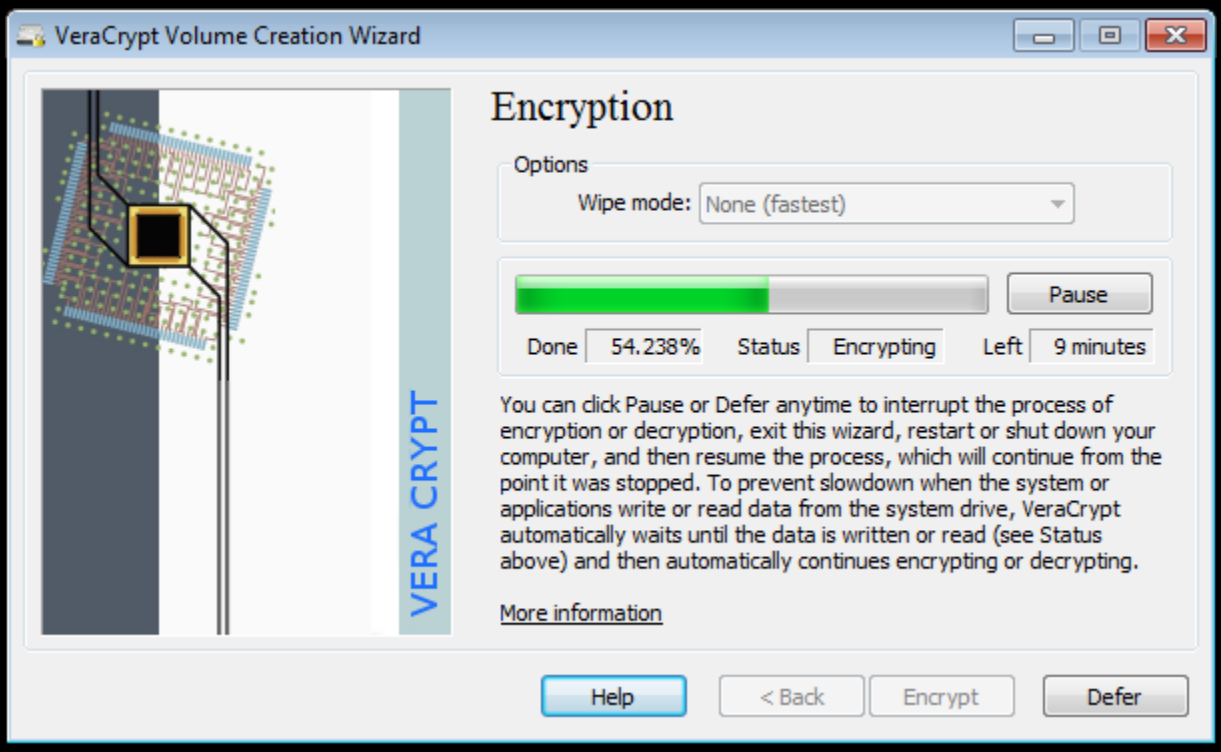
losing your files. An attacker or law enforcement or whomever can write data to the outer partition, which would either expose that a hidden partition exists when it can't fill the outer partition completely or would overwrite the inner partition. The latter depends on whether or not you set TrueCrypt to allow the inner partition to be deleted when someone attempts to fill the outer partition fully. Before its support was discontinued, TrueCrypt developers were attempting to get full Windows 8 support, command-line use, and to encrypt system partitions on UEFI when only BIOS was supported. With

that said, TrueCrypt wasn’t just used for data partition encryption but system partition encryption as well. You could set it up to encrypt your current Windows system or create a hidden Windows system, which would delete your current system. How the latter works is that in creates a dual partition system just like the outer and inner volumes over standard partitions. You would have to install one copy of Windows on the outer volume and another copy of Windows that you would actually use on the inner volume. TrueCrypt support was killed suspiciously with stating that TrueCrypt is very vulnerable, releasing an update that only allowed users to view partitions and not create new ones, and advising switch over to BitLocker. Gibson Research Corporation decided to complete an audit of TrueCrypt to view whether or not it was insecure or not. It was found to still be secure at the time so it just adds to the suspicion. Regardless, there were several alternatives based directly off of TrueCrypt with added security and support such as VeraCrypt and CipherShed. TrueCrypt also has command-line use alternative under Linux and DragonFly BSD called tc-play.

VERACRYPT

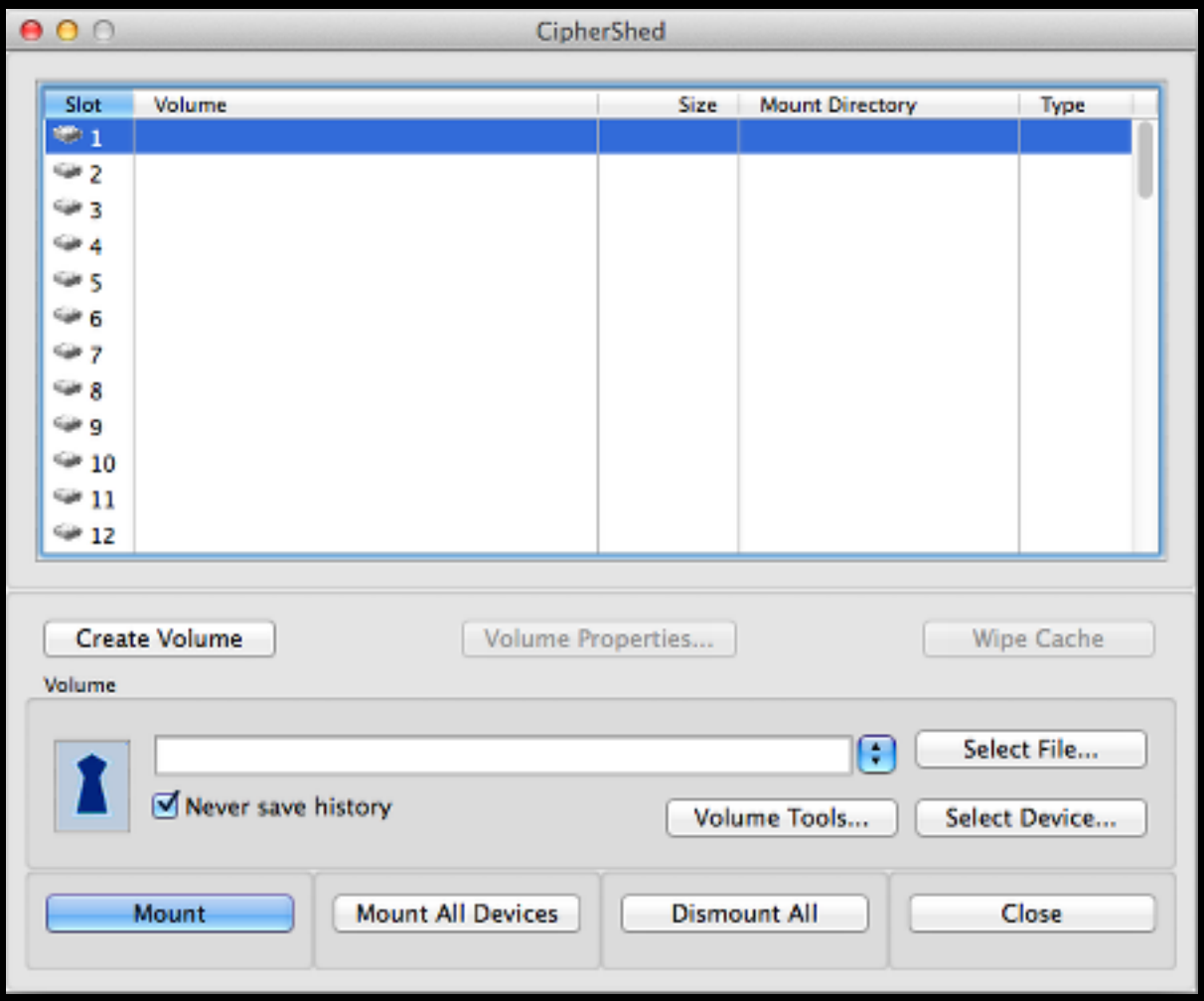
VeraCrypt has been called the true child of TrueCrypt, but is only supported on Microsoft, OS X, and Linux and with command-line support. It’s included added technical, security measures and the developers are attempting to add UEFI support. However, they have stated that they will never bother to support *nix systems for hidden, system

encryptions. Two phases of an audit already completed showed no malicious code or vulnerabilities. Apart from the aforementioned, it's identical to TrueCrypt, thus why it has earned being called the true child of TrueCrypt.



CIPHERSHED

CipherShed is an incomplete fork of TrueCrypt, yet maintains Windows, OS X, Linux, DragonFly BSD, and Android support. However, it lacks on-the-fly encryption. It's still in development, but worth noting since its planned to support DragonFly BSD and Android unlike VeraCrypt.



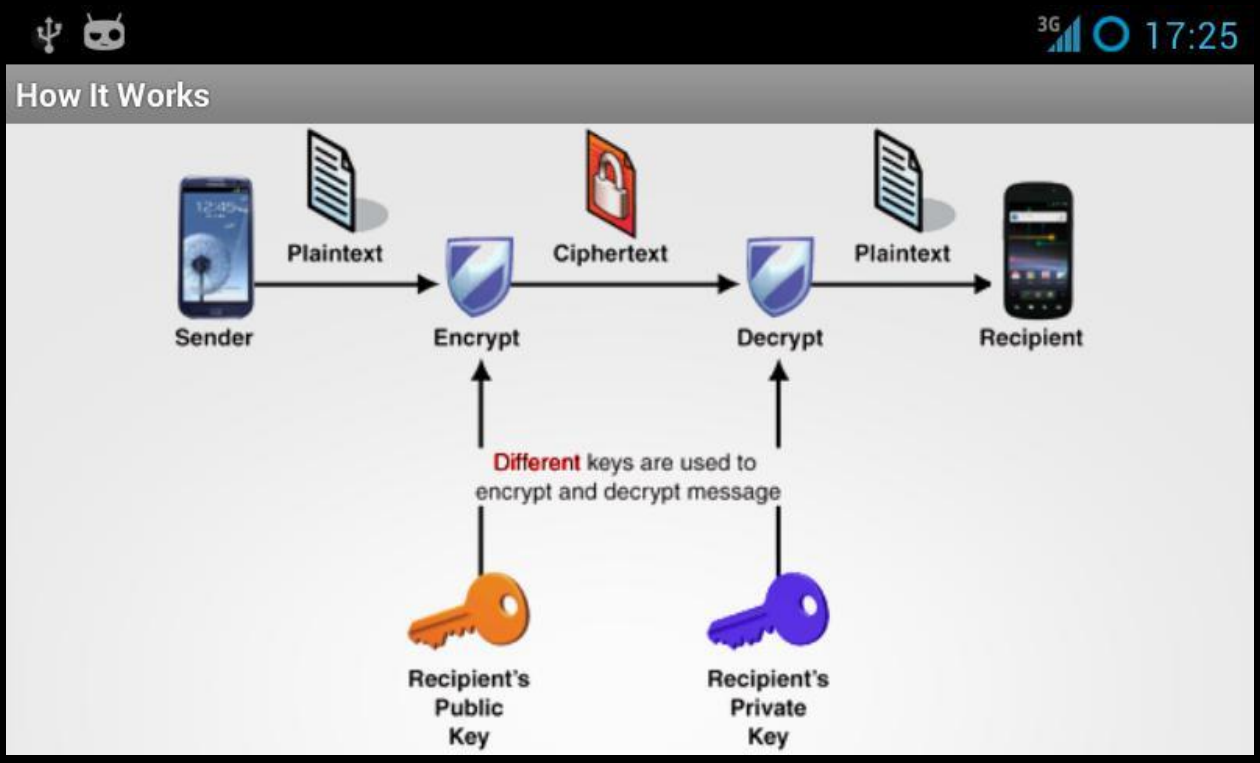
DOWNLOAD & INSTALL VERACRYPT

FILE ENCRYPTION

Next is encrypting files themselves and not just the system and partitions on which they can be found. Any file that is a file can be encrypted. A folder has to be compressed into any compression file like a zip in order to be encrypted.

PGP / GnuPG ----------

PGP is Pretty Good Privacy. It’s a data encryption / decryption tool for digitally signing files of all sorts, especially email, and was created by Phil Zimmerman. Due to copyright issues, it led to the creation of OpenPGP. While Symantec now owns PGP, there is a widely-used and recognized, open-source alternative called GnuPG, or GNU

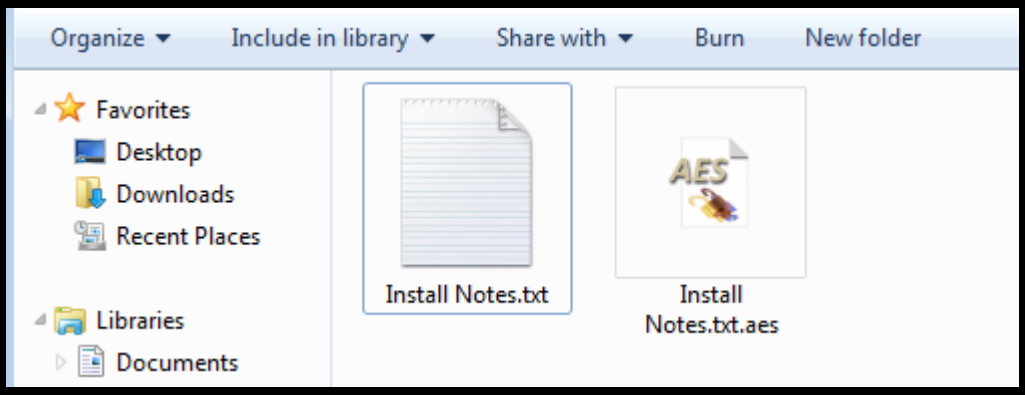


Privacy Guard. While GnuPG is Linux-focused, it’s cross-platform with different names per OS. It’s called GPG4Win for Windows, iGolder for web, and MacGPG on OS X; it’s still GnuPG on Android since Android is based on Linux. If you want to encrypt your emails without using an encrypted email service provider, want to encrypt your files, or you want to use pwd.sh, then you will need to install GnuPG (or any alternative for files like AES Crypt). GnuPG is just the CLI (command line interface) form though on Linux. In order to have a GUI (graphical user interface) on Linux, you need to install the appropriate package for whichever DE (desktop environment) you’re using like Seahorse for Gnome or KGPG for KDE. It’s revered for its functionality and support across numerous services. It’s works with the Enigmail mail extension on Thunderbird, Firefox, Chrome, and SeaMonkey, email clients like Thunderbird, KMail, Outlook, Evolution, instant messaging services like Psi and Fire, secure file signatures in place of hashes, and more. You already hear about PGP anymore since Symantec bought it, but OpenPGP standards still exist that keeps the name in our minds. Otherwise, it’s GnuPG.

AES CRYPT

AES Crypt is another favorite encryption tool of mine and it’s solely for using AES256 on files. It cannot encrypt a folder, but it can encrypt a zip file so just compress whatever folder you want to encrypt. It supports Windows, Linux, OS X, Java, C#, and Andriod, but

it’s called Crypt4All on Android. It can be used via CLI, but it’s mostly supported to be used by side-clicking any file and selecting

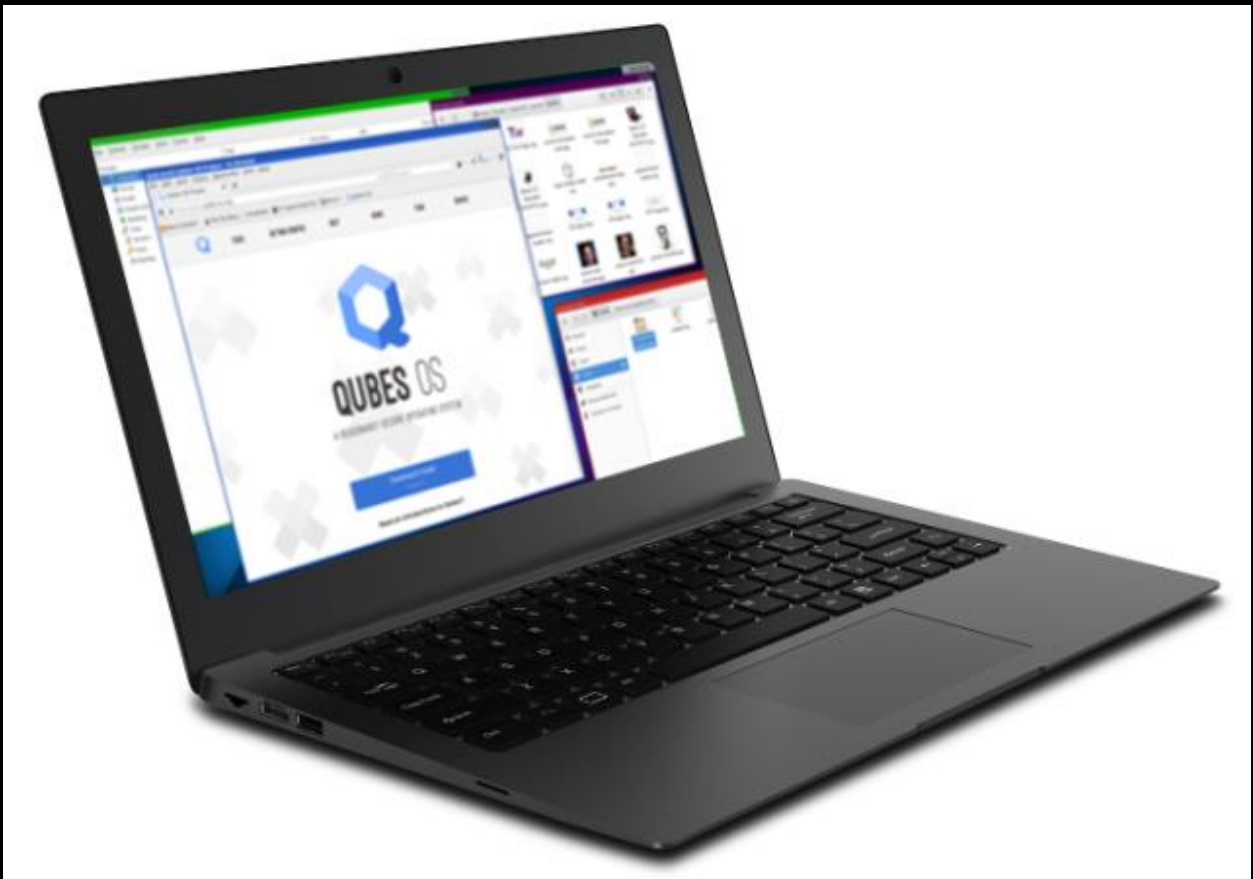


AES Crypt from the menu of options. Doing this will bring up a window prompting for password to encrypt the file. You can set the file type to open AES Crypt by default, but it’s not recommended. As previously stated under Self-Created Safe under Passwords, using AES Crypt will generate a new file. It would appear all file encryption tools do this in case you still need the plaintext file on an error occurs during the encryption process. While I don’t recommend setting AES Crypt to be the default tool to open any editable file, the .aes file created does open AES Crypt by default as would be expected. Don’t lose your password.

DOWNLOAD & INSTALL AES CRYPT

SYSSEC

SYSSEC is system security. This is one of the most talked about forms of security, especially with anti-malware products. EMSEC has been dropped from this guide since it’s difficult for attackers to use side channel attacks against your CPU electromagnetic radiation within your proximity and since it’s as easy to thwart as purchasing a metal case for your desktop and metallic laptops. The best examples of BASEC-approved, metallic laptops are the Librem laptops by Purism. If you’re



a Mac user, you’re already used to paying for overpriced hardware, but

the Librem laptops are actually secure and Purism actually cares about security. Purism has partnered with independent hardware developers to build and compile hardware that respects the users' privacy, security, and freedom without enabling, let alone building, spying features. I recommend it used with Qubes OS, especially as the system you use if public if you do so. Qubes OS will be covered later in this chapter under Other Linux.

Before we delve into operating systems, we first need to cover automation, maintenance, physical security, and anti-malware. There's a lot to go over with operating systems, but you should make your choices based on as much as the tools used to ensure SYSSEC as the operating system themselves and the developers' philosophies. System hardening can go a long way, but it's a lot easier to do on *nix systems than the draconian Windows ecosystem.

METAPOD

AUTOMATION

Automation plays a huge part in how we use our systems. After all, the way we develop computers is to make our lives easier by handling mundane tasks that could otherwise be automated or simplified. We wouldn’t need a computer to solve great logical problems if we could do the same with a pen and paper. IoT, or Internet of Things, exists for just this purpose, but there’s no use in tackling that security mess until the basics of security are understood. Instead, let’s focus on the automation tools that exist already on your systems and how they could be used.

CRON

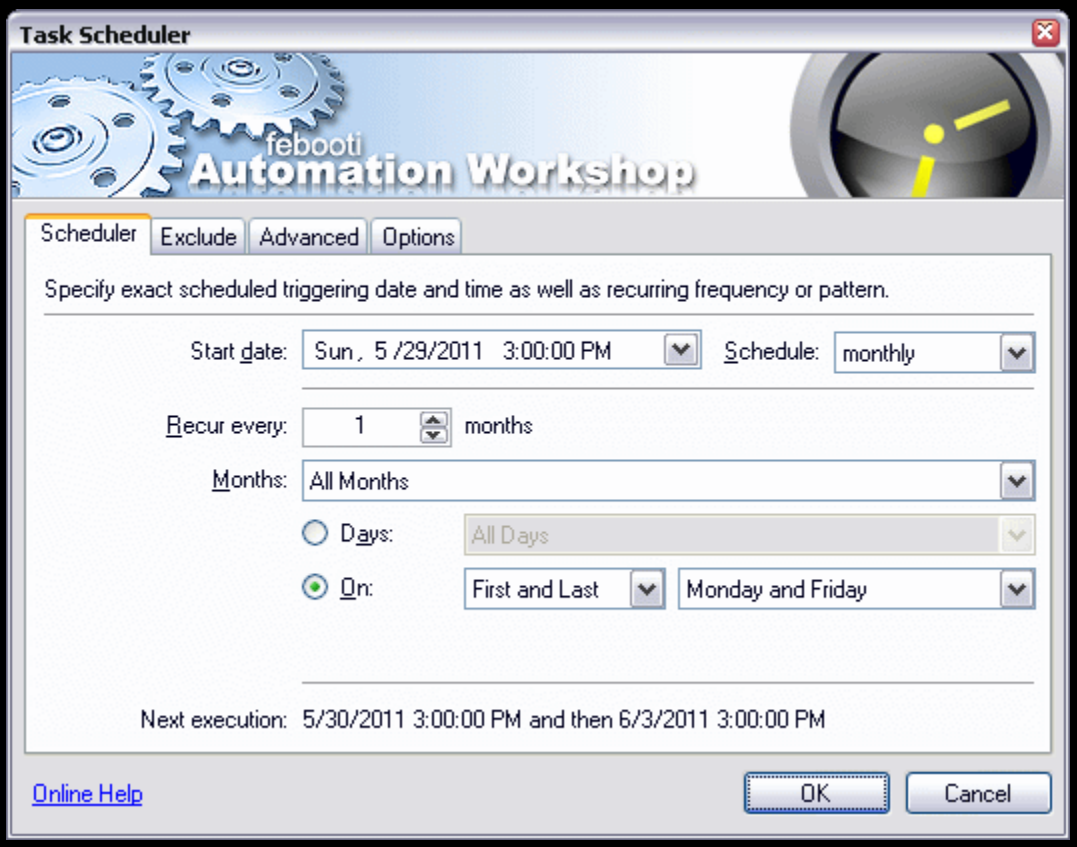
Cron is a great automation tool preinstalled on Linux systems to run commands and / or scripts based on time including hour, minute, day, month, and workday. It’s accessed by opening a terminal and entering “crontab –e” without quotes, but trying to edit the crontab file under /etc does nothing since Cron will create its own crontab file. Scripts ran need their full paths written so “~/SCRIPT” won’t function properly like “/home/USER/SCRIPT” would. If root permissions are needed, then use “sudo crontab –e” without quotes to access the root crontab file without having to enter the same command in the user crontab file with the user’s password. How you enter a time is by

entering data in all five points that appears as “* * * * *” without quotes and with spaces between each point. Only use the asterisks for time ranges you don’t want to specify. For example, I run Bleachbit every night at 11:55, which appears as “55 23 * * * bleachbit COMMAND” in the crontab file. “55” indicates at 55 minutes into the hour, 23 means 11PM since *nix systems use a 24-hour clock, and the three asterisks that follow means day, month, and weekday aren’t specified so the cronjob is run every day. Cronjobs can also be specified to run at certain time ranges and repeatedly without repeating the command. For example, “0,30 0-23 * * 0 COMMAND” runs a command every Sunday every half hour for every hour, which could also be ran with only defining the “0,30” aspect. I don’t use cron to run maintenance and cleaning every night but system updates, powering off the machine for the night, running clamav, setting up Conky configurations, backing up Firefox bookmarks, running BitTorrent Sync to back up data, dismount

encrypted data partitions, etc. By automating maintenance, back-ups, and security tools, you can keep your machine secure with little interaction and Cron is definitely a capable automation tool.

TASK SCHEDULER

Task Scheduler is the Cron for Windows, but comes with a GUI unlike Cron. Actually, Task Scheduler is a lot more feature-rich than Cron by running commands using the same schedule criteria, when a specific system event occurs, when the system becomes idle, when the system is booted, when the user logs on, and more. It can be accessed under the following tree:



Control Panel > System and Security > Administrative Tools > Task Scheduler

The process of setting up a task is even easier here than on Cron. However, like Cron, you’re expected to know commands and scripts in order to make use of certain functions. I have my Windows VM set up to save my Microsoft Office Work at 23:30 and then shut down. If I wanted to run Bleachbit, I would use the easy set-up to configure the schedule to run Bleachbit and then I would enter “bleachbit_console.exe --clean –preset” to run Bleachbit. You’ll have to look into the command for each program you want to run at a specific time.

HAUNTER

DOWNLOAD & INSTALL NETDATA

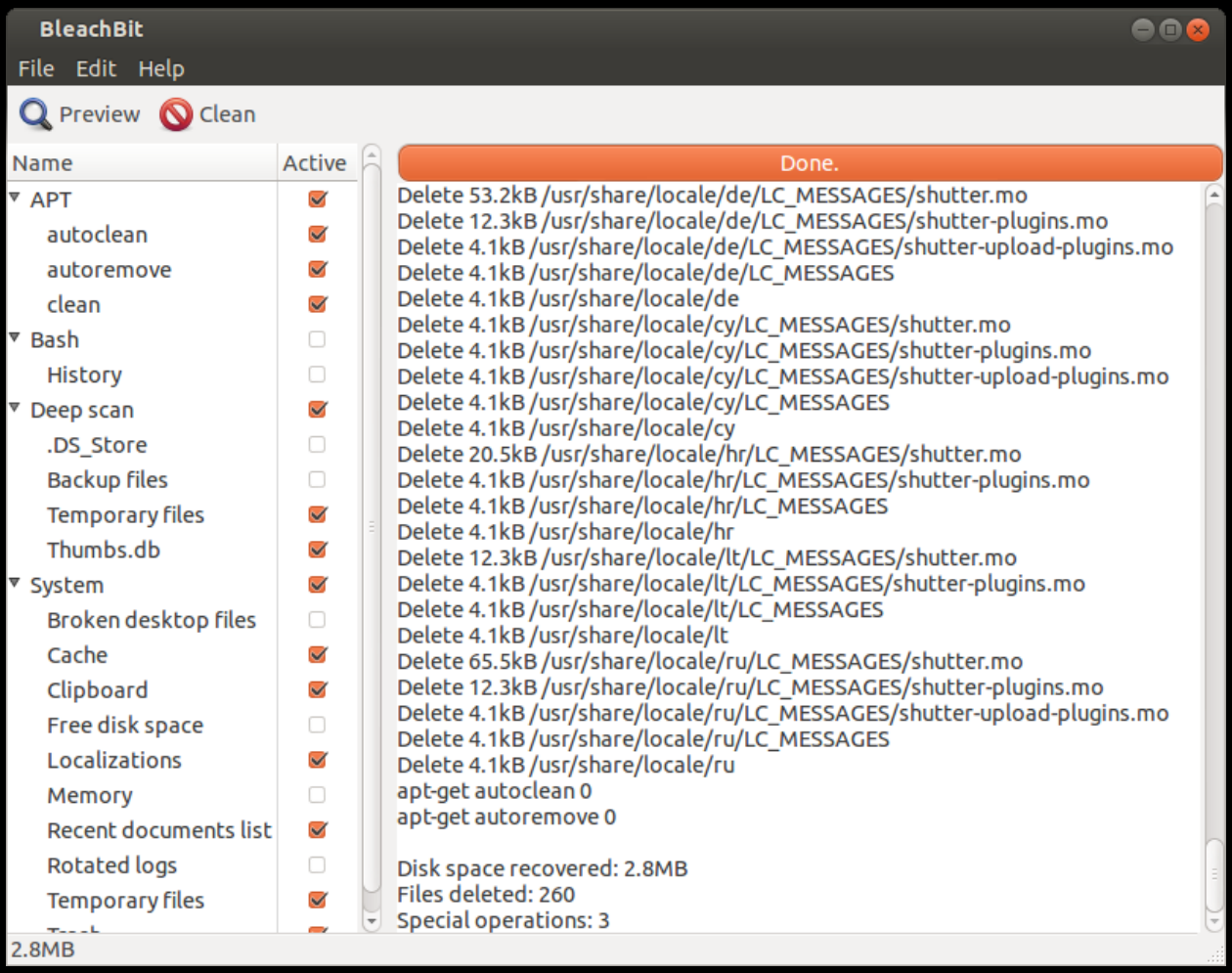
MAINTENANCE

Cache, history, cookies, temp files, etc. are bits of data that should be actively and routinely removed. These files store information relating to your activities that may reveal your digital footprint. It’s best to make sure applications you use never store this information. In the Browser section, with Firefox, I explain my set-up and how no information beyond cookies are saved and an add-on I have to immediately delete cookies. However, it’s not for everyone and some may want to save their browsing history to find a previously-visited link later. Excluding browsers, a lot of our applications create cache that isn’t necessary outside of your current session. There are a few tools that exist to take care of this issue.

BLEACHBIT

Bleachbit exists on Linux and Windows. On Linux, it’s a great application that takes care of a lot of temporary files created, utilizes *nix commands to remove outdated packages, and can be used via terminal (read: you can code it to work in cronjobs). On Windows, it’s pretty good, but it falls short to CCleaner and NCleaner. However, CCleaner and NCleaner lack the options to free disk space by eating up all the free space, grabbing whatever scraps of data it can

find, and deleting the large file to creates in the process. For Windows use, it’s best to use it alongside NCleaner.

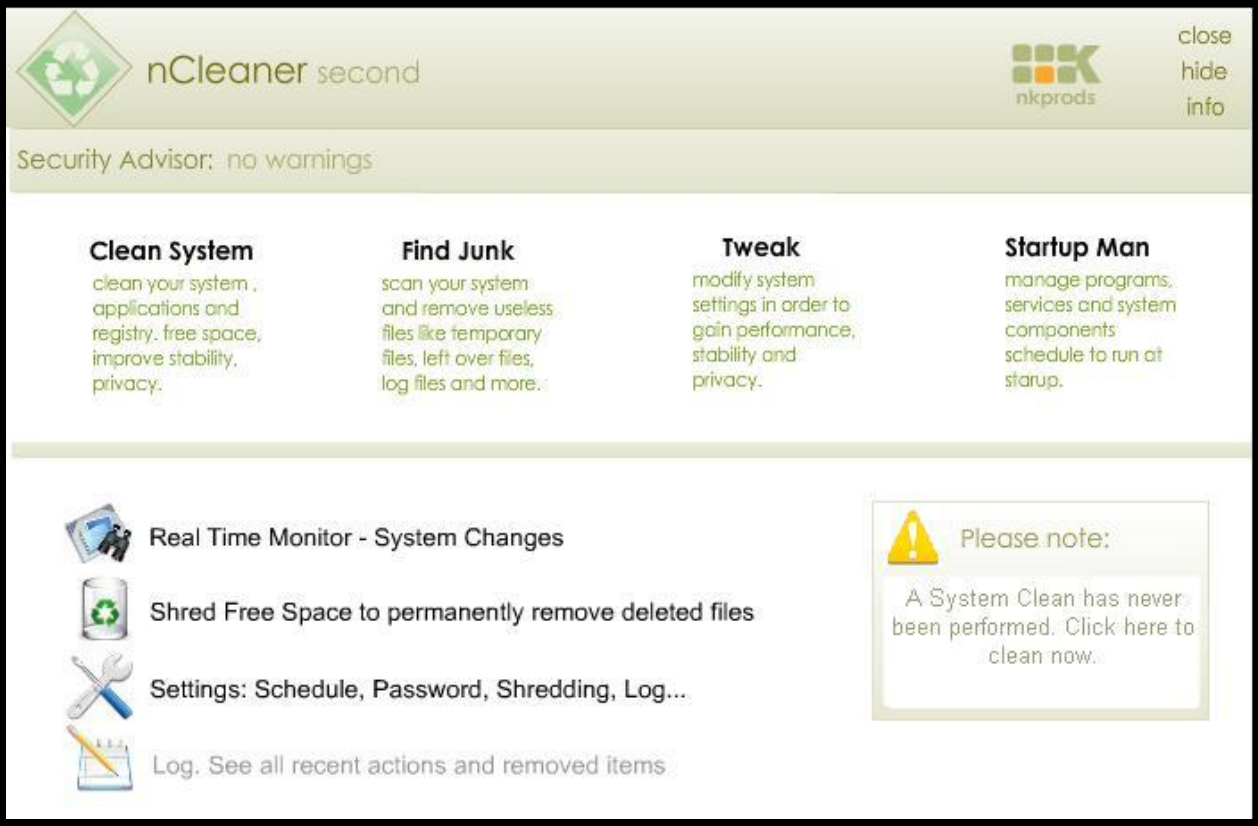


Bleachbit can be customized via CLI or GUI to run certain options. Freeing up disk space is great, but this step can take a very long time depending on your CPU and storage space. A 2TB HDD on an i7-3630 quadcore CPU at 2.4GHz takes several hours. I only use this feature weekly or monthly due to the long time constraint. What Bleachbit can remove includes cache, cookies, form history (auto-fill), passwords, DOM storage, clipboard, recent documents list, memory, trash, broken

files, CLI history, etc. One additional difference between the Linux and Windows version is that the Linux requires two different instances for information it can delete: user and root. Run root first or, if using cronjobs, set the root job to run before the user job. This will be discussed in Cronjobs. Bleachbit can also be set to only run against specified partitions in settings.

NCLEANER

NCleaner exists on Windows only. It's a great cleaning, privacy, security, and management application that blows CCleaner out of the water. It's also a double-edged sword. There are parts of the application that can be adjusted for better management and security of your Windows OS, but it doesn't go into detail for some functions.



While there are short descriptions of each setting, there’s no warning of how changing said setting may break your system if you’re new to the app. I’ve broken BitDefender numerous times from failing to exclude needed files from the “Find Junk” section. Changes in “Tweak” or “Startup Mon” can either be very useful or break necessary system services. Use at your own risk. It’s recommended over CCleaner since it’s a lot more feature rich and useful. Excluding freeing up disk space, it can do everything Bleachbit can and more. It only uses a GUI and it provides a Security Advisor at the top of the app to signal necessary changes needed to be made. Windows applications can also be automated like Linux as specified in Cronjobs. Like Bleachbit, NCleaner can be set to only run against specified drive letters.

GRIMER

DOWNLOAD & INSTALL BLEACHBIT

PHYSICAL SECURITY

Physical security is another large aspect that often goes ignored, but it’s specific to SYSSEC and easy to set up. The first suggestion is to invest in Kensington cable locks to keep laptops, desktops, and monitors from being stolen. If you’re extra concerned, you can always place your systems in locked,

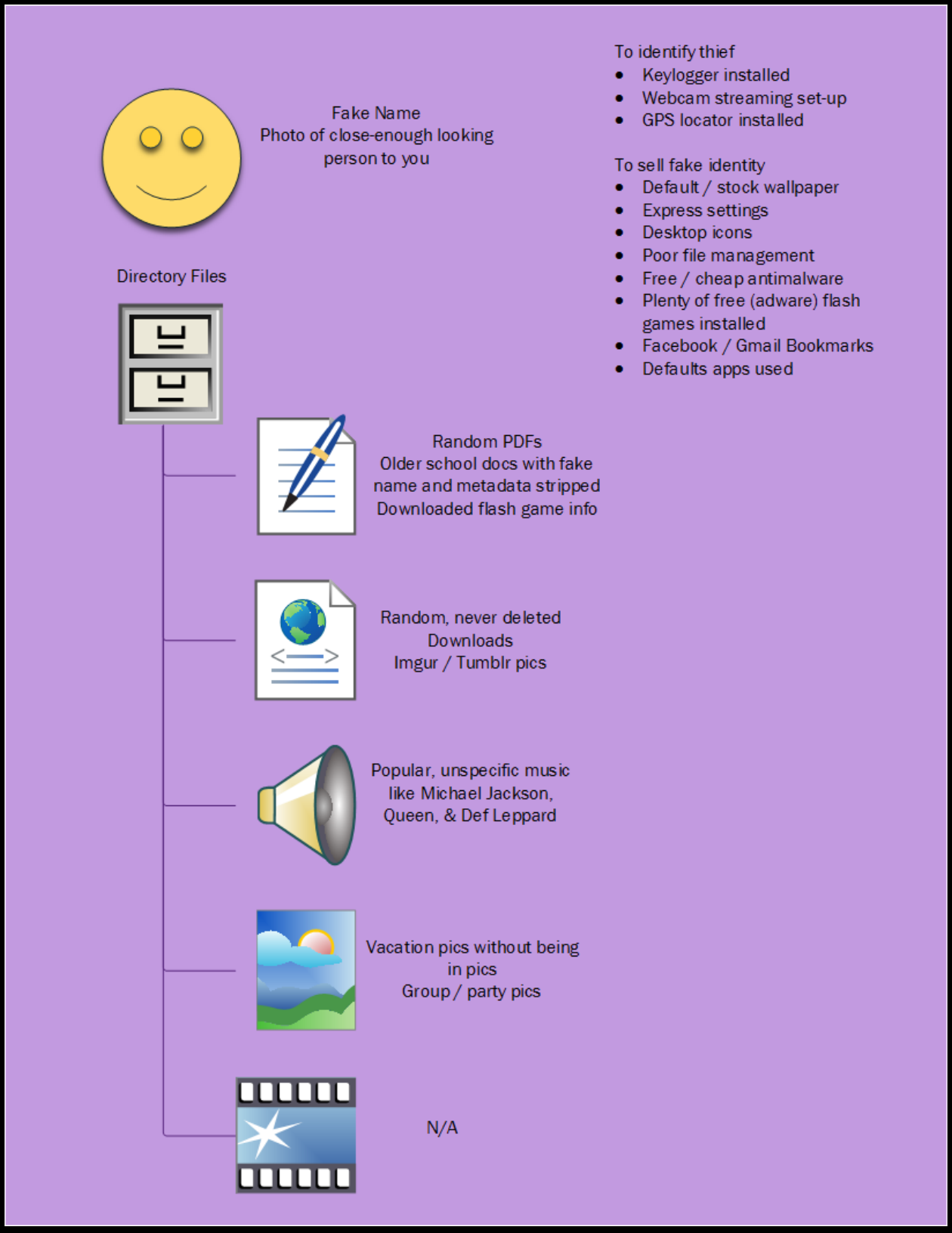
ventilated cabinets. As long as the heat can dissipate, you shouldn’t have an issue. Incognito Toolkit has a few suggestions, of which I’ve modified and added a few, of constantly checking your peripheral cables, placing fingernail polish on screws to see if touched, placing a small scrap of paper into a phone case to see if opened, making markings and engravings to identify your device(s) if stolen, and to install your own keylogger in case anyone else has accessed your computer. The latter piece of advice is the same as the advice for

PROJECT HONEYDRIVE, but Incognito Toolkit’s advice is lacking in two ways. One, if your system is stolen, a keylogger alone won’t help. How would you retrieve the information? You need to add an element of syncing the data to another system or account. The second way is that it doesn’t necessarily identify the thief or attacker. Install webcam recording software too and also have it sync to another system or account. If storage is an issue, have it take photos every few seconds instead of recording video.

Another issue is what to do with systems that are obsolete or otherwise useless. Do not simply throw away or sell the electronics you don’t want anymore. Take out anything with memory and throw it in the microwave or burn it. If you don’t know what memory components look like, research them or throw the whole motherboard with storage drives in the microwave. No amount of reformatting actually works on hard-disk drives. Solid state drives are a different story, but they aren’t fool-proof either. Magnets, wood chippers, endless reformatting, etc. are solutions that aren’t 100% either. If you have access to large machinery like a wood chipper, I suggest smelting your drives instead of grinding them just like I don’t recommend paper shredding since they’re still pieces that can be recovered.

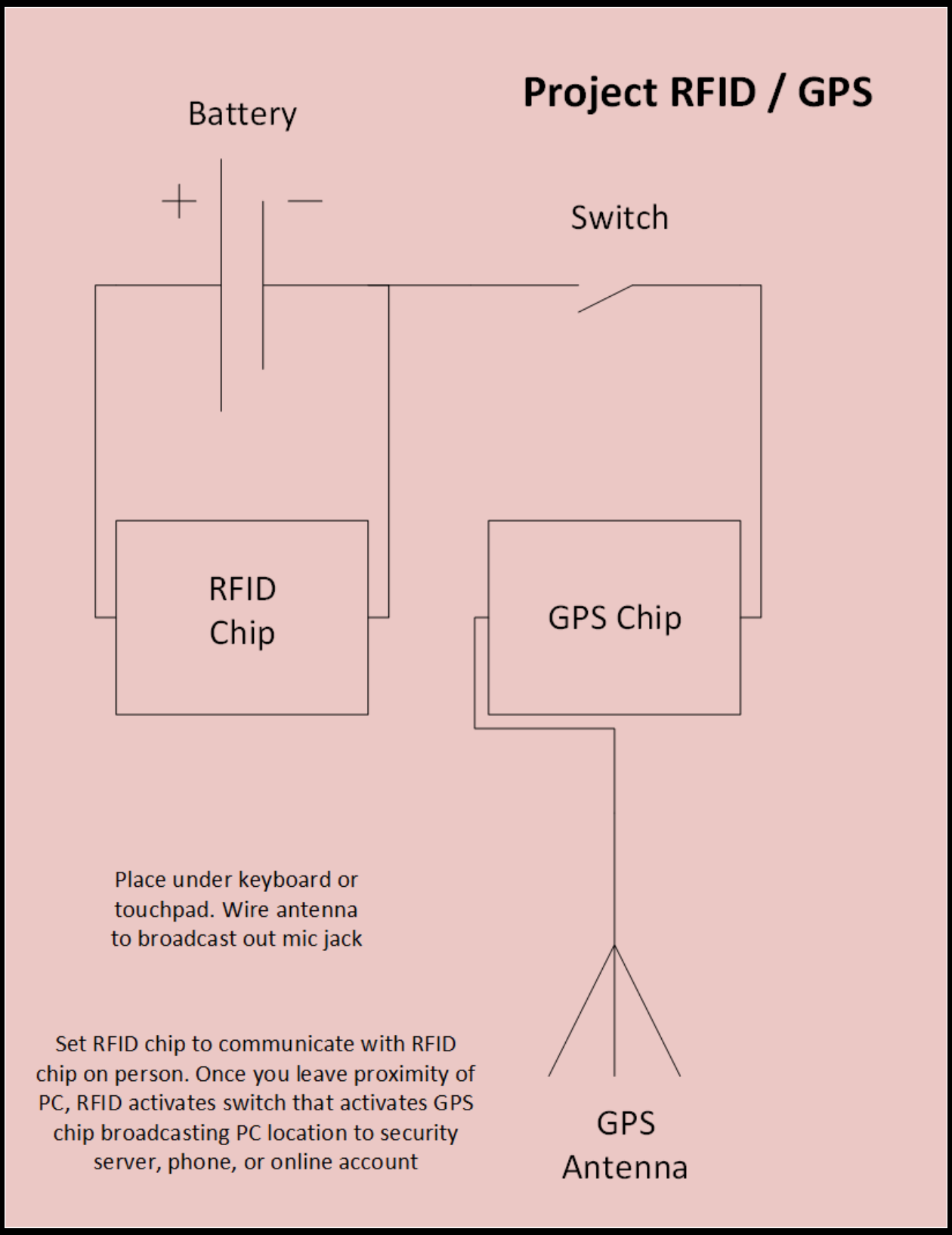
KOFFING

PROJECT HONEYDRIVE



1) Use separate drive to act as honeypot. Laptops with only one drive bay is still possible with replacing obsolete disk drive with removable storage drive bay and storage drive. PROJECT HONEYDRIVE is NOT possible on ultrabooks with only one storage drive and no disk drive. PROJECT HONEYDRIVE is useless if FDE is not used and honeydrive is on the same drive as the primary OS.
2) Keep system and security settings within honeypot at default.
3) Create and implement fake identity with user account.
4) Follow diagram for filling commonly-used folders with junk data.
5) Install software: keylogger, stealthy webcam recorder, and GPS locator. DO NOT RECORD AUDIO.
6) Install and configure means of syncing Step 5 data to security server, a phone, or user account.

PROJECT RFID / GPS



PROJECT HONEYDRIVE only works for dumb thieves that boot the system without removing the drives and placing the drives into a write-blocker. PROJECT RFID / GPS is a conceptual project for stopping smart thieves.

01) Purchase 2 RFID chips, 1 GPS chip, and 1 GPS antenna. You'll need equipment small enough to hide in the laptop. Use a box to conceal everything but the antenna for desktops. If metal case is used for either type, antenna needs to partially stick out to broadcast.
02) Purchase electrical equipment: wire, switch, battery, solder, soldering iron, wire stripper, anti-static wristband, electrical tape, etc.
03) Wire chips, battery, and switch together by the diagram.
04) Configure RFID chips to interact with each other. Set 2nd RFID chip on person. Set 1st RFID chip to activate switch when 2nd RFID chip leaves proximity.
05) Set GPS chip to broadcast to security server, a phone, or user account.

ANTI-MALWARE

Anti-malware and AVs, or anti-virus, solutions are the same thing with a different name for marketing purposes thank to ‘80s movies. This section really only matters for Windows users since Bitdefender on Linux is bad, Avast support on Linux is dead, and the only AV, or anti-virus, solution of note on Linux is clamav / clam-tk and it’s not really needed. In fact, most AVs aren’t essential if you conduct safe browsing habits, but you should still use it on Windows as an additional security layer.

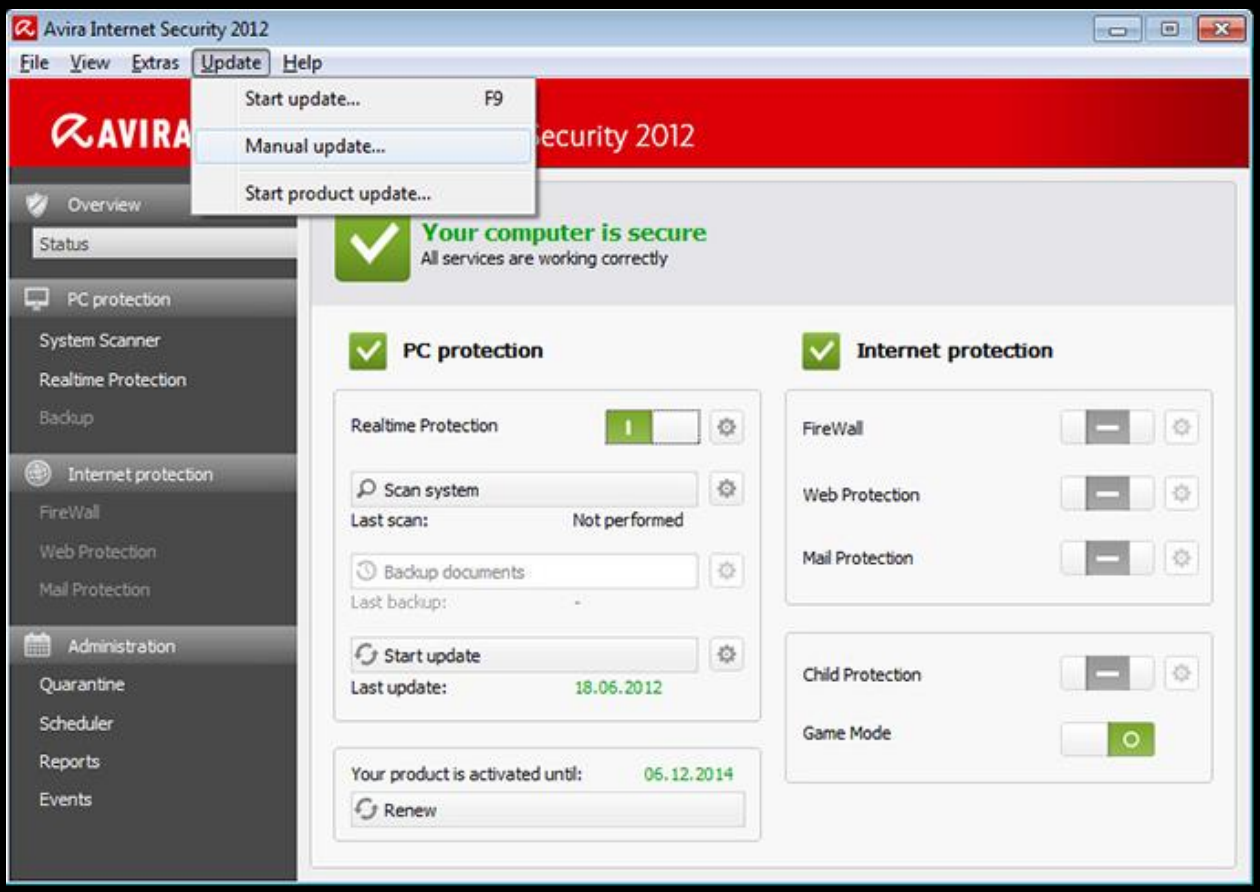
BITDEFENDER

BitDefender is your best security suite option on Windows if you’re willing to pay for it. It’s as equally terrible at catching malware since malware definitions themselves are not great, but it comes with a plethora of security features worth exploiting. One of which is the Privacy feature. You can set BitDefender to stop any networking service from accessing your data based on the data you enter. It’s a catch-22 to enter your PII into this AV and trust that it’s secure and won’t use the data maliciously. If you’ve ignored the Finances in the PERSEC chapter and bought a year license with your banking or credit card, there’s no point in worrying about the suite not having the data you already gave it. However, if you do use it and you have a Google

account with your actual PII set up, you'll love how many notifications you'll get about BitDefender blocking Google. Another great service is the app firewall built in that blocks certain apps from the network. Microsoft Office doesn't need Internet access. I suggest trying to use it to block whatever telemetry services on Windows 10 that you can that were on the apps you couldn't or wouldn't delete. Their latest feature includes a vulnerability scan too! The security settings you can play with are very simple and straight forward. I've only mentioned some of the security features, but professional reviews constantly state how it destroys the other competitors.

AVIRA

Avira is your best free option for anti-malware security on Windows. Avira has finally been worth recommending to everyone. It was the most powerful AV, free and premium included), but it ate resources making systems unusable and had an older design that left many questioning whether it was a legitimate AV. For a while, Avira was updated with a lighter, sleeker design, but it was ineffective at removing malware

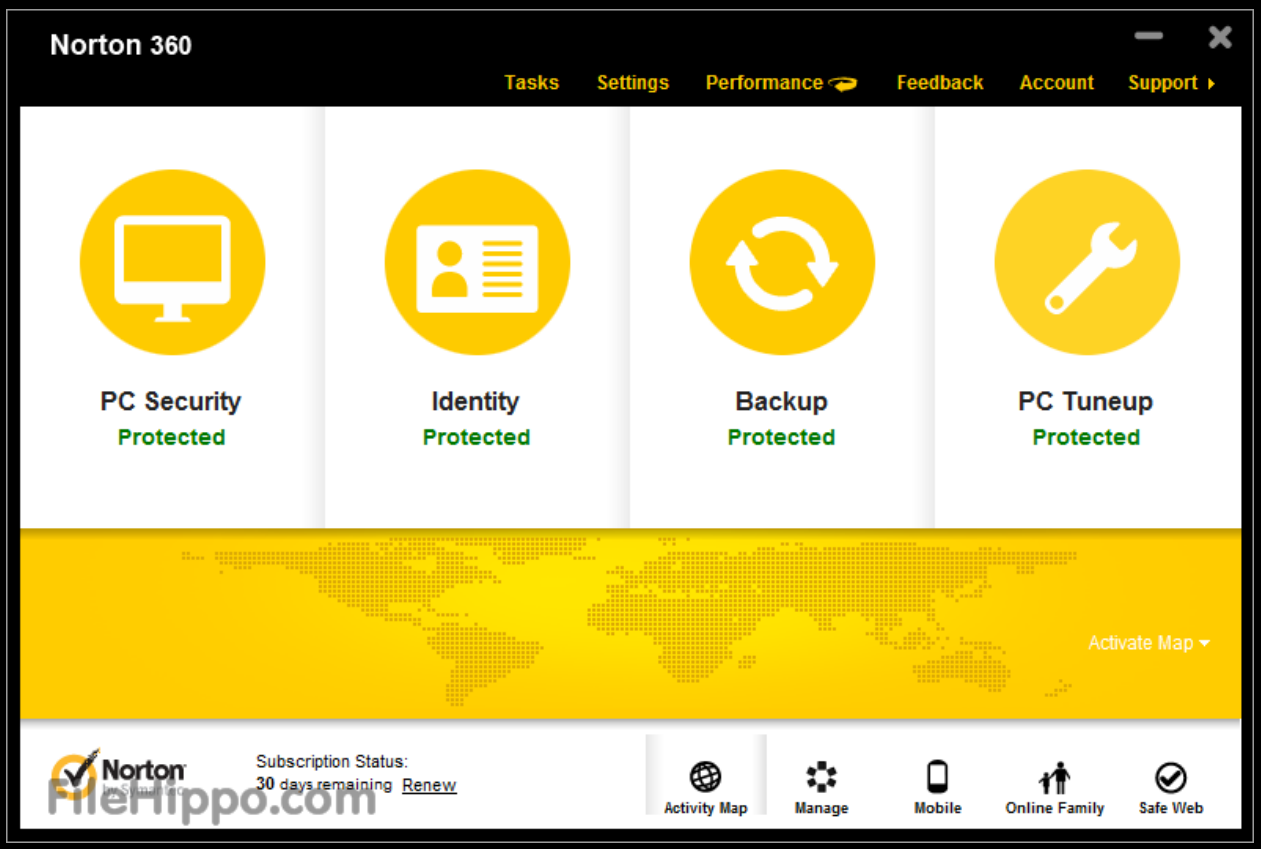


like a Norton clone. Now it’s circled back and has been greatly recommended as a free AV solution, which now includes the firewall app that was previously only for premium users. What separates it from BitDefender is that it’s not a great security suite by comparison.

However, it’s the second best choice and the first if you don’t want to spend anything. As previously implied, the other difference is that it’s more powerful for searching and removing malware. This is still true. I use both on Windows; Avira as an AV and BitDefender as a suite of other security apps.

NORTON

Norton is only mentioned for the same reasons why Windows is mentioned. Do not use these services if possible. Norton is terrible at detecting and removing malware. It’s even bad at other security functions! The last time I used Norton was in 2012 to remove programs it deemed as untrustworthy and potentially unsafe. It scanned itself



as such, removed itself, and caused a BSOD, or blue screen of death. It was broken upon reboot. There’s so many jokes about how bad Norton is that it’s not funny to see someone using it. You’re a lot less safe than you realize.

OPERATING SYSTEMS

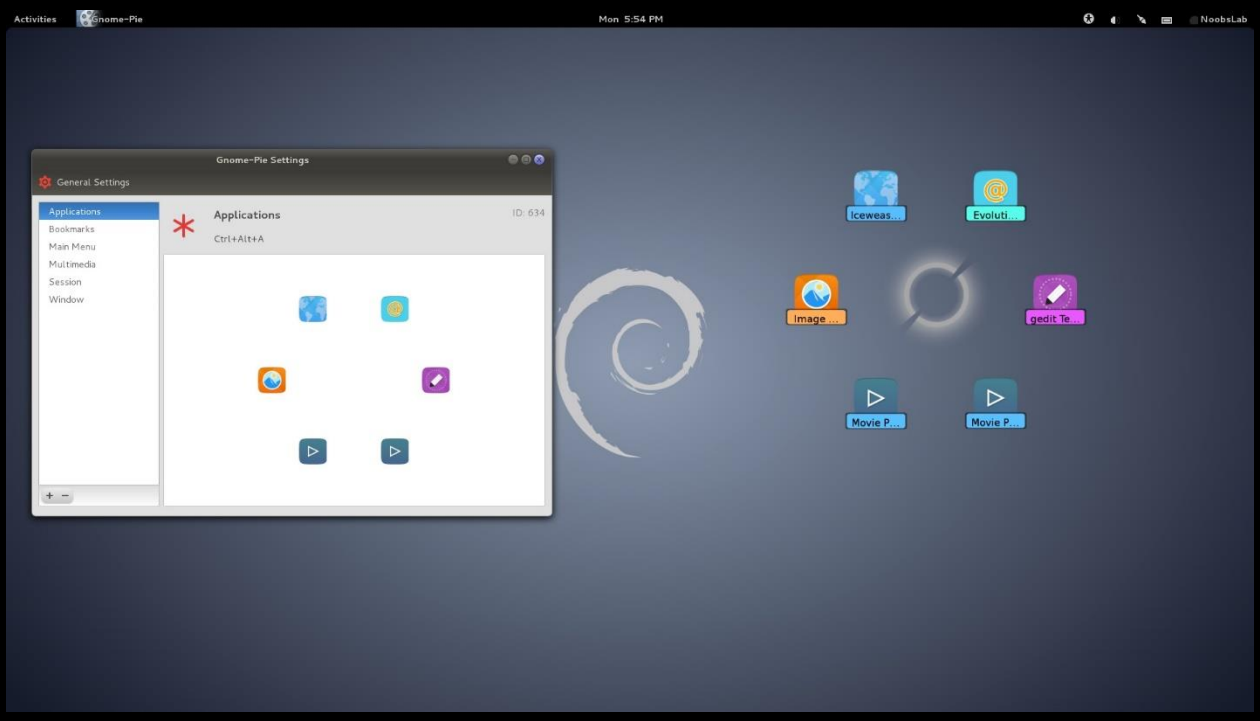
The OS you use matters. Some are more secure than others, some are more functional, some are purpose-specific, and others are just easier to use. Since you would already know a bit about Windows, I'll only cover some areas including why you shouldn't use Windows as your primary OS, what AVs to use if you do use Windows for anything, what maintenance tools to use, and how to automate tasks. The latter two will be discussed throughout the chapter. As for the cons, Windows security is poor, it's a heavily targeted OS franchise, the terminal use is lacking (but they did just add bash), Microsoft has installed myriad telemetry services, half the telemetry services can't be uninstalled or deleted, blocking Microsoft telemetry IP addresses is not easy and involves a lot of work, it's not free or open-source, etc. The few reasons is to use Windows over Linux are gaming support, Microsoft Office 2013+ support, Adobe Suite support, and a large array of not-universally-known apps that may work only or better on Windows than Linux like the aforementioned or Tresorit. This is why I advise still maintaining a copy of Windows for some resource-intense services like gaming or using a Windows VM on a Linux Host for app suites like Microsoft Office and Adobe Suite.

POPULAR LINUX

This section is about the most popular Linux tree based on Debian. The RHEL tree is not included only because I don’t use it, but CentOS and RHEL are worth researching if you’re interested. Rolling releases means one version of a distro or operating can be installed on top of the other without deleting all of the data like how Windows has conducted updates since Windows 8. What a rolling release is a distro release that doesn’t greatly change from version to version since the packages are constantly updated. This can be a bad thing since constant package updates without a still system can lead to numerous errors.

DEBIAN

Like Slackware and Red Hat, Debian is the mother of myriad Linux distros and the most popular of the three. In fact, the most popular Linux distro in existence, Ubuntu, is based on Debian, both of which do rolling releases. However, Debian doesn’t suffer the same system errors with rolling releases like Ubuntu since Debian developers have a solid, consistent testing plan. Debian uses the Gnome DE, or desktop environment, the apt, dpkg, and GDebi package managers, and is a very powerful, versatile Linux distro that’s been made to use for so many purposes. Let’s reiterate that many Linux distros are based on Debian.



Its uses extend from PCs to network servers, has been adapted to the Raspberry Pi ecosystem as Raspbian, and has been called too difficult to install due to choosing functionality over simplicity by Linus Torvalds, the creator of the Linux Kernel that has taken the name of the GNU operating system as Linux. Thus, I don’t recommend it for any new user unless they realize how much they love Ubuntu or Linux Mint and want the raw power Debian offers that made it the mother of so many Linux distros. Picking up a copy of Debian Administrator’s Handbook isn’t just a great idea for Debian use but all Debian-based distros like most of the distros discussed in this chapter.

UBUNTU

Ubuntu is a Debian-based Linux distro with its own DE called Unity and is the most popular Linux distro in existence. It’s been adopted for

multiple uses from a desktop distro to a cloud distro, a server distro, a tablet distro, a phone distro, a Raspberry Pi distro, a drone distro, and more. Ubuntu even used to have a cloud service called Ubuntu One. Over the past few years, Canonical, the developers of Ubuntu, have partnered with Amazon bringing a new store to Ubuntu

as well as some invasive telemetry services and has created their own phone to rival Android and iOS. Ubuntu has an extensive community of documentation and users to answer questions asked and is heavily supported by that community and Canonical. They release updates every 6 months where every April of an even-numbered year is the LTS, or long-term support, version and the other three until the next even-numbered year are experimental versions. Even though I don’t use Ubuntu as any of my major systems, I will say that Ubuntu 12.04 LTS

Precise Pangolin is still a very useful version of which I use in cases of emergencies that my PROJECT USB UFDs would be of no use such as using boot repair. I've recently downloaded the 16.04 desktop and server versions to test, especially with the new Snaps apps container.

LINUX MINT

Linux Mint is hands down easiest to install and use Linux distro I've seen yet and a have a TB repository of Linux distros I've tested. It's definitely my most recommended distro for both new users and anyone needing to create a system in a hurry. It's fairly difficult not to understand how to use with their elegant DE and it blows Ubuntu out of the water since the point of Ubuntu was also elegance with simplicity.

Linux Mint is built on top of Ubuntu like Ubuntu is built on top of

Debian. However, Linux Mint is like Ubuntu with less invasion from Amazon and Canonical through the use of lenses, less system errors, and a more elegant DE called Cinnamon that would appear familiar for Windows users. It does do updates like Ubuntu, but the developers have stopped trying to build experimental builds on top of the Ubuntu experimental builds due to major issues. Instead, as of 2014, Linux Mint has its own experiment builds and we're do to see the Linux Mint 18 (LTS) version sometime soon. Linux Mint doesn't do rolling releases either since doing so often leads to system errors like Ubuntu often experiences. It's my current primary OS, but that's because Qubes can work on my system with UEFI. It's great for VMs and quick uses, but I'm ready to move on to Black Arch with the i3 WM, or windows manager. It does include some changes over Ubuntu such as mintInstall (software manager), mintUpdate (update manager), mintMenu (main menu), mintBackup (backup tool), mintUpload (upload manager), mintNanny (parental control domain blocker), and mintWelcome (an annoying welcome screen that you'll want to uninstall soon enough). There's also a Debian-based version that skips Ubuntu entirely, but I don't recommend it like I don't recommend Debian for new users.

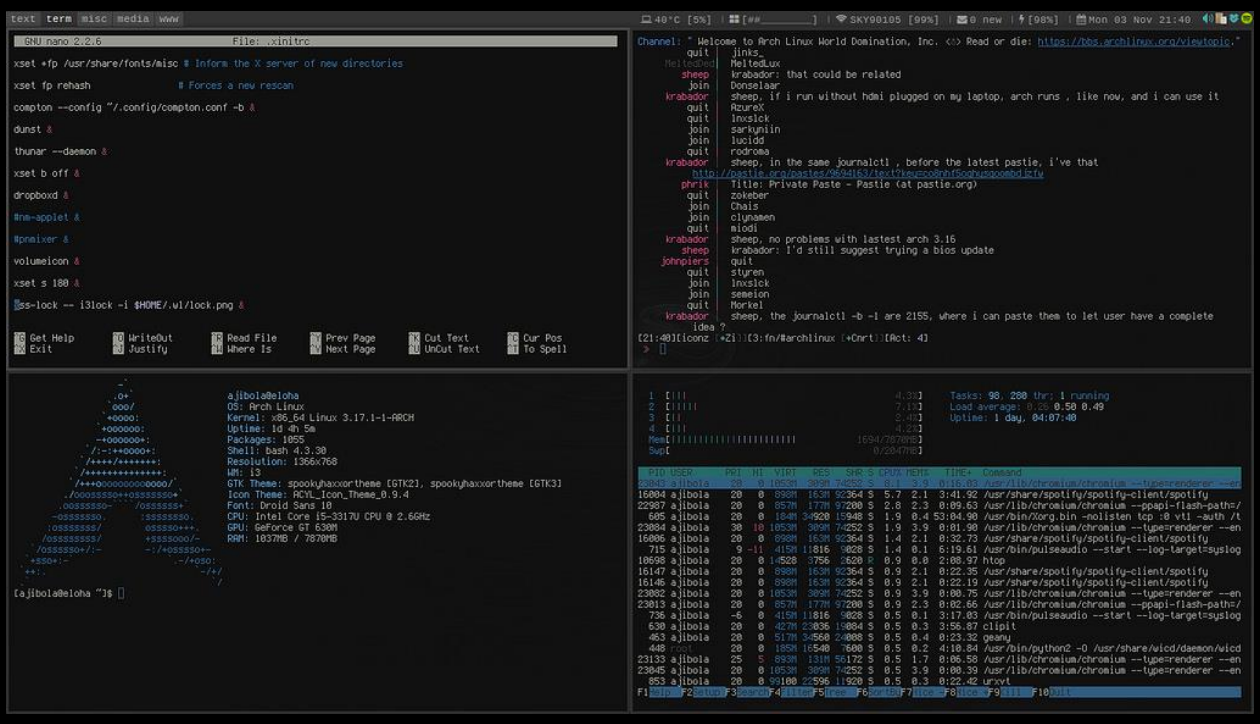
MACHAMP

OTHER LINUX

This section is about other notable Linux systems commonly used. Gentoo and OpenSUSE are not included because 1) I don’t use them and 2) they don’t have as much software support as other distros. I can’t say they’re worth researching, but they’re easy to find if you’re interested.

ARCH LINUX

Arch Linux is far from a basic user Linux distro and will haunt you forever with the installation alone. I suggest becoming well experienced with other Linux distros first so you can get a feel for the terminal. However, this is still an OS worth noting to everyone.

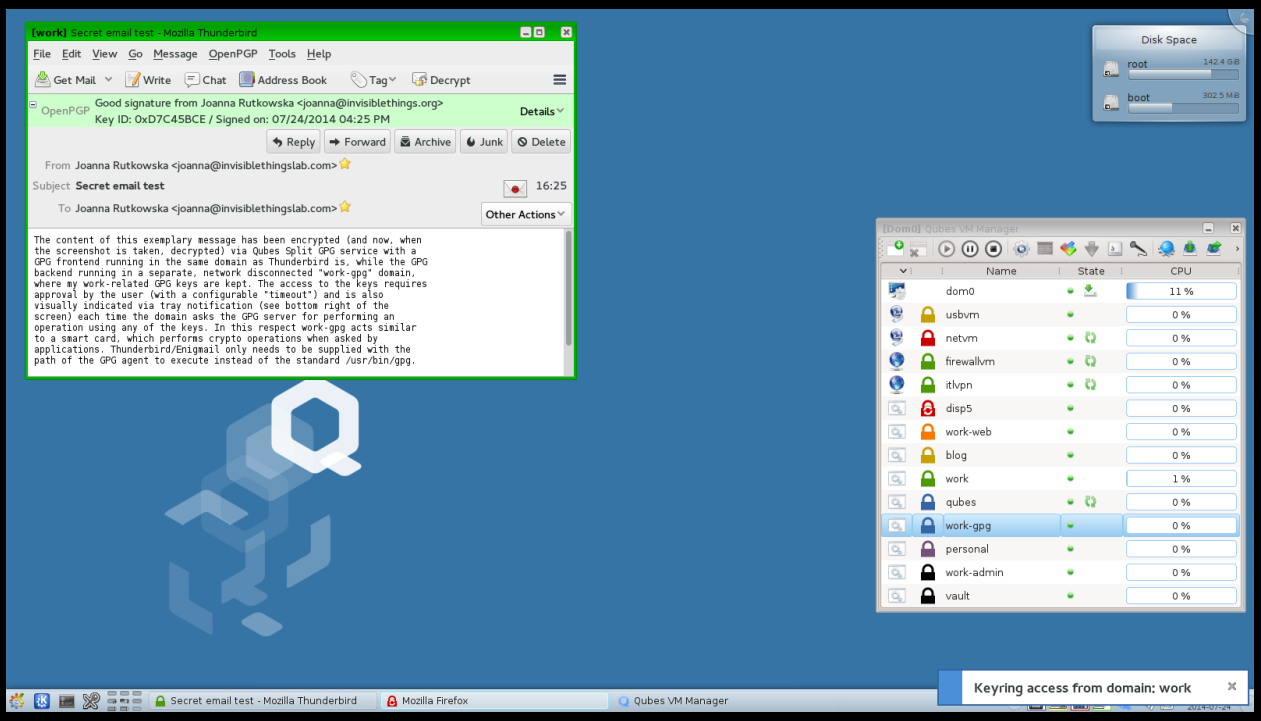


It’s a lightweight, transparent OS that you can build to be almost anything. It’s inspired by CRUX, but it’s not based on any other distro like most of the others mentioned in this chapter. While it may be insane to use without experience of the terminal, the entire point of Arch Linux is the application of the KISS principle, or “keep it simple, stupid,” with minimalism and simplicity. It’s one of the few operating systems so light-weight and diverse that it could be ran on a Raspberry Pi. Not even Debian can without a lightweight fork built specially for RPi. The good news is that it has even more documentation as ArchWiki than Ubuntu, but doesn’t have the same community of answering questions asked as Ubuntu. I suggest Black Arch over Arch Linux for three reasons: the installation process is a little easier, installing with FDE is as just easy as on any other Linux distro, and it comes preconfigured with penetration testing scripts you could use against your systems to test the system hardening and security configurations.

QUBES OS

Qubes OS is the new ‘it’ Linux system, especially in regards to security. It’s been called both the most secure Linux distro made yet and a Xen distro vs Linux since it uses Xen hypervisor to virtualize multiple user environments into lightweight VMs. This distro is a replacement to the VMware or VirtualBox tactics of PROJECT DEVICE PERSEC. The other distros it supports within its VMs are Fedora (which

is based on Red Hat), Debian, Whonix (which is a security-by-virtualization distro itself), and Windows. It already separates VMs into categories of work, shopping, random, and unsafe. The use of random led to the addition of the general browsing VM of PROJECT DEVICE PERSEC. Basically, the host OS isn't much of a usable OS like

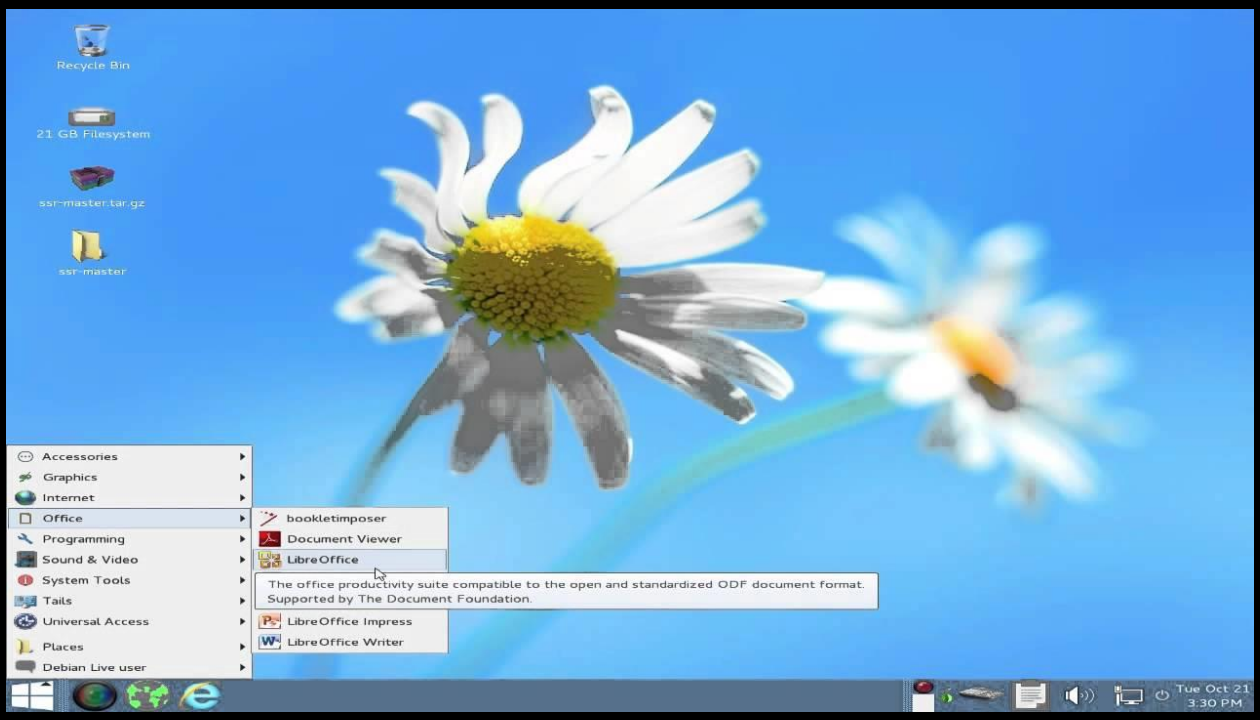


your other systems, but instead has you use the VMs for those purposes. Remember the security aspects previously discussed in PERSEC under Virtualization. The use of VMs makes it harder for an attacker to actually attack the host OS and the data on it when s / he attacks the guest OS. The one drawback is that it will have kernel panics if you install it on a system using UEFI vs BIOS. I don't use Qubes because I can't, but I really want to purchase a Librem 15 by Pursim with Qubes installed so I can use it as my public system for the

moments I have to use my systems in public. Even though Qubes can come preinstalled on a Librem laptop, anyone can download it and install it on their system or a 64GB+ UFD. It’s the easiest and most versatile means of staying secure via virtualization, it’s much lighter than PROCJET DEVICE PERSEC, and you can technically install any Linux distro you want as a VM such as Tails and Kali Linux.

TAILS

Tails, or The Amnesic Incognito Live System, is a security- and privacy-focused, Debian-based Linux distro. It’s meant to be ran as a Live disk or UFD so that it can erase all data on it once powered off. The incognito aspect is that it doesn’t save data, the amnesic aspect is that it erases data, and the live system keeps any changes that were made during a session from being saved. That makes it return to

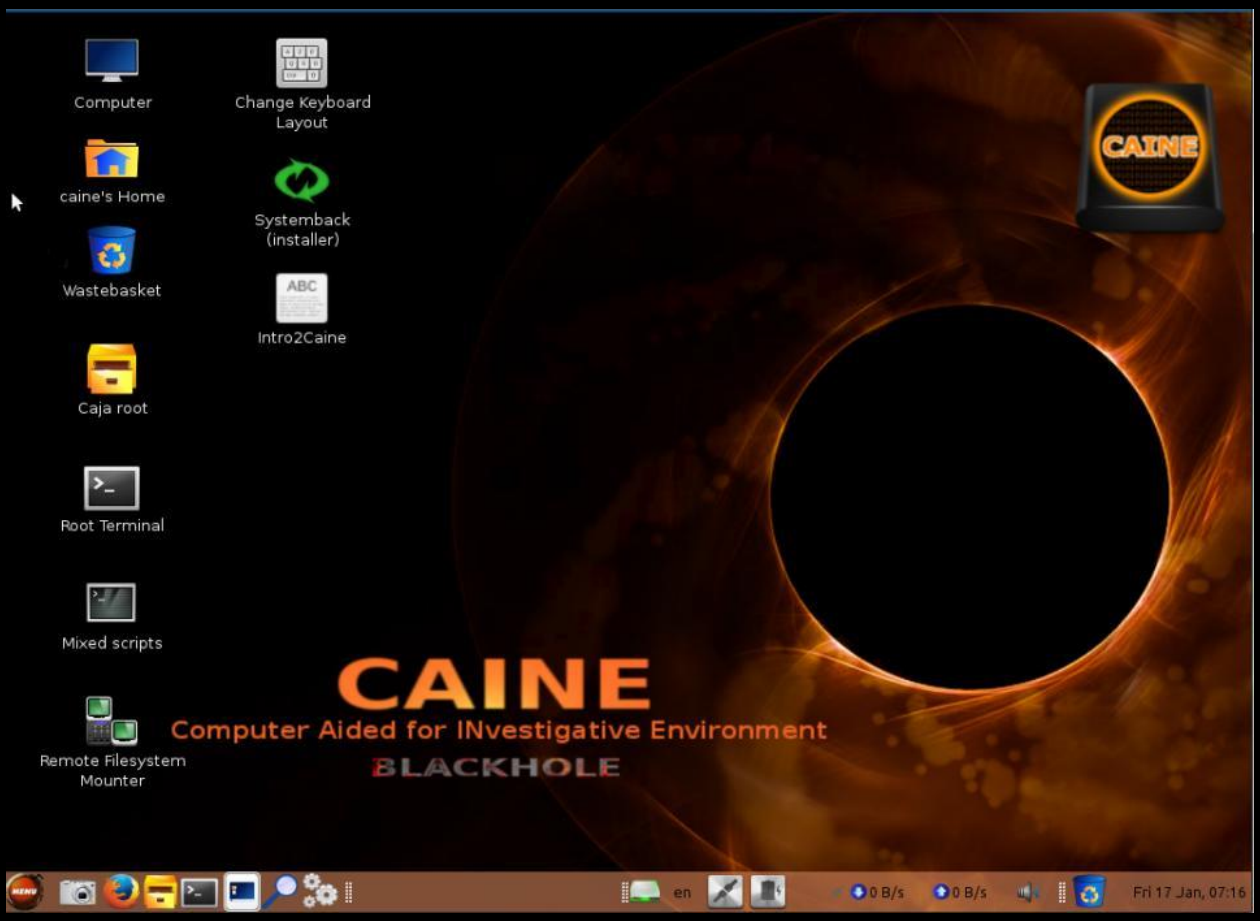


the default set-up every boot. It’s meant to be used with Tor to keep all network connections private and secure, the Tor browser, Pidgin chat client with OTR, or off-the-record, end-to-end encrypted instant messaging, I2P as an alternative to Tor, Electrum Bitcoin wallet, and more. Tails also includes myriad encryption tools for every purpose including data partitions, files, instant messaging, emails, networking, and more. It even includes Windows camoflauge to make itself roughly appear like a Windows system for prying eyes, but the support is currently broken in Gnome. The devs are trying to add it back though. Tails is the best privacy-based Linux distro out there with Whonix as a close second. Whonix is closer to Qubes though so it’s not a true rival like FreePTO.

FreePTO isn’t named as an alternative since support for it has ended. The developers recommended switching to TAILS.

CAINE

CAINE, or Computer Aided INvestigative Environment, is an Ubuntu-based distro for digital forensics. Digital forensics is the act of reactive security to recover and investigate material found in computer devices in response to an incident, which is often used for computer crimes. However, it can also be used for data or system recovery like when you manage to lock yourself out of your system by accidentally disabling your user account on your host OS. CAINE runs as a live system on disk or UFD that uses autopsy (image analysis tool), tinfoleak (Twitter

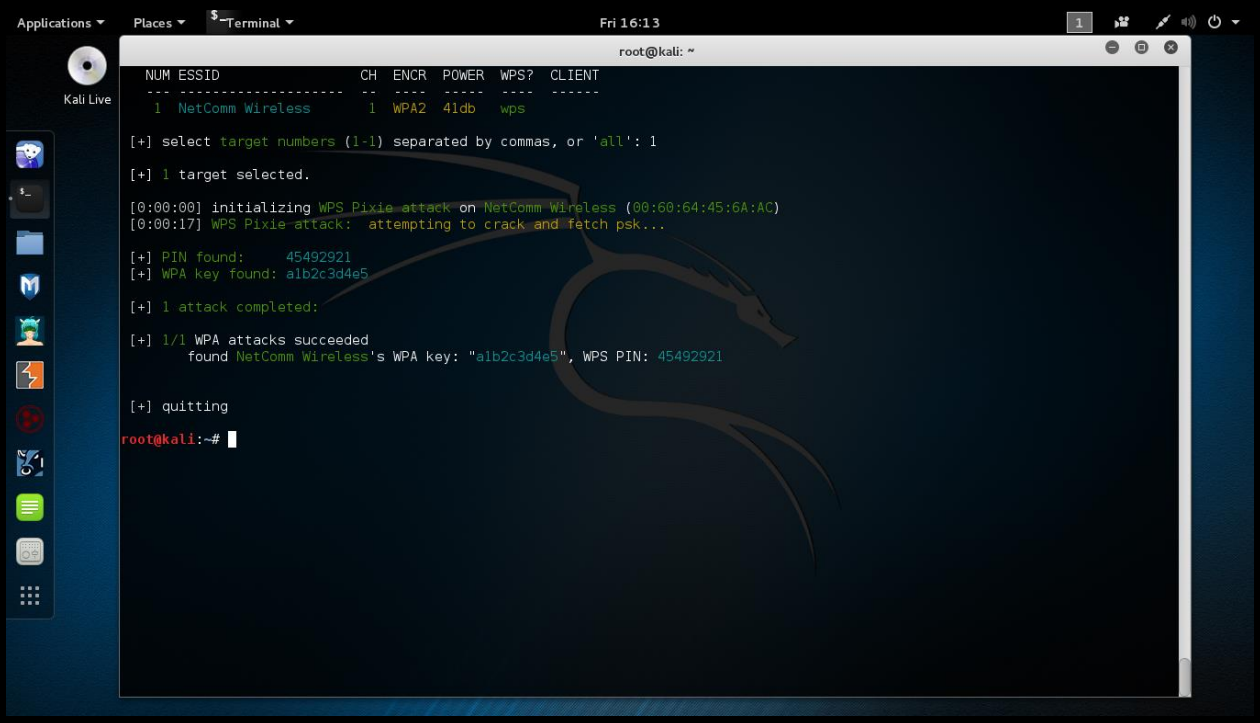


metadata harvester), bulk extractor (email and URL extraction tool), EXIFTool (photo metadata reader and manipulator), Guymager (system image creator), and many of the penetration testing tools used by Kali, but those will be mentioned below. Attackers can use CAINE to retrieve data from a target like investigators can from a suspect. However, it’s a free, popular, open-source forensic-specific distro that’s worth maintaining a copy in case an incident occurs.

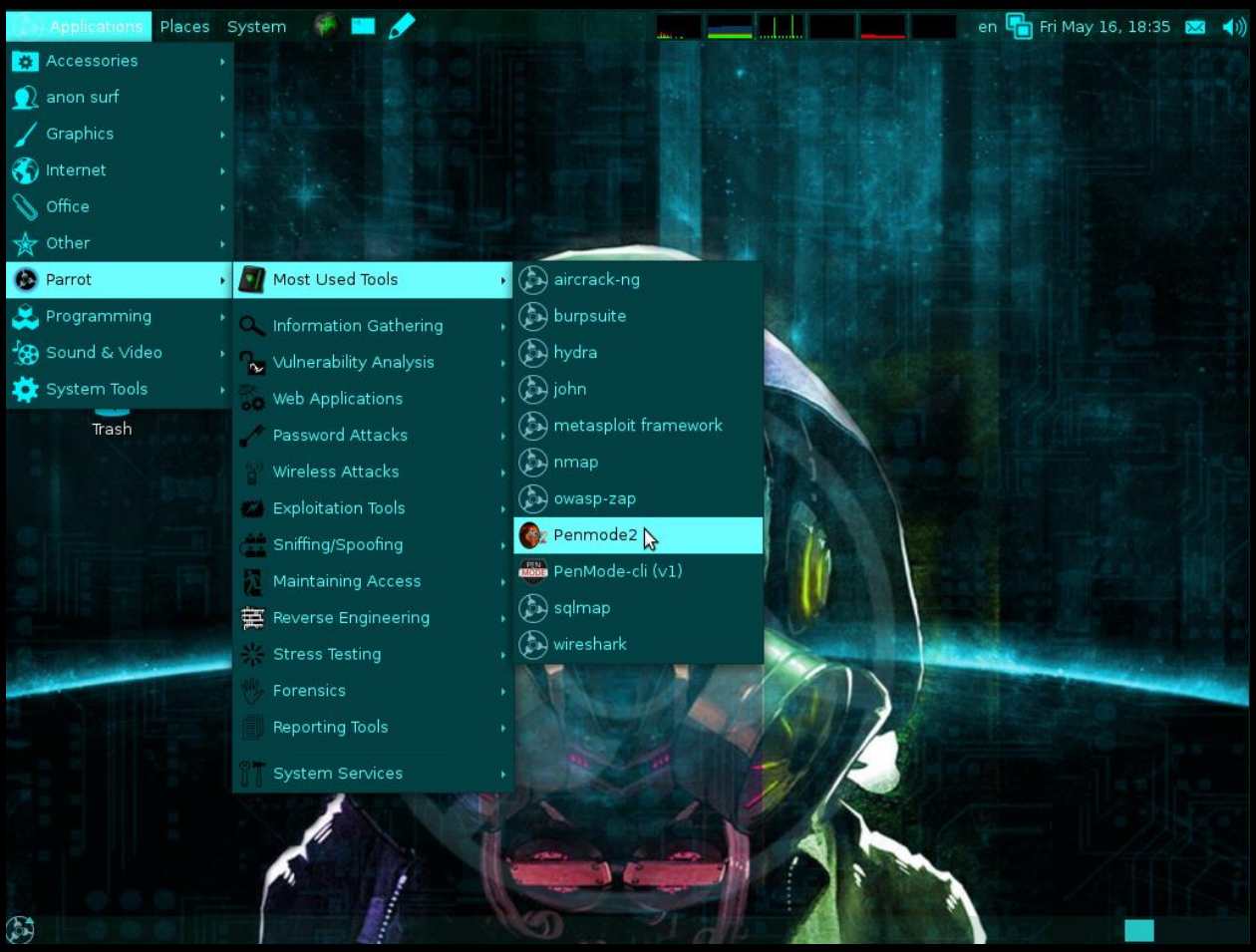
DEFT Linux isn’t named as an alternative since their site is dead and there doesn’t appear to be any indication of whether or not DEFT Linux is still active or not.

KALI LINUX

Kali Linux is a Debian-based penetration testing and digital forensics distro that’s very well-known with roots to BackTrack. Penetration testing is the act of offensive security to attack a system or network in order to exploit the vulnerabilities found to test the severity of those vulnerabilities and write a report of the actions taken and security recommendations to patch those vulnerabilities. Let’s start a tangent and explain that skids, or script kiddies, often confuse this for “hacking.” While these are tools that can be generally used for “hacking,” a skid is the type of person that would really use these. Skids are individuals that attempt “hacking” yet don’t understand coding, network engineering, system administration, database management, web development, and more. They’re basically laymen that purchase or obtain security tools made by others for their own purposes and pretend to be “hackers,” while not understanding how easy it is to detect and thwart skid tools. I use “hacking” and “hackers” in quotes because I believe the true definition of hacking is the original and not the 80s Hollywood version of attackers. The original definition of “hacker” was someone that broke down a computer process to better understand how it works and manipulate to do whatever the individual instructed. When it started to be used to define malicious “hackers,” the term cracker was created, yet it failed to replace what the world has perverted of “hackers.”

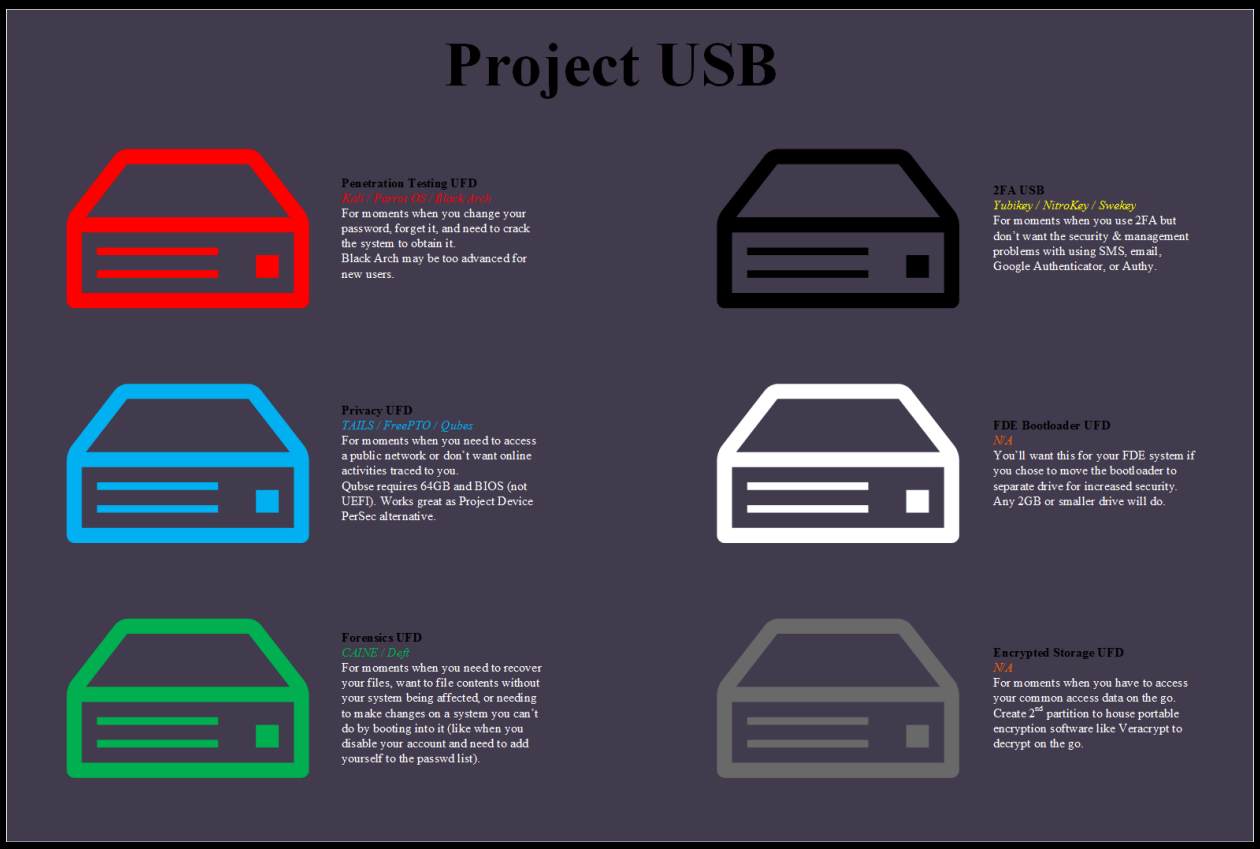


Kali Linux's preinstalled tools include but are not limited to Armitago (attack management GUI), nmap (port scanner), Wireshark (packet analyzer), John the Ripper (password cracker), Aircrack-ng (Wi-Fi penetration testing), OWASP ZAP (web app vulnerability scanner), and more. It's essentially the pre-configured penetration testing distro and it's had support on multiple Chromebooks, Raspberry Pi, and more. Kali Linux even exists as Kali Linux Nethunter for the Nexus line of Android devices. It's a custom ROM Nexus Android users can install on their phones and tablets, but we can just as easily install the suite of tools from F-Droid and the Nethunter app from the Kali Linux site.



Parrot Security OS is an alternative to Kali Linux that’s built on Ubuntu and conducts forensics. However, Parrot Security OS also engages in vulnerability assessment and mitigation and anonymous surfing attempting to be the all-in-one security distro. It’s claimed to be a cloud-oriented penetration testing distro, which is why it also comes with a server / cloud edition alongside its light and full editions.

PROJECT USB



01) Purchase 3 UFDs and follow the examples on the left.

02) Install a forensic, penetration testing, and privacy-based Linux distro on each.

PHONES

Phones are as much a nuisance as wireless networks and email if not worse and smartphones are even worse than other cell phones in regards to security. If you can help it, never use a smartphone over a PC. However, that’s fairly unlikely like giving up email. Instead, there’s some advice you can mull over and decide if you want to stick with smartphones and secure them or move over to burner phones. Regardless of your choice, your use of cell phones can still be traced and you can still be found. Cell phones can be traced via triangulation without GPS enabled since you’re connecting to a cell tower in order to use the phone. A few tips for this are to carry your phone in an aluminum case when not in use or turn it off and remove the battery. Some phones don’t have removable batteries and using an aluminum case means you won’t receive any communication to the phone while the signal is blocked by the case.

Like PCs, smartphones have OSes worth discussing. Blackberry has the best mobile security out of the three major phone operating systems, I haven’t tried the Turing or Black Phone, and the Amazon and Firefox phones are dead projects. Blackberry isn’t discussed because it’s a dying company and one that has managed to stay relevant by partnering with Google to produce Blackberry phones with Android for a secure,

professional Android phone. This leaves the discussion to Android and how you can secure it, burner phones and how you can obtain them, and iPhone and why you shouldn’t use them. For additional security, it’s advised visiting Is My Cell Phone Bugged?

BURNER PHONES

Burner phones are the best privacy-based mobile technology out there using satellite connections vs solely radio waves. They’re inexpensive, easy to use, and great for communication without the added vulnerabilities that smartphones offer. It’s the application of KISS, or keep it simple, stupid, while allowing calls and texts. Of

course, using a payphone or friends phone when the occasion arises is an even easier way of staying private, but we're working under the assumption that you need a phone in case of emergencies.

Unfortunately, burner phones require some form of identification in order to activate one and this varies from state to state. First, use cash of the gift / prepaid card system previously discussed in PERSEC under Finances. Second, you can use a friend, pay a stranger, or wear a disguise to purchase one since there will likely be cameras in the store that records you actions there. Third, you can either use a friends' phone or a strangers' phone to receive a text from a friend that's actually the activation text. Regardless, delete the message.

Using email addresses instead of the phones in the third step is the easiest. Use the disposable email services or create a temporary, encrypted email on a live system or VM. If you choose this step, make sure to delete the VM when you're done. I always advise defragging the disk and clearing up the free space when done so all traces of evidence are gone. The easiest way to go about this is to create a separate partition or use a separate drive, whether UFD or SD card, that's large enough to house a Linux VM (Linux Mint is only 8GB when fully installed and Arch is less). The reason for this is so that you don't spend a lot of time and resources using a disk freeing tool like Bleachbit for an entire drive. Also, you don't need to use a disk defragging tool on flash memory like UFDs, SD cards, or SSDs. If you

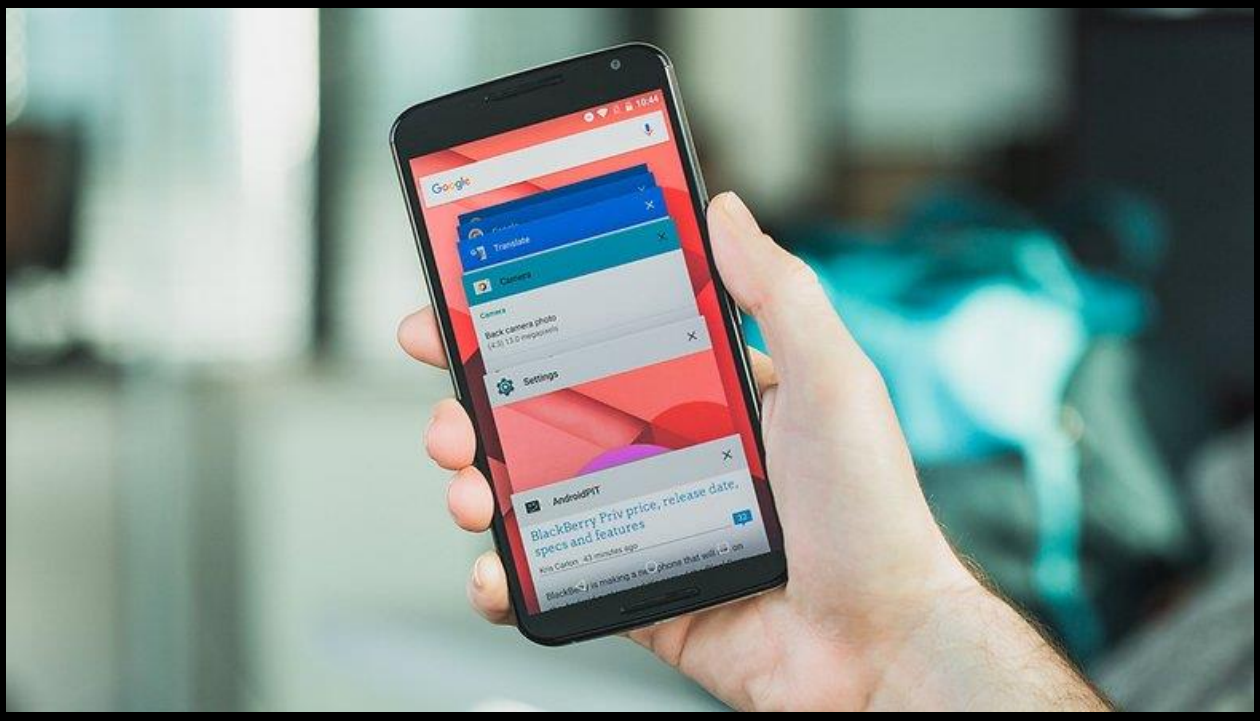
don’t know if you have an SSD or HDD, you most likely have an HDD so defrag. If you used an SSD or HDD with creating a partition, don’t forget to delete the partition and add it back to the original partition.

iPHONE

Don’t ever use an iPhone. Apple doesn’t take security seriously, especially not as much as they take design and marketing. Even Snowden has stated that he will never use an iPhone. They’re very easy to track and break. As it turns out of late, they’re even easy to bypass the FDE used. As if using an iPhone wasn’t bad enough, what’s worse is jailbreaking an iPhone. Jailbreaking is not at all like rooting and unlocking an Android phone. Rooting involves obtaining root privileges or administrator privileges. Unlocking involves making the bootloader accessible to change. Both of these do not alter the security of the phone, but rooting can be detrimental if a user gives root permissions to a malicious app. Jailbreaking involves destroying all security protocols for increased customization and leaves the user open to attack by anyone. Over 95% of iPhones that have been jailbroken were reported to have been “hacked” in the past few years. It’s a bad idea to use an iPhone, but it’s a worse idea to jailbreak one.

ANDROID

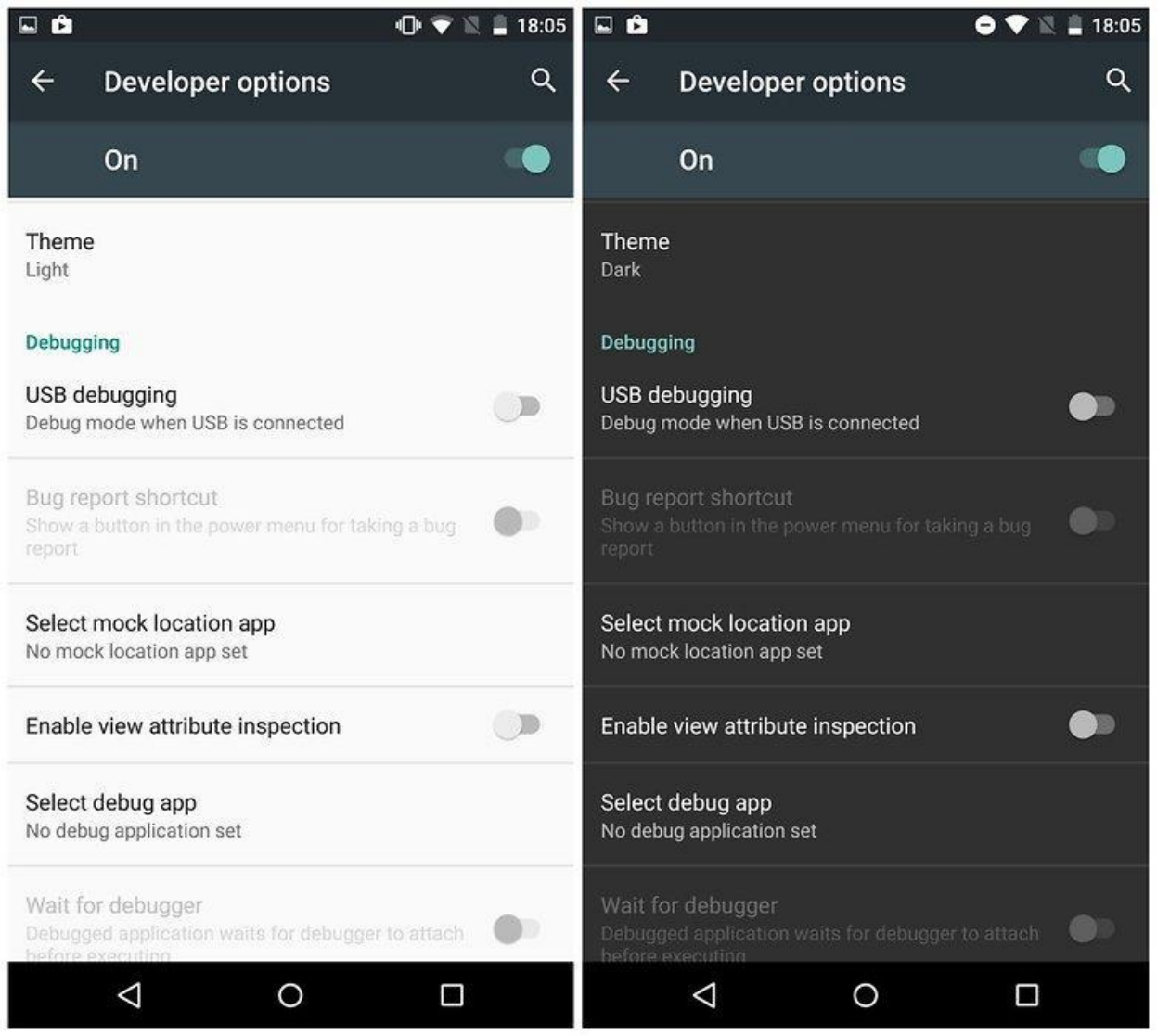
Android is your only decent option for a secure smartphone that has a lot of support. Otherwise, I would recommend Black Phone, Turing Phone, and Replicant over Android, even though I haven’t used the former two. Android can be made to be mostly secure, especially if you use the Nexus line and not the Samsung line of products. The good news is that there are numerous ways to keep your phone secure and that most security issues are just like PC security issues: the user. The amount of layers of security you have to bypass to infect an Android phone is quite a few. One such issue is the use of apps outside the Play Store. Unfortunately, this means maintaining a Google account. I have a Google account still that I’m trying to kill off. However, I still use Android and since most app platforms are lackluster in comparison to the Play Store, I have an encrypted email account set with a new Google account where everything that can be stripped is stripped. My only means of purchasing the recommended security apps is via gift cards. Keep your use of Google services to a minimum, follow the security settings, and experiment with a few apps. You’re first going to want to root and unlock the phone. There’s plenty of videos and tutorials out there for many Android phones so finding one that works shouldn’t be an issue.



SETTINGS ----------

- If you have an unlimited plan, disengage Wi-Fi.
- If you have a PC, disengage Wi-Fi. Your phone isn’t as secure as your PC.
- Unless in use, disengage Bluetooth.
- Alter sleep mode based on how long you generally use your phone. I have mine set to go to sleep after being idle for 2 minutes.
- Filter your notifications from the lockscreen.
- Use a 16-character password.
- Do not engage Quick unlock. If you do, don’t use it around prying eyes.
- Set the power button to instantly lock and make a habit of manually locking your phone.

- Encrypt your phone.
- Leave ‘unknown sources’ disabled unless needed. Make sure you know where the APK came from before installing it.
- Set up screen pinning with password.
- Enable Privacy Guard by default. Go through and toggle the app permissions. Each one varies on use, but I usually disable most. Disabling GPS for Google Maps means it can’t locate you and disabling camera access to a camera app means you can’t use it.
- Disable GPS by default.
- Set up developer options by clicking ‘Build Number’ multiple times in a row.
- Enable Advanced reboot if you access your recovery often and / or want more reboot controls.
- Leave Android debugging disabled by default unless in use. A powered-on phone with USB debugging enabled can have its security bypassed by plugging it into a PC.
- Set up mock locations for extra GPS security. When you need GPS, you need to disable this feature.
- Add the back button as an app killswitch.

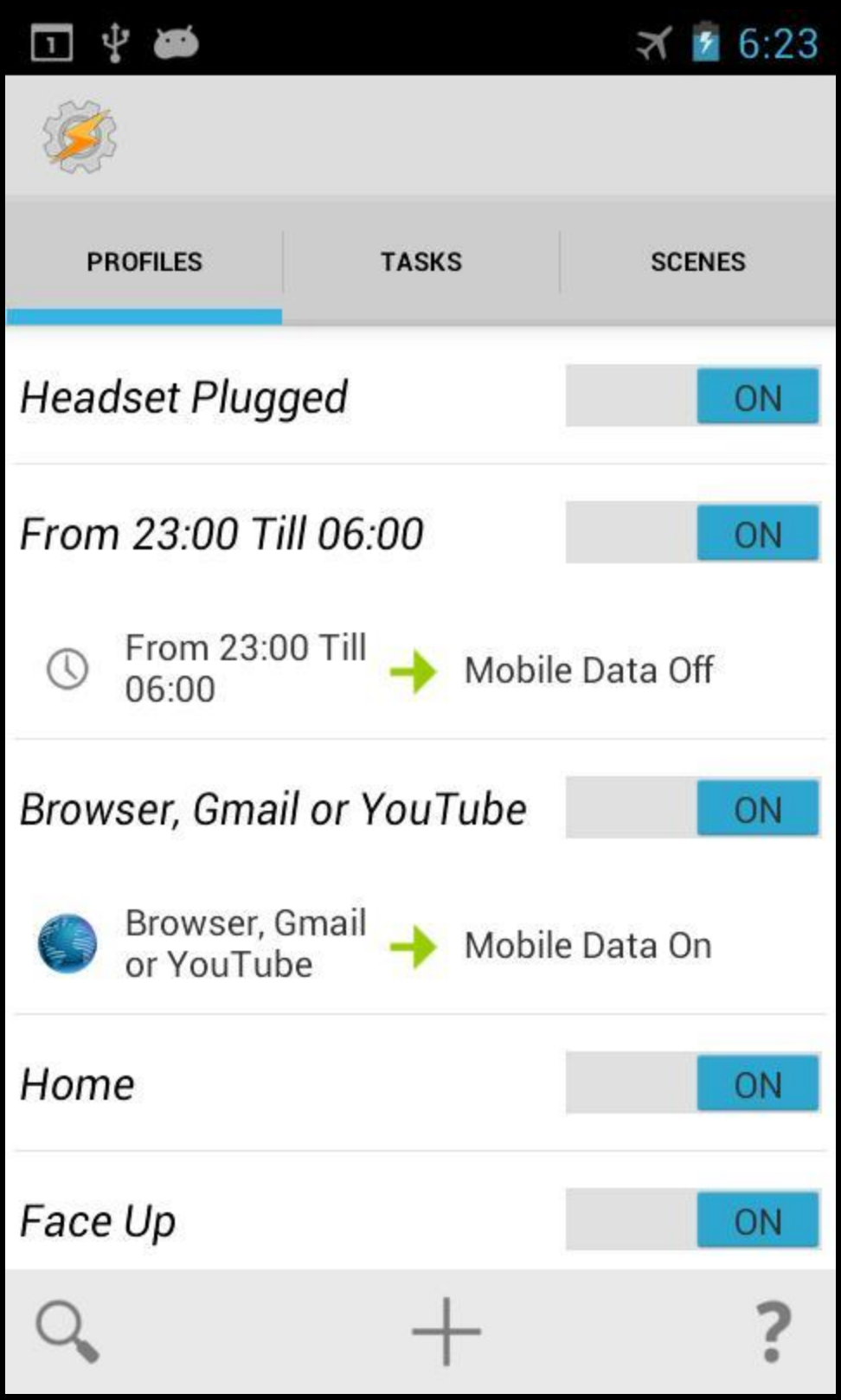


APPS

There’s a few apps I use that have proven very useful, most of which I would recommend and others of which are overkill. An example would be my use of three adblocking apps when one should suffice.

- AFWall+ (root-required; app firewall)
- CCleaner (like CCleaner for Windows or Bleachbit; root-required for system app management)
- Crypt4All (AES Crypt for Android)

- ES File Explorer (root-required for access outside SD card; best and very versatile Android file explorer)
- F-Droid (trustworthy app repo for privacy and security apps)
- Obscuracam (EXIF-removing and face-blurring camera app)
- Security Settings (necessary security app for changing Android security settings with Tasker)
- Signal (encrypted text messaging and calling app)
- StickMount (USB-mounting app)
- SuperSU (management app for apps with root permissions)
- Sync (BitTorrent Sync “cloud” service)
- Tasker (automation app like Cron for Android)
- Titanium Back-up (app, app data, and system data backing up app)
- Trigger (lightweight, Tasker alternative with better NFC support)
- Yubico Authenticator (for using Yubikey Neo with phone for 2FA)



You can’t have your phone encrypted and requiring password on boot-up before decrypting if you want to use Tasker for security purposes. It’s a trade-off and one that isn’t great, but I made the choice to support Tasker since I use my own 2FA profile. I have Smart Lock set up to recognize my Yubikey and unlock the phone. However, this always opens up Yubico Authenticator.

I’ve added an app lock to it for dual security and set Tasker to launch it when unlocked by entering the password instead. Thieves will either have to have the Yubikey and know the 8-digit pin or know the 16-character password and the 8-digit pin. I’ve also set Tasker to take a photo of anyone that enters a wrong password. Unfortunately, the thief must enter at least 4 characters for Android to register this as a failed attempt and not just an accidental unlock as if in someone’s pocket. Switching to Signal breaks SMS features with Tasker so it’s another trade-off. I use the email features instead. There’s a just a few examples of many that you can do with Tasker that makes Android even more secure than other mobile operating systems built for the general public.

PROJECT MOBILE

PROJECT MOBILE is like PROJECT DEVICE PERSEC and BASEC combined since smartphones are the weakest vulnerability, excluding social media only by social networks. This project isn’t set with rules but an experimentation of the apps and settings based on the previously mentioned information. Some of the Tasker profiles and tasks depend on purchasing the Security Settings app:

- Set CCleaner to notify user when it hasn’t been used in 24 hours.
- Set Titanium Backup to back up modified apps, app data, and system data.

- Set BitTorrent Sync to back up other, relevant phone data and Titanium back-ups to security server or whichever system.
- Set Tasker to reboot phone daily.
- Set AFwall+ to restrict most apps that need network connection to VPN.
- Set AFWall+ to allow system apps and Google Play to use unencrypted mobile data. Otherwise, network capabilities break.
- Set Tasker to kill VPN, place phone in airplane mode, wait 5 seconds, leave airplane mode, and restart VPN when mobile data connection is lost.
- Set Tasker to act as app lock.
- Set Tasker to active app lock profile and task when phone is rebooted. This is needed since the following task only works after the phone has been unlocked once after boot meaning the first session doesn’t engage the 2nd lock.
- Set Tasker to active app lock profile and task when phone is unlocked.
- Set Tasker to block camera, mic, and GPS by default.
- Set Tasker to unlock camera when Obscuracam started.
- Set Tasker to take photo of anyone that fails to unlock the phone.
- Set Tasker to enable GPS and send geolocation data to security server or user account when it receives a specified text.

NETSEC

NETSEC is network Security. Like SYSSEC, this is one of the most discussed types of cyber security. However, excluding the technical aspects, a lot of NETSEC-related issues can be solved with PERSEC from social engineering awareness to safe browsing habits. The technical side of NETSEC still matters though and will provide additional security PERSEC cannot. This ranges from browser plugins to encrypted traffic and from the network type to firewall rules. NETSEC matters because you’re opening your system to every network you connect to and the users on those networks exponentially increasing security risks you wouldn’t find with SYSSEC and PERSEC in an offline world. Your online presence makes you a great target and you will be targeted. There’s a lot of confusion with the dark web, dark net, and deep web. Let me break it down. There’s the Clearnet and the dark net and then there’s the surface web, deep web, and dark web. There’s also dark Internet, but that only applies to servers online that can’t be connected to in any way, shape, of form. Clearnet is the use of networking without encrypting network traffic and dark net is the exact opposite encrypting network traffic. Surface web is the part of the web where contents are indexed and accessible by search engines and the deep web is the polar opposite where contents can’t be indexed

by search engines. Dark web’s definition is unclear and constantly argued about. My definition has been the use of dark net services over the web like Tor. Wikipedia’s definition is the use of the web over dark nets. It’s really the same definition. It’s the part of the web that’s only accessible via dark net services like Tor and I2P. It’s argued that the dark web is a small part of the deep web, but that’s untrue since many dark webs sites are accessible to multiple dark web search engines.

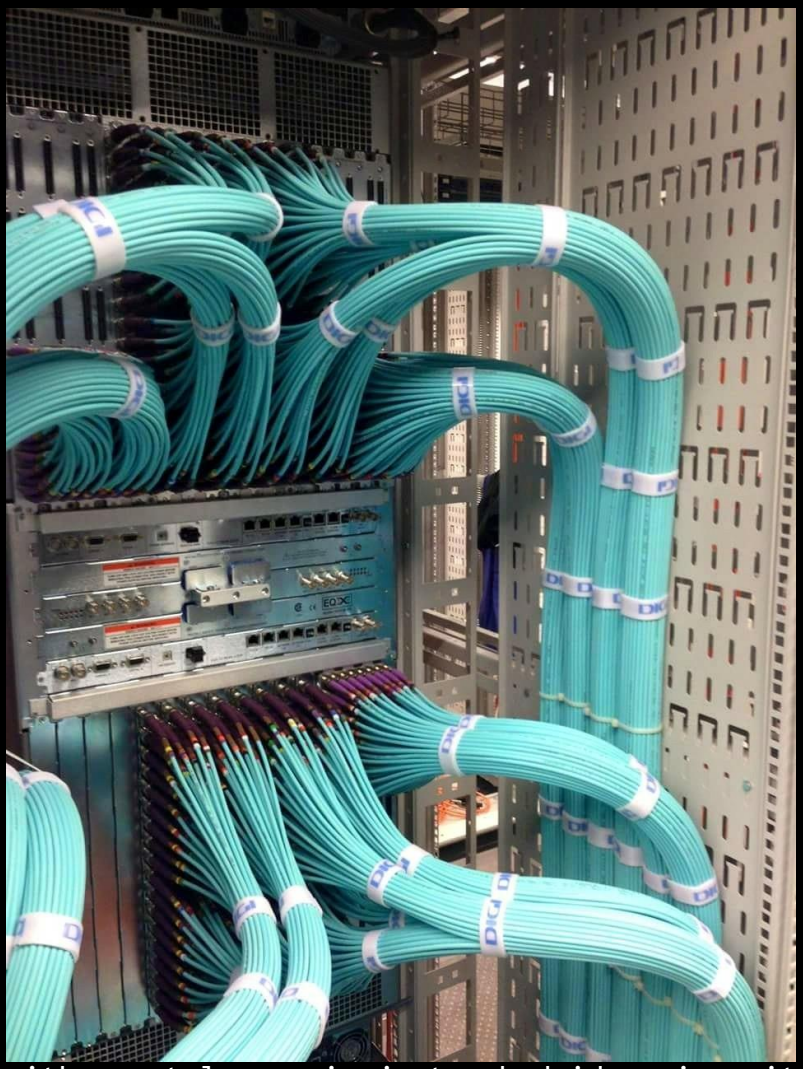
MUK

NETWORKING

As previously stated, the types of networks you use matter. The type of network you should use depends on the network location. For example, when you're at a coffee shop with free, public Wi-Fi, use the Wi-Fi vs. a wired connection. You can't hide behind the number of users on a public network if they're using the wireless network and you're the only one using the wired network. Granted, it's unlikely you would have wired access and there's a lot of security precautions you need to take before even considering joining a public network.

WIRED

Wired networks should be your default networks, especially for home settings. There's no radio waves for attackers to pick up. In fact, in order to breach your network, an attacker must have physical access to your cables, computer, router, modem, switch, etc. Your neighbor can't intrude on your network to download the latest episode of Game of Thrones from his home across the street if he can't access it. Granted, there's still security precautions that should be taken on a wired network regardless from installing an IDS, establishing firewall rules or using a physical firewall, using MAC filtering, etc. Also,



wired networking is faster than wireless networking. You don’t have the same interferences and distant issues over cables. Placing a desktop in a faraday cage to block EMF (electromagnetic frequency (EMSEC issue)) doesn’t disrupt network traffic when wired networks are used, but using Wi-Fi on a desktop with a metal case is just a bad idea since it won’t work with the wireless adaptor inside the case. Wired networks are your best friend like companion cubes!

WIRELESS ----------

Wireless networks are inherently insecure, especially compared to wired networks. Your router is broadcasting the networks’ radio waves openly. Encrypting the traffic with WPA2 is a great idea, but doesn’t make you secure enough. If you have a basic, commonly-used password, aircrack-ng can crack your password quickly. If you don’t have MAC

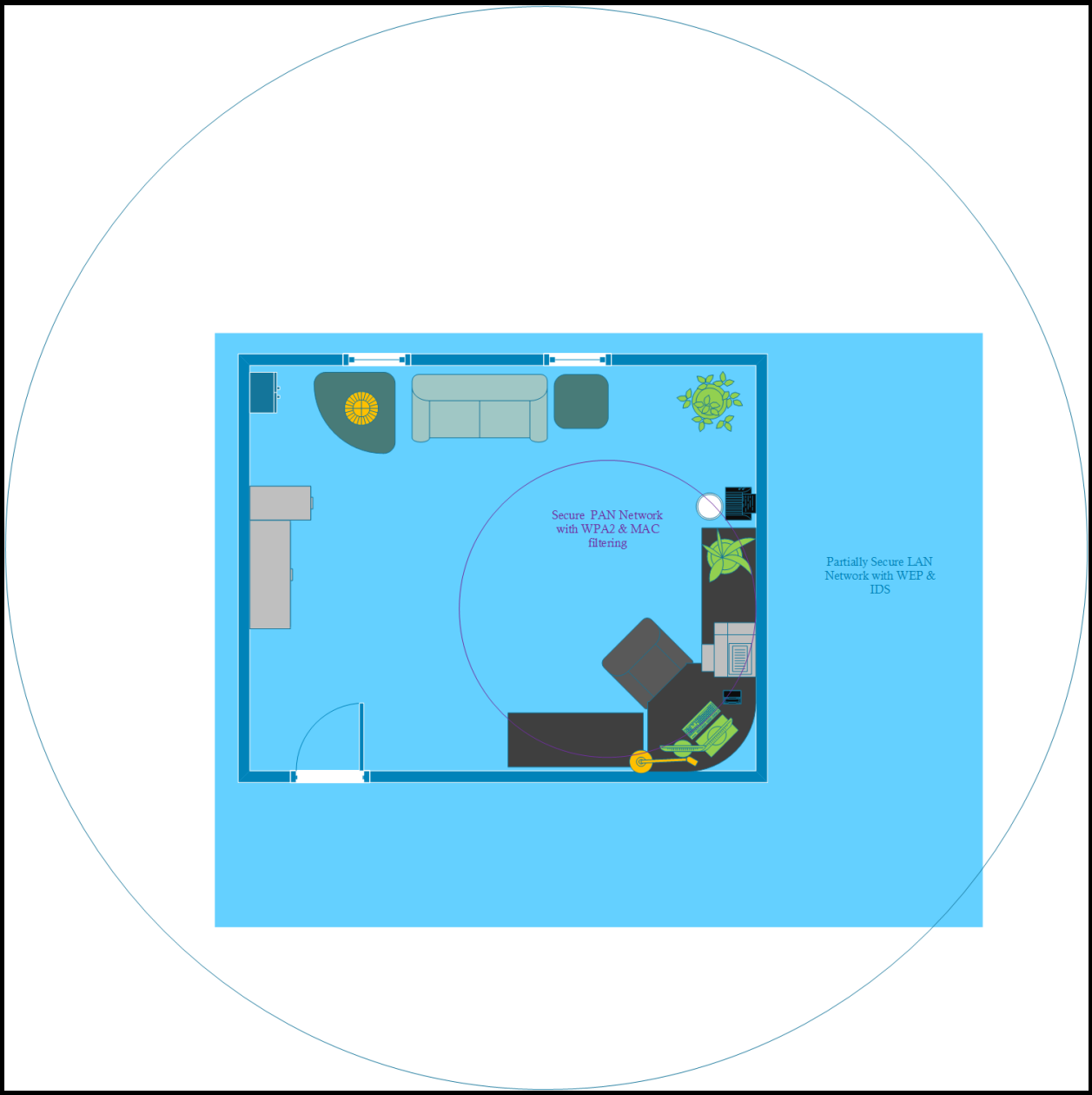
filtering set, you can be spoofed or attacked with MiTM attacks, or Man-in-the-Middle. Do NOT disable SSID broadcasting. 1) Your SSID is still broadcasted by the computers connected to the network, 2) it makes it unnecessarily difficult for you to connect to your network when the connection is lost, and, most importantly, 3) it tells attackers you're new to NETSEC that you don't know the first point and that your network is still broadcasting radio waves that can be picked up by anyone. Your network is only hidden from network GUIs, not packet analyzers and sniffers.

Don't use wireless networks at home unless you either 1) live in such a large home that your network doesn't broadcast outside your home's walls or 2) adjust the range to where it only broadcasts as far as the

walls within your home. If you live in a dink apartment, don’t even use Wi-Fi. You’d have to limit the range to PAN, or personal area network. That’s a small range that only extends to a small space in a single room. If you’re adamant about using Wi-Fi, complete Project Honeynet.

WEEZING

PROJECT HONEYNET



This project is only for if you’re adamant about using Wi-Fi over wired networks.

01) Purchase router that supports custom firmware that allows dual networks: OpenWRT, DD-WRT, Tomato, etc.

02) Configure router with custom firmware.

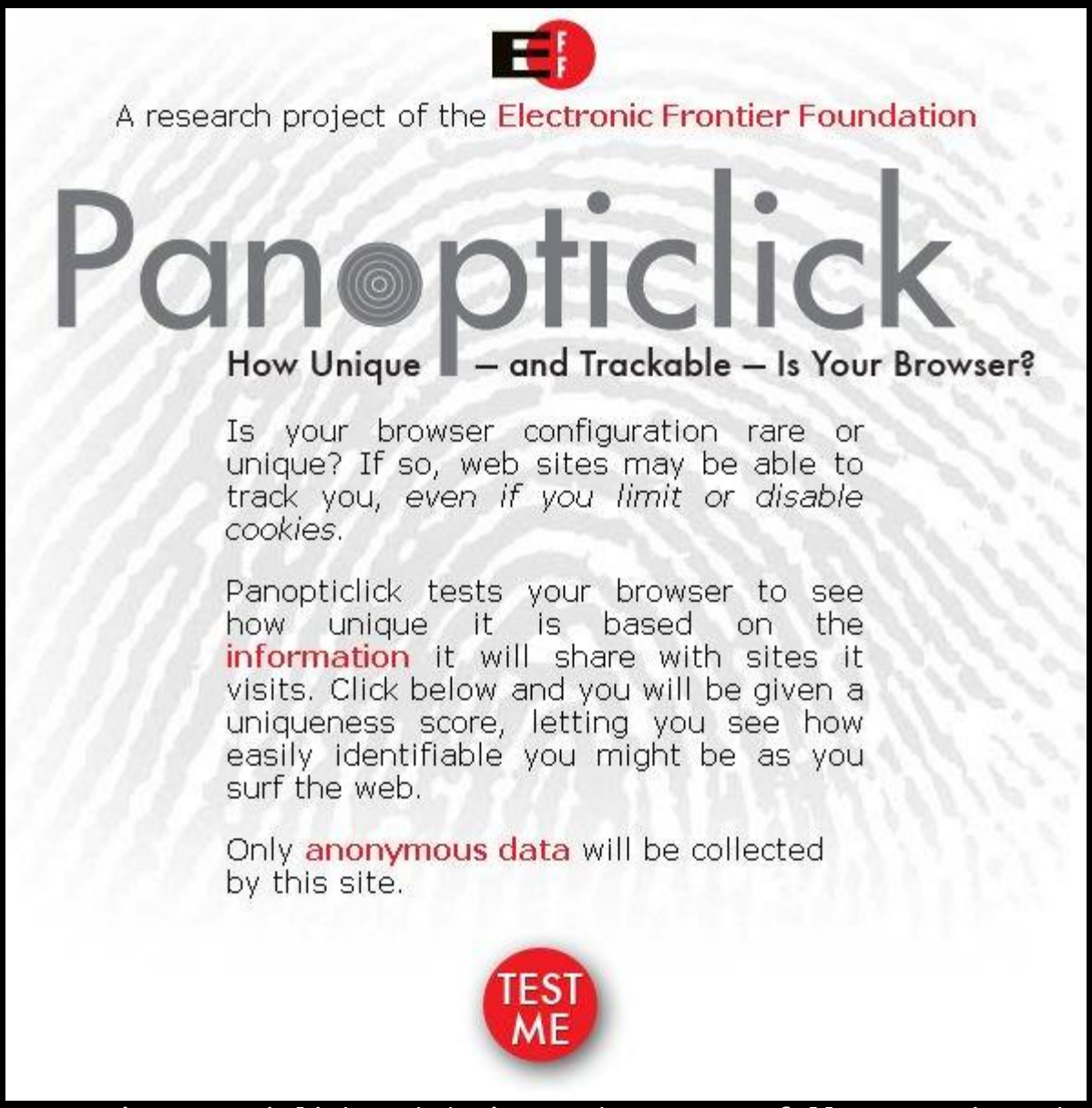
03) Configure router to use two networks.

04) Configure first network with normal broadcast range, with WEP encryption, add an IDS, and no additional security.

05) Configure second network with PAN range, with WPA2 encryption, and MAC filtering.

BROWSERS

Don’t use other tools for services you can use with a browser. Don’t use a PDF reader when Chrome and Firefox can read PDFs, but do use a PDF editor for editing PDFs since Chrome and Firefox are limited to just reading. One reason why is you’re introducing unnecessary vulnerabilities by adding another piece of software you have to manage, especially with that software’s actual vulnerabilities. Another reason is resource management. If you’re already running a browser, you’re not adding much by opening a PDF in a new tab, but you are adding more resources by having to start and run a separate program while running the browser. We’re mostly on our browsers when on our computers so there’s a reason why browsers have added file supports. The same could be said for more files than just PDF. You can also watch MP4s, but not WMVs. The support can be tacky for some files and the features are definitely limited. Like with editing PDFs, if you want to watch any video file or have more features than watching, pausing, expanding to full screen, volume control, and moving to a specific time in a video, use tools like VLC or whatever video player of your choice. Look into what files your browser supports and ask yourself if you need a separate program for the same feature.



Use EFF's Panopticlick and don't use browser at full screen in order to test and obfuscate your browser fingerprint. A browser fingerprint identifies you based on your settings, apps, plugins, OS, screen size, etc. It violates PERSEC, but there are several extensions that can help. The two most popular browsers are Firefox and Chrome. The real differences between the two are that Chrome is more polished with better dev use and syncing capabilities and that Firefox is more

customizable, has better extensions, respects user privacy, and is lighter on resources like RAM. Which is better at security depends on your customization with extensions, otherwise Chrome is more secure out of the box. Make certain to block 3rd party cookies. If necessary, download / install a browser for single purpose. I use Chromium with several of my favorite security extensions disabled to use several sites that would otherwise be unusable or gaping vulnerabilities on my Firefox set-up.

FIREFOX

Firefox will always be my most recommended browser for anyone that cares about privacy and wants more security- and privacy-focused add-ons than the Chrome Web Store has to offer. My suggested security preferences are to set DuckDuckGo as your only search engine (privacy-based search engine that uses “!” or bangs to access other search engines) with ‘provide search suggestions’ disabled, block pop-ups, enable Tracking Protection and Do Not Track, disable Location Bar options, disable history or use custom settings and add exceptions to sites that need cookies like ProtonMail, disable everything under Data Choices, and disable updating search engines. The latter only screws with your search engine settings by resetting default to Yahoo! every update and adding all removed search engines back to Firefox. You should also open about:config to make and experiment with the

configurations. Some of these changes will break sites so try to only add a few at a time and start testing:

- browser.bookmarks.autoExportHTML;true
- browser.cache.disk.enable;false
- browser.cache.disk_cache_ssl;false
- browser.cache.offline.enable;false
- browser.formfill.enable;false
- browser.privatebrowsing.autostart;true
- browser.safebrowsing.enabled;true
- datareporting.healthreport.uploadEnabled;false
- dom.event.clipboardevents.enabled;false
- #dom.storage.enabled;false (this will break ProtonMail)
- geo.enabled;false
- media.peerconnection.enabled;false
- network.cookie.lifetimePolicy;2
- network.cookie.thirdparty.sessionOnly;true
- network.dns.disablePrefetch;true
- network.http.sendRefererHeader;0 (caution; may break sites)
- network.http.sendSecureXSiteReferrer;false
- network.prefetch-next;false
- plugin.scan.plid.all;false
- privacy.donottrackheader.enabled;true

- privacy.donottrackheader.value*;1
- privacy.trackingprotection.enabled;true
- #security.ssl.require_safe_negotiation;true
- security.ssl.treat_unsafe_negotiation_as_broken;true
- security.ssl3.ecdhe_ecdsa_rc4_128_sha;false
- security.ssl3.ecdhe_rsa_rc4_128_sha;false
- security.ssl3.rsa_des_ede3_sha;false
- security.ssl3.rsa_rc4_128_md5;false
- security.ssl3.rsa_rc4_128_sha;false
- toolkit.telemetry.enabled;false

Next, we need to discuss browser extensions. Most of these are available on Chrome as well, but the ones that aren’t will be specified with alternatives for Chrome found later on this page under Chromium / Chrome. The recommended extensions include:

- **Disconnect** – blocks ad trackers, social widgets, and other tracking elements without the potential spying concern found with rival Ghostery.
- **uBlock Origin** – lightweight adblocker that allows user full control beyond AdBlock Plus that allows specific ads with the same features as ABP. This may conflict with Disconnect on Chromium / Chrome browsers.

- **HTTPS Everywhere** – EFF's best creation. It forces every site to use HTTPS (encrypted web traffic) over HTTP (unencrypted and very visible web traffic) if HTTPS support exists.
- **Privacy Badger** – Another EFF creation, but that rivals Disconnect. It's a tracker-blocking tool that needs to learn web patterns to learn which trackers to block and leaves some trackers open so 1) some sites work and 2) users have to tweak the settings for their own, personal use. Relying solely on Disconnect with no settings changes is bad.
- **Web of Trust (WOT)** – ranks sites by security reputation letting you know which sites are safe and which are not.
- **NoScript (Firefox only)** – blocks all scripts from running on pages without your authorization. This is a very time-consuming extension that will require a lot of experimenting to allow the scripts needed for the site to run while everything else is blocked. It's the extension I recommend the most, but also the extension that will have you pulling out your hair the most.
- **Private Tab (Firefox only)** – this is Incognito Mode for tabs. No history or cache is saved.
- **Random Agent Spoofer (Firefox only)** – spoofs your OS and browser settings to obfuscate your browser fingerprint. It's best to set at Random (desktop) for profiles and Random for periodic changes.

- **Self-Destructing Cookies (Firefox only)** – exactly what it sounds like. Any cookies saved are almost immediately deleted.
- **Flagfox (Firefox only)** – lets you know which country the web server you're accessing is based.
- **UnloadTab (Firefox only)** – saves resources like RAM by suspending tabs when they haven't been used for a minute. This is perfect if you use a lot of tabs.

CHROMIUM / CHROME

Chromium is my secondary choice in browser and is the open-source version of the Chrome browser. Everything of note for the Chrome browser will work on the Chromium browser. Let me explain my reasoning behind using Chromium as my secondary browser beyond Firefox having greater privacy and security customization and apps. Chromium / Chrome offers much better Google support from account integration to YouTube use. However, if you were to make Chromium / Chrome your default browser, use a Google account, and use ScriptSafe (Chromium / Chrome version of NoScript), then you would have a broken service. Google requires JavaScript functionality and ScriptSafe is the perfect replica of NoScript with customization and control. In fact, since I don't use Chromium / Chrome as my default browser, I don't recommend mirroring every security configuration and extension for it. I still recommend Web of Trust, HTTPS Everywhere, Disconnect, uBlock Origin, and TheGreatSuspender (UnloadTab for Chromium / Chrome but with even

greater customization). Since some sites require 3rd party cookies, instead of adding the security risk to my primary browser by whitelisting such sites, I use Chromium / Chrome with 3rd party cookies enabled. This also means by use of this browser is very limited to just those whitelisted sites and I use Firefox for everything else. **I also recommend adding WebRTC Block, especially if you use a VPN since WebRTC will leak your actual IP**. We already covered how to do this with Firefox with the about:config changes under media.peerconneciton. As for the settings, I recommend adding DuckDuckGo as the primary search engine, keep local data until browser is quit, block plugin content by default, disable location, notification, microphone, camera access, and automatic downloads, disable prediction and reporting services, enable dangerous site protection and Do Not Track, and disable autofill and saved password functionality. Since Chromium / Chrome doesn’t allow you to not save history data without having to use Incognito mode, don’t forget to clear browsing data each time you quit the browser.

EMAIL

I advise against using email for the most part, but too many services require some form of email during set-up. They’re inherently insecure like wireless networking, especially any using IMAP, POP, and SNMP. Don’t think using email services from different countries will not still be traced back to you post Snowden Revelations. Privacytools.io has some naivety in their description of not using VPNs hosted in any of the 14 Eyes countries thinking 1) that US or any other 14 Eyes country will mean VPN data is unsafe and 2) that other countries can’t be “hacked” or made to give up their data. Unless your data is in Iceland or Switzerland, your data is just as accessible across the globe and even Iceland and Switzerland aren’t impenetrable or incorruptible.

If you’re going to use email services that aren’t especially made for encryption, you’ll want to use GnuPG or PGP and Enigmail (Firefox) or Mailvelope (Chromium / Chrome) to send encrypted messages. This is far from easy and even hardcore crypto users find it annoying, myself included. It’s still effective, but it’s neither an easy-to-use email encryption type or an easy-to-learn email encryption type. I recommend email services that were made to be encrypted instead. However, there’s one large caveat. The previously mentioned methods of email

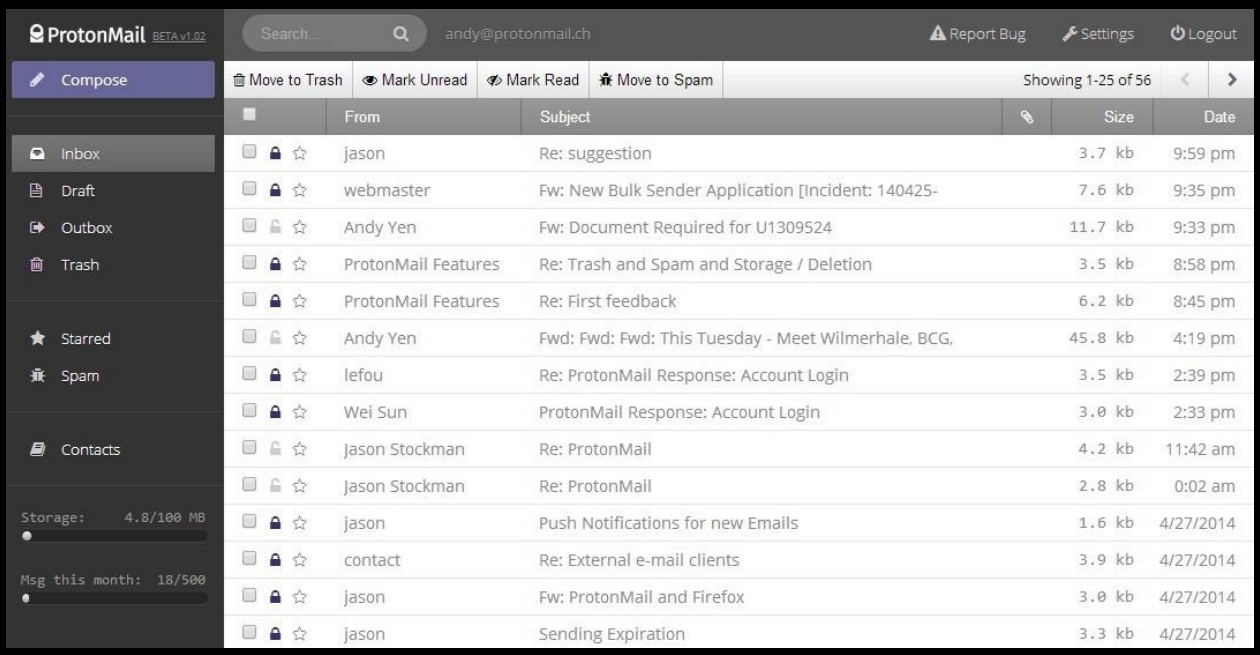
encryption have you decrypt private keys locally. These easier-to-use methods due to server-side. It’s up to you if you want extreme security at extreme inconvenience or great security at great convenience.

PROTONMAIL

ProtonMail is a Switzerland-based, end-to-end encrypted email service originally created at CERN (same birthplace as the web) that’s been advertised with Mr. Robot, offers mailbox encryption on top of email encryption, is easy to use with a sleek design, includes free and premium tiers, has open-source encryption, and has browser, iOS, and Android support. After logging in to your account, you’re made to decrypt the mailbox that only you can access, which offer an additional layer of security, especially if your login credentials got nabbed. Unfortunately, it doesn’t offer 2FA yet, but it is in development. There’s a lot of requests for it to add email client support with IMAP, POP, and SNMP, but that’s a terrible idea. Those services aren’t secure and many web-based encryption email services ignore them so user email is actually secure. It would be the equivalent of having a perfectly secure home system and network set-up, but then you use an iPhone as your smartphone.

The free version includes up to 500MB of storage, 1 address (unless you signed up during beta like me where you get a .ch domain with .com), up to 150 messages sent a day, and 20 labels. The other tiers

can be customized with up to 20GB storage, 10 custom domains, 50 addresses, 1,000 messages sent a day, 200 labels, and full support from $48 to $288 annually. You can set up a recovery email, which would also be the email address if you use email notifications to notify another email account you have unread mail. This makes



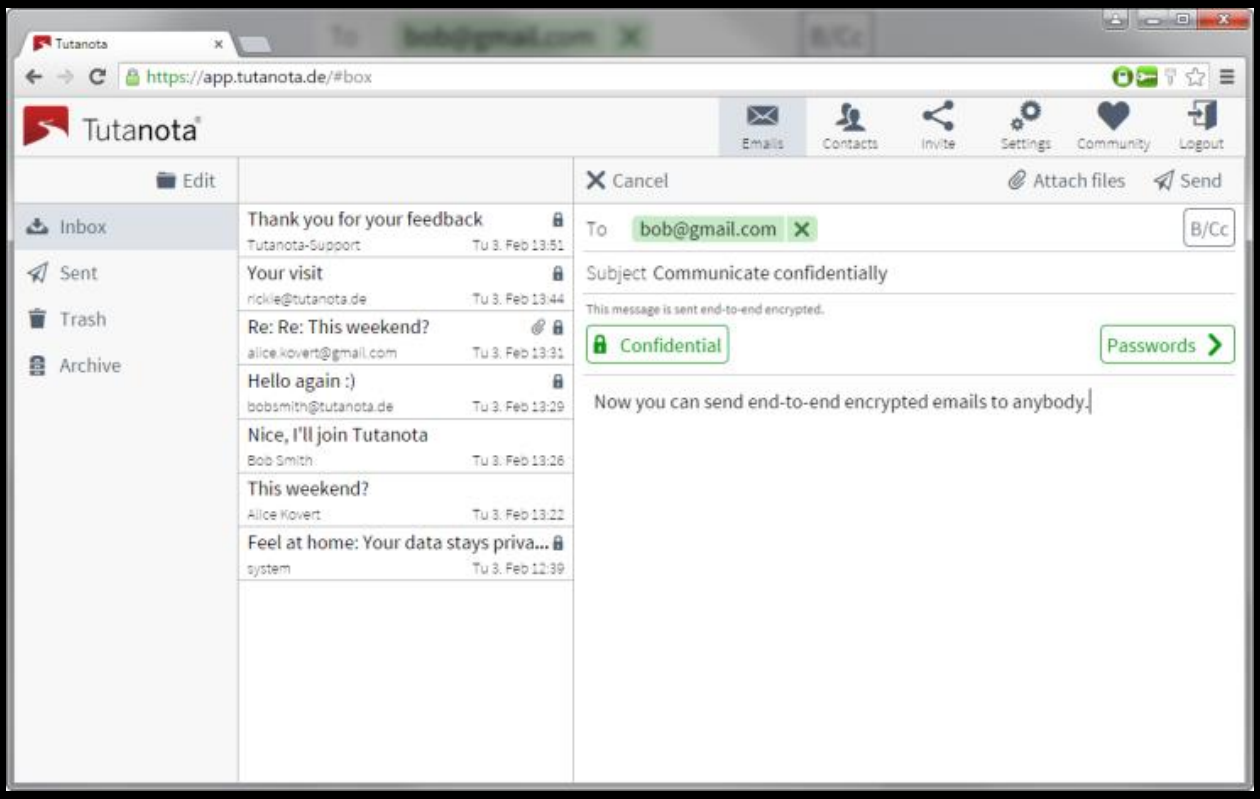
ProtonMail the perfect email service to have multiple accounts with a separate email service like Tutanota to act as a hub (notification) account. You have the options to display photos manually (photos have been used in email to spread malware), to create whitelist, blacklist, and spam filters, to have basic, advanced, or no login logs that can be downloaded, appearance customization with custom CSS support too, and payment options that allow credit cards (think disposable), PayPal, and Bitcoins. It doesn’t have the means to instantly import

Gmail emails or export own emails yet, but they’re always trying to add more services. Let’s hope an email client is made one day.

TUTANOTA

Tutanota is a Germany-based, end-to-end encrypted email service, that’s just as easy to use as ProtonMail without the mailbox encryption, sleek design, or filters. However, it does have browser, iOS, and Android support, free and premium tiers, and open-source encryption. Now, while it doesn’t offer mailbox encryption, it does offer something equally great. When Tutanota users email users of different email services, Tutanota does create an encrypted account to store emails for the recipient for just that encrypted connection. It’s like a relay mailbox that the unencrypted user can access via an email link so long as they have the password and view every single encrypted email sent to them by the sender with that password. It would be great if both services adopted both mailbox strategies. I would also say it’s easier to delete than ProtonMail making it the perfect encrypted email service to use when actual disposable services are blocked. What Tutanota offers is last successful login log with a counter of failed logins, filters including spam, device control, 1GB storage, custom domains, addresses, and storage with premium accounts, user management, and welcome message and logo design for premium users. The premium pricing ranges from $13.50 annually for additional users, 1GB storage per user, 5 addresses, custom domain support, more

advanced inbox rules, and welcome message and logo customization to $675 annually for 1TB storage and the same premium additions.



CHAT

Chat services are definitely recommended over email addresses, even though sites and services don’t send notifications and recovery information to chat services. They don’t have the same inherent security flaws as email since they don’t use the same vulnerable ports and services. The great news is that there’s myriad, secure chat services from computer to mobile use. BitTorrent’s Bleep, a peer-to-peer, end-to-end encrypted chat service with cross-platform support, hasn’t been added to the list due to previous issues of delays and difficulties with voice calls. Otherwise, I would add that to the top of the list of recommended chat apps with Signal.

- **Signal** – mobile, encrypted app with browser support on Chromium / Chrome that uses end-to-end instant messaging replacing your default texting app as your secure texting app. It’s free, open-source, allows group chat, identity auditing with connections, and allows voice calls replacing your phone app as well. It works best if your contacts use Signal too, otherwise connections are not encrypted with non-Signal users.
- **ChatSecure** – mobile, encrypted app built on top of Google’s old Talk app with XMPP use. It uses OTR, or off-the-record, encryption and privacy rules and is a part of The Guardian

Project, which includes Orbot (Android Tor client), Orfox and Orweb (Android Tor browsers), Ostel (end-to-end encrypted VoIP service), and ObscuraCam previously mentioned in SYSSEC under Android. Until Signal was released, ChatSecure was the highest recommended mobile, encrypted chat service.

- **IRC** – an old chat service still used today that can be secure or not depending on the user's configuration. In fact, it's not like the other services listed here since it's not a chat service that was built with encryption in mind. Internet Relay Chat is mid-'90s tech that uses channels and peer-to-peer connections with each client requiring a server to communicate. However, it offers way too many options in-chat to ever be discounted from creating secret channels to establishing channel operators and from making users invisible to banning users from channels. Mr. Robot has shown that IRC hasn't lost any of its power or sleekness.
- **CryptoCat** – a browser-based, end-to-end encrypted IM service that's open-source and free. It's a great tool that's been recommended numerous times, but previous uses with others show that it's apparently not an easy-to-understand service from not figuring out how to install the extension to not knowing the difference between the chatroom name and usernames.
- **hack.chat** – a browser-based, minimalist IM service that uses HTTPS encryption, custom channel support, and includes Android

apps if you don’t want to use the mobile browser. It functions through the hack.chat site with custom channel names at the end of the URL so no installations are needed. It’s certainly light enough not to need an app so I don’t recommend installing one for Android, but hack.chat is a lightweight alternative to CryptoCat that’s too difficult for users not to understand how to use it.

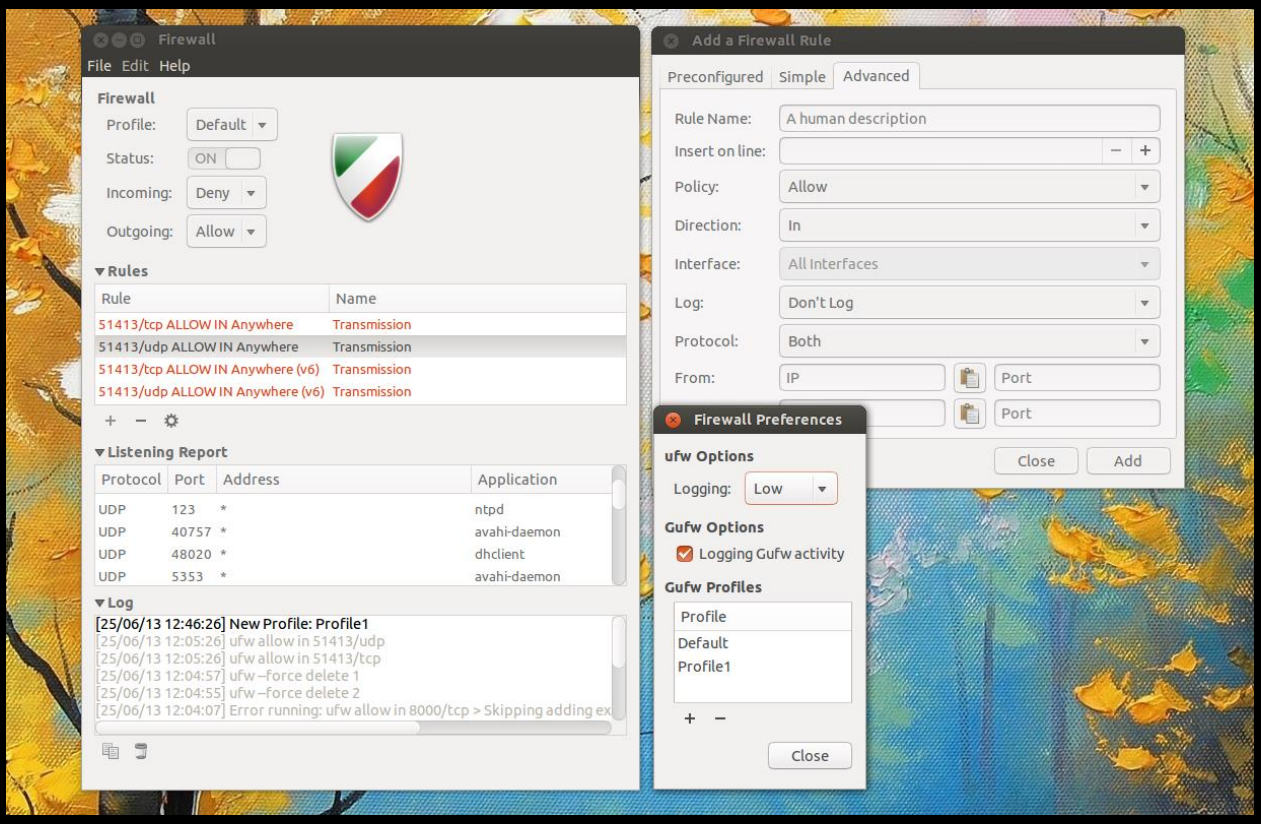
- **FireChat** – mobile, peer-to-peer IM service that’s neither encrypted nor uses an Internet connection. In fact, it uses mesh networking with Bluetooth, Wi-Fi, and Apple’s Multipeer Connectivity Framework. It’s a chat service that’s meant for local use and has proven great for communicating during protests when authorities block Internet connections.
- **Jitsi / Pidgin** – both services are free, open-source IM services that are cross-platform on computers with multiple communication types support like XMPP and use OTR encryption and privacy rules. However, Jitsi also has Android support.
- **Tox** – cross-platform, end-to-end encrypted, peer-to-peer IM and voice calling chat service that’s free and open-source. If you want a secure IM service that’s cross-paltform, this is your best option since it has Windows, Linux, OS X, Android, iOS, Sailfish, and FreeBSD support.

FIREWALL

Firewalls are undeniably the most critical aspect of NETSEC that monitors and controls incoming and outgoing network traffic on the given network or network connection. It’s the filter that can keep your apps and programs from leaking your data online and stop attackers from intruding on your network. Where you set up firewalls on your network matter. Placing it outside your network makes it accessible to attackers, placing it beside your network gives attackers the choice to bypass it, and integrating it with the network can lead to configuration problems if not done properly. It’s generally recommended to place the firewall just within the network acting as a barrier between your router and your devices, but you can configure it within the router too so long as you have firewall configuration experience. There are two types of firewalls: network firewalls and host-based firewalls. You would know these as hardware and software firewalls. The network / hardware firewalls are software firewalls acting on computer hardware whether bought as a firewall or created with routers or Raspberry Pis. The host-based firewalls are the software generally found on your computer. For Linux, I recommend UFW. For Windows, I recommend firewall apps because Windows Defender sucks. You could also go out of your way and construct your own.

UFW / IPTABLES ----------

ufw is the uncomplicated firewall, which is a CLI tool. If you want the GUI version, install Gufw too. It’s a Linux firewall tool that uses iptables for configuration and iptables is a Linux kernel firewall to configure rules over tables it chains and saves. Instead

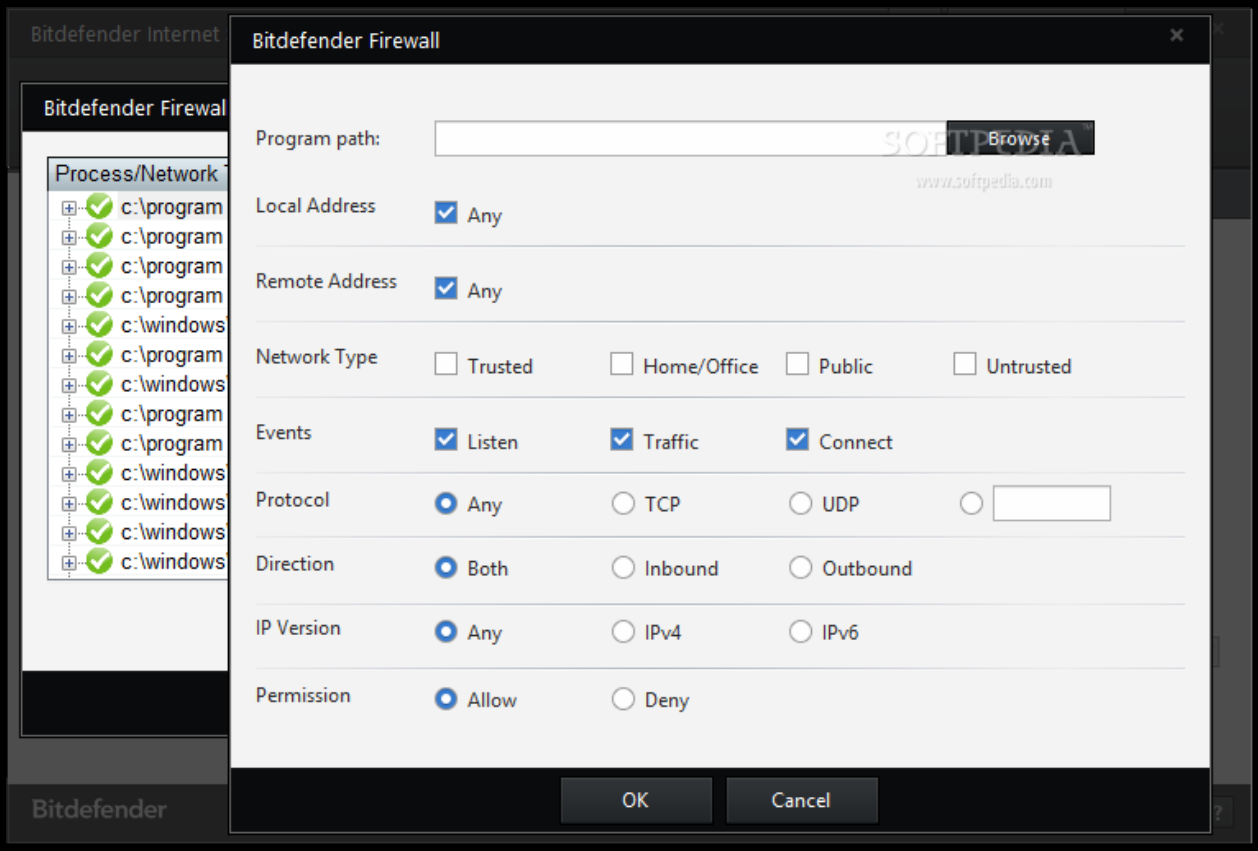


of saving rules individually, they are chained together in sequences over a table, which is why you won’t see the latest rule changes necessarily at the bottom of iptables. G / ufw has IPv6 support, reports status, has verbose logging, allows app integration, sets default policies (set ‘deny all’ as default), rejects incoming rules, allows different logging levels, has bash support, has reset options, and more. G / ufw are the ‘it’ Linux firewalls to use, but they

require a bit of knowledge and experience in both setting up firewalls and how to use. They’re not as friendly as app firewalls.

BITDEFENDER

If you’re already using Windows and you’re cautious about malware, purchase the BitDefender Security Suite. Prices vary, but I’ll let you research that since they offer more than one product, multiple licenses, and prices do vary over time. It’s not the greatest at malware scanning, but all AVs are horribly ineffective at malware protection. Remember, it’s a security suite that’s awesome for reasons unrelated to its AV functions. In this case, it would be the app firewall that’s easy-to-use and non-intrusive.

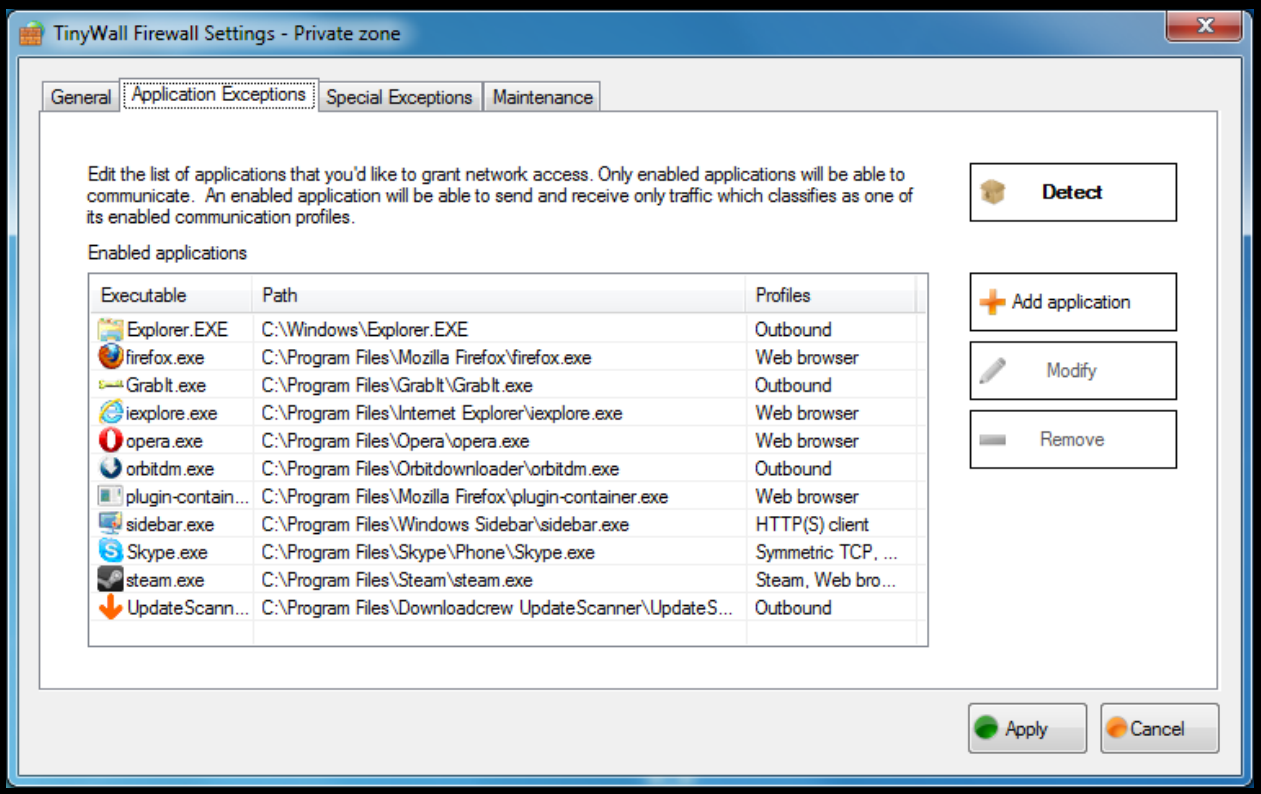


BitDefender’s firewall uses four network types of trusted, home / office, public, and untrusted, three stealth modes of on, off, and remote, whether or not you want to use generic settings, and views incoming and outgoing network data. Adding firewall rules can use any combination of network types, allows local and remote addresses, and event types of listening, traffic, and connecting. Each rule can be set with TCP, UDP, or any protocol types, inbound, outbound, or both types of traffic, IPv4, IPv6, or both IP versions, and whether or not the rule permits or blocks traffic with the rule settings. After setting up the rules, you can view firewall logs under firewall events. The logs will include the application with file path, protocol used, port accessed, whether or not BitDefender permitted or blocked the traffic, and the date and time of the event. If you’re already using Windows and need an AV, why not use BitDefender?

TINYWALL

TinyWall is an easy-to-use, lightweight, non-intrusive app firewall for Windows. If your intention was to have an app firewall that was single-serving and not part of a security suite, then you found your best solution. TinyWall doesn’t need you to understand ports, protocols, and app details to function and doesn’t use constant pop-ups. What it includes is automatic learning mode, firewall tampering protection, settings lockdown via password, quick modes, host file protection, IPv6 support, view ports and port statuses on your

machine, and more. It works with Windows Firewall to function as a firewall without the terrible default configuration or learning curve required to use it. In this regard, TinyWall is great for the layman. However, it’s also great for when you’re in a hurry and need security like Pokedex.sh is to BASEC.sh.



CHARIZARD

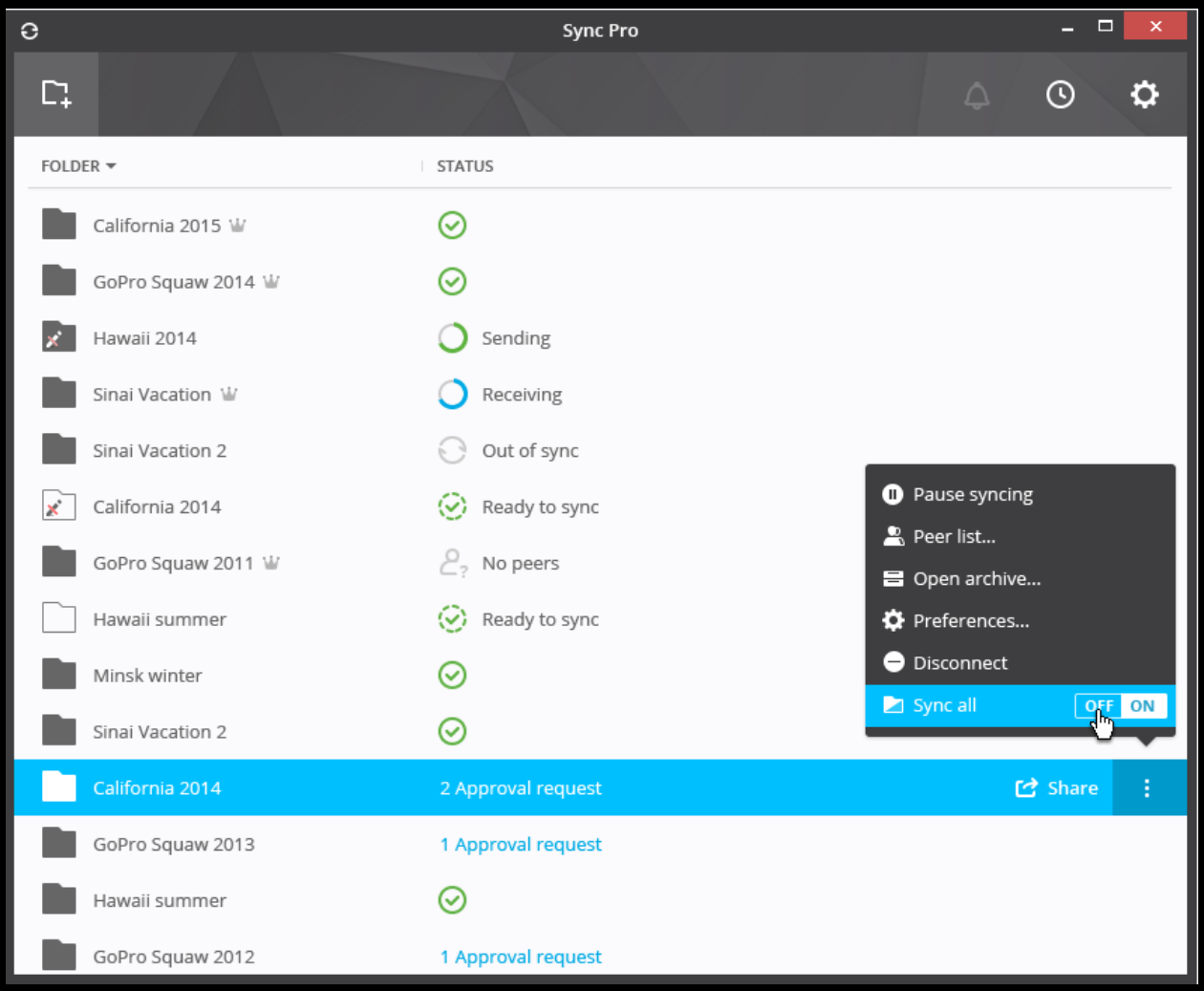
CLOUD

Many older power users will go on security rants about the problems with cloud technology. They're right about your data being insecure in the same sense that you're safe from "hacks" if you don't own or use a computer. There are several cloud services that are secure, but you'd do best by encrypting files before sharing them across machines anyway. File encryption is perfect for this as well as using partition encryption on removable media such as UFDs and SD cards when sharing locally. However, sometimes you need to share data over an Internet connection and using Google Drive, Microsoft's OneDrive, Box, and Dropbox are just bad ideas. The latter two are less secure that Google Drive and OneDrive. You do have encrypted options though.

BITTORRENT SYNC

BitTorrent Sync is not an encrypted cloud service in the least, but it offers what others do not: shortest-path transfer without cloud or uploading to 3rd party servers. The only time a 3rd party server is used is as a temporary relay server between two ends using VPNs. The data is immediately overwritten by other people's data when your connection is disconnected and others use the server for the same purpose. There's no file size limitation since all the files are saved on your own system and whatever devices are connected. For example, sharing

files with friends is easiest with BitTorrent Sync. You'll both have local copies and no one else. You're not limited to the uploading and downloading bandwidth of a cloud service but your own ISP bandwidth.

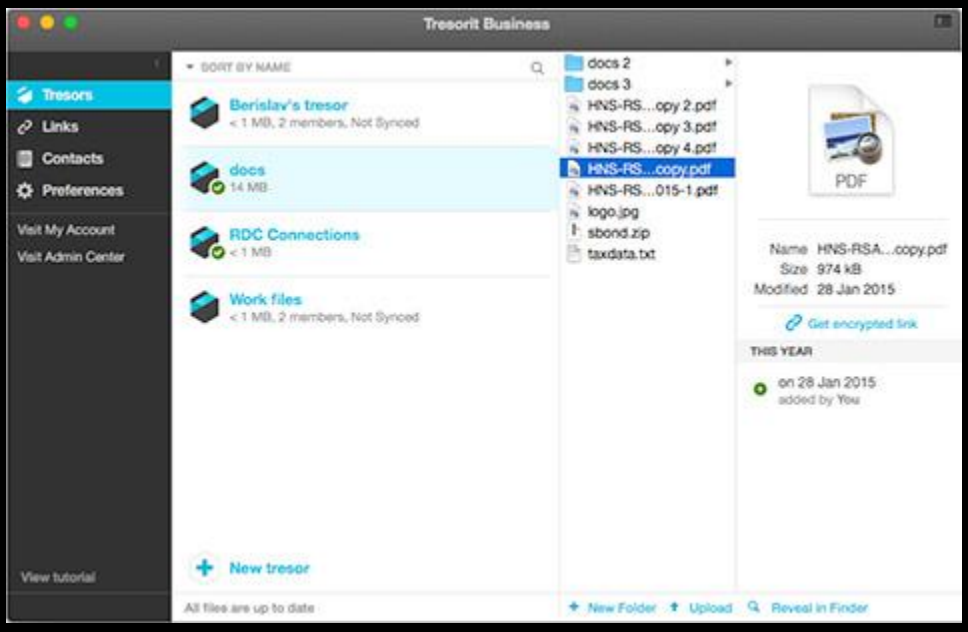


You can modify bandwidth used as well as how you share the files or folders connected, permissions of reading and writing, requiring users to authenticate files, expiration dates on links, and more. The premium version includes save space with selective sync, changing folder permissions at any time vs only before sharing, and with business use permitted since there's also dedicated enterprise

versions. It’s the alternative to cloud services to share files and it’s support covers Linux, Windows, OS X, FreeBSD, iOS, Android, Windows Phone, Amazon’s Fire OS, and numerous NAS architectures.

TRESORIT

Tresorit is a Hungary- and Switzerland-based, end-to-end encrypted cloud service that offers cross-platform support on Linux, Windows, OS X, Android, iOS, Windows Phone, and BlackBerry. After the Snowden Revelations, the devs started a “hacking” contest to crack Tresorit’s encryption or otherwise exploit their cloud services. The reward was initially $10,000 which had risen to $25,000 and then $50,000 after a few months. After a well over a year, no one was able to crack the encryption.

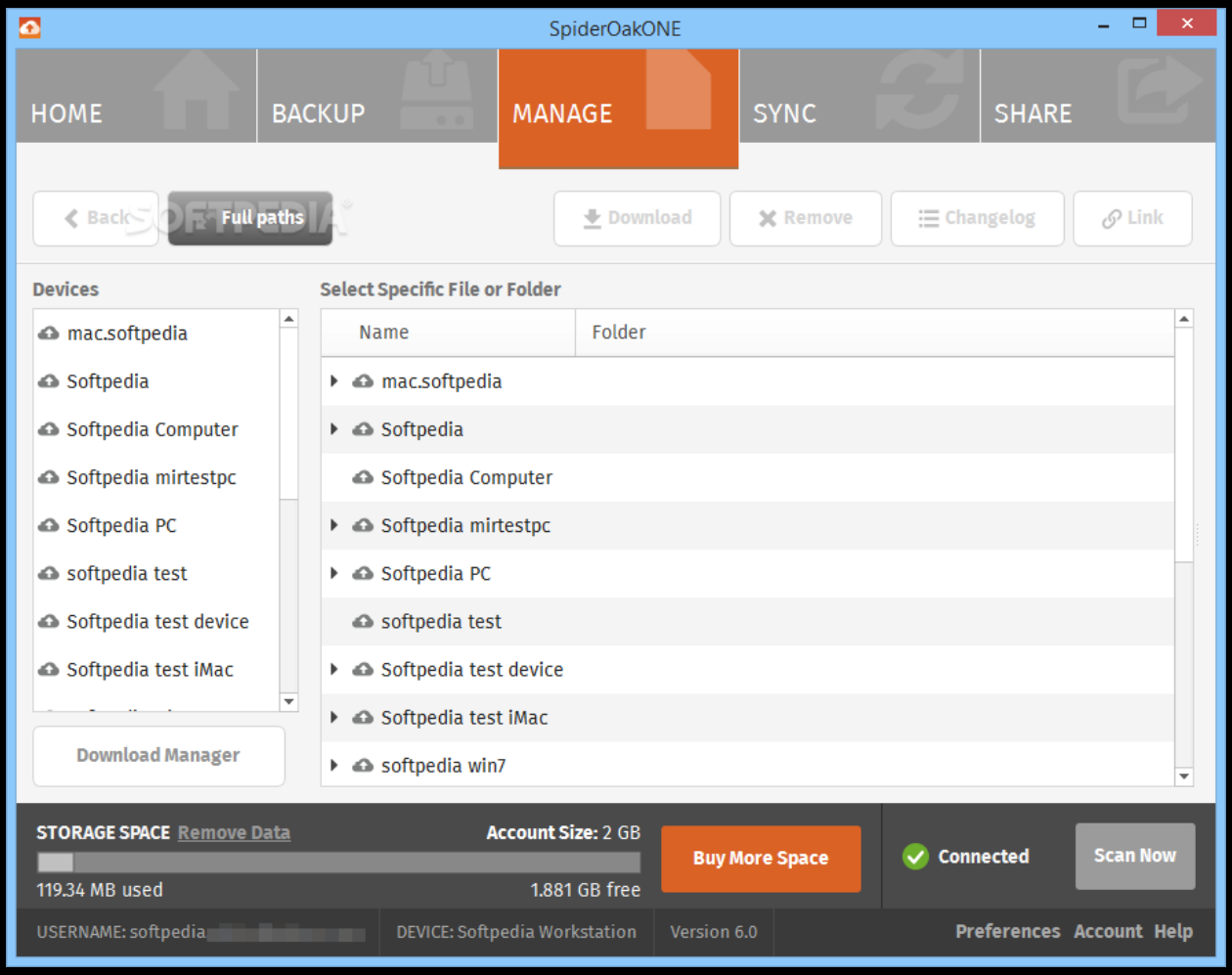


Tresorit has a sleek, easy-to-use design and used to offer free accounts. Unless you acted when the promotions occurred, you have to now pay to use Tresorit, but there are 14-day free trials. The premium account is $12.50 a month for 100GB storage, zero-knowledge syncing, equally secure across all devices, and offers

version and activity history. My switch from my 15GB account to BitTorrent Sync only occurred since Tresorit doesn’t redownload or modify Tresorit files on Android after syncing so commonly used files would have to be downloaded again constantly. However, I still maintain my account for Project Honeydrive since it’s an excellent service worth using whether with free or premium accounts.

SPIDEROAK / SPIDEROAKONE

SpiderOak is a US-based, client-side encrypted cloud service that offers cross-platform suppert with Linux distros Debian, Fedora, and Slackware, Windows, OS X, Android, and iOS. It’s been around for almost ten years, whereas Tresorit has for five, is somewhat open-source with plans to go fully open-source, and uses zero-knowledge privacy where only the users can view contents. It’s not wise to trust client-side encryption when end-to-end encryption is safer. SpiderOakONE is the Linux version of SpiderOak that’s built on top of Canonical’s discontinued UbuntuONE which is as visible in the syncing as it is in design. Beyond the 2GB of storage for a 60-day trial, SpiderOak comes in three tiers: $80 annually for 30GB, $130 annually for 1TB, and $280 annually for 5TB. If price is your only issue, then $130 for 1TB with SpiderOak is better than $150 for 100GB with Tresorit. However, if security is your issue, I advise using Tresorit instead since it uses end-to-end encryption and has been very transparent about the successful “hacking” contest.



One reason you would want to use SpiderOak over Tresorit, besides a free trial four-times as long, is the use of sharerooms. Tresorit users can’t share files with non-Tresorit users since an account is needed to view Tresorit links. However, this isn’t the same for SpiderOak. You can create sharerooms, or links to folders and / or files, that users can view over the web and download the contents if wanted.

OwnCloud and SSH aren’t mentioned since OwnCloud has a learning curve and SSH is a secure way to share files, but it’s neither easy to use

nor automate. Plus, OwnCloud is really just a client-server application where users have to build their cloud servers and sync data to it. In this regard, using Raspberry Pis to create an OwnCloud server and syncing with BitTorrent Sync is a popular project. However, this option is very unnecessary if you don’t need a centralized server for your own local files.

CLOYSTER

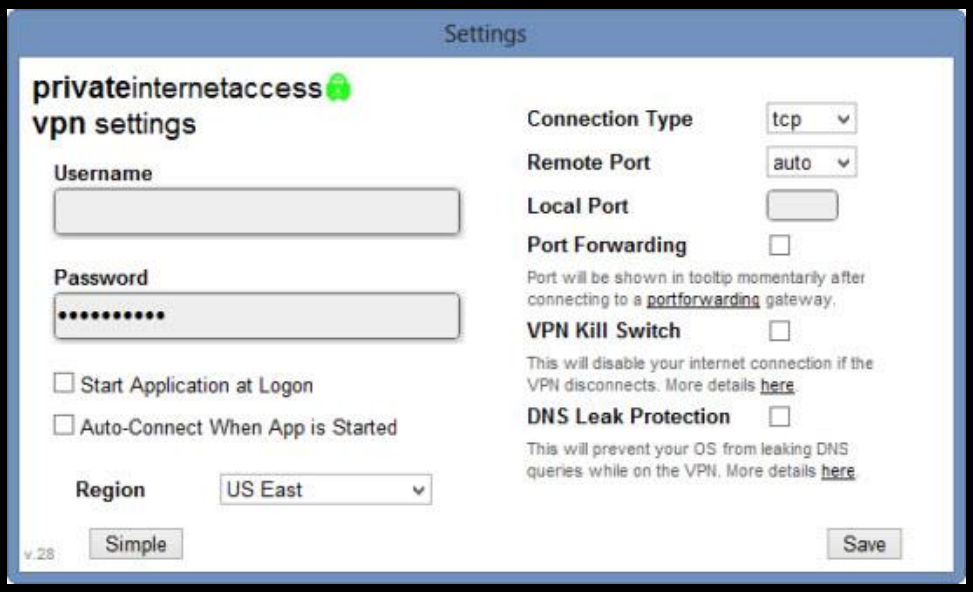
DOWNLOAD & INSTALL BITTORRENT SYNC

VPN

VPNs are another best friend along with wired networks. VPNs, or virtual private networks, can secure and encrypt network traffic and / or use proxy functionality to hide user geolocation data. Proxies are commonly used in schools to block site restrictions and VPNs have been used to commit “geolocation piracy” to bypass counterproductive geolocation restrictions to maximize on customer price gouging. You should really only use this for the good of privacy, but it and Tor has been used for evil. It makes someone conducting digital reconnaissance against your online accounts from the public IP information difficult without knowing how to track and crack the VPN service. For example, let’s say you use Twitter, you’ve left the security settings at default, and you don’t use a VPN or Tor to obfuscate your network information. Anyone can use Tinfoleak to extract your network and geolocation information down to your GPS coordinates to find the exact spot you were during your last tweet. VPNs are part of the dark net (like Tor is part of the dark web) through packet and tunnel encryption. If you want to find the best VPNs, TorrentFreak does an annual review. While PIA is touted by many as the best, cheapest, most secure, and most privacy-respecting VPN, PIA does support TorrentFreak which may lead to bias.

PRIVATE INTERNET ACCESS

Private Internet Access is a great VPN subscription for $40 annually with P2P and VoIP support, PPTP, OpenVPN, L2TP / IPSec support, covers 5 devices simultaneously, SOCKS5 Proxy, unlimited bandwidth, and over 3,300 servers in 25 countries. PIA doesn't keep logs from traffic and DNS data to metadata (which was seen when the FBI wasn't capable of retrieving a suspects' VPN logs), accepts Bitcoin and PIA gift cards, and doesn't filter, monitor, censor, or interfere with user traffic. Additional layers of security include a kill switch to kill Internet traffic when the VPN is disabled, IPv6 leak protection, DNS leak protection, and mixes user traffic together to better obfuscate user traffic. The incident with the FBI was the very first incident reported that the FBI contacted PIA over user data unlike most popular Internet services. It's best used with AES256, RSA4096, and SHA256. It's versatile and lightweight. It's not recommended if you've done PROJECT DEVICE PERSEC, but you can put PIA on your router so that all devices on the network uses the



same VPN connection vs each computer using their own. However, this links your network traffic to a single VPN instance. I can’t justify the router use since I only have 4 systems with a constant VPN connection and 2 systems with VPN connection when used occasionally. Be careful using PIA’s kill switch with Bitdefender on Windows. Network loss will activate the kill switch, which Bitdefender interprets as an attack. The conflict causes a BSOD, or blue screen of death.

TORGUARD

Torguard is touted as the rival to PIA for the title of the best, most secure, and privacy-respecting VPN. However, it costs $60, which is $20 more expensive than PIA. In fact, Torguard is almost identical to PIA so if any features are not explicitly mentioned here, know that’s because it’s the same as PIA. Torguard has over 1,600 servers in over 50 countries, uses up to RSA2048, accepts over 200 types of payment options with numerous cryptocurrency options, and was made for P2P use. Torguard also includes bundles of different services where the Torguard VPN includes the Torguard Proxy, the Torguard Proxy alone, Torguard email, or all three combined. In order to have SOCKS5, SSH, and HTTPS support, users must buy the full bundle, which appear to be popular and broken. I still recommend PIA over Torguard, but Torguard is the next best choice if you need multiple VPN accounts. Using the

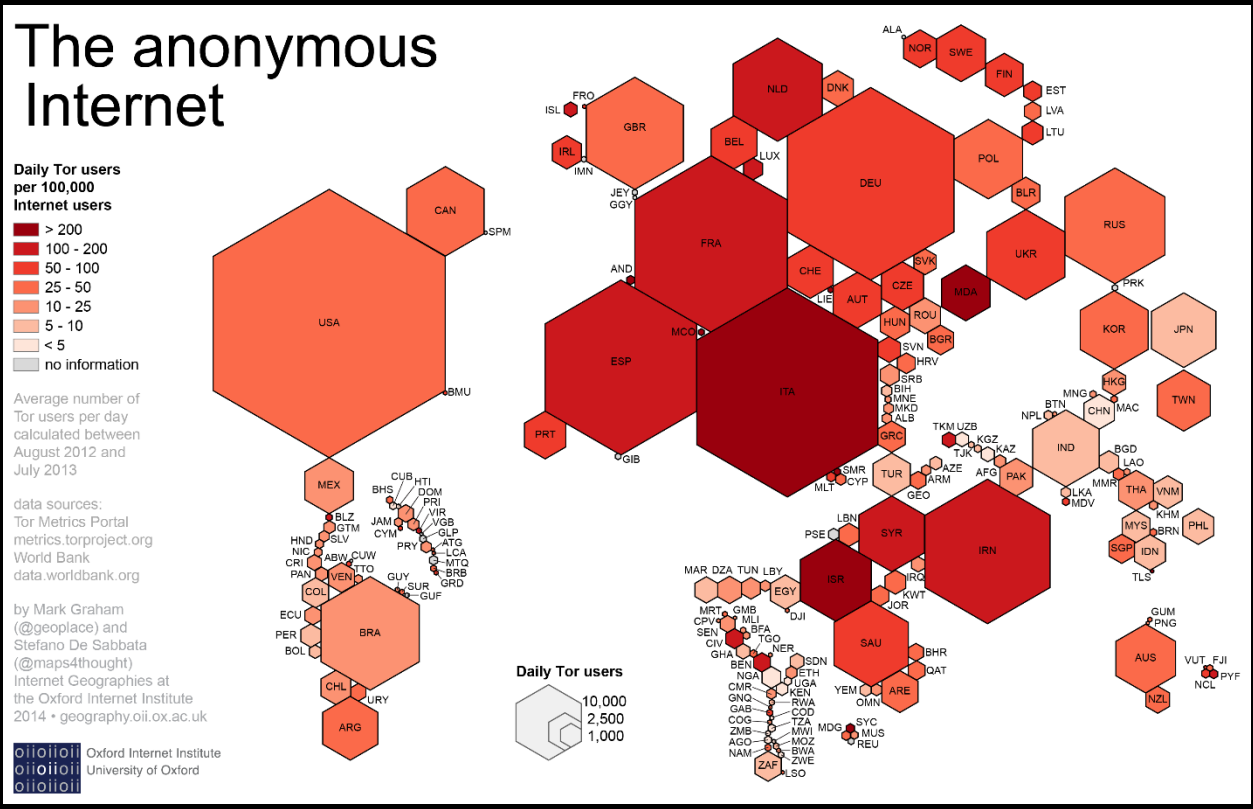
same service with multiple accounts may not be the best use of PERSEC depending on what you’re doing.

GASTLY

DOWNLOAD & INSTALL DNSCRYPT

TOR

Tor, also known as The Onion Router, is an anonymous networking service meant to scramble and hide the identifying network information of its users. It works by encrypting data and the destination IP address multiple times and sends the data out to a relay server. Each relay server decrypts one of the encrypted layers and sends the data to the next relay server until it reaches the destination.



These servers are communal and the philosophy behind Tor is that there’s safety in numbers; the more users that use Tor, the safer each Tor user is. However, this philosophy is better adopted my VPN servers

since VPN servers are safer in comparison, especially considering how many VPN users outnumber Tor users.

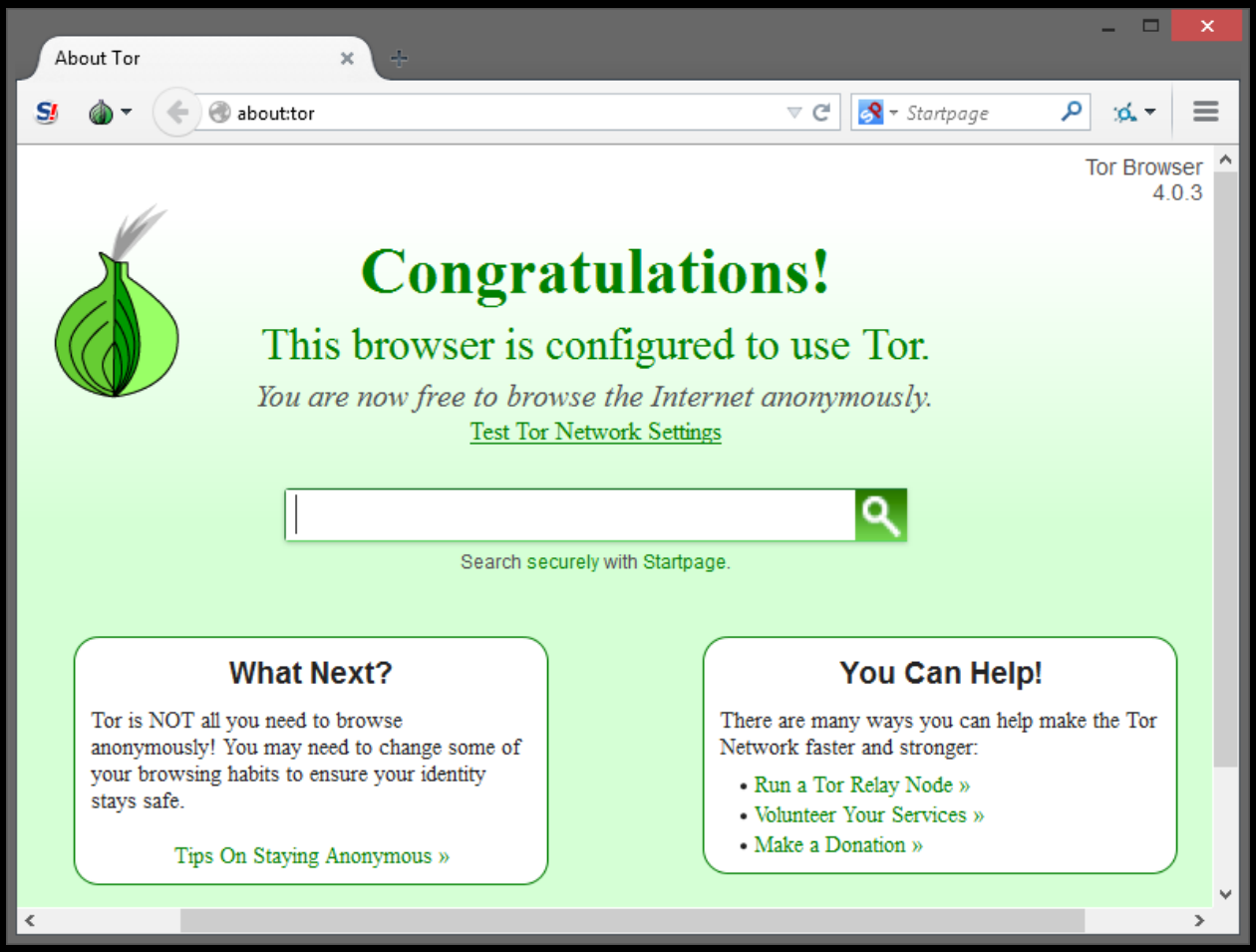
USE

There’s specific uses for Tor since it’s a unique networking service that calls attention to itself. The very first rule is to always use a VPN connection when using Tor. Your ISPs log which IP addresses are using Tor. They can’t see the traffic, but they can detect that Tor is used. VPNs masks this use since VPNs secure the tunnels and packets, not just the packets. Public connections are a different story and using Tor bridge relays is an alternative to using VPNs for the same effect. The second rule is to never use P2P services over Tor. It’s unsafe and ends up cracking your anonymity. The third rule is to only use Tor when needed. Constant use of Tor is just as identifying and suspect as using it over the Clearnet and with P2P services. Moderation is key for a great number of things in life; using Tor only when needed is one of those things. You can use it more than just when needed, but it should not be the primary browser you use for general browsing. That’s just bad PERSEC.

BROWSER

I recommend using the Tor browser with Tor. It’s Firefox with TorButton, TorLauncher, NoScript, HTTPS Everywhere, and Tor proxy. Some users advise not installing plugins. I recommend this for the most part since those plugins will violate your anonymity for

security. The preset extensions and safe browsing habits should be the only security you need and the habits aspect is covered by BASEC.



However, if you use Tor Hidden Services, then I recommend installing one additional tool: Darkweb Everywhere. It’s a fork of HTTPS Everywhere that forces sites to use Hidden Services where applicable like HTTPS Everywhere does with HTTPS. I also have a couple more rules for Tor use but with the browser. The first is to never open anything downloaded via Tor while the Tor connection is still active. An alternative to this rule is to use PROJECT DEVICE PERSEC to mimic a VM used for general browsing but with general Tor browsing, move the

downloaded file(s) to the host, and open there. For sake of being safe than sorry, it’s best you just close Tor to view the file(s). The second and final rule is to use Bitcoin for purchases. You can use prepaid cards, but it’s up to you to remember what cards are used for what purposes. Using a single prepaid card for purchasing a VPN subscription and this week’s groceries defeats the purpose. It’s easier to manage finances by only using Bitcoin over Tor and VPNs and disposable plastic over VPNs alone.

DOWNLOAD & INSTALL TOR

IDS / IPS

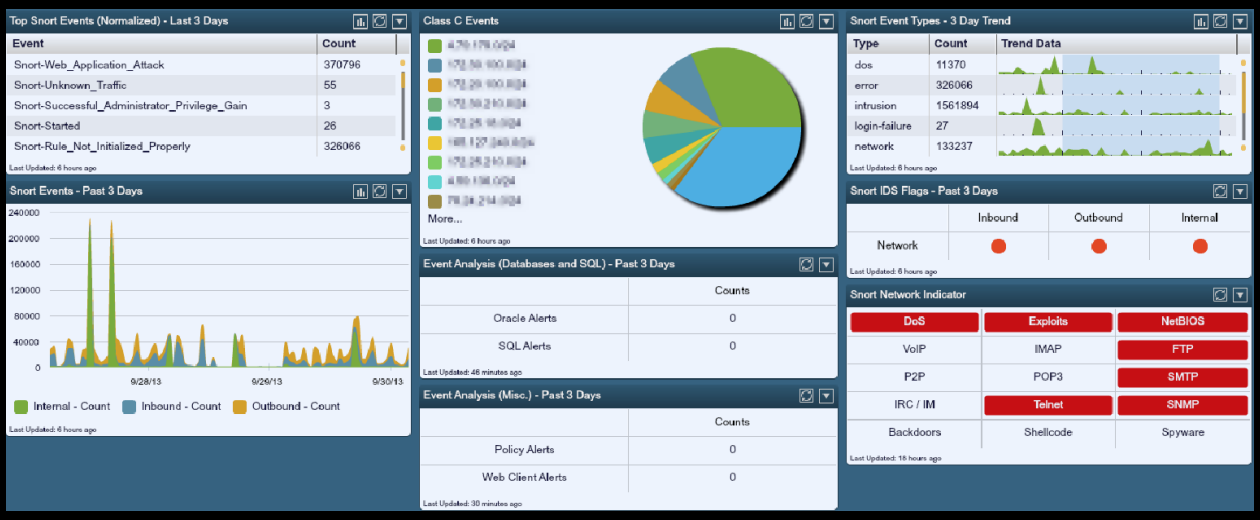
An IDS is an intrusion detection system that monitors cached network traffic to detect malicious activity. It’s a lightweight, logging system for users to analyze which traffic is normal, which traffic is suspect, and how they want to go about handling suspicious traffic. It’s neither a live system nor a preventive system. It only logs network traffic.

An IPS is an intrusion prevention system that blocks live, malicious traffic. It’s a heavyweight, blocking system that analyzes traffic itself, makes decisions based on preset rules, and is the evolution of an IDS. Some state an active IDS and IPS are the same and others say an IPS is actually an IDPS since there’s a discourse on whether or not an IP actually logs traffic.

SNORT

Snort is a well-known IDS / IPS solution that’s open-source, cross-platform, and has free and premium tiers. It’s very effective and customizable, but comes with quite a learning curve. In the past, several of their own installation guides were either lacking in specific commands or failed to include packages needed that Linux distros no longer had preinstalled. Snort is one of many tools that I recommend setting up to be automated to generate and display reports,

but the only tool I advise on not having on your main system. Snort can be installed on other devices such as a Raspberry Pi and still be very effective. However, as previously mentioned, Snort may be too difficult to install. Autosnort (Ubuntu version) makes the process extremely easy with only needing input from a user in four areas: MySQL password (twice), Oink code for Snort's IDS rules, and the interface (wireless or wired) that Snort will be sniffing). Since I only recommend wired networks, the interface should be eth0. However, if you're adamant about using wireless networks and have completed Project Honeynet, I recommend setting up Autosnort on a RPi3 with the interface as eth1.

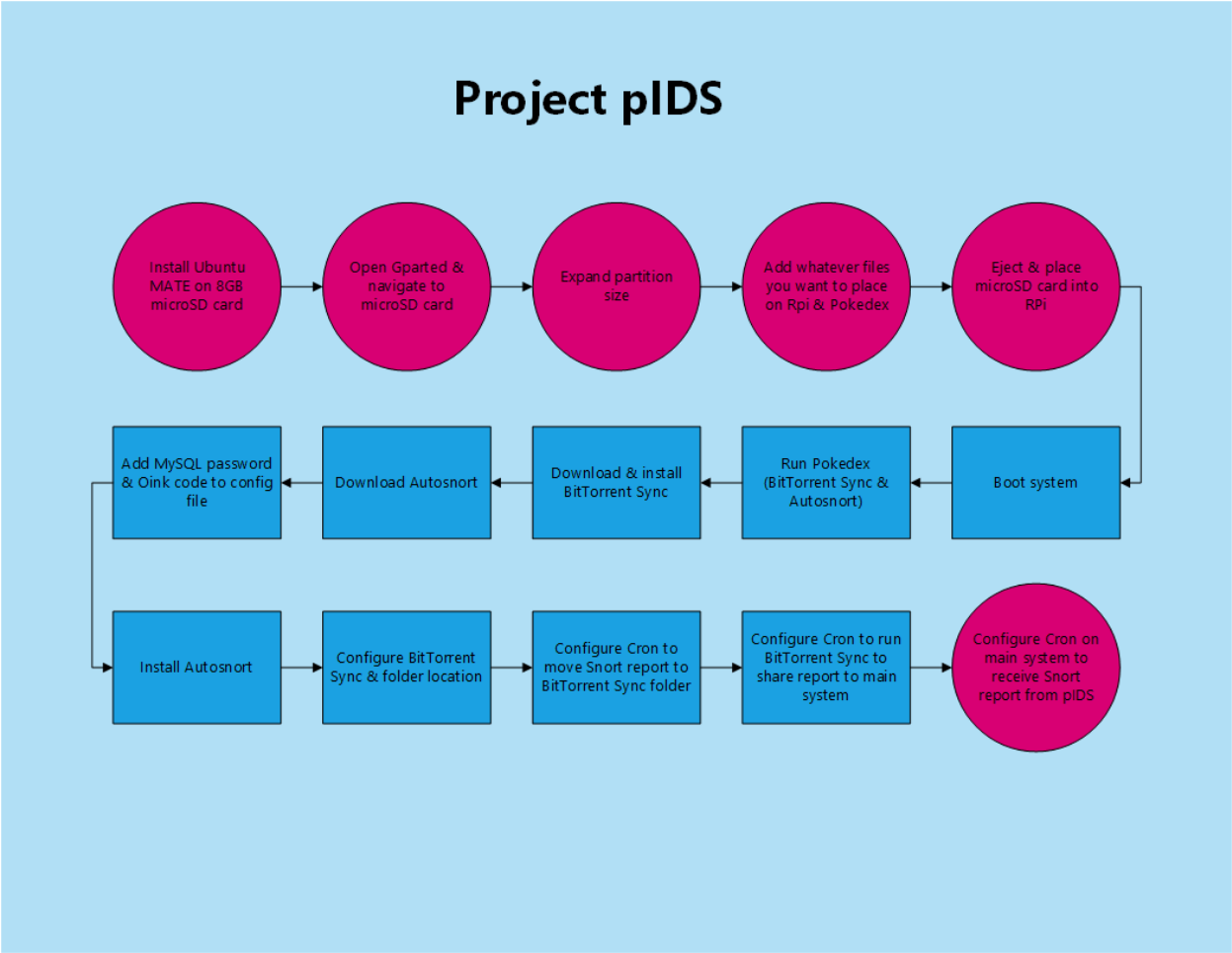


SURICATA

Suricata is another well-known IDS / IPS solution that's open source, cross-platform, only with a free tier. The latter means it's not as a high-quality IDS / IPS solution as Snort, but still worth researching. While Snort has been around since 1998, Suricata has only been around

since 2010, which may explain the differences in quality and features. It’s also a network system monitor that rivals Netdata but with less details.

PROJECT pIDS



This project isn’t a part of PROJECT HONEYNET but for the network you actually use.

01) Purchase Raspberry Pi, microSD card, HDMI cable, and power adaptor. Preferably purchase Model 2.

02) Download and install Ubuntu MATE on microSD card.

03) Download and install BitTorrent Sync on host.

04) Expand microSD card storage space and add Pokedex and Pokemon scripts to home directory.

05) Place microSD card into Raspberry Pi, plug power adaptor into outlet and RPi, plug HDMI cable into TV and RPi, and power on TV.

06) Run Pokedex and Pokemon scripts excluding Charizard, Cloyster, and Gastly since you won’t need SSH and firewall rules to disrupt IDS.

07) Run Autosnort and BitTorrent Sync options.

08) Set up Cron to run BitTorrent Sync weekly to sync IDS report.

09) Set up Cron to run BitTorrent Sync weekly to receive IDS report on host.

DOWNLOAD & INSTALL AUTOSNORT

FUTURE ADDITIONS

BASEC has plans to evolve beyond its current prototype stage. Why keep it a script-system that could be a program? Why only explain how to secure a system post installation vs pre installation too? Why limit support only to Linux for system hardening? Why not elements that are intermediate or advanced beyond the current projects for users to advance even further? Projects are a great means of accomplishing security feats, many of which can be used to cover these very issues.

PROJECT WINDOWS INSTALLATION

This project is to add installing a secure Windows OS.

01) Install Windows with custom settings of disabling all express settings disabled.

02) Remove of Windows apps including OneDrive.

03) Block Microsoft telemetry IP addresses.

04) Configure security apps and settings.

05) Set up BitLocker FDE.

PROJECT LINUX INSTALLATION

This project is to install a secure Linux OS.

01) Edit partition table.

a. Create /tmp partition.

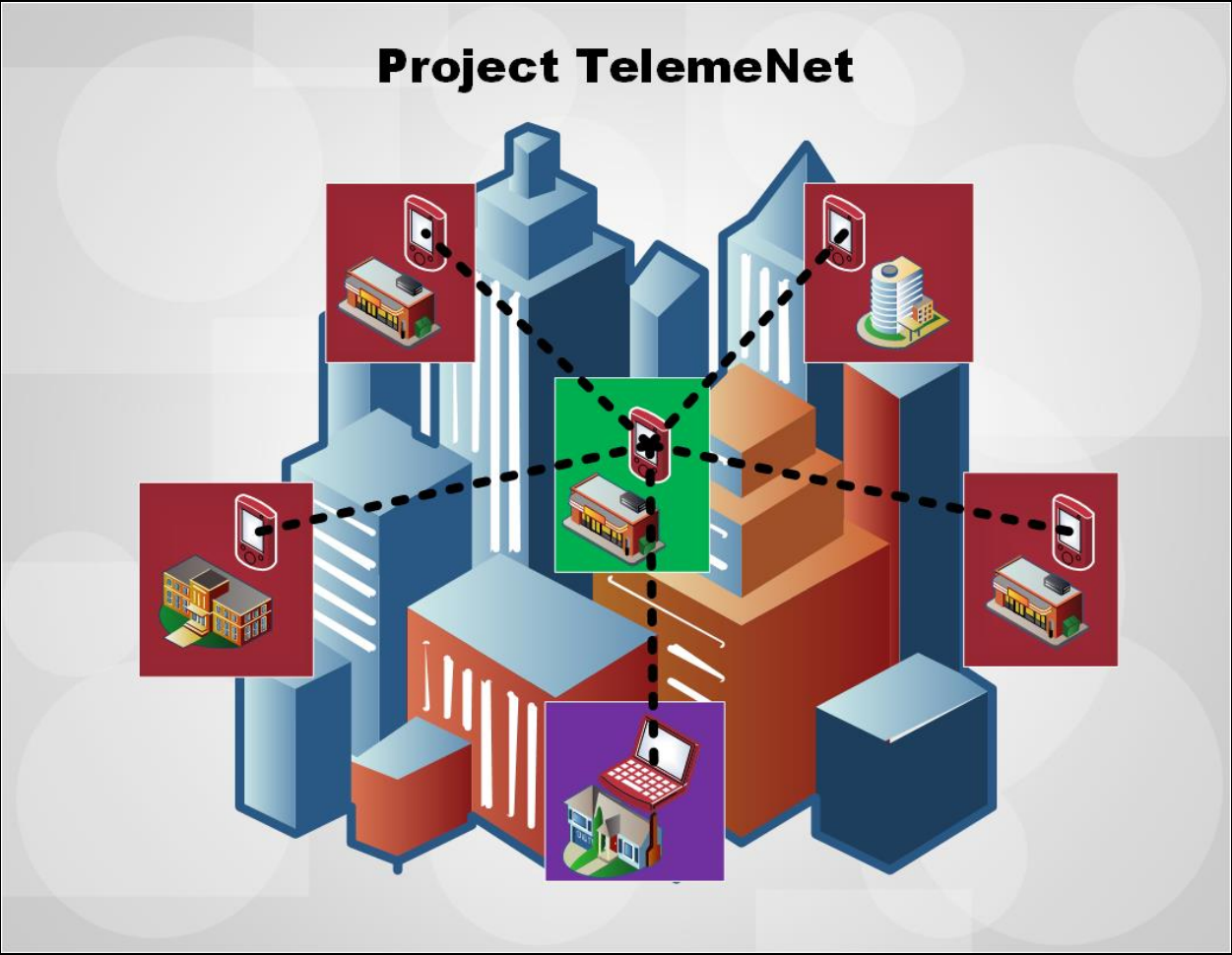
b. Create swap partition.

c. Create /home partition if wanted.

02) Install Linux with FDE.

03) Run BASEC scripts, excluding Machamp.

PROJECT TELEMENET



PROJECT TELEMENET is an advanced project to obfuscate geolocation data on public accounts others are aware exists. The goal is to make it difficult for attackers to commit digital reconnaissance against you and obtain your geolocation data when their user accounts' privacy settings fail and your VPNs are exploited (like NSA with WebRTC). This projects only works if you live in a large city, can make deals with local coffee shops to use their free Wi-Fi, and are using a small, reasonable amount of accounts. You really shouldn’t have any public account that others know exists like social media.

01) Purchase multiple Rasberry Pis.

02) Configure bots to use public, disposable accounts.

03) Configure bots to mimic user behavior.

04) Harden RPis.

05) Set RPis on public networks. Make deals with network owners where applicable. For example, local coffee shops are willing if you give them your business.

06) Hide RPis at locations using public networks.

07) Configure RPis to speak to central RPi so public accounts are traded to each other scrambling geolocation data and existence of RPis.

08) Add own PC to TelemeNet if wanted. Not advised. Instead, I advise obtaining a Librem laptop for public use and checking the RPis remotely from a public network or visiting each location to check RPis manually.